Chapitre IV
Structures algébriques usuelles

Table des matières

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* : $\forall x, y \in G$,
$$x * y = y * x.$$

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 $(G, .)$ (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 le groupe **symétrique** de l'ensemble 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 et si G est commutatif.
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 $-x$ et ils sont tous commutatifs.
   — 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 $\frac{1}{x}$ et ils sont tous commutatifs.
   — Pour $\mathcal{S}_X$ muni de la composition : l'élément neutre est l'application identité $\mathrm{id} : x \mapsto x$; le symétrique de σ est son application réciproque σ^{-1}. En général, $(\mathcal{S}_X, \circ)$ n'est pas commutatif.

   > *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 commutatif.
2.

Exercice ∗2.

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

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

Alors 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 $(x_1y_1, x_2, y_2) \in G_1 \times G_2$.
Donc . est bien une loi de composition interne.
De plus, par associativité des lois sur G_1 et G_2, la loi . est associative.
Soit $(x_1, x_2) \in G$.

— Élément neutre : on a

$$(x_1, x_2).(e_1, e_2) = (x_1e_1, x_2e_2) = (x_1, x_2) = (e_1x_1, e_2x_2) = (e_1, e_2).(x_1, x_2);$$

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

— Symétrique : on a

$$(x_1, x_2).(x_1^{-1}, x_2^{-1}) = (x_1x_1^{-1}, x_2x_2^{-1}) = (e_1, e_2) = (x_1^{-1}x_1, x_2^{-1}x_2) = (x_1^{-1}, x_2^{-1}).(x_1, x_2);$$

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

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 :

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

si, et seulement si,

$$(x_1x_2, y_1y_2) = (x_2x_1, y_2y_1),$$

si, et seulement si,

$$x_1x_2 = x_2x_1 \quad \text{et} \quad y_1y_2 = y_2y_1.$$

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 $H \subset G$. Alors 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 $f : G_1 \to G_2$.
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 $(\mathbb{R}_+^*, \times)$.

— 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 $\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{C}^* \\ k & \mapsto & e^{i\frac{2k\pi}{n}} \end{array} \right.$ 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 $f : G_1 \to G_2$ un morphisme de groupes.

— On appelle **noyau de** f l'ensemble $\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\}$.

— On appelle **image de** f l'ensemble $\mathrm{Im}(f) = f(G_1) = \{f(x) \mid x \in G_1\}$.

Lemme ∗1. -NoValue-

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

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

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 $f : G_1 \to G_2$ un morphisme de groupes. Alors :
- $f^{-1}(H_2)$ est un sous-groupe de G_1 ;
- $f(H_1)$ 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 :

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

  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 $f : G_1 \to G_2$ un morphisme de groupes. Alors :
- $\mathrm{Ker}(f)$ est un sous-groupe de G_1 ;
- $\mathrm{Im}(f)$ est un sous-groupe de G_2.

Démonstration.

- On a :

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

  Or $\{e_2\}$ est un sous-groupe de G_2, donc, d'après la proposition précédente, $\mathrm{Ker}(f)$ est

un sous-groupe de G_1 comme image réciproque d'un sous-groupe par un morphisme de groupes.

— On a :

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

Or G_1 est un sous-groupe de G_1, donc, d'après la proposition précédente, $\mathrm{Im}(f)$ 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 $f : G_1 \to G_2$ un morphisme de groupes. On note e_1 l'élément neutre de G_1.

Alors l'application f est injective si, et seulement si, $\mathrm{Ker}(f) = \{e_1\}$

Démonstration.

- ($\Rightarrow$). On suppose f injective. Soit $x \in \mathrm{Ker}(f)$. Alors $f(x) = e_2 = f(e_1)$. Par injectivité de f, il en résulte que $x = e_1$. Par suite, $\mathrm{Ker}(f) = \{e_1\}$.
- ($\Leftarrow$). On suppose $\mathrm{Ker}(f) = \{e_1\}$. 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 $xx'^{-1} \in \mathrm{Ker}(f) = \{e_1\}$; 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 $\det : O_n(\mathbb{R}) \to \mathbb{R}^*$.

Exercice ∗5.

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 $|e^z| = e^{|z|} > 0$ 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, $\mathrm{Im}(\exp) = \mathbb{C}^*$. Il en résulte que exp est surjective de $\mathbb{C}$ dans $\mathbb{C}^*$.

Noyau : On a $z = x + iy \in \mathrm{Ker}(\exp)$ 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 $\mathrm{Ker}(\exp) = \{i2k\pi \mid k \in \mathbb{Z}\}$.

Exercice ∗6.

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 $SL_n(\mathbb{R}) = \mathrm{Ker}(\det)$ 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 $f : G_1 \to G_2$. 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 et un **automorphisme de groupes**. On note $\mathrm{Aut}(G)$ 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 $x \in \mathrm{Ker}(f_g)$. 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 $f : G_1 \to G_2$. 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. □

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 ∗7. 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 $\mathrm{Im}(\varphi) \subset \mathcal{S}_G$.
   (b) Monter 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 $\mathrm{Im}(\varphi) \subset \mathcal{S}_G$.

   (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 $x \in G$:

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

   et donc $\varphi(g.g')(x) = f(g) \circ \varphi(g')$.
   Ainsi, φ est un morphisme de G dans $\mathcal{S}_G$.
   Montrons son injectivité. Soit $g \in \mathrm{Ker}(\varphi)$. Alors $\varphi(g) = \mathrm{id}$. Ainsi, on a :

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

   Par suite, $\mathrm{Ker}(g) = \{e\}$ 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 $\mathrm{Im}(\varphi)$ de $\mathcal{S}_G$.

Exercice ∗8.

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

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

Correction.

1. — *1ère façon* (si on se rappelle du groupe symétrique de G noté $\mathcal{S}_G$) : montrons que $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathcal{S}_G, \circ)$.
On a bien $\mathrm{Aut}(G) \subset \mathcal{S}_G$ 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 $x, x,' \in G$, $\mathrm{Id}_G(xx') = xx' = \mathrm{Id}_G(x)\mathrm{Id}_G(x')$ donc c'est un morphisme de groupes.
De plus, pour tous $\varphi, \psi \in \mathrm{Aut}(G)$, 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 $\mathrm{Aut}(G)$.
Par suite, $\mathrm{Aut}(G)$ 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 $\varphi, \psi \in \mathrm{Aut}(G)$. Alors $\varphi \circ \psi : G \to G$ 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 $\mathrm{Aut}(G)$.
Par suite, $\circ$ est une loi de composition interne sur $\mathrm{Aut}(G)$. Elle est associative et d'élément neutre la fonction identité $\mathrm{Id}_G : G \to G$. D'après la proposition précédente, si ψ est un automorphisme de G, alors ψ^{-1} l'est aussi, donc tout élément de $\mathrm{Aut}(G)$ possède un symétrique pour la loi $\circ$: il s'agit de sa réciproque.
Ainsi, $(\mathrm{Aut}(G), \circ)$ 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 :
$$\psi_g \circ \psi_{g^{-1}}(x) = \psi_e(x) = exe^{-1} = x = \mathrm{id}(x);$$
et de même
$$\psi_{g^{-1}} \circ \psi_g(x) = \psi_e(x) = exe^{-1} = x = \mathrm{id}(x).$$
Donc $\psi_{g^{-1}} = (\psi_g)^{-1}$.

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

i) $\mathrm{id} = \psi_e \in \mathrm{Int}(G)$;

ii) Soit $\psi_g, \psi_{g'} \in \mathrm{Int}(G)$ avec $g, g' \in G$. On a, d'après les remarques précédentes :

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

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

Partie A

Compléments sur les groupes

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

a. Sous-groupe engendré par une partie

Proposition 1. *Intersection de sous-groupes*

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

Exercice 1.

Que dire d'une réunion de sous-groupes ?

Correction.

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 $\mathbb{C}$.

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.

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

Alors $\langle A \rangle$ 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 $\langle A \rangle = \bigcap_{\mathcal{H}_A} H$ 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. □

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 :

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

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

Démonstration.

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

- $\subset$ 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 $n, m \in \mathbb{N}^*$, $a_1, ..., a_n, a'_1, ..., a'_m \in A \cup A^{-1} \cup \{e\}$ tels que $x = a_1 ... a_n$ et $y = a'_1, ..., a'_m$. Alors

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

  où

$$a''_i = \begin{cases} a_i \in A \cup A^{-1} \cup \{e\} & \text{si } i \in [\![1, n]\!]; \\ a'^{-1}_{i-n} \in A \cup A^{-1} \cup \{e\} & \text{si } i \in [\![n+1, n+m]\!]. \end{cases}$$

  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 $\langle A\rangle \subset E(A)$.

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

Exemple 1.

— $\mathbb{Z}$ est engendré par 1, i.e. $\mathbb{Z} = \langle 1\rangle$;
— Soit $n \in \mathbb{N}^*$. Le groupe $\mathcal{S}_n$ des permutations de $[\![1, n]\!]$ est engendré par les transpositions.

Exercice 2.

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 $2u+3v = 1$. On pose alors $u = nu'$ et $v = nv'$ et on obtient :

$$n = 2u + 3v = \begin{cases} \underbrace{2 + \ldots + 2}_{u \text{ termes}} + \underbrace{3 + \ldots + 3}_{v \text{ termes}} & \text{si } u, v \geq 0 \\ \underbrace{(-2) + \ldots + (-2)}_{|u| \text{ termes}} + \underbrace{3 + \ldots + 3}_{v \text{ termes}} & \text{si } u > 0 \text{ et } v \geq 0 \\ \underbrace{2 + \ldots + 2}_{u \text{ termes}} + \underbrace{(-3) + \ldots + (-3)}_{|v| \text{ termes}} & \text{si } u \geq 0 \text{ et } v < 0 \\ \underbrace{(-2) + \ldots + (-2)}_{|u| \text{ termes}} + \underbrace{(-3) + \ldots + (-3)}_{|v| \text{ termes}} & \text{si } u, v < 0 \end{cases}$$

donc $n \in \langle A\rangle$.
Notre conjecture est donc vraie !

b. les sous-groupes de $\mathbb{Z}$

Théorème 1. *Division euclidienne*

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Alors 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 démonter l'unicité du couple (q, r)). □

Théorème 2.

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

Démonstration.

- ($\Leftarrow$). On suppose qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$. Alors $0 = n.0 \in H$. De plus, pour tous $x, y \in H$, il existe $p, q \in \mathbb{Z}$ tels que $x = np$ et $y = nq$ donc :

$$x - y = np - nq = n\underbrace{(p - q)}_{\in \mathbb{Z}} \in H.$$

  Donc H est un sous-groupe de $\mathbb{Z}$.

- ($\Rightarrow$).
  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.
  On a, pour tout $k \in \mathbb{Z}$,

$$nk = \begin{cases} \underbrace{n + ... + n}_{k \text{ termes}} \in H & \text{si } k \geq 0, \\ -\underbrace{(n + ... + n)}_{-k \text{ termes}} \in H & \text{si } k < 0; \end{cases}$$

  donc $n\mathbb{Z} \subset H$.

  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 $r < n$ tel que

$$x = nq + r$$

  Comme $n\mathbb{Z} \subset H$, $nq \in H$ et donc $r = x - nq$ appartient à H. Or n est le plus petit élément positif et non nul de H et $r < n$, donc $r = 0$. Par suite, $x = nq \in n\mathbb{Z}$.
  Il en résulte que $H = n\mathbb{Z}$.

  □

Proposition 3.

Si H est un sous-groupe de $\mathbb{Z}$, alors il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Correction.

Soit H un sous-groupe de $\mathbb{Z}$. L'existence est assurée par le théorème précédent. Montrons l'unicité. Soit $n, m \in \mathbb{N}$ tels que $n\mathbb{Z} = H = m\mathbb{Z}$. Ainsi $n \in n\mathbb{Z} \subset m\mathbb{Z}$, d'où $m|n$ donc $m = |m| \leq |n| = n$ (n, m étant positifs). De manière analogue, comme $m \in n\mathbb{Z}$, $n \leq m$.
Il en résulte que $n = m$. D'où le résultat.

Exercice 3.

Montrer que pour $p \in \mathbb{Z} \setminus \mathbb{N}$, $p\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (À quel sous-groupe de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ est-il égal ?)

Correction.

Pour tout $k \in \mathbb{Z}$, $pk = (-p)(-k)$, donc $p\mathbb{Z} = (-p)\mathbb{Z}$ qui est un sous-groupe de $\mathbb{Z}$ d'après le théorème précédent.

2. 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 :

$$a \equiv b \bmod n.$$

Proposition 4.

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 sur $\mathbb{Z}$, i.e. pour tous $a, b, c, d \in \mathbb{Z}$, si $a \equiv b \bmod n$ et $c \equiv d \bmod n$, alors

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

Démonstration.

Montrons que $\cdot \equiv \cdot \bmod n$ 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 $a \equiv a \bmod n$.
- (*Symétrie*) On suppose $a \equiv b \bmod n$. 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 $b \equiv a \bmod n$.
- (*Transitivité*) On suppose $a \equiv b \bmod n$ et $b \equiv c \bmod n$. 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 $a \equiv c \bmod n$.

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 $a \equiv b \bmod n$ et $c \equiv d \bmod n$. 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 $a + c \equiv b + d \bmod n$.

Et on a :

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

donc $ac \equiv bd \bmod n$. □

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 $\overline{k} = \{x \in \mathbb{Z} \mid x \equiv k \bmod n\}$ 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 1.

— On a $\overline{0} = n\mathbb{Z}$, $\overline{1} = 1 + n\mathbb{Z}$, ... , $\overline{k} = k + n\mathbb{Z}$.

— 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 $\alpha = \overline{k}$. On dit alors que k est **représentant de la classe** α.

Exercice 4.

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

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

Démonstration.

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

2. Si $x \equiv y \mod n$, alors il existe $p \in \mathbb{Z}$ tel que $y - x = pn$. Par suite, pour tout $q \in \mathbb{Z}$,
$$y + qn = x + pn + qn = x + (p+q)n \in x + n\mathbb{Z} = \overline{x},$$
et
$$x + qn = y - pn + qn = x + (q-p)n \in y + n\mathbb{Z} = \overline{y},$$
d'où $\overline{y} \subset \overline{x}$ et $\overline{x} \subset \overline{y}$. Donc $\overline{x} = \overline{y}$.
Réciproquement, si $\overline{x} = \overline{y}$, alors en particulier, $x = x + 0n \in \overline{x} = \overline{y}$, donc par définition, $x \equiv y \mod n$.

3. Soit $x, y \in \mathbb{Z}$. On suppose $\overline{x} \cap \overline{y} \neq \emptyset$. Alors il existe $k = \overline{x} \cap \overline{y}$, donc $k \equiv x \mod n$ et $k \equiv y \mod n$. Par symétrie et transitivité, on a alors :
$$x \equiv y \mod n.$$
Par suite, d'après le résultat précédent, $\overline{x} = \overline{y}$.

□

Proposition 5.

Soit $n \in \mathbb{N}^*$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n et on a :
$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

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
$$\{\overline{0}, \overline{1}, ..., \overline{n-1}\} \subset \mathbb{Z}/n\mathbb{Z}.$$
Montrons que $\mathbb{Z}/n\mathbb{Z} \subset \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. 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 $r \in [\![0, n-1]\!]$. Alors

$$k \equiv r \mod n.$$

Donc $\alpha = \overline{k} = \overline{r} \in \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. D'où l'inclusion.
Il en résulte que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. □

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 $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$, $-\overline{k} = \overline{-k}$.

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 $p \equiv p' \mod n$ et $q \equiv q' \mod n$, donc :

$$p + q \equiv p' + q' \mod n.$$

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 $a = \overline{x}, \beta = \overline{y}, \gamma = \overline{z} \in \mathbb{Z}/n\mathbb{Z}$.

- (*Associativité*). On a :

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

- (*Élément neutre*). On a :

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

- (*Symétrique*). On a :

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

□

Proposition 6.

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

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

est un morphisme surjectif de groupe.

Démonstration.

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

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

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 $\alpha = \overline{k}$. Donc π_n est surjective. □

Exercice 5.

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

Correction.

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

3. Groupes monogènes

a. Généralités et exemples

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 $\{x\}$.

Définition 3. *Groupe monogène*

Soit G un groupe. On dit que G est **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.

Proposition 7.

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

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

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, $E(x) = \langle x \rangle$.

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 2. *Groupes monogènes classiques*

— pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est engendré par $\overline{1}$, i.e. $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$;

— pour $n \in \mathbb{N}^*$, le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est engendré par $e^{i\frac{2\pi}{n}}$, i.e. $\mathbb{U}_n = \langle e^{i\frac{2\pi}{n}} \rangle$;

Exercice 6.

1. Montrer que $(\mathbb{Z}^2, +)$ est un groupe commutatif.
2. Est-il monogène ? Sinon, donner un ensemble minimal (de cardinal le plus petit possible) qui engendre $\mathbb{Z}^2$.

Correction.

1. $(\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}, +)$ un groupe comme le produit des groupes $\mathbb{Z}$ par $\mathbb{Z}$ chacun muni de l'addition. De plus, $(\mathbb{Z}, +)$ est commutatif, donc le produit de $\mathbb{Z}$, par $\mathbb{Z}$ l'est aussi.
2. Non, il n'est pas monogène. En effet, pour tout $(n, m) \in \mathbb{Z}^2$, on a par exemple $(n+1, m) \notin \langle (n, m) \rangle$ donc $\langle (n, m) \rangle \neq \mathbb{Z}^2$.
   La paire $\{(1, 0), (0, 1)\}$ engendre $\mathbb{Z}^2$.

Définition 4. *Groupe cyclique*

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

Question 1.

Parmi les groupes de l'exemple précédent, lesquels sont cycliques ?

Correction.

$\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{U}_n$.

b. Classification des groupes monogènes

Proposition-Notation 8.

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

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

est un morphisme de groupes.

Démonstration.

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

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

donc φ_k est un morphisme de groupes. □

Théorème 4. *Classification des groupes monogènes*

- Tout groupe monogène *infini* est isomorphe à $(\mathbb{Z}, +)$;
- Tout groupe monogène *de cardinal* $n \in \mathbb{N}^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

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 précédente. On a

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

donc φ_x est un morphisme surjectif.

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

- $n = 0$. Alors $\mathrm{Ker}(\varphi_x) = \{0\}$, 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 $\mathrm{Ker}(\varphi_x) = n\mathbb{Z} \neq \{0\}$, donc φ_x n'est pas injective.
  Soit $\alpha \in \mathbb{Z}/n\mathbb{Z}$ et $p, q \in \alpha$. Alors on a $p - q \in n\mathbb{Z} = \mathrm{Ker}(f_x)$ 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 :

  $$\widetilde{\varphi}_x : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathrm{G} \\ \alpha & \mapsto & x^p = \varphi_x(p) \quad \text{où } p \in \alpha \end{array} \right.$$

  Alors
  - $\widetilde{\varphi}_x$ est un morphisme de groupes. En effet, pour tous $p, q \in \mathbb{Z}$,

    $$\widetilde{\varphi}_x(\overline{p} + \overline{q}) = \widetilde{\varphi}_x(\overline{p+q}) = \varphi_x(p+q) = x^{p+q} = x^p x^q = \varphi_x(p)\varphi_x(q) = \widetilde{\varphi}_x(\overline{p})\widetilde{\varphi}_x(\overline{q}).$$

  - $\widetilde{\varphi}_x$ est surjectif. En effet, pour tout $y \in \langle x \rangle$, il existe $k \in \mathbb{Z}$ tel que $y = x^k$ et

    $$y = x^k = \varphi_x(k) = \widetilde{\varphi}_x(\overline{k}).$$

    Donc $\overline{k}$ est un antécédent de y par $\widetilde{\varphi}_x$.
  - $\widetilde{\varphi}_x$ est injectif. En effet, si $\overline{k} \in \mathrm{Ker}(\widetilde{\varphi}_x)$, alors

    $$e = \widetilde{\varphi}_x(\overline{k}) = \varphi_x(k),$$

    donc $k \in \mathrm{Ker}(\varphi_x) = n\mathbb{Z}$. Par suite, $k \equiv 0 \bmod n$, d'où $\overline{k} = \overline{0}$.
    Il en résulte que $\mathrm{Ker}(\widetilde{\varphi}_x) = \{\overline{0}\}$.

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

□

Exemple 3.

Soit $n \in \mathbb{N}^*$. Le groupe $(\mathbb{U}_n, .)$ 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, $(\mathbb{U}_n, .)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. De plus, l'isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{U}_n$ est donné par :
>
> $$\overline{k} \mapsto e^{i\frac{2k\pi}{n}}.$$

Exercice 7.

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.

On remarque que $G = \left\langle \begin{pmatrix} 3 & 1 \\ 0 & 3 \end{pmatrix} \right\rangle$. Donc G est monogène. De plus, G est infini, donc G est isomorphe à $\mathbb{Z}$.

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

Théorème 5. *Théorème de Bézout*

Soit $n, m \in \mathbb{Z}$. Alors n et m sont premiers entre eux si, et seulement si, il existe $u, v \in \mathbb{Z}$ tels que

$$un + vm = 1.$$

Démonstration.

Vue en Sup. □

Exercice 8.

Soit $n, m \in \mathbb{Z}$ et $d = \text{pgcd}(n, m)$. Déduire du théorème de Bézout qu'il existe $u, v \in \mathbb{Z}$ tels que $un + vm = d$.

Correction.

d est le plus grand diviseur commun de n, m donc il existe $p, q \in \mathbb{Z}$ premiers entre eux tels que $n = dp$ et $m = dq$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$; donc on a, en multipliant la précédente égalité par d :

$$un + vm = d.$$

Proposition 9.

Soit $n \in \mathbb{N}$ et $k \in \mathbb{Z}$. Alors $\overline{k}$ 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 $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$. Alors il existe $u \in \mathbb{Z}$ tel que

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

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

  $$uk + vn = 1.$$

  D'après le théorème de Bézout, 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, il existe $u, v \in \mathbb{Z}$ tels que :
$$uk + vn = 1.$$
Par suite, pour tout $p \in [\![0, n-1]\!]$,
$$p = puk + pvn,$$
d'où, si on note $q = pu$, $p \equiv puk = qk \mod n$ i.e.
$$\overline{p} = q\overline{k}.$$
Par suite, $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$.

□

4. Ordre d'un élément

Définition 5. *Ordre d'un élément*

Soit G un groupe et $x \in G$. On dit que x est **d'ordre fini** 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 :
$$o(x) = \#\langle x \rangle.$$

Proposition 10.

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

i) Le nombre d est le plus petit entier naturel non nul qui vérifie l'égalité $x^n = e$.

ii) Pour tout $n \in \mathbb{Z}$, $x^n = e$ si, et seulement si, d divise n.

Démonstration.

Comme $\langle x \rangle = \{e, x, ..., x^{d-1}\}$ est un groupe monogène de cardinal d, on peut considérer l'isomorphisme $\varphi_x : \overline{k} \mapsto x^k$ de $\mathbb{Z}/d\mathbb{Z}$ dans $\langle x \rangle$.

i) On a
$$x^d = \varphi_x(\overline{d}) = \varphi_x(\overline{0}) = x^0 = e.$$
De plus, si $n \in \mathbb{N}^*$ est tel que $x^n = e$, alors $n > d - 1$ car pour tout $i \in [\![1, d-1]\!]$, $x^i \neq e$. Donc $n \geq d$.

ii) Soit $n \in \mathbb{Z}$.
- ($\Rightarrow$). On suppose $x^n = e$. Alors $\varphi_x(n) = e$ donc $\overline{n} \in \mathrm{Ker}(\varphi_x) = \{\overline{0}\}$. Ainsi $n \equiv 0 \mod d$ donc $d|n$.
- ($\Leftarrow$). On suppose $d|n$. Alors il existe $k \in \mathbb{Z}$ tel que $n = dk$, donc
$$x^n = x^{dk} = (x^d)^k = e^k = e.$$

□

Exercice 9.

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

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

Correction.

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

$$(x^n)^m = e \Leftrightarrow x^{nm} = e \Leftrightarrow k|nm \Leftrightarrow nq|nm \Leftrightarrow q|m$$

   Et de plus $(x^n)^q = e$ donc q est le plus petit entier naturel m non nul tel que $(x^n)^m = e$. Donc $o(x^n) = q = k/n$.

2. Considérons $d = \text{pgcd}(p, k)$. Montrons que $\langle x^d \rangle = \langle x^p \rangle$.
   — On a $\langle x^d \rangle \subset \langle x^p \rangle$. En effet, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$up + vk = d.$$

   Alors

$$x^d = x^{up+vk} = (x^p)^u \underbrace{(x^k)^v}_{=e} = (x^p)^u \in \langle x^p \rangle.$$

   Donc $\langle x^d \rangle \subset \langle x^p \rangle$
   — On a $\langle x^p \rangle \subset \langle x^d \rangle$. En effet, $d|p$ donc il existe $q \in \mathbb{Z}$ tel que $p = dq$ et donc :

$$x^p = x^{dq} = (x^d)^q \in \langle x^d \rangle.$$

   Donc $\langle x^p \rangle \subset \langle x^d \rangle$
   Ainsi, $o(x^p) = \#\langle x^p \rangle = \#\langle x^d \rangle = k/d (= ppcm(p, k)/p)$.

Proposition 11.

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* - voire TD pour la démonstration du cas général (non exigible).

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, $o(x)|n$. □

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 $a, b \in A$,

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

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 $B \subset A$. Alors 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 $x, y \in B$, $x.y \in B$.

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 $1 = \underbrace{1}_{\in\mathbb{Z}} + i.\underbrace{0}_{\in\mathbb{Z}} \in \mathbb{Z} + i\mathbb{Z}$.

   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 :

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

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 $1 = \underbrace{1}_{\in\mathbb{Q}} + \sqrt{2}.\underbrace{0}_{\in\mathbb{Q}} \in \mathbb{Q} + \sqrt{2}\mathbb{Q}$.

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

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

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 :

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

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. Alors 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 $f : A \to B$ 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'anneau 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 $f : A \to B$ un morphisme d'anneaux.

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

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

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

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

Proposition **3.

Soit A_1, A_2 des anneaux et $f : A_1 \to A_2$ un morphisme d'anneaux. Alors $\mathrm{Im}(f)$ est un sous-anneau de A_2.

Démonstration.

i) $1_{A_2} = f(1_{A_1}) \in \mathrm{Im}(f)$;

ii) pour $f(x), f(y) \in \mathrm{Im}(f)$ avec $x, y \in A_1$,

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

iii) pour $f(x), f(y) \in \mathrm{Im}(f)$ avec $x, y \in A_1$,

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

Donc $\mathrm{Im}(f)$ est un sous-anneau de A_2.

□

Remarque **4. ATTENTION !

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

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

Partie B

Compléments sur les anneaux ; idéaux

1. Structure d'anneau produit

Proposition 12. *Structure d'anneau produit*

Soit $(A_1, +, \cdot), (A_2, +, \cdot)$ des anneaux et on note $A = A_1 \times A_2$. On considère les lois de composition suivantes sur A : pour $(x_1, x_2), (y_1, y_2) \in A$,

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2) \quad \text{et} \quad (x_1, x_2).(y_1, y_2) := (x_1.y_1, x_2.y_2).$$

Alors A muni de ces lois est un anneau et :

- L'élément nul de A est $0_A = (0_{A_1}, 0_{A_2})$.
- L'unité de A est $1_A = (1_{A_1}, 1_{A_2})$.

Démonstration.

— $(A, +)$ est un groupe commutatif d'élément neutre $0_A = (0_{A_1}, 0_{A_2})$ comme groupe produit des groupes commutatifs $(A_1, +)$ et $(A_2, +)$.

— La loi $\cdot$ est associative par associativité des lois multiplicatives de A_1 et A_2.

— *Distributivité :* Soit $x = (x_1, x_2), y = (y_1, y_2), z = (z_1, z_2) \in A$, alors :

$$\begin{aligned} x.(y+z) &= (x_1, x_2).(y_1 + z_1, y_2 + z_2) \\ &= (x_1.(y_1 + z_1), x_2.(y_2 + z_2)) \\ &= (x_1.y_1 + x_1.z_1, x_2.y_2 + x_2.z_2) \\ &= (x_1.y_1, x_2.y_2) + (x_1.z_1, x_2.z_2) \\ &= (x_1, x_2).(y_1, y_2) + (x_1, x_2).(z_1.z_2) \\ &= x.y + x.z \end{aligned}$$

et de même

$$(y+z).x = y.x + z.x$$

— Pour tous $x = (x_1, x_2) \in A$,

$$\begin{aligned} x.1_A &= (x_1, x_2).(1_{A_1}, 1_{A_2}) \\ &= (x_1.1_{A_1}, x_2.1_{A_2}) \\ &= (x_1, x_2) \\ &= x \\ &= (1_{A_1}.x_1, 1_{A_2}.x_2) \\ &= (1_{A_1}, 1_{A_2}).(x_1, x_2) \\ &= 1_A.x \end{aligned}$$

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. □

Remarque 3.

Par récurrence, on peut ainsi munir un produit fini d'anneaux d'une structure d'anneau.

Exercice 10.

Montrer que $A = A_1 \times A_2$ est commutatif si, et seulement si, A_1 et A_2 sont commutatifs.

Correction.

Soit $x_1, y_1 \in A_1$, $x_2, y_2 \in A_2$. On a :

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

si, et seulement si,

$$(x_1x_2, y_1y_2) = (x_2x_1, y_2y_1),$$

si, et seulement si,

$$x_1x_2 = x_2x_1 \quad \text{et} \quad y_1y_2 = y_2y_1.$$

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 $a \in A$,

$$ax \in I.$$

Exemple 4.

Soit A, B des anneaux commutatifs.

— A et $\{0_A\}$ sont des idéaux de A.

— Pour $f : A \to B$ un morphisme d'anneaux, $\mathrm{Ker}(f)$ est un idéal de A.

> En effet,
>
> i) $\mathrm{Ker}(f)$ est un sous-groupe du groupe $(A, +)$ comme image réciproque de $\{0_B\}$ par f.
>
> ii) Soit $x \in \mathrm{Ker}(f)$ et $a \in A$; on a :
>
> $$f(ax) = f(a)f(x) = f(a)0_B = 0_B,$$
>
> donc $ax \in \mathrm{Ker}(f)$.

Exercice 11.

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

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

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

2. Si $u \in I$, alors

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

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

Proposition 13. *Image réciproque d'un idéal*

Soit A, B des anneaux commutatifs, $f : A \to B$ un morphisme et J un idéal de B. Alors $f^{-1}(J)$ 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 :

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

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

b. Opérations sur les idéaux

Proposition 14. *Somme d'idéaux*

Soit A un anneau commutatif et I, J des idéaux de A.
Alors l'ensemble $I + J = \{x + y \mid x \in I\ , y \in J\}$ est un idéal de A.

Démonstration.

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 :

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

car I, J sont stables par multiplication par les éléments de A.
Il en résulte que $I+J$ est un idéal de A. □

Remarque 4.

On peut généraliser ce résultat par récurrence : une somme finie d'idéaux est un idéal.

Proposition 15. *Intersection d'idéaux*

Soit A un anneau commutatif et $(I_k)_{k\in K}$ une famille quelconque d'idéaux de A.
Alors $\bigcap_{k\in K} I_k$ est un idéal de A.

Démonstration.

$I = \bigcap_{k\in K} I_k$ est un sous-groupe de $(A,+)$ comme intersections de sous-groupes de $(A,+)$.
Soit $x \in I$ et $a \in A$. Alors pour tout $k \in K$, $x \in I_k$ qui est un idéal de A donc $ax \in I_k$ pour tout $k \in K$. Par suite, $ax \in I$.
Il en résulte que I est un idéal de A. □

Définition-Proposition 7.

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

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

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 $J \in \mathcal{I}_H$, $X \subset I$.
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. □

Définition-Proposition 8.

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

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

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

Démonstration.

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

$\underline{I_x \subset Ax :}$
Comme I_x est contenu dans tous les idéaux contenant x, montrons que Ax est un idéal contenant x :
On a $x = 1_A.x \in Ax$ donc Ax contient x.
On vient de voir que Ax est non vide (on aurait pu également voir que $0_A = 0_A.x \in Ax$) et pour tous $ax, bx \in Ax$ avec $a, b \in A$, on a, par distributivité de $\cdot$ par rapport à $+$:

$$ax - bx = (a - b)x \in Ax$$

donc Ax est un sous-groupe de $(A, +)$.
De plus, pour tout $b \in A$ et tous $ax \in Ax$ avec $a \in A$, par associativité de $\cdot$:

$$b.(ax) = (ba).x \in Ax.$$

Il en résulte que Ax est un sous-anneau de A qui contient x donc $I_x \subset Ax$.

$\underline{Ax \subset I_x :}$
Soit $ax \in Ax$ 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 $ax \in I_x$. D'où $Ax \subset I_x$.

Conclusion : on a $I_x = Ax = \{ax \mid a \in A\}$. □

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 5.

Pour $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n dans $\mathbb{Z}$ est l'idéal principal engendré par $\{n\}$.

c. 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 $y = ax$.

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

Proposition 16. *Caractérisation de la divisibilité en terme d'idéaux*

Soit A un anneau commutatif intègre et $x, y \in A$. Alors $x|y$ si, et seulement si, $Ay \subset Ax$.

Démonstration.

- ($\Rightarrow$). On suppose $x|y$. Alors il existe $a \in A$ tel que $y = ax$. Soit $a'y \in Ay$. Alors
$$a'y = a'ax \in Ax,$$
car A est stable par $\cdot$. Donc $Ay \subset Ax$.
- ($\Leftarrow$). On suppose $Ay \subset Ax$. Alors en particulier, $y = 1_A.y \in Ax$ donc il existe $a \in A$ tel que $y = ax$. D'où $x|y$.

□

Exercice 12.

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

1. Montrer que $x|y$ et $y|x$ si, et seulement s'il existe $u \in A^\times$ tel que $y = ux$. Dans ce cas, on dit que x et y sont **associés**.
2. Montrer que $Ax = Ay$ si, et seulement si, x et y sont associés.

Correction.

1. - ($\Rightarrow$). On suppose $x|y$ et $y|x$. Alors il existe $u, v \in \mathbb{Z}$ tels que $y = ux$ et $x = vy$. Ainsi, par exemple, $x = vux$ d'où $x(1_A - vu) = 0_A$. Comme A est intègre, alors
$$x = 0_A \text{ ou } 1_A - vu = 0_A.$$
1er cas : $x = 0_A$. Alors $y = 0_A$ et par exemple, $y = 1_A x$.
2eme cas : $1_A - vu = 0_A$. Alors $vu = 1_A$ donc u est inversible d'inverse v.
Dans tous les cas il existe $u \in A^\times$ tel que $y = ux$.
   - ($\Leftarrow$). On suppose qu'il existe $u \in A^\times$ tel que $y = ux$. Alors $y = ux$ et $x = u^{-1}y$ donc

$x|y$ et $y|x$

2. On a $Ax = Ay$ si, et seulement si, $Ax \subset Ay$ et $Ay \subset Ax$ si, et seulement si, $x|y$ et $y|x$ (d'après la proposition précédente).

d. Exemples : les idéaux de $\mathbb{Z}$

Théorème 6. *Idéaux de $\mathbb{Z}$*

Soit I un idéal de $\mathbb{Z}$. Alors 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 la proposition 3. □

Corollaire 1.

$\mathbb{Z}$ est un anneau principal.

Démonstration.

En effet, 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 $\{n\}$. □

Proposition 17.

Soit $a, b \in \mathbb{Z}$ non tous nuls.

- Le pgcd d de a et b est l'unique générateur positif de l'idéal $a\mathbb{Z} + b\mathbb{Z}$.
- Le ppcm m de a et b est l'unique générateur positif de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$.

Démonstration.

- Comme une somme d'idéaux est un idéal, d'après le théorème 6, il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Montrons que d est le pgcd de a et b i.e. le plus petit diviseur positif commun de a et b. On note d' ce pgcd.
  On a $a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $b = a \times 0 + b \times 1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ donc d est un diviseur commun de a et b. Or tout diviseur commun divise le pgcd donc $d|d'$.
  De plus, comme $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, il existe $u', v' \in \mathbb{Z}$ tels que $d = au' + bv'$. Or d' étant un diviseur commun de a et b, par combinaison linéaire $d'|d$.
  Ainsi, d, d' étant positifs, $d = d'$.
- Comme une intersection d'idéaux est un idéal, d'après le théorème 6, il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Montrons que m est le ppcm de a et b i.e. le plus petit

multiple positif commun de a et b. On note m' ce ppcm.
Comme m' est un multiple commun de a et b, on $m' \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ donc $m|m'$.
De plus, comme $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, m est un multiple commun de a et b. Or le ppcm divise tout multiple commun donc $m'|m$.
Ainsi, m, m' étant positifs, $m = m'$.

□

Remarque 5.

La proposition précédente nous invite à revoir certaines définitions de bases de l'arithmétique dans $\mathbb{Z}$: on pourrait oublier nos "vieilles" définitions du pgcd et de ppcm et les redéfinir en termes d'idéaux ! Et c'est ce qu'on fera pour les polynômes. Un des avantages de partir des idéaux pour la définition du pgcd est que la relation de Bézout devient immédiate !

3. L'anneau $\mathbb{Z}/n\mathbb{Z}$

a. Structure d'anneau

Théorème 7. *Structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$*

Soit $n \in \mathbb{N}^*$. 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 $x, y \in \mathbb{Z}$,

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x}.\overline{y} = \overline{x.y}.$$

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. □

Proposition 18.

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

$$\pi_n : \left| \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array} \right.$$

est un morphisme surjectif d'anneaux de noyau $\mathrm{Ker}(\pi_n) = n\mathbb{Z}$.

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 $\mathrm{Ker}(\pi_n) = n\mathbb{Z}$.

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 :

$$\pi_n(pq) = \overline{pq} = \overline{pq} = \pi_n(p)\pi_n(q).$$

□

b. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$

Proposition 19. *Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$*

Soit $n \in \mathbb{N}$ et $k \in \mathbb{Z}$. Alors $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement, si k est premier avec n.

Démonstration.

$$\overline{k} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z}$$

si, et seulement si,

$$\text{il existe } \overline{u} \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \overline{k}\overline{u} = \overline{1}$$

si, et seulement si,

$$\text{il existe } u \in \mathbb{Z} \text{ tel que } ku \equiv 1 \mod n$$

si, et seulement si,

$$\text{il existe } u, v \in \mathbb{Z} \text{ tels que } ku + nv = 1$$

si, et seulement si,

$$k \text{ et } n \text{ sont premiers entre eux.}$$

□

Corollaire 2.

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)⇒iii)⇒ii)⇒i)

- i)⇒iii) Si n est premier, alors pour tout $k \in [\![1, n-1]\!]$, k est premier avec n donc $\overline{k}$ est inversible. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps
- ii)⇒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)⇒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 $p, q \in [\![2, n-1]\!]$. On a alors $\overline{p} \neq \overline{0}$ et $\overline{q} \neq \overline{0}$ et
$$\overline{pq} = \overline{0},$$
par suite $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

□

Notation 2.

Soit p un nombre premier. On note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

Exercice 13.

1. Déterminer les éléments inversibles de $\mathbb{Z}/10\mathbb{Z}$ et calculer l'inverse de $\overline{9}$ et $\overline{7}$.
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 $\overline{9}.\overline{9} = \overline{1}$. Donc $\overline{9}$ est sa propre inverse dans $\mathbb{Z}/10\mathbb{Z}$.
   On a $7 \times 3 = 21 = 1 + 2 \times 10$ donc $\overline{7}.\overline{3} = \overline{1}$. Donc $\overline{3}$ est l'inverse de $\overline{7}$ 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 $\overline{-63}.\overline{41} = \overline{1}$. Par suite $\overline{-63} = \overline{89}$ est l'inverse de $\overline{41}$ dans $\mathbb{Z}/152\mathbb{Z}$.

c. Théorème Chinois

Théorème 8. *Théorème Chinois*

Soit $n, m \in \mathbb{N}$ deux entiers premiers entre eux. Alors les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes et l'application :
$$\varphi \left| \begin{array}{ccc} \mathbb{Z}/(nm)\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \overline{k}^{nm} & \mapsto & \left(\overline{k}^{n}, \overline{k}^{m}\right) \end{array} \right.$$
est un isomorphisme d'anneaux.

Démonstration.

Montrons que φ est bien définie : si $p \equiv q \bmod nm$, alors $p - q \in nm\mathbb{Z}$. Or $nm\mathbb{Z} \subset n\mathbb{Z}$ et $nm\mathbb{Z} \subset m\mathbb{Z}$, donc $p \equiv q \bmod n$ et $p \equiv q \bmod m$. Ainsi $\varphi(\overline{p}^{nm}) = \varphi(\overline{q}^{nm})$ donc φ est bien définie.

φ est un morphisme d'anneaux car $\overline{k}^{nm} \mapsto \overline{k}^{n}$ et $\overline{k}^{nm} \mapsto \overline{k}^{m}$ sont des morphismes d'anneaux. On a :

$$\mathrm{Ker}(\varphi) = \{\overline{k}^{nm} \mid \overline{k}^{n} = \overline{0}^{n}, \overline{k}^{m} = \overline{0}^{m}\},$$

Or si $\overline{k}^{n} = \overline{0}^{n}$ et $\overline{k}^{m} = \overline{0}^{m}$, alors k est un multiple commun de n et m qui sont premiers entre eux, donc k est un multiple de nm i.e. $\overline{k}^{nm} = \overline{0}^{nm}$. D'où $\mathrm{Ker}(\varphi) = \{\overline{0}^{nm}\}$. Par suite φ est injective.

De plus, f 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). □

Corollaire 3. *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 :

$$\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod m \end{cases}$$

et les solutions de ce système sont exactement les entiers congrus à k modulo nm.

Méthode de résolution :

n et m étant premier 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

$$\begin{cases} x_1 \equiv 0 \bmod n \\ x_1 \equiv 1 \bmod m \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 1 \bmod n \\ x_2 \equiv 0 \bmod m \end{cases}$$

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 14.

Résoudre les systèmes suivants :

$$(S_1) \begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 4 \bmod 7 \end{cases} \quad \text{et } (S_2) \begin{cases} 3x \equiv 2 \bmod 5 \\ 5x \equiv 1 \bmod 6 \end{cases}$$

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 :

$$\begin{cases} x_1 \equiv 1 \bmod 6 \\ x_1 \equiv 0 \bmod 7 \end{cases} \quad \text{et} \quad \begin{cases} x_2 \equiv 0 \bmod 6 \\ x_2 \equiv 1 \bmod 7 \end{cases}$$

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 $\overline{3}$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$ et sont inverse est $\overline{2}$ car $3 \times 2 = 6 = 1 + 5$.

Ainsi, on a $3x \equiv 2 \bmod 5 \Leftrightarrow x \equiv 4 \bmod 5$.

On a 5 et 6 premiers entre eux, donc $\overline{5}$ est inversible dans $\mathbb{Z}/6\mathbb{Z}$ et sont inverse est $\overline{5}$ car $5 \times 5 = 24 = 1 + 4 \times 6$.

Ainsi, on a $5x \equiv 1 \bmod 6 \Leftrightarrow x \equiv 5 \bmod 6$.

d'où :

$$(S_2) \Leftrightarrow \begin{cases} x \equiv 4 \bmod 5 \\ x \equiv 5 \bmod 6 \end{cases}$$

Et on résout comme précédemment.

Exercice 15.

Résoudre l'équation $x^2 + x + 11 \equiv 0 \bmod 143$.

Correction.

On a $143 = 11 \times 13$ et 11 est premier avec 13 donc d'après le théorème chinois, $(*)$ $x^2 + x + 11 \equiv 0 \bmod 143$ si, et seulement si,

$$(1)\ x^2 + x + 11 \equiv 0 \bmod 11 \quad \text{et} \quad (2)\ x^2 + x + 11 \equiv 0 \bmod 13$$

Donc si x_1 est une solution de (1) et x_2 une solution de (2), alors $x = x_1 u + x_2 v$ 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

$$(x+1)x = x^2 + x \equiv x^2 + x + 11 \equiv 0 \bmod 11$$

et

$$(x-1)(x+2) = x^2 + x - 2 \equiv x^2 + x + 11 \equiv 0 \bmod 13$$

Donc les solutions de (1) sont $x \equiv 0 \bmod 11$ et $x \equiv -1 \bmod 11$ et les solutions de (2) sont $x \equiv 1 \bmod 13$ et $x \equiv -2 \bmod 13$.

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 :

$$x \equiv 66 \bmod 143$$

$$x \equiv 11 \bmod 143$$

$$x \equiv -12 \bmod 143$$
$$x \equiv 76 \bmod 143$$

Méthode : Que faire dans le cas d'un système : $\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q \end{cases}$ 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 $a \equiv b \bmod d$.

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 un classe modulo $M\mathbb{Z}$.

Exercice 16.

Résoudre les systèmes suivants :

$$(S_1) \begin{cases} x \equiv 1 \bmod 6 \\ x \equiv 4 \bmod 15 \end{cases} \quad \text{et} \quad (S_2) \begin{cases} 3x \equiv 6 \bmod 18 \\ x \equiv 1 \bmod 21 \end{cases}$$

d. Indicatrice d'Euler

Définition 11. *Fonction indicatrice d'Euler*

On appelle **fonction indicatrice d'Euler** l'application $\varphi : \mathbb{N}^* \to \mathbb{N}$ définie, pour $n \in \mathbb{N}^*$, par :

$$\varphi(n) = \#\{k \in [\![1, n]\!] \mid k \text{ et } n \text{ sont premiers entre eux}\}.$$

Proposition 20. *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 $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ 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 $x \in [\![1, p^\alpha]\!]$, x est n'est pas premier avec p^α si, et seulement si $x \in p\mathbb{Z}$, i.e.

$$x \in [\![1, p^\alpha]\!] \cap \{kp \mid k \in \mathbb{Z}\} = \{kp \mid k \in [\![1, p^{\alpha-1}]\!]\}.$$

Donc

$$\varphi(n) = \#[\![1, p^\alpha]\!] - \#[\![1, p^{\alpha-1}]\!] = p^\alpha - p^{\alpha-1}.$$

v) Soit $n, m \in \mathbb{N}^*$ avec n et m premiers entre eux. D'après le théorème chinois, $\mathbb{Z}/nm\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Donc $\overline{x}^{nm}$ est inversible dans $\mathbb{Z}/nm\mathbb{Z}$ si, et seulement si, $\overline{x}^n$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et $\overline{x}^m$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$ d'où :

$$\varphi(nm) = \#(\mathbb{Z}/nm\mathbb{Z})^\times = \#(\mathbb{Z}/n\mathbb{Z})^\times.\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(n)\varphi(m).$$

□

Exercice 17.

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

$$\sum_{d|n} \varphi(d) = n$$

Correction.

Considérons l'ensemble $F = \{\frac{k}{n} \mid k \in [\![1, n]\!]\}$. 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

$$F = \bigcup_{d|n} F_d \quad \text{où } F_d = \{\frac{i}{d} \mid \text{pgcd}(i, d) = 1 \text{et} 1 \leq i \leq d\}.$$

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 4.

Soit $n \in \mathbb{N}$ avec $n \geq 2$. On considère $n = p_1^{\alpha_1} ... p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$ sa décomposition en facteurs

premiers. Alors :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)...\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

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 :

$$\varphi(n) = \prod_{i=1}^{k}\varphi(p_i^{\alpha_i}) = \prod_{i=1}^{k}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod_{i=1}^{k} p_i^{\alpha_i}\left(1 - p_i^{-1}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

□

Théorème 9. *Théorème d'Euler*

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Alors, pour tout $a \in \mathbb{Z}$ tel que a et n sont premiers entre eux,

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Démonstration.

L'entier a est premier avec n donc $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Or $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ est un groupe fini, donc $o(\overline{a})|\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. Ainsi,

$$\overline{a}^{\varphi(n)} = \overline{1}.$$

□

Corollaire 5. *Petit théorème de Fermat*

Soit p un nombre premier. Alors pour tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$,

$$a^{p-1} \equiv 1 \bmod p$$

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. □

Partie C

Anneaux de polynômes

Dans toute cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$ 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

a. Divisibilité

Théorème 10. *Division euclidienne dans $\mathbb{K}[X]$*

Soit $A, B \in \mathbb{K}[X]$ et $B \neq 0$. Alors il existe un unique couple $(Q, R) \in (\mathbb{K}[X])^2$ tel que :

$$A = BQ + R \quad \text{et} \quad \deg(R) \leq \deg(B) - 1.$$

On appelle Q le **quotient** et R le **reste** de la division euclidienne de A par B.

Démonstration.

Vue en sup. □

Remarque 6.

Ainsi $B|A$ si, et seulement si le reste R est nul.

b. Inversibles

On rappelle le fait suivant :

Proposition 21.

Les éléments inversibles de $\mathbb{K}[X]$ sont les éléments de $\mathbb{K}^*$ i.e. $\mathbb{K}[X]^\times = \mathbb{K}^*$.

c. Polynômes irréductibles

Définition 12. *Polynôme irréductible*

On dit que $A \in \mathbb{K}[X]$ est un **polynôme irréductible** dans $\mathbb{K}[X]$ si $\deg(A) \geq 1$ et :

$$B|A \quad \Rightarrow \quad B = \lambda \text{ ou } B = \lambda A \text{ avec } \lambda \in \mathbb{K}.$$

Remarque 7.

Ainsi, si $A = PQ$ avec $\deg(P) \geq 1$ et $\deg(Q) \geq 1$ alors A n'est pas irréductible dans $\mathbb{K}[X]$.

Exemple 6.

— $X^2 + X + 5$ et $X + 1$ 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 18.

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 !

d. Polynômes premiers entre eux

Définition 13. *Polynômes premiers entre eux*

Soit $A, B \in \mathbb{K}[X]$. On dit que A et B sont **premiers entre eux** si, pour $P \in \mathbb{K}[X]$

$$P|A \text{ et } P|B \quad \Rightarrow \quad P \in \mathbb{K}^*,$$

i.e. si les seuls diviseurs communs de A et B sont les polynômes constants non nuls.

Proposition 22.

Soit $A, B \in \mathbb{K}[X]$ tel B est irréductible. Alors A et B sont premiers entre eux si, et seulement si, B ne divise pas A.

Démonstration.

- ($\Rightarrow$). On raisonne par contraposée : si B divise A alors A et B ne sont pas premiers entre eux car B est un diviseur commun non constant de A et B.
- ($\Leftarrow$). On raisonne également par contraposée : on suppose A et B ne sont pas premiers entre eux. Alors ils admettent un diviseur commun non constant P. En particulier, P divise B et B est irréductible, donc il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda B$. Ainsi, comme $P|A$, il existe Q tel que :
$$A = PQ = \lambda BQ = B(\lambda Q),$$
donc $B|A$.

□

2. Idéaux de $\mathbb{K}[X]$

Théorème 11.

Les idéaux de $\mathbb{K}[X]$ sont les $P\mathbb{K}[X]$ pour $P \in \mathbb{K}[X]$.

Démonstration.

Pour $P \in \mathbb{K}[X]$, $P\mathbb{K}[X]$ est un idéal comme idéal engendré par P.

Soit I un idéal de $\mathbb{K}[X]$.

- *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 $p \in \mathbb{N}$. Soit $P \in I$ 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, on a l'inclusion voulue car pour tout $A \in \mathbb{K}[X]$, $PA \in I$.

  — $I \subset P\mathbb{K}[X]$. 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 $\deg(R) < P$ 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 $I = P\mathbb{K}[X]$.

□

Corollaire 6.

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

Définition 14.

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls.

— Le **PGCD** de A et B est le générateur unitaire de l'idéal $A\mathbb{K}[X] + B\mathbb{K}[X]$;

— Le **PPCM** de A et B est le générateur unitaire de l'idéal $A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

Exercice 19.

1. Soit I un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$. Montrer qu'il existe un unique polynôme unitaire P tel que $I = P\mathbb{K}[X]$.
2. En déduire que le PGCD et le PPCM de deux polynômes non nuls sont bien définis.

Correction.

1. Si I est un idéal de $\mathbb{K}[X]$ alors il existe $Q \in \mathbb{K}[X]$ tel que $I = Q\mathbb{K}[X]$. De plus, comme $I \neq \{0\}$, on a $Q \neq 0$ donc, en notant $q \in \mathbb{K}$ le coefficient dominant du polynôme Q, on a $q \neq 0$.
   Pour $P \in \mathbb{K}[X]$, on remarque : $Q\mathbb{K}[X] = P\mathbb{K}[X]$ si, et seulement si, $Q|P$ et $P|Q$ si, et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $P = \lambda Q$.
   Posons $P = \frac{1}{q}Q$. Alors, d'après la remarque précédente, $P\mathbb{K}[X] = Q\mathbb{K}[X] = I$ et P est unitaire. D'où l'existence.
   Pour l'unicité, si P, R sont unitaires et $P\mathbb{K}[X] = I = R\mathbb{K}[X]$ alors, toujours d'après la remarque, il existe $\lambda \in \mathbb{K}^*$ tel que $R = \lambda P$. Donc R et P sont de même degré et donc les coefficients dominants de R et λP sont égaux d'où $1 = \lambda \times 1$ i.e. $\lambda = 1$. Ainsi, $R = P$.
2. $A\mathbb{K}[X] + B\mathbb{K}[X]$ et $A\mathbb{K}[X] \cap B\mathbb{K}[X]$ sont des idéaux de $\mathbb{K}[X]$ donc d'après la question précédente, le PGCD et le PPCM sont bien définis.

Notation 3.

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls.

— On note $A \wedge B$ le PGCD de A et B ;

— On note $A \vee B$ le PPCM de A et B.

Proposition 23.

Soit $A, B, D, M, P \in \mathbb{K}[X]$ des polynômes non nuls avec D, M unitaires. Alors :

- $D = A \wedge B$ si, et seulement si, D vérifie les deux conditions :
  i) $D|A$ et $D|B$;

ii) si $P|A$ et $P|B$ alors $P|D$.

- $M = A \vee B$ si, et seulement si, M vérifie les deux conditions :
  i) $A|M$ et $B|M$;
  ii) si $A|P$ et $B|P$ alors $M|P$.

Démonstration.

On note $\mathcal{D} = A\mathbb{K}[X] + B\mathbb{K}[X]$ et $\mathcal{M} = A\mathbb{K}[X] \cap B\mathbb{K}[X]$.

- ($\Rightarrow$) . On suppose $D = A \wedge B$. Alors

$$\mathcal{D} = D\mathbb{K}[X],$$

donc $A\mathbb{K}[X] \subset D\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset D\mathbb{K}[X]$, d'où

$$D|A \text{ et } D|B.$$

et de plus, si $P|A$ et $P|B$ alors $A\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset P\mathbb{K}[X]$ et donc

$$D\mathbb{K}[X] = \mathcal{D} \subset P\mathbb{K}[X];$$

d'où $D|P$.

($\Leftarrow$) . On suppose i) et ii). $D|A$ et $D|B$ donc $A\mathbb{K}[X] \subset D\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset D\mathbb{K}[X]$. Ainsi,

$$\mathcal{D} \subset D\mathbb{K}[X].$$

De plus, comme $\mathcal{D}$ est principal, il existe P tel que $\mathcal{D} = P\mathbb{K}[X]$. Alors $A\mathbb{K}[X] \subset P\mathbb{K}[X]$ et $B\mathbb{K}[X] \subset P\mathbb{K}[X]$ et donc $P|A$ et $P|B$ d'où, d'après ii), $P|D$. Par suite, $D\mathbb{K}[X] \subset P\mathbb{K}[X] = \mathcal{D}$.

Il résulte que $D\mathbb{K}[X] = \mathcal{D}$ et comme D est unitaire, $D = A \wedge B$.

- ($\Rightarrow$) . On suppose $M = A \vee B$. Alors

$$\mathcal{M} = M\mathbb{K}[X],$$

donc $M\mathbb{K}[X] \subset A\mathbb{K}[X]$ et $M\mathbb{K}[X] \subset B\mathbb{K}[X]$, d'où

$$A|M \text{ et } B|M.$$

et de plus, si $A|P$ et $B|P$ alors $P\mathbb{K}[X] \subset A\mathbb{K}[X]$ et $P\mathbb{K}[X] \subset B\mathbb{K}[X]$ et donc

$$P\mathbb{K}[X] \subset \mathcal{M} = M\mathbb{K}[X];$$

d'où $M|P$.

($\Leftarrow$) . On suppose i) et ii). $A|M$ et $B|M$ donc $M\mathbb{K}[X] \subset A\mathbb{K}[X]$ et $M\mathbb{K}[X] \subset B\mathbb{K}[X]$. Ainsi,

$$M\mathbb{K}[X] \subset \mathcal{M}.$$

De plus, comme $\mathcal{M}$ est principal, il existe P tel que $\mathcal{M} = P\mathbb{K}[X]$. Alors $P\mathbb{K}[X] \subset A\mathbb{K}[X]$ et $P\mathbb{K}[X] \subset B\mathbb{K}[X]$ et donc $A|P$ et $B|P$ d'où, d'après ii), $M|P$. Par suite, $\mathcal{M} = P\mathbb{K}[X] \subset M\mathbb{K}[X]$.

Il résulte que $M\mathbb{K}[X] = \mathcal{M}$ et comme M est unitaire, $M = A \vee B$.

□

b. Relation de Bézout et algorithme d'Euclide

Proposition 24. *Relation de Bézout*

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls et $D = A \wedge B$. Alors il existe $U, V \in \mathbb{K}[X]$ tels que

$$D = AU + BV.$$

Démonstration.

On a $D \in D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$, donc il existe $U, V \in \mathbb{K}[X]$ tels que $D = AU + BV$. □

Proposition 25.

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls et R le reste de la division euclidienne de A par B. Alors

$$A \wedge B = B \wedge R.$$

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 $D = D'$. □

Théorème 12. *Algorithme d'Euclide pour les polynômes*

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls avec $\deg(A) \geq \deg(B)$ et $D = A \wedge B$. Alors la suite récurrente (R_n) :

$$\begin{cases} R_0 = A,\ R_1 = B; \\ R_{n+2} \text{ est le reste de la division euclidienne de } R_n \text{ par } R_{n+1} \end{cases}$$

est stationnaire en 0 et D est égal au polynôme unitaire associé à R_d où $d = \max\{n \in \mathbb{N} \mid R_n \neq 0\}$.

Démonstration.

Pour $n \in \mathbb{N}$, $\deg(R_{n+2}) < \deg(R_{n+1})$ et donc $\deg(R_{n+2}) \leq \deg(R_{n+1}) - 1$. Donc si $n = \deg(A)$, on a :

$\deg(R_{n+2}) < \deg(R_{n+1}) \leq \deg(R_n) - 1 \leq \deg(R_{n-1}) - 2 \leq \ldots \leq \deg(R_1) - n = \deg(B) - n \leq \deg(A) = n - n = 0,$

donc $\deg(R_{n+2}) = 0$.

De plus, par 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 :

$$U = R_d \wedge 0 = R_{d-1} \wedge R_d = R_{d-2} \wedge R_{d-1} = ... = R_0 \wedge R_1 = A \wedge B = D.$$

□

c. Lien avec les polynômes premiers entre eux

Proposition 26.

Soit $A, B \in \mathbb{K}[X]$ des polynômes non nuls. Alors A et B sont premiers entre eux si, et seulement si, $A \wedge B = 1$.

Démonstration.

On note $D = A \wedge B$.

- ($\Rightarrow$). On suppose A, B premiers entre eux. On a $D|A$ et $D|B$ alors $D \in \mathbb{K}^*$. Or D est unitaire, donc $D = 1$.
- ($\Leftarrow$). On suppose $D = 1$. Soit $P \in \mathbb{K}[X]$ tel que $P|A$ et $P|B$. D'après la relation de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. Par suite, $P|AU + BV = 1$ et donc $P \in \mathbb{K}^*$.

□

Théorème 13. *Théorème de Bézout pour les polynômes*

Soit $A, B \in \mathbb{K}[X]$ des polynômes. Alors A et B sont premiers entre eux si, et seulement si, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.

Démonstration.

On note $D = A \wedge B$.

- ($\Rightarrow$). On suppose A, B premiers entre eux. D'après la proposition précédente, $D = 1$. Donc, d'après la relation de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$.
- ($\Leftarrow$). On suppose qu'il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$. On a $D\mathbb{K}[X] = A\mathbb{K}[X] + B\mathbb{K}[X]$ donc $1 \in D\mathbb{K}[X]$. Alors $D\mathbb{K}[X]$ est un idéal qui contient l'unité de l'anneau, donc $D\mathbb{K}[X] = \mathbb{K}[X]$. Comme 1 est unitaire, $D = 1$.

□

Théorème 14. *Lemme de Gauss*

Soit $A, B, C \in \mathbb{K}[X]$. Si A et B sont premiers entre eux et si $A|BC$ alors $A|C$.

Démonstration.

D'après le théorème de Bézout, il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$, donc $C = AUC + BCV$. Or $A|BC$, donc $BCV, AUV \in A\mathbb{K}[X]$; d'où $C \in A\mathbb{K}[X]$. Par suite, $A|C$. □

4. Décomposition d'un polynôme en facteurs irréductibles

a. Décomposition en facteurs irréductibles

Proposition 27.

On a les propriétés suivantes :

- Tout polynôme de degré supérieur ou égal à 1 possède un diviseur irréductible.
- Si A est irréductible et $A|P_1...P_n$, alors il existe $i \in [\![1, n]\!]$ 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 divise 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 $P_1, ..., P_{n+1} \in \mathbb{K}[X]$ tels que $A|P_1...P_{n+1}$. Alors $A|(P_1...P_n)P_{n+1}$. 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, $A|P_1...P_n$. Par suite, par hypothèse de récurrence, il existe $i \in [\![1, n]\!]$ tel que $A|P_i$.

  Dans tous les cas, il existe $i \in [\![1, n+1]\!]$ 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 15. *Décomposition en facteurs irréductibles*

Soit $A \in \mathbb{K}[X]$ un polynôme non constant. Alors 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 $i, j \in [\![1, n]\!]$, $i \neq j$, 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 :

    $$B = \lambda P_1^{\alpha_1} ... P_i^{\alpha_i}$$

    d'où

    $$A = \lambda P_1^{\alpha_1} ... P_i^{\alpha_i} . P$$

    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 décomposition 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 $P_1 | \prod_{i=1}^{m} Q_i^{\beta_i}$ et P_1 est irréductible, alors il existe j tel que $P_1 | Q_j$. 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 $Q_2^{\alpha_2} ... Q_m^{\alpha_m}$ on a $P_1^{\alpha_1} | Q_1^{\beta_1}$, 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 $i = 2, 3, ...$
  Ainsi, les deux décompositions sont les mêmes.

□

b. Irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$

Théorème 16. *Théorème de D'Alembert-Gauss*

Tout polynôme non constant de $\mathbb{C}$ admet au moins un racine dans $\mathbb{C}$.

Proposition 28.

— 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 D

Algèbres

Dans toute cette partie, $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

1. Structure d'algèbre

Définition 15.

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.

Exemple 7.

— $(\mathbb{K}[X], \times)$ est une algèbre sur $\mathbb{K}$;

— si E est un espace vectoriel sur $\mathbb{K}$, $(\mathcal{L}(E), \circ)$ est une algèbre sur $\mathbb{K}$;

— $(M_n(\mathbb{K}), \times)$ est une algèbre sur $\mathbb{K}$;

— si X est un ensemble, $(\mathcal{F}(X, \mathbb{K}), \times)$ est une algèbre sur $\mathbb{K}$.

2. Sous-algèbres

Définition 16. *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 8.

— $\mathrm{Vect}(1_A)$ et A sont des sous-algèbres de A ;

— L'ensemble $T_n^+(\mathbb{K})$ des matrices triangulaires supérieures est une sous-algèbre de $M_n(\mathbb{K})$.

3. Morphismes d'algèbres

Définition 17. *Morphisme d'algèbre*

Soit A, B deux algèbres sur $\mathbb{K}$ et $f : A \to B$. On dit que f est un **morphisme d'algèbres** si :

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

Exemple 9.

— $\lambda \mapsto \lambda 1_A$ est un morphisme d'algèbres de $\mathbb{K}$ dans $\mathrm{Vect}(1_A)$;

— Pour $P \in GL_n(\mathbb{K})$, $M \mapsto PMP^{-1}$ est un morphisme d'algèbres de $M_n(\mathbb{K})$ dans lui-même.

Proposition 29.

Soit A, B deux algèbres sur $\mathbb{K}$ et $f : A \to B$ un morphisme d'algèbres. Alors

— Le noyau $\mathrm{Ker}(f)$ est un idéal de l'anneau $(A, +, \cdot)$

— L'image $\mathrm{Im}(f)$ est une sous-algèbre de B.

Démonstration.

— $\mathrm{Ker}(f)$ est un idéal de l'anneau $(A, +, \cdot)$ car c'est le noyau d'un morphisme d'anneaux.

— • $\mathrm{Im}(f)$ est un sous-anneau de B comme image de l'anneau A par le morphisme d'anneaux f.

• Il reste à montrer que $\mathrm{Im}(f)$ est stable par multiplication externe : soit $\lambda \in \mathbb{K}$ et $f(x) \in \mathrm{Im}(f)$ avec $x \in A$. Alors :

$$\lambda f(x) = f(\lambda x) \in \mathrm{Im}(f).$$

Donc $\mathrm{Im}(f)$ est une sous-algèbre de B.

□

4. Algèbres et polynômes

a. Polynômes appliqués à un élément d'une algèbre

Notation 4. *Polynôme d'un élément*

Soit A une algèbre sur $\mathbb{K}$, $u \in A$ et $P \in \mathbb{K}[X]$ avec $P = \sum_{i=0}^{n} a_i X^i$. On note $P(u)$ l'élément de A

$$P(u) = \sum_{i=0}^{n} a_i u^i = a_0 1_A + a_1 u + ... + a_n u^n.$$

Exemple 10.

— Soit E un espace vectoriel sur $\mathbb{K}$. Pour $f \in \mathcal{L}(E)$ et $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$,

$$P(f) = a_0 \mathrm{Id}_E + a_1 f + ... + a_n f^n;$$

— Soit $n \in \mathbb{N}^*$. Pour $M \in M_n(\mathbb{K})$ et $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{K}[X]$,

$$P(M) = a_0 I_n + a_1 M + ... + a_n M^n.$$

Proposition-Notation 30.

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$. L'application notée

$$f_u : \left| \begin{array}{ccc} \mathbb{K}[X] & \to & A \\ P & \mapsto & P(u) \end{array} \right.$$

est un morphisme d'algèbres.

Démonstration.

Soit $\lambda, \mu \in \mathbb{K}$, $P, Q \in \mathbb{K}[X]$. On a :

i)
$$\begin{aligned} f_u(\lambda P + \mu Q) &= (\lambda P + \mu Q)(u) \\ &= (\lambda P)(u) + (\mu Q)(u) \\ &= \lambda P(u) + \mu Q(u) \\ &= f_u(u) + f_u(u) \end{aligned}$$

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

Définition 18. *Idéal et polynôme annulateur*

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$. On appelle **idéal annulateur de** u l'ensemble

$$\mathrm{Ker}(f_u) = \{P \in \mathbb{K}[X] \mid P(u) = 0_A\}.$$

Un polynôme $P \in \mathbb{K}[X]$ est appelé **polynôme annulateur de** u s'il appartient à l'idéal annulateur de u i.e. si $P(u) = 0$.

On a montré dans la partie précédente que $\mathbb{K}[X]$ est un anneau principal. Ceci justifie la définition suivante :

Définition 19. *Polynôme minimal*

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$ d'idéal annulateur non réduit à 0_A. On appelle **polynôme minimal de** u et on note π_u le générateur unitaire de l'idéal annulateur de u.

Exemple 11.

Soit A une algèbre sur $\mathbb{K}$.

— 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 un **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) $\pi_u = X^2 - X$.
2) $\pi_u = X$, auquel cas $u = 0_A$
3) $\pi_u = X - 1$, auquel cas $u = 1_A$

Exercice 20.

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.
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.

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 $f^3 = \mathrm{Id}_{\mathbb{R}^3}$.
Par suite, $X^3 - 1$ est un polynôme annulateur de f.
Remarque : 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.
Remarque : 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. Algèbre engendrée par un élément

Notation 5.

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$. On note

$$\mathbb{K}[u] = \{P(u) \mid P \in \mathbb{K}[X]\}.$$

Proposition 31.

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$. Alors $\mathbb{K}[u]$ est une sous-algèbre *commutative* de A.

Démonstration.

On a $\mathbb{K}[u] = \mathrm{Im}(f_u)$ donc $\mathbb{K}[u]$ est une sous-algèbre de A comme image d'un morphisme d'algèbres. De plus, pour $P(u), Q(u) \in \mathbb{K}[u]$ avec $P, Q \in \mathbb{K}[X]$, on a :

$$P(u)Q(u) = (PQ)(u) = (QP)(u) = Q(u)P(u);$$

Donc $\cdot$ est commutative sur $\mathbb{K}[u]$. □

Proposition 32.

Soit A une algèbre sur $\mathbb{K}$ et $u \in A$. Si u admet un polynôme minimal $\pi_u \in \mathbb{K}[X]$ avec $d = \deg(\pi_u)$, alors $\mathbb{K}[u]$ est un espace vectoriel de dimension finie d et

$$\left(u^k\right)_{0 \leq k \leq d-1}$$

est une base de $\mathbb{K}[u]$.

Démonstration.

On suppose que u admet un polynôme minimal π_u avec $d = \deg(\pi_u)$. Montrons que $\left(u^k\right)_{0 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$.

- *Famille libre :* soit $\lambda_0, ..., \lambda_{d-1} \in \mathbb{K}$ des scalaires tels que $\sum_{k=1}^{d-1} \lambda_k u^k = 0_A$. Alors le polynôme $P = \sum_{k=1}^{d-1} \lambda_k X^k$ 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 $k \in [\![0, d-1]\!]$, $\lambda_k = 0$. Donc la famille $\left(u^k\right)_{0 \leq k \leq d-1}$ est libre.
- *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 $\lambda_0, ..., \lambda_{d-1} \in \mathbb{K}$ tels que $R = \sum_{k=1}^{d-1} \lambda_k X^k$. Il en résulte que :
$$P(u) = R(u) = \sum_{k=1}^{d-1} \lambda_k u^k \in \text{Vect}\left(u^k\right)_{0 \leq k \leq d-1}.$$
Et ainsi, $\left(u^k\right)_{0 \leq k \leq d-1}$ est génératrice.

Donc $\left(u^k\right)_{0 \leq k \leq d-1}$ est une base de $\mathbb{K}[u]$ et de plus, cette base comporte d vecteurs donc $\dim(\mathbb{K}[u]) = d$. □

Question 2.

Que dire de $\mathbb{K}[u]$ lorsque u n'admet pas de polynôme annulateur non nul ?

Correction.

Si u n'admet pas de polynôme annulateur, alors pour tout $P \in \mathbb{K}[X]$ avec $P \neq 0$, $P(u) \neq 0$, ce qui permet de montrer que la famille $\left(u^k\right)_{k \in \mathbb{N}}$ 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 $\left(u^k\right)_{0 \leq k \leq d-1}$ 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 21.

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 annulateur.
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 :
$$\begin{cases} 2^n = 2a + b \\ 3^n = 3a + b \end{cases} \Leftrightarrow \begin{cases} a = 3^n - 2^n \\ b = 3.2^n - 2.3^n \end{cases}$$
et donc on obtient :
$$A^n = Q(A)\underbrace{P(A)}_{=0_3} + R(A) = aA + b = (3^n - 2^n)A + (3.2^n - 2.3^n)I_3.$$

Proposition 33.

Soit A une algèbre sur $\mathbb{K}$ de dimension finie. Alors tout élément de A admet un polynôme minimal.

Démonstration.

Notons $n \in \mathbb{N}$ la dimension de A.
Soit $u \in A$. Montrons que u possède un polynôme annulateur non nul. La famille $(1_A, u, ..., u^n)$ est liée car composée de $n+1$ vecteurs dans un espace de dimension n. Ainsi, il existe $\lambda_0, ..., \lambda_n \in \mathbb{K}$ 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. □