

Chapitre IV

Structures algébriques usuelles

Table des matières

Rappels de Sup' sur les groupes	3
1. Structure de groupe	3
2. Sous-groupes	6
3. Morphismes de groupes	7
Partie A : Compléments sur les groupes	16
1. Sous-groupe engendré par une partie	16
2. Les sous-groupes de $\mathbb{Z}$	24
3. Le groupe $\mathbb{Z}/n\mathbb{Z}$	26
4. Groupes monogènes	32
5. Ordre d'un élément	38
Rappels de Sup' sur les anneaux	43
1. Structure d'anneau	43
2. Sous-anneaux	44
3. Inversibles d'un anneau	46
4. Morphismes d'anneaux	47
Partie B : Compléments sur les anneaux ; idéaux	50
1. Structure d'anneau produit	50
2. Idéaux d'un anneau commutatif	51
3. Divisibilité, PGCD et PPCM	57
Partie C : Anneaux $\mathbb{Z}/n\mathbb{Z}$ et arithmétique des entiers	63
1. Idéaux de $\mathbb{Z}$ et PGCD	63
2. Anneaux $\mathbb{Z}/n\mathbb{Z}$	64
3. Applications à l'arithmétique des entiers	66
Partie D : Anneaux de polynômes	73
1. Propriétés arithmétiques élémentaires	73
2. Idéaux de $\mathbb{K}[X]$	76
3. Propriétés relatives au PGCD	77
4. Décomposition d'un polynôme en facteurs irréductibles	78
Partie E : Algèbres	82
1. Structure d'algèbre	82
2. Sous-algèbres	82
3. Morphismes d'algèbres	85
4. Algèbres et polynômes	86
5. Norme d'algèbre	93

Partie *

Rappels de Sup' sur les groupes

Cette partie a été vue en classe de Sup' et n'est présente dans ce cours qu'à titre de révisions. *Le lecteur pourra faire les exercices de cette partie pour s'assurer de bien maîtriser ses bases !*

1. Structure de groupe

Définition *1. Groupe

Soit G un ensemble et $*$ une loi de composition interne sur G . On dit que le couple $(G, *)$ est **une structure de groupe**, ou plus simplement G est un **groupe** (muni de la loi $*$), si :

i) *Associativité* : $\forall x, y, z \in G$,

$$(x * y) * z = x * (y * z);$$

ii) *Élément neutre* : $\exists e \in G, \forall x \in G$,

$$e * x = x = x * e;$$

iii) *Symétrique* : $\forall x \in G, \exists y \in G$,

$$x * y = e = y * x.$$

On dit de plus qu'un groupe G est **commutatif** si :

iv) *Commutativité* : $\forall x, y \in G$,

$$x * y = y * x.$$

On appelle **ordre** d'un groupe G , son cardinal qu'on note usuellement de plus façon : $|G|$ ou $\#G$ ou encore $\text{Card}(G)$.

Remarque *1.

On rappelle deux des principales notations pour la loi d'un groupe :

- La notation additive $(G, +)$ qui est utilisée exclusivement dans le cas commutatif. Dans ce cas, l'élément neutre est noté 0 et le symétrique de $x \in G$ est noté $-x$.
- La notation multiplicative $(G, \cdot)$ (ou $(G, \times)$) qui peut s'employer dans les cas commutatifs ou non. Dans ce cas, l'élément neutre est souvent noté e ou 1 et le symétrique de $x \in G$ est noté x^{-1} .

Exemple *1.

- Les ensembles de nombres suivants munis de l'addition sont des groupes : $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- Les ensembles de nombres suivants munis de la multiplication sont des groupes : $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{C}^*, \mathbb{U}, \mathbb{U}_n$ (pour $n \in \mathbb{N}^*$).

On utilise ici les notations :

$$\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\} \quad \text{et pour } n \in \mathbb{N}^*, \quad \mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

- Pour X un ensemble, l'ensemble $\mathcal{S}_X$ des permutations de X (i.e. des bijections de X dans X) est un groupe pour la composition. Ce groupe est appelé groupe **symétrique** de X ou encore groupe **des permutations** de X .
- Pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et $n \in \mathbb{N}^*$, L'ensemble $GL_n(\mathbb{K})$ des matrices inversibles est un groupe pour le produit matriciel.
- Pour $n \in \mathbb{N}^*$, l'ensemble $O_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid {}^tMM = I_n\}$ des matrices orthogonales est un groupe pour le produit matriciel.

Exercice *1.

1. Déterminer, pour chaque groupe G parmi ceux de l'exemple précédent, l'élément neutre de G , le symétrique d'un élément dans G , si G est commutatif et l'ordre de G .
2. Les ensembles munis des lois suivantes sont-ils des groupes ? $(\mathbb{N}, +)$, $(\mathbb{Z}, \times)$, $(SL_n(\mathbb{R}), \times)$, $(GL_n(\mathbb{R}), +)$.

Correction.

1. — Pour $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis de l'addition : l'élément neutre est 0 ; le symétrique de x est son opposé $-x$; ils sont tous commutatifs et sont d'ordre infini.
- Pour $\mathbb{Q}^*, \mathbb{Q}_+^*, \mathbb{R}^*, \mathbb{R}_+^*, \mathbb{C}^*, \mathbb{U}, \mathbb{U}_n$ munis de la multiplication : l'élément neutre est 1 ; le symétrique de x est son inverse $\frac{1}{x}$; ils sont tous commutatifs et sont tous d'ordre infini sauf $\mathbb{U}_n$ qui est d'ordre n .
- Pour $\mathcal{S}_X$ muni de la composition : l'élément neutre est l'application identité $\text{id} : x \mapsto x$; le symétrique de σ est son application réciproque σ^{-1} . En général, $(\mathcal{S}_X, \circ)$ n'est pas commutatif.
De plus, $\mathcal{S}_X$ est d'ordre infini si X est infini (il y a une infinité de transpositions par exemple) et est d'ordre $n!$ si $\#X = n$.

Exercice pour le lecteur : montrer que $(\mathcal{S}_X, \circ)$ est commutatif si, et seulement si, X contient 1 ou 2 éléments.

Indication : Déterminer $\mathcal{S}_X$ pour $X = \{1\}, \{1, 2\}$ et $\{1, 2, 3\}$ et écrire leurs tables d'opérations.

- Pour $GL_n(\mathbb{K})$ et $O_n(\mathbb{R})$ munis de la multiplication matricielle : l'élément neutre est la matrice identité I_n ; le symétrique de M est sa matrice inverse M^{-1} . Si $n \geq 2$, ils ne sont pas commutatifs.
Ces groupes sont infinis sauf $O_1(\mathbb{R})$ qui est d'ordre 2.

2.

Exercice *2.

Soit $(G, \cdot)$ un groupe et $g \in G$. Alors les applications φ_g et ψ_g de G dans G telles que

$$\varphi_g : x \mapsto gx \quad \text{et} \quad \psi_g : x \mapsto xg$$

sont bijectives.

Correction.

Soit $x, y \in G$ tel que $\varphi_g(x) = \varphi_g(y)$. Alors $g^{-1}gx = g^{-1}gy$, donc $x = ex = ey = y$. Par suite, φ_g est injective.

Soit $y \in G$. Alors $\varphi_g(g^{-1}y) = gg^{-1}y = ey = y$. Donc y possède un antécédent par φ_g . Par suite, φ_g est surjective.

Il en résulte que φ_g est bijective.

On emploie un raisonnement similaire pour ψ_g .

Proposition *1. Structure de groupe produit

Soit $(G_1, \cdot), (G_2, \cdot)$ des groupes et on note $G = G_1 \times G_2$. On considère la loi de composition suivante sur G : pour $(x_1, x_2), (y_1, y_2) \in G$,

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1 \cdot y_1, x_2 \cdot y_2).$$

L'ensemble G muni de cette loi est un groupe et :

- L'élément neutre de G est $e = (e_1, e_2)$ où e_1 est l'élément neutre de G_1 et e_2 l'élément neutre de G_2 .
- Le symétrique de $(x_1, x_2) \in G$, est (x_1^{-1}, x_2^{-1}) .

Démonstration.

Pour tous $x_1, y_1 \in G_1$ et $x_2, y_2 \in G_2$, $x_1, y_1 \in G_1$ et $(x_2, y_2) \in G_2$ donc $(x_1 y_1, x_2 y_2) \in G_1 \times G_2$. Donc $\cdot$ est bien une loi de composition interne.

De plus, par associativité des lois sur G_1 et G_2 , la loi $\cdot$ est associative.

Soit $(x_1, x_2) \in G$.

— Élément neutre : on a

$$(x_1, x_2) \cdot (e_1, e_2) = (x_1 e_1, x_2 e_2) = (x_1, x_2) = (e_1 x_1, e_2 x_2) = (e_1, e_2) \cdot (x_1, x_2);$$

donc $e = (e_1, e_2)$ est un élément neutre pour la loi $\cdot$.

— Symétrique : on a

$$(x_1, x_2) \cdot (x_1^{-1}, x_2^{-1}) = (x_1 x_1^{-1}, x_2 x_2^{-1}) = (e_1, e_2) = (x_1^{-1} x_1, x_2^{-1} x_2) = (x_1^{-1}, x_2^{-1}) \cdot (x_1, x_2);$$

donc (x_1^{-1}, x_2^{-1}) est le symétrique de (x_1, x_2) pour la loi $\cdot$.

Il en résulte que G est un groupe. □

Remarque *2.

Par récurrence, on peut ainsi munir un produit fini de groupes d'une structure de groupe.

Exercice *3.

Montrer que $G = G_1 \times G_2$ est commutatif si, et seulement si, G_1 et G_2 sont commutatifs.

Correction.

Soit $x_1, y_1 \in G_1, x_2, y_2 \in G_2$. On a :

$$(x_1, x_2) \cdot (y_1, y_2) = (y_1, y_2) \cdot (x_1, x_2),$$

si, et seulement si,

$$(x_1 x_2, y_1 y_2) = (x_2 x_1, y_2 y_1),$$

si, et seulement si,

$$x_1 x_2 = x_2 x_1 \quad \text{et} \quad y_1 y_2 = y_2 y_1.$$

2. Sous-groupes**a. Généralités****Définition *2.** Sous-groupe

Soit G un groupe et $H \subset G$. On dit que H est un sous-groupe de G si :

- H est non vide ;
- pour tous $x, y \in H, x.y \in H$;
- pour $x \in H, x^{-1} \in H$.

Proposition *2. Caractérisation des sous-groupes

Soit G un groupe et $H \subset G$. L'ensemble H est un sous-groupe de G , si, et seulement si :

- i) L'élément neutre e de G appartient à H ;
- ii) pour tous $x, y \in H, x.y^{-1} \in H$.

Démonstration.

- ($\Rightarrow$). On suppose que H est un sous-groupe de G . Alors,
 - i) H est non vide, donc il existe $x \in H$, et d'après les hypothèses, $x^{-1} \in H$. Par suite, $e = x.x^{-1} \in H$.
 - ii) Pour tous $x, y \in H, y^{-1} \in H$ d'après les hypothèses, donc

$$x.y^{-1} \in H.$$

- ($\Leftarrow$). On suppose i) et ii) vérifiés. Alors
 - H est non vide, car $e \in H$.
 - Soit $x \in H$. Alors d'après i) et ii),

$$x^{-1} = e.x^{-1} \in H.$$

- Soit $x, y \in H$. Alors $y^{-1} \in H$ d'après ce qui précède et $y = (y^{-1})^{-1}$, donc, d'après ii)

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

Il en résulte que H est un sous-groupe de G .

□

Exemple *2.

- Si G est un groupe, $\{e\}$ et G sont des sous-groupes de G . On les appelle les sous-groupes triviaux de G .
- La chaîne d'inclusions suivante est également une chaîne de sous-groupes :

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

- Soit $n \in \mathbb{N}^*$. $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$.
- Soit $n \in \mathbb{N}^*$. $O_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.

3. Morphismes de groupes

a. Définition

Définition *3. Morphisme de groupes

Soit $(G_1, *)$, $(G_2, \star)$ des groupes et $f : G_1 \rightarrow G_2$.

On dit que f est un **morphisme de groupes** si, pour tous $x, y \in G_1$:

$$f(x * y) = f(x) \star f(y).$$

Exemple *3.

- L'exponentielle est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.
- Soit $n \in \mathbb{N}^*$. Le déterminant est un morphisme de groupes de $(GL_n(\mathbb{K}), \times)$ dans $(\mathbb{K}^*, \times)$.
- Soit $n \in \mathbb{N}^*$. La signature ε est un morphisme de groupes de $(\mathcal{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$

Exercice *4.

Soit $n \in \mathbb{N}^*$. Montrer que l'application $\text{com} : M \mapsto \text{com}(M)$ est un morphisme de $(GL_n(\mathbb{K}), \times)$ dans lui-même.

Correction.

Pour $M \in GL_n(\mathbb{K})$, on a $M^{-1} = \frac{1}{\det(M)} {}^t \text{com}(M)$, donc

$$\text{com}(M) = \det(M) \cdot {}^t(M^{-1}) \in GL_n(\mathbb{K}).$$

Ainsi, com est une application de $GL_n(\mathbb{K})$ dans lui-même.

Soit $M, N \in GL_n(\mathbb{K})$. On a, par propriétés du déterminant, de la transposée et de l'inverse d'un produit :

$$\begin{aligned}
\text{com}(MN) &= \det(MN) {}^t(MN)^{-1} \\
&= \det(M) \det(N) {}^t(N^{-1} M^{-1}) \\
&= \det(M) {}^t(M^{-1}) \det(N) {}^t(N^{-1}) \\
\text{com}(MN) &= \text{com}(M) \text{com}(N).
\end{aligned}$$

Par suite, $\text{com} : M \mapsto \text{com}(M)$ est un morphisme de $(GL_n(\mathbb{K}), \times)$ dans lui-même.

Exercice *5.

Soit $n \in \mathbb{N}$. Montrer que l'application $\varphi : \begin{cases} \mathbb{Z} & \rightarrow \mathbb{C}^* \\ k & \mapsto e^{i \frac{2k\pi}{n}} \end{cases}$ est un morphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{C}^*, \times)$.

Correction.

Soit $k, k' \in \mathbb{Z}$. Alors

$$\varphi(k + k') = e^{i \frac{2(k+k')\pi}{n}} = e^{i \frac{2k\pi}{n}} e^{i \frac{2k'\pi}{n}} = \varphi(k) \varphi(k').$$

Donc φ est un morphisme de groupes.

b. Noyau, Image et sous-groupes

Définition *4. Noyau, Image d'un morphisme de groupes

Soit G_1, G_2 des groupes d'éléments neutres respectifs e_1, e_2 et $f : G_1 \rightarrow G_2$ un morphisme de groupes.

- On appelle **noyau de f** l'ensemble $\text{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\}$.
- On appelle **image de f** l'ensemble $\text{Im}(f) = f(G_1) = \{f(x) \mid x \in G_1\}$.

Lemme *1.

Soit G_1, G_2 des groupes d'éléments neutres respectifs e_1, e_2 et $f : G_1 \rightarrow G_2$ un morphisme de groupes. On a :

$$f(e_1) = e_2; \quad \forall x \in G_1, f(x^{-1}) = f(x)^{-1} \text{ et } \forall x \in G_1, \forall n \in \mathbb{N}^*, f(x^n) = f(x)^n.$$

Démonstration.

Soit $x \in G_1$.

- On a, $f(e_1)f(e_1) = f(e_1e_1) = f(e_1) = f(e_1)e_2$. Donc, en composant à gauche cette égalité par $(f(e_1))^{-1}$, on obtient le résultat :

$$f(e_1) = e_2.$$

- On a $f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2$, donc en composant à droite cette égalité par $(f(x))^{-1}$, on obtient le résultat :

$$f(x^{-1}) = f(x)^{-1}.$$

- On raisonne par récurrence sur $n \in \mathbb{N}^*$.

Initialisation : On $f(x^1) = f(x) = f(x)^1$.

Hérédité : Soit $n \in \mathbb{N}^*$. On suppose que $f(x^n) = f(x)^n$. Alors on a :

$$f(x^{n+1}) = f(x^n x) = f(x^n)f(x) = f(x)^n f(x) = f(x)^{n+1}.$$

Ce qui achève le raisonnement par récurrence.

Il en résulte que, pour tout $n \in \mathbb{N}^*$,

$$f(x^n) = f(x)^n.$$

□

Proposition *3.

Soit G_1, G_2 des groupes, H_1, H_2 des sous-groupes de G_1, G_2 respectivement et $f : G_1 \rightarrow G_2$ un morphisme de groupes. On a :

- l'ensemble $f^{-1}(H_2)$ est un sous-groupe de G_1 ;
- l'ensemble $f(H_1)$ est un sous-groupe de G_2 .

Démonstration.

- i) On a $f(e_1) = e_2 \in H_2$, donc $e_1 \in f^{-1}(H_2)$.
- ii) Soit $x, y \in f^{-1}(H_2)$. Montrons que $xy^{-1} \in f^{-1}(H_2)$. On a :

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in H_2,$$

car $f(x), f(y) \in H_2$ et H_2 est un sous-groupe. Donc $xy^{-1} \in f^{-1}(H_2)$.

Il en résulte que $f^{-1}(H_2)$ est un sous-groupe de G_1 .

- i) On a $e_1 \in H_1$ et $f(e_1) = e_2$, donc $e_2 \in f(H_1)$.
- ii) Soit $x, y \in f(H_1)$. Montrons que $xy^{-1} \in f(H_1)$. Il existe $z, t \in H_1$ tels que $x = f(z)$ et $y = f(t)$. On a alors :

$$xy^{-1} = f(z)f(t)^{-1} = f(z)f(t^{-1}) = f(zf(t^{-1})) \in f(H_1)$$

car $z, t \in H_2$ et H_2 est un sous-groupe. Donc $xy^{-1} \in f(H_1)$.
Il en résulte que $f(H_1)$ est un sous-groupe de G_2 . □

Corollaire *1.

Soit G_1, G_2 des groupes et $f : G_1 \rightarrow G_2$ un morphisme de groupes. On a :

- l'ensemble $\text{Ker}(f)$ est un sous-groupe de G_1 ;
- l'ensemble $\text{Im}(f)$ est un sous-groupe de G_2 .

Démonstration.

— On a :

$$\text{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\});$$

Or $\{e_2\}$ est un sous-groupe de G_2 , donc, d'après la proposition précédente, $\text{Ker}(f)$ est un sous-groupe de G_1 comme image réciproque d'un sous-groupe par un morphisme de groupes.

— On a :

$$\text{Im}(f) = f(G_1);$$

Or G_1 est un sous-groupe de G_1 , donc, d'après la proposition précédente, $\text{Im}(f)$ est un sous-groupe de G_2 comme image directe d'un sous-groupe par un morphisme de groupes. □

Proposition *4.

Soit G_1, G_2 des groupes et $f : G_1 \rightarrow G_2$ un morphisme de groupes. On note e_1 l'élément neutre de G_1 .

L'application f est injective si, et seulement si, $\text{Ker}(f) = \{e_1\}$.

Démonstration.

- ($\Rightarrow$). On suppose f injective. Soit $x \in \text{Ker}(f)$. Alors $f(x) = e_2 = f(e_1)$. Par injectivité de f , il en résulte que $x = e_1$. Par suite, $\text{Ker}(f) = \{e_1\}$.
- ($\Leftarrow$). On suppose $\text{Ker}(f) = \{e_1\}$. Soit $x, x' \in G_1$ tels que $f(x) = f(x')$. Alors on a :

$$f(xx'^{-1}) = f(x)f(x'^{-1}) = f(x)f(x')^{-1} = e_2,$$

donc $xx'^{-1} \in \text{Ker}(f) = \{e_1\}$; d'où $xx'^{-1} = e_1$. Par suite $x = x'$.
Il en résulte que f est injective. □

Exemple *4.

- Soit $n \in \mathbb{N}^*$. L'application $z \mapsto z^n$ de $\mathbb{C}^*$ dans $\mathbb{C}^*$ est un morphisme de groupes surjectif et son noyau est $\mathbb{U}_n$.

En effet : soit $z, z' \in \mathbb{C}^*$. On note $f : z \mapsto z^n$. Alors :

$$f(zz') = (zz')^n = z^n z'^n = f(z)f(z'),$$

car la multiplication sur $\mathbb{C}^*$ est commutative. Donc f est un morphisme de groupes.

De plus, pour $\zeta = re^{i\theta} \in \mathbb{C}^*$, $z = r^{\frac{1}{n}} e^{i\frac{\theta}{n}}$ est un antécédent de ζ par f . Donc f est surjective de $\mathbb{C}^*$ dans lui-même.

- Le groupe spécial orthogonal $SO_n(\mathbb{R})$ des matrices orthogonales de déterminant 1 est un sous-groupe de $O_n(\mathbb{R})$: il est l'image réciproque de $\{1\}$ par le morphisme de groupes $\det : O_n(\mathbb{R}) \rightarrow \mathbb{R}^*$.

Exercice *6.

Montrer que $\exp : z \mapsto e^z$ est un morphisme de groupes surjectif de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$ et déterminer son noyau.

Remarque : on définira "proprement" l'exponentielle complexe dans le chapitre dédié aux séries entières. Pour cet exercice, on prendra la définition de $\exp$ et ses propriétés vues en Sup', à savoir : $\exp(0) = 1$ et pour $z = re^{i\theta} \in \mathbb{C}^*$, $\exp(z) = e^r e^{i\theta}$ où e^r est l'exponentielle réelle de r et $e^{i\theta} = \cos(\theta) + i \sin(\theta)$.

Correction.

Soit $z, z' \in \mathbb{C}$. On a $|e^z| = e^{\operatorname{Re} z} > 0$ donc $e^z \in \mathbb{C}^*$ et $\exp(z + z') = \exp(z)\exp(z')$. Donc $\exp$ est un morphisme de groupes de $(\mathbb{C}, +)$ dans $(\mathbb{C}^*, \times)$.

Image : Pour $\zeta = re^{i\theta} \in \mathbb{C}^*$ avec $r \in \mathbb{R}_+^*$ et $\theta \in [0, 2\pi[$, $z = \ln(r) + i\theta$ est un antécédent de ζ par $\exp$. Par suite, $\operatorname{Im}(\exp) = \mathbb{C}^*$. Il en résulte que $\exp$ est surjective de $\mathbb{C}$ dans $\mathbb{C}^*$.

Noyau : On a $z = x + iy \in \operatorname{Ker}(\exp)$ si, et seulement si, $e^x e^{iy} = e^z = 1$. Par suite, $x = 0$ (car $e^x = |e^z| = 1$) et $y \in \{2k\pi \mid k \in \mathbb{Z}\}$. (Et réciproquement, un élément de cette forme est dans le noyau).

Il en résulte que $\operatorname{Ker}(\exp) = \{i2k\pi \mid k \in \mathbb{Z}\}$.

Exercice *7.

Soit $n \in \mathbb{N}^*$. On note :

$$SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid \det(M) = 1\}$$

Montrer que $SL_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.

Correction.

Pour tous $A, B \in M_n(\mathbb{R})$, on a $\det(AB) = \det(A)\det(B)$, donc l'application $\det$ restreinte à $GL_n(\mathbb{R})$ est un morphisme de groupes de $GL_n(\mathbb{R})$ dans $\mathbb{R}^*$. De plus, on remarque que $SL_n(\mathbb{R}) = \text{Ker}(\det)$ donc $SL_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$ comme noyau d'un morphisme de groupes.

c. Isomorphismes de groupes

Définition *5. Isomorphisme de groupes

Soit G_1, G_2 des groupes et $f : G_1 \rightarrow G_2$. Si f est un morphisme de groupes bijectif, on dit que f est un **isomorphisme de groupes**.

Si f est un isomorphisme de groupes et $G_1 = G_2$, on dit que f est un **automorphisme de groupes**. On note $\text{Aut}(G)$ l'ensemble des automorphismes de G .

Exemple *5.

- L'exponentielle est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

On a montré précédemment que $\exp$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$ et de plus $\exp$ est bijective de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$ de réciproque $\ln$.
Donc $\exp$ est un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

- Soit G un groupe et $g \in G$. L'application $x \mapsto gxg^{-1}$ est un automorphisme de G (on appelle automorphismes intérieurs de G de telles applications).

Soit $g \in G$. Notons $f_g : x \mapsto gxg^{-1}$.

Morphisme : Soit $x, x' \in G$. On a :

$$f_g(xx') = g^{-1}xx'g = g^{-1}xgg^{-1}x'g = f_g(x)f_g(x').$$

Image : On a, pour tout $y \in G$, $y = gg^{-1}ygg^{-1} = f_g(g^{-1}yg)$; d'où $x = g^{-1}yg$ est un antécédent de y par f_g . Par suite, f_g est surjective de G dans G .

Noyau : Soit $x \in \text{Ker}(f_g)$. Alors $g^{-1}xg = f_g(x) = e$, donc, en composant cette égalité à gauche par g et à droite par g^{-1} , on obtient $x = e$. Par suite, f_g est injective.

Proposition *5.

Soit G_1, G_2 des groupes et $f : G_1 \rightarrow G_2$. Si f est un isomorphisme, alors f^{-1} est également un isomorphisme de groupes.

Démonstration.

On suppose que f est un isomorphisme. Alors f^{-1} existe et est bijective de G_2 dans G_1 . Montrons que, de plus, f^{-1} est un morphisme de groupes.

Soit $y, y' \in G_2$. Comme f est bijective, il existe $x, x' \in G_1$ tels que $y = f(x)$, $y' = f(x')$ et $x = f^{-1}(y)$, $x' = f^{-1}(y')$. On a :

$$f^{-1}(yy') = f^{-1}(f(x)f(x')) = f^{-1}(f(xx')) = xx' = f^{-1}(y)f^{-1}(y').$$

Donc f^{-1} est un morphisme de groupes.

Il en résulte que f^{-1} est un isomorphisme de groupes. $\square$

Exemple *6.

Le logarithme népérien est un isomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

On a montré dans les exercices précédents que $\exp$ est un isomorphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$. Or $\ln$ est la réciproque de cette fonction, donc, d'après la proposition précédente $\ln$ est un isomorphisme de groupes.

Exercice *8. Théorème de Cayley

1. Soit G un groupe. On considère $\mathcal{S}_G$ le groupe symétrique de G (groupe des permutations de G). On note φ l'application de G dans $\mathcal{F}(G, G)$ (ensemble des fonctions de G dans G) telle que, pour tout $g \in G$, $\varphi(g) : x \mapsto g.x$.
 - (a) Montrer que $\text{Im}(\varphi) \subset \mathcal{S}_G$.
 - (b) Montrer que φ est un morphisme injectif de G dans $\mathcal{S}_G$.
2. En déduire le résultat suivant :

Théorème de Cayley

Tout groupe est isomorphe à un sous-groupe d'un groupe symétrique.

Correction.

1. (a) D'après l'exercice *2, pour tout $g \in G$, $\varphi(g)$ est une bijection de G dans G i.e. $\varphi(g) \in \mathcal{S}_G$. D'où $\text{Im}(\varphi) \subset \mathcal{S}_G$.
(b) Montrons que φ est un morphisme de groupes de $(G, \cdot)$ dans $(\mathcal{S}_G, \circ)$. Soit $g, g' \in G$. On a, pour tout $x \in G$:

$$\begin{aligned}\varphi(g.g')(x) &= (g.g').x \\ &= g.(g'.x) \text{ par associativité de } \cdot \\ &= g.\varphi(g')(x) = \varphi(g)(\varphi(g')(x)) \\ \varphi(g.g')(x) &= (\varphi(g) \circ \varphi(g'))(x)\end{aligned}$$

et donc $\varphi(g.g')(x) = \varphi(g) \circ \varphi(g')$.

Ainsi, φ est un morphisme de G dans $\mathcal{S}_G$.

Montrons son injectivité. Soit $g \in \text{Ker}(\varphi)$. Alors $\varphi(g) = \text{id}$. Ainsi, on a :

$$g = g.e = \varphi(g)(e) = \text{id}(e) = e.$$

Par suite, $\text{Ker}(\varphi) = \{e\}$ et donc φ est injective.

2. Soit G un groupe. D'après la question précédente, l'application φ est un morphisme injectif de G dans $\mathcal{S}_G$ groupe symétrique de G donc φ est un isomorphisme de G dans le sous-groupe $\text{Im}(\varphi)$ de $\mathcal{S}_G$.

Exercice *9.

Soit G un groupe et $\text{Aut}(G)$ l'ensemble des automorphismes de G .

1. Montrer que, muni de la composition des applications, $\text{Aut}(G)$ est un groupe.
2. On note $\text{Int}(G) = \{\psi_g : x \mapsto gxg^{-1} \mid g \in G\}$. Montrer que $\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.

Correction.

1. — 1ère façon (si on se rappelle du groupe symétrique de G noté $\mathcal{S}_G$) : montrons que $\text{Aut}(G)$ est un sous-groupe de $(\mathcal{S}_G, \circ)$.

On a bien $\text{Aut}(G) \subset \mathcal{S}_G$ car tout automorphisme de G est en particulier une application bijective de G dans G .

L'élément neutre Id_G de $(\mathcal{S}_G, \circ)$ est bien un automorphisme : comme il est dans $\mathcal{S}_G$, il est bijectif de G dans G et pour tout $x, x' \in G$, $\text{Id}_G(xx') = xx' = \text{Id}_G(x)\text{Id}_G(x')$ donc c'est un morphisme de groupes.

De plus, pour tous $\varphi, \psi \in \text{Aut}(G)$, ψ^{-1} est un automorphisme d'après la proposition précédente et on a, pour $g, g' \in G$:

$$\begin{aligned} \varphi \circ \psi^{-1}(gg') &= \varphi(\psi^{-1}(gg')) \\ &= \varphi(\psi^{-1}(g).\psi^{-1}(g')) \\ &= \varphi(\psi^{-1}(g)).\varphi(\psi^{-1}(g')) \\ &= \varphi \circ \psi^{-1}(g).\varphi \circ \psi^{-1}(g'). \end{aligned}$$

Donc $\varphi \circ \psi^{-1}$ appartient à $\text{Aut}(G)$.

Par suite, $\text{Aut}(G)$ est un sous-groupe de $(\mathcal{S}_G, \circ)$ et c'est donc un groupe.

- 2ème façon (si on ne se rappelle pas du groupe symétrique de G) : montrons le avec la définition !

Soit $\varphi, \psi \in \text{Aut}(G)$. Alors $\varphi \circ \psi : G \rightarrow G$ est bijective comme composée d'applications bijectives et on a, pour $g, g' \in G$:

$$\varphi \circ \psi(gg') = \varphi(\psi(gg')) = \varphi(\psi(g).\psi(g')) = \varphi(\psi(g)).\varphi(\psi(g')) = \varphi \circ \psi(g).\varphi \circ \psi(g').$$

Donc $\varphi \circ \psi$ appartient à $\text{Aut}(G)$.

Par suite, $\circ$ est une loi de composition interne sur $\text{Aut}(G)$. Elle est associative et d'élément neutre la fonction identité $\text{Id}_G : G \rightarrow G$. D'après la proposition précédente, si ψ est un automorphisme de G , alors ψ^{-1} l'est aussi, donc tout élément de $\text{Aut}(G)$ possède

un symétrique pour la loi $\circ$: il s'agit de sa réciproque.
Ainsi, $(\text{Aut}(G), \circ)$ est un groupe.

Question : au fait, est-il commutatif ?

2. Remarquons tout d'abord deux faits. Soit $g, g' \in G$.

- $\psi_g \circ \psi_{g'} = \psi_{gg'}$. En effet, pour tout $x \in G$, on a :

$$\psi_g \circ \psi_{g'}(x) = \psi_g(g'xg'^{-1}) = g(g'xg'^{-1})g^{-1} = (gg')x(gg')^{-1} = \psi_{gg'}(x).$$

- $(\psi_g)^{-1} = \psi_{g^{-1}}$. En effet, pour tout $x \in G$, on a, d'après le point précédent :

$$\psi_g \circ \psi_{g^{-1}}(x) = \psi_e(x) = exe^{-1} = x = \text{id}(x);$$

et de même

$$\psi_{g^{-1}} \circ \psi_g(x) = \psi_e(x) = exe^{-1} = x = \text{id}(x).$$

Donc $\psi_{g^{-1}} = (\psi_g)^{-1}$.

Montrons alors que $\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.

- $\text{id} = \psi_e \in \text{Int}(G)$;
- Soit $\psi_g, \psi_{g'} \in \text{Int}(G)$ avec $g, g' \in G$. On a, d'après les remarques précédentes :

$$\psi_g \circ (\psi_{g'})^{-1} = \psi_g \circ \psi_{g'^{-1}} = \psi_{gg'^{-1}} \in \text{Int}(G).$$

Donc $\text{Int}(G)$ est un sous-groupe de $\text{Aut}(G)$.

Partie A

Compléments sur les groupes

1. Sous-groupe engendré par une partie

a. Définition

Proposition 1. *Intersection de sous-groupes*

Soit G un groupe et $(H_i)_{i \in I}$ une famille quelconque de sous-groupes de G . L'ensemble $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Autrement dit, une intersection quelconque de sous-groupes est un sous-groupe.

Démonstration.

On note $H = \bigcap_{i \in I} H_i$.

- i) On a, pour tout $i \in I$, $e \in H_i$ car H_i est un sous-groupe de G . Donc $e \in H$.
- ii) Soit $x, y \in H$. Alors, pour tout $i \in I$, $x, y \in H_i$ qui est un sous-groupe de G , donc, pour tout $i \in I$,

$$x.y^{-1} \in H_i.$$

Par suite, $x.y^{-1} \in H$.

Il en résulte que H est un sous-groupe de G . □

Question 1.

Que dire d'une réunion de sous-groupes ?

Réponse.

En général, une réunion de sous-groupes n'est pas un sous-groupe. Prendre par exemple les sous-groupes $i\mathbb{R}$ et $\mathbb{R}$ de $\mathbb{C}$.

Exercice : montrer qu'une réunion de deux sous-groupes est un sous-groupe si, et seulement si, l'un est inclus dans l'autre.

Par contre, si on prend strictement plus que deux sous-groupes, la caractérisation précédente ne tient plus : par exemple, le groupe $\{-1, 1\}^2$ est union de trois sous-groupes non inclus les uns dans les autres.

Définition-Proposition 1.

Soit G un groupe et $A \subset G$. On note $\langle A \rangle$ l'intersection de tous les sous-groupes de G contenant A , i.e.

$$\langle A \rangle = \bigcap_{H \in \mathcal{H}_A} H \quad \text{où } \mathcal{H}_A = \{H \text{ sous-groupe de } G \mid A \subset H\}.$$

L'ensemble $\langle A \rangle$ est le plus petit sous-groupe de G contenant A et on l'appelle le **sous-groupe engendré par A** .

Si de plus $\langle A \rangle = G$, on dit que A **engendre** G .

Démonstration.

Une intersection quelconque de sous-groupes de G est un sous-groupe de G , donc $\langle A \rangle = \bigcap_{H \in \mathcal{H}_A} H$ est un sous-groupe de G . De plus, pour tout $H \in \mathcal{H}_A$, $A \subset H$, donc $A \subset \bigcap_{H \in \mathcal{H}_A} H = \langle A \rangle$.

Montrons alors que $\langle A \rangle$ est le plus petit sous groupe contenant A .

Soit $K \in \mathcal{H}_A$. Alors $\langle A \rangle = \bigcap_{H \in \mathcal{H}_A} H \subset K$. Donc $\langle A \rangle$ est le plus petit sous groupe contenant A . $\square$

b. Propriétés et exemples

La proposition suivante permet de se faire une meilleure idée de la notion de sous-groupe engendré : on y montre que le sous-groupe engendré par une partie est l'ensemble des éléments du groupe qui s'écrivent comme la composition d'un nombre fini d'éléments ou de symétriques d'éléments de cette partie.

Proposition 2.

Soit G un groupe et $A \subset G$. On a :

$$\langle A \rangle = \{a_1 \dots a_n \mid n \in \mathbb{N}^*, a_1, \dots, a_n \in A \cup A^{-1} \cup \{e\}\}.$$

où $A^{-1} = \{a^{-1} \mid a \in A\}$.

Démonstration.

On note $E(A) = \{a_1 \dots a_n \mid n \in \mathbb{N}^*, a_1, \dots, a_n \in A \cup A^{-1} \cup \{e\}\}$. On procède par double inclusion pour montrer que $\langle A \rangle = E(A)$.

⊂ Pour cette inclusion, il suffit de montrer que $E(A)$ est un sous-groupe de G contenant A car $\langle A \rangle$ est le plus petit d'entre eux pour l'inclusion. Allons-y !

On remarque tout d'abord que $A \subset E(A)$; en effet, pour tout $a \in A$, $a \in A \cup A^{-1} \cup \{e\}$, donc $a \in E(A)$.

Montrons que $E(A)$ est un sous-groupe de G .

i) On a $e \in \{e\} \subset A \cup A^{-1} \cup \{e\}$ donc pour $n = 1$ et $a_1 = e$, on a $e = a_1 \in E(A)$.

ii) Soit $x, y \in E(A)$. Alors il existe $n, m \in \mathbb{N}^*$, $a_1, \dots, a_n, a'_1, \dots, a'_m \in A \cup A^{-1} \cup \{e\}$ tels que $x = a_1 \dots a_n$ et $y = a'_1 \dots a'_m$. Alors

$$\begin{aligned} xy^{-1} &= a_1 \dots a_n (a'_1 \dots a'_m)^{-1} \\ &= a_1 \dots a_n a'^{-1}_m \dots a'^{-1}_1 \\ &= a''_1 \dots a''_{n+m} \end{aligned}$$

où

$$a_i'' = \begin{cases} a_i \in A \cup A^{-1} \cup \{e\} & \text{si } i \in \llbracket 1, n \rrbracket; \\ a_{i-n}'^{-1} \in A \cup A^{-1} \cup \{e\} & \text{si } i \in \llbracket n+1, n+m \rrbracket. \end{cases}$$

Par suite $xy^{-1} \in E(A)$.

Il en résulte que $E(A)$ est un sous-groupe de G .

Ainsi, $\langle A \rangle$ étant le plus petit sous-groupe de G contenant A et $E(A)$ étant un sous-groupe de G contenant A , on a $\langle A \rangle \subset E(A)$.

⊃ Soit $x \in E(A)$ et H un sous-groupe de G contenant A . Alors il existe $n \in \mathbb{N}^*$ tel que $x = a_1 \dots a_n$ avec $a_1, \dots, a_n \in A \cup A^{-1} \cup \{e\} \subset H$ car H contient A et H est un sous-groupe de G . Comme H est stable par composition $x = a_1 \dots a_n \in H$.

Comme $\langle A \rangle$ est par définition l'intersection de tous les sous-groupes de G contenant A et chacun de ces sous-groupes contiennent $E(A)$ donc $E(A) \subset \langle A \rangle$.

Il en résulte que $E(A) = \langle A \rangle$. □

Remarque 1.

Par mesure de simplicité, pour G un groupe et $x \in G$, on notera $\langle x \rangle$ en lieu et place de $\langle \{x\} \rangle$ pour désigner le sous-groupe engendré par le singleton $\{x\}$.

Proposition 3.

Soit $(G, .)$ un groupe et $x \in G$. On a :

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}.$$

Démonstration.

On montre directement cette proposition mais on aura pu bien-sûr utiliser la proposition 2 pour conclure plus efficacement.

Montrons que $E(x) = \{x^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de G . Comme G est un groupe, $E(x) \subset G$; de plus :

- i) $e = x^0 \in E(x)$;
- ii) Soit $y, z \in E(x)$. Alors il existe $k, k' \in \mathbb{Z}$ tels que $y = x^k$ et $z = x^{k'}$, et on a :

$$yz^{-1} = x^k x^{-k'} = x^{k-k'} \in E(x).$$

Donc $E(x)$ est un sous-groupe de G et il contient $\{x\}$: en effet, $x = x^1 \in E(x)$.

Par suite, $\langle x \rangle \subset E(x)$.

Réciproquement : soit $y \in E(x)$. Alors il existe $k \in \mathbb{Z}$ tel que $y = x^k$. Or $\langle x \rangle$ est un sous-groupe de G et $x \in \langle x \rangle$, donc $y = x^k \in \langle x \rangle$. Ainsi, $E(x) \subset \langle x \rangle$.

Il en résulte que $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. □

Remarque 2.

Attention, pour la notation additive $(G, +)$, cette égalité devient :

$$\langle x \rangle = \{kx \mid k \in \mathbb{Z}\}.$$

Exemple 1.

1. Dans un groupe G d'élément neutre e , on a $\langle \emptyset \rangle = \{e\} = \langle e \rangle$ et $\langle G \rangle = G$.
2. Dans $(\mathbb{C}^*, \times)$, pour $n \in \mathbb{N}^*$, $\langle e^{i\frac{2\pi}{n}} \rangle = \mathbb{U}_n$.
3. Dans $(\mathbb{Z}, +)$, pour $n \in \mathbb{Z}$, on a $\langle n \rangle = n\mathbb{Z}$.
En particulier, $\mathbb{Z}$ est engendré par $\{1\}$, i.e. $\mathbb{Z} = \langle 1 \rangle$;
4. Dans $(\mathbb{C}, +)$, $\langle \{1, i\} \rangle = \mathbb{Z}[i]$ où $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (couramment appelé *ensemble des entiers de Gauss*).
5. Soit $n \in \mathbb{N}^*$. Le groupe $(\mathcal{S}_n, \circ)$ des permutations de $\llbracket 1, n \rrbracket$ est engendré par l'ensemble des transpositions.
6. Soit $n \in \mathbb{N}^*$. Le groupes $(GL_n(\mathbb{K}), \times)$ est engendré par l'ensemble des dilatations et des transvections.

1. Soit G un groupe d'élément neutre e .
Alors $\langle \emptyset \rangle$ est un sous-groupe de G donc $\{e\} \subset \langle \emptyset \rangle$ et $\{e\}$ est un sous-groupe de G contenant $\emptyset$ donc, $\langle \emptyset \rangle$ étant le plus petit sous-groupe contenant $\emptyset$, on a $\langle \emptyset \rangle = \{e\}$.
Il suffit de remplacer $\emptyset$ par $\{e\}$ dans le raisonnement précédent pour obtenir $\langle e \rangle = \{e\}$.
De plus, on a $G \subset \langle G \rangle \subset G$ donc $\langle G \rangle = G$.

2. Considérons le groupe $(\mathbb{C}^*, \times)$. Soit $n \in \mathbb{N}^*$. Alors :

$$\langle e^{i\frac{2\pi}{n}} \rangle = \{e^{i\frac{2k\pi}{n}} \mid k \in \mathbb{Z}\} = \mathbb{U}_n.$$

3. Considérons le groupe $(\mathbb{Z}, +)$. Soit $n \in \mathbb{Z}$. Alors :

$$\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}.$$

En particulier, $\langle 1 \rangle = 1\mathbb{Z} = \mathbb{Z}$.

4. Considérons le groupe $(\mathbb{C}, +)$. Montrons que $\langle \{1, i\} \rangle = \mathbb{Z}[i]$. Procédons par double inclusion.

$\subseteq$ Montrons que $\mathbb{Z}[i]$ est un sous-groupe de $\mathbb{C}$ contenant $\{1, i\}$.

— On a $0 = \underbrace{0}_{\in \mathbb{Z}} + \underbrace{0}_{\in \mathbb{Z}} i \in \mathbb{Z}[i]$.

— Pour tous $z = a + bi, \zeta = c + di \in \mathbb{Z}[i]$ avec $a, b, c, d \in \mathbb{Z}$, on a, comme $(\mathbb{Z}, +)$ est un groupe :

$$z - \zeta = (a + bi) - (c + di) = \underbrace{(a - c)}_{\in \mathbb{Z}} + \underbrace{(b - d)}_{\in \mathbb{Z}} i \in \mathbb{Z}[i]$$

Donc $\mathbb{Z}[i]$ est un sous-groupe de $\mathbb{C}$ et on a $1 = \underbrace{1}_{\in \mathbb{Z}} + \underbrace{0}_{\in \mathbb{Z}} i \in \mathbb{Z}[i]$; $i = \underbrace{0}_{\in \mathbb{Z}} + \underbrace{1}_{\in \mathbb{Z}} i \in \mathbb{Z}[i]$; d'où $\{1, i\} \subset \mathbb{Z}[i]$.

Par suite, $\langle \{1, i\} \rangle$ étant le plus petit sous-groupe de $\mathbb{C}$ contenant $\{1, i\}$, on a $\langle \{1, i\} \rangle \subset \mathbb{Z}[i]$.

⊇ Soit $z = a + bi \in \mathbb{Z}[i]$ avec $a, b \in \mathbb{Z}$. Alors, on a :

$$z = |a|(\pm 1) + |b|(\pm i) = \underbrace{(\pm 1) + \dots + (\pm 1)}_{|a|\text{termes}} + \underbrace{(\pm i) + \dots + (\pm i)}_{|b|\text{termes}}$$

où $\pm 1, \pm i \in \{1, i\} \cup \{-1, -i\} \cup \{0\}$.

Ainsi, d'après la proposition 2, $z \in \langle \{1, i\} \rangle$. D'où $\mathbb{Z}[i] \subset \langle \{1, i\} \rangle$.

Il en résulte que $\langle \{1, i\} \rangle = \mathbb{Z}[i]$.

5. Soit $n \in \mathbb{N}^*$. On note $\mathcal{T}$ l'ensemble des transpositions de $\mathcal{S}_n$. D'après le cours de Sup', on sait que, pour tout $\sigma \in \mathcal{S}_n$, il existe $k \in \mathbb{N}^*$ et $\tau_1, \dots, \tau_k \in \mathcal{T}$ tels que $\sigma = \tau_1 \circ \dots \circ \tau_k$; d'où, d'après la proposition 2, $\sigma \in \langle \mathcal{T} \rangle$.

Par suite, on a $\mathcal{S}_n \subset \langle \mathcal{T} \rangle \subset \mathcal{S}_n$ et donc $\langle \mathcal{T} \rangle = \mathcal{S}_n$.

6. On rappelle que les matrices de transvections sont les matrices de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ pour $\lambda \in \mathbb{K}$ et $i, j \in \llbracket 1, n \rrbracket$ avec $i \neq j$; et les matrices de dilatations sont les matrices de la forme $D_i(\alpha) = I_n + (\alpha - 1)E_{i,i}$ pour $\alpha \in \mathbb{K}^*$ et $i \in \llbracket 1, n \rrbracket$.

On note $\mathcal{E}_n$ l'ensemble des matrices de transvections et de dilatations de taille $n \times n$.

Alors, $\mathcal{E}_n \subset GL_n(\mathbb{K})$ car les matrices de $\mathcal{E}_n$ sont de déterminant non nul, d'où $\langle \mathcal{E}_n \rangle \subset GL_n(\mathbb{K})$.

De plus, pour $M \in GL_n(\mathbb{K})$, en effectuant l'algorithme du pivot de Gauss (sans échange de ligne) et sa remontée, on obtient qu'il existe $p \in \mathbb{N}^*$ et $O_1, \dots, O_p \in \mathcal{E}_n$ (O pour "opération élémentaire sur les lignes via une transvection ou une dilatation") tels que :

$$O_p \dots O_1 M = I_n,$$

d'où $M = O_1^{-1} \dots O_p^{-1}$.

Or, on remarque que $\mathcal{E}_n$ est stable par passage à l'inverse : en effet, pour tous $\lambda, \alpha \in \mathbb{K}$ et $i, j \in \llbracket 1, n \rrbracket$ avec $i \neq j$, $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda) \in \mathcal{E}_n$ et $D_i(\alpha)^{-1} = D_i(\frac{1}{\alpha}) \in \mathcal{E}_n$, donc $M = O_1^{-1} \dots O_p^{-1} \in \langle \mathcal{E}_n \rangle$.

Et ainsi, $GL_n(\mathbb{K}) \subset \langle \mathcal{E}_n \rangle$.

Il en résulte que $GL_n(\mathbb{K}) = \langle \mathcal{E}_n \rangle$ i.e. $GL_n(\mathbb{K})$ est engendré par l'ensemble des transvections et dilatations.

Exercice 1.

Déterminer le sous-groupe engendré par $A = \{2, 3\}$ dans $\mathbb{Z}$.

Correction.

En faisant un petit dessin, on se convainc que $\langle A \rangle = \mathbb{Z}$; montrons cette conjecture !

Comme $\langle A \rangle$ est un sous-groupe de $\mathbb{Z}$, on a en particulier $\langle A \rangle \subset \mathbb{Z}$. Montrons l'inclusion réciproque. Soit $n \in \mathbb{Z}$. Alors, comme 2 et 3 sont premiers entre eux, d'après le théorème de Bézout (on retrouvera l'énoncé de ce théorème vu en Sup' un peu plus loin), il existe $u, v \in \mathbb{Z}$ tel que $2u + 3v = 1$. Par suite, $1 \in \langle A \rangle$ qui est un sous-groupe de $\mathbb{Z}$, donc $\mathbb{Z} = \langle 1 \rangle \subset \langle A \rangle$.

D'où $\langle A \rangle = \mathbb{Z}$.

Exercice 2.

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Le groupe $(\mathcal{S}_n, \circ)$ des permutations de $\llbracket 1, n \rrbracket$ est engendré par l'ensemble des transpositions élémentaires i.e. de la forme $\tau_{i,i+1}$ (transposition qui échange i et $i+1$) pour $i \in \llbracket 1, n-1 \rrbracket$.

Correction.

Si $\tau_{i,j}$ est la transposition qui échange i et j avec $i, j \in \llbracket 1, n \rrbracket$ et $i < j$, on a :

$$\tau_{i,j} = \prod_{k=i}^{j-1} \tau_{k,k+1} \circ \prod_{k=2}^{j-i} \tau_{j-k,j-k+1}$$

D'après l'exemple précédent, $\mathcal{S}_n$ est engendré par les transpositions donc, d'après ce qui précède toute permutation est donc composée de transpositions élémentaires.
Il en résulte que $\mathcal{S}_n$ est engendré par l'ensemble des transpositions élémentaires.

Proposition 4.

Soit $(G, +)$ un groupe abélien, $n \in \mathbb{N}^*$ et $H_1, \dots, H_n$ des sous-groupes de G .

L'ensemble $H_1 + \dots + H_n = \{h_1 + \dots + h_n \mid \forall i \in \llbracket 1, n \rrbracket, h_i \in H_i\}$ est le sous-groupe de G engendré par $\bigcup_{i=1}^n H_i$.

Démonstration.

On note 0 l'élément neutre de G et $H = H_1 + \dots + H_n$.

Tout d'abord, on remarque que, d'après la proposition 2, on a :

$$H \subset \left\{ a_1 + \dots + a_k \mid k \in \mathbb{N}^*, a_1, \dots, a_k \in \bigcup_{i=1}^n H_i \cup \left(-\bigcup_{i=1}^n H_i \right) \cup \{0\} \right\} = \left\langle \bigcup_{i=1}^n H_i \right\rangle.$$

Ensuite, pour tout $j \in \llbracket 1, n \rrbracket$, on a $0 \in H_j$ car H_j est un sous-groupe de G donc, pour tout $i \in \llbracket 1, n \rrbracket$ et tout $h_i \in H_i$, on a :

$$h_i = 0 + \dots + 0 + h_i + 0 + \dots + 0 \in H_1 + \dots + H_n = H.$$

D'où $\bigcup_{i=1}^n H_i \subset H$.

Il nous reste donc à montrer que H est un sous-groupe de G pour conclure.

- On a $0 = 0 + \dots + 0 \in H_1 + \dots + H_n = H$ car, pour tout $i \in \llbracket 1, n \rrbracket$, 0 appartient au sous-groupe H_i .

- Pour tout $x = x_1 + \dots + x_n, y = y_1 + \dots + y_n \in H$, on a, par commutativité et associativité de $+$:

$$x - y = (x_1 + \dots + x_n) - (y_1 + \dots + y_n) = (x_1 - y_1) + \dots + (x_n - y_n) \in H_1 + \dots + H_n = H,$$

car, pour tout $i \in \llbracket 1, n \rrbracket$, H_i étant un sous-groupe, $x_i - y_i$ appartient à H_i .

Par suite, H est un sous-groupe de G contenant $\bigcup_{i=1}^n H_i$, donc $\left\langle \bigcup_{i=1}^n H_i \right\rangle \subset H$. Il en résulte que

$$H_1 + \dots + H_n = H = \left\langle \bigcup_{i=1}^n H_i \right\rangle. \quad \square$$

Proposition 5.

Soit G un groupe et $A \subset G$.

- Le sous-groupe $\langle A \rangle$ engendré par A est un groupe commutatif si, et seulement si, pour tous $a, b \in A$, $ab = ba$.

En particulier, pour $x \in G$, $\langle x \rangle$ est un groupe commutatif.

- Si $A = \{a_1, \dots, a_n\}$ avec $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in G$ qui commutent deux à deux, alors :

$$\langle A \rangle = \{a_1^{k_1} \dots a_n^{k_n} \mid k_1, \dots, k_n \in \mathbb{Z}\}.$$

Démonstration.

- $(\Rightarrow)$ On suppose que $\langle A \rangle$ est commutatif. Alors, pour tous $a, b \in A$, comme $A \subset \langle A \rangle$, on a $a, b \in \langle A \rangle$ qui est commutatif, donc $ab = ba$.

- $(\Leftarrow)$ On suppose que, pour tous $a, b \in A$, $ab = ba$.

On établit tout d'abord le fait suivant : si $x, y \in G$ commutent, alors x, x^{-1}, y, y^{-1} commutent deux à deux. Soit $x, y \in G$. On suppose $xy = yx$.

- Indépendamment de l'hypothèse, on a : $xx^{-1} = e = x^{-1}x$ (de même pour y et y^{-1});
- Sous l'hypothèse $xy = yx$, on remarque que :

$$\begin{aligned} x^{-1}y(yx^{-1})^{-1} &= x^{-1}(yx)y^{-1} \\ &= x^{-1}(xy)y^{-1} \\ &= (x^{-1}x)(yy^{-1}) \\ x^{-1}y(yx^{-1})^{-1} &= e \end{aligned}$$

d'où $x^{-1}y = yx^{-1}$ puis, en prenant le symétrique de chaque membre de l'égalité, on obtient également $y^{-1}x = xy^{-1}$.

Utilisons ce résultat pour montrer que $\langle A \rangle$ est commutatif.

Soit $x, y \in \langle A \rangle$. Alors il existe $n, m \in \mathbb{N}^*$ et $a_1, \dots, a_n, b_1, \dots, b_m \in A \cup A^{-1} \cup \{e\}$ tels que $x = a_1 \dots a_n$ et $y = b_1 \dots b_m$.

Comme tous les éléments de A commutent, d'après le résultat précédent, tous les

éléments de $A \cup A^{-1}$ commutent ; puis, comme e commute avec tous les éléments de G , on obtient que tous les éléments de $A \cup A^{-1} \cup \{e\}$ commutent.
Par suite, les éléments $a_1, \dots, a_n, b_1, \dots, b_m \in A \cup A^{-1} \cup \{e\}$ commutent deux à deux, d'où :

$$xy = (a_1 \dots a_n)(b_1 \dots b_m) = a_1 \dots a_n b_1 \dots b_m = b_1 \dots b_m a_1 \dots a_n = (b_1 \dots b_m)(a_1 \dots a_n) = yx.$$

Il en résulte que $\langle A \rangle$ est commutatif.

Pour le cas particulier $\langle x \rangle$ avec $x \in G$, il suffit de remarquer que x commute avec lui-même et d'appliquer le résultat que nous venons de prouver.

- On suppose $A = \{a_1, \dots, a_n\}$ avec $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in G$ qui commutent deux à deux. On pose $E(A) = \{a_1^{k_1} \dots a_n^{k_n} \mid k_1, \dots, k_n \in \mathbb{Z}\}$.

Alors $E(A)$:

- ★ contient A car, pour tout $i \in \llbracket 1, n \rrbracket$, $a_i = a_1^0 \dots a_i^1 \dots a_n^0$;
- ★ est un sous-groupe de G car $e = a_1^0 \dots a_n^0$ et, comme les a_i commutent entre eux, les composées des a_i commutent entre elles, donc, pour tous $k_1, \dots, k_n, l_1, \dots, l_n \in \mathbb{Z}$,

$$\begin{aligned} a_1^{k_1} \dots a_n^{k_n} (a_1^{l_1} \dots a_n^{l_n})^{-1} &= a_1^{k_1} \dots a_n^{k_n} a_n^{-l_n} \dots a_1^{-l_1} \\ &= a_1^{k_1 - l_1} \dots a_n^{k_n - l_n} \in E(A). \end{aligned}$$

Par suite, $\langle A \rangle \subset E(A)$.

De plus, on a :

$$\begin{aligned} E(A) &= \{a_1^{k_1} \dots a_n^{k_n} \mid k_1, \dots, k_n \in \mathbb{Z}\} \\ &\subset \{b_1 \dots b_m \mid m \in \mathbb{N}^*, b_1, \dots, b_m \in \{a_1^{\pm 1}, \dots, a_n^{\pm 1}\} \cup \{e\}\} = \langle A \rangle \end{aligned}$$

où la dernière égalité provient de la proposition 2.

Ainsi, on a $E(A) = \langle A \rangle$.

□

Proposition 6.

Soit G_1, G_2 des groupes, $f : G_1 \rightarrow G_2$ un morphisme de groupes et $A \subset G_1$. On a $f(\langle A \rangle) = \langle f(A) \rangle$.

Démonstration.

Remarquons tout d'abord que, comme $f(e_1) = e_2$ et, pour tout $x \in G_1$, $f(x^{-1}) = f(x)^{-1}$ car f est un morphisme de groupes, on a $f(\{e_1\}) = \{e_2\}$ et $f(A^{-1}) = f(A)^{-1}$; donc, par propriétés de l'image directe d'une fonction, $f(A \cup A^{-1} \cup \{e_1\}) = f(A) \cup f(A)^{-1} \cup \{e_2\}$.

Procédons par double inclusion :

- $f(\langle A \rangle) \subset \langle f(A) \rangle$: Soit $y \in f(\langle A \rangle)$. Alors, il existe $x \in \langle A \rangle$ tel que $y = f(x)$. Ainsi, d'après la proposition 2, il existe $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in A \cup A^{-1} \cup \{e_1\}$. Or, d'après la remarque initiale, pour tout $i \in \llbracket 1, n \rrbracket$, $f(a_i) \in f(A) \cup f(A)^{-1} \cup \{e_2\}$; donc, comme f est

un morphisme de groupes, on a, d'après la proposition 2 :

$$y = f(x) = f(a_1 \dots a_n) = f(a_1) \dots f(a_n) \in \langle f(A) \rangle.$$

D'où $f(\langle A \rangle) \subset \langle f(A) \rangle$.

- $\langle f(A) \rangle \subset f(\langle A \rangle)$: Soit $y \in \langle f(A) \rangle$. D'après la proposition 2, il existe $n \in \mathbb{N}^*$ et $b_1 \dots b_n \in f(A) \cup f(A)^{-1} \cup \{e_2\} = f(A \cup A^{-1} \cup \{e_1\})$ tels que $y = b_1 \dots b_n$. Ainsi, pour tout $i \in \llbracket 1, n \rrbracket$, il existe $a_i \in A \cup A^{-1} \cup \{e_1\}$ tel que $b_i = f(a_i)$. Par suite, comme f est un morphisme de groupes, d'après la proposition 2, on a :

$$y = b_1 \dots b_n = f(a_1) \dots f(a_n) = f(\underbrace{a_1 \dots a_n}_{\in \langle A \rangle}) \in f(\langle A \rangle).$$

D'où $\langle f(A) \rangle \subset f(\langle A \rangle)$.

Il en résulte que $f(\langle A \rangle) = \langle f(A) \rangle$. □

2. Les sous-groupes de $\mathbb{Z}$

Théorème 1. Division euclidienne

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

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

Démonstration.

Vue en Sup'. (Idée : pour $a \geq 0$, l'ensemble $\{p \in \mathbb{N} \mid bp \leq a\}$ est non vide et majoré, or toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément : il s'agit du quotient q . Il ne reste plus qu'à encadrer le reste $r = a - bq$ et à démontrer l'unicité du couple (q, r)). □

Théorème 2. Caractérisation des sous-groupes de $\mathbb{Z}$

Soit $H \subset \mathbb{Z}$. L'ensemble H est un sous-groupe de $(\mathbb{Z}, +)$ si, et seulement si, il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration.

- $(\Leftarrow)$. On suppose qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Alors $H = \langle n \rangle$, donc H est un sous-groupe de $\mathbb{Z}$.
- $(\Rightarrow)$. On suppose que H est un sous-groupe de $(\mathbb{Z}, +)$.

Montrons l'existence.

1er cas : $H = \{0\}$. Alors $H = 0\mathbb{Z}$.

2eme cas : $H \neq \{0\}$. Pour $k \in H \setminus \{0\}$, $|k| \in H \cap \mathbb{N}^*$. Or tout sous-ensemble non vide de $\mathbb{N}$ possède un plus petit élément, donc $H \cap \mathbb{N}^*$ possède un plus petit élément n .

Comme H est un sous-groupe de $\mathbb{Z}$ contenant n et que $n\mathbb{Z} = \langle n \rangle$ est le plus petit sous-groupe de $\mathbb{Z}$ contenant n , on a $n\mathbb{Z} \subset H$. Réciproquement, si $x \in H \subset \mathbb{Z}$, la division euclidienne de x par n nous fournit un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ avec $0 \leq r < n$ tel que

$$x = nq + r$$

Comme $n\mathbb{Z} \subset H$, $nq \in H$ et donc, H étant un sous-groupe de $\mathbb{Z}$, $r = x - nq$ appartient à H . Or n est le plus petit élément positif et non nul de H et $0 \leq r < n$, donc $r = 0$. Par suite, $x = nq \in n\mathbb{Z}$. Ainsi, $H \subset n\mathbb{Z}$.

Il en résulte que $H = n\mathbb{Z}$.

Montrons l'unicité d'un tel entier naturel :

Soit $n, m \in \mathbb{N}$ tels que $n\mathbb{Z} = H = m\mathbb{Z}$. Si n ou $m = 0$, $H = \{0\}$ et donc, comme $n, m \in H$, on a $n = 0 = m$. Supposons n et m non nuls. Alors on a $n \in n\mathbb{Z} \subset m\mathbb{Z}$, d'où $m|n$ donc $m = |m| \leq |n| = n$ (n, m étant positifs et $n \neq 0$). De manière analogue, comme $m \in n\mathbb{Z}$, $n \leq m$.

Il en résulte que $n = m$. D'où l'unicité. □

Question 2.

Soit $p \in \mathbb{Z} \setminus \mathbb{N}$. À quel sous-groupe de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ le sous-groupe $p\mathbb{Z}$ est-il égal ?)

Réponse.

Pour tout $k \in \mathbb{Z}$, $pk = (-p)(-k)$, donc $p\mathbb{Z} = (-p)\mathbb{Z}$.

Exercice 3.

Soit $n \in \mathbb{N}$. Décrire tous les sous-groupes de $(n\mathbb{Z}, +)$.

Correction.

Analysons !

Soit H un sous-groupe de $n\mathbb{Z}$. Alors, comme $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, H est un sous-groupe de $\mathbb{Z}$. Ainsi, d'après la caractérisation des sous-groupes de $\mathbb{Z}$, il existe $m \in \mathbb{N}$ tel que $H = m\mathbb{Z}$. Or $H \subset n\mathbb{Z}$ donc, comme $m = m \cdot 1 \in m\mathbb{Z} = H$, on a $m \in n\mathbb{Z}$ i.e. $n|m$.

Ce résultat nous donne envie de conjecturer : H est un sous-groupe de $n\mathbb{Z}$ si, et seulement si, il existe $k \in \mathbb{Z}$ tel que $H = (nk)\mathbb{Z}$.

Nous avons déjà prouvé l'implication directe, puis, pour la réciproque, il suffit de remarquer que $nk \in n\mathbb{Z}$ et donc $(nk)\mathbb{Z} \subset n\mathbb{Z}$.

Exercice 4.

Soit $(a, b) \in \mathbb{Z}^2$ avec a, b non nuls.

1. Montrer que $a\mathbb{Z} + b\mathbb{Z} = \{au + bv \mid u, v \in \mathbb{Z}\}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$.
2. En déduire qu'il existe des uniques $d, m \in \mathbb{N}$ tels que :

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \quad \text{et} \quad a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

Puis montrer que $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.

Correction.

1. D'après la proposition 5, $a\mathbb{Z} + b\mathbb{Z} = \langle \{a, b\} \rangle$ donc $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.
De plus, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ comme intersection de sous-groupes de $\mathbb{Z}$.
2. Comme $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$ en vertu de la question précédente, d'après la caractérisation des sous-groupes de $\mathbb{Z}$ (Théorème 2), il existe des uniques $d, m \in \mathbb{N}$ tels que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

— Montrons que $d = \text{pgcd}(a, b)$ i.e. le plus grand diviseur positif commun de a et b .

On a $a = a.1 + b.0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $b = a.0 + b.1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ donc a, b sont des multiples de d i.e. d est un diviseur commun de a et b . De plus, comme $a, b \in d\mathbb{Z}$, $d \neq 0$ car $(a, b) \neq (0, 0)$.

Soit δ un diviseur commun positif de a et b . Comme $d = d.1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$. Or $\delta|a$ et $\delta|b$ donc il existe $p, q \in \mathbb{Z}$ tels que $a = \delta p$ et $b = \delta q$ donc

$$d = au + bv = \delta \underbrace{(pu + qv)}_{\in \mathbb{Z}}.$$

D'où $\delta|d$. Ainsi, comme $\delta, d \geq 0$ et $d \neq 0$, $\delta \leq d$.

Il en résulte que d est le plus grand diviseur positif commun de a et b i.e. $d = \text{pgcd}(a, b)$.

— Montrons que $m = \text{ppcm}(a, b)$ i.e. le plus petit multiple strictement positif commun de a et b .

On a $m = m.1 \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, donc, par définition de $a\mathbb{Z} \cap b\mathbb{Z}$, m est un multiple commun de a et b .

Soit μ un multiple commun strictement positif de a et b (existe bien car $ab \in m\mathbb{Z}$ donc $m\mathbb{Z} \neq \{0\}$). Alors $\mu \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ et donc $m|\mu$. Or $m, \mu \geq 0$ et $\mu \neq 0$, donc $m \leq \mu$.

Il en résulte que m est le plus petit multiple strictement positif commun de a et b i.e. $m = \text{ppcm}(a, b)$.

3. Le groupe $\mathbb{Z}/n\mathbb{Z}$

a. Congruences

On rappelle la relation de congruence entre deux entiers relatifs pour un entier naturel non nul fixé :

Définition 2. Relation de congruence

Soit $n \in \mathbb{N}^*$. Pour $a, b \in \mathbb{Z}$, on dit que a **est congru à b modulo n** si

$$b - a \in n\mathbb{Z};$$

on note :

$$a \equiv b \pmod{n}.$$

Proposition 7.

Soit $n \in \mathbb{N}^*$. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. De plus, elle est *compatible* avec l'addition et la multiplication sur $\mathbb{Z}$, i.e. pour tous $a, b, c, d \in \mathbb{Z}$, si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$\begin{cases} a + c \equiv b + d \pmod{n}; \\ ac \equiv bd \pmod{n}. \end{cases}$$

Démonstration.

Montrons que $\cdot \equiv \cdot \pmod{n}$ est une relation d'équivalence sur $\mathbb{Z}$.

Soit $a, b, c \in \mathbb{Z}$.

- (*Réflexivité*) On a $a - a = 0 = 0.n \in n\mathbb{Z}$, donc $a \equiv a \pmod{n}$.
- (*Symétrie*) On suppose $a \equiv b \pmod{n}$. Alors il existe $k \in \mathbb{Z}$ tel que $b - a = kn$. On a :

$$a - b = -(b - a) = (-k)n \in n\mathbb{Z},$$

donc $b \equiv a \pmod{n}$.

- (*Transitivité*) On suppose $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$. Alors il existe $k, k' \in \mathbb{Z}$ tel que $b - a = kn$ et $c - b = k'n$. Par suite,

$$c - a = (c - b) + (b - a) = (k + k')n \in n\mathbb{Z},$$

donc $a \equiv c \pmod{n}$.

Il en résulte que la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. Montrons de plus qu'elle est compatible avec l'addition et la multiplication :

Soit $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$. Alors il existe $k, k' \in \mathbb{Z}$ tel que $b - a = nk$ et $d - c = nk'$. On a alors :

$$(b + d) - (a + c) = (b - a) + (d - c) = n(k + k') \in n\mathbb{Z},$$

donc $a + c \equiv b + d \pmod{n}$.

Et on a :

$$bd - ac = (b - a)c + (d - c)b = n(kc + k'b) \in n\mathbb{Z},$$

donc $ac \equiv bd \pmod{n}$. □

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

Notation 1. Classes d'équivalence modulo n

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

- Pour $k \in \mathbb{Z}$, on note $\bar{k} = \{x \in \mathbb{Z} \mid x \equiv k \pmod{n}\}$ la classe d'équivalence de k pour la relation de congruence modulo n ;
- On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation de congruence modulo n .

Remarque 3.

- On a $\bar{0} = n\mathbb{Z}$, $\bar{1} = 1 + n\mathbb{Z}$, $\dots$, $\bar{k} = k + n\mathbb{Z}$.
- Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ est une classe d'équivalence pour la relation de congruence modulo n , si k est un entier tel que $k \in \alpha$, alors $\alpha = \bar{k}$. On dit alors que k est **représentant de la classe** α .

Exercice 5.

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

1. Écrire une description explicite de l'ensemble $\bar{k}$ pour $k \in \mathbb{Z}$ fixé.
2. Montrer que pour tous $x, y \in \mathbb{Z}$, $x \equiv y \pmod{n}$ si, et seulement si, $\bar{x} = \bar{y}$.
3. Montrer que deux classes d'équivalence sont soit disjointes, soit égales.

Démonstration.

1.

$$\begin{aligned}
 \bar{k} &= \{x \in \mathbb{Z} \mid k \equiv x \pmod{n}\} \\
 &= \{x \in \mathbb{Z} \mid x - k \in n\mathbb{Z}\} \\
 &= \{x \in \mathbb{Z} \mid \exists p \in \mathbb{Z}, x = k + pn\} \\
 &= \{k + pn \mid p \in \mathbb{Z}\} \\
 &=: k + n\mathbb{Z}
 \end{aligned}$$

2. Si $x \equiv y \pmod{n}$, alors il existe $p \in \mathbb{Z}$ tel que $y - x = pn$. Par suite, pour tout $q \in \mathbb{Z}$,

$$y + qn = x + pn + qn = x + (p + q)n \in x + n\mathbb{Z} = \bar{x},$$

et

$$x + qn = y - pn + qn = x + (q - p)n \in y + n\mathbb{Z} = \bar{y},$$

d'où $\bar{y} \subset \bar{x}$ et $\bar{x} \subset \bar{y}$. Donc $\bar{x} = \bar{y}$.

Réciproquement, si $\bar{x} = \bar{y}$, alors en particulier, $x = x + 0n \in \bar{x} = \bar{y}$, donc par définition, $x \equiv y \pmod{n}$.

3. Soit $x, y \in \mathbb{Z}$. On suppose $\bar{x} \cap \bar{y} \neq \emptyset$. Alors il existe $k \in \bar{x} \cap \bar{y}$, donc $k \equiv x \pmod{n}$ et $k \equiv y \pmod{n}$. Par symétrie et transitivité, on a alors :

$$x \equiv y \pmod{n}.$$

Par suite, d'après le résultat précédent, $\bar{x} = \bar{y}$.

□

Proposition 8.

Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n et on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

Démonstration.

$\mathbb{Z}/n\mathbb{Z}$ étant l'ensemble des classes d'équivalence de la relation de congruence modulo n , pour tout $k \in \mathbb{Z}$, $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, donc

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \subset \mathbb{Z}/n\mathbb{Z}.$$

Montrons que $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ et k un représentant de α (alors $\alpha = \overline{k}$).

On a, par division euclidienne, $k = nq + r$ où $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ avec $r \in \llbracket 0, n-1 \rrbracket$. Alors

$$k \equiv r \pmod{n}.$$

Donc $\alpha = \overline{k} = \overline{r} \in \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. D'où l'inclusion.

Il en résulte que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. □

c. Le groupe $\mathbb{Z}/n\mathbb{Z}$ **Théorème 3.** *Structure de groupe sur $\mathbb{Z}/n\mathbb{Z}$*

Soit $n \in \mathbb{N}^*$. Il existe sur $\mathbb{Z}/n\mathbb{Z}$ une loi de composition interne notée $+$ et appelée **loi additive quotient** telle que, pour tous $x, y \in \mathbb{Z}$,

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Muni de cette loi, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif où :

- l'élément neutre est $\overline{0}$;
- pour $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, $-\overline{k} = \overline{-k}$.

De plus, pour tous $p \in \mathbb{Z}$, $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, $p\overline{k} = \overline{pk}$.

Démonstration.

Soit $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$. Si $p, p' \in \mathbb{Z}$ sont des représentants de α et q, q' des représentants de β , alors $p \equiv p' \pmod{n}$ et $q \equiv q' \pmod{n}$, donc :

$$p + q \equiv p' + q' \pmod{n}.$$

Ainsi, on peut poser $\alpha + \beta := \overline{p + q}$ car la classe de $\overline{p + q}$ ne dépend pas du choix des représentants p et q de α et β respectivement.

Vérifions alors que muni de cette opération, $\mathbb{Z}/n\mathbb{Z}$ est bien un groupe.

Soit $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}/n\mathbb{Z}$ avec $x, y, z \in \mathbb{Z}$.

- (*Associativité*). On a, par associativité de la loi $+$ de $\mathbb{Z}$:

$$\begin{aligned}
(\bar{x} + \bar{y}) + \bar{z} &= \overline{x + y} + \bar{z} \\
&= \overline{(x + y) + z} \\
&= \overline{x + (y + z)} \\
&= \bar{x} + \overline{y + z} \\
&= \bar{x} + (\bar{y} + \bar{z})
\end{aligned}$$

— (Élément neutre). Comme 0 est l'élément neutre de + dans $\mathbb{Z}$, on a :

$$\bar{0} + \bar{x} = \overline{0 + x} = \bar{x} = \overline{x + 0} = \bar{x} + \bar{0}.$$

— (Symétrie). Comme $-x$ est le symétrique de x pour + dans $\mathbb{Z}$ On a :

$$\bar{x} + \overline{-x} = \overline{x + (-x)} = \bar{0} = \overline{-x + x} = \overline{-x} + \bar{x}.$$

Soit $k \in \mathbb{Z}$. Pour $p \in \mathbb{Z}$, on a $0\bar{k} = \bar{0} = \overline{0k}$ et par une récurrence élémentaire :

$$p\bar{k} = \begin{cases} \underbrace{\bar{k} + \bar{k} + \dots + \bar{k}}_{p \text{ termes}} = \overline{\underbrace{k + k + \dots + k}_{p \text{ termes}}} & \text{si } p > 0 \\ \underbrace{\overline{-k} + \overline{-k} + \dots + \overline{-k}}_{|p| \text{ termes}} = \overline{\underbrace{-k - k - \dots - k}_{|p| \text{ termes}}} & \text{si } p < 0 \end{cases} = \overline{pk}.$$

□

Exemple 2.

— Dans $\mathbb{Z}/12\mathbb{Z}$, on a :

$$\bar{7} + \bar{8} = \overline{7 + 8} = \bar{15} = \bar{3}.$$

— Soit $n \in \mathbb{N}^*$, on a $\langle \bar{1} \rangle = \mathbb{Z}/n\mathbb{Z}$.

— Il suffit de remarquer que $15 \equiv 3 \pmod{12}$.

— Soit $n \in \mathbb{N}^*$. On a, pour tout $k \in \mathbb{Z}$, d'après le théorème précédent, $k\bar{1} = \overline{k \cdot 1} = \bar{k}$, d'où :

$$\langle \bar{1} \rangle = \{k\bar{1} \mid k \in \mathbb{Z}\} = \{\bar{k} \mid k \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}.$$

Exercice 6.

- Établir la table d'addition du groupe $(\mathbb{Z}/4\mathbb{Z}, +)$ et déterminer le sous-groupe engendré par $\{\bar{k}\}$ pour chaque $\bar{k} \in (\mathbb{Z}/4\mathbb{Z}, +)$.
- Soit $n \in \mathbb{N}^*$. Déterminer le sous-groupe engendré par $\{\overline{n-1}\}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Correction.

1.

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

De plus, on a :

— $\langle \bar{0} \rangle = \{\bar{0}\}$ car $2\bar{0} = \bar{0}$ (ou en utilisant que $\langle e \rangle = \{e\}$ dans un groupe d'élément neutre e).

— $\langle \bar{1} \rangle = \mathbb{Z}/4\mathbb{Z}$ car $2\bar{1} = \bar{2}$, $3\bar{1} = \bar{3}$, $4\bar{1} = \bar{0}$ (ou en utilisant l'exemple précédent).

— $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$ car $2\bar{2} = \bar{0}$.

— $\langle \bar{3} \rangle = \mathbb{Z}/4\mathbb{Z}$ car $2\bar{3} = \bar{2}$, $3\bar{3} = \bar{1}$, $4\bar{3} = \bar{0}$.

2. Soit $n \in \mathbb{N}^*$. On a $\langle \overline{n-1} \rangle \subset \mathbb{Z}/n\mathbb{Z}$.

De plus, pour tout $k \in \mathbb{Z}$, on remarque que $k = (-k) \times (-1)$, donc $\bar{k} = (-k)\overline{-1} = (-k)\overline{n-1} \in \langle \overline{n-1} \rangle$. Ainsi, $\mathbb{Z}/n\mathbb{Z} \subset \langle \overline{n-1} \rangle$.

Il en résulte que $\langle \overline{n-1} \rangle = \mathbb{Z}/n\mathbb{Z}$.

Proposition 9.

Soit $n \in \mathbb{N}^*$. L'application $\pi_n : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ telle que, pour $k \in \mathbb{Z}$,

$$\pi_n(k) = \bar{k}$$

est un morphisme surjectif de groupes.

Démonstration.

Soit $x, y \in \mathbb{Z}$. On a, par définition de l'addition sur $\mathbb{Z}/n\mathbb{Z}$:

$$\pi_n(x + y) = \overline{x + y} = \bar{x} + \bar{y} = \pi_n(x) + \pi_n(y).$$

Donc π_n est un morphisme de groupes.

De plus, pour tout $\alpha \in \mathbb{Z}/n\mathbb{Z}$, si k est un représentant de α , alors k est un antécédent de α par π_n car $\alpha = \bar{k}$. Donc π_n est surjective. $\square$

Exercice 7.

Soit $n \in \mathbb{N}^*$. Déterminer le noyau de $\pi_n : k \mapsto \bar{k}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Correction.

On a, pour $k \in \mathbb{Z}$, $\bar{k} = \bar{0}$ si, et seulement si, $k \equiv 0 \pmod{n}$, i.e. $k = k-0 \in n\mathbb{Z}$. Ainsi, $\text{Ker}(\pi_n) = n\mathbb{Z}$.

4. Groupes monogènes

a. Généralités et exemples

Définition 3. *Groupe monogène / groupe cyclique*

Soit G un groupe.

- On dit que G est un groupe **monogène** s'il est engendré par un seul élément i.e. s'il existe $x \in G$ tel que :

$$\langle x \rangle = G.$$

Dans ce cas, on dira que l'élément est un **générateur** de G ou encore que G est **engendré** par x .

- On dit que G est un groupe **cyclique** s'il est monogène et fini.

Exemple 3. *Groupes monogènes classiques*

- $(\mathbb{Z}, +)$ est un groupe monogène et n'est pas cyclique.
- pour $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique : il est fini et est engendré par $\bar{1}$, i.e. $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$;
- pour $n \in \mathbb{N}^*$, $(\mathbb{U}_n, \times)$ est un groupe cyclique : il est fini et est engendré par $e^{i\frac{2\pi}{n}}$, i.e. $\mathbb{U}_n = \langle e^{i\frac{2\pi}{n}} \rangle$;

- D'après l'exemple 1 (point 3.), on a $\mathbb{Z} = \langle 1 \rangle$, donc $\mathbb{Z}$ est engendré par 1. De plus, $\mathbb{Z}$ est infini (car pour tout $n \in \mathbb{N}$, $\#\mathbb{Z} \geq n = \#\llbracket 1, n \rrbracket$), donc $\mathbb{Z}$ n'est pas cyclique.
- D'après l'exemple 2, on a $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$, donc $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\bar{1}$ i.e. $\mathbb{Z}/n\mathbb{Z}$ est monogène. De plus, il est fini car de cardinal n , donc $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique.
- D'après l'exemple 1 (point 2.), on a $\mathbb{U}_n = \langle e^{i\frac{2\pi}{n}} \rangle$, donc $\mathbb{U}_n$ est engendré par $e^{i\frac{2\pi}{n}}$ i.e. $\mathbb{U}_n$ est monogène. De plus, il est fini car de cardinal n , donc $\mathbb{U}_n$ est un groupe cyclique.

Remarque 4.

Le terme *cyclique* s'inspire de ce qui se passe dans les groupes $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{U}_n$ (ou même de n'importe quel groupe cyclique comme on le verra par la suite) ; en effet, si on considère une par une les composées successives d'un générateur, on "tourne en rond" sur tous les éléments du groupe !

Exercice 8.

Montrer que $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, +)$ est cyclique mais que $((\mathbb{Z}/2\mathbb{Z})^2, +)$ ne l'est pas.

Correction.

— On remarque que $x = (\bar{1}^2, \bar{1}^3)$ engendre $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. En effet :

$$\begin{array}{ll} 2x &= (\bar{0}^2, \bar{2}^3) & 3x &= (\bar{1}^2, \bar{0}^3) \\ 4x &= (\bar{0}^2, \bar{1}^3) & 5x &= (\bar{1}^2, \bar{2}^3) \\ 6x &= (\bar{0}^2, \bar{0}^3) \end{array}$$

Donc $\langle (\bar{1}^2, \bar{1}^3) \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et ainsi, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est monogène. De plus, ce groupe est fini de cardinal 6 donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique.

— Après calculs très rapides, on obtient :

- * $\langle (\bar{0}, \bar{0}) \rangle = \{(\bar{0}, \bar{0})\} \neq (\mathbb{Z}/2\mathbb{Z})^2$;
- * $\langle (\bar{1}, \bar{0}) \rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\} \neq (\mathbb{Z}/2\mathbb{Z})^2$;
- * $\langle (\bar{0}, \bar{1}) \rangle = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\} \neq (\mathbb{Z}/2\mathbb{Z})^2$;
- * $\langle (\bar{1}, \bar{1}) \rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\} \neq (\mathbb{Z}/2\mathbb{Z})^2$;

Ainsi, aucun élément de $(\mathbb{Z}/2\mathbb{Z})^2$ n'engendre $(\mathbb{Z}/2\mathbb{Z})^2$. Par suite, $(\mathbb{Z}/2\mathbb{Z})^2$ n'est pas monogène et donc n'est pas cyclique.

Exercice 9.

Montrer que le groupe $(\mathbb{Z}^2, +)$ n'est pas monogène puis déterminer un ensemble de cardinal le plus petit possible qui engendre $\mathbb{Z}^2$.

Correction.

Soit $(n, m) \in \mathbb{Z}^2$. Montrons que $\langle (n, m) \rangle \neq \mathbb{Z}^2$.

On a $\langle (n, m) \rangle = \{(kn, km) \mid k \in \mathbb{Z}\}$, donc, pour tout $(p, q) = (kn, km) \in \langle (n, m) \rangle$ avec $k \in \mathbb{Z}$, on a :

$$\begin{vmatrix} p & n \\ q & m \end{vmatrix} = pm - nq = knm - knm = 0.$$

On va ainsi chercher un couple (p, q) de $\mathbb{Z}^2$ tel que ce déterminant ne s'annule pas : en effet, par contraposée, celui-ci n'appartiendra pas à $\langle (n, m) \rangle$.

— 1er cas : $(n, m) \neq (0, 0)$. On pose $p = m$ et $q = -n$. Alors on a :

$$\begin{vmatrix} p & n \\ q & m \end{vmatrix} = \begin{vmatrix} m & n \\ -n & m \end{vmatrix} = m^2 + n^2 \neq 0.$$

D'où $(p, q) \notin \langle (n, m) \rangle$. Ainsi, $\langle (n, m) \rangle \neq \mathbb{Z}^2$.

Intuitivement, on se rend compte que tous les couples du sous-groupe engendré par (n, m) sont sur la droite vectorielle engendrée par (n, m) dans $\mathbb{R}^2$: on va alors prendre un vecteur à coordonnées entières facilement constructible qui n'est pas sur cette droite, par exemple, ici, un vecteur orthogonal à (n, m) !

- 2eme cas : $(n, m) = (0, 0)$. Ici, on ne va pas utiliser notre déterminant qui s'annulera toujours comme $(n, m) = (0, 0)$. Simplement, on remarque que dans ce cas, $\langle (0, 0) \rangle = \{(0, 0)\} \neq \mathbb{Z}^2$.

Dans tous les cas, $\langle (n, m) \rangle \neq \mathbb{Z}^2$. Ceci étant vrai pour tout couple de $\mathbb{Z}^2$, $\mathbb{Z}^2$ n'est pas monogène.

De plus, la paire $\{(1, 0), (0, 1)\}$ engendre $\mathbb{Z}^2$ car $\langle \{(1, 0), (0, 1)\} \rangle = \{n(1, 0) + m(0, 1) \mid n, m \in \mathbb{Z}\} = \{(n, m) \mid n, m \in \mathbb{Z}\} = \mathbb{Z}^2$. On a donc exhibé un ensemble de cardinal 2 qui engendre $\mathbb{Z}^2$ et ce cardinal est bien minimal car on a remarqué précédemment qu'aucun ensemble de cardinal 1 n'engendre $\mathbb{Z}^2$.

Exercice 10.

Montrer que pour $n \in \mathbb{N}$ avec $n \geq 3$, le groupe $(\mathcal{S}_n, \circ)$ des permutations de $\llbracket 1, n \rrbracket$ n'est pas monogène.

Correction.

Pour $n \geq 3$, $\mathcal{S}_n$ n'est pas un groupe commutatif : en effet, les transpositions $\tau_{1,2}$ et $\tau_{2,3}$ ne commutent pas. Or, d'après la proposition 5, tout groupe monogène est commutatif, donc $\mathcal{S}_n$ n'est pas monogène.

b. Classification des groupes monogènes

Proposition-Notation 10.

Soit G un groupe et $x \in G$. Alors l'application notée $\varphi_x : \mathbb{Z} \rightarrow G$ telle que, pour $k \in \mathbb{Z}$:

$$\varphi_x(k) = x^k$$

est un morphisme de groupes.

Démonstration.

Soit G un groupe et $x \in G$. Pour $k, k' \in \mathbb{Z}$, on a :

$$\varphi_x(k + k') = x^{k+k'} = x^k x^{k'} = \varphi_x(k) \varphi_x(k')$$

donc φ_k est un morphisme de groupes. □

Théorème 4. Classification des groupes monogènes

- Tout groupe monogène *infini* est isomorphe au groupe $(\mathbb{Z}, +)$. De plus, si G est un groupe monogène infini engendré par $x \in G$, l'application $k \mapsto x^k$ de $\mathbb{Z}$ dans G est un isomorphisme de groupes.

- Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
De plus, si G est un groupe cyclique d'ordre n engendré par $x \in G$, l'application $\bar{k} \mapsto x^k$ de $\mathbb{Z}/n\mathbb{Z}$ dans G est bien définie et est un isomorphisme de groupes.

Démonstration.

Soit G un groupe monogène. Alors il existe $x \in G$ tel que $G = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. Considérons le morphisme de φ_x de la proposition-notation 10. On a

$$\text{Im}(\varphi_x) = \{\varphi_x(k) \mid k \in \mathbb{Z}\} = \{x^k \mid k \in \mathbb{Z}\} = G;$$

donc φ_x est un morphisme surjectif.

Comme φ_x est un morphisme de groupes, alors $\text{Ker}(\varphi_x)$ est un sous-groupe de $\mathbb{Z}$. Ainsi, d'après la caractérisation des sous-groupes de $\mathbb{Z}$ (Théorème 2), il existe un unique $n \in \mathbb{N}$ tel que $\text{Ker}(\varphi_x) = n\mathbb{Z}$. On a donc l'alternative suivante :

- $n = 0$. Alors $\text{Ker}(\varphi_x) = \{0\}$, d'où φ_x est injective, et donc φ_x est un isomorphisme de groupes. Ainsi, G est isomorphe à $(\mathbb{Z}, +)$.
- $n > 0$. Alors $\text{Ker}(\varphi_x) = n\mathbb{Z} \neq \{0\}$, donc φ_x n'est pas injective.
Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ et $p, q \in \alpha$. Alors on a $p - q \in n\mathbb{Z} = \text{Ker}(\varphi_x)$ donc

$$\varphi_x(p) = \varphi_x(q).$$

Ainsi, φ_x est constante sur chaque classe d'équivalence de $\mathbb{Z}/n\mathbb{Z}$. Par suite, on peut définir l'application :

$$\tilde{\varphi}_x : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \rightarrow & G \\ \alpha & \mapsto & \varphi_x(p) (= x^p) \end{array} \quad \text{où } p \in \alpha$$

Alors

- $\tilde{\varphi}_x$ est un morphisme de groupes. En effet, comme φ_x est un morphisme de groupes, pour tous $p, q \in \mathbb{Z}$, on a :

$$\tilde{\varphi}_x(\overline{p+q}) = \tilde{\varphi}_x(\overline{p+q}) = \varphi_x(p+q) = \varphi_x(p)\varphi_x(q) = \tilde{\varphi}_x(\overline{p})\tilde{\varphi}_x(\overline{q}).$$

- $\tilde{\varphi}_x$ est surjectif. En effet, pour tout $y \in \langle x \rangle$, comme φ_x est surjective, il existe $k \in \mathbb{Z}$ tel que $y = \varphi_x(k)$ et

$$y = \varphi_x(k) = \tilde{\varphi}_x(\bar{k}).$$

Donc $\bar{k}$ est un antécédent de y par $\tilde{\varphi}_x$.

- $\tilde{\varphi}_x$ est injectif. En effet, si $\bar{k} \in \text{Ker}(\tilde{\varphi}_x)$, alors

$$e = \tilde{\varphi}_x(\bar{k}) = \varphi_x(k),$$

donc $k \in \text{Ker}(\varphi_x) = n\mathbb{Z}$. Par suite, $k \equiv 0 \pmod{n}$, d'où $\bar{k} = \bar{0}$.

Il en résulte que $\text{Ker}(\tilde{\varphi}_x) = \{\bar{0}\}$.

Par suite, $\tilde{\varphi}_x$ est un isomorphisme de groupes. Ainsi, G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. □

Exemple 4.

Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{U}_n, \cdot)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

En effet, $\mathbb{U}_n = \langle e^{i\frac{2\pi}{n}} \rangle$ et $\#\mathbb{U}_n = n$; donc, d'après le théorème précédent, $(\mathbb{U}_n, \cdot)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. De plus, un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{U}_n$ est donné par :

$$\bar{k} \mapsto e^{i\frac{2k\pi}{n}}.$$

Exercice 11.

Montrer que $G = \left\{ \begin{pmatrix} 3^n & n3^{n-1} \\ 0 & 3^n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ est un sous-groupe de $GL_2(\mathbb{R})$ isomorphe à $\mathbb{Z}$.

Correction.

Pour $n \in \mathbb{Z}$, on note $A_n = \begin{pmatrix} 3^n & n3^{n-1} \\ 0 & 3^n \end{pmatrix}$.

On a, pour tous $n, m \in \mathbb{Z}$:

$$A_n A_m = \begin{pmatrix} 3^n 3^m & 3^n \times m3^{m-1} + n3^{n-1} \times 3^m \\ 0 & 3^n 3^m \end{pmatrix} = \begin{pmatrix} 3^{n+m} & (n+m)3^{(n+m)-1} \\ 0 & 3^{n+m} \end{pmatrix} = A_{n+m}$$

Par suite, par récurrence sur $\mathbb{N}$, on obtient, pour tout $n \in \mathbb{N}$, $A_1^n = A_n$; puis, pour $m \in \mathbb{Z}$, en remarquant que $A_m A_{-m} = A_0 = I_2$, on déduit que A_m est inversible d'inverse A_{-m} et ainsi, pour tout $n \in \mathbb{N}$, $A_1^{-n} = (A_1^n)^{-1} = A_n^{-1} = A_{-n}$.

Il en résulte que, pour tout $n \in \mathbb{Z}$, $A_1^n = A_n$.

Par suite, on a

$$\langle A_1 \rangle = \{A_1^n \mid n \in \mathbb{N}\} = \{A_n \mid n \in \mathbb{N}\} = G.$$

Donc G est engendré par $A_1 = \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix}$ et donc G est monogène.

De plus, comme pour tous $n, m \in \mathbb{Z}$ avec $n \neq m$, on a $3^n \neq 3^m$; donc $A_n \neq A_m$. Ainsi, G est infini et monogène donc, d'après le théorème de classification des groupes monogènes (Théorème 4), il est isomorphe à $\mathbb{Z}$.

Remarque : bon, cette correction est quelque peu "surfaite" dans le sens où elle veut illustrer le théorème de classification des groupes monogènes. Il serait plus direct et même plus rapide de montrer que l'application $n \mapsto A_n$ est un isomorphisme de groupes de $\mathbb{Z}$ dans G (d'ailleurs tous les calculs qu'on a fait ici le prouvent, hormis la surjectivité qui est immédiate).

c. Les générateurs de $\mathbb{Z}/n\mathbb{Z}$

On a vu précédemment que $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\{\bar{1}\}$. Dans ce paragraphe, on va caractériser les éléments de $\mathbb{Z}/n\mathbb{Z}$ qui, comme $\bar{1}$, engendrent $\mathbb{Z}/n\mathbb{Z}$. Pour cela, nous avons besoin d'un théorème vu en Sup', très important en arithmétique : le théorème de Bézout. Rappelons ici son énoncé et sa démonstration.

Proposition 11. Relation de Bézout

Soit $a, b \in \mathbb{Z}$ non tous nuls. On pose $d = \text{pgcd}(a, b)$. Il existe $u, v \in \mathbb{Z}$ tels que :

$$au + bv = d.$$

Correction.

La démonstration vue en Sup' de ce résultat est basée sur la remontée de l'algorithme d'Euclide. Mais on peut en donner une autre démonstration, non constructive cette fois, qui repose sur la caractérisation des sous-groupes de $\mathbb{Z}$ (Théorème 2).

D'après la question 2 de l'exercice 4, on a l'égalité :

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Or $d = d \times 1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, donc il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$.

Théorème 5. Théorème de Bézout

Soit $a, b \in \mathbb{Z}$. Les entiers a et b sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1.$$

Démonstration.

($\Rightarrow$) On suppose a et b premiers entre eux. Alors $\text{pgcd}(a, b) = 1$, donc, d'après la proposition 11 (Relation de Bézout), il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

($\Leftarrow$) On suppose qu'il existe $u, v \in \mathbb{Z}$ tels que $nu + mv = 1$. Pour tout diviseur d positif commun de a et b , on a d divise $au + bv = 1$; donc $d = 1$.

Par suite, $\text{pgcd}(a, b) = 1$ et donc a et b sont premiers entre eux. □

Proposition 12.

Soit $n \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. La classe $\bar{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, k et n sont premiers entre eux.

Démonstration.

- ($\Rightarrow$). On suppose que $\mathbb{Z}/n\mathbb{Z} = \langle \bar{k} \rangle$. Alors il existe $u \in \mathbb{Z}$ tel que

$$u\bar{k} = \bar{1}.$$

Par suite, $uk \equiv 1 \pmod{n}$, et donc, il existe $v \in \mathbb{Z}$ tel que

$$uk + vn = 1.$$

D'après le théorème de Bézout (Théorème 5), il en résulte que k et n sont premiers entre eux.

- ($\Leftarrow$). On suppose que k et n sont premiers entre eux. D'après le théorème de Bézout (Théorème 5), il existe $u, v \in \mathbb{Z}$ tels que :

$$uk + vn = 1.$$

Par suite, pour tout $p \in \llbracket 0, n-1 \rrbracket$,

$$p = puk + pvn,$$

d'où, si on note $q = pu$, $p \equiv puk = qk \pmod n$ i.e.

$$\bar{p} = q\bar{k}.$$

Par suite, $\bar{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$.

□

5. Ordre d'un élément

Définition 4. Ordre d'un élément

Soit G un groupe et $x \in G$. On dit que x est **d'ordre fini**, ou encore que x est un **élément de torsion**, si le cardinal de $\langle x \rangle$ est fini.

Dans ce cas, on appelle **ordre de x** et on note $o(x)$ le nombre entier naturel :

$$o(x) = \#\langle x \rangle.$$

Si x n'est pas d'ordre fini, on dit que x est **d'ordre infini** et on note $o(x) = +\infty$.

Exemple 5.

- Dans un groupe G d'élément neutre e , e est d'ordre fini égal à 1 et c'est le seul élément d'ordre 1.
- Dans un groupe G fini, tout élément est d'ordre fini, inférieur au cardinal de G .
- Dans $\mathbb{Z}$, tout entier non nul est d'ordre infini.
- Dans $\mathbb{Z}/12\mathbb{Z}$, par exemple : $o(\bar{1}) = 12$; $o(\bar{3}) = 4$; $o(\bar{6}) = 2$.
- Dans $GL_2(\mathbb{Z})$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ est d'ordre 2 et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

- On a $\langle e \rangle = \{e\}$ donc e est d'ordre fini égal à 1. Puis, pour tout $x \in G$ avec $x \neq e$, $\{e, x\} \subset \langle x \rangle$; d'où $2 \leq o(x)$.
- Pour tout $x \in G$, on a $\langle x \rangle \subset G$ donc G étant un ensemble fini, $\langle x \rangle$ est fini et on a de plus $o(x) \leq \#G$.
- Pour tout $n \in \mathbb{Z} \setminus \{0\}$, on a $\langle n \rangle = n\mathbb{Z}$ et $n\mathbb{Z}$ est un ensemble infini car $n \neq 0$, d'où $o(n) = +\infty$.
- Plaçons dans $\mathbb{Z}/12\mathbb{Z}$. On a :
 $\star \langle \bar{1} \rangle = \mathbb{Z}/12\mathbb{Z}$ donc $o(\bar{1}) = 12$;

$\star \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ donc $o(\overline{3}) = 4$;
 $\star \langle \overline{6} \rangle = \{\overline{0}, \overline{6}\}$ donc $o(\overline{6}) = 2$.
 — Dans $GL_2(\mathbb{Z})$, on a :

$$\left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ I_2, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$
 donc $o\left(\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 2$ et

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$
 donc $o\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = +\infty$.

Théorème 6. Caractérisation de l'ordre d'un élément

Soit G un groupe et $x \in G$ un élément d'ordre fini $n \in \mathbb{N}^*$.

- i) Pour tout $k \in \mathbb{Z}$, $x^k = e$ si, et seulement si, n divise k .
- ii) Le nombre n est le plus petit entier naturel non nul qui vérifie l'égalité $x^k = e$ où k est un entier relatif.

Démonstration.

On note $H = \langle x \rangle$. Alors, comme x est d'ordre fini n , H est un groupe cyclique d'ordre n , il est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\varphi : \overline{k} \rightarrow x^k$ un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans H d'après la classification des groupes monogènes (Théorème 4).

Pour tout $k \in \mathbb{Z}$, on a :

$$x^k = e \Leftrightarrow \varphi(\overline{k}) = e \Leftrightarrow \overline{k} \in \text{Ker}(\varphi) = \{\overline{0}\} \Leftrightarrow \overline{k} = \overline{0},$$

d'où :

$$x^k = e \Leftrightarrow k \in n\mathbb{Z} \text{ i.e. } n \text{ divise } k.$$

De plus, n étant le plus petit multiple strictement positif de n , n est la plus petite solution entière non nulle de l'équation $x^k = e$ d'inconnue $k \in \mathbb{Z}$. $\square$

Méthode : détermination de l'ordre d'un élément x dans un groupe G .

En vertu de la proposition précédente, on peut déterminer l'ordre de x en résolvant l'équation $x^k = e$ d'inconnue $k \in \mathbb{N}^*$: l'ordre de x est alors le plus petit élément de l'ensemble des solutions de cette équation (attention : dans $\mathbb{N}^*$!)

Exercice 12.

Soit G un groupe et x un élément d'ordre fini n .

1. Soit $d \in \mathbb{N}$ tel que $d|n$. Quel est l'ordre de x^d ?
2. Soit $p \in \mathbb{N}$. Quel est l'ordre de x^p ?

Correction.

1. Il existe $q \in \mathbb{N}$ tel que $n = dq$. Alors on a, pour tout $k \in \mathbb{Z}$:

$$(x^d)^k = e \Leftrightarrow x^{dk} = e \Leftrightarrow n|dk \Leftrightarrow dq|dk \Leftrightarrow q|k$$

Ainsi, $(x^d)^k = e \Leftrightarrow k \in q\mathbb{Z}$ et q est le plus petit entier naturel non nul de l'ensemble $q\mathbb{Z}$ donc $o(x^d) = q = n/d$.

2. On pose $d = \text{pgcd}(p, n)$, $n' = n/d$ et $p' = p/d$. Alors n' et p' sont premiers entre eux, donc, d'après le lemme de Gauss, on a, pour tout $k \in \mathbb{Z}$:

$$(x^p)^k = e \Leftrightarrow x^{pk} = e \Leftrightarrow n|pk \Leftrightarrow n'd|p'k \Leftrightarrow n'|p'k \Leftrightarrow n'|k.$$

Ainsi, $(x^p)^k = e \Leftrightarrow k \in n'\mathbb{Z}$ et n' est le plus petit entier naturel non nul de l'ensemble $n'\mathbb{Z}$ donc $o(x^p) = n/d (= \text{ppcm}(p, n)/p)$.

Proposition 13.

Soit G un groupe fini. Alors tout élément x de G est d'ordre fini et $o(x)$ divise $\#G$.

Démonstration.

Pour tout $x \in G$, on a $\langle x \rangle \subset G$, donc $o(x) = \#\langle x \rangle \leq \#G$ d'où x est d'ordre fini. Soit $x \in G$.

Montrons $o(x)$ divise $\#G$. *Démonstration dans le cas où G est commutatif.*

Notons $n = \#G$. L'application $g \mapsto xg$ est une bijection de G dans G (en effet, $g \mapsto x^{-1}g$ est la réciproque de cette application) donc, on a, par le changement bijectif d'indice $g = xh$:

$$\prod_{g \in G} g = \prod_{h \in G} xh = x^n \prod_{h \in G} h,$$

Donc $x^n = e$. Par suite, $o(x)|n$. □

Remarque 5.

La démonstration proposée pour le résultat précédent est astucieuse et n'est valable que dans le cas particulier où G est commutatif.

Pour la démonstration dans le cas non commutatif, on prouve en fait un énoncé plus général et très utile : le théorème de Lagrange. Celui-ci affirme que l'ordre de tout sous-groupe d'un groupe de cardinal fini divise l'ordre du groupe.

Ce résultat n'est pas explicitement au programme (on ne peut donc pas l'utiliser dans nos

raisonnements, contrairement à la proposition précédente qui en est un cas particulier) mais c'est un grand classique de la théorie des groupes finis. On en propose un plan de démonstration dans l'exercice suivant.

Exercice 13. *Théorème de Lagrange*

1. Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence sur X .
 - (a) Montrer que deux classes d'équivalence de $\mathcal{R}$ sont soit disjointes, soit égales.
 - (b) En déduire que la famille des classes d'équivalence de $\mathcal{R}$ forment une partition de X .
2. (a) Soit $(G, \cdot)$ un groupe et H un sous-groupe de G . Montrer que la relation $\sim$ définie, pour $x, y \in G$, par :

$$x \sim y \Leftrightarrow x^{-1}y \in H,$$

est une relation d'équivalence sur G .

- (b) En déduire le théorème de Lagrange :

Théorème de Lagrange

L'ordre de tout sous-groupe d'un groupe d'ordre fini divise l'ordre du groupe.

Correction.

1. Soit X un ensemble et $\mathcal{R}$ une relation d'équivalence sur X .
 - (a) Soit C, C' deux classes d'équivalence de $\mathcal{R}$. Si $C \cap C' \neq \emptyset$ alors il existe $z \in C \cap C'$ d'où, par définition, $C = \text{Cl}_z = C'$. D'où l'alternative.
 - (b) Les classes d'équivalences sont non vides par définition et disjointes. De plus, pour tout $x \in X$, $x \in \text{Cl}_x$ donc la famille des classes d'équivalence forme une partition de X .
2. (a) Montrons que $\sim$ est une relation d'équivalence sur G .
 - *Réflexivité.* Soit $x \in G$. On a $x^{-1}x = e \in H$ car H est un sous-groupe de G . D'où $x \sim x$.
 - *Symétrie.* Soit $x, y \in G$. On suppose $x \sim y$ i.e. $x^{-1}y \in H$. Alors $y^{-1}x = (x^{-1}y)^{-1} \in H$ car H est un sous-groupe de G . D'où $y \sim x$.
 - *Transitivité.* Soit $x, y, z \in G$. On suppose $x \sim y$ et $y \sim z$ i.e. $x^{-1}y \in H$ et $y^{-1}z \in H$. Alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ car H est un sous-groupe de G . D'où $x \sim z$.

Il en résulte que $\sim$ est une relation d'équivalence sur G .
- (b) Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G . D'après la question 1b et 2a, l'ensemble des classes d'équivalence de la relation d'équivalence $\sim$ forme une partition de G et est fini (car G est fini) de cardinal disons $k \in \mathbb{N}^*$.

De plus, pour $x \in G$, on a :

$$\text{Cl}_x = \{y \in G \mid x \sim y\} = \{y \in G \mid x^{-1}y \in H\} = \{y \in G \mid y \in xH\} = xH,$$

et de plus, l'application $g \mapsto xg$ est bijective de G dans G donc $\#\text{Cl}_x = \#xH = \#H$. Par suite, si $C_1, \dots, C_k$ est la liste exhaustive des classes d'équivalence deux à deux différentes de la relation d'équivalence $\sim$, on a :

$$\#G = \# \left(\bigcup_{i=1}^k C_i \right) = \sum_{i=1}^k \underbrace{\#C_i}_{=\#H} = k \times \#H.$$

Il en résulte que $\#H$ divise $\#G$.

Partie **

Rappels de Sup' sur les anneaux

1. Structure d'anneau

a. Définitions et exemples

Définition **1. Anneau

Soit A un ensemble muni de deux lois de composition interne sur $+$ et $\cdot$. On dit que le triplet $(A, +, \cdot)$ est **une structure d'anneau**, ou plus simplement A est un **anneau** (muni des lois $+$ et $\cdot$), si :

- i) $(A, +)$ est un groupe *commutatif* d'élément neutre 0_A ;
- ii) la loi $\cdot$ est associative ;
- iii) *Distributivité* : pour tous $a, b, c \in A$,

$$a.(b + c) = a.b + a.c \quad \text{et} \quad (b + c).a = b.a + c.a$$

- iv) *Unité* : la loi $\cdot$ possède un élément neutre noté 1_A et appelé **unité de A** .

On dit de plus qu'un anneau A est **commutatif** si la loi $\cdot$ est commutative.

Définition **2. Corps

Un anneau $(A, +, \cdot)$ commutatif tel que $(A \setminus \{0_A\}, \cdot)$ est un groupe est appelé un **corps**.

Remarque **1.

- Un anneau A est dit trivial si $0_A = 1_A$. Dans ce cas $A = \{0_A\}$.
- Il découle de la définition qu'un corps ne peut pas être un anneau trivial.

Exemple **1.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs munis de l'addition et de la multiplication des nombres. Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont même des corps munis de ces opérations.
- $\mathbb{R}[X], \mathbb{C}[X]$ sont des anneaux commutatifs munis de l'addition et de la multiplication des polynômes.
- Soit $n \in \mathbb{N}$, $M_n(\mathbb{R})$ et $M_n(\mathbb{C})$ sont des anneaux non commutatifs (sauf pour $n = 1$) munis de l'addition et de la multiplication des matrices.
- Soit E un espace vectoriel. $\mathcal{L}(E)$ est un anneau non commutatif (sauf si E est de dimension inférieure ou égale à 1) muni de l'addition et de la composition des applications.

b. Anneaux intègres

Définition **3. Anneau intègre

Soit A un anneau. On dit que A est **intègre** si, pour tous $a, b \in A$,

$$a.b = 0_A \Rightarrow a = 0_A \text{ ou } b = 0_A.$$

Remarque **2.

- Dans un anneau, un élément $a \neq 0_A$ est un **diviseur de zéro** s'il existe $b \neq 0_A$ tel que $a.b = 0_A$.
- Dans un anneau intègre, tout élément $a \neq 0_A$ est **régulier** pour la loi $\cdot$ i.e. pour tous $x, y \in A$, $ax = ay \Rightarrow x = y$.

Exercice **1.

1. Parmi les exemples d'anneaux précédents, lesquels sont intègres et lesquels ne le sont pas ?
2. Donner un exemple d'anneau commutatif non trivial qui n'est pas intègre.

Correction.

1. — $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont intègres.
— $\mathbb{R}[X], \mathbb{C}[X]$ sont intègres.
— Soit $n \in \mathbb{N}$, $M_n(\mathbb{R})$ et $M_n(\mathbb{C})$ ne sont pas intègres.
— Soit E un espace vectoriel. $\mathcal{L}(E)$ n'est pas intègre.
2. On considère $\mathcal{F}(\mathbb{R}, \mathbb{R})$ muni de la l'addition et de la multiplication des fonctions. Alors, $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ est un anneau commutatif mais n'est pas intègre : si on considère $A, B \subset \mathbb{R}$ non vides et disjoints, alors le produit des fonctions indicatrices de A et B est la fonction nulle.

2. Sous-anneaux

Définition **4. Sous-anneau

Soit $(A, +, \cdot)$ un anneau et $B \subset A$. On dit que B est un **sous-anneau** de A si :

- i) B un sous-groupe de $(A, +)$;
- ii) B est stable par $\cdot$ i.e. pour tout $a, b \in B$, $a.b \in B$.
- iii) L'unité 1_A de A appartient à B .

Remarque **3.

Si $(A, +, \cdot)$ est un anneau et $B \subset A$ est un sous-anneau de A , alors $(B, +, \cdot)$ est un anneau.

Définition **5. Sous-corps

Soit $(K, +, \cdot)$ un corps et $L \subset K$. On dit que L est un **sous-corps de K** si L est un sous-anneau de K qui est un corps.

Proposition **1. Caractérisation des sous-anneaux

Soit $(A, +, \cdot)$ un anneau et $B \subset A$. L'ensemble B est un sous-anneau de A si, et seulement si,

- i) $1_A \in B$;
- ii) pour tous $x, y \in B$, $x - y \in B$;
- iii) pour tous $x, y \in B$, $x \cdot y \in B$.

Démonstration.

- $(\Rightarrow)$. Immédiat ;
- $(\Leftarrow)$. Il suffit de montrer que $0_A \in B$. On a, d'après i), $1_A \in B$ et d'après ii)

$$0_A = 1_A - 1_A \in B.$$

□

Exemple **2.

- $\mathbb{R}$ est un sous-corps de $\mathbb{C}$, $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ et $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.
- L'ensemble des matrices diagonales est un sous-anneau de $M_n(\mathbb{R})$.

Exercice **2.

1. Montrer que $\mathbb{Z} + i\mathbb{Z} = \{n + im \mid n, m \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{C}$;
2. Montrer que $\mathbb{Q} + \sqrt{2}\mathbb{Q} = \{p + \sqrt{2}q \mid p, q \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{R}$.

Correction.

1. i) On a $1 = \underbrace{1}_{\in \mathbb{Z}} + i \cdot \underbrace{0}_{\in \mathbb{Z}} \in \mathbb{Z} + i\mathbb{Z}$.

ii) Soit $x = n + im, y = n' + im' \in \mathbb{Z} + i\mathbb{Z}$. On a :

$$\begin{aligned} x - y &= n + im - (n' + im') \\ &= \underbrace{n - n'}_{\in \mathbb{Z}} + i \underbrace{(m - m')}_{\in \mathbb{Z}} \end{aligned}$$

Donc $x - y \in \mathbb{Z} + i\mathbb{Z}$.

iii) Soit $x = n + im, y = n' + im' \in \mathbb{Z} + i\mathbb{Z}$. On a :

$$x.y = (n + im).(n' + im') \\ \underbrace{nn' - mm'}_{\in \mathbb{Z}} + i \underbrace{(nm' + n'm)}_{\in \mathbb{Z}}$$

Donc $x.y \in \mathbb{Z} + i\mathbb{Z}$.

Il en résulte que $\mathbb{Z} + i\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$.

2. i) On a $1 = \underbrace{1}_{\in \mathbb{Q}} + \sqrt{2} \cdot \underbrace{0}_{\in \mathbb{Q}} \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

ii) Soit $x = p + \sqrt{2}q, y = p' + \sqrt{2}q' \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$. On a :

$$x - y = p + \sqrt{2}q - (p' + \sqrt{2}q') \\ \underbrace{p - p'}_{\in \mathbb{Q}} + \sqrt{2} \underbrace{(q - q')}_{\in \mathbb{Q}}$$

Donc $x - y \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

iii) Soit $x = p + \sqrt{2}q, y = p' + \sqrt{2}q' \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$. On a :

$$x.y = (p + \sqrt{2}q).(p' + \sqrt{2}q') \\ \underbrace{pp' + 2qq'}_{\in \mathbb{Q}} + \sqrt{2} \underbrace{(pq' + p'q)}_{\in \mathbb{Q}}$$

Donc $x.y \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

Il en résulte que $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ est un sous-anneau de $\mathbb{R}$. Montrons que $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ est un corps. Soit $x = p + \sqrt{2}q \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$ avec $p, q \neq 0$. Alors en particulier, $x \in \mathbb{R}^*$: en effet, $\mathbb{Q} + \sqrt{2}\mathbb{Q} \subset \mathbb{R}$ et $p + \sqrt{2}q \neq 0$ car sinon le rationnel p serait égal à l'irrationnel $-\sqrt{2}q$ ce qui est impossible. Ainsi on a :

$$x^{-1} = \frac{1}{x} = \frac{1}{p + \sqrt{2}q} = \frac{p - \sqrt{2}q}{p^2 - 2q^2} = \underbrace{\frac{p}{p^2 - 2q^2}}_{\in \mathbb{Q}} + \sqrt{2} \underbrace{\frac{-q}{p^2 - 2q^2}}_{\in \mathbb{Q}} \in \mathbb{Q} + \sqrt{2}\mathbb{Q}.$$

Par suite, tout élément non nul est inversible. Il en résulte que $\mathbb{Q} + \sqrt{2}\mathbb{Q}$ est un corps et donc un sous-corps de $\mathbb{R}$.

3. Inversibles d'un anneau

Définition **6. Groupe des inversibles

Soit $(A, +, \cdot)$ un anneau. On appelle **groupe des inversibles** (ou **groupe des unités**) et on note $A^\times$ (ou $U(A)$) l'ensemble des éléments inversibles de $(A, \cdot)$.

Proposition **2.

Soit $(A, +, \cdot)$ un anneau. Le groupe des inversibles $A^\times$ muni de la loi $\cdot$ est un groupe.

Démonstration.

Montrons que $\cdot$ est une loi de composition *interne* sur $A^\times$: pour tous $x, y \in A^\times$, x, y sont inversibles et

$$(xy).(y^{-1}x^{-1}) = 1_A,$$

donc xy est inversible, d'où $xy \in A^\times$. Par suite $\cdot$ est bien une loi de composition interne sur $x, y \in A^\times$.

- i) La loi $\cdot$ est associative car $(A, +, \cdot)$ est un anneau ;
- ii) 1_A est l'élément neutre de $\cdot$ donc il suffit de vérifier que $1_A \in A^\times$. En effet on $1_A.1_A = 1_A$ donc 1_A est inversible d'où $1_A \in A^\times$;
- iii) Tout élément x de $A^\times$ est inversible par définition et x^{-1} étant également inversible, il appartient à $A^\times$.

Donc $(A^\times, \cdot)$ est un groupe □

Exemple **3.

- $\mathbb{Z}^\times = \{-1, 1\}$; $\mathbb{R}^\times = \mathbb{R}^*$; $\mathbb{C}^\times = \mathbb{C}^*$;
- $\mathbb{K}[X]^\times = \mathbb{K}^*$;
- $M_n(\mathbb{K})^\times = GL_n(\mathbb{K})$

4. Morphismes d'anneaux

a. Définition

Définition **7. Morphisme d'anneaux

Soit A, B deux anneaux et $f : A \rightarrow B$ une application. On dit que f est un **morphisme d'anneaux** si :

- i) pour tous $x, y \in A$, $f(x + y) = f(x) + f(y)$;
- ii) pour tous $x, y \in A$, $f(xy) = f(x)f(y)$;
- iii) $f(1_A) = 1_B$.

Un morphisme d'anneaux bijectif est appelé un **isomorphisme d'anneaux**.

Exercice **3.

Soit A un anneau non trivial et $u \in A^\times$. Montrer que $\varphi_u : x \mapsto uxu^{-1}$ est un isomorphisme d'anneaux.

b. Noyaux, images et sous-anneaux

Définition **8. Noyau/Image

Soit A, B des anneaux et $f : A \rightarrow B$ un morphisme d'anneaux.

— Le **noyau** de f est le sous-ensemble de A

$$\text{Ker}(f) = \{a \in A \mid f(a) = 0_B\}.$$

— L'**image** de f est le sous-ensemble de B

$$\text{Im}(f) = f(A) = \{f(a) \mid a \in A\}.$$

Proposition **3.

Soit A, B des anneaux et $f : A \rightarrow B$ un morphisme d'anneaux. L'ensemble $\text{Im}(f)$ est un sous-anneau de B .

Démonstration.

i) $1_B = f(1_A) \in \text{Im}(f)$;

ii) pour $f(x), f(y) \in \text{Im}(f)$ avec $x, y \in A$,

$$f(x) - f(y) = f(x - y) \in \text{Im}(f);$$

iii) pour $f(x), f(y) \in \text{Im}(f)$ avec $x, y \in A$,

$$f(x)f(y) = f(xy) \in \text{Im}(f).$$

Donc $\text{Im}(f)$ est un sous-anneau de B . □

Remarque **4. ATTENTION!

Contrairement au cas des groupes où le noyau d'un morphisme est un sous-groupe, le **noyau d'un morphisme d'anneaux n'est JAMAIS un sous-anneau de l'anneau de départ** (à moins que l'anneau d'arrivée ne soit trivial).

En effet, si $B \neq \{0_B\}$, $1_A \notin \text{Ker}(f)$ car $f(1_A) = 1_B \neq 0_B$. Ainsi, $\text{Ker}(f)$ ne peut pas être un sous-anneau puisqu'il ne contient pas 1_A .

c. Morphismes et groupes des inversibles

Proposition **4.

Soit A, B des anneaux. Si $f : A \rightarrow B$ est un morphisme d'anneaux alors f induit un morphisme de groupes de $A^\times$ dans $B^\times$.

En particulier, si A et B sont isomorphes en tant qu'anneaux, $A^\times$ et $B^\times$ sont isomorphes en tant que groupes.

Démonstration.

Soit $f : A \rightarrow B$ un morphisme d'anneaux et $g = f|_{A^\times}$. Pour tout $a \in A^\times$, il existe $b \in A^\times$ tel que $ab = 1_A$ d'où, f étant un morphisme d'anneaux :

$$g(a)g(b) = f(a)f(b) = f(ab) = f(1_A) = 1_B,$$

et donc $g(a) \in B^\times$.

Par suite, g est une application de $A^\times$ dans $B^\times$ et, et pour tout $a, a' \in A^\times$, comme f est un morphisme d'anneau, on a :

$$g(aa') = f(aa') = f(a)f(a') = g(a)g(a'),$$

donc g est un morphisme de groupes.

De plus, si f est un isomorphisme d'anneaux, f^{-1} l'est aussi et leur restriction à $A^\times$ et $B^\times$ respectivement sont des morphismes de groupes réciproque l'un de l'autre, d'où $A^\times$ et $B^\times$ sont isomorphes en tant que groupes dans ce cas. $\square$

Partie B

Compléments sur les anneaux ; idéaux

1. Structure d'anneau produit

Définition-Proposition 5. *Structure d'anneau produit*

Soit $n \in \mathbb{N}^*$, $A_1, \dots, A_n$ des anneaux. On note $A = A_1 \times \dots \times A_n$. On considère les lois de composition suivantes sur A : pour $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in A$,

$$x + y = (x_1 + \dots + y_n, x_n + \dots + y_n) \quad \text{et} \quad x \cdot y = (x_1 \cdot y_1, \dots, x_n \cdot y_n).$$

Alors A muni de ces lois est un anneau et :

- L'élément nul de A est $0_A = (0_{A_1}, \dots, 0_{A_n})$.
- L'unité de A est $1_A = (1_{A_1}, \dots, 1_{A_n})$.

L'anneau A est appelé **anneau produit** des anneaux $A_1, \dots, A_n$.

Démonstration.

- $(A, +)$ est un groupe commutatif d'élément neutre $0_A = (0_{A_1}, \dots, 0_{A_n})$ comme groupe produit des groupes commutatifs $(A_1, +), \dots, (A_n, +)$.
- La loi $\cdot$ est associative par associativité des lois multiplicatives de $A_1, \dots, A_n$.
- *Distributivité* : Soit $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n), z = (z_1, \dots, z_n) \in A$, alors :

$$\begin{aligned} x \cdot (y + z) &= (x_1, \dots, x_n) \cdot (y_1 + z_1, \dots, y_n + z_n) \\ &= (x_1 \cdot (y_1 + z_1), \dots, x_n \cdot (y_n + z_n)) \\ &= (x_1 \cdot y_1 + x_1 \cdot z_1, \dots, x_n \cdot y_n + x_n \cdot z_n) \\ &= (x_1 \cdot y_1, \dots, x_n \cdot y_n) + (x_1 \cdot z_1, \dots, x_n \cdot z_n) \\ &= (x_1, \dots, x_n) \cdot (y_1, \dots, y_n) + (x_1, \dots, x_n) \cdot (z_1, \dots, z_n) \\ &= x \cdot y + x \cdot z \end{aligned}$$

et de même

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

- Pour tous $x = (x_1, \dots, x_n) \in A$,

$$\begin{aligned} x \cdot 1_A &= (x_1, \dots, x_n) \cdot (1_{A_1}, \dots, 1_{A_n}) \\ &= (x_1 \cdot 1_{A_1}, \dots, x_n \cdot 1_{A_n}) \\ &= (x_1, \dots, x_n) \\ &= x \\ &= (1_{A_1} \cdot x_1, \dots, 1_{A_n} \cdot x_n) \\ &= (1_{A_1}, \dots, 1_{A_n}) \cdot (x_1, \dots, x_n) \\ &= 1_A \cdot x \end{aligned}$$

donc $x.1_A = x = 1_A.x$ donc 1_A est l'élément neutre pour la multiplication.
Il en résulte que $(A, +, \cdot)$ est un anneau. $\square$

Proposition 14.

Soit $n \in \mathbb{N}^*$, $A_1, \dots, A_n$ des anneaux et on considère l'anneau produit $A_1 \times \dots \times A_n$. On a :

$$(A_1 \times \dots \times A_n)^\times = A_1^\times \times \dots \times A_n^\times.$$

Démonstration.

On a $(a_1, \dots, a_n) \in (A_1 \times \dots \times A_n)^\times$ si, et seulement si, il existe $(b_1, \dots, b_n) \in A_1 \times \dots \times A_n$ tel que $(a_1, \dots, a_n).(b_1, \dots, b_n) = (1_{A_1}, \dots, 1_{A_n})$ si, et seulement si, il existe $a_1 \in A_1, \dots, b_n \in A_n$ tels que $a_1.b_1 = 1_{A_1}, \dots, a_n.b_n = 1_{A_n}$ si, et seulement si, $(a_1, \dots, a_n) \in A_1^\times \times \dots \times A_n^\times$. $\square$

Exercice 14.

Soit $n \in \mathbb{N}^*$, $A_1, \dots, A_n$ des anneaux. Montrer que $A = A_1 \times \dots \times A_n$ est commutatif si, et seulement si, $A_1, \dots, A_n$ sont commutatifs.

Correction.

Soit $x_1, y_1 \in A_1, \dots, x_n, y_n \in A_n$. On a :

$$(x_1, \dots, x_n).(y_1, \dots, y_n) = (y_1, \dots, y_n).(x_1, \dots, x_n),$$

si, et seulement si,

$$(x_1 y_1, \dots, x_n y_n) = (y_1 x_1, \dots, y_n x_n),$$

si, et seulement si,

$$x_1 y_1 = y_1 x_1, \dots, x_n y_n = y_n x_n.$$

2. Idéaux d'un anneau commutatif

a. Définition et premières propriétés

Définition 6. Idéal d'un anneau commutatif

Soit A un anneau commutatif et $I \subset A$. On dit que I est un **idéal** de A si :

- i) I est un sous-groupe de $(A, +)$;
- ii) I est stable par multiplication par les éléments de A , i.e. pour tout $x \in I$ et tout $a \in A$,

$$xa \in I.$$

Exemple 6.

Soit A, B des anneaux commutatifs.

- A et $\{0_A\}$ sont des idéaux de A .
- Pour $f : A \rightarrow B$ un morphisme d'anneaux, $\text{Ker}(f)$ est un idéal de A .
- Pour $n \in \mathbb{Z}$, $n\mathbb{Z}$ est un idéal de l'anneau $(\mathbb{Z}, +, \times)$.
- L'ensemble $I = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}) \mid \forall x \in \mathbb{R}_+, f(x) = 0\}$ est un idéal de l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$.

- A est un sous-groupe de $(A, +)$ qui est un groupe par définition et il est stable par produit car $\cdot$ est une loi de composition interne sur A ; d'où A est un idéal de A . L'ensemble $\{0_A\}$ est un sous-groupe de $(A, +)$ car 0_A est l'élément neutre de $+$ et il est stable par produit avec les éléments de A car, pour tout $a \in A$, $0_A \cdot a = 0_A$; d'où $\{0_A\}$ est un idéal de A .
- i) $\text{Ker}(f)$ est un sous-groupe du groupe $(A, +)$ comme image réciproque de $\{0_B\}$ par f .

ii) Soit $x \in \text{Ker}(f)$ et $a \in A$; on a :

$$f(xa) = f(x)f(a) = 0_B f(a) = 0_B,$$

donc $xa \in \text{Ker}(f)$.

Ainsi $\text{Ker}(f)$ est un idéal de A .

- i) $n\mathbb{Z} = \langle n \rangle$ est un sous-groupe du groupe $(\mathbb{Z}, +)$.
- ii) Soit $nk \in n\mathbb{Z}$ et $a \in \mathbb{Z}$; on a :

$$(nk)a = n(ka) \in n\mathbb{Z},$$

donc $(nk)a \in n\mathbb{Z}$.

Ainsi, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

- On peut bien-sûr montrer que I est un idéal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ avec la définition mais on peut également remarquer que l'application $r : f \mapsto f|_{\mathbb{R}_+}$, qui à une fonction de $\mathbb{R}$ dans lui-même associe sa restriction à $\mathbb{R}_+$, est un morphisme d'anneaux de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ dans $\mathcal{F}(\mathbb{R}_+, \mathbb{R})$ et que $I = \text{Ker}(r)$ est ainsi un idéal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$ comme noyau d'un morphisme d'anneaux d'après ce qui précède.

Exercice 15.

Soit A un anneau et I un idéal de A .

1. Montrer que si $1_A \in I$, alors $I = A$.
2. Soit $u \in A^\times$. En déduire que si $u \in I$, alors $I = A$.

Correction.

1. On suppose $1_A \in I$. On a $I \subset A$. Montrons $A \subset I$. Soit $a \in A$. Alors

$$\underbrace{1_A}_{\in I} \cdot \underbrace{a}_{\in A} \in I.$$

Donc $a \in I$; d'où $A \subset I$.
Il en résulte que $I = A$.

2. Si $u \in I$, alors

$$1_A = \underbrace{u}_{\in I} \cdot \underbrace{u^{-1}}_{\in A} \in I.$$

Donc d'après la question précédente $I = A$.

Proposition 15. Image réciproque d'un idéal

Soit A, B des anneaux commutatifs, $f : A \rightarrow B$ un morphisme et J un idéal de B . L'ensemble $f^{-1}(J)$ est un idéal de A .

Démonstration.

- i) $f^{-1}(J)$ est un sous-groupe du groupe $(A, +)$ comme image réciproque du sous-groupe J de $(B, +)$ par f .
- ii) Soit $x \in f^{-1}(J)$ et $a \in A$; on a :

$$f(xa) = \underbrace{f(x)}_{\in J} \underbrace{f(a)}_{\in B} \in J$$

donc $xa \in f^{-1}(J)$.
Donc $f^{-1}(J)$ est un idéal de A . □

Remarque 6.

Avec la proposition précédente, on retrouve donc que le noyau d'un morphisme d'anneaux est un idéal de l'anneau de départ.

Proposition 16. Intersection d'idéaux

Soit A un anneau commutatif.

Toute intersection d'une famille d'idéaux de A est un idéal de A .

Démonstration.

Soit K un ensemble et $(I_k)_{k \in K}$ une famille d'idéaux de A .

L'ensemble $I = \bigcap_{k \in K} I_k$ est un sous-groupe de $(A, +)$ comme intersection de sous-groupes de $(A, +)$.

Soit $x \in I$ et $a \in A$. Pour tout $k \in K$, $x \in I_k$ qui est un idéal de A , donc $xa \in I_k$. Par suite, $xa \in I$.

Il en résulte que I est un idéal de A . □

b. Idéaux engendrés et idéaux principaux

Définition-Proposition 7.

Soit A un anneau commutatif et $X \subset A$. On appelle **idéal engendré par X** l'ensemble :

$$I = \bigcap_{J \in \mathcal{I}_X} J \text{ où } \mathcal{I}_X = \{J \text{ idéal de } A \mid X \subset J\};$$

autrement dit, I est l'intersection de tous les idéaux contenant X .

L'idéal engendré par X est le plus petit idéal contenant X .

Démonstration.

I est un idéal comme intersection d'idéaux et comme $X \subset J$ pour tout $J \in \mathcal{I}_X$, $X \subset I$.

Par suite, I est le plus petit idéal contenant X ; en effet, I est inclus dans tous les idéaux contenant X car il est défini comme leur intersection. $\square$

Définition-Proposition 8.

Soit A un anneau commutatif et $x \in A$. L'idéal engendré par le singleton $\{x\}$ est égal à l'ensemble :

$$xA = \{xa \mid a \in A\} \quad (= Ax = \{ax \mid a \in A\}).$$

L'élément x est appelé **générateur** de l'idéal xA engendré par $\{x\}$.

Démonstration.

On note $I_x = \bigcap_{J \in \mathcal{I}_{\{x\}}} J$ l'idéal engendré par $\{x\}$. Montrons que $I_x = xA$.

$I_x \subset xA$:

Comme I_x est contenu dans tous les idéaux contenant x , montrons que xA est un idéal contenant x :

On a $x = x.1_A \in xA$ donc xA contient x .

On vient de voir que xA est non vide (on aurait pu également voir que $0_A = x.0_A \in xA$) et pour tous $xa, xb \in xA$ avec $a, b \in A$, on a, par distributivité de $\cdot$ par rapport à $+$:

$$xa - xb = x(a - b) \in xA$$

donc xA est un sous-groupe de $(A, +)$.

De plus, pour tout $b \in A$ et tous $xa \in xA$ avec $a \in A$, par associativité de $\cdot$:

$$(xa).b = x.(ab) \in xA.$$

Il en résulte que xA est un idéal de A qui contient x donc $I_x \subset xA$.

$xA \subset I_x$:

Soit $xa \in xA$ où $a \in A$. Comme I est un idéal et que x appartient à I_x , par stabilité de I_x par multiplication par les éléments de A , on a $xa \in I_x$. D'où $xA \subset I_x$.

Conclusion : on a $I_x = xA = \{xa \mid a \in A\}$. $\square$

Définition 9.

Soit A un anneau commutatif.

- On dit qu'un idéal de A est **principal** s'il est engendré par un singleton.
- On dit que l'anneau A est **principal** si A est intègre et si tous ses idéaux sont principaux.

Exemple 7.

- Pour $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n dans $\mathbb{Z}$ est l'idéal principal engendré par $\{n\}$.
- Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

- On a $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ est bien l'idéal engendré par $\{n\}$
- Nous démontrerons ces résultats dans la suite (Corollaires 2 et 8).

c. Somme d'idéaux**Notation 2.**

Soit A un anneau commutatif.

Pour $n \in \mathbb{N}^*$ et $I_1, \dots, I_n \subset A$, on appelle **somme de** $I_1, \dots, I_n$ et on note $I_1 + \dots + I_n$, ou encore

$\sum_{k=1}^n I_k$, l'ensemble :

$$I_1 + \dots + I_n = \{x_1 + \dots + x_n \mid \forall k \in \llbracket 1, n \rrbracket, x_k \in I_k\}.$$

Remarque 7.

Par commutativité et associativité de l'opération $+$ dans A , l'ordre des termes dans la somme $I_1 + \dots + I_n$ n'est pas importante et on a $I_1 + \dots + I_n = (I_1 + \dots + I_{n-1}) + I_n$.

Proposition 17.

Une somme finie d'idéaux d'un anneau commutatif est un idéal de cet anneau.

Démonstration.

Soit A un anneau commutatif, $n \in \mathbb{N}^*$ et $I_1, \dots, I_n$ des idéaux de A . On note $I = I_1 + \dots + I_n$.

- D'après la proposition 4, $I_1 + \dots + I_n$ est un sous-groupe de $(A, +)$.
- Soit $x = x_1 + \dots + x_n \in I$ avec, pour tout $k \in \llbracket 1, n \rrbracket$, $x_k \in I_k$ et $a \in A$. On a, par distributivité de $\times$ par rapport à $+$:

$$xa = (x_1 + \dots + x_n)a = x_1a + \dots + x_na.$$

Or, pour tout $k \in \llbracket 1, n \rrbracket$, I_k est un idéal de A donc $x_k a \in I_k$, d'où :

$$xa = x_1 a + \dots + x_n a \in I_1 + \dots + I_n = I.$$

Il en résulte que I est un idéal de A . □

Proposition 18.

Soit A un anneau commutatif, $n \in \mathbb{N}^*$ et $I_1, \dots, I_n$ des idéaux de A .

L'ensemble la somme $I_1 + \dots + I_n$ est l'idéal engendré par $\bigcup_{k=1}^n I_k$.

Démonstration.

On note J l'idéal engendré par $\bigcup_{k=1}^n I_k$ et $I = I_1 + \dots + I_n$.

Pour tout $j \in \llbracket 1, n \rrbracket$, on a $0_A \in I_j$ car I_j est un idéal de A donc, pour tout $k \in \llbracket 1, n \rrbracket$ et tout $x_k \in I_k$, on a :

$$x_k = 0_A + \dots + 0_A + x_k + 0_1 + \dots + 0_A \in I_1 + \dots + I_n.$$

D'où $\bigcup_{k=1}^n I_k \subset I_1 + \dots + I_n$.

Par suite, I étant un idéal et J étant le plus petit idéal contenant $\bigcup_{k=1}^n I_k$, on a $J \subset I$.

De plus, J étant un sous-groupe de $(A, +)$, pour tout $x = x_1 + \dots + x_n \in I$ avec, pour tout $k \in \llbracket 1, n \rrbracket$, $x_k \in I_k$, on a $x = x_1 + \dots + x_n \in J$. D'où $I \subset J$.

Il en résulte que $I = J$. □

Dans l'exercice suivant, on propose une preuve plus "directe" qu'une somme finie d'idéal est un idéal.

Exercice 16.

Soit A un anneau commutatif.

1. Montrer, de manière directe, que si I, J sont des idéaux de A , alors $I + J$ est un idéal de A .
2. En déduire, en utilisant un raisonnement par récurrence, que toute somme finie d'idéaux de A est un idéal de A .

Correction.

1. Montrons que $I + J$ est un sous-groupe de $(A, +)$. On a

$$0_A = \underbrace{0_A}_{\in I} + \underbrace{0_A}_{\in J} \in I + J$$

car I, J sont des sous-groupes de $(A, +)$; et pour tous $x = x_I + x_J, y = y_I + y_J \in I + J$,

$$x - y = x_I + x_J - (y_I + y_J) = \underbrace{(x_I - y_I)}_{\in I} + \underbrace{(x_J - y_J)}_{\in J} \in I + J,$$

car I, J sont des sous-groupes de $(A, +)$;

Donc $I + J$ est un sous-groupe de $(A, +)$

Soit $x = x_I + x_J \in I + J$ et $a \in A$. Par distributivité, on a :

$$xa = (x_I + x_J)a = \underbrace{(x_I a)}_{\in I} + \underbrace{(x_J a)}_{\in J} \in I + J,$$

car I, J sont stables par multiplication par les éléments de A .

Il en résulte que $I + J$ est un idéal de A .

2. Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_n =$ "Pour tous $I_1, \dots, I_n$ idéaux de A , $I = I_1 + \dots + I_n$ est un idéal de A ". Montrons, par récurrence sur $\mathbb{N}^*$, que, pour tout $n \in \mathbb{N}^*$, la propriété $\mathcal{P}_n$ est vraie.

— **Initialisation.** Soit I_1 un idéal de A . Alors $\sum_{k=1}^1 I_k = I_1$ est un idéal de A .

Par suite, $\mathcal{P}_1$ est vraie.

— **Hérédité.** Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}_n$ vraie.

Soit $I_1, \dots, I_{n+1}$ des idéaux de A . Alors, par hypothèse de récurrence, $J = I_1 + \dots + I_n$ est un idéal de A .

Par suite, on a :

$$I = I_1 + \dots + I_{n+1} = (I_1 + \dots + I_n) + I_{n+1} = J + I_{n+1},$$

d'où I est un idéal de A comme somme de deux idéaux de A (question 1).

Par suite, $\mathcal{P}_{n+1}$ est vraie.

Ce qui achève le raisonnement par récurrence. Il en résulte que, pour tout $n \in \mathbb{N}^*$, $\mathcal{P}_n$ est vraie.

3. Divisibilité, PGCD et PPCM

a. Divisibilité dans un anneau commutatif intègre

Définition 10. *Diviseur et multiple*

Soit A un anneau commutatif intègre et $x, y \in A$.

— On dit que x **divise** y et on note $x|y$ s'il existe $a \in A$ tel que $y = xa$.

Dans ce cas, on dira également que x est un **diviseur de** y ou encore que y est un **multiple de** x .

— On dit que x et y sont **associés** dans A si $x|y$ et $y|x$.

Proposition 19. Caractérisation de la divisibilité en terme d'idéaux

Soit A un anneau commutatif intègre et $x, y \in A$. On a $x|y$ si, et seulement si, $yA \subset xA$.

Démonstration.

- $(\Rightarrow)$. On suppose $x|y$. Alors il existe $a \in A$ tel que $y = xa$. Soit $ya' \in yA$. Alors

$$ya' = (xa)a' = x(aa') \in xA,$$

car A est stable par $\cdot$. Donc $yA \subset xA$.

- $(\Leftarrow)$. On suppose $yA \subset xA$. Alors en particulier, $y = y \cdot 1_A \in yA \subset xA$ donc il existe $a \in A$ tel que $y = xa$. D'où $x|y$. □

Corollaire 1.

Soit A un anneau commutatif intègre et $x, y \in A$. Les éléments x et y sont associés dans A si, et seulement si, ils engendrent le même idéal i.e. $xA = yA$.

Démonstration.

On a $xA = yA$ si, et seulement si, $xA \subset yA$ et $yA \subset xA$ si, et seulement si, d'après la proposition précédente, $y|x$ et $x|y$. □

Proposition 20.

Soit A un anneau commutatif intègre et $x, y \in A$. Les éléments x et y sont associés dans A si, et seulement si, il existe $u \in A^\times$ tel que $y = xu$.

L'ensemble des éléments associés à x dans A est l'ensemble $xA^\times = \{xu \mid u \in A^\times\}$.

Démonstration.

- $(\Rightarrow)$. On suppose $x|y$ et $y|x$. Alors il existe $u, v \in \mathbb{Z}$ tels que $y = xu$ et $x = yv$. Ainsi, on a par exemple, $x = x(uv)$ d'où $x(1_A - uv) = 0_A$. Or A est un anneau intègre, donc :

$$x = 0_A \text{ ou } 1_A - uv = 0_A.$$

1er cas : $x = 0_A$. Alors $y = 0_A$ et par exemple, $y = x \cdot 1_A$ avec $1_A \in A^\times$.

2eme cas : $1_A - uv = 0_A$. Alors $uv = 1_A$ donc u est inversible dans A d'inverse v .

Dans tous les cas il existe $u \in A^\times$ tel que $y = xu$.

- $(\Leftarrow)$. On suppose qu'il existe $u \in A^\times$ tel que $y = xu$. Alors $y = xu$ et $x = yu^{-1}$ donc $x|y$ et $y|x$. □

b. Notion de PGCD dans un anneau principal

Comme, dans un anneau principal, tous les idéaux sont principaux, la définition suivante a bien un sens en vertu des propositions 17 et 16.

Définition 11.

Soit A un anneau commutatif **principal**, $n \in \mathbb{N}^*$ et $d, m, a_1, \dots, a_n \in A$.

- On dit que d est un **PGCD** de $a_1, \dots, a_n$ si d est un générateur de l'idéal $a_1A + \dots + a_nA$ i.e. si

$$a_1A + \dots + a_nA = dA.$$

- On dit que d est un **PPCM** de $a_1, \dots, a_n$ si m est un générateur de l'idéal $a_1A \cap \dots \cap a_nA$ i.e. si

$$a_1A \cap \dots \cap a_nA = mA.$$

Proposition 21.

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $x, y, a_1, \dots, a_n \in A$. Si x, y sont des PGCD (respectivement, des PPCM) de $a_1, \dots, a_n$, alors ils sont associés.

Démonstration.

Si x, y sont des PGCD de $a_1, \dots, a_n$, alors $xA = a_1A + \dots + a_nA = yA$, donc, d'après le corollaire 1, x et y sont associés. $\square$

Remarque 8.

Lorsque, dans un anneau principal donné, on dispose d'un moyen canonique de distinguer un élément parmi ses associés, on pourra parler **du** PGCD et **du** PPCM! C'est ce qu'on fera dans la suite pour les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$.

Proposition 22.

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $d, m, a_1, \dots, a_n \in A$.

- Un PGCD de $a_1, \dots, a_n$ est un diviseur commun de $a_1, \dots, a_n$.
- Un PPCM de $a_1, \dots, a_n$ est un multiple commun de $a_1, \dots, a_n$.

Démonstration.

- Soit d un PGCD de $a_1, \dots, a_n$ i.e. $dA = a_1A + \dots + a_nA$. Alors, pour tout $i \in \llbracket 1, n \rrbracket$, on a

$$a_iA \subset a_1A + \dots + a_nA = dA,$$

donc, d'après la caractérisation de la divisibilité en terme d'idéaux (Proposition 19), $d|a_i$.

Par suite, d est un diviseur commun de $a_1, \dots, a_n$.

- Soit m un PPCM de $a_1, \dots, a_n$ i.e. $mA = a_1A \cap \dots \cap a_nA$. Alors, pour tout $i \in \llbracket 1, n \rrbracket$, on a

$$mA = a_1A \cap \dots \cap a_nA \subset a_iA,$$

donc, d'après la caractérisation de la divisibilité en terme d'idéaux (Proposition 19), $a_i | m$.

Par suite, m est un multiple commun de $a_1, \dots, a_n$.

□

Proposition 23.

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $d, m, a_1, \dots, a_n \in A$.

- L'élément d est un PGCD de $a_1, \dots, a_n$ si, et seulement si, d est un diviseur commun de $a_1, \dots, a_n$ et, pour tout diviseur commun δ de $a_1, \dots, a_n$, δ divise d .
- L'élément m est un PPCM de $a_1, \dots, a_n$ si, et seulement si, m est un multiple commun de $a_1, \dots, a_n$ et, pour tout multiple commun μ de $a_1, \dots, a_n$, m divise μ .

Démonstration.

- $(\Rightarrow)$. On suppose que d est un PGCD de $a_1, \dots, a_n$. Soit δ un diviseur commun de $a_1, \dots, a_n$.
Alors, d'après la caractérisation de la divisibilité en terme d'idéaux (Proposition 19), pour tout $i \in \llbracket 1, n \rrbracket$, $a_iA \subset \delta A$.
Par suite, l'idéal δA contient l'ensemble $\bigcup_{i=1}^n a_iA$, et donc, $dA = a_1A + \dots + a_nA$ étant le plus petit idéal contenant cet ensemble (Proposition 18), on obtient $dA \subset \delta A$ et donc, d divise δ .
De plus, d'après la proposition 22, d est un diviseur commun de $a_1, \dots, a_n$.
- $(\Leftarrow)$. On suppose que d est un diviseur commun de $a_1, \dots, a_n$ et que tout diviseur commun de $a_1, \dots, a_n$ divise d .
Soit δ un PGCD de $a_1, \dots, a_n$. Alors, d'après la proposition 22, δ est un diviseur commun de $a_1, \dots, a_n$. Ainsi, par hypothèse, δ divise d . Et de plus, comme d est un diviseur commun de $a_1, \dots, a_n$, d'après l'implication directe, on a d divise δ .
Il en résulte, d'après la caractérisation de la divisibilité en terme d'idéaux, que $dA = \delta A = a_1A + \dots + a_nA$, d'où d est un PGCD de $a_1, \dots, a_n$.
- • $(\Rightarrow)$. On suppose que m est un PPCM de $a_1, \dots, a_n$. Soit μ un multiple commun de $a_1, \dots, a_n$.
Alors, d'après la caractérisation de la divisibilité en terme d'idéaux (Proposition 19), pour tout $i \in \llbracket 1, n \rrbracket$, $\mu A \subset a_iA$.
Par suite, on a $\mu A = a_1A \cap \dots \cap a_nA = mA$ et donc, m divise μ .
De plus, d'après la proposition 22, m est un multiple commun de $a_1, \dots, a_n$.
- $(\Leftarrow)$. On suppose que m est un multiple commun de $a_1, \dots, a_n$ et que m divise tout multiple commun de $a_1, \dots, a_n$.
Soit μ un PPCM de $a_1, \dots, a_n$. Alors, d'après la proposition 22, μ est un multiple commun de $a_1, \dots, a_n$. Ainsi, par hypothèse, m divise μ . Et de plus, comme m est un multiple commun de $a_1, \dots, a_n$, d'après l'implication directe, on a μ divise m .
Il en résulte, d'après la caractérisation de la divisibilité en terme d'idéaux, que $mA = \mu A$.

$\mu A = a_1 A \cap \dots \cap a_n A$, d'où m est un PPCM de $a_1, \dots, a_n$.

□

c. Relation et théorème de Bézout

Proposition 24. *Relation de Bézout*

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $d, a_1, \dots, a_n \in A$.
Si d est un PGCD de $a_1, \dots, a_n$, alors il existe $x_1, \dots, x_n \in A$ tels que :

$$a_1 x_1 + \dots + a_n x_n = d.$$

Démonstration.

Si d est un PGCD de $a_1, \dots, a_n$, on a :

$$d = d 1_A \in dA = a_1 A + \dots + a_n A,$$

donc il existe $x_1, \dots, x_n \in A$ tels que $d = a_1 x_1 + \dots + a_n x_n$.

□

Définition 12.

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in A$.

- On dit que $a_1, \dots, a_n$ sont **premiers entre eux dans leur ensemble** si 1_A est un PGCD de $a_1, \dots, a_n$.
- Si $n \geq 2$, on dit que $a_1, \dots, a_n$ sont **premiers entre eux deux à deux** si, pour tous $i, j \in \llbracket 1, n \rrbracket$ avec $i \neq j$, 1_A est un PGCD de a_i et a_j .

Exemple 8.

Les nombres entiers 8, 15 et 77 sont premiers entre eux dans leur ensemble.

Proposition 25.

Soit A un anneau commutatif principal, $n \in \mathbb{N}$ avec $n \geq 2$ et $a_1, \dots, a_n \in A$. Si $a_1, \dots, a_n$ sont premiers entre eux deux à deux alors ils sont premiers entre eux dans leur ensemble.

Remarque 9.

La réciproque de la proposition précédente est fausse.

Exercice 17.

Dans $\mathbb{Z}$, trouver trois nombres qui sont premiers dans leur ensemble mais pas premiers entre eux deux à deux.

Théorème 7. Théorème de Bézout

Soit A un anneau commutatif principal, $n \in \mathbb{N}^*$ et $d, a_1, \dots, a_n \in A$.

Les éléments $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe $x_1, \dots, x_n \in A$ tels que :

$$a_1x_1 + \dots + a_nx_n = 1_A.$$

Démonstration.

L'implication directe provient de la relation de Bézout (Proposition 24).

Réciproquement, supposons qu'il existe $x_1, \dots, x_n \in A$ tels que $a_1x_1 + \dots + a_nx_n = 1_A$.

Alors 1_A appartient à l'idéal $a_1A + \dots + a_nA$ d'où $A = 1_AA$ étant le plus petit idéal contenant 1_A , on a :

$$A \subset a_1A + \dots + a_nA \subset A,$$

d'où $1_AA = A = a_1A + \dots + a_nA$.

Par suite, 1_A est un PGCD de $a_1, \dots, a_n$. □

Partie C

Anneaux $\mathbb{Z}/n\mathbb{Z}$ et arithmétique des entiers

1. Idéaux de $\mathbb{Z}$ et PGCD

a. Caractérisation des idéaux de $\mathbb{Z}$

Théorème 8. *Idéaux de $\mathbb{Z}$*

Soit I un idéal de $\mathbb{Z}$. Il existe un unique $n \in \mathbb{N}$ tel que $I = n\mathbb{Z}$.

Démonstration.

Soit I un idéal de l'anneau $\mathbb{Z}$. Alors c'est un sous-groupe de $(\mathbb{Z}, +)$. Par suite, il est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ et ce n est unique d'après le théorème 2. $\square$

Corollaire 2.

$\mathbb{Z}$ est un anneau principal.

Démonstration.

En effet, $\mathbb{Z}$ est un anneau commutatif intègre et d'après le théorème précédent, tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z} = \mathbb{Z}n$ où $n \in \mathbb{N}$; or $n\mathbb{Z}$ est un idéal principal car engendré par le singleton $\{n\}$. $\square$

b. PGCD, PPCM et théorème de Bézout généralisé

Dans l'anneau $\mathbb{Z}$, une classe d'éléments associés contient un nombre et son opposé. On a donc un choix "canonique" pour distinguer un élément dans cette classe : prendre celui qui est positif ! Ceci nous permet de définir le PGCD et le PPCM de plusieurs nombres entiers

Définition 13.

Soit $n \in \mathbb{N}^*$ et $a_1, \dots, a_n \in \mathbb{Z}$ non tous nuls.

- On appelle **PGCD** de $a_1, \dots, a_n$ et on note $\text{pgcd}(a_1, \dots, a_n)$, ou encore $a_1 \wedge \dots \wedge a_n$, l'unique générateur positif de l'idéal $a_1\mathbb{Z} + \dots + a_n\mathbb{Z}$.
- On appelle **PPCM** de $a_1, \dots, a_n$ et on note $\text{ppcm}(a_1, \dots, a_n)$, ou encore $a_1 \vee \dots \vee a_n$, l'unique générateur positif de l'idéal $a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z}$.

Remarque 10.

En vertu de la remarque 7 et de la commutativité et associativité de l'intersection, les opérations $\wedge$ et $\vee$ sont commutatives et associatives.

Théorème 9. Relation et théorème de Bézout généralisée

Soit $n \in \mathbb{N}^*$ et $d, a_1, \dots, a_n \in \mathbb{Z}$.

- *Relation de Bézout généralisée.* Si $d = \text{pgcd}(a_1, \dots, a_n)$, alors il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que :

$$a_1 u_1 + \dots + a_n u_n = d.$$

- *Théorème de Bézout généralisé.* Les entiers $a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que :

$$a_1 u_1 + \dots + a_n u_n = 1.$$

Démonstration.

Comme $\mathbb{Z}$ est un anneau principal, on peut appliquer directement la relation de Bézout (Proposition 24) et le théorème de Bézout (Théorème 7) vu pour les anneaux principaux. $\square$

2. Anneaux $\mathbb{Z}/n\mathbb{Z}$

Dans ce paragraphe, n désigne un entier naturel non nul.

a. Structure d'anneau

Théorème 10. Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$

Il existe sur $\mathbb{Z}/n\mathbb{Z}$ des lois de composition internes notée $+$ et $\cdot$ appelées respectivement **loi additive quotient** et **loi multiplicative quotient** telles que, pour tous $x, y \in \mathbb{Z}$,

$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{et} \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

Muni de ces lois, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif où l'élément nul est $\overline{0}$ et l'unité est $\overline{1}$.

Démonstration.

On a montré que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif. Il s'agit ici de montrer que la multiplication $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ est bien définie et qu'elle vérifie les axiomes requis pour la structure d'anneau. $\square$

Proposition 26.

L'application :

$$\pi_n : \begin{array}{ccc} \mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \bar{k} \end{array}$$

est un morphisme surjectif d'anneaux de noyau $\text{Ker}(\pi_n) = n\mathbb{Z}$.

Démonstration.

On a déjà montré que π_n est un morphisme surjectif de groupes de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ de noyau $\text{Ker}(\pi_n) = n\mathbb{Z}$.

Il reste à montrer que $\pi_n(pq) = \pi_n(p)\pi_n(q)$ pour tous $p, q \in \mathbb{Z}$.

Soit $p, q \in \mathbb{Z}$, on a :

$$\pi_n(pq) = \overline{pq} = \overline{p} \overline{q} = \pi_n(p)\pi_n(q).$$

□

b. Inversibilité dans les anneaux $\mathbb{Z}/n\mathbb{Z}$

Proposition 27. *Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$*

Soit $k \in \mathbb{Z}$. La classe $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement, si k est premier avec n .

Démonstration.

$\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

si, et seulement si,

il existe $\bar{u} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{k}\bar{u} = \bar{1}$

si, et seulement si,

il existe $u \in \mathbb{Z}$ tel que $ku \equiv 1 \pmod{n}$

si, et seulement si,

il existe $u, v \in \mathbb{Z}$ tels que $ku + nv = 1$

si, et seulement si,

k et n sont premiers entre eux.

□

Corollaire 3.

Soit $n \in \mathbb{N}^*$. On a équivalence entre :

- i) n est premier ;
- ii) $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre ;
- iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Démonstration.

Démontrons $i) \Rightarrow iii) \Rightarrow ii) \Rightarrow i)$

- $i) \Rightarrow iii)$ Si n est premier, alors pour tout $k \in \llbracket 1, n-1 \rrbracket$, k est premier avec n donc $\bar{k}$ est inversible. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps.
- $ii) \Rightarrow iii)$ Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, alors tous ses éléments non nuls sont inversibles et donc sont réguliers. Ainsi, $\mathbb{Z}/n\mathbb{Z}$ est intègre.
- $iii) \Rightarrow i)$ Raisonnons par contraposée. On suppose que n n'est pas premier. Si $n = 1$, l'anneau est trivial et donc n'est pas intègre. Supposons $n \geq 2$. Alors $n = pq$ avec $p, q \in \llbracket 2, n-1 \rrbracket$. On a alors $\bar{p} \neq \bar{0}$ et $\bar{q} \neq \bar{0}$ et

$$\overline{pq} = \bar{0},$$

par suite $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. □

Notation 3.

Soit p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Exercice 18.

1. Déterminer les éléments inversibles de $\mathbb{Z}/10\mathbb{Z}$ et calculer l'inverse de $\bar{9}$ et $\bar{7}$.
2. Déterminer l'inverse de $\overline{41}$ dans $\mathbb{Z}/152\mathbb{Z}$.

Correction.

1. On a $9 \times 9 = 81 = 1 + 8 \times 10$ donc $\bar{9}.\bar{9} = \bar{1}$. Donc $\bar{9}$ est sa propre inverse dans $\mathbb{Z}/10\mathbb{Z}$.
On a $7 \times 3 = 21 = 1 + 2 \times 10$ donc $\bar{7}.\bar{3} = \bar{1}$. Donc $\bar{3}$ est l'inverse de $\bar{7}$ dans $\mathbb{Z}/10\mathbb{Z}$.
2. En appliquant l'algorithme d'Euclide pour le calcul du pgcd on obtient 1 et donc $\overline{41}$ est inversible dans $\mathbb{Z}/152\mathbb{Z}$. Ainsi, en remontant l'algorithme d'Euclide, on trouve les coefficients de Bézout suivants :

$$(-63) \times 41 + 17 \times 152 = 1,$$

et donc $\overline{-63}.\overline{41} = \bar{1}$. Par suite $\overline{-63} = \overline{89}$ est l'inverse de $\overline{41}$ dans $\mathbb{Z}/152\mathbb{Z}$.

3. Applications à l'arithmétique des entiers

a. Théorème Chinois

Théorème 11. *Théorème Chinois*

Soit $n, m \in \mathbb{N}$ deux entiers premiers entre eux. Les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes et l'application :

$$\varphi \left| \begin{array}{ccc} \mathbb{Z}/(nm)\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \bar{k}^{nm} & \mapsto & (\bar{k}^n, \bar{k}^m) \end{array} \right.$$

est un isomorphisme d'anneaux.

Démonstration.

Montrons que φ est bien définie : si $p \equiv q \pmod{nm}$, alors $p - q \in nm\mathbb{Z}$. Or $nm\mathbb{Z} \subset n\mathbb{Z}$ et $nm\mathbb{Z} \subset m\mathbb{Z}$, donc $p \equiv q \pmod{n}$ et $p \equiv q \pmod{m}$. Ainsi $\varphi(\bar{p}^{nm}) = \varphi(\bar{q}^{nm})$ donc φ est bien définie.

φ est un morphisme d'anneaux car $\bar{k}^{nm} \mapsto \bar{k}^n$ et $\bar{k}^{nm} \mapsto \bar{k}^m$ sont des morphismes d'anneaux. On a :

$$\text{Ker}(\varphi) = \{\bar{k}^{nm} \mid \bar{k}^n = \bar{0}^n, \bar{k}^m = \bar{0}^m\},$$

Or si $\bar{k}^n = \bar{0}^n$ et $\bar{k}^m = \bar{0}^m$, alors k est un multiple commun de n et m qui sont premiers entre eux, donc, d'après le corollaire du lemme de Gauss, k est un multiple de nm i.e. $\bar{k}^{nm} = \bar{0}^{nm}$. D'où $\text{Ker}(\varphi) = \{\bar{0}^{nm}\}$. Par suite φ est injective.

De plus, φ est bijective car φ est injective et $\mathbb{Z}/(nm)\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ ont tout deux même cardinal (nm) . $\square$

Corollaire 4.

Soit $n, m \in \mathbb{N}$ deux entiers premiers entre eux. Les groupes $(\mathbb{Z}/(nm)\mathbb{Z})^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ sont isomorphes.

Démonstration.

D'après le théorème Chinois, les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes donc, en vertu de la proposition 3, leurs groupes d'inversibles $(\mathbb{Z}/(nm)\mathbb{Z})^\times$ et $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times$ le sont en tant que groupes. Or, d'après la proposition 14, $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, d'où le résultat. $\square$

Corollaire 5. *Application du théorème Chinois*

Soit $n, m \in \mathbb{N}$ deux entiers premiers entre eux. Pour tout $a, b \in \mathbb{Z}$, il existe un entier k vérifiant le système :

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

et les solutions de ce système sont exactement les entiers congrus à k modulo nm .

Méthode de résolution :

n et m étant premiers entre eux, on cherche deux entiers $u, v \in \mathbb{Z}$ tels que $nu + mv = 1$. Ainsi, les entiers $x_1 = nu$ et $x_2 = mv$ vérifient

$$\begin{cases} x_1 \equiv 0 \pmod{n} \\ x_1 \equiv 1 \pmod{m} \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 1 \pmod{n} \\ x_2 \equiv 0 \pmod{m} \end{cases}$$

Ainsi, $x = bx_1 + ax_2$ est solution du système initial (*Toujours vérifier que ce x est bien solution pour éviter les erreurs dans les calculs précédents !*) ; par suite l'ensemble des solutions est :

$$x + nm\mathbb{Z} = \{x + nmk \mid k \in \mathbb{Z}\}.$$

Exercice 19.

Résoudre les systèmes suivants :

$$(S_1) \begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 4 \pmod{7} \end{cases} \quad \text{et} \quad (S_2) \begin{cases} 3x \equiv 2 \pmod{5} \\ 5x \equiv 1 \pmod{6} \end{cases}$$

Correction.

(S_1) On a $6 \times (-1) + 7 \times 1 = 1$ donc $x_1 = 7 \times 1$ et $x_2 = 6 \times (-1)$ vérifient :

$$\begin{cases} x_1 \equiv 1 \pmod{6} \\ x_1 \equiv 0 \pmod{7} \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0 \pmod{6} \\ x_2 \equiv 1 \pmod{7} \end{cases}$$

donc $x = 1 \times x_1 + 4 \times x_2 = -17$ est une solution de (S_1). Ainsi l'ensemble des solutions de (S_1) est

$$\{-17 + 42k \mid k \in \mathbb{Z}\}.$$

(S_2) On a 3 et 5 premiers entre eux, donc $\bar{3}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$ et son inverse est $\bar{2}$ car $3 \times 2 = 6 = 1 + 5$.

Ainsi, on a $3x \equiv 2 \pmod{5} \Leftrightarrow x \equiv 4 \pmod{5}$.

On a 5 et 6 premiers entre eux, donc $\bar{5}$ est inversible dans $\mathbb{Z}/6\mathbb{Z}$ et son inverse est $\bar{5}$ car $5 \times 5 = 25 = 1 + 4 \times 6$.

Ainsi, on a $5x \equiv 1 \pmod{6} \Leftrightarrow x \equiv 5 \pmod{6}$.

d'où :

$$(S_2) \Leftrightarrow \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \end{cases}$$

Et on résout comme précédemment.

Exercice 20.

Résoudre l'équation $x^2 + x + 11 \equiv 0 \pmod{143}$.

Correction.

On a $143 = 11 \times 13$ et 11 est premier avec 13 donc d'après le théorème chinois, $(*) x^2 + x + 11 \equiv 0 \pmod{143}$ si, et seulement si,

$$(1) x^2 + x + 11 \equiv 0 \pmod{11} \quad \text{et} \quad (2) x^2 + x + 11 \equiv 0 \pmod{13}$$

Donc si x_1 est une solution de (1) et x_2 une solution de (2), alors $x = x_1u + x_2v$ est solution de $(*)$ où $u, v \in \mathbb{Z}$ sont tels que $11u + 13v = 1$, et toutes les solutions sont de cette forme.

On a

$$(x+1)x = x^2 + x \equiv x^2 + x + 11 \equiv 0 \pmod{11}$$

et

$$(x-1)(x+2) = x^2 + x - 2 \equiv x^2 + x + 11 \equiv 0 \pmod{13}$$

Donc les solutions de (1) sont $x \equiv 0 \pmod{11}$ et $x \equiv -1 \pmod{11}$ et les solutions de (2) sont $x \equiv 1 \pmod{13}$ et $x \equiv -2 \pmod{13}$.

Déterminons les coefficients u et v : on a $6 \times 11 - 5 \times 13 = 1$, d'où $u = 6$ et $v = 5$.

Ainsi, on a donc les solutions suivantes :

$$x \equiv 66 \pmod{143}$$

$$x \equiv 11 \pmod{143}$$

$$x \equiv -12 \pmod{143}$$

$$x \equiv 76 \pmod{143}$$

Méthode : Que faire dans le cas d'un système : $\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases}$ où p et q ne sont pas premiers entre eux ?

Soit $d = \text{pgcd}(p, q)$ et $M = \text{ppcm}(p, q)$. Alors on peut montrer qu'il existe une solution à ce système, si et seulement si $a \equiv b \pmod{d}$.

Dans ce cas, une solution est donnée par $x = a + qu\frac{b-a}{d}$ où u est un entier qui vérifie $pu + qv = d$ (où $v \in \mathbb{Z}$) et de plus, l'ensemble des solutions forme une classe modulo $M\mathbb{Z}$.

Exercice 21.

Résoudre les systèmes suivants :

$$(S_1) \begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 4 \pmod{15} \end{cases} \quad \text{et} \quad (S_2) \begin{cases} 3x \equiv 6 \pmod{18} \\ x \equiv 1 \pmod{21} \end{cases}$$

b. Indicatrice d'Euler

Définition 14. Fonction indicatrice d'Euler

On appelle **fonction indicatrice d'Euler** l'application $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$ définie, pour $n \in \mathbb{N}^*$, par :

$$\varphi(n) = \#\{k \in \llbracket 1, n \rrbracket \mid k \text{ et } n \text{ sont premiers entre eux}\}.$$

Proposition 28. Propriétés de l'indicatrice d'Euler

i) $\varphi(1) = 1,$

ii) pour $n \geq 2$, $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times,$

iii) pour p premier,

$$\varphi(p) = p - 1,$$

iv) pour p premier et $\alpha \in \mathbb{N}^*$,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

v) pour $n, m \in \mathbb{N}^*$ avec n et m premiers entre eux,

$$\varphi(nm) = \varphi(n)\varphi(m).$$

Démonstration.

i) 1 est premier avec lui-même d'où $\varphi(1) = 1,$

ii) pour $n \geq 2$, on a $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si, et seulement, si k premier avec n , d'où le résultat.

iii) pour p premier, alors chaque nombre compris entre 1 et $p - 1$ est premier avec p d'où le résultat.

iv) Soit p premier et $\alpha \in \mathbb{N}^*$. Pour $x \in \llbracket 1, p^\alpha \rrbracket$, x n'est pas premier avec p^α si, et seulement si $x \in p\mathbb{Z}$, i.e.

$$x \in \llbracket 1, p^\alpha \rrbracket \cap \{kp \mid k \in \mathbb{Z}\} = \{kp \mid k \in \llbracket 1, p^{\alpha-1} \rrbracket\}.$$

Ainsi, on a :

$$\varphi(p^\alpha) = \#\llbracket 1, p^\alpha \rrbracket - \#\llbracket 1, p^{\alpha-1} \rrbracket = p^\alpha - p^{\alpha-1}.$$

v) Soit $n, m \in \mathbb{N}^*$ avec n et m premiers entre eux. D'après le théorème chinois ou plus précisément d'après le corollaire 4, $(\mathbb{Z}/nm\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ et donc, en particulier, en bijection, d'où :

$$\varphi(nm) = \#(\mathbb{Z}/nm\mathbb{Z})^\times = \#(\mathbb{Z}/n\mathbb{Z})^\times \cdot \#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(n)\varphi(m).$$

□

Exercice 22.

Soit $n \in \mathbb{N}^*$. Montrer l'identité :

$$\sum_{d|n} \varphi(d) = n$$

Correction.

Considérons l'ensemble $F = \left\{ \frac{k}{n} \mid k \in \llbracket 1, n \rrbracket \right\}$. Alors $\#F = n$. De plus, chaque élément de F admet une forme irréductible $\frac{i}{d}$ où $d|n$ et i et d sont premiers entre eux. On a donc

$$F = \bigcup_{d|n} F_d \quad \text{où} \quad F_d = \left\{ \frac{i}{d} \mid \text{pgcd}(i, d) = 1 \text{ et } 1 \leq i \leq d \right\}.$$

De plus, les F_d sont disjoints par unicité du représentant irréductible d'un rationnel. Par suite, les F_d pour $d|n$ forment une partition de F et donc :

$$n = \#F = \sum_{d|n} \#F_d = \sum_{d|n} \varphi(d).$$

Corollaire 6.

Soit $n \in \mathbb{N}$ avec $n \geq 2$. On considère $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i}$ sa décomposition en facteurs premiers. On a :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

Démonstration.

On applique par récurrence le point v) de la proposition précédente car chaque $p_i^{\alpha_i}$ est premier avec chaque $p_j^{\alpha_j}$ ($i \neq j$) puis on applique le point iv) pour obtenir :

$$\varphi(n) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^k p_i^{\alpha_i} (1 - p_i^{-1}) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

□

c. Théorème d'Euler et petit théorème de Fermat

Théorème 12. *Théorème d'Euler*

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Pour tout $a \in \mathbb{Z}$ tel que a et n sont premiers entre eux, on a :

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Démonstration.

L'entier a est premier avec n donc $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Or $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe fini, donc $o(\bar{a}) | \#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. Ainsi,

$$\bar{a}^{\varphi(n)} = \bar{1}.$$

□

Corollaire 7. *Petit théorème de Fermat*

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$, on a :

$$a^{p-1} \equiv 1 \pmod{p}$$

Démonstration.

Si p est premier, $\varphi(p) = p - 1$ et tout entier qui n'est pas multiple de p est premier avec p . On applique alors le théorème d'Euler. $\square$

Partie D

Anneaux de polynômes

Dans toute cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ (ou même n'importe quel corps, mais dans les exemples pratiques, on se bornera aux sous-corps de $\mathbb{C}$, notamment $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{Q}$) et on considère l'anneau commutatif intègre (muni de ses opérations usuelles) $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$.

1. Propriétés arithmétiques élémentaires

Dans ce paragraphe, on rappelle et complète quelques propriétés de l'arithmétique des polynômes.

a. Division euclidienne

Théorème 13. *Division euclidienne dans $\mathbb{K}[X]$*

Soit $A, B \in \mathbb{K}[X]$ et $B \neq 0$. Il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

$$A = BQ + R \quad \text{et} \quad \deg(R) < \deg(B).$$

On appelle Q le **quotient** et R le **reste** de la division euclidienne de A par B .

Démonstration.

Vue en sup. On rappelle tout de même une idée de preuve de l'existence : on procède par récurrence forte sur le degré et pour l'hérédité, après avoir traité les cas triviaux, si $n \geq m$ sont les degrés de A, B respectivement et a_n, b_m leurs coefficients dominants, on écrit, $\mathbb{K}$ étant un corps, $A = A' + a_n b_m X^{n-m} B$ où $A' = A - \frac{a_n}{b_m} X^{n-m} B = BQ' + R$ par hypothèse de récurrence et ainsi $A = BQ + R$ avec $Q = (Q' + a_n b_m X^{n-m})$ et $\deg(R) < \deg(B)$. $\square$

b. Inversibles

Proposition 29.

Les éléments inversibles de l'anneau $\mathbb{K}[X]$ sont les polynômes constants non nuls qu'on identifie à $\mathbb{K}^*$ i.e. $\mathbb{K}[X]^\times = \mathbb{K}^*$.

c. Polynômes unitaires

Définition 15.

Soit $A \in \mathbb{K}[X]$. On dit que A est un polynôme **unitaire** s'il est non nul et que son coefficient dominant est égal à 1.

Proposition 30.

Soit $A \in \mathbb{K}[X] \setminus \{0\}$. Il existe un unique polynôme unitaire associé à A .
 En particulier, il existe un unique polynôme B unitaire tel que $B\mathbb{K}[X] = A\mathbb{K}[X]$.

Démonstration.

Si A est un polynôme non nul de $\mathbb{K}[X]$ et $\lambda \in \mathbb{K}^*$ est son coefficient dominant, alors $B = \frac{1}{\lambda}A$ est unitaire et associé à A . De plus, si C est un polynôme unitaire associé à A , alors il existe $\mu \in \mathbb{K}^*$ tel que $C = \mu A$.

Par suite, on a $C = \frac{\mu}{\lambda}B$ et ainsi, par identification des coefficients polynomiaux et en particulier des coefficients dominants, on a $1 = \frac{\mu}{\lambda}$ et donc $C = B$. D'où l'unicité.

La dernière assertion découle ainsi de la proposition 1. □

d. Racines**Définition 16.**

Soit $P \in \mathbb{K}[X]$ et $a \in \mathbb{K}$.

- On dit que a est une **racine** de P si $P(a) = 0$.
- Soit $m \in \mathbb{N}^*$. On dit que a est une racine **de multiplicité** m de P si $(X - a)^m$ divise P et $(X - a)^{m+1}$ ne divise pas P .

Proposition 31. *Caractérisation de la multiplicité d'une racine*

Soit $P \in \mathbb{K}[X]$, $a \in \mathbb{K}$ et $m \in \mathbb{N}^*$. Les assertions suivantes sont équivalentes :

- i) l'élément a est racine de multiplicité m de P ;
- ii) il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a)^m Q$ avec $Q(a) \neq 0$;
- iii) pour tout $k \in \llbracket 0, m - 1 \rrbracket$, $X - a$ divise $P^{(k)}$ et $X - a$ ne divise pas $P^{(m)}$.

Remarque 11.

- Il est usuel d'étendre la définition de la multiplicité à $m = 0$: a est une racine de multiplicité 0 de P si a n'est pas racine de P ;
- On emploiera souvent le vocabulaire suivant : **racine simple** pour racine de multiplicité 1 ; **racine double** pour racine de multiplicité 2 ; **racine triple**, etc...

Proposition 32.

Soit $n \in \mathbb{N}$. Un polynôme de $\mathbb{K}[X]$ de degré n admet au plus n racines comptées avec multiplicité.

Démonstration.

On rappelle ici les idées d'une démonstration de ce résultat. On procède par récurrence sur le degré et pour l'hérédité, on utilise le fait que si a est racine d'un polynôme P , celui-ci s'écrit, d'après la formule géométrique qui donne l'expression de $x^n - y^n$ dans un anneau commutatif, $P = (X - a)Q$ avec Q de degré strictement inférieur à celui de P . Ainsi, $\mathbb{K}$ étant en particulier un anneau intègre, les racines de P sont exactement a et les racines de Q : on applique alors l'hypothèse de récurrence. *Oui, si l'anneau des coefficients n'est pas intègre, cela ne tient plus, en effet : pour $a = 0$, $b, c \neq 0$ tels que $bc = 0$ dans $\mathbb{K}$ et $P = bX = (X - a)Q$ où $Q = b$, on vérifie que c est une racine de P alors que celle-ci n'est ni égal à a ni racine de Q .* $\square$

e. Polynômes irréductibles

Définition 17. Polynôme irréductible

Soit $A \in \mathbb{K}[X]$. On dit que A est un **polynôme irréductible** dans $\mathbb{K}[X]$ si $\deg(A) \geq 1$ et si, pour tout $B \in \mathbb{K}[X]$ tel que B divise A , il existe $\lambda \in \mathbb{K}[X]^\times = \mathbb{K}^*$ tel que

$$B = \lambda \text{ ou } B = \lambda A.$$

Remarque 12.

On remarque que les polynômes constants, par définition, ne sont pas irréductibles.

Proposition 33.

Soit $A \in \mathbb{K}[X]$. Le polynôme A n'est pas irréductible dans $\mathbb{K}[X]$ si, et seulement si, il existe $P, Q \in \mathbb{K}[X]$ tels que $A = PQ$ et $\deg(P) \geq 1$, $\deg(Q) \geq 1$.

Exemple 9.

- Les polynômes de degré 1 sont irréductibles dans $\mathbb{K}[X]$.
- $X^2 + 1$ et $X^2 + X + 5$ sont irréductibles dans $\mathbb{R}[X]$ mais $X^2 + 2X + 1$ ne l'est pas.
- $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 23.

1. Donner des exemples de polynômes irréductibles dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.
2. $P = X^3 + X + 1$ est-il irréductible dans $\mathbb{Q}[X]$?

Correction.

1. Dans $\mathbb{C}[X]$, $iX + 1$; dans $\mathbb{R}[X]$, $X^2 + 21$.
2. On suppose par l'absurde que P n'est pas irréductible. Alors il existe A, B non constants tels

que $P = AB$. Alors quitte à échanger A et B , on peut supposer $\deg(A) = 2$ et $\deg(B) = 1$. Par suite, B admet une racine $\frac{p}{q} \in \mathbb{Q}$ mise ici sous forme irréductible i.e. p et q sont premiers entre eux, qui est donc une racine de P également.

Par suite $0 = P(\frac{p}{q}) = \frac{p^3}{q^3} + \frac{p}{q} + 1$. Ainsi,

$$p^3 + pq^2 + q^3 = 0;$$

donc $q|p^3$ et $p|q^3$. Il en résulte que $p = \pm 1$ et $q = \pm 1$ car p et q sont premiers entre eux. Par suite, $\frac{p}{q} = \pm 1$. Or $P(1) = 3$ et $P(-1) = -1$, contradiction !

2. Idéaux de $\mathbb{K}[X]$

Théorème 14.

Soit I un idéal de $\mathbb{K}[X]$. Il existe un unique $P \in \mathbb{K}[X]$ tel que $I = P\mathbb{K}[X]$ avec P unitaire si $I \neq \{0\}$.

Démonstration.

Soit I un idéal de $\mathbb{K}[X]$. Montrons tout d'abord qu'il existe $P \in \mathbb{K}[X]$ tel que $I = P\mathbb{K}[X]$.

- 1er cas : $I = \{0\}$. Alors $I = 0\mathbb{K}[X]$.
- 2eme cas : $I \neq \{0\}$. Alors $\{\deg(P) \mid P \in I \setminus \{0\}\}$ est un ensemble non vide de $\mathbb{N}$ et donc possède un plus petit élément $p \in \mathbb{N}$. Par suite, il existe $P \in I$ un polynôme de degré p .

Montrons que $I = P\mathbb{K}[X]$.

- $P\mathbb{K}[X] \subset I$. Comme P appartient à I qui est un idéal et $P\mathbb{K}[X]$ est le plus petit idéal contenant P .
- $I \subset P\mathbb{K}[X]$. Soit $A \in I$. La division euclidienne de A par P nous donne l'existence de $Q, R \in \mathbb{K}[X]$ avec $\deg(R) < \deg(P)$ tels que $A = PQ + R$. Ainsi $R = A - PQ \in I$ car $A \in I$ et $PQ \in P\mathbb{K}[X] \subset I$. Par suite, comme $\deg(R) < \deg(P)$ et P est de degré minimal dans $I \setminus \{0\}$, on a $R = 0$. Donc $A = PQ \in P\mathbb{K}[X]$.

Il en résulte que $I = P\mathbb{K}[X]$.

Montrons l'unicité. Le polynôme nul est le seul générateur de l'idéal $\{0\} = 0\mathbb{K}[X]$ d'où l'unicité dans le cas $I = \{0\}$.

Si $I \neq \{0\}$, d'après ce qui précède, il existe un polynôme Q de degré $q \geq 0$ tel que $I = Q\mathbb{K}[X]$. En particulier, Q est non nul donc, d'après la proposition 30, il existe un unique P unitaire tel que $I = Q\mathbb{K}[X] = P\mathbb{K}[X]$. $\square$

Corollaire 8.

L'anneau $\mathbb{K}[X]$ est principal.

Correction.

L'anneau $\mathbb{K}[X]$ est intègre et d'après le théorème précédent, tous ses idéaux sont principaux, donc $\mathbb{K}[X]$ est un anneau principal.

3. Propriétés relatives au PGCD

a. PGCD et PPCM

Dans l'anneau $\mathbb{K}[X]$, une classe d'éléments non nuls associés contient toujours un polynôme unitaire (voire Proposition 30). On a donc un choix canonique pour distinguer un élément dans cette classe : prendre ce polynôme unitaire ! Ceci nous permet de définir le PGCD et le PPCM de plusieurs polynômes non tous nuls.

Définition 18.

Soit $n \in \mathbb{N}^*$ et $A_1, \dots, A_n \in \mathbb{K}[X]$.

- Si A et B sont non tous nuls, on appelle **PGCD** de $A_1, \dots, A_n$ et on note $A_1 \wedge \dots \wedge A_n$ ou encore $\text{PGCD}(A_1, \dots, A_n)$ l'unique générateur unitaire de l'idéal $A_1\mathbb{K}[X] + \dots + A_n\mathbb{K}[X]$;
- Si A et B sont non nuls, on appelle **PPCM** de $A_1, \dots, A_n$ et on note $A_1 \vee \dots \vee A_n$ ou encore $\text{PPCM}(A_1, \dots, A_n)$ l'unique générateur unitaire de l'idéal $A\mathbb{K}[X] \cap \dots \cap A_n\mathbb{K}[X]$.

b. Relation, théorème de Bézout et algorithme d'Euclide

Théorème 15. *Relation et théorème de Bézout généralisée*

Soit $n \in \mathbb{N}^*$ et $D, A_1, \dots, A_n \in \mathbb{K}[X]$.

- *Relation de Bézout généralisée.* Si $D = \text{PGCD}(A_1, \dots, A_n)$, alors il existe $U_1, \dots, U_n \in \mathbb{K}[X]$ tels que :

$$A_1U_1 + \dots + A_nU_n = D.$$

- *Théorème de Bézout généralisé.* Les polynômes $A_1, \dots, A_n$ sont premiers entre eux dans leur ensemble si, et seulement si, il existe $A_1, \dots, A_n \in \mathbb{K}[X]$ tels que :

$$A_1U_1 + \dots + A_nU_n = 1.$$

Démonstration.

Comme $\mathbb{K}[X]$ est un anneau principal, on peut appliquer directement la relation de Bézout (Proposition 24) et le théorème de Bézout (Théorème 7) vu pour les anneaux principaux. $\square$

Proposition 34.

Soit $A, B \in \mathbb{K}[X]$ des polynômes tous non nuls et R le reste de la division euclidienne de A par B . On a :

$$A \wedge B = B \wedge R.$$

Démonstration.

On note Q le quotient de la division et $D = A \wedge B$, $D' = B \wedge R$. Montrons que $D|D'$ et $D'|D$.

- $D|D'$: On a $R = A - BQ \in A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$ donc D divise R , et D divise B donc $D|B \wedge R = D'$.
- $D'|D$: On a $A = BQ + R \in B\mathbb{K}[X] + R\mathbb{K}[X] = D'\mathbb{K}[X]$ donc D' divise A , et D' divise B donc $D'|A \wedge B = D$.

Par suite, D et D' sont associés. Or D et D' sont unitaires, donc $D = D'$. $\square$

Théorème 16. Algorithme d'Euclide pour les polynômes

Soit $A, B \in \mathbb{K}[X]$ des polynômes tous non nuls avec $\deg(A) \geq \deg(B)$ et $D = A \wedge B$. La suite récurrente $(R_n)_{n \in \mathbb{N}}$ définie par :

$$\begin{cases} R_0 = A, R_1 = B; \\ R_{n+2} \text{ est le reste de la division euclidienne de } R_n \text{ par } R_{n+1} \end{cases}$$

est stationnaire en 0 et D est égal à l'unique polynôme unitaire associé à R_d où $d = \max\{n \in \mathbb{N} \mid R_n \neq 0\}$.

Démonstration.

Pour $n \in \mathbb{N}^*$, $\deg(R_n) < \deg(R_{n-1})$ et donc $\deg(R_n) \leq \deg(R_{n-1}) - 1$. Donc si $n = \deg(A) \in \mathbb{N}$ (en effet, comme A et B sont tous non nuls et $\deg(A) \geq \deg(B)$, $A \neq 0$), on a, de proche en proche :

$$\begin{aligned} \deg(R_{n+2}) &< \deg(R_{n+1}) \\ &\leq \deg(R_n) - 1 \\ &\leq \deg(R_{n-1}) - 2 \\ &\vdots \\ &\leq \deg(R_1) - n = \deg(B) - n \\ &\leq \deg(A) - n = 0 \end{aligned}$$

d'où $\deg(R_{n+2}) = -\infty$ i.e. $R_{n+2} = 0$.

De plus, d'après la proposition précédente, on a, pour $d = \max\{n \in \mathbb{N} \mid R_n \neq 0\}$ et U le polynôme unitaire associé à R_d , de proche en proche :

$$U = 0 \wedge R_d = R_{d+1} \wedge R_d = R_d \wedge R_{d-1} = R_{d-1} \wedge R_{d-2} = \dots = R_1 \wedge R_0 = A \wedge B = D.$$

$\square$

4. Décomposition d'un polynôme en facteurs irréductibles

a. Décomposition en facteurs irréductibles et polynômes scindés

Proposition 35.

On a les propriétés suivantes :

- Tout polynôme de degré supérieur ou égal à 1 possède un diviseur irréductible.
- Si A est irréductible et $A|P_1 \dots P_n$, alors il existe $i \in \llbracket 1, n \rrbracket$ tel que $A|P_i$.
- Tout polynôme de degré 1 est irréductible.
- Un polynôme de degré 2 ou 3 est irréductible si, et seulement si, il n'a pas de racine dans $\mathbb{K}$.

Démonstration.

- Soit P un polynôme de degré supérieur ou égal à 1. Alors l'ensemble des polynômes non constant qui divisent P est non vide car il contient P . Ainsi, il existe un polynôme A non constant de degré minimal qui divise P . Or si $A = UV$ avec $U, V \in \mathbb{K}[X]$, alors $\deg(U), \deg(V) \leq \deg(A)$ et $U|P, V|P$. Par suite, par minimalité du degré de A , soit $\deg(U) = \deg(A)$ ou $\deg(V) = \deg(A)$ d'où U ou V est constant. Ainsi, pour tout $U \in \mathbb{K}[X]$ tel que $U|A$, $U = \lambda$ ou $U = \lambda A$ avec $\lambda \in \mathbb{K}^*$. Par suite, A est irréductible.

Il en résulte que P possède un diviseur irréductible.

- On raisonne par récurrence sur $n \in \mathbb{N}^*$. Pour $n = 1$, si $A|P_1$ alors $A|P_1$! Soit $n \in \mathbb{N}^*$. On suppose la propriété vraie pour n . Soit $P_1, \dots, P_{n+1} \in \mathbb{K}[X]$ tels que $A|P_1 \dots P_{n+1}$. Alors $A|(P_1 \dots P_n)P_{n+1}$. On a alors deux cas :
 - $A|P_{n+1}$.
 - $A \nmid P_{n+1}$. Alors A et P_{n+1} sont premiers entre eux car A est irréductible, donc, d'après le Lemme de Gauss, $A|P_1 \dots P_n$. Par suite, par hypothèse de récurrence, il existe $i \in \llbracket 1, n \rrbracket$ tel que $A|P_i$.

Dans tous les cas, il existe $i \in \llbracket 1, n+1 \rrbracket$ tel que $A|P_i$. Donc la propriété est vraie pour $n+1$. Ce qui achève le raisonnement par récurrence.

- Si $aX + b = PQ$ alors $\deg(P) + \deg(Q) = 1$ donc $\deg(P) = 1$ ou 0 et inversement pour Q . Si $\deg(Q) = 0$, alors $Q = \lambda \in \mathbb{K}^*$ et $P = \frac{1}{\lambda}(aX + b)$ et inversement. Par suite, si $P|aX + b$, P est constant ou $P = \lambda(aX + b)$. Il en résulte que $aX + b$ est irréductible.
- Soit P un polynôme de degré 2 ou 3.
 - ($\Rightarrow$). Par contraposée. Si P admet une racine a dans $\mathbb{K}$, alors $X - a|P$ et $\deg(P) > 1 = \deg(X - a)$, donc P n'est pas irréductible.
 - ($\Leftarrow$). Par contraposée. Si $P = AB$ avec A et B non associée à P alors $\deg(A), \deg(B) < \deg(P) = 2$ ou 3. Ainsi, soit $\deg(A) = 1$, soit $\deg(B) = 1$. Et donc A ou B possède une racine et donc P en possède une.

□

Théorème 17. *Décomposition en facteurs irréductibles*

Soit $A \in \mathbb{K}[X]$ un polynôme non constant. Le polynôme A s'écrit de façon unique comme le produit

$$A = \lambda \prod_{i=1}^n P_i^{\alpha_i},$$

où $\lambda \in \mathbb{K}^*$, $n \in \mathbb{N}$, et pour $i, j \in \llbracket 1, n \rrbracket$, $i \neq j$, P_i est un polynôme unitaire irréductible, $\alpha_i \in \mathbb{N}^*$

et $P_i \neq P_j$.

Démonstration.

- **Existence de la décomposition :** On raisonne par récurrence sur le degré $n \in \mathbb{N}^*$ d'un polynôme.

— Initialisation. Pour $n = 1$, $A = aX + b = a(X + \frac{b}{a})$.

— Hérédité. Soit $n \in \mathbb{N}^*$. On suppose la propriété vraie pour $1 \leq k \leq n$. Soit A de degré $n + 1$ et P un diviseur irréductible unitaire de A . Alors il existe $B \in \mathbb{K}[X]$ tel que $A = PB$. Or comme P est irréductible, $\deg(P) \geq 1$, d'où $\deg(B) \leq n$. On applique alors l'hypothèse de récurrence à B :

$$B = \lambda P_1^{\alpha_1} \dots P_i^{\alpha_i}$$

d'où

$$A = \lambda P_1^{\alpha_1} \dots P_i^{\alpha_i} . P$$

et si P est dans la liste, cela rajoute une puissance à un P_j ; s'il ne l'est pas, la forme précédente est la forme voulue. Ce qui achève le raisonnement par récurrence.

- **Unicité de la décomposition :** Soit $A = \lambda \prod_{i=1}^n P_i^{\alpha_i} = \mu \prod_{i=1}^m Q_i^{\beta_i}$ deux décompositions de A . On a $\lambda = \mu$ car les P_i, Q_i étant unitaires, λ et μ sont égaux au coefficient dominant de A . Donc

$$\prod_{i=1}^n P_i^{\alpha_i} = \prod_{i=1}^m Q_i^{\beta_i}.$$

Donc $P_1 \mid \prod_{i=1}^m Q_i^{\beta_i}$ et P_1 est irréductible, alors il existe j tel que $P_1 \mid Q_j$. Quitte à changer l'ordre entre les Q_i , on peut supposer que $Q_j = Q_1$.

Q_1 étant irréductible et P_1, Q_1 unitaire, on a donc $P_1 = Q_1$. Ainsi, $P_1 = Q_1$ étant premier avec $Q_2^{\alpha_2} \dots Q_m^{\alpha_m}$ on a $P_1^{\alpha_1} \mid Q_1^{\beta_1}$, d'où

$$\alpha_1 \leq \beta_1.$$

En raisonnant de manière analogue avec Q_1 , on trouve $\beta_1 \leq \alpha_1$ d'où $\alpha_1 = \beta_1$.

On obtient donc $\prod_{i=2}^n P_i^{\alpha_i} = \prod_{i=2}^m Q_i^{\beta_i}$ et on procède de la même manière pour $i = 2, 3, \dots$. Ainsi, les deux décompositions sont les mêmes. □

Définition 19. Polynôme scindé

Soit $P \in \mathbb{K}[X]$ non constant. On dit que P est un **polynôme scindé** sur $\mathbb{K}$ si ses facteurs irréductibles dans $\mathbb{K}[X]$ sont tous de degré 1 i.e. il existe $\lambda \in \mathbb{K}$, $k \in \mathbb{N}^*$, $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ et $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que :

$$P = \lambda \prod_{i=1}^k (X - \lambda_i)^{\alpha_i}$$

Si de plus, dans la décomposition précédente, $\alpha_1 = 1, \dots, \alpha_k = 1$ i.e. les racines $\lambda_1, \dots, \lambda_k$ de P sont simples, on dit que P est scindé à **racines simples** sur $\mathbb{K}$ ou encore P est **simplement** scindé sur $\mathbb{K}$.

Exemple 10.

Le polynôme $P = X^2 + 1$ est scindé à racines simples sur $\mathbb{C}$ car $P = (X - i)(X + i)$ mais il n'est pas scindé sur $\mathbb{R}$ car il est de degré 2 sans aucune racine réelle.

b. Irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$ **Théorème 18.** *Théorème de D'Alembert-Gauss*

Tout polynôme non constant de $\mathbb{C}$ admet au moins une racine dans $\mathbb{C}$.

Corollaire 9.

Tout polynôme non constant est scindé sur $\mathbb{C}$.

Proposition 36.

- Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
- Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Partie E

Algèbres

Dans toute cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

1. Structure d'algèbre

Définition 20.

Soit A un espace vectoriel sur $\mathbb{K}$ et $\cdot$ une loi de composition interne sur A . On dit que le couple $(A, \cdot)$ ou plus simplement que A est une **algèbre sur $\mathbb{K}$** si :

- i) la loi $\cdot$ est associative ;
- ii) la loi $\cdot$ est bilinéaire ;
- iii) la loi $\cdot$ possède un élément neutre 1_A .

De plus, on dit qu'une algèbre A est **commutative** si, pour tous $x, y \in A$, $xy = yx$.

Remarque 13.

Une algèbre est en particulier munie de structures d'anneau et d'espace vectoriel.

Exemple 11.

- $(\mathbb{K}, \times)$ est une algèbre commutative sur $\mathbb{K}$;
- $(\mathbb{K}[X], \times)$ est une algèbre commutative sur $\mathbb{K}$;
- Soit E un espace vectoriel sur $\mathbb{K}$. $(\mathcal{F}(E, E), \circ)$ est une algèbre sur $\mathbb{K}$. Cette algèbre est commutative si E de dimension 1 et non commutative si E est de dimension supérieure ou égale à 2 ;
- Soit $n \in \mathbb{N}^*$. $(M_n(\mathbb{K}), \times)$ est une algèbre sur $\mathbb{K}$; commutative si $n = 1$ et non commutative si $n \geq 2$;
- si X est un ensemble, $(\mathcal{F}(X, \mathbb{K}), \times)$ est une algèbre commutative sur $\mathbb{K}$.

2. Sous-algèbres

a. Définition

Définition 21. Sous-algèbre

Soit $(A, \cdot)$ une algèbre sur $\mathbb{K}$ et $B \subset A$. On dit que B est une **sous-algèbre** de A si :

- i) B est un sous-espace vectoriel de A ;
- ii) B est stable par $\cdot$;

iii) $1_A \in B$.

Exemple 12.

- Les ensembles $\text{Vect}(1_A)$ et A sont des sous-algèbres de A ;
- Soit E un espace vectoriel sur $\mathbb{K}$. L'ensemble $\mathcal{L}(E)$ est une sous-algèbre de $\mathcal{F}(E, E)$.
- Soit $n \in \mathbb{N}^*$. L'ensemble $T_n^+(\mathbb{K})$ des matrices triangulaires supérieures est une sous-algèbre de $M_n(\mathbb{K})$.

b. Sous-algèbre engendrée par une partie

Proposition 37.

Soit A une algèbre et $(B_i)_{i \in I}$ une famille quelconque de sous-algèbres de A . L'ensemble $\bigcap_{i \in I} B_i$ est une sous-algèbre de A .

Autrement dit, une intersection quelconque de sous-algèbres est une sous-algèbre.

Démonstration.

On pose $B = \bigcap_{i \in I} B_i \subset A$.

- i) Comme une intersection quelconque de sous-espaces vectoriels est un sous-espace vectoriel, B est un sous-espace vectoriel de A .
- ii) Soit $x, y \in B$. Alors, pour tout $i \in I$, $x, y \in B_i$ qui est une sous-algèbre de A et donc B_i est stable par $\cdot$; d'où $xy \in B_i$. Par suite, $xy \in B$.
- iii) Pour tout $i \in I$, $1_A \in B_i$ qui est une sous-algèbre de A et donc B_i contient 1_A . Par suite, $1_A \in B$.

Il en résulte que $B = \bigcap_{i \in I} B_i$ est une sous-algèbre de A . □

Définition-Proposition 22. Sous-algèbre engendrée par une partie

Soit A une algèbre et X une partie de A .

On appelle **sous-algèbre de A engendrée par X** la sous-algèbre :

$$\bigcap_{B \in \mathcal{A}_X} B \quad \text{où } \mathcal{A}_X = \{B \text{ sous-algèbre de } A \mid X \subset B\}.$$

La sous-algèbre de A engendrée par X est la plus petite sous-algèbre de A contenant X .

Soit B est une sous-algèbre de A . On dit que X **engendre l'algèbre B** ou **l'algèbre B est engendrée par X** si la sous-algèbre de A engendrée par X est égale à B .

Démonstration.

On note $B_X = \bigcap_{B \in \mathcal{A}_X} B$. D'après la proposition 37, B_X est une sous-algèbre de A . Elle contient X car, pour tout $B \in \mathcal{A}_X$, $X \subset B$ et, il s'agit de plus petite sous-algèbre contenant X , car, si B est une sous-algèbre contenant X , $B_X = \bigcap_{B' \in \mathcal{A}_X} B' \subset B$. $\square$

Exemple 13.

- Soit A une algèbre. La sous-algèbre de A engendrée par l'ensemble vide est égale à $\text{Vect}(1_A)$. En particulier, une sous-algèbre de A engendrée par une partie quelconque contient $\text{Vect}(1_A)$.
- L'algèbre $\mathbb{K}[X]$ est engendrée par $\{X\}$.

- On note B la sous-algèbre de A engendrée par l'ensemble vide. Comme B est une sous-algèbre, elle contient 1_A et donc, comme B est en particulier un sous-espace vectoriel de A , B contient $\text{Vect}(1_A)$ qui est une sous-algèbre de A qui contient l'ensemble vide. Or B étant la plus petite sous-algèbre de A qui contient $\emptyset$, $B = \text{Vect}(1_A)$.

De plus, la sous-algèbre B' de A engendrée par $X \subset A$ contient $\emptyset$, donc, B étant la plus petite des sous-algèbres de A contenant $\emptyset$, on a $\text{Vect}(1_A) = B \subset B'$.

- Notons A la sous-algèbre de $\mathbb{K}[X]$ engendrée par $\{X\}$. Comme sous-algèbre de $\mathbb{K}[X]$, A contient 1 et, pour tout $n \in \mathbb{N}^*$, $X^n \in A$ car A est stable par produit. Ainsi, A contient la base canonique $(X^n)_{n \in \mathbb{N}}$ de $\mathbb{K}[X]$, donc, comme A est en particulier un sous-espace vectoriel de $\mathbb{K}[X]$, on a :

$$\mathbb{K}[X] = \text{Vect}((X^n)_{n \in \mathbb{N}}) \subset A \subset \mathbb{K}[X],$$

d'où $A = \mathbb{K}[X]$.

Proposition 38.

Soit A une algèbre et X une partie de A .

La sous-algèbre de A engendrée par X est l'ensemble des combinaisons linéaires de produits finis d'éléments de X (avec la convention qu'une somme vide vaut 0_A et qu'un produit vide vaut 1_A).

Démonstration.

Considérons A_X la sous-algèbre de A engendrée par X et B l'ensemble des combinaisons linéaires de produits finis d'éléments de X .

En tant que sous-algèbre de A , A_X est stable par combinaisons linéaires et produits d'éléments de X , donc $B \subset A_X$.

Il reste à montrer $A_X \subset B$. Pour cela, il suffit de vérifier que B est une sous-algèbre qui contient X .

- B est un sous-espace vectoriel de A car 0_A est la combinaison linéaire vide et une combinaison linéaire de combinaisons linéaires est une combinaison linéaire.
- B est stable par produit car, par bilinéarité de $\cdot$, un produit de combinaisons linéaires de

produits est une combinaison linéaire de produits.

— L'élément 1_A vaut le produit vide et donc appartient à B .

Ainsi, B est une sous-algèbre de A et celle-ci contient X car chaque élément x de X s'écrit comme la somme d'un seul produit d'un seul élément... x !

Comme A_X est la plus petite sous-algèbre de A qui contient X , on a $A_X \subset B$.

Il en résulte que $A_X = B$. □

Exercice 24.

Soit $n \in \mathbb{N}^*$. Montrer que l'algèbre $M_n(\mathbb{K})$ est engendrée par la paire $\{E_{1,1}, C\}$ où :

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Correction.

On a noté $\mathcal{A}$ la sous-algèbre engendrée par $\{E_{1,1}, C\}$. Comme $\mathcal{A}$ est en particulier un sous-espace vectoriel de $M_n(\mathbb{K})$, il nous suffit de montrer que les matrices élémentaires $E_{i,j}$ pour $i, j \in \llbracket 1, n \rrbracket$ appartiennent à $\mathcal{A}$ puisqu'elles forment une base de $M_n(\mathbb{K})$.

On remarque tout d'abord que multiplier une matrice à gauche par C revient à permuter ses lignes circulairement d'un cran vers le bas ; et, multiplier une matrice à droite par C revient à permuter ses colonnes circulairement d'un cran vers la gauche.

En particulier, cela implique que $C^n = I_n$; donc C est inversible d'inverse $C^{-1} = C^{n-1} \in \mathcal{A}$ car $\mathcal{A}$ est stable par produit, et multiplier à droite par C^{-1} revient à permuter circulairement les colonnes d'un cran vers la droite.

Ainsi, pour tous $i, j \in \llbracket 1, n-1 \rrbracket$, on a :

$$CE_{i,j} = E_{i+1,j} \text{ et } E_{i,j}C^{-1} = E_{i,j+1}$$

Par suite, on obtient, pour tous $i, j \in \llbracket 1, n \rrbracket$:

$$E_{i,j} = C^{i-1}E_{1,1}C^{-(j-1)} \in \mathcal{A}$$

car $\mathcal{A}$ est stable par produit.

Concluons grâce à notre remarque initiale : comme $(E_{i,j})_{i,j \in \llbracket 1, n \rrbracket}$ est une base de l'espace vectoriel $M_n(\mathbb{K})$ et $\mathcal{A}$ est en particulier un sous-espace vectoriel de $M_n(\mathbb{K})$ qui contient ces vecteurs, $\mathcal{A}$ est de dimension au moins n^2 dans l'espace vectoriel $M_n(\mathbb{K})$; d'où $\mathcal{A} = M_n(\mathbb{K})$.

3. Morphismes d'algèbres

Définition 23. Morphisme d'algèbre

Soit A, B deux algèbres sur $\mathbb{K}$ et $f : A \rightarrow B$. On dit que f est un **morphisme d'algèbres** si :

- i) L'application f est linéaire de l'espace vectoriel A dans l'espace vectoriel B i.e. pour tous $\lambda, \mu \in \mathbb{K}$ et tous $x, y \in A$,

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y);$$

- ii) pour tous $x, y \in A$,

$$f(xy) = f(x)f(y);$$

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

Un morphisme d'algèbres bijectif est appelé un **isomorphisme d'algèbres**.

Exemple 14.

- $\lambda \mapsto \lambda 1_A$ est un morphisme d'algèbres de $\mathbb{K}$ dans $\text{Vect}(1_A)$;
- Soit $n \in \mathbb{N}^*$, E un espace vectoriel de dimension n et $\mathcal{B}$ une base de E . L'application $\text{Mat}_{\mathcal{B}} : f \mapsto \text{Mat}_{\mathcal{B}}(f)$ est un isomorphisme d'algèbres de $\mathcal{L}(E)$ dans $M_n(\mathbb{K})$.
- Soit $n \in \mathbb{N}^*$. Pour $P \in GL_n(\mathbb{K})$, $M \mapsto PMP^{-1}$ est un isomorphisme d'algèbres de $M_n(\mathbb{K})$ dans lui-même.

Proposition 39.

Soit A, B deux algèbres sur $\mathbb{K}$ et $f : A \rightarrow B$ un morphisme d'algèbres.

- Le noyau $\text{Ker}(f)$ est un idéal de l'anneau $(A, +, \cdot)$.
- L'image $\text{Im}(f)$ est une sous-algèbre de B .

Démonstration.

- $\text{Ker}(f)$ est un idéal de l'anneau $(A, +, \cdot)$ car c'est le noyau d'un morphisme d'anneaux.
- • $\text{Im}(f)$ est un sous-espace vectoriel de B comme image de l'espace vectoriel A par f qui en particulier une application linéaire.
- Il reste à montrer que $\text{Im}(f)$ est stable par produit. Soit $f(x), f(y) \in \text{Im}(f)$ avec $x, y \in A$. Alors $xy \in A$ car A est une algèbre et par propriété d'un morphisme d'algèbres :

$$f(x)f(y) = f(xy) \in \text{Im}(f).$$

- Par propriété d'un morphisme d'algèbres, on a $1_B = f(1_A) \in \text{Im}(f)$.
Il en résulte que $\text{Im}(f)$ est une sous-algèbre de B .

□

4. Algèbres et polynômes

Dans ce paragraphe, A désigne une algèbre sur $\mathbb{K}$.

a. Polynômes appliqués à un élément d'une algèbre

Notation 4. Polynôme d'un élément

Soit $u \in A$ et $P \in \mathbb{K}[X]$ avec $P = \sum_{i=0}^n a_i X^i$. On note $P(u)$ l'élément de A :

$$P(u) = \sum_{i=0}^n a_i u^i = a_0 1_A + a_1 u + \dots + a_n u^n.$$

Exemple 15.

— Soit E un espace vectoriel sur $\mathbb{K}$. Pour $f \in \mathcal{L}(E)$ et $P = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$,

$$P(f) = a_0 \text{Id}_E + a_1 f + \dots + a_n f^n;$$

— Soit $n \in \mathbb{N}^*$. Pour $M \in M_n(\mathbb{K})$ et $P = \sum_{i=0}^n a_i X^i \in \mathbb{K}[X]$,

$$P(M) = a_0 I_n + a_1 M + \dots + a_n M^n.$$

Proposition 40.

Soit $u \in A$ et $P = \sum_{k=0}^{+\infty} a_k X^k, Q = \sum_{k=0}^{+\infty} b_k X^k \in \mathbb{K}[X]$. On a :

$$(P + Q)(u) = P(u) + Q(u) \quad \text{et} \quad (PQ)(u) = P(u)Q(u).$$

En particulier, $P(u)$ et $Q(u)$ commutent pour l'opération $\cdot$.

Démonstration.

On a :

$$P + Q = \sum_{k=0}^{+\infty} (a_k + b_k) X^k \quad \text{et} \quad PQ = \sum_{k=0}^{+\infty} \sum_{l=0}^{+\infty} a_k b_l X^{k+l},$$

donc :

$$(P + Q)(u) = \sum_{k=0}^{+\infty} (a_k + b_k) u^k \quad \text{et} \quad (PQ)(u) = \sum_{k=0}^{+\infty} \sum_{l=0}^{+\infty} a_k b_l u^{k+l}.$$

Or, par propriétés des opérations dans l'espace vectoriel A , on a :

$$P(u) + Q(u) = \sum_{k=0}^{+\infty} a_k u^k + \sum_{k=0}^{+\infty} b_k u^k = \sum_{k=0}^{+\infty} (a_k + b_k) u^k = (P + Q)(u);$$

et, de plus, comme $\cdot$ est bilinéaire, on a :

$$P(u)Q(u) = \left(\sum_{k=0}^{+\infty} a_k u^k \right) \left(\sum_{l=0}^{+\infty} b_l u^l \right) = \sum_{k=0}^{+\infty} \sum_{l=0}^{+\infty} a_k b_l u^{k+l} = (PQ)(u).$$

Enfin, comme $\mathbb{K}[X]$ est un anneau commutatif, on a $PQ = QP$, d'où :

$$P(u)Q(u) = (PQ)(u) = (QP)(u) = Q(u)P(u).$$

□

Proposition-Notation 41.

Soit $u \in A$. L'application notée :

$$f_u : \begin{array}{ccc} \mathbb{K}[X] & \rightarrow & A \\ P & \mapsto & P(u) \end{array}$$

est un morphisme d'algèbres.

Démonstration.

Soit $\lambda, \mu \in \mathbb{K}$, $P, Q \in \mathbb{K}[X]$. On a, d'après la proposition 40 :

i)

$$\begin{aligned} f_u(\lambda P + \mu Q) &= (\lambda P + \mu Q)(u) \\ &= (\lambda P)(u) + (\mu Q)(u) \\ &= \lambda P(u) + \mu Q(u) \\ &= f_u(P) + f_u(Q) \end{aligned}$$

ii)

$$\begin{aligned} f_u(PQ) &= (PQ)(u) \\ &= P(u)Q(u) \\ &= f_u(P)f_u(Q) \end{aligned}$$

iii) $f_u(1) = 1(u) = 1_A$

Il en résulte que f_u est un morphisme d'algèbres.

□

b. Polynômes annulateurs et polynôme minimal

Définition 24. Idéal et polynôme annulateur

Soit $u \in A$. On appelle **idéal annulateur de u** l'ensemble

$$\text{Ker}(f_u) = \{P \in \mathbb{K}[X] \mid P(u) = 0_A\}.$$

Soit $P \in \mathbb{K}[X]$. Si P appartient à l'idéal annulateur de u i.e. si $P(u) = 0_A$, on dit que P est un **polynôme annulateur de u** .

On a montré dans la partie précédente que $\mathbb{K}[X]$ est un anneau principal. Ceci justifie la définition suivante :

Définition 25. Polynôme minimal

Soit $u \in A$.

Si l'idéal annulateur de u n'est pas réduit à 0_A i.e. si u possède un polynôme annulateur non nul, on appelle **polynôme minimal de u** et on note π_u l'unique générateur unitaire de l'idéal annulateur de u . Dans ce cas, on dit que u **admet un polynôme minimal**.

Exemple 16.

- Un élément u de A est dit **nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $u^n = 0$.
Dans ce cas, le polynôme X^n est un polynôme annulateur de u . Comme le polynôme minimal de u divise X^n donc il existe $k \leq n$ tel que $\pi_u = X^k$.
- Un élément u de A est dit **idempotent** si $u^2 = u$.
Dans ce cas, $X^2 - X$ est un polynôme annulateur de u . Comme $\pi_u | X^2 - X$, alors on a trois cas possibles :
 1. $\pi_u = X$, auquel cas $u = 0_A$;
 2. $\pi_u = X - 1$, auquel cas $u = 1_A$;
 3. $\pi_u = X^2 - X$, auquel cas $u \neq 0_A$ et $u \neq 1_A$.

Proposition 42.

Soit $u \in A$ tel que u admet un polynôme minimal π_u . Il existe $\lambda \in \mathbb{K}$ tel que $u = \lambda 1_A$ si, et seulement si, $\deg(\pi_u) = 1$.

Démonstration.

On a :

Il existe $\lambda \in \mathbb{K}$ tel que $u = \lambda 1_A$ si, et seulement si,

Il existe $\lambda \in \mathbb{K}$ tel que $u - \lambda 1_A = 0_A$ si, et seulement si,

Il existe $\lambda \in \mathbb{K}$ tel que $X - \lambda$ est un polynôme annulateur de u si, et seulement si,

Il existe $\lambda \in \mathbb{K}$ tel que $X - \lambda$ est le polynôme minimal de A si, et seulement si,

$\deg(\pi_u) = 1$. □

Exercice 25.

1. Soit $f \in \mathcal{L}(\mathbb{R}^3)$ tel que $f(x, y, z) = (y, z, x)$. Calculer f^3 et en déduire un polynôme annulateur de f puis le polynôme minimal de f .
2. Soit $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(\mathbb{R})$. Calculer A^3 et déterminer un polynôme annulateur de A puis le polynôme minimal de A .

Correction.

1. On a, pour $(x, y, z) \in \mathbb{R}^3$:

$$f^3(x, y, z) = f^2(y, z, x) = f(z, x, y) = x, y, z$$

Donc $f^3 = \text{Id}_{\mathbb{R}^3}$.

Par suite, $X^3 - 1$ est un polynôme annulateur de f .

De plus, on a $P = X^3 - 1 = (X - 1)(X^2 + X + 1)$ donc P est le polynôme minimal de f car ni $X - 1$, ni $X^2 + X + 1$ ne sont des polynômes annulateurs de f .

2. On a

$$A^3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0_3,$$

donc X^3 est un polynôme annulateur de A .

De plus X et X^2 sont les seuls diviseurs non triviaux de X^3 et aucun des deux n'est un polynôme annulateur de A donc X^3 est le polynôme minimal de A . Ainsi, A est une matrice nilpotente d'indice 3.

c. Sous-algèbre engendrée par un élément

Définition-Proposition 26.

Soit $u \in A$. On appelle **sous-algèbre engendré par u** et on note $\mathbb{K}[u]$ l'ensemble :

$$\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}.$$

L'ensemble $\mathbb{K}[u]$ est une sous-algèbre *commutative* de A égale à la sous-algèbre de A engendrée par $\{u\}$.

Démonstration.

On a $\mathbb{K}[u] = \text{Im}(f_u)$ donc $\mathbb{K}[u]$ est une sous-algèbre de A comme image d'un morphisme d'algèbres. De plus, d'après la proposition 40, pour $P(u), Q(u) \in \mathbb{K}[u]$ avec $P, Q \in \mathbb{K}[X]$, $P(u)$ et $Q(u)$ commutent pour $\cdot$, donc $\cdot$ est commutative sur $\mathbb{K}[u]$.

Montrons que $\mathbb{K}[u]$ est la sous-algèbre A_u de A engendrée par $\{u\}$.

On a $u = P(u)$ avec $P = X$, donc $u \in \mathbb{K}[u]$. Par suite, $\mathbb{K}[u]$ est une sous-algèbre contenant $\{u\}$, d'où $A_u \subset \mathbb{K}[u]$.

Montrons l'inclusion réciproque. Soit $x \in \mathbb{K}[u]$. Alors il existe $P = \sum_{k=0}^n a_k X^k \in \mathbb{K}[X]$ tel que $x = P(u)$. Par suite, comme A_u est une sous-algèbre de A contenant u et donc, en particulier, un sous-espace vectoriel de A , stable par $\cdot$, contenant $u^0 = 1_A$ et u ; on a :

$$x = P(u) = \sum_{k=0}^n a_k \underbrace{u^k}_{\in A_u} \in A_u.$$

D'où $\mathbb{K}[u] \subset A_u$.

Il en résulte que $\mathbb{K}[u] = A_u$ i.e. $\mathbb{K}[u]$ est la sous-algèbre de A engendrée par $\{u\}$. □

Proposition 43.

Soit $u \in A$. Si u admet un polynôme minimal $\pi_u \in \mathbb{K}[X]$ avec $d = \deg(\pi_u)$, alors $\mathbb{K}[u]$ est une algèbre de dimension finie d et

$$(u^k)_{0 \leq k \leq d-1}$$

est une base de $\mathbb{K}[u]$.

Démonstration.

On suppose que u admet un polynôme minimal π_u avec $d = \deg(\pi_u)$.

Tout d'abord, comme $\mathbb{K}[u]$ est une sous-algèbre contenant u , on a $u^0 = 1_A, u \in \mathbb{K}[u]$ et ainsi, $\mathbb{K}[u]$ étant stable par produit, pour tout $k \in \mathbb{N}$, $u^k \in \mathbb{K}[u]$.

Montrons que $(u^k)_{0 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$.

- *Famille libre* : soit $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{K}$ des scalaires tels que $\sum_{k=0}^{d-1} \lambda_k u^k = 0_A$. Alors le polynôme $P = \sum_{k=0}^{d-1} \lambda_k X^k$ est un polynôme annulateur de u de degré $\leq d-1 < d = \deg(\pi_u)$. Or π_u est de degré minimal parmi les polynômes annulateurs non nuls de u . Donc $P = 0$ et ainsi, pour tout $k \in \llbracket 0, d-1 \rrbracket$, $\lambda_k = 0$. Donc la famille $(u^k)_{0 \leq k \leq d-1}$ est libre dans l'espace vectoriel $\mathbb{K}[u]$.
- *Famille génératrice* : Soit $P(u) \in \mathbb{K}[u]$. Alors $P \in \mathbb{K}[X]$ et par division euclidienne de ce polynôme par π_u , il existe $Q, R \in \mathbb{K}[X]$ tels que $P = \pi_u Q + R$ et $\deg(R) < d-1$. Par suite,

$$P(u) = \underbrace{\pi_u(u)}_{=0_A} Q(u) + R(u) = R(u).$$

et R est de degré $\leq d-1$ donc il existe $\lambda_0, \dots, \lambda_{d-1} \in \mathbb{K}$ tels que $R = \sum_{k=0}^{d-1} \lambda_k X^k$. Il en résulte que :

$$P(u) = R(u) = \sum_{k=0}^{d-1} \lambda_k u^k \in \text{Vect} (u^k)_{0 \leq k \leq d-1}.$$

Et ainsi, $(u^k)_{0 \leq k \leq d-1}$ est génératrice dans l'espace vectoriel $\mathbb{K}[u]$.

Donc $(u^k)_{0 \leq k \leq d-1}$ est une base de l'espace vectoriel $\mathbb{K}[u]$ et, de plus, cette base comporte d vecteurs donc $\dim(\mathbb{K}[u]) = d$. □

Question 3.

Que dire de la dimension de $\mathbb{K}[u]$ lorsque u n'admet pas de polynôme annulateur non nul ?

Correction.

Si u n'admet pas de polynôme annulateur non nul, alors, pour tout $P \in \mathbb{K}[X]$ avec $P \neq 0$, $P(u) \neq 0$, ce qui permet de montrer que la famille $(u^k)_{k \in \mathbb{N}}$ est une famille libre de $\mathbb{K}[u]$. Comme cette famille est infinie, il en résulte que $\dim(\mathbb{K}[u]) = +\infty$.

Méthode : Connaissant le polynôme minimal π_u d'un élément u d'une algèbre A , on peut, pour $P \in \mathbb{K}[X]$, donner la décomposition de $P(u)$ dans la base $(u^k)_{0 \leq k \leq d-1}$ de $\mathbb{K}[u]$: il suffit de déterminer le reste R de la division euclidienne de P par π_u et d'évaluer R en u pour obtenir la décomposition voulue.

Ainsi, cette méthode donne un moyen pratique pour calculer les puissances successives u^n de u pour $n \in \mathbb{N}^*$!

Exercice 26.

Soit $A = \begin{pmatrix} 8 & -3 & -6 \\ -2 & 3 & 2 \\ 6 & -3 & -4 \end{pmatrix}$

1. Calculer A^2 et déterminer un polynôme annulateur de A .
2. Ce polynôme est-il le polynôme minimal de A ?
3. Montrer que A est inversible en utilisant son polynôme minimal.
4. Calculer A^n pour $n \in \mathbb{N}$.

Correction.

1. On a

$$A^2 = \begin{pmatrix} 34 & -15 & -30 \\ -10 & 9 & 10 \\ 30 & -15 & -26 \end{pmatrix}$$

et on remarque que $A^2 - 5A = -6I_3$ i.e. $A^2 - 5A + 6I_3 = 0_3$. Ainsi, le polynôme

$$P = X^2 - 5X + 6$$

est un polynôme annulateur de A .

2. On a $P = (X - 2)(X - 3)$ donc on a trois possibilités pour π_A du fait que $\deg(\pi_A) \geq 1$ et $\pi_A | P$:

- $\pi_A = X - 2$: impossible car $A \neq 2I_3$
- $\pi_A = X - 3$: impossible car $A \neq 3I_3$
- et donc $\pi_A = (X - 2)(X - 3)$!

Par suite P est le polynôme minimal de A .

3. On a $A^2 - 5A + 6I_3 = 0_3$ donc $A(\frac{-1}{6}(A - 5I_3)) = I_3$. Par suite A est inversible et son inverse est :

$$\frac{-1}{6}(A - 5I_3).$$

4. On effectue la division euclidienne de X^n par P qui est de degré 2, alors il existe $Q, R \in \mathbb{K}[X]$ tels que $\deg(R) \leq 1$ et

$$X^n = QP + R \quad (*)$$

Comme R est de degré au plus 1, il existe $a, b \in \mathbb{K}$ tels que $R = aX + b$. les nombres 2 et 3 étant des racines de P i.e. $P(2) = 0$ et $P(3) = 0$, en évaluant $(*)$ en 2 et 3 on obtient :

$$\begin{cases} 2^n = 2a + b \\ 3^n = 3a + b \end{cases} \Leftrightarrow \begin{cases} a = 3^n - 2^n \\ b = 3 \cdot 2^n - 2 \cdot 3^n \end{cases}$$

et donc on obtient :

$$A^n = Q(A) \underbrace{P(A)}_{=0_3} + R(A) = aA + b = (3^n - 2^n)A + (3 \cdot 2^n - 2 \cdot 3^n)I_3.$$

Proposition 44.

Soit $n \in \mathbb{N}$, A une algèbre sur $\mathbb{K}$ de dimension finie n et $u \in A$. L'élément u admet un polynôme minimal π_u et $\deg(\pi_u) \leq n$.

Démonstration.

Soit $u \in A$. Montrons que u possède un polynôme annulateur non nul. La famille $(1_A, u, \dots, u^n)$ est liée car composée de $n+1$ vecteurs dans un espace de dimension n . Ainsi, il existe $\lambda_0, \dots, \lambda_n \in \mathbb{K}$ non tous nuls tels que :

$$\sum_{i=0}^n \lambda_i u^i = 0_A.$$

Par suite, $P = \sum_{i=0}^n \lambda_i X^i$ est un polynôme annulateur non nul de u d'où u admet un polynôme minimal π_u et de plus, $\deg(\pi_u) \leq \deg(P) \leq n$. $\square$

Remarque 14.

En particulier, dans $M_n(\mathbb{K})$, toute matrice admet un polynôme minimal de degré inférieur ou égal à n^2 . On verra dans le chapitre sur la réduction des endomorphismes et des matrices carrées qu'en réalité, on a bien mieux : en effet, le degré maximal du polynôme minimal d'une matrice de $M_n(\mathbb{K})$ est en fait égal à n .

5. Norme d'algèbre

Dans ce paragraphe, A désigne une algèbre sur $\mathbb{K}$.

Définition 27.

Soit $\|\cdot\| : A \rightarrow \mathbb{R}$. On dit que $\|\cdot\|$ est une **norme d'algèbre** sur A , ou encore, est une **norme sous-multiplicative** sur A , si $\|\cdot\|$ est une norme sur l'espace vectoriel A et si, pour tous $a, b \in A$:

$$\|ab\| \leq \|a\| \cdot \|b\|.$$

Exemple 17.

- La valeur absolue et le module sont des normes d'algèbres sur $\mathbb{R}$ et $\mathbb{C}$ respectivement.
- Soit $n \in \mathbb{N}^*$. L'application $\|\cdot\|_2 : M \rightarrow \sqrt{\text{Tr}({}^t M M)}$ est une norme d'algèbre (une norme sous-multiplicative) sur $M_n(\mathbb{R})$.

- Vu en Sup' !
- La norme $\|\cdot\|_2$ est la norme associée au produit scalaire canonique sur $M_n(\mathbb{R})$, à savoir $(\cdot|\cdot) : (M, N) \mapsto \text{Tr}({}^tMN)$. On remarque que pour $A = (a_{i,j})_{1 \leq i,j \leq n}$, on a :

$$\|A\|_2^2 = \sum_{1 \leq i,j \leq n} a_{i,j}^2.$$

On considère $\langle \cdot, \cdot \rangle$ le produit scalaire canonique de $M_{n,1}(\mathbb{R})$ i.e., pour $X, Y \in M_{n,1}(\mathbb{R})$, $\langle X, Y \rangle = {}^tXY$; et $\|\cdot\|$ sa norme associée sur $M_{n,1}(\mathbb{R})$.

Soit $M, N \in M_n(\mathbb{R})$. On note, pour $i \in \llbracket 1, n \rrbracket$:

- L_i la i -ème ligne de M ;
- C_i la i -ème colonne de N .

Alors, avec ces notations, on a :

$$\star MN = (\langle {}^tL_i, C_j \rangle)_{1 \leq i,j \leq n} \text{ et donc :}$$

$$\|MN\|_2^2 = \text{Tr}({}^t(MN)(MN)) = \sum_{1 \leq i,j \leq n} \langle {}^tL_i, C_j \rangle^2;$$

$$\star {}^tNN = (\langle C_i, C_j \rangle)_{1 \leq i,j \leq n} \text{ et donc :}$$

$$\|N\|_2^2 = \text{Tr}({}^tNN) = \sum_{i=1}^n \langle C_i, C_i \rangle = \sum_{i=1}^n \|C_i\|^2;$$

$$\star M^tM = (\langle {}^tL_i, {}^tL_j \rangle)_{1 \leq i,j \leq n} \text{ et donc, comme pour tous } A, B \in M_n(\mathbb{R}), \text{Tr}(AB) = \text{Tr}(BA) :$$

$$\|M\|_2^2 = \text{Tr}({}^tMM) = \text{Tr}(M^tM) = \sum_{i=1}^n \langle {}^tL_i, {}^tL_i \rangle = \sum_{i=1}^n \|{}^tL_i\|^2;$$

Or, d'après l'inégalité de Cauchy-Schwarz pour le produit scalaire $\langle \cdot, \cdot \rangle$, on a, pour tous $i, j \in \llbracket 1, n \rrbracket$:

$$\langle {}^tL_i, C_j \rangle^2 \leq \|{}^tL_i\|^2 \cdot \|C_j\|^2,$$

donc :

$$\begin{aligned} \|MN\|_2^2 &= \sum_{1 \leq i,j \leq n} \langle {}^tL_i, C_j \rangle^2 \\ &\leq \sum_{1 \leq i,j \leq n} \|{}^tL_i\|^2 \cdot \|C_j\|^2 \\ &\leq \left(\sum_{i=1}^n \|{}^tL_i\|^2 \right) \cdot \left(\sum_{j=1}^n \|C_j\|^2 \right) \\ &\leq \|M\|_2^2 \cdot \|N\|_2^2 \end{aligned}$$

d'où, par croissance de la fonction racine carrée sur $\mathbb{R}_+$:

$$\|MN\|_2 \leq \|M\|_2 \cdot \|N\|_2$$

Il en résulte que $\|\cdot\|_2$ est une norme d'algèbre sur $M_n(\mathbb{R})$.

Exercice 27.

1. Soit $n \in \mathbb{N}^*$. On considère les normes $\|\cdot\|_1$ et $\|\cdot\|_\infty$ sur l'algèbre $M_n(\mathbb{K})$ où, pour $M = (m_{i,j})_{1 \leq i,j \leq n}$:

$$\|M\|_1 = \sum_{1 \leq i,j \leq n} |m_{i,j}| \quad \text{et} \quad \|M\|_\infty = \max_{1 \leq i,j \leq n} (|m_{i,j}|).$$

- (a) Les normes $\|\cdot\|_1$ et $\|\cdot\|_\infty$ sont-elles des normes d'algèbres ?
 (b) Déterminer une norme d'algèbre sur $M_n(\mathbb{K})$ proportionnelle à la norme infinie $\|\cdot\|_\infty$.
2. Déterminer, sur l'algèbre $(C([0,1], \mathbb{R}), \times)$, quelles normes sont sous-multiplicatives parmi les normes de la convergence en moyenne, de la convergence en moyenne quadratique, de la convergence uniforme.

Correction.

1. Pour $n = 1$, les deux normes considérées sont égales à la valeur absolue/module sur $\mathbb{K} = M_1(\mathbb{K})$ qui est une norme d'algèbre. Plaçons nous dans le cas $n \geq 2$:

- (a) On remarque que pour $A = (1)_{1 \leq i,j \leq n}$, $A^2 = (n)_{1 \leq i,j \leq n}$ d'où, comme $n > 1$:

$$\|A^2\|_\infty = n > 1 = \|A\|_\infty \cdot \|A\|_\infty$$

donc $\|\cdot\|_\infty$ n'est pas sous-multiplicative.

Soit $A = (a_{i,j})_{1 \leq i,j \leq n}$, $B = (b_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbb{K})$. On a :

$$\|AB\|_1 = \sum_{1 \leq i,j \leq n} \left| \sum_{k=1}^n a_{i,k} b_{k,j} \right| \leq \sum_{1 \leq i,j,k \leq n} |a_{i,k}| \cdot |b_{k,j}|.$$

Or :

$$\|A\|_1 \cdot \|B\|_1 = \left(\sum_{1 \leq i,k \leq n} |a_{i,k}| \right) \left(\sum_{1 \leq l,j \leq n} |b_{l,j}| \right) = \sum_{1 \leq i,j,k,l \leq n} |a_{i,k}| \cdot |b_{l,j}|$$

et ainsi

$$\|AB\|_1 \leq \sum_{1 \leq i,j,k \leq n} |a_{i,k}| \cdot |b_{k,j}| \leq \sum_{1 \leq i,j,k,l \leq n} |a_{i,k}| \cdot |b_{l,j}| = \|A\|_1 \cdot \|B\|_1$$

donc $\|\cdot\|_1$ est une norme d'algèbre sur $M_n(\mathbb{K})$.

- (b) Analysons. Soit $\alpha > 0$. On pose $\|\cdot\| = \alpha \cdot \|\cdot\|_\infty$. Alors $\|\cdot\|$ est une norme sur $M_n(\mathbb{K})$ car $\alpha > 0$ et on a, pour tous $A = (a_{i,j})_{1 \leq i,j \leq n}$, $B = (b_{i,j})_{1 \leq i,j \leq n} \in M_n(\mathbb{K})$:

$$\begin{aligned} \|AB\| &= \alpha \|AB\|_\infty \\ &= \alpha \max_{1 \leq i,j \leq n} \left(\left| \sum_{k=1}^n a_{i,k} b_{k,j} \right| \right) \\ &\leq \alpha \max_{1 \leq i,j \leq n} \left(\sum_{k=1}^n \underbrace{|a_{i,k}|}_{\leq \|A\|_\infty} \cdot \underbrace{|b_{k,j}|}_{\leq \|B\|_\infty} \right) \\ \|AB\| &\leq \alpha n \|A\|_\infty \|B\|_\infty = \frac{n}{\alpha} \|A\| \|B\| \end{aligned}$$

Ainsi, en posant $\alpha = n > 0$, $\|\cdot\|$ est sous-multiplicative sur $M_n(\mathbb{K})$ et est proportionnelle à la norme $\|\cdot\|_\infty$.

2. — Commençons par la norme $\|\cdot\|_\infty$ de la convergence uniforme. Pour tous $f, g \in C([0, 1], \mathbb{R})$, on a :

$$\|f.g\|_\infty = \sup_{t \in [0, 1]} |f(t)g(t)| = \sup_{t \in [0, 1]} (\underbrace{|f(t)|}_{\leq \|f\|_\infty} \cdot \underbrace{|g(t)|}_{\leq \|g\|_\infty}) \leq \|f\|_\infty \cdot \|g\|_\infty.$$

Par suite, $\|\cdot\|_\infty$ est une norme d'algèbre sur $C([0, 1], \mathbb{R})$.

- Pour les normes de la convergence en moyenne et en moyenne quadratique, on voit rapidement que ce ne sont pas des normes d'algèbre : pour $f : x \mapsto x$, on a

$$\|f^2\|_1 = \frac{1}{3} \text{ et } \|f\|_1^2 = \frac{1}{4}$$

puis

$$\|f^2\|_2 = \frac{1}{\sqrt{5}} \text{ et } \|f\|_2^2 = \frac{1}{3}.$$

Dans le chapitre "Topologie des espaces vectoriels normés", on montrera que sur toute algèbre de dimension finie, il existe une norme sous-multiplicative. En dimension infinie, ce n'est pas le cas en général, comme en atteste l'exercice suivant :

Exercice 28.

On note $A = \mathbb{K}^{\mathbb{N}}$ l'espace vectoriel des suites à valeurs réelles et on considère, sur A , la loi $\times$ de multiplication terme à terme des suites.

1. Justifier que $(A, \times)$ est une algèbre.
2. Montrer qu'il n'existe pas de norme sous-multiplicative sur A .

Correction.

1. On a $A = \mathcal{F}(\mathbb{N}, \mathbb{K})$.
2. Supposons par l'absurde qu'il existe une norme $\|\cdot\|$ sous-multiplicative sur A .
Pour $k \in \mathbb{N}$, on pose $e(k) \in A$ la suite, définie pour $n \in \mathbb{N}$, par :

$$e(k)_n = \delta_{k,n} = \begin{cases} 0 & \text{si } n \neq k \\ 1 & \text{si } n = k \end{cases}$$

Considérons la suite $u = (u_n)_{n \in \mathbb{N}} \in A$. On pose $k = \lfloor \|u\| \rfloor + 1$ la partie entière de $\|u\|$ plus 1. Alors $k \in \mathbb{N}$ et $k > \|u\|$.

De plus, on a, pour $n \in \mathbb{N}$:

$$(u.e(k))_n = u_n \cdot \delta_{k,n} = \begin{cases} 0 & \text{si } n \neq k \\ k & \text{si } n = k \end{cases}$$

d'où $u.e(k) = ke(k)$. Ainsi, par sous-multiplicativité de la norme, on obtient :

$$k\|e(k)\| = \|ke(k)\| = \|u.e(k)\| \leq \|u\| \cdot \|e(k)\|$$

Or, $\|e(k)\| \neq 0$ car $e(k) \neq (0)_{n \in \mathbb{N}}$, d'où :

$$k \leq \|u\| < k.$$

Contradiction !

Il en résulte qu'il n'existe pas de norme sous-multiplicative sur $\mathbb{K}^{\mathbb{N}}$.

E&P

Exercices et problèmes

Exercice 29. *Sous-groupes et groupes monogènes*

Soit G un groupe. Un sous-groupe H de G est dit **propre** s'il est différent de G .

Dans cette exercice, on cherche à montrer que si un groupe est monogène, alors tous ses sous-groupes propres le sont et que la réciproque de cette implication est fausse.

1. Justifier que, si tous les sous-groupes de G sont monogènes, alors G est monogène.
2. On suppose G monogène. Montrer que tout sous-groupe de G est monogène.
3. Dans cette question, on souhaite montrer que l'implication $I =$ "si tous les sous-groupes propres de G sont monogènes alors G est monogène" est fausse.

Pour $n \in \mathbb{N}^*$, on note :

$$\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

l'ensemble des racines n -ième de l'unité. On rappelle que $\mathbb{U}_n$ est un sous-groupe cyclique de $(\mathbb{C}^*, \cdot)$ de cardinal n .

- (a) Soit $n \in \mathbb{N}^*$ et $z \in \mathbb{U}_n$. Montrer que, pour tout $d \in \mathbb{N}^*$ diviseur de n , $\mathbb{U}_d \subset \mathbb{U}_n$; puis que si, pour tout $d \in \mathbb{N}^*$ diviseur de n avec $d < n$, $z \notin \mathbb{U}_d$, alors $\mathbb{U}_n = \langle z \rangle$.

Soit p un nombre premier. On considère l'ensemble P suivant, appelé **p -groupe de Prüfer** :

$$P = \bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n}.$$

- (a) Montrer que P est bien un groupe muni de la multiplication complexe.
- (b) Montrer que P n'est pas de type fini i.e. qu'il n'est pas engendré par un ensemble fini de générateurs.
- (c) Soit $z \in P \setminus \{1\}$. Justifier qu'il existe un unique $n_z \in \mathbb{N}^*$ tel que $z \in \mathbb{U}_{p^{n_z}} \setminus \mathbb{U}_{p^{n_z-1}}$, puis montrer que $\mathbb{U}_{n_z} = \langle z \rangle$.
- (d) Montrer que P fournit un contre-exemple pour l'implication I .

Correction.

1. Le groupe G est un sous-groupe de G donc si tous les sous-groupes de G sont monogènes, G l'est aussi !
2. Soit G un groupe monogène d'élément neutre noté e et H un sous-groupe de G .
Si $H = \{e\}$, alors $H = \langle e \rangle$ donc H est monogène.
Supposons H non réduit à $\{e\}$. Comme G est monogène, il existe $x \in G$ tel que $G = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. Comme $H \neq \{e\}$, l'ensemble $\{k \in \mathbb{N}^* \mid x^k \in H\}$ est une partie non vide de $\mathbb{N}^*$ et donc possède un plus petit élément $d \in \mathbb{N}^*$. Montrons que $H = \langle x^d \rangle$.
Comme le sous-groupe H contient x^d par définition de d et $\langle x^d \rangle$ est le plus petit sous-groupe

contenant x^d , on a $\langle x^d \rangle \subset H$.

Soit $h \in H$. En particulier, h appartient à $G = \langle x \rangle$ donc il existe $n \in \mathbb{Z}$ tel que $h = x^n$. Ainsi, d'après le théorème de division euclidienne, il existe $q, r \in \mathbb{Z}$ tel que $n = dq + r$ avec $r \in \llbracket 0, d-1 \rrbracket$.

Comme H est un sous-groupe de G , on a $x^{dq} = (x^d)^q \in H$ et donc $x^r = x^{n-dq} = x^n \cdot (x^{dq})^{-1} \in H$. Or, d est le plus petit entier naturel k non nul tel que $x^k \in H$, d'où, comme $r \in \llbracket 0, d-1 \rrbracket$ et $x^r \in H$, on obtient $r = 0$ et donc $h = x^{dq} = (x^d)^q \in \langle x^d \rangle$.

Ainsi, $H \subset \langle x^d \rangle$.

Par suite, $H = \langle x^d \rangle$, d'où H est monogène.

Il en résulte que tout sous-groupe monogène d'un groupe monogène est monogène.

3. (a) Soit $n \in \mathbb{N}^*$ et $z \in \mathbb{U}_n$.
 - Soit $d \in \mathbb{N}^*$ tel que $d|n$. Alors il existe $k \in \mathbb{N}$ tel que $n = dk$ et, pour tout $z \in \mathbb{U}_d$, on a $z^n = (z^d)^k = 1^k = 1$, d'où $z \in \mathbb{U}_n$.
Par suite, $\mathbb{U}_d \subset \mathbb{U}_n$.
 - On suppose que, pour tout $d \in \mathbb{N}^*$ tel que $d|n$ et $d < n$, $z \notin \mathbb{U}_d$. Notons k l'ordre de z dans le groupe $\mathbb{U}_n$. Alors $z^k = 1$ et $k|n = \#\mathbb{U}_n$; or, par hypothèse, pour tout entier positif d diviseur de n et différent de n , $z^d \neq 1$, d'où $k = n$. Il en résulte que z est un générateur de $\mathbb{U}_n$.
- (b) Montrons que P est un groupe muni de la multiplication des complexes comme sous-groupe de $(\mathbb{C}^*, \cdot)$.
 - Pour tout $k \in \mathbb{N}^*$, $\mathbb{U}_k \subset \mathbb{C}^*$, donc $\bigcup_{n \in \mathbb{N}} \mathbb{U}_{p^n} \subset \mathbb{C}^*$.
 - On a $1 \in \mathbb{U}_1 = \mathbb{U}_{p^0} \subset P$.
 - Soit $z, t \in P$. Alors il existe $n, m \in \mathbb{N}$ tel que $z \in \mathbb{U}_{p^n}$ et $t \in \mathbb{U}_{p^m}$. Ainsi, pour $k = \max(n, m) \in \mathbb{N}$, on a $p^n | p^k$ et $p^m | p^k$ donc, d'après la question 3a, $\mathbb{U}_{p^n} \subset \mathbb{U}_{p^k}$ et $\mathbb{U}_{p^m} \subset \mathbb{U}_{p^k}$. Ainsi, z, t appartiennent à $\mathbb{U}_{p^k}$ qui est un groupe pour $\cdot$, donc $z \cdot t^{-1} \in \mathbb{U}_{p^k} \subset P$.

Ainsi, par la caractérisation des sous-groupes, P est un sous-groupe de $(\mathbb{C}^*, \cdot)$.

- (c) Montrons que P n'est pas de type fini. Supposons par l'absurde que P est de type fini. Alors il existe $q \in \mathbb{N}^*$ et $z_1, \dots, z_q \in P$ tels que $P = \langle z_1, \dots, z_q \rangle$. Pour tout $i \in \llbracket 1, q \rrbracket$, il existe $n_i \in \mathbb{N}$ tel que $z_i \in \mathbb{U}_{p^{n_i}}$. On pose $d = \max(n_1, \dots, n_q)$. Alors, pour tout $i \in \llbracket 1, q \rrbracket$, $n_i \leq d$ et donc $p^{n_i} | p^d \in \mathbb{N}$, d'où, d'après la question 3a :

$$z_i \in \mathbb{U}_{p^{n_i}} \subset \mathbb{U}_{p^d}.$$

Par suite, $P = \langle z_1, \dots, z_q \rangle \subset \mathbb{U}_{p^d}$ car $\mathbb{U}_{p^d}$ est un sous-groupe.

Contradiction ! car $e^{\frac{2i\pi}{p^{d+1}}} \in P$ et $e^{\frac{2i\pi}{p^{d+1}}} \notin \mathbb{U}_{p^d}$. Il en résulte que P n'est pas de type fini.

- (d) Soit $z \in P$ avec $z \neq 1$. Comme $P = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_{p^n}$ et $z \notin \mathbb{U}_{p^0} = \{1\}$, l'ensemble $\{n \in \mathbb{N}^* \mid z \in \mathbb{U}_{p^n}\}$ est une partie non vide de $\mathbb{N}^*$, donc elle possède un plus petit élément $n_z \in \mathbb{N}^*$. Par définition de n_z , n_z est unique et $z \in \mathbb{U}_{p^{n_z}} \setminus \mathbb{U}_{p^{n_z-1}}$. Montrons que z est un générateur de $\mathbb{U}_{p^{n_z}}$. On utilise la question 3a. Comme p est premier, les diviseurs entiers positifs de p^{n_z} qui lui sont strictement inférieurs sont $1, p, \dots, p^{n_z-1}$. Or, comme, pour tous $i, j \in \mathbb{N}$ avec $i \leq j$, $p^i | p^j$, on a $\mathbb{U}_1, \dots, \mathbb{U}_{p^{n_z-1}} \subset \mathbb{U}_{p^{n_z-1}}$. Ainsi, comme $z \notin \mathbb{U}_{p^{n_z-1}}$, on a $z \notin \mathbb{U}_d$ pour tout diviseur d strictement positif et strictement inférieur à p^{n_z} de p^{n_z} . Ainsi, comme $z \in \mathbb{U}_{p^{n_z}}$, d'après la question 3a, z est un générateur de $\mathbb{U}_{p^{n_z}}$.

- (e) Le groupe P n'est pas de type fini donc il n'est pas monogène. Pour confirmer que P est bien un contre-exemple pour l'implication I , montrons que tous ses sous-groupes propres sont monogènes (et même mieux : qu'ils sont cycliques!).

Soit H un sous-groupe propre de P . Alors il existe $z \in P \setminus H$. Comme H est un sous-groupe de P , il contient l'élément neutre 1 donc $z \neq 1$. Ainsi, d'après la question précédente, il existe un unique $n_z \in \mathbb{N}^*$ tel que $\mathbb{U}_{p^{n_z}} \setminus \mathbb{U}_{p^{n_z-1}}$.

Montrons que $H \subset \mathbb{U}_{p^{n_z-1}}$. Supposons par l'absurde qu'il existe $h \in H$ tel $h \notin \mathbb{U}_{p^{n_z-1}}$. Alors $h \neq 1$ donc, d'après la question précédente, il existe $n_h \in \mathbb{N}^*$ tel que $\mathbb{U}_{p^{n_h}} \setminus \mathbb{U}_{p^{n_h-1}}$ et h engendre $\mathbb{U}_{p^{n_h}}$. De plus, comme $h \notin \mathbb{U}_{p^{n_z-1}}$, par inclusion des $\mathbb{U}_{p^k}$ pour k allant de 0 à $n_z - 1$, on a $n_h \geq n_z$.

Ainsi, on a $p^{n_z} | p^{n_h}$ donc $z \in \mathbb{U}_{p^{n_z}} \subset \mathbb{U}_{p^{n_h}} = \langle h \rangle \subset H$ car H est un sous-groupe. Contradiction!

Par suite, $H \subset \mathbb{U}_{p^{n_z}}$.

Or, $\mathbb{U}_{p^{n_z}}$ est monogène et, d'après la question 2, tous les sous-groupes d'un groupe monogène sont monogènes, donc H est monogène comme sous-groupe de $\mathbb{U}_{p^{n_z}}$ (et même cyclique car $\mathbb{U}_{p^{n_z}}$ est de cardinal fini).

Ainsi, tous les sous-groupes propres de P sont monogènes et P ne l'est pas. Il en résulte que P est bien un contre-exemple pour l'implication I .

Problème 1. Groupes d'ordre pq

Classification des groupes d'ordre pq avec p, q premiers

Dans ce problème, nous allons étudier les groupes de cardinal pq avec p, q des nombres premiers. Notre but, est de montrer l'existence d'éléments d'ordre p et q dans de tels groupes (Parties 1., 2. et 7) et de classer ces groupes à isomorphisme près (Parties 3. à 6.).

Dans toute la suite, $(G, \cdot)$ désigne un groupe et on notera e son élément neutre.

De plus, pour $A \subset G$, on note $\langle A \rangle$ le sous-groupe de G engendré par A et, par souci de simplicité, pour $x, y \in G$, on notera $\langle x \rangle = \langle \{x\} \rangle$ et $\langle x, y \rangle = \langle \{x, y\} \rangle$.

On prendra bien soin de tenir compte des hypothèses à chaque début de partie et sous-partie !

1. Ordre des éléments d'un groupe cyclique

Dans cette partie seulement, on suppose que G est fini de cardinal $n \in \mathbb{N}^*$ et qu'il existe $x \in G$ tel que $o(x) = n$.

1. Par le cours, justifier que G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.
2. Montrer que, pour tout $d \in \mathbb{N}^*$ avec d divise n , il existe $y \in G$ tel que $o(y) = d$.

2. Éléments d'ordre p et q dans un groupe d'ordre pq non monogène

A. Une relation d'équivalence sur G

On considère, sur G , la relation binaire $\sim$ définie, pour $x, y \in G$, par :

$$x \sim y \text{ si, et seulement si, } \langle x \rangle = \langle y \rangle.$$

3. Montrer que $\sim$ est une relation d'équivalence sur G .
4. Pour $x \in G$ d'ordre fini égal à $n \in \mathbb{N}^*$, déterminer la classe d'équivalence Cl_x de x pour la relation $\sim$ et le nombre d'éléments dans cette classe.

B. Groupes d'ordre pq non monogène avec $p < q$

Soit p, q des nombres premiers avec $p < q$. On suppose que G est de cardinal pq et que G n'est pas monogène.

- On note k le nombre de classes d'équivalence différentes définies par des éléments d'ordre p dans G pour la relation $\sim$ et,
- on note l le nombre de classes d'équivalence différentes définies par des éléments d'ordre q dans G pour la relation $\sim$.

5. Montrer que :

$$pq - 1 = k(p - 1) + l(q - 1).$$

6. Effectuer la division euclidienne de $pq - 1$ par $q - 1$ et en déduire que $l \leq p$ puis que $k \geq 1$.

7. Montrer que si $p - 1$ ne divise pas $q - 1$, alors $l \geq 1$.

On admet, dans la suite du problème, que, dans tous les cas, $l \geq 1$. On montrera ce résultat dans la dernière partie (Partie 7).

C. Conclusion

Soit p, q des nombres premiers. *Attention ! on ne suppose plus $p < q$!*

8. Montrer que si G est non monogène de cardinal pq avec p, q premiers, il existe $x, y \in G$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$ tel que $o(x) = q$ et $o(y) = p$.

On traitera séparément les cas $p \neq q$ et $p = q$.

3. Construction d'une bijection entre un groupe de cardinal pq et $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Soit $p, q \in \mathbb{N}^*$ et $x, y \in G$ des éléments d'ordres finis respectivement q et p .

On suppose que $\langle x \rangle \cap \langle y \rangle = \{e\}$.

9. Montrer que, pour tous $a, b, c, d \in \mathbb{Z}$:

$$x^a y^b = x^c y^d \text{ si, et seulement si, } a \equiv c [q] \text{ et } b \equiv d [p].$$

10. En déduire que l'application $\varphi_{(x,y)} : \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rightarrow G$, définie, pour $(\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, par :

$$\varphi_{(x,y)}(\bar{a}, \bar{b}) = x^a y^b$$

est bien définie et injective.

11. On suppose que G est de cardinal pq . Justifier que l'application $\varphi_{(x,y)}$ est une bijection de $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sur G et montrer que $G = \langle x, y \rangle = \{x^a y^b \mid (\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\}$.

4. Stabilité par conjugaison

A. Conjugaison et sous-groupe engendré

12. Soit $x \in G$.

(a) Soit $(H, \cdot)$ un groupe et $f : G \rightarrow H$ un morphisme de groupes. Montrer que $f(\langle x \rangle) = \langle f(x) \rangle$.

(b) En déduire que, pour tout $y \in G$,

$$y^{-1} \langle x \rangle y = \langle y^{-1} x y \rangle.$$

Les hypothèses suivantes sont valables pour les deux sous-parties ci-après (B. Cas $p < q$ et C. Cas $p = q$).

Soit p et q des nombres premiers. On suppose que G est d'ordre pq et que G n'est pas monogène.

B. Cas $p < q$

On suppose $p < q$. On reprend les notations de la partie 2. On rappelle qu'on a admis $l \geq 1$.

13. En utilisant la bijection construite dans la question précédente, montrer par l'absurde que $l = 1$; puis que $k = q$.

14. Soit $x \in G$ tel que $o(x) = q$. Montrer que, pour tout $y \in G$:

$$y^{-b}\langle x \rangle y^b = \langle x \rangle.$$

C. Cas $p = q$

On suppose $p = q$.

15. Soit $x \in G \setminus \{e\}$. Montrer par l'absurde que, pour tout $y \in G \setminus \{e\}$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$, $y^{-1}xy \in \langle x \rangle$.

16. En déduire que, pour tous $x, y \in G \setminus \{e\}$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$, et, pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$:

$$y^{-b}\langle x \rangle y^b = \langle x \rangle.$$

5. Produit semi-direct : loi de composition interne sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Soit p, q des nombres premiers.

A. Morphismes de $\mathbb{Z}/p\mathbb{Z}$ dans un groupe

Soit $(H, \cdot)$ un groupe d'élément neutre e_H et $f : \mathbb{Z}/p\mathbb{Z} \rightarrow H$ un morphisme de groupes.

17. Montrer qu'il existe $h \in H$ tel que, pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, $f(\bar{b}) = h^b$ et de plus, $h = e_H$ ou h est d'ordre fini égal à p .

18. (a) Montrer que f n'est pas injectif si, et seulement si, f est constant en l'identité.

(b) On suppose que H est fini et non réduit à $\{e_H\}$. Montrer que si f est injectif alors p divise $\text{Card}(H)$.

B. Caractérisation de $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ et action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$

On rappelle que $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ désigne le groupe des automorphismes de $(\mathbb{Z}/q\mathbb{Z}, +)$.

On appelle **action par automorphismes** de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$, tout morphisme de groupes de $\mathbb{Z}/p\mathbb{Z}$ dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$. Pour plus de simplicité, dans toute la suite, on emploiera (abusivement) le terme **action** pour "action par automorphismes".

19. (a) Montrer que, pour tout $\bar{a} \in (\mathbb{Z}/q\mathbb{Z})^\times$, l'application $f_{\bar{a}} : \bar{i} \mapsto \bar{a}.\bar{i}$ appartient à $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

(b) Montrer que les groupes $(\text{Aut}(\mathbb{Z}/q\mathbb{Z}), \circ)$ et $((\mathbb{Z}/q\mathbb{Z})^\times, \times)$ sont isomorphes.

20. En déduire que, pour $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$, si α est injective, alors p divise $q - 1$.

21. On suppose $p = q$. Soit $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ une action de $\mathbb{Z}/p\mathbb{Z}$ sur lui-même. Montrer que α est constante en l'identité.

C. Loi sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ via une action par automorphismes

Étant donné une action α de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$ (i.e. $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ un morphisme de groupes), on définit sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, la loi de composition interne notée $*_\alpha$, de la façon suivante : pour $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$,

$$(\bar{a}, \bar{b}) *_\alpha (\bar{c}, \bar{d}) = (\bar{a} + \alpha(\bar{b})(\bar{c}), \bar{b} + \bar{d}).$$

22. Montrer que $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ est un groupe.

Ce groupe est communément appelé "produit semi-direct de $\mathbb{Z}/q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ suivant α ".

23. Montrer que $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ est commutatif si, et seulement si, α n'est pas injectif.

Quelle structure de groupe connue retrouve-t-on pour $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ si α n'est pas injectif?

6. Classification des groupes d'ordre pq

Soit p, q des nombres premiers avec $p \leq q$ et on suppose que G est de cardinal pq .

A. Un isomorphisme entre G et un produit semi-direct dans le cas non monogène

On suppose que G n'est pas monogène.

En vertu des parties 3. et 4., il existe $x, y \in G$ (fixés pour la suite de cette sous-partie) tels que $o(x) = q$, $o(y) = p$ et $\langle x \rangle \cap \langle y \rangle = \{e\}$; ce qui implique les propriétés suivantes :

- i) l'application $\varphi_{(x,y)} : (\bar{a}, \bar{b}) \mapsto x^a y^b$ est une bijection de $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sur G ;
- ii) pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$:

$$y^{-b} \langle x \rangle y^b = \langle x \rangle.$$

24. Montrer que, pour tout $(\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, il existe un unique $\overline{\pi_{(\bar{a}, \bar{b})}} \in \mathbb{Z}/q\mathbb{Z}$ tel que :

$$y^{-b} x^a y^b = x^{\overline{\pi_{(\bar{a}, \bar{b})}}}$$

Dans la toute la suite, on considère, pour $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, l'application $\alpha_{\bar{b}} : \mathbb{Z}/q\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ définie par :

$$\alpha_{\bar{b}} : \bar{a} \mapsto \overline{\pi_{(\bar{a}, \bar{b})}}$$

et l'application α de $\mathbb{Z}/p\mathbb{Z}$ dans l'ensemble des fonctions de $\mathbb{Z}/q\mathbb{Z}$ dans lui-même :

$$\alpha : \bar{b} \mapsto \alpha_{\bar{b}}.$$

- 25. (a) Montrer que α est à valeurs dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$.
- (b) Montrer que $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$.
- 26. (a) Montrer que G et $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ sont isomorphes.
- (b) En déduire que la paire $\{(\bar{1}, \bar{0}), (\bar{0}, \bar{1})\}$ engendre $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$.
- (c) On rappelle l'hypothèse G non monogène et on suppose de plus que $p < q$.
 - i. Montrer que x et y ne commutent pas.
 - ii. En déduire que p divise $q - 1$.

B. Classification des groupes d'ordre pq avec $p < q$

On suppose $p < q$.

27. Montrer que G est :

- soit, si p ne divise pas $q - 1$, isomorphe à $(\mathbb{Z}/pq\mathbb{Z}, +)$;
- soit, si p divise $q - 1$, isomorphe à $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$.

Indication : attention à bien traiter le cas G monogène !

C. Classification des groupes d'ordre p^2

On suppose $p = q$.

28. Montrer que G est :

- soit isomorphe à $(\mathbb{Z}/p^2\mathbb{Z}, +)$;
 - soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2, +)$;
- et, qu'en particulier, G est commutatif.

7. Théorème de Cauchy

29. Soit q un nombre premier. On suppose que G est de cardinal $n \in \mathbb{N}^*$ et que q divise n .
Le but de cette question est de montrer le *Théorème de Cauchy* i.e. qu'il existe $x \in G$ d'ordre q .

On considère l'ensemble $\mathcal{F}_q(G)$ des fonctions de $\mathbb{Z}/q\mathbb{Z}$ dans G . On pose :

$$E = \{f \in \mathcal{F}_q(G) \mid f(\bar{0})f(\bar{1})\dots f(\overline{q-1}) = e\}.$$

et on note $\mathcal{R}$ la relation binaire sur E définie, pour $f, g \in E$, par :

$$f \mathcal{R} g \text{ si, et seulement si, } \exists \bar{m} \in \mathbb{Z}/q\mathbb{Z}, \forall \bar{k} \in \mathbb{Z}/q\mathbb{Z}, f(\bar{k} + \bar{m}) = g(\bar{k}).$$

- (a) Déterminer le cardinal de E .
- (b) Montrer que $\mathcal{R}$ est une relation d'équivalence sur E .
- (c) On considère l'application S de $\mathcal{F}_b(G)$ dans lui-même définie, pour $f \in \mathcal{F}_b(G)$, par $S(f) : \bar{k} \mapsto f(\bar{k} + \bar{1})$.
Montrer les résultats suivants : $S^q = \text{Id}$, $S(E) \subset E$, et, pour tout $f \in E$, $S(f) \mathcal{R} f$.
En déduire que, pour $f \in E$, la classe d'équivalence C_f de f pour $\mathcal{R}$ vérifie :

$$C_f = \{S^m(f) \mid m \in \llbracket 0, q-1 \rrbracket\}.$$

- (d) Soit $f \in E$. Montrer que le cardinal de la classe d'équivalence C_f de f pour $\mathcal{R}$ est égal à 1 ou q et que, de plus, si $\text{Card}(C_f) = 1$, alors f est constante.
- (e) En déduire qu'il existe $x \in G$ d'ordre q .

30. En déduire que, dans la partie 2., on a bien $l \geq 1$.

Correction.

1. Ordre des éléments d'un groupe cyclique

Dans cette partie seulement, on suppose que G est fini de cardinal $n \in \mathbb{N}^*$ et qu'il existe $x \in G$ tel que $o(x) = n$.

- 1. Comme $o(x) = n = \text{Card}(G)$, on a $\langle x \rangle = G$, donc G est un groupe cyclique de cardinal

n et ainsi, d'après le théorème de classification des groupes monogènes, G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

2. Soit $d \in \mathbb{N}^*$ avec d divise n . Alors il existe $k \in \mathbb{N}^*$ tel que $n = dk$ et on pose $y = x^k \in G$. On a alors, pour tout $m \in \mathbb{Z}$:

$$y^m = e \Leftrightarrow x^{km} = (x^k)^m = e,$$

d'où, comme $o(x) = n$, $dk = n \mid km$ et donc $d \mid m$ i.e. $m \in d\mathbb{Z}$.

Par suite, $o(y) \mid d$ et comme d est le plus petit entier naturel non nul de $d\mathbb{Z}$, $o(y) = d$.

2. Éléments d'ordre p et q dans un groupe d'ordre pq

A. Une relation d'équivalence sur G

3. Montrons que $\sim$ est une relation d'équivalence sur G . Soit $x, y, z \in G$.
- *Reflexivité.* On a, par réflexivité de l'égalité, $\langle x \rangle = \langle x \rangle$ donc $x \sim x$.
 - *Symétrie.* On suppose $x \sim y$. Alors $\langle x \rangle = \langle y \rangle$; d'où, par symétrie de l'égalité, $\langle y \rangle = \langle x \rangle$ et donc $y \sim x$.
 - *Transitivité.* On suppose $x \sim y$ et $y \sim z$. Alors $\langle x \rangle = \langle y \rangle$ et $\langle y \rangle = \langle z \rangle$; d'où, par transitivité de l'égalité, $\langle x \rangle = \langle z \rangle$ et donc $x \sim z$.

Il en résulte que $\sim$ est une relation d'équivalence sur G .

4. Soit $x \in G$ un élément d'ordre fini égal à $n \in \mathbb{N}^*$. On note $H = \langle x \rangle$ qui est donc un groupe cyclique de cardinal n : ainsi, d'après le théorème de classification des groupe monogène, il est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$ et l'application $f : \bar{k} \mapsto x^k$ est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ sur H . On a $y \sim x$ si, et seulement si, $\langle y \rangle = H$ i.e. y engendre H ; or, y engendre H si, et seulement si, $f^{-1}(y)$ engendre $\mathbb{Z}/n\mathbb{Z}$ car f^{-1} est un isomorphisme, et il y a exactement $\varphi(n)$ générateurs de $\mathbb{Z}/n\mathbb{Z}$ où φ est l'indicatrice d'Euler : il s'agit des $\bar{k}$ tels que $k \in \llbracket 0, n \rrbracket$ et k, n premiers entre eux.

Par suite, il y a $\varphi(n)$ éléments dans la classe d'équivalence de x pour la relation $\sim$ et :

$$\text{Cl}_x = f(\{\bar{k} \mid k \in \llbracket 0, n \rrbracket \text{ et } k \wedge n = 1\}) = \{x^k \mid k \in \llbracket 0, n \rrbracket \text{ et } k \wedge n = 1\}.$$

B. Groupes d'ordre pq non monogène avec $p < q$

Soit p, q des nombres premiers avec $p < q$. On suppose que G est de cardinal pq et que G n'est pas monogène.

5. Pour tout $x \in G$, on a $o(x)$ divise pq donc, comme p, q sont premiers $o(x) = 1, p, q$ ou pq ; or, comme G n'est pas monogène, $o(x) \neq pq$.

Ainsi, on a trois cas possibles pour $x \in G$:

- $o(x) = 1$: ceci équivaut à $x = e$ et on a alors $\text{Cl}_x = \{e\}$ qui possède 1 élément;
- $o(x) = p$: dans ce cas, on a $\text{Cl}_x = \langle x \rangle \setminus \{e\}$ qui possède $p - 1$ éléments. En effet, comme p est premier, d'après la question 4 :

$$\text{Cl}_x = \{x^k \mid k \in \llbracket 0, p \rrbracket \text{ et } k \wedge p = 1\} = \{x^k \mid k \in \llbracket 1, p - 1 \rrbracket\} = \langle x \rangle \setminus \{e\}.$$

Le nombre k de classes différentes définies par les éléments d'ordre p est bien fini car G est fini;

- $o(x) = q$: de même que dans le cas précédent, on a $\text{Cl}_x = \langle x \rangle \setminus \{e\}$ qui possède $q - 1$ éléments.

Le nombre l de classes différentes définies par les éléments d'ordre q est bien fini car G est fini.

Comme les classes d'équivalence d'une relation d'équivalence sur un ensemble forment une partition de cet ensemble, on a, en notant $P_1, \dots, P_k$ les classes différentes des éléments d'ordre p (toutes de cardinal $p - 1$) et $Q_1, \dots, Q_l$ celles des éléments d'ordre q (toutes de cardinal $q - 1$) :

$$G = \text{Cl}_e \sqcup \bigsqcup_{i=1}^k P_i \sqcup \bigsqcup_{i=1}^l Q_i$$

d'où, en passant aux cardinaux :

$$pq = 1 + k(p - 1) + l(q - 1).$$

D'où le résultat.

6. On a $pq - 1 = p(q - 1) + (p - 1)$ avec $0 \leq p - 1 < q - 1$ car $1 \leq p < q$ donc il s'agit bien de la division euclidienne de $pq - 1$ par $q - 1$. Ainsi, comme $k(p - 1) \geq 0$, on a $l \leq p$ et $k(p - 1) \geq p - 1$ par maximalité du quotient de la division euclidienne. Comme $p - 1 > 0$ car $p \geq 2$, on obtient $k \geq 1$.

7. Montrons le résultat par contraposée : on suppose que $l = 0$.

Alors on a :

$$q(p - 1) = pq - 1 = k(p - 1)$$

d'où $q - 1 = (q + k)(p - 1)$ et donc $p - 1$ divise $q - 1$.

Il en résulte, par contraposée, que si $p - 1$ ne divise pas $q - 1$, alors $l \geq 1$.

C. Conclusion

8. Soit G est de cardinal pq avec p, q premiers. Quitte à échanger p et q , on suppose $p \leq q$.

- *1er cas* : $p < q$. D'après les résultats et le fait admis de la partie B., on a $k, l \geq 1$. Ainsi, il existe au moins une classe d'équivalence définie par un élément d'ordre p , disons x et au moins une classe d'équivalence définie par un élément d'ordre q , disons y . Comme x et y n'ont pas le même ordre, les classes $\text{Cl}_x = \langle x \rangle \setminus \{e\}$ de x et $\text{Cl}_y = \langle y \rangle \setminus \{e\}$ de y sont différentes et donc disjointes. Par suite,

$$\langle x \rangle \cap \langle y \rangle = \{e\}.$$

- *2nd cas* : $p = q$. Alors G est d'ordre p^2 et non monogène donc tout élément est d'ordre soit 1, soit p . Par un raisonnement similaire à la question 5, on obtient, pour c le nombre de classes d'équivalence différentes de celle de e (et donc toutes définies par des éléments d'ordre p) :

$$p^2 = c(p - 1) + 1$$

et donc $c = p + 1 \geq 2$. Ainsi, il existe au moins deux classes disjointes définies par des éléments d'ordre p disons x et y , d'où :

$$\langle x \rangle \cap \langle y \rangle = \{e\}.$$

3. Construction d'une bijection entre un groupe de cardinal pq et $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Soit $p, q \in \mathbb{N}^*$ et $x, y \in G$ des éléments d'ordres finis respectivement q et p .

On suppose que $\langle x \rangle \cap \langle y \rangle = \{e\}$.

9. Soit $a, b, c, d \in \mathbb{Z}$. Alors

$$x^a y^b = x^c y^d \text{ si, et seulement si, } x^{a-b} = y^{d-b}$$

Ainsi, x^{a-b} et y^{d-b} appartiennent à $\langle x \rangle \cap \langle y \rangle = \{e\}$ et donc sont égaux à e .

Par suite, $q = o(x)|a-b$ et $p = o(y)|d-b$ ce qui équivaut à $a \equiv c [q]$ et $b \equiv d [p]$.

Réciproquement, si $a \equiv c [q]$ et $b \equiv d [p]$ alors $x^{a-b} = e = y^{d-b}$ d'où $x^a y^b = x^c y^d$.

10. Montrons que $\varphi_{(x,y)}$ est bien définie. Soit $a, b, c, d \in \mathbb{Z}$ tels que $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$ (dans $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$) i.e. $a \equiv c [q]$ et $b \equiv d [p]$. Alors on a, d'après la question précédente :

$$\varphi_{(x,y)}(\bar{a}, \bar{b}) = x^a y^b = x^c y^d = \varphi_{(x,y)}(\bar{c}, \bar{d})$$

Donc $\varphi_{(x,y)}$ est bien définie.

De plus, pour tous $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ tels que $\varphi_{(x,y)}(\bar{a}, \bar{b}) = \varphi_{(x,y)}(\bar{c}, \bar{d})$, on a $x^a y^b = x^c y^d$; d'où, toujours d'après la question précédente, $a \equiv c [q]$ et $b \equiv d [p]$ et donc $(\bar{a}, \bar{b}) = (\bar{c}, \bar{d})$.

Par suite, $\varphi_{(x,y)}$ est injective.

11. On suppose que G est de cardinal pq . D'après la question précédente, $\varphi_{(x,y)}$ est injective, donc :

$$\text{Card}(\varphi_{(x,y)}(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})) = \text{Card}(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) = pq = \text{Card}(G).$$

Or, $\varphi_{(x,y)}(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \subset G$ d'où $\text{Im}(\varphi_{(x,y)}) = G$ et ainsi $\varphi_{(x,y)}$ est surjective et donc bijective.

De plus,

$$G = \text{Im}(\varphi_{(x,y)}) = \{x^a y^b \mid (\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\} \subset \langle x, y \rangle \subset G,$$

par suite, $G = \langle x, y \rangle = \{x^a y^b \mid (\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\}$.

4. Stabilité par conjugaison

A. Conjugaison et sous-groupe engendré

12. Soit $x \in G$.

(a) Soit $(H, \cdot)$ un groupe et $f : G \rightarrow H$ un morphisme de groupes.

Comme f est un morphisme de groupes, pour tout $n \in \mathbb{N}$, on a $f(x^n) = f(x)^n$. Par suite :

$$f(\langle x \rangle) = \{f(x^n) \mid n \in \mathbb{N}\} = \{f(x)^n \mid n \in \mathbb{N}\} = \langle f(x) \rangle.$$

(b) Soit $y \in G$. L'application $f : g \mapsto y^{-1}gy$ est un morphisme de groupes de G dans lui-même : en effet, pour tous $g, h \in G$, on a,

$$f(g) \cdot f(h) = (y^{-1}gy)(y^{-1}hy) = y^{-1}g(yy^{-1})hy = y^{-1}(gh)y = f(gh).$$

Par suite, d'après la question précédente, on a :

$$y^{-1}\langle x \rangle y = f(\langle x \rangle) = \langle f(x) \rangle = \langle y^{-1}xy \rangle.$$

Les hypothèses suivantes sont valables pour les deux sous-parties ci-après (B. Cas $p < q$ et C. Cas $p = q$).

Soit p et q des nombres premiers. On suppose que G est d'ordre pq et que G n'est pas monogène.

B. Cas $p < q$

On suppose $p < q$. On reprend les notations de la partie 2.

13. Supposons par l'absurde que $l \neq 1$. Alors, comme $l \geq 1$, cela revient à $l \geq 2$. Ainsi, il existe deux classes disjointes définies par des éléments d'ordre q , donc il existe $x, y \in G$ tels que $o(x) = q = o(y)$ et $\langle x \rangle \cap \langle y \rangle = \{e\}$. Par suite, d'après la question 11, $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ qui est de cardinal q^2 est en bijection avec G qui de cardinal $pq < q^2$. Contradiction !

Par suite, $l = 1$. Ainsi, on a :

$$q(p-1) + (p-1) = pq - 1 = k(p-1) + (p-1),$$

d'où $k = q$.

14. Soit $x \in G$ avec $o(x) = q$. Soit $y \in G$ et $b \in \mathbb{Z}$. On pose $z = y^b$. On a :

$$(z^{-1}xz)^q = z^{-1} \underbrace{x^q}_{=e} z = e,$$

donc, comme q est premier, soit $o(z^{-1}xz) = 1$, soit $o(z^{-1}xz) = q$. Or $x \neq e$ donc $z^{-1}xz \neq e$ et ainsi, $o(z^{-1}xz) = q$.

D'après la question précédente, il existe une unique classe d'éléments d'ordre q , donc $z^{-1}xz \sim x$ i.e. $\langle z^{-1}xz \rangle = \langle x \rangle$.

Par suite, d'après la question 12b, on obtient :

$$y^{-b}\langle x \rangle y^b = z^{-1}\langle x \rangle z = \langle z^{-1}xz \rangle = \langle x \rangle.$$

C. Cas $p = q$

On suppose $p = q$.

15. Soit $x \in G \setminus \{e\}$. On suppose par l'absurde qu'il existe $y \in G \setminus \{e\}$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$ tel que $y^{-1}xy \notin \langle x \rangle$. Posons $z = y^{-1}xy$. Alors $z \neq e$ car $e \in \langle x \rangle$ donc z est d'ordre p dans G car G n'est pas monogène et, de plus, $\langle z \rangle \neq \langle x \rangle$ car $z \notin \langle x \rangle$. Ainsi, x et z appartiennent à deux classes d'équivalences (pour $\sim$) différentes donc disjointes, d'où $\langle x \rangle \cap \langle z \rangle = \{e\}$.

Par suite, d'après la question 11, $G = \langle x, z \rangle = \{x^a z^b \mid (\bar{a}, \bar{b}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}\}$.

Ainsi, comme $y \in G$, il existe $a, b \in \mathbb{Z}$ tels que :

$$x^a y^{-1} x^b y = x^a z^b = y.$$

D'où, en composant à gauche par x^{-a} et à droite par $y^{-1}x^{-b}$, on obtient :

$$y^{-1} = x^{-a-b}.$$

Ainsi, $y = x^{a+b} \in \langle x \rangle \cap \langle y \rangle = \{e\}$. Contradiction car $y \neq e$.

Par suite, pour tout $y \in G \setminus \{e\}$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$, $y^{-1}xy \in \langle x \rangle$.

16. Soit $x, y \in G \setminus \{e\}$ avec $\langle x \rangle \cap \langle y \rangle = \{e\}$. L'égalité est triviale si $\bar{b} = \bar{0}$.

Pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, $y^b \neq e$ et $\langle y^b \rangle \cap \langle x \rangle = \{e\}$ car $\langle y^b \rangle = \langle y \rangle$ donc, d'après la question 12b et la question précédente :

$$y^{-b}\langle x \rangle y^b = \langle y^{-b}xy^b \rangle \subset \langle x \rangle,$$

et il y a égalité car $y^{-b}xy^b$ et x sont d'ordre p tous les deux.

5. Produit semi-direct : loi de composition interne sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Soit p, q des nombres premiers.

A. Morphismes de $\mathbb{Z}/p\mathbb{Z}$ dans un groupe

Soit $(H, \cdot)$ un groupe d'élément neutre e_H et $f : \mathbb{Z}/p\mathbb{Z} \rightarrow H$ un morphisme de groupes.

17. On pose $h = f(\bar{1}) \in H$. Pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$, on a, f étant un morphisme de groupes :

$$f(\bar{b}) = f(b\bar{1}) = f(\bar{1})^b = h^b.$$

De plus, on a $h^p = f(\bar{p}) = f(\bar{0}) = e_H$ donc h est d'ordre fini et $o(h) \mid p$ d'où $o(h) = 1$ i.e. $h = e_H$ ou $o(h) = p$.

18. (a) Montrons l'implication réciproque. Comme $\mathbb{Z}/p\mathbb{Z}$ possède au moins deux éléments ($p \geq 2$ car p premier), e_H admet au moins deux antécédents par f et donc f n'est pas injective.

D'après la question précédente, il existe $h \in H$ tel que $f : \bar{b} \mapsto h^b$. Supposons f non injectif. Alors il existe $\bar{a} \in H \setminus \{\bar{0}\}$ tel que $f(\bar{a}) = e_H$. Or, comme p est premier et $\bar{a} \neq \bar{0}$, $\bar{a}$ engendre $\mathbb{Z}/p\mathbb{Z}$; ainsi, il existe $n \in \mathbb{Z}$ tel que $\bar{1} = n\bar{a}$ d'où :

$$h = f(\bar{1}) = f(\bar{a})^n = e_H^n = e_H.$$

Donc $f : \bar{b} \mapsto h^b = e_H^b = e_H$ est constante en e_H .

- (b) On suppose que H est fini non réduit à $\{e_H\}$. D'après la question 17, il existe $h \in H$ tel que $f : \bar{b} \mapsto h^b$ avec $h = e_H$ ou $o(h) \mid p$.

Si f est injectif, H possédant un élément différent de e_H , on a alors $h = f(\bar{1}) \neq e_H$ donc $o(h) = p$.

Or, l'ordre de tout élément divise le cardinal du groupe, donc p divise $\text{Card}(H)$.

B. Caractérisation de $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ et action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/q\mathbb{Z}$

19. (a) Soit $\bar{a} \in (\mathbb{Z}/q\mathbb{Z})^\times$. Pour tout $\bar{i}, \bar{j} \in \mathbb{Z}/q\mathbb{Z}$, on a, par distributivité dans l'anneaux $\mathbb{Z}/q\mathbb{Z}$:

$$f_{\bar{a}}(\bar{i} + \bar{j}) = \bar{a}(\bar{i} + \bar{j}) = \bar{a}\bar{i} + \bar{a}\bar{j} = f_{\bar{a}}(\bar{i}) + f_{\bar{a}}(\bar{j}).$$

Donc $f_{\bar{a}}$ est un morphisme de groupes de $\mathbb{Z}/q\mathbb{Z}$ dans lui-même.

Comme $\mathbb{Z}/q\mathbb{Z}$ est un groupe fini, il suffit de montrer que $f_{\bar{a}}$ est injective pour montrer que $f_{\bar{a}} \in \text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Soit $\bar{i} \in \mathbb{Z}/q\mathbb{Z}$ tel que $f_{\bar{a}}(\bar{i}) = \bar{0}$. Alors $\bar{a}\bar{i} = \bar{0}$ donc $\bar{i} = \bar{0}$ car $\bar{a}$ est inversible dans l'anneau $\mathbb{Z}/q\mathbb{Z}$.

Par suite, $f_{\bar{a}}$ est injective et donc $f_{\bar{a}} \in \text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

- (b) Montrons que l'application $f : \bar{a} \mapsto f_{\bar{a}}$ est un isomorphisme de $((\mathbb{Z}/q\mathbb{Z})^\times, \times)$ dans $(\text{Aut}(\mathbb{Z}/q\mathbb{Z}), \circ)$.

Soit $\bar{a}, \bar{b} \in (\mathbb{Z}/q\mathbb{Z})^\times$. On a, pour tout $\bar{i} \in \mathbb{Z}/q\mathbb{Z}$, par associativité de $\times$:

$$\begin{aligned} f_{\bar{a}\bar{b}}(\bar{i}) &= (\bar{a}\bar{b})\bar{i} \\ &= \bar{a}(\bar{b}\bar{i}) \\ &= f_{\bar{a}}(f_{\bar{b}}(\bar{i})) \\ f_{\bar{a}\bar{b}}(\bar{i}) &= f_{\bar{a}} \circ f_{\bar{b}}(\bar{i}). \end{aligned}$$

D'où $f(\bar{a}\bar{b}) = f(\bar{a}) \circ f(\bar{b})$.

Par suite, f est un morphisme de groupes.

Montrons que f est bijectif.

— *Injectivité.* Soit $\bar{a} \in (\mathbb{Z}/q\mathbb{Z})^\times$ tel que $f_{\bar{a}} = \text{id}$. Alors, en particulier :

$$\bar{1} = f_{\bar{a}}(\bar{1}) = \bar{a}\bar{1} = \bar{a}.$$

Par suite, $\text{Ker}(f) = \{\bar{1}\}$ et donc f est injective.

— *Surjectivité.* Soit $g \in \text{Aut}(\mathbb{Z}/q\mathbb{Z})$. On pose $\bar{a} = g(\bar{1}) \in \mathbb{Z}/q\mathbb{Z}$. L'application g étant un isomorphisme de groupes, on a $\bar{a} = g(\bar{1}) \neq \bar{0}$ car $\bar{1} \neq \bar{0}$ d'où $\bar{a} \in (\mathbb{Z}/q\mathbb{Z})^\times$ car q est premier.

Remarque. On a été un peu fainéant ici : si q n'avait pas été premier, on aurait dû conclure en utilisant le fait que $\bar{1}$ est un générateur de $(\mathbb{Z}/q\mathbb{Z}, +)$ et donc que $\bar{a}$ aussi car g est un isomorphisme de groupes ; et tout générateur de $(\mathbb{Z}/q\mathbb{Z}, +)$ est également inversible dans l'anneau $\mathbb{Z}/q\mathbb{Z}$!

De plus, pour tout $\bar{i} \in \mathbb{Z}/q\mathbb{Z}$, on a, g étant un morphisme de groupes :

$$\begin{aligned} f_{\bar{a}}(\bar{i}) &= \bar{a}.\bar{i} \\ &= \overline{a.i} \\ &= \overline{i.a} \\ &= i.\bar{a} \\ &= i.g(\bar{1}) \\ &= g(i.\bar{1}) \\ f_{\bar{a}}(\bar{i}) &= g(\bar{i}). \end{aligned}$$

Par suite, $g = f(\bar{a})$ avec $\bar{a} \in (\mathbb{Z}/q\mathbb{Z})^\times$.

Ainsi f est surjective.

Il en résulte que f est un isomorphisme de $(\mathbb{Z}/q\mathbb{Z})^\times$ et $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Remarque. Pour la bijectivité, on aurait également pu exhiber la fonction réciproque de f , en l'occurrence l'application $G : g \mapsto g(\bar{1})$ définie sur $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ - mais les calculs et arguments de preuve sont essentiellement les mêmes que précédemment.

Ainsi, $(\mathbb{Z}/q\mathbb{Z})^\times$ et $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ sont isomorphes.

20. Soit $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme de groupes. On suppose α injectif.

Le groupe $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est fini de cardinal $q - 1 > 0$ car, d'après la question précédente, il est isomorphe au groupe $(\mathbb{Z}/q\mathbb{Z})^\times$ - qui est bien de cardinal $q - 1$ car q est premier.

D'après la question 18b, on a alors :

$$p \mid \text{Card}(\text{Aut}(\mathbb{Z}/q\mathbb{Z})) = q - 1.$$

21. On suppose $p = q$. Soit $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ un morphisme de groupes.

Comme $0 < p - 1 < p$, on a p ne divise pas $p - 1 = q - 1$. Par contraposée de la question précédente, le morphisme α n'est pas injectif et donc, d'après la question 18a, α est constant en l'identité.

C. Loi sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ via une action par automorphismes

22. — Par définition, $*_{\alpha}$ est une loi de composition interne sur $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

— Montrons l'associativité : pour $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}), (\bar{e}, \bar{f}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, on a, par associativité de $+$ dans $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$ et du fait que α est un morphisme à valeurs dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$:

$$\begin{aligned} ((\bar{a}, \bar{b}) *_{\alpha} (\bar{c}, \bar{d})) *_{\alpha} (\bar{e}, \bar{f}) &= (\bar{a} + \alpha(\bar{b})(\bar{c}), \bar{b} + \bar{d}) *_{\alpha} (\bar{e}, \bar{f}) \\ &= (\bar{a} + \alpha(\bar{b})(\bar{c}) + \alpha(\bar{b} + \bar{d})(\bar{e}), (\bar{b} + \bar{d}) + \bar{f}) \\ &= (\bar{a} + \alpha(\bar{b})(\bar{c}) + \alpha(\bar{b}) \circ \alpha(\bar{d})(\bar{e}), \bar{b} + \bar{d} + \bar{f}) \\ &= (\bar{a} + \alpha(\bar{b})(\bar{c} + \alpha(\bar{d})(\bar{e})), \bar{b} + (\bar{d} + \bar{f})) \\ &= (\bar{a}, \bar{b}) *_{\alpha} (\bar{c} + \alpha(\bar{d})(\bar{e}), \bar{d} + \bar{f}) \\ ((\bar{a}, \bar{b}) *_{\alpha} (\bar{c}, \bar{d})) *_{\alpha} (\bar{e}, \bar{f}) &= (\bar{a}, \bar{b}) *_{\alpha} ((\bar{c}, \bar{d}) *_{\alpha} (\bar{e}, \bar{f})) \end{aligned}$$

Donc $*_{\alpha}$ est un loi de composition interne associative.

— Montrons que $(\bar{0}, \bar{0})$ est un élément neutre pour la loi $*_{\alpha}$: pour $(\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, on a, comme α est un morphisme à valeurs dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$:

$$(\bar{a}, \bar{b}) *_{\alpha} (\bar{0}, \bar{0}) = (\bar{a} + \underbrace{\alpha(\bar{b})(\bar{0})}_{=\bar{0}}, \bar{b} + \bar{0}) = (\bar{a}, \bar{b}),$$

et

$$(\bar{0}, \bar{0}) *_{\alpha} (\bar{a}, \bar{b}) = (\bar{0} + \underbrace{\alpha(\bar{0})(\bar{a})}_{=\text{id}}, \bar{0} + \bar{b}) = (\bar{a}, \bar{b}).$$

Donc $(\bar{0}, \bar{0})$ est un élément neutre pour le loi $*_{\alpha}$.

— Montrons que tout élément admet un symétrique pour $*_{\alpha}$: pour $(\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, on a $(\alpha(\bar{b})(\bar{a}), \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et comme α est un morphisme à valeurs dans $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$:

$$\begin{aligned} (\bar{a}, \bar{b}) *_{\alpha} (\alpha(\bar{b})(\bar{a}), \bar{b}) &= (\bar{a} + \alpha(\bar{b})(\alpha(\bar{b})(\bar{a})), \bar{b} + \bar{b}) \\ &= (\bar{a} + \alpha(\bar{b}) \circ \alpha(\bar{b})(\bar{a}), \bar{b} + \bar{b}) \\ &= (\bar{a} + \alpha(\bar{b} + \bar{b})(\bar{a}), \bar{b} + \bar{b}) \\ &= (\bar{a} + \underbrace{\alpha(\bar{0})(\bar{a})}_{=\text{id}}, \bar{b} + \bar{b}) \\ &= (\bar{a} + \bar{a}, \bar{b} + \bar{b}) \\ (\bar{a}, \bar{b}) *_{\alpha} (\alpha(\bar{b})(\bar{a}), \bar{b}) &= (\bar{0}, \bar{0}), \end{aligned}$$

et

$$\begin{aligned} (\alpha(\bar{b})(\bar{a}), \bar{b}) *_{\alpha} (\bar{a}, \bar{b}) &= (\alpha(\bar{b})(\bar{a}) + \alpha(\bar{b})(\bar{a}), \bar{b} + \bar{b}) \\ &= (\alpha(\bar{b})(\bar{a} + \bar{a}), \bar{b} + \bar{b}) \\ &= (\alpha(\bar{b})(\bar{0}), \bar{b} + \bar{b}) \\ (\alpha(\bar{b})(\bar{a}), \bar{b}) *_{\alpha} (\bar{a}, \bar{b}) &= (\bar{0}, \bar{0}). \end{aligned}$$

Donc tout élément admet un symétrique pour $*_{\alpha}$.

Il en résulte que $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ est un groupe.

23. — ($\Rightarrow$) Par contraposée. On suppose α injectif. Alors, comme $\bar{1} \neq \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}$, $\alpha(\bar{1}) \neq \text{id}$ donc il existe $\bar{a} \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$ tel que $\alpha(\bar{1})(\bar{a}) \neq \bar{a}$. Ainsi, on a :

$$(\bar{0}, \bar{1}) *_{\alpha} (\bar{a}, \bar{0}) = (\alpha(\bar{1})(\bar{a}), \bar{1}) \neq (\bar{a}, \bar{1}) = (\bar{a}, \bar{0}) *_{\alpha} (\bar{0}, \bar{1}).$$

Donc $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ n'est pas commutatif.

- ($\Leftarrow$) On suppose α non injectif. D'après la proposition 18a, α est constant en l'identité, donc, pour tous $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, on a :

$$\begin{aligned} (\bar{a}, \bar{b}) *_{\alpha} (\bar{c}, \bar{d}) &= (\bar{a} + \underbrace{\alpha(\bar{b})(\bar{c})}_{=\text{id}}, \bar{b} + \bar{d}) \\ &= (\bar{a} + \bar{c}, \bar{b} + \bar{d}) \\ &= (\bar{c} + \bar{a}, \bar{d} + \bar{b}) \\ &= (\bar{c} + \underbrace{\alpha(\bar{d})(\bar{a})}_{=\text{id}}, \bar{d} + \bar{b}) \\ (\bar{a}, \bar{b}) *_{\alpha} (\bar{c}, \bar{d}) &= (\bar{c}, \bar{d}) *_{\alpha} (\bar{a}, \bar{b}) \end{aligned}$$

Donc $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ est commutatif.

Lorsque α n'est pas injectif, on remarque alors avec le calcul précédent que $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ est simplement le groupe produit direct $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +)$.

6. Classification des groupes d'ordre pq

Soit p, q des nombres premiers avec $p \leq q$ et on suppose que G est de cardinal pq .

A. Un isomorphisme entre G et un produit semi-direct dans le cas non monogène

On suppose que G n'est pas monogène.

En vertu des parties 3., 4. et 5., il existe $x, y \in G$ (fixés pour la suite de cette sous-partie) tels que $o(x) = q$, $o(y) = p$ et $\langle x \rangle \cap \langle y \rangle = \{e\}$; ce qui implique les propriétés suivantes :

- i) l'application $\varphi_{(x,y)} : (\bar{a}, \bar{b}) \mapsto x^{\bar{a}}y^{\bar{b}}$ est une bijection de $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sur G ;
- ii) pour tout $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$:

$$y^{-\bar{b}}\langle x \rangle y^{\bar{b}} = \langle x \rangle.$$

24. Soit $(\bar{a}, \bar{b}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. D'après la propriété ii), on a :

$$y^{-\bar{b}}x^{\bar{a}}y^{\bar{b}} \in y^{-\bar{b}}\langle x \rangle y^{\bar{b}} = \langle x \rangle,$$

donc il existe un unique $\pi_{(\bar{a}, \bar{b})} \in \llbracket 0, q-1 \rrbracket$ tel que :

$$y^{-\bar{b}}x^{\bar{a}}y^{\bar{b}} = x^{\pi_{(\bar{a}, \bar{b})}}.$$

D'où l'unicité de $\overline{\pi_{(\bar{a}, \bar{b})}} \in \mathbb{Z}/q\mathbb{Z}$.

25. (a) Soit $\bar{b} \in \mathbb{Z}/p\mathbb{Z}$.

— Montrons que $\alpha_{\bar{b}}$ est un morphisme de groupes.

On a, pour tout $\bar{a}, \bar{c} \in \mathbb{Z}/q\mathbb{Z}$:

$$x^{\pi_{(\bar{a}+\bar{c}, \bar{b})}} = y^{-\bar{b}}x^{\bar{a}+\bar{c}}y^{\bar{b}} = (y^{-\bar{b}}x^{\bar{a}}y^{\bar{b}})(y^{-\bar{b}}x^{\bar{c}}y^{\bar{b}}) = x^{\pi_{(\bar{a}, \bar{b})}}x^{\pi_{(\bar{c}, \bar{b})}} = x^{\pi_{(\bar{a}, \bar{b})} + \pi_{(\bar{c}, \bar{b})}},$$

d'où $\pi_{(\bar{a}+\bar{c}, \bar{b})} \equiv \pi_{(\bar{a}, \bar{b})} + \pi_{(\bar{c}, \bar{b})} [q]$ et ainsi :

$$\alpha_{\bar{b}}(\bar{a} + \bar{c}) = \overline{\pi_{(\bar{a}+\bar{c}, \bar{b})}} = \overline{\pi_{(\bar{a}, \bar{b})}} + \overline{\pi_{(\bar{c}, \bar{b})}} = \alpha_{\bar{b}}(\bar{a}) + \alpha_{\bar{b}}(\bar{c}).$$

Par suite, $\alpha_{\bar{b}}$ est un morphisme de groupes.

— Montrons que $\alpha_{\bar{b}}$ est bijective. Pour cela, il suffit de montrer qu'elle est injective car $\mathbb{Z}/q\mathbb{Z}$ est fini.

Soit $\bar{a} \in \mathbb{Z}/q\mathbb{Z}$ tel que $\alpha_{\bar{b}}(\bar{a}) = \bar{0}$. Alors, on a :

$$y^{-b}x^a y^b = x^0 = e$$

donc, en composant à gauche par y^b et à droite par y^{-b} , on obtient $x^a = e$ i.e. $a \equiv 0 [q]$; et donc $\bar{a} = \bar{0}$.

Par suite, $\alpha_{\bar{b}}$ est injective et donc bijective.

Il en résulte que $\alpha_{\bar{b}}$ appartient à $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$.

(b) Soit $\bar{b}, \bar{c} \in \mathbb{Z}/p\mathbb{Z}$.

Montrons que $\alpha_{\bar{b}} \circ \alpha_{\bar{c}} = \alpha_{\bar{b}+\bar{c}}$.

Soit $\bar{a} \in \mathbb{Z}/q\mathbb{Z}$. On pose $\pi_1 = \alpha_{\bar{b}}(\alpha_{\bar{c}}(\bar{a}))$, $\pi_2 = \alpha_{\bar{b}+\bar{c}}(\bar{a})$ et $\pi_3 = \alpha_{\bar{c}}(\bar{a})$. Alors, on a :

$$\begin{aligned} x^{\pi_1} &= y^{-b}x^{\pi_3}y^b \\ &= y^{-b}(y^{-c}x^a y^c)y^b \\ &= y^{-(b+c)}x^a y^{b+c} \\ x^{\pi_1} &= x^{\pi_2} \end{aligned}$$

d'où $\alpha_{\bar{b}} \circ \alpha_{\bar{c}}(\bar{a}) = \overline{\pi_1} = \overline{\pi_2} = \alpha_{\bar{b}+\bar{c}}(\bar{a})$.

Par suite, $\alpha_{\bar{b}} \circ \alpha_{\bar{c}} = \alpha_{\bar{b}+\bar{c}}$.

Il en résulte que $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est un morphisme de groupes.

26. (a) Montrons que l'application $\varphi_{(x,y)}$ est un isomorphisme de groupes de $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ dans $(G, \cdot)$. Comme $\varphi_{(x,y)}$ est bijective d'après la propriété i), il suffit de montrer que c'est un morphisme de groupes.

Soit $(\bar{a}, \bar{b}), (\bar{c}, \bar{d}) \in \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. On note $\pi = \pi_{(\bar{c}, \bar{b})}$ i.e. $\bar{\pi} = \alpha_{\bar{b}}(\bar{c})$. On a :

$$\begin{aligned} \varphi_{(x,y)}((\bar{a}, \bar{b}) *_\alpha (\bar{c}, \bar{d})) &= \varphi_{(x,y)}(\bar{a} + \alpha_{\bar{b}}(\bar{c}), \bar{b} + \bar{d}) \\ &= \varphi_{(x,y)}(\bar{a} + \bar{\pi}, \bar{b} + \bar{d}) \\ &= x^{a+\pi}y^{b+d} \\ &= x^a x^\pi y^b y^d \\ &= x^a y^b (y^{-b}x^\pi y^b) y^d \\ &= (x^a y^b) \cdot (x^\pi y^d) \\ \varphi_{(x,y)}((\bar{a}, \bar{b}) *_\alpha (\bar{c}, \bar{d})) &= \varphi_{(x,y)}(\bar{a}, \bar{b}) \cdot \varphi_{(x,y)}(\bar{c}, \bar{d}). \end{aligned}$$

Donc $\varphi_{(x,y)}$ est un isomorphisme de groupes de $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_\alpha)$ dans $G, \cdot$.

(b) Comme $\varphi_{(x,y)}$ est un isomorphisme de groupes et $G = \langle x, y \rangle$, on a :

$$\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = \langle \varphi_{(x,y)}^{-1}(x), \varphi_{(x,y)}^{-1}(y) \rangle = \langle (\bar{1}, \bar{0}), (\bar{0}, \bar{1}) \rangle.$$

(c) On suppose G non monogène et $p < q$.

- i. Supposons par l'absurde que x et y commutent. Alors on a, pour tout $n \in \mathbb{N}$, $(xy)^n = x^n y^n$. Ainsi, on a :

$$(xy)^{pq} = (x^q)^p (y^p)^q = e$$

donc $o(xy) | pq$ et si, pour $n \in \mathbb{N}$, $(xy)^n = e$, alors $x^n = y^{-n}$, donc $x^n, y^{-n} \in \langle x \rangle \cap \langle y \rangle = \{e\}$; d'où $x^n = e$ et $y^n = e$ i.e. $q | n$ et $p | n$. Or p et q sont premiers entre eux car nombres premiers différents, donc, pour tout $n \in \mathbb{N}$ tel que $(xy)^n = e$, $pq | n$ et donc $pq | o(xy)$.

Il en résulte que $o(xy) = pq = \text{Card}(G)$ donc G est monogène. Contradiction !

Par suite, x et y ne commutent pas.

- ii. D'après la question précédente, x et y ne commutent pas. Ainsi, G n'est pas commutatif et donc, par isomorphisme (Question 26a), $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ ne l'est pas non plus. Par suite, d'après la question 23, le morphisme $\alpha : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ est injectif.

Il en résulte, d'après la question 20, que p divise $q - 1$.

B. Classification des groupes d'ordre pq avec $p < q$

On suppose $p < q$.

27. — On suppose que p ne divise pas $q - 1$. Alors, comme $p < q$, par contraposée de la question 26(c)ii, G est monogène. Par suite, d'après la question 1, G (qui est de cardinal $n = pq$) est isomorphe à $(\mathbb{Z}/pq\mathbb{Z}, +)$.
- L'hypothèse n'est pas importante ici ! On traite deux cas comme indiqué :
- Si G n'est pas monogène, alors, d'après la question 26a, G et $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ sont isomorphes (et notons que dans ce cas, p divise $q - 1$ d'après la question 26(c)ii).
 - Si G est monogène, alors comme précédemment, G est isomorphe à $(\mathbb{Z}/pq\mathbb{Z}, +)$. Or, comme p et q sont premiers entre eux (car nombres premiers différents), d'après le théorème Chinois, $(\mathbb{Z}/pq\mathbb{Z}, +)$ et $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +)$ sont isomorphes ; donc, par transitivité, G est isomorphe à $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, +)$ qui est égal à $(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$ avec α non injectif (Question 23).

C. Classification des groupes d'ordre p^2

On suppose $p = q$.

28. On raisonne par disjonction de cas :
- Si G est monogène, d'après la question 1, G est isomorphe au groupe $(\mathbb{Z}/p^2\mathbb{Z}, +)$ - qui est commutatif ;
 - Si G n'est pas monogène, alors, d'après la question 26a, G est isomorphe à $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha})$. Or, d'après la question 25b, α est une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$ donc, d'après la question 21, α est constante en l'identité.
- Par suite, d'après la question 23, on a $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, *_{\alpha}) = ((\mathbb{Z}/p\mathbb{Z})^2, +)$.

Il en résulte que G est isomorphe au groupe $((\mathbb{Z}/p\mathbb{Z})^2, +)$ qui est commutatif.

7. Théorème de Cauchy

29. Soit q un nombre premier. On suppose que G est de cardinal $n \in \mathbb{N}^*$ et que q divise n .

- (a) L'application $F : f \mapsto (f(\bar{1}), f(\bar{2}), \dots, f(\overline{q-1}))$ est une bijection de E sur G^{q-1} car, pour tout $(x_1, \dots, x_{q-1}) \in G^{q-1}$, la fonction $f \in \mathcal{F}_q(G)$ telle que, pour $k \in \llbracket 0, q-1 \rrbracket$:

$$f(\bar{k}) = \begin{cases} x_k & \text{si } k \neq 0 \\ (x_1 \dots x_{q-1})^{-1} & \text{si } k = 0 \end{cases}$$

appartient à E et est l'unique antécédent de $(x_1, \dots, x_{q-1})$ par F .

Par suite, $\text{Card}(E) = \text{Card}(G^{q-1}) = n^{q-1}$.

- (b) Montrons que $\mathcal{R}$ est une relation d'équivalence sur E . Soit $f, g, h \in E$.

- *Reflexivité.* $f \mathcal{R} f$ car, avec $\bar{0} \in \mathbb{Z}/q\mathbb{Z}$, on a bien, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$, $f(\bar{k} + \bar{0}) = f(\bar{k})$.
- *Symétrie.* On suppose $f \mathcal{R} g$. Alors il existe $\bar{m} \in \mathbb{Z}/q\mathbb{Z}$ tel que, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$, $f(\bar{k} + \bar{m}) = g(\bar{k})$.

On a alors, pour $\bar{m} \in \mathbb{Z}/q\mathbb{Z}$ et pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$:

$$g(\bar{k} + \bar{m}) = g(\overline{k - m}) = f(\overline{k - m} + \bar{m}) = f(\bar{k}).$$

D'où $g \mathcal{R} f$.

- *Transitivité.* On suppose $f \mathcal{R} g$ et $g \mathcal{R} h$. Alors il existe $\bar{m}, \bar{m}' \in \mathbb{Z}/q\mathbb{Z}$ tel que, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$, $f(\bar{k} + \bar{m}) = g(\bar{k})$ et $g(\bar{k} + \bar{m}') = h(\bar{k})$.

On a alors, pour $\bar{m} + \bar{m}' \in \mathbb{Z}/q\mathbb{Z}$ et pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$:

$$f(\bar{k} + \overline{m + m'}) = f(\overline{k + m'} + \bar{m}) = g(\overline{k + m'}) = g(\bar{k} + \bar{m}') = h(\bar{k}).$$

D'où $f \mathcal{R} h$.

Il en résulte que $\mathcal{R}$ est une relation d'équivalence sur E .

- (c) Soit $f \in \mathcal{F}_b(G)$.

— On a, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$:

$$S^q(f)(\bar{k}) = f(\overline{k + q}) = f(\bar{k}).$$

Donc $S^q(f) = f$.

— On suppose $f \in E$:

$$\begin{aligned} \prod_{k=0}^{q-1} S(f)(\bar{k}) &= \prod_{k=0}^{q-1} f(\overline{k+1}) \\ &= \left(\prod_{k=1}^{q-1} f(\bar{k}) \right) f(\bar{0}) \\ &= f(\bar{0})^{-1} \left(\prod_{k=0}^{q-1} f(\bar{k}) \right) f(\bar{0}) \\ &= f(\bar{0})^{-1} \cdot e \cdot f(\bar{0}) \\ \prod_{k=0}^{q-1} S(f)(\bar{k}) &= e. \end{aligned}$$

D'où $S(f) \in E$.

— On suppose $f \in E$. On a, pour $\bar{1} \in \mathbb{Z}/q\mathbb{Z}$ et pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$, $f(\bar{k} + \bar{1}) = S(f)(\bar{k})$ et donc, comme $S(f) \in E$, on obtient $S(f) \mathcal{R} f$.

Soit $f \in E$ et C_f sa classe d'équivalence.

D'après ce qui précède, par transitivité de proche en proche, on a $S^m(f) \mathcal{R} f$ pour tout $m \in \mathbb{Z}$.

Par suite, $\{S^m(f) \mid m \in \llbracket 0, q-1 \rrbracket\} \subset C_f$.

De plus, si $g \in C_f$, alors il existe $\bar{m} \in \mathbb{Z}/q\mathbb{Z}$ tel que, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$,

$$S^m(f)(\bar{k}) = f(\bar{k} + \bar{m}) = g(\bar{k}).$$

D'où $g = S^m(f)$ et de plus, comme $S^q = \text{Id}$, on peut choisir pour m le représentant de $\bar{m}$ dans $\llbracket 0, q-1 \rrbracket$.

Il en résulte que :

$$C_f = \{S^m(f) \mid m \in \llbracket 0, q-1 \rrbracket\}.$$

(d) Soit $f \in E$ et C_f sa classe d'équivalence pour $\mathcal{R}$.

D'après la question précédente, on a :

$$C_f = \{S^m(f) \mid m \in \llbracket 0, q-1 \rrbracket\}.$$

ensemble qui possède entre 1 et q éléments.

Montrons que si deux éléments $S^m(f)$ et $S^{m'}(f)$ avec $m \neq m'$ sont égaux, f est constante.

Soit $m, m' \in \llbracket 0, q-1 \rrbracket$ avec $m < m'$. On suppose $S^m(f) = S^{m'}(f)$.

Alors, pour $d = m' - m \in \llbracket 1, q-1 \rrbracket$, on a, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$:

$$S^d(f)(\bar{k}) = f(\underbrace{\bar{d} + \bar{k}}_{=\bar{m}' + \bar{k} - \bar{m}}) = S^{m'}(f)(\overline{k - m}) = S^m(f)(\overline{k - m}) = f(\overline{\bar{m} + \bar{k} - \bar{m}}) = f(\bar{k}).$$

Donc $S^d = \text{Id}$.

Or, comme $d \in \llbracket 1, q-1 \rrbracket$ et q est premier, d et q sont premiers entre eux, donc, d'après le théorème de Bézout, il existe u, v tels que $1 = ud + vq$ et ainsi :

$$S(f) = (S^d)^u \circ (S^q)^v (f) = (\text{Id})^u \circ (\text{Id})^v (f) = f.$$

Par suite, pour tout $\bar{k} \in \mathbb{Z}/q\mathbb{Z}$, $f(\bar{k} + \bar{1}) = f(\bar{k})$. Donc f est constante en $f(\bar{0})$. Il en résulte qu'on a l'alternative suivante,

- Les éléments de C_f sont tous différents : alors $\text{Card}(C_f) = q$;
- Deux éléments $S^m(f)$ de C_f d'exposants différents sont égaux : alors f est constante et alors, pour tout $m \in \llbracket 0, q-1 \rrbracket$, $S^m(f) = f$. D'où $C_f = \{f\}$ i.e. $\text{Card}(C_f) = 1$ et, de plus, f est constante.

(e) D'après la question précédente, les classes d'équivalence sont soit de cardinal 1, soit de cardinal q .

On note alors c_1 le nombre de classes de cardinal 1 et c_q le nombre de classe de cardinal q .

Les classes d'équivalence formant une partition de E , on a la relation, en utilisant le résultat de la question 29a :

$$c_1 + qc_q = \text{Card}(E) = n^{q-1}.$$

Or, q divise n , donc $c_1 = n^{q-1} - qc_q \equiv 0 [q]$.

De plus, la fonction constante en e appartient à E et sa classe d'équivalence est de cardinal 1, donc $c_1 \neq 0$.

Par suite, $c_1 > 1$ car $c_1 \geq 1$ et $1 \not\equiv 0 [q]$ puisque $q > 1$. Par suite, il existe une classe d'équivalence de cardinal 1 (et même $kq - 1$ classes avec un certain $k \in \mathbb{N}^*$) qui n'est pas celle de la fonction constante en e .

Ainsi, il existe $x \in G \setminus \{e\}$ tel que la fonction f constante en x appartient à E et donc :

$$x^q = \prod_{k=0}^{q-1} f(\bar{k}) = e,$$

d'où x est d'ordre q dans G .

30. On suppose G de cardinal pq avec p, q premiers. Comme q est premier et q divise $n = pq$, d'après la question précédente, il existe x d'ordre q et donc, il existe au moins une classe d'équivalence pour $\sim$ d'éléments d'ordre q , d'où $l \geq 1$.