Chapitre X : Structures algébriques

Retranscrit par Samy Youssoufine

6 février 2026

UM6P
University
Mohammed VI
Polytechnic

EMINES
School of Industrial Management

Note importante

Document Incomplet. Peut contenir des erreurs/sections incomplètes.

Table des matières

Ce chapitre est consacré aux structures algébriques. Il s'agit d'un chapitre d'introduction à l'algèbre. Elle occupera tout le deuxième semestre ainsi que le troisième semestre. Elle ne nécessite quasiment aucune connaissances préalable en analyse.

1 Groupes

1.1 Généralités

1.1.1 Magma

Définition 1.1.1.1 *(Magma)*

Soit E un ensemble non-vide.
On appelle un loi de composition interne dans E (LCI) tout application :

$$(*) : \begin{cases} E \times E \to E \\ (x, y) \mapsto x * y \end{cases}$$

C'est pour cela qu'on dit que c'est une loi de composition *interne* : on associe à deux éléments de E un élément de E (on reste dans E).
Dans ce cas, $(E, *)$ est appelé **magma**.

Exemple 1.1.1.1

1. $+$ est une LCI dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
2. $-$ n'est pas une LCI dans $\mathbb{N}$ car par exemple $2 - 3 = -1 \notin \mathbb{N}$.
3. $\times$ est une LCI dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

Définition 1.1.1.2

Soit G un ensemble non-vide muni d'une LCI $*$.
On dit que :

1. $*$ est **associative** si $\forall (x, y, z) \in G^3$, on a $(x * y) * z = x * (y * z)$.
2. $*$ admet un **élément neutre** dans G s'il existe $e \in G$ tel que

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

3. $x \in G$ admet un **symétrique** pour $*$ s'il existe $y \in G$ tel que

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

où e est l'élément neutre de G. On dit que x est **symétrisable** pour $*$. On appelle y le **symétrique** de x pour $*$, et on le note x^{-1} ou $-x$ si $*$ est additive.

4. $*$ est **commutative** si $\forall (x, y) \in G^2$, on a $x * y = y * x$.

Remarque 1.1.1.1

On peut toujours noter le symétrique de x par x^{-1}, mais on utilise la notation $-x$ uniquement lorsque la loi est additive (pour simplifier les écritures). On dit qu'une loi est additive si elle agit d'une manière similaire à l'addition usuelle.

Attention

Il faut faire attention à la terminologie utilisée. On associe de préférence l'élément neutre à la loi dans l'ensemble. On ne dit pas, par exemple, que 0 est l'élément neutre de $\mathbb{R}$, mais plutôt que 0 est l'élément neutre de la loi $+$ dans $\mathbb{R}$, ou que c'est l'élément neutre de $\mathbb{R}$ pour la loi $+$.

1.1.2 Groupes

Définition 1.1.1.3 *(Groupe)*

Soit G un ensemble non-vide muni d'une LCI $*$.
On dit que $(G, *)$ est un **groupe** si :

1. $*$ est associative.
2. $*$ admet un élément neutre dans G.
3. Tout élément de G est symétrisable pour $*$.

Si de plus $*$ est commutative, on dit que $(G, *)$ est un **groupe commutatif** (abélien).

Méthode

Pour montrer que $(G, *)$ est un groupe, on commence par vérifier que $*$ est une loi de composition interne dans G. Ensuite, on vérifie l'associativité, l'existence d'un élément neutre, et enfin que tout élément de G est symétrisable pour $*$.
Si on veut montrer que $(G, *)$ est un groupe commutatif, on vérifie que $*$ est commutative juste après avoir montré qu'elle est associative, pour ne montrer qu'une seule égalité et éviter les répétitions.

Propriété 1.1.1.1

Soit $(E, *)$ un magma tel que $*$ admet un élément neutre e.

1. e est unique.
2. Si $*$ est associative, et $a \in E$ est symétrisable, alors le symétrique est unique ; i.e. $\exists! b \in G, a * b = b * a = e$.

Preuve

1. Supposons qu'il existe deux éléments neutres e et e'. Alors, par définition de l'élément neutre, on a $e * e' = e$ et $e * e' = e'$. Donc, $e = e'$.
2. Soit $a \in G$ symétrisable, et supposons qu'il existe deux symétriques b et b' de a. Alors, par définition du symétrique, on a $a * b = e$ et $a * b' = e$. En multipliant à gauche par b' dans la première égalité, on obtient :

$$b' * (a * b) = b' * e \implies (b' * a) * b = b'.$$

En utilisant l'associativité, on a :

$$e * b = b' \implies b = b'.$$

■

Exemple 1.1.1.2

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ est un groupe commutatif.
- Soit E un ensemble de cardinal $\text{card}(E) > 2$. On note S_E l'ensemble des applications bijectives de E vers E. On munit S_E par la loi $\circ$ (composition), i.e. $\forall f, g \in S_E, f \circ g : \begin{cases} E \to E \\ x \to f(g(x)) \end{cases}$
  Alors, $(S_E, \circ)$ est un groupe non commutatif.

Pour montrer que $(S_E, \circ)$ est un groupe, on vérifie si :

- $\circ$ est une LCI dans S_E :
  Soit $f, g \in S_E$. Comme f et g sont bijectives, alors $f \circ g$ est bijective, et $f \circ g : E \to E$. Donc, $f \circ g \in S_E$. Donc, $\circ$ est une LCI dans S_E.
- $\circ$ est associative :
  Soit $f, g, h \in S_E$. Montrons que $(f \circ g) \circ h = f \circ (g \circ h)$.
  Pour montrer que deux applications sont égales, il suffit de montrer que leurs images sont égales (pour tout x de leur ensemble de départ).
  Soit $x \in E$. On a $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$.
  De même, on a $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$.
  Donc, $(f \circ g) \circ h = f \circ (g \circ h)$.
  Note : il est parfaitement possible des les calculer plus rapidement, mais cette méthode est plus "rigoureuse" et "sécurisée".

- $\circ$ admet un élément neutre dans S_E :
  On pose $id_E : \begin{cases} E \to E \\ x \to x \end{cases}$
  Soit $f \in S_E$. On a $f \circ id_E = f$ et $id_E \circ f = f$. Donc, id_E est l'élément neutre de $\circ$ dans S_E.
- $\forall f \in S_E, f$ admet une bijection réciproque $f^{-1} \in S_E$ telle que $f \circ f^{-1} = id_E$ et $f^{-1} \circ f = id_E$. Donc, tout élément de S_E est symétrisable pour $\circ$.
- On peut déjà conclure que $(S_E, \circ)$ est un groupe. Montrons que ce n'est pas un groupe commutatif.
- $\circ$ n'est pas commutative. On procède à la démonstration par contre-exemple (méthode classique). On pose $E = \{x_1, x_2, x_3\}$ de cardinal $3 > 2$. On définit $f, g \in S_E$ par :

$$f : \begin{cases} x_1 \to x_2 \\ x_2 \to x_3 \\ x_3 \to x_1 \end{cases} \quad , \quad g : \begin{cases} x_1 \to x_3 \\ x_2 \to x_1 \\ x_3 \to x_2 \end{cases}$$

  Après calculs, on trouve que $(f \circ g)(x_2) = x_3 \neq (g \circ f)(x_2) = x_1$. Donc, $f \circ g \neq g \circ f$. Donc, $\circ$ n'est pas commutative.

On conclut que $(S_E, \circ)$ est un groupe non commutatif.

Remarque 1.1.1.2

1. Lorsque $E = \{1, \ldots, n\}$ tel que $n \in \mathbb{N}^*$, alors S_E est noté par S_n.
   Et $\forall f \in S_n$, f est appelée une **permutation** de $\{1, \ldots, n\}$, et notée par $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$.
   Le cardinal de S_n est $n!$ (factorielle de n).
2. $(S_E, \circ)$ est un groupe non commutatif dès que $\text{card}\,(E) > 2$. Par contre, si $\text{card}\,(E) = 2$, alors $(S_E, \circ)$ est un groupe commutatif isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$.

Propriété 1.1.1.2

Soient $(G, *)$ un groupe, $a, b \in G$.
Alors $(a * b)^{-1} = b^{-1} * a^{-1}$.

Preuve

$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$. De même, $(b^{-1} * a^{-1}) * (a * b) = e$. On en déduit que $(a * b)^{-1} = b^{-1} * a^{-1}$. ■

Exercice 1.1.1.1

Soit $(G, *)$ un groupe tel que $\forall x \in G, x * x = e$. Montrer que G est un groupe commutatif.

1.1.3 Sous-groupes

Définition 1.1.1.4 *(Sous-groupe)*

Soit $(G, *)$ un groupe et $H \subset G$. On dit que $(H, *)$ est un **sous-groupe** de $(G, *)$ si et seulement si :

1. H est non-vide.
2. H est stable par $* : \forall x, y \in H, x * y \in H$.
3. $\forall x \in H, x^{-1} \in H$.

Propriété 1.1.1.3 *(Caractérisation d'un sous-groupe)*

Soient $(G, *)$ un groupe et H une partie de G.
On peut dire que :

$$H \text{ est un sous-groupe de } (G, *) \iff \begin{cases} H \neq \emptyset \\ \forall x, y \in H, x * y^{-1} \in H \end{cases}$$

Preuve

- **Démonstration dans le sens direct $\implies$:** Trivial (mais à refaire).
- **Démonstration dans le sens réciproque $\impliedby$:**
  - On a $H \neq \emptyset$.
  - Donc $\exists a \in H$.
  - On a $a * a^{-1} = \boxed{e_G \in H}$.
    - H contient l'élément neutre de G.
  - On a $\forall x \in H, e_G * x^{-1} = x^{-1} \in H$.
  - Soient $x, y \in H$. Alors, $y^{-1} \in H$.
  - Donc, $x * y = x * (y^{-1})^{-1} \in H$.
    - C'est-à-dire que H est stable par $*$.
  - H est donc un sous-groupe de $(G, *)$.

■

Remarque 1.1.1.3

1. Si H est un sous-groupe de $(G, *)$, alors l'élément neutre de H est l'élément neutre de G.
2. Tout sous-groupe d'un groupe est lui-même un groupe.

Propriété 1.1.1.4 ***(Sous-groupes triviaux)***

Soit $(G, *)$ un groupe.
Alors, $\{e_G\}$ et G sont des sous-groupes de $(G, *)$, appelés **sous-groupes triviaux** de $(G, *)$.

Exemple 1.1.1.3

- $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$.
- $(\{-1, 1\}, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$.
- On pose $\mathbb{Z}[i] = \{a + ib \text{ tels que } a, b \in \mathbb{Z}\}$ (Entiers de Gauss). Et on pose $\mathbb{Z}[j] = \{a + jb \text{ tels que } a, b \in \mathbb{Z}\}$, avec $j = e^{i\frac{\pi}{3}}$. (Entiers de Eisenstein). Alors, $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$ sont des sous-groupes de $(\mathbb{C}, +)$.

Propriété 1.1.1.5

Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Preuve

Pour démontrer ça, on commence par vérifier que $n\mathbb{Z}$ est bien un sous-groupe de $(\mathbb{Z}, +)$ pour tout $n \in \mathbb{N}$. Ensuite, on montre que si H est un sous-groupe quelconque de $(\mathbb{Z}, +)$, alors il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

- $\forall n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
  - $n\mathbb{Z} \subset \mathbb{Z}$ car $\forall k \in \mathbb{Z}, nk \in \mathbb{Z}$.
  - $n\mathbb{Z} \neq \emptyset$ car $0 \in n\mathbb{Z}$.
  - Soient $a, b \in n\mathbb{Z}$.
    - $\exists k, l \in \mathbb{Z}$ tels que $a = nk$ et $b = nl$.
    - Donc, $a - b = n(k - l) \in n\mathbb{Z}$.
  - Donc, $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$.
- Soit H un sous-groupe quelconque de $(\mathbb{Z}, +)$, non réduit au singleton $\{0\}$.
  - On pose $H^+ = H \cap \mathbb{N}^*$.
  - $H^+ \neq \emptyset$ car $H \neq \{0\}$ et H est stable par l'opposé.
  - En effet, H est un sous-groupe, alors $-a \in H$ pour tout $a \in H$.
  - Donc a et $-a \in H \implies H^+ \neq \emptyset$.

▷ On a $H^+ \subset \mathbb{N}^*$, donc H^+ admet un minimum n.
— Nous allons essayer de montrer que $H = n\mathbb{Z}$.
▷ On a $n \in H$, donc $nk = \begin{cases} \underbrace{n + \cdots + n}_{k \text{ fois}} \text{ pour } k \geq 0 \\ \underbrace{-(n + \cdots + n)}_{k \text{ fois}} \text{ pour } k \leq 0 \end{cases} \in H$.
▷ Donc $x \in H$, i.e. $n\mathbb{Z} \subset H$.
▷ Soit $a \in H$.
— Par le théorème de la division euclidienne, il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = nq + r$ et $0 \leq r < n$.
— Or, $nq \in H$ (car $n\mathbb{Z} \subset H$) et $a \in H$, donc $r = a - nq \in H$ (car H est stable par l'opposé et par l'addition).
— Si $r \neq 0$, alors $r \in H^+$ et $r < n$, ce qui contredit la minimalité de n.
— Donc, $r = 0$, et ainsi $a = nq \in n\mathbb{Z}$.
▷ Donc, $H \subset n\mathbb{Z}$.
▷ On en déduit que $H = n\mathbb{Z}$.

■

Remarque 1.1.1.4

Les sous-groupes de $(\mathbb{R}, +)$ sont ou bien denses dans $\mathbb{R}$, ou bien de la forme $a\mathbb{Z}$ avec $a > 0$ (Traité dans le DS nř2 d'octobre 2025).

Propriété 1.1.1.6

Soit $(G, *)$ un groupe.

1. Si $H_{i_{i\in I}}$ est une famille de sous-groupes de $(G, *)$, alors l'intersection $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G, *)$.
2. $H \cup K$ est un sous-groupe de $(G, *)$ si et seulement si $H \subset K$ ou $K \subset H$.

Preuve

▶ **Démonstration de 1. :**
▷ $\forall i \in I, H_i \subset G \implies \bigcap_{i\in I} H_i \subset G$.
▷ $\forall i \in I, H_i \neq \emptyset \implies \bigcap_{i\in I} H_i \neq \emptyset$ (car $e \in H_i$).
▷ Soient $a, b \in \bigcap_{i\in I} H_i$.
▷ Alors $\forall i \in I, a, b \in H_i \implies \forall i \in I, a * b^{-1} \in H_i$ (car H_i est un sous-groupe).
▷ Donc, $a * b^{-1} \in \bigcap_{i\in I} H_i$.
▷ Donc, $\bigcap_{i\in I} H_i$ est un sous-groupe de $(G, *)$.
▶ **Démonstration de 2. :**

- ▷ Dans le sens indirect ($\Longleftarrow$), la démonstration est triviale.
- ▷ Dans le sens direct ($\Longrightarrow$), on procède par absurde. On admet que $H \not\subset K$ et $K \not\subset H$.
- ▷ Donc $\exists h \in H, h \notin K$ et $\exists k \in K, k \notin H$.
- ▷ On a $h, k \in H \cup K \implies h * k \in H \cup K$ (car H et K sont des sous-groupes).
- ▷ Si $h * k \in H$, alors $\exists h_1 \in H$ tel que $h * k = h_1$.
  - — Donc $k = h^{-1} * h_1 \in H$ (car H est stable par $*$ et par l'inverse). (On compose à gauche !)
  - — Ce qui est absurde.
- ▷ Si $h * k \in K$, alors $\exists k_1 \in K$ tel que $h * k = k_1$.
  - — Donc $h = k_1 * k^{-1} \in K$ (car K est stable par $*$ et par l'inverse). (On compose à droite !)
  - — Ce qui est absurde.
- ▷ On en déduit que $H \subset K$ ou $K \subset H$.

■

Propriété 1.1.1.7 ***(Groupe des applications à valeurs dans un groupe)***

Soit $(G, *)$ un groupe et D un ensemble non-vide.
On note G^D l'ensemble des applications de D vers G.
Alors $(G^D, \star)$ est un groupe, où $\star$ est définie par :

$$\forall f, g \in G^D, \quad f \star g : \begin{cases} D \to G \\ x \mapsto f(x) * g(x) \end{cases}$$

Remarque 1.1.1.5

On se permet de noter les deux lois de la même manière ($*$ et $\star$) lorsqu'il n'y a pas d'ambiguïté possible. Dans le cours manuscrit, on entoure $\star$ d'un cercle coloré pour le différencier.

Attention

$\star$ est définie de manière "naturelle" à partir de $*$. On l'utilise pour effectuer des opérations sur des *applications* à valeurs dans un groupe, tandis que $*$ est utilisée pour effectuer des opérations sur des *éléments* du groupe.

Preuve

▶ **Démonstration que $\star$ est une LCI dans G^D :**

- ▷ On a $\forall f, g \in G^D, (f \star g)(x) = f(x) * g(x) \in G$ (car $*$ est une LCI dans G).

- ▷ Donc $f \star g \in G^D$.
- ▷ D'où $\star$ est une LCI dans G^D.

▶ **Démonstration que $\star$ est associative :**

- ▷ Soient $f, g, h \in G^D, x \in D$.
- ▷ On a $((f \star g) \star h)(x) = (f \star g)(x) * h(x) = (f(x) * g(x)) * h(x)$.
- ▷ De même, on a $(f \star (g \star h))(x) = f(x) * (g \star h)(x) = f(x) * (g(x) * h(x))$.
- ▷ Or, $*$ est associative dans G, donc $(f(x) * g(x)) * h(x) = f(x) * (g(x) * h(x))$.
- ▷ Donc, $((f \star g) \star h)(x) = (f \star (g \star h))(x)$.
- ▷ Donc, $(f \star g) \star h = f \star (g \star h)$.
- ▷ Donc, $\star$ est associative.

▶ **Démonstration de l'existence d'un élément neutre :**

- ▷ On pose $e : \begin{cases} D \to G \\ x \mapsto e_G \end{cases}$, où e_G est l'élément neutre de G.
- ▷ Soit $f \in G^D, x \in D$.
- ▷ On a $(f \star e)(x) = f(x) * e_G = f(x)$, car $f(x) \in G$.
- ▷ De même, on a $(e \star f)(x) = e_G * f(x) = f(x)$, car $f(x) \in G$.
- ▷ Donc, $f \star e = f$ et $e \star f = f$.
- ▷ Donc, e est l'élément neutre de $\star$ dans G^D.

▶ **Démonstration que tout élément de G^D est symétrisable pour $\star$:**

- ▷ Soit $f \in G^D$.
- ▷ On pose $f' : \begin{cases} D \to G \\ x \mapsto f(x)^{-1} \end{cases} \in G^D$, où $f(x)^{-1}$ est le symétrique de $f(x)$ pour $*$ dans G.
- ▷ On a $\forall x \in D, (f \star f')(x) = f(x) * f(x)^{-1} = e_G = e(x)$.
- ▷ De même, on a $\forall x \in D, (f' \star f)(x) = f(x)^{-1} * f(x) = e_G = e(x)$.
- ▷ Donc, $f \star f' = e$ et $f' \star f = e$.
- ▷ Donc, f est symétrisable pour $\star$.
- ▷ Donc, tout élément de G^D est symétrisable pour $\star$.

▶ On en déduit que $(G^D, \star)$ est un groupe.

■

Remarque 1.1.1.6

Si $(G, *)$ est un groupe abélien, alors $(G^D, \star)$ est aussi un groupe abélien.

Exemple 1.1.1.4

- Soit I un intervalle de $\mathbb{R}$ non-vide. Alors, $(\mathbb{R}^I, +)$ est un groupe abélien, où $+$ est définie par : $\forall f, g \in \mathbb{R}^I, f + g : x \mapsto f(x) + g(x)$.
- $(\mathbb{C}^{\mathbb{N}}, +)$ est un groupe abélien, où $+$ est définie par : $\forall (u_n), (v_n) \in \mathbb{C}^{\mathbb{N}}, (u_n)+(v_n) : (n \mapsto u_n + v_n)$.

1.2 Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$

Définition 1.1.2.5 *(Rappel de la relation d'équivalence)*

Une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'équivalence si :

1. $\forall x \in E, x\mathcal{R}x$ (réflexivité).
2. $\forall (x, y) \in E^2, x\mathcal{R}y \implies y\mathcal{R}x$ (symétrie).
3. $\forall (x, y, z) \in E^3, x\mathcal{R}y$ et $y\mathcal{R}z \implies x\mathcal{R}z$ (transitivité).

1.2.1 Classes d'équivalence et partition

Définition 1.1.2.6 *(Classes d'équivalence)*

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E.
Pour tout $x \in E$, on appelle **classe d'équivalence** de x pour $\mathcal{R}$ l'ensemble :

$$\mathcal{C}\ell(x) = \{y \in E \text{ tel que } y\mathcal{R}x\}$$

Propriété 1.1.2.8

$\forall x, y \in E, x\mathcal{R}y \iff \mathcal{C}\ell(x) = \mathcal{C}\ell(y)$.
i.e. deux éléments sont en relation si et seulement si leurs classes d'équivalence sont égales.

Preuve

- **Démonstration dans le sens réciproque $\impliedby$:** On a $x \in \mathcal{C}\ell(x) = \mathcal{C}\ell(y)$, donc $x \in \mathcal{C}\ell(y)$, i.e. $x\mathcal{R}y$.
- **Démonstration dans le sens direct $\implies$:** Soit $z \in \mathcal{C}\ell(x)$. Alors, $z\mathcal{R}x$ et $x\mathcal{R}y$, donc $z\mathcal{R}y$ (par transitivité). Donc, $z \in \mathcal{C}\ell(y)$. Ainsi, $\mathcal{C}\ell(x) \subset \mathcal{C}\ell(y)$. De même, on montre que $\mathcal{C}\ell(y) \subset \mathcal{C}\ell(x)$. Donc, $\mathcal{C}\ell(x) = \mathcal{C}\ell(y)$.

■

Propriété 1.1.2.9

Si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, alors les classes d'équivalence forment **une partition** de E.
i.e. : Elles sont non-vides, disjointes deux à deux, et leur réunion est égale à E.

Preuve

- $\forall x \in E, x \in \mathcal{C}\ell(x) \implies \mathcal{C}\ell(x) \neq \emptyset$.
- Soient $x, y \in E$ tels que $\mathcal{C}\ell(x) \neq \mathcal{C}\ell(y)$.
  Soit $z \in \mathcal{C}\ell(x) \cap \mathcal{C}\ell(y)$. Alors, $z\mathcal{R}x$ et $z\mathcal{R}y$, donc $x\mathcal{R}y$ (par symétrie et transitivité). Donc, $\mathcal{C}\ell(x) = \mathcal{C}\ell(y)$, ce qui est absurde. Donc, $\mathcal{C}\ell(x) \cap \mathcal{C}\ell(y) = \emptyset$.
- Montrons que $\bigcup_{x\in E} \mathcal{C}\ell(x) = E$.
  On a $\forall x \in E, \mathcal{C}\ell(x) \subset E$, donc $\bigcup_{x\in E} \mathcal{C}\ell(x) \subset E$.
  Soit $y \in E$. On a $y \in \mathcal{C}\ell(y)$, donc $y \in \bigcup_{x\in E} \mathcal{C}\ell(x)$. Donc, $E \subset \bigcup_{x\in E} \mathcal{C}\ell(x)$.
  On en déduit que $\bigcup_{x\in E} \mathcal{C}\ell(x) = E$.

■

Remarque 1.1.2.7

On a déjà montré que "$\cdot \equiv \cdot[n]$" est une relation d'équivalence sur $\mathbb{Z}$ (Chapitre IX).
Pour tout $x \in \mathbb{Z}$, on note $\mathcal{C}\ell(x)$ par $\overline{x}$, et l'ensemble des classes d'équivalence par $\mathbb{Z}/n\mathbb{Z} = \{\mathcal{C}\ell(x) \text{ tel que } x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Proposition 1.1.2.1

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien, où $+$ est définie par :

$$\forall \overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}, \quad \overline{a} + \overline{b} = \overline{a+b}$$

Preuve

Montrons que $+$ est bien définie.
$+$ est bel et bien définie si et seulement si elle ne dépend pas du choix du représentant de la classe d'équivalence.
Soient $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ dans $\mathbb{Z}/n\mathbb{Z}$.
Donc $x \equiv x'[n]$ et $y \equiv y'[n]$.
i.e. $\exists k_1, k_2 \in \mathbb{Z}$ tels que $x' = x + k_1 n$ et $y' = y + k_2 n$.
Donc $x + y = x' + y' - (k_1 + k_2)n$. Donc $x + y \equiv x' + y'[n]$. Donc, $\overline{x+y} = \overline{x'+y'}$. ■

MQ GRP ABE-LIEN Z/NZ 21/01

1.2.2 Groupe engendré par une partie

Définition 1.1.2.7 *(Groupe engendré)*

Soit $(G, \cdot)$ un groupe et $A \subset G$.
On appelle **groupe engendré** par A le plus petit sous-groupe de $(G, \cdot)$, soit $\bigcap_{\substack{H \text{ s.g. de } G \\ A \subset H}} H$, contenant A, noté $\langle A \rangle$.

Exemple 1.1.2.5

1. Si $A = \emptyset$, alors $\langle A \rangle = \{e_G\}$, parce que c'est le plus petit sous-groupe de $(G, \cdot)$.
2. Si A est un sous-groupe de $(G, \cdot)$, alors $\langle A \rangle = A$.
3. Si $A = \{a\}$ avec $a \in G$, alors $\langle A \rangle = \{a^n \text{ tel que } n \in \mathbb{Z}\}$, avec $a^0 = e_G$ et $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ fois}}$ pour $n > 0$, ou $a^n = \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-n \text{ fois}}$ pour $n < 0$. On le note aussi par $\langle a \rangle$.

Définition 1.1.2.8 *(Groupes monogènes et groupes cycliques)*

Soit $(G, \cdot)$ un groupe.

1. On dit que $(G, \cdot)$ est un **groupe monogène** s'il existe $a \in G$ tel que $G = \langle a \rangle$, et on dit que a est un **générateur** de G.
2. On dit que $(G, \cdot)$ est un **groupe cyclique** s'il existe $A \subset G$ fini tel que $G = \langle A \rangle$.

Exemple 1.1.2.6

1. $(\mathbb{Z}, +)$ est un groupe monogène, engendré par 1 (ou -1).
2. $\mathbb{U}_n = \{z \in \mathbb{C} \text{ tel que } |z| = 1\}$ est un groupe cyclique, engendré par $e^{i\frac{2\pi}{n}} = \omega$. Donc $\mathbb{U}_n = \langle \omega \rangle = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.

Définition 1.1.2.9

Soient $(G, \cdot)$ un groupe et $a \in G$.
Si $\langle a \rangle$ est un groupe fini, on appelle **ordre** de a dans G le cardinal de $\langle a \rangle$, noté par $o(a) = \text{card}(\langle a \rangle)$.

Exemple 1.1.2.7

▶ Pour $(\mathbb{Z}/6\mathbb{Z}, +)$, on a $o(\overline{2}) = 3$ car $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$, et on a $o(\overline{3}) = 2$, et $o(\overline{5}) = 6$.

qqch sur les générateurs ici ☹

Propriété 1.1.2.10

Soit $(G, \cdot)$ un groupe fini d'élément neutre e. Alors, $\forall a \in G, o(a) = \min(\{k \in \mathbb{N}^* \text{ tel que } a^k = e\})$.

Preuve

- On pose $A = \{k \in \mathbb{N}^* \text{ tel que } a^k = e\}$. Montrons que $A \neq \emptyset$ et qu'il admet un minimum.
  - On a $\langle a \rangle = \{a^n \text{ tel que } n \in \mathbb{Z}\} \subset G$ est fini.
  - Donc l'application $\psi : \begin{cases} \overbrace{\mathbb{Z}}^{\text{infini}} \to \overbrace{\langle a \rangle}^{\text{fini}} \\ n \mapsto a^n \end{cases}$ n'est pas injective.
    - *Si l'application était injective, alors on aurait une infinité d'éléments dans $\langle a \rangle$, ce qui est absurde, car $\langle a \rangle$ est fini.*
  - Donc $\exists k_1, k_2 \in \mathbb{Z}$ tel que $a^{k_1} = a^{k_2}$ et $k_1 \neq k_2$.
  - Donc $a^{|k_1 - k_2|} = e$.
  - Donc $|k_1 - k_2| \in A$, donc $A \neq \emptyset$.
  - En plus, $A \subset \mathbb{N}^*$, donc A admet un minimum. On pose $S = \min(A)$.
- Montrons que $\langle a \rangle = \{e, a, a^2, \ldots, a^{S-1}\}$.
  - On pose $H = \{e, a, a^2, \ldots, a^{S-1}\}$.
  - On a $H \subset \langle a \rangle$.
  - Soit $x \in \langle a \rangle$, donc $\exists n \in \mathbb{Z}$ tel que $x = a^n$.
  - Par le théorème de la division euclidienne, il existe $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $n = qS + r$ et $0 \leq r < S$.
  - Donc, $x = a^n = a^{qS+r} = (a^S)^q * a^r = e^q * a^r = a^r$, sachant que $a^S = e$ (car $S \in A$).
  - Donc, $x \in H$.

■

Méthode

En pratique, pour chercher l'ordre d'un élément a dans un groupe fini $(G, \cdot)$, on ne cherche pas à calculer tous les éléments de $\langle a \rangle$, mais on cherche le plus petit entier $k \geq 1$ tel que $a^k = e$.

1.3 Théorème de Lagrange

Théorème 1.1.3.1 ***(Théorème de Lagrange)***

Soit $(G, \cdot)$ un groupe fini et $(H, \cdot)$ un sous-groupe de $(G, \cdot)$.
Alors, $\text{card}\,(H)$ divise $\text{card}\,(G)$ (on note $\text{card}\,(H) \mid \text{card}\,(G)$).

Preuve

Soit H un sous-groupe de $(G, \cdot)$.
On définit une relation binaire $\mathcal{R}$ sur G par : $\forall x, y \in G, x\mathcal{R}y \iff x^{-1} \cdot y \in H$.

- Montrons que $\mathcal{R}$ est une relation d'équivalence.
  - **Réflexivité :** Soit $x \in G$. On a $x^{-1} \cdot x = e_G \in H$, donc $x\mathcal{R}x$.
  - **Symétrie :** Soient $x, y \in G$ tels que $x\mathcal{R}y$. Donc, $x^{-1} \cdot y \in H$. Donc, $(x^{-1} \cdot y)^{-1} = y^{-1} \cdot x \in H$ (car H est stable par l'inverse). Donc, $y\mathcal{R}x$.
  - **Transitivité :** Soient $x, y, z \in G$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Donc, $x^{-1} \cdot y \in H$ et $y^{-1} \cdot z \in H$. Donc, $(x^{-1} \cdot y) \cdot (y^{-1} \cdot z) = x^{-1} \cdot z \in H$ (car H est stable par $\cdot$). Donc, $x\mathcal{R}z$.
- On en déduit que $\mathcal{R}$ est une relation d'équivalence sur G.
- Soit $\mathcal{C}\ell\,(x)$ la classe d'équivalence de $x \in G$ pour la relation $\mathcal{R}$.
  - On a $\mathcal{C}\ell\,(x) = \{y \in G \text{ tel que } x^{-1} \cdot y \in H\} = \{x \cdot h \text{ tel que } h \in H\}$.
- On montre que toutes les classes d'équivalence ont le même cardinal que H.
  - Soit $x \in G$. On définit l'application $\varphi : \begin{cases} H \to \mathcal{C}\ell\,(x) \\ h \mapsto x \cdot h \end{cases}$.
  - Montrons que φ est une bijection.
    - **Injectivité :** Soient $h_1, h_2 \in H$ tels que $\varphi(h_1) = \varphi(h_2)$. Donc, $x \cdot h_1 = x \cdot h_2$. Donc, $h_1 = h_2$ (en composant à gauche par x^{-1}). Donc, φ est injective.
    - **Surjectivité :** Soit $y \in \mathcal{C}\ell\,(x)$. Donc, $\exists h \in H$ tel que $y = x \cdot h$. Donc, $\varphi(h) = y$. Donc, φ est surjective.
  - On en déduit que φ est une bijection.
  - Donc, $\text{card}\,(\mathcal{C}\ell\,(x)) = \text{card}\,(H)$.
- Soit $\{\mathcal{C}\ell\,(x_i)\}_{i \in I}$ l'ensemble des classes d'équivalence de G pour la relation $\mathcal{R}$.
  - On a $\bigcup_{i \in I} \mathcal{C}\ell\,(x_i) = G$ et les $\mathcal{C}\ell\,(x_i)$ sont disjointes deux à deux.
  - Donc, $\text{card}\,(G) = \sum_{i \in I} \text{card}\,(\mathcal{C}\ell\,(x_i))$.
  - Donc, $\text{card}\,(G) = \sum_{i \in I} \text{card}\,(H) = \text{card}\,(H) \cdot \text{card}\,(I)$.
- On en déduit que $\text{card}\,(H) \mid \text{card}\,(G)$.

■

→ Conséquence 1.1.3.1

1. Si $(G, \cdot)$ est un groupe fini de cardinal premier, alors ses seuls sous-groupes sont les sous-groupes triviaux $\{e_G\}$ et G. Dans ce cas, on dit que G est un **groupe simple**. Par exemple, $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe simple pour tout p premier, sachant que le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est n.
2. Soit $(G, \cdot)$ un groupe fini tel que $\text{card}\,(G) = n \in \mathbb{N}^*$. On a $\langle a \rangle$ est un sous-groupe de G, donc $o(a) = \text{card}\,(\langle a \rangle)$ divise n, d'après le théorème de Lagrange. Or, on a $a^{o(a)} = e_G$. Donc, $a^n = e_G$.
3. Si G est un sous-groupe de $(\mathbb{C}^*, \times)$ tel que $\text{card}\,(G) = n \in \mathbb{N}^*$, alors $\forall z \in G, z^n = 1$. Donc $G \subset \mathbb{U}_n = \{z \in \mathbb{C} \text{ tel que } |z| = 1\}$. Or $\text{card}\,(\mathbb{U}_n) = n = \text{card}\,(G)$. Donc, $G = \mathbb{U}_n$, vu qu'il s'agit de deux ensembles finis de même cardinal tels que $G \subset \mathbb{U}_n$. Cela veut dire que le seul sous-groupe de $(\mathbb{C}^*, \times)$ de cardinal n est $\mathbb{U}_n$.

2 Anneaux et Corps

2.1 Anneaux

Définition 2.2.1.10 ***(Anneau)***

Soit A un ensemble non-vide muni de deux lois de composition interne notées $+$ et $\times$. Notons que ce ne sont pas les mêmes lois que les additions et multiplications usuelles, elles ont uniquement des "rôles" additifs et multiplicatifs similaires.
On dit que $(A, +, \times)$ est un **anneau** si :

1. $(A, +)$ est un groupe abélien.
2. $\times$ est associative dans A et admet un élément neutre dans A.
3. La loi $\times$ est distributive par rapport à la loi $+$, i.e. :
   - $\forall (a, b, c) \in A^3, a \times (b + c) = (a \times b) + (a \times c)$ (distributivité à gauche).
   - $\forall (a, b, c) \in A^3, (a + b) \times c = (a \times c) + (b \times c)$ (distributivité à droite).

Si, de plus, la loi $\times$ est commutative dans A, on dit que $(A, +, \times)$ est un **anneau commutatif**.

Remarque 2.2.1.8

On ne peut plus parler d'élément neutre de l'anneau, car il y a deux lois de composition interne. On parle donc d'élément neutre pour la loi $\times$ ou pour la loi $+$.

- L'élément neutre pour la loi $+$ est noté 0_A.
- L'élément neutre pour la loi $\times$ est noté 1_A.

Idem, on ne peut pas parler de symétrique d'un élément dans un anneau, mais uniquement de son opposé pour la loi $+$.

Exemple 2.2.1.8

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathbb{K}^{\mathbb{N}}, +, \times)$ est un anneau commutatif, où $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$, sachant que $\mathbb{K}^{\mathbb{N}}$ et le groupe des applications de $\mathbb{N}$ à valeurs dans $\mathbb{K}$ (1.1.3).

- On munit $\mathbb{Z}/n\mathbb{Z}$ des lois $+$ et $\dot{\times}$ définies par : $\forall \overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$,
  - $\overline{a} + \overline{b} = \overline{a+b}$,
  - $\overline{a} \times \overline{b} = \overline{a \dot{\times} b}$.

  $\dot{\times}$ est bien définie. Prenons $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ dans $\mathbb{Z}/n\mathbb{Z}$. Après calculs, on trouve bel et bien que $\overline{xy} = \overline{x'y'}$.
  Donc $\overline{x} \dot{\times} \overline{y} = \overline{x'} \dot{\times} \overline{y'}$.
  Ainsi, $(\mathbb{Z}/n\mathbb{Z}, +, \dot{\times})$ est un anneau commutatif.

Propriété 2.2.1.11

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

- $a \in A$ est dit **inversible** lorsque a est inversible pour la loi $\times$, i.e. $\exists b \in A$ tel que $a \times b = b \times a = 1_A$. Dans ce cas, b est unique et on le note a^{-1}.
- On note $A^* = \{a \in A \text{ tel que } a \text{ est inversible}\}$ l'ensemble des éléments inversibles de l'anneau $(A, +, \times)$.

Attention

L'ensemble A^* n'est pas l'ensemble $A \setminus \{0_A\}$! Mais ils coïncident dans le cas particulier des corps (voir plus loin). Voir le premier exemple en 2.1.

Remarque 2.2.1.9

On parle d'élément inversible pour la loi $\times$, mais on évite le terme "symétrisable" pour éviter toute confusion avec le terme "symétrique" qui concerne la loi $+$.

Exemple 2.2.1.9

- $\mathbb{U}_{\mathbb{Z}} = \{-1, 1\}$.
- $\mathbb{U}_{\mathbb{K}} = \mathbb{K} \setminus \{0\}$, où $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$.
- $\mathbb{U}_{\mathbb{Z}/n\mathbb{Z}} = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \exists \overline{b} \in \mathbb{Z}/n\mathbb{Z}, \overline{a} \dot{\times} \overline{b} = \overline{1}\}$
  $= \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \text{ tel que } \operatorname{pgcd}(a, n) = 1\}$ (en utilisant le théorème de Bézout).
  Par exemple, $\mathbb{U}_{\mathbb{Z}/9\mathbb{Z}} = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.
- $\mathbb{U}_{\mathbb{Z}/11\mathbb{Z}} = \mathbb{Z}/11\mathbb{Z} \setminus \overline{0}$ car 11 est premier.

Propriété 2.2.1.12

Soit $(A, +, \times)$ un anneau. Alors, $(A^* = \mathbb{U}_A, \times)$ est un groupe, appelé le groupe des inversibles de l'anneau A.

Remarque 2.2.1.10 *(Hors programme)*

Le cardinal de $\mathbb{U}_{\mathbb{Z}/n\mathbb{Z}}$ **ne divise pas** n, parce que $\mathbb{U}_{\mathbb{Z}/n\mathbb{Z}}$ n'est pas un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ (les deux lois sont différentes). Par exemple, pour $n = 8$, on a $\text{card}\left(\mathbb{U}_{\mathbb{Z}/8\mathbb{Z}}\right) = 4$ qui ne divise pas 8. Le cardinal du groupe $(\mathbb{Z}/n\mathbb{Z}, \times)$ est donné par la fonction indicatrice d'Euler $\varphi(n)$.

$$\varphi(n) = \text{card}\left(\mathbb{U}_{\mathbb{Z}/n\mathbb{Z}}\right) = \text{card}\left(\{k \in [\![1, n]\!] \text{ tel que } \text{pgcd}(k, n) = 1\}\right)$$

Par exemple, $\varphi(9) = 9\left(1 - \frac{1}{3}\right) = 6$, et $\varphi(11) = 11\left(1 - \frac{1}{11}\right) = 10$.
Si n est premier, alors $\varphi(n) = n - 1$ (ce sont tous les éléments sauf $\overline{0}$ qui sont inversibles).

Remarque 2.2.1.11

Soit $(A, +, \times)$ un anneau. On a toujours $0_A \times a = a \times 0_A = 0_A$, pour tout $a \in A$. On a aussi $-1_A \times a = a \times -1_A = -a$, pour tout $a \in A$.
Preuve du premier point : Soit $a \in A$. On a $0_A \times a + 0_A \times a = (0_A + 0_A) \times a = 0_A \times a$. Donc, intuitivement, en "simplifiant" $0_A \times a$ des deux côtés, on obtient $0_A \times a = 0_A$. De même, on montre que $a \times 0_A = 0_A$.

Définition 2.2.1.11 *(Diviseur de zéro)*

Soit $(A, +, \times)$ un anneau. On dit que $a \in A \setminus \{0_A\}$ est un **diviseur de zéro** s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = 0_A$ ou $b \times a = 0_A$.

Exemple 2.2.1.10

- $\overline{2}$ est un diviseur de zéro dans $\mathbb{Z}/6\mathbb{Z}$ car $\overline{2} \dot{\times} \overline{3} = \overline{0}$.

Définition 2.2.1.12 *(Anneau intègre)*

Soit $(A, +, \times)$ un anneau. On dit que A est un **anneau intègre** lorsque :

- $(A, +, \times)$ est un anneau commutatif.
- A est sans diviseurs de zéro, i.e. : $\forall a, b \in A, a \times b = 0_A \implies a = 0_A$ ou $b = 0_A$.

Remarque 2.2.1.12

La seule définition que nous allons utiliser est celle indiquée ci-dessus. Cependant, on peut définir des anneaux semi-intègres sans avoir besoin de la commutativité de la multiplication...

Exemple 2.2.1.11

1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux intègres.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \dot{\times})$ est intègre si et seulement si n est premier.

Preuve *(Deuxième exemple)*

■

recop ◡.

2.2 Sous-anneaux

Définition 2.2.2.13 *(Sous-anneau)*

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

- B est non-vide (il doit contenir au moins l'élément 1_A, qui est le plus facile à montrer).
- B est stable par les lois $+$ et $\times$, i.e. :
  - $\forall (a, b) \in B^2, a - b \in B$,
  - $\forall (a, b) \in B^2, a \times b \in B$.

Remarque 2.2.2.13

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

Exemple 2.2.2.12

$\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$, où $\mathbb{Z}[i] = \{a + ib \text{ tel que } (a, b) \in \mathbb{Z}^2\}$ (entiers de Gauss).

- $1_{\mathbb{C}} = 1 + i0 \in \mathbb{Z}[i]$, donc $\mathbb{Z}[i]$ est non-vide.
- Soient $x = a + ib$ et $y = c + id$ dans $\mathbb{Z}[i]$.
- On a $x + y = (a + c) + i(b + d) \in \mathbb{Z}[i]$ car $(a + c, b + d) \in \mathbb{Z}^2$.
- On a $x \times y = (ac - bd) + i(ad + bc) \in \mathbb{Z}[i]$ car $(ac - bd, ad + bc) \in \mathbb{Z}^2$.

Définition 2.2.2.14 *(Élément nilpotent)*

Soit $(A, +, \times)$ un anneau. On dit que $a \in A$ est un **élément nilpotent** s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$, où $a^n = \underbrace{a \times a \times \ldots \times a}_{n \text{ fois}}$.

Exemple 2.2.2.13

1. Dans $\mathbb{Z}/8\mathbb{Z}$, $\overline{2}$ est nilpotent car $\overline{2}^3 = \overline{8} = \overline{0}$.
2. Dans $\mathbb{Z}/9\mathbb{Z}$, $\overline{3}$ est nilpotent car $\overline{3}^2 = \overline{9} = \overline{0}$, idem pour $\overline{6}$.

Propriété 2.2.2.13

Soient $(A, +, \times)$ un anneau commutatif et $a, b \in A$. Alors, $\forall n \in \mathbb{N}^*, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}$ (formule du binôme de Newton), avec la convention $a^0 = 1_A$ et $0_A^0 = 1_A$.
Preuve par récurrence sur n.

Application 2.2.2.1

Soit $(A, +, \times)$ un anneau commutatif.
Si $a, b \in A$ sont nilpotents, i.e. $\exists n, m \in \mathbb{N}$ tel que $a^n = 0_A, b^m = 0_A$, alors $a + b$ est nilpotent.
En effet :
Soit $N = n + m$. On a :

$$(a+b)^N = \sum_{k=0}^{N} \binom{N}{k} a^k \times b^{N-k}$$

Si $k \geq n$, alors $a^k = 0_A$.
Si $N - k \geq m$, alors $b^{N-k} = 0_A$.
Donc, dans la somme précédente, tous les termes sont nuls. Donc, $(a+b)^N = 0_A$.
On remarque aussi que $(-a)^n = (-1_A)^n \times a^n = 0_A$, donc $-a$ est nilpotent.
Conclusion : Si $(A, +, \times)$ est un anneau commutatif, alors $\mathcal{N}(a) = \{a \in A$ tel que a est nilpotent$\}$ est un sous-groupe de $(A, +)$.

2.3 Corps

Définition 2.2.3.15 *(Corps)*

Soit K un ensemble non-vide muni de deux lois de composition interne $+$ et $\times$.
On dit que $(K, +, \times)$ est un **corps** si :

1. $(K, +, \times)$ est un anneau.
2. $\forall x \in K \setminus \{0_K\}, x \in K^*$, i.e. : x est inversible dans $K \setminus \{0_K\}$.

Si, de plus, la loi $\times$ est commutative dans K, on dit que $(K, +, \times)$ est un **corps commutatif**.

Remarque 2.2.3.14

$$(K,+,\times) \text{ est un corps } \iff \begin{cases} (K,+) \text{ est un groupe abélien} \\ (K\setminus\{0_K\},\times) \text{ est un groupe} \\ \times \text{ est distributive par rapport à } + \text{ dans } K \end{cases}$$

Exemple 2.2.3.14

1. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.
2. $(\mathbb{Z}/n\mathbb{Z},+,\dot{\times})$ est un corps si et seulement si n est un nombre premier, parce que dans ce cas, $U_{\mathbb{Z}/n\mathbb{Z}} = \mathbb{Z}/n\mathbb{Z}\setminus\{\overline{0}\}$.

Définition 2.2.3.16 *(Sous-corps)*

Soient $(K,+,\times)$ un corps et L une partie de K. On dit que L est un **sous-corps** de K si et seulement si L est un sous-anneau de K et que $\forall x \in L\setminus\{0_L\}, x^{-1} \in L$.
Si L est un sous-corps de K, alors cela équivaut à dire que K est une extension de L.

Exemple 2.2.3.15

On pose $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \text{ tels que } (a,b)\in\mathbb{Q}^2\}$.
$\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $(\mathbb{R},+,\times)$.

Définition 2.2.3.17 *(Idéal d'un anneau commutatif)*

Soit A un anneau commutatif. Soit I une partie de A.
On dit que I est un **idéal** de A lorsque :

$$\begin{cases} I \subset A \quad (0) \quad \text{rappel} \\ I \text{ est un sous-groupe de } (A,+) \quad (1) \\ \forall a\in A, \forall x\in I, a\cdot x \in I \text{ i.e. } AI\subset I \quad (2) \end{cases}$$

Remarque 2.2.3.15

Si I est un idéal de A tel que $1_A \in I$, alors $I = A$, parce que pour tout $a\in A$, on a $a\cdot 1_A = a \in I$ d'après la condition (2).
Les sous-groupes triviaux de $(A,+)$, à savoir $\{0_A\}$ et A sont toujours des idéaux de l'anneau commutatif A.

Exercice 2.2.3.2

Soit $(K, +, \times)$ un corps commutatif. Montrer que les seuls idéaux de K sont $\{0_K\}$ et K.
Solution :
Il est clair que $\{0_K\}$ et K sont des idéaux de K.
Soit I un idéal de K tel que $I \neq \{0_K\}$. Donc, $\exists a \in I$ tel que $a \neq 0_K$. Montrons que $I = K$.

- On sait que $I \neq \{0_K\}$, donc $\exists x \in K$ tel que $x \neq 0_K$ et $x \in I$.
- Donc $x \cdot x^{-1} = 1_K \in I$ (car I est stable par la multiplication par un élément de K).
- Alors, d'après la remarque précédente, on a $I = K$.

Propriété 2.2.3.14 ***(Idéal engendré par un élément)***

Soit $(A, +, \times)$ un anneau commutatif et $x \in A$. Alors, l'ensemble $xA = \{a \times x \text{ tel que } a \in A\}$ est le plus petit idéal de A contenant x.
Cet idéal est appelé l'idéal engendré par x.

Preuve

- Montrons que xA est un idéal de A.
  - On a clairement $xA \subset A$.
  - Montrons que xA est un sous-groupe de $(A, +)$.
    - $0_A = 0_A \times x \in xA$, donc xA est non-vide.
    - Soient $u, v \in xA$. Donc, $\exists a, b \in A$ tels que $u = a \times x$ et $v = b \times x$.
    - Donc, $u - v = (a - b) \times x \in xA$ (car $(A, +)$ est un groupe).
  - Donc, xA est un sous-groupe de $(A, +)$.
  - Montrons que $\forall a \in A, \forall y \in xA, a \times y \in xA$.
    - Soit $a \in A$ et $y \in xA$. Donc, $\exists b \in A$ tel que $y = b \times x$.
    - Donc, $a \times y = a \times (b \times x) = (a \times b) \times x \in xA$ (car $(A, \times)$ est associative).
  - Donc, $\forall a \in A, \forall y \in xA, a \times y \in xA$.
- On en déduit que xA est un idéal de A.
- Montrons que xA est le plus petit idéal de A contenant x. Nous allons, pour cela, montrer que pour tout idéal I de A contenant x, on a $xA \subset I$.
  - Soit I un idéal de A tel que $x \in I$.
  - Soit $y \in xA$. Donc, $\exists a \in A$ tel que $y = a \times x$.
  - Or, comme $x \in I$ et que I est stable par la multiplication par un élément de A, on a $y = a \times x \in I$. Cela veut dire que $xA \subset I$.
- On en déduit que xA est le plus petit idéal de A contenant x.

■

Remarque 2.2.3.16

La réciproque de l'exercice précédent est vraie : si tous les idéaux d'un anneau commutatif A sont triviaux, alors A est un corps commutatif.

Preuve

Soit $x \in A \setminus \{0_A\}$. Montrons que x est inversible dans A.
On sait que xA est un idéal de A.
Donc $xA = \{0_A\}$ ou $xA = A$.
Or, $x \in xA$ et $x \neq 0_A$, donc $xA \neq \{0_A\}$.
Donc, $xA = A$.
On a donc $1_A \in xA$, sachant que $1_A \in A$.
Donc $\exists y \in A$ tel que $1_A = y \times x$.
Donc x est inversible dans A.
On en déduit que $(A, +, \times)$ est un corps commutatif. ■

Exemple 2.2.3.16

Les idéaux de $\mathbb{Z}/4\mathbb{Z}$ sont :

- $\{\overline{0}\}$,
- $\mathbb{Z}/4\mathbb{Z}$,
- $\{\overline{0}, \overline{2}\}$ (idéal engendré par $\overline{2}$). D'après le théorème de Lagrange, on sait que le cardinal de cet idéal divise 4, car tout idéal est un sous-groupe de $(\mathbb{Z}/4\mathbb{Z}, +)$. L'idéal ne peut pas contenir $\overline{1}$ ou $\overline{3} = \overline{-1}$, sinon il serait égal à $\mathbb{Z}/4\mathbb{Z}$. Donc, le seul idéal de cardinal 2 est $\{\overline{0}, \overline{2}\}$.

Propriété 2.2.3.15

Soient $(A, +, \times)$ un anneau commutatif et I, J deux idéaux de A. Alors,$I \cap J$ et $I + J = \{x + y$ tel que $(x, y) \in I \times J\}$ sont des idéaux de A.

Preuve

- Montrons que $I \cap J$ et $I + J$ sont des sous-groupes de $(A, +)$.
  - $I \cap J$ est clairement un sous-groupe de $(A, +)$ (propriétés d'intersection).
  - Montrons que $I + J$ est un sous-groupe de $(A, +)$.
    - $0_A = 0_A + 0_A \in I + J$, donc $I + J$ est non-vide.
    - Soient $u, v \in I + J$. Donc, $\exists (a, b), (c, d) \in I \times J$ tels que $u = a + b$ et $v = c + d$.
    - Donc, $u - v = (a - c) + (b - d) \in I + J$ (car I et J sont des sous-groupes de $(A, +)$).
  - Donc, $I + J$ est un sous-groupe de $(A, +)$.

- Montrons que $\forall a \in A, \forall x \in I \cap J, a \times x \in I \cap J$ et $\forall a \in A, \forall y \in I+J, a \times y \in I+J$.
  - Soit $a \in A$ et $x \in I \cap J$. Donc, $x \in I$ et $x \in J$.
  - Donc, $a \times x \in I$ (car I est un idéal de A) et $a \times x \in J$ (car J est un idéal de A).
  - Donc, $a \times x \in I \cap J$.
  - Soit $a \in A$ et $y \in I + J$. Donc, $\exists (b, c) \in I \times J$ tel que $y = b + c$.
  - Donc, $a \times y = a \times (b + c) = (a \times b) + (a \times c) \in I + J$ (car I et J sont des idéaux de A).

■

Exemple 2.2.3.17

Dans $(\mathbb{Z}, +, \times)$, on a $2\mathbb{Z} + 3\mathbb{Z} = n\mathbb{Z}$, où $n = \text{pgcd}(2, 3) = 1$ (voir chapitre suivant). Donc, $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.

3 Morphismes

3.1 Morphismes de groupes

Définition 3.3.1.18

- Morphismes et isomorphismes de groupes
  - Soient $(G, *)$ et (G', T) deux groupes et $f : G \to G'$ une application. On dit que f est un **morphisme de groupes** si :

$$\forall x, y \in G, f(x * y) = f(x) T f(y)$$

  - Si, de plus, f est bijective, on dit que f est un **isomorphisme de groupes**, et on écrit dans ce cas $G \cong G'$. On note $\mathrm{Isom}(G, G')$ l'ensemble des isomorphismes de groupes de G vers G'.
- Endomorphismes et automorphismes de groupes
  - Si $f : G \to G$, avec $(G, *)$ un groupe et f un morphisme de groupes, on dit que f est un **endomorphisme** de G. Attention : les lois de compositions sont les mêmes dans le domaine et le codomaine.
  - Si, de plus, f est bijective, on dit que f est un **automorphisme** de G. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Exemple 3.3.1.18

Soient $(\mathbb{R}_+^*, \times)$ et $(\mathbb{R}, +)$ deux groupes. L'application $\begin{cases} f : \mathbb{R}_+^* \to \mathbb{R} \\ x \mapsto \ln(x) \end{cases}$ est un isomorphisme de groupes entre $(\mathbb{R}_+^*, \times)$ et $(\mathbb{R}, +)$. On a en effet :

$$\forall (x, y) \in (\mathbb{R}_+^*)^2, f(x \times y) = \ln(x \times y) = \ln(x) + \ln(y) = f(x) + f(y)$$

De plus, f est bijective, avec $f^{-1} : \mathbb{R} \to \mathbb{R}_+^*, y \mapsto e^y$.
Soit $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, k \mapsto \overline{k}$. C'est un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(\mathbb{Z}/n\mathbb{Z}, +)$. Il est surjectif (surjectif canonique entre $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$) mais pas injectif.
Soit $(G, \cdot)$ un groupe et $a \in G$. L'application $f : \begin{cases} (\mathbb{Z}, +) \to (\langle a \rangle, \cdot) \\ k \mapsto a^k \end{cases}$ est un morphisme de groupes. Il est surjectif par définition de $\langle a \rangle$.

Propriété 3.3.1.16

Soient $f : (G, *) \to (G', T)$ un morphisme de groupes et e, e' les éléments neutres de G et G'.

1. $f(e) = e'$.
2. $(f(x))^{-1} = f(x^{-1})$, pour tout $x \in G$.
3. Si H est un sous-groupe de $(G, *)$, alors $f(H) = \{f(h) \text{ tel que } h \in H\}$ est un sous-groupe de (G', T).
4. Si K est un sous-groupe de (G', T), alors $f^{-1}(K) = \{g \in G \text{ tel que } f(g) \in K\}$ est un sous-groupe de $(G, *)$.

Attention

Il ne faut pas confondre les notations $f^{-1}(y)$ et $f^{-1}(\{y\})$. La première notation désigne l'antécédent de y par f, tandis que la deuxième notation désigne l'image réciproque de l'ensemble $\{y\}$ par f. La première notation n'a de sens que si f est bijective, tandis que la deuxième notation a toujours un sens, elle est définie pour toute application f ; $x \in f^{-1}(K) \iff f(x) \in K$.

Preuve

- Preuve du premier point
  - On a $f(e) = f(e * e) = f(e)Tf(e)$.
  - En "simplifiant" $f(e)$ des deux côtés, on obtient $f(e) = e'$.
- Preuve du quatrième point
  - On a $f^{-1}(K) = \{x \in G \text{ tel que } f(x) \in K\} \subset G$.
  - Donc $x^{-1} \in f^{-1}(K) \iff f(x) \in K$.
  - Montrons que $f^{-1}(K)$ est non-vide.
    - On a $e' \in K$ (car K est un sous-groupe de (G', T)).
    - Donc, $f(e) = e' \in K$, donc $e \in f^{-1}(K)$.
  - Soient $x, y \in f^{-1}(K)$. Montrons que $x * y^{-1} \in f^{-1}(K)$.
    - On a $f(x * y^{-1}) = f(x)Tf(y^{-1}) = f(x)T\,(f(y))^{-1}$ (d'après le deuxième point).
    - Or, $f(x) \in K$ et $f(y) \in K$ (car $x, y \in f^{-1}(K)$).
    - Donc, $f(x)T\,(f(y))^{-1} \in K$ (car K est un sous-groupe de (G', T)).
    - Donc, $f(x * y^{-1}) \in K$, donc $x * y^{-1} \in f^{-1}(K)$.
  - Donc, $f^{-1}(K)$ est un sous-groupe de $(G, *)$.

■

recop 2,3

Définition 3.3.1.19 ***(Noyau et Image)***

Soit $f : (G, *) \to (G', T)$ un morphisme de groupes, et e l'élément neutre de $*$ dans G, et e' l'élément neutre de T dans G'.

- On appelle **noyau** de f l'ensemble $\mathrm{Ker}(f) = f^{-1}(\{e'\}) = \{x \in G \text{ tel que } f(x) = e'\}$. La notation $\mathrm{Ker}(f)$ vient de l'anglais *kernel* (noyau). e appartient toujours à $\mathrm{Ker}(f)$, par défaut. On sait que $\mathrm{Ker}(f)$ est un sous-groupe de $(G, *)$ (propriété précédente).
- On appelle **image** de f l'ensemble $\mathrm{Im}(f) = f(G) = \{f(x) \text{ tel que } x \in G\}$. On sait que $\mathrm{Im}(f)$ est un sous-groupe de (G', T) (propriété précédente).

Propriété 3.3.1.17

Soient $f : (G, *) \to (G', T)$ un morphisme de groupes et e, e' les éléments neutres de les lois $*$ et T dans G et G' (respectivement).
f est injectif si et seulement si $\mathrm{Ker}(f) = \{e\}$.
f est surjectif si et seulement si $\mathrm{Im}(f) = G'$.

Attention

La propriété précédente est très importante. Elle permet de montrer l'injectivité d'un morphisme de groupes en étudiant uniquement son noyau, ce qui est souvent plus simple.

Preuve

1. Démonstration de la propriété liée à l'injectivité.
   - a) $\Longrightarrow$ Démonstration dans le sens direct.
     i. Supposons que f est injectif.
     ii. Soit $x \in \mathrm{Ker}(f)$. Donc, $f(x) = e'$.
     iii. Or, $f(e) = e'$ (d'après la première propriété sur les morphismes de groupes).
     iv. Donc, par injectivité de f, on a $x = e$.
     v. Donc, $\mathrm{Ker}(f) \subset \{e\}$.
     vi. Comme $e \in \mathrm{Ker}(f)$, on a $\{e\} \subset \mathrm{Ker}(f)$.
     vii. Donc, $\mathrm{Ker}(f) = \{e\}$.
   - b) $\Longleftarrow$ Démonstration dans le sens réciproque.
     i. Supposons que $\mathrm{Ker}(f) = \{e\}$.
     ii. Soient $x, y \in G$ tels que $f(x) = f(y)$.
     iii. Alors, $f(x)T(f(y))^{-1} = e'$.
     iv. Donc, $f(x * y^{-1}) = e'$.
     v. Donc, $x * y^{-1} \in \mathrm{Ker}(f)$.
     vi. Par hypothèse, $\mathrm{Ker}(f) = \{e\}$, donc $x * y^{-1} = e$.

vii. Donc, $x = y$.

viii. Ainsi, f est injectif.

2. Démonstration de la propriété liée à la surjectivité.

a) Si f est surjectif, alors (équivalence $\iff$) par définition de la surjectivité, on a $f(G) = G'$, ce qui équivaut à dire que $\mathrm{Im}(f) = G'$. L'équivalence est donc démontrée.

■

Exemple 3.3.1.19

$$f : \begin{cases} (\mathbb{R}, +) \to (\mathbb{U}, \times) \\ \theta \mapsto e^{i\theta} \end{cases}$$

- On a $\forall \theta, \theta' \in \mathbb{R}, f(\theta + \theta') = e^{i(\theta+\theta')} = e^{i\theta} \times e^{i\theta'} = f(\theta) \times f(\theta')$.
- Donc f est bel et bien un morphisme de groupes.
- On a $\forall z \in \mathbb{U}, \exists \theta \in \mathbb{R}, ze^{i\theta} = f(\theta)$, donc f est surjectif, ce qui équivaut à dire que $f(\mathbb{R}) = \mathbb{U}$.
- On a $\mathrm{Ker}(f) = \{\theta \in \mathbb{R} \text{ tel que } e^{i\theta} = 1\} = \{2k\pi \text{ tel que } k \in \mathbb{Z}\} = 2\pi\mathbb{Z} \neq \{0\}$.
- Donc f n'est pas injectif.

Propriété 3.3.1.18

Soit $(G, *)$ un groupe. Alors, $(\mathrm{Aut}(G), \circ)$ est un groupe (où $\circ$ est la composition d'applications).

Preuve

On remarque que $\mathrm{Aut}(G) \subset S_G$, où S_G est l'ensemble des applications bijectives de G dans G.
Montrons alors que $\mathrm{Aut}(G)$ est un sous-groupe de $(S_G, \circ)$.

- On sait déjà que $\mathrm{Aut}(G) \subset S_G$.
- L'application identité id_G est un automorphisme de G, donc $\mathrm{id}_G \in \mathrm{Aut}(G)$, donc $\mathrm{Aut}(G)$ est non-vide.
- Soient $f, g \in \mathrm{Aut}(G)$.
- Comme f et g sont bijectives, $f \circ g$ est bijective.
- $\forall x, y \in G, (f \circ g)(x * y) = f(g(x * y)) = f(g(x) * g(y)) = f(g(x)) * f(g(y)) = (f \circ g)(x) * (f \circ g)(y)$.
- Donc $f \circ g \in \mathrm{Aut}(G)$ (1).
- Soit $f \in \mathrm{Aut}(G)$. Montrons que $f^{-1} \in \mathrm{Aut}(G)$.

- Comme f est bijective, f^{-1} est bijective.
- Soient $x, y \in G$. On a $f^{-1}(x*y) = f^{-1}(f(f^{-1}(x)) * f(f^{-1}(y))) = f^{-1}(f(f^{-1}(x) * f^{-1}(y))) = f^{-1}(x) * f^{-1}(y)$.
- Donc, $f^{-1} \in \mathrm{Aut}(G)$ (2).
- D'après (1) et (2), on en déduit que $\mathrm{Aut}(G)$ est un sous-groupe de $(S_G, \circ)$.
- Donc, $(\mathrm{Aut}(G), \circ)$ est un groupe.

■

Attention

Dans la preuve précédente, on a utilisé la définition propre d'un sous-groupe (montrer que l'ensemble est non-vide, stable par l'opération et par l'inversion) et pas sa caractérisation (montrer que pour tous x, y dans l'ensemble, $x * y^{-1}$ est dans l'ensemble). En effet, il n'est pas évident de montrer que pour tous $f, g \in \mathrm{Aut}(G)$, $f \circ g^{-1} \in \mathrm{Aut}(G)$.

Exercice 3.3.1.3

Soit $(G, *)$ un groupe d'élément neutre e.

1. Montrer que $\forall a \in G$, l'application $f_a : \begin{cases} G \to G \\ x \mapsto a * x * a^{-1} \end{cases}$ est un automorphisme de G (appelé **automorphisme intérieur** de G).
2. On note $\mathrm{Int}(G) = \{f_a \text{ tel que } a \in G\}$. Montrer que $(\mathrm{Int}(G), \circ)$ est un groupe.
3. On pose $\varphi : \begin{cases} G \to \mathrm{Int}(G) \\ a \mapsto f_a \end{cases}$
   Montrer que φ est un morphisme de groupes.
4. Déterminer $\mathrm{Ker}(\varphi)$.

Solution :

- Preuve du premier point
  - Soient $x, y \in G$.
  - On a $f_a(x*y) = a*(x*y)*a^{-1} = (a*x)*(y*a^{-1}) = (a*x*a^{-1})*(a*y*a^{-1}) = f_a(x) * f_a(y)$.
  - Donc, f_a est un morphisme de groupes.
  - Montrons que f_a est bijective.
    - Soit $y \in G$. Montrons qu'il existe un unique $x \in G$ tel que $f_a(x) = y$.
    - On a $f_a(x) = y \iff a * x * a^{-1} = y \iff x = a^{-1} * y * a$.
    - Donc, pour tout $y \in G$, il existe un unique $x \in G$ tel que $f_a(x) = y$.
  - Donc, f_a est bijective.
  - On en déduit que f_a est un automorphisme de G.

- Preuve du deuxième point
  - On sait que $(G, *)$ est un groupe.
  - Donc $(\mathrm{Aut}(G), \circ)$ est un groupe (propriété précédente).
  - Montrons que $\mathrm{Int}(G)$ est un sous-groupe de $(\mathrm{Aut}(G), \circ)$.
    - On a clairement $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$.
    - Montrons que $\mathrm{Int}(G)$ est non-vide.
      - On a $f_e(x) = e * x * e^{-1} = x$, donc $f_e = \mathrm{id}_G$.
      - Donc, $f_e \in \mathrm{Int}(G)$, donc $\mathrm{Int}(G)$ est non-vide.
    - Soient $f_a, f_b \in \mathrm{Int}(G)$. Montrons que $f_a \circ f_b^{-1} \in \mathrm{Int}(G)$.
      - On a $\forall x \in G, (f_a \circ f_b^{-1})(x) = f_a(f_b^{-1}(x))$.
      - Or, $\forall x \in G, f_b^{-1}(x) = b^{-1} * x * b$ (car f_b est bijective).
      - Donc, $\forall x \in G, (f_a \circ f_b^{-1})(x) = f_a(b^{-1} * x * b) = a * (b^{-1} * x * b) * a^{-1} = (a * b^{-1}) * x * (a * b^{-1})^{-1}$.
      - Donc, $f_a \circ f_b^{-1} = f_{a*b^{-1}}$.
      - (On remarque que $f_a \circ f_b = f_{a*b}$)
      - Donc, $f_a \circ f_b^{-1} \in \mathrm{Int}(G)$.
    - Donc, $\mathrm{Int}(G)$ est un sous-groupe de $(\mathrm{Aut}(G), \circ)$.
- Preuve du troisième point
  - Soient $a, b \in G$.
  - On a $\varphi(a * b) = f_{a*b}$.
  - Or, $\forall x \in G, (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x * b^{-1}) = a * (b * x * b^{-1}) * a^{-1} = (a * b) * x * (a * b)^{-1} = f_{a*b}(x)$.
  - Donc, $\varphi(a * b) = f_{a*b} = f_a \circ f_b = \varphi(a) \circ \varphi(b)$.
  - On en déduit que φ est un morphisme de groupes.
- Preuve du quatrième point
  - On a $\mathrm{Ker}(\varphi) = \{a \in G \text{ tel que } \varphi(a) = \mathrm{id}_G\} = \{a \in G \text{ tel que } f_a = \mathrm{id}_G\}$.
  - Donc, $\mathrm{Ker}(\varphi) = \{a \in G \text{ tel que } \forall x \in G, a * x * a^{-1} = x\}$.
  - Donc, $\mathrm{Ker}(\varphi) = \{a \in G \text{ tel que } \forall x \in G, a * x = x * a\}$.
  - On en déduit que $\mathrm{Ker}(\varphi)$ est le centre de G.

3.2 Morphismes d'anneaux

Définition 3.3.2.20 *(Morphisme d'anneaux)*

Soient $(A, +, \times)$ et $(A', \oplus, \odot)$ deux anneaux. On dit que $f : A \to A'$ est un **morphisme d'anneaux** si :

1. $\forall x, y \in A, f(x + y) = f(x) \oplus f(y)$,
2. $\forall x, y \in A, f(x \times y) = f(x) \odot f(y)$,
3. $f(1_A) = 1_{A'}$.

Et si, de plus, f est bijective, on dit que f est un **isomorphisme d'anneaux**.

Attention

Dans le cours manuscrit, la notation pour la loi de A' est la même que pour celle de A. Ici, on utilise des notations différentes pour éviter toute confusion. Ce choix dans le cours manuscrit a été fait pour alléger les notations et continuer à utiliser les notations habituelles.

Remarque 3.3.2.17

Si $f : A \to A'$ est un morphisme d'anneaux, alors $f : (A, +) \to (A', \oplus)$ est un morphisme de groupes.

Propriété 3.3.2.19

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

1. L'image de l'image réciproque par f d'un sous-anneau est un sous-anneau.
2. Si A et A' sont des anneaux commutatifs, que I est un idéal de $(A, +, \times)$, et que f est surjectif, alors $f(I)$ est un idéal de $(A', \oplus, \odot)$.
3. Si J est un idéal de $(A', \oplus, \odot)$, alors $f^{-1}(J)$ est un idéal de $(A, +, \times)$.

Preuve

- Preuve du premier point
  - Elle est analogue à la preuve du troisième point de la propriété sur les morphismes de groupes.
- Preuve du deuxième point
  - Supposons que f est surjectif. Soit I un idéal de A.
  - On a $f(I) \subset f(A) \subset A'$.
  - On a I est un sous-groupe de $(A, +)$, cela implique que $f(I)$ est un sous-groupe de $(A', \oplus)$, car f est un morphisme d'anneaux, donc en particulier

un morphisme de groupes.

- ▷ Soient $a \in A', y \in f(I)$. Montrons que $ay \in f(I)$.
  - — Comme $y \in f(I)$, alors $\exists x \in I$ tel que $y = f(x)$.
  - — Comme f est surjectif, $\exists b \in A$ tel que $f(b) = a$.
  - — Donc, $ay = f(b) \odot f(x) = f(b \times x) \in f(I)$ (car f est un morphisme d'anneaux), sachant que $b \times x \in I$ (car I est un idéal de A).
- ▷ Donc, $f(I)$ est un idéal de $(A', \oplus, \odot)$.

▶ Preuve du troisième point

- ▷ Soit J un idéal de A'.
- ▷ On a $f^{-1}(J)$ est un sous-groupe de $(A, +)$ (propriété sur les morphismes de groupes).
- ▷ Soient $a \in A, y \in f^{-1}(J)$. Montrons que $a \times y \in f^{-1}(J)$.
  - — Comme $y \in f^{-1}(J)$, alors $f(y) \in J$.
  - — Donc, $f(a \times y) = f(a) \odot f(y) \in J$ (car f est un morphisme d'anneaux), sachant que $f(y) \in J$ et que J est un idéal de A'.
  - — Donc, $a \times y \in f^{-1}(J)$.
- ▷ Donc, $f^{-1}(J)$ est un idéal de $(A, +, \times)$.

■

→ Conséquence 3.3.2.2

Soit $f : A \to A'$ un morphisme d'anneaux.

▶ $\mathrm{Ker}(f) = f^{-1}(\{0_{A'}\})$ est un idéal de $(A, +, \times)$.

▶ Si f est injectif, cela équivaut à dire que $\mathrm{Ker}(f) = \{0_A\}$.

Définition 3.3.2.21 ***(Caractéristique d'un anneau)***

Soit $(A, +, \times)$ un anneau. On définit le morphisme d'anneau suivant :

$$f : \begin{cases} \mathbb{Z} \to A \\ n \mapsto n \cdot 1_A = \begin{cases} \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}, & \text{si } n > 0 \\ 0_A, & \text{si } n = 0 \end{cases} \end{cases}$$

▶ Si f est injectif, alors $\mathrm{Ker}(f) = \{0\}$

- ▷ Dans ce cas, on dit que la **caractéristique** de l'anneau A est 0.
- ▷ On note $\mathrm{Car}(A) = 0$.

▶ Si f est non-injectif, c.à.d. $\mathrm{Ker}(f) \neq \{0\}$, alors :

- ▷ Comme $\mathrm{Ker}(f)$ est un idéal de $\mathbb{Z}$ (donc un sous-groupe de $(\mathbb{Z}, +)$), alors $\exists! c \in \mathbb{N}^*$ tel que $\mathrm{Ker}(f) = c\mathbb{Z}$ avec $c = \min(\{n \in \mathbb{N}^* \text{ tel que } n \cdot 1_A = 0_A\})$.

- ▷ Dans ce cas, on dit que la **caractéristique** de l'anneau A est c.
- ▷ On note $\mathrm{Car}(A) = c$.

▶ Conclusion : La caractéristique d'un anneau A est :

$$\mathrm{Car}(A) = \begin{cases} 0, & \text{si } f \text{ est injectif} \\ \min(\{n \in \mathbb{N}^* \text{ tel que } n \cdot 1_A = 0_A\}), & \text{sinon} \end{cases}$$

démontrer que c'est un morphisme d'anneaux

Preuve

▶ On pose $E = \{n \in \mathbb{N}^* \text{ tel que } n \cdot 1_A = 0_A\}$.
▶ Dans le cas où $\mathrm{Ker}(f) \neq \{0\}$, on a $\exists n \in \mathbb{Z}$ tel que $n \neq 0$ et $n \cdot 1_A = 0_A$.
▶ Or $-n \in \mathrm{Ker}(f)$ aussi, parce que $(-n)\cdot 1_A = -(n \cdot 1_A) = -0_A = 0_A$, donc $n \in E$.
▶ Donc, $E \neq \emptyset$.
▶ On pose $c = \min(E)$.
▶ Montrons que $\mathrm{Ker}(f) = c\mathbb{Z}$. $\mathrm{Ker}(f) = \{n \in \mathbb{Z} \text{ tel que } n \cdot 1_A = 0_A\}$.
▶ On sait que $c \in \mathrm{Ker}(f)$, donc $c\mathbb{Z} \subset \mathrm{Ker}(f)$.
▶ Soit $n \in \mathrm{Ker}(f)$. Donc, $n \cdot 1_A = 0_A$.
▶ Par division euclidienne, on a $n = qc + r$ avec $q \in \mathbb{Z}$ et $r \in \{0, \ldots, c-1\}$.
▶ Si $r > 0$, alors $n - qc \in \mathbb{N}^*$.
▶ Or $n \in \mathrm{Ker}(f)$ et $c \in \mathrm{Ker}(f)$ alors $n - qc \in \mathrm{Ker}(f)$ (car $\mathrm{Ker}(f)$ est un sous-groupe de $(\mathbb{Z}, +)$).
▶ Donc, $r = n - qc \in E$.
▶ Donc $r \geq c$ (car $c = \min(E)$).
▶ Contradiction.
▶ Donc, $r = 0$, et par suite $n = qc \in c\mathbb{Z}$.
▶ Donc, $\mathrm{Ker}(f) \subset c\mathbb{Z}$.
▶ On en déduit que $\mathrm{Ker}(f) = c\mathbb{Z}$.

■

Exemple 3.3.2.20

1. $A = \mathbb{Z}$. On a $f : \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ n \mapsto n \cdot 1 = n \end{cases}$ est injectif. Donc, $\mathrm{Car}(\mathbb{Z}) = 0$.
2. Soit $n \geq 1$. On pose $A = \mathbb{Z}/n\mathbb{Z}$. On a $f : \begin{cases} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ k \mapsto k\overline{1} = \overline{k} \end{cases}$. On a $\mathrm{Ker}(f) = \{k \in \mathbb{Z} \text{ tel que } f(k) = \overline{0}\} = n\mathbb{Z}$. Donc, $\mathrm{Car}(\mathbb{Z}/n\mathbb{Z}) = n$.

Propriété 3.3.2.20

Soit A un anneau **intègre**.
$\mathrm{Car}(A) = 0$ ou un nombre premier.

Preuve

On suppose que $\mathrm{Car}(A) \neq 0$, et $\mathrm{Car}(A)$ n'est pas premier.
Donc $\mathrm{Car}(A) = c = \min(\{n \in \mathbb{N}^* \text{ tel que } n \cdot 1_A = 0_A\})$ est composé.
Donc $\exists a, b \in \mathbb{N}^*$ tels que $c = ab$, avec $1 \leq a < c$ et $1 \leq b < c$. (On peut considérer l'inégalité stricte dans le cas où $c \neq 1$).
On a $c \cdot 1_A = 0_A$.
Ce qui implique que $(ab) \cdot 1_A = (a \cdot 1_A) \times (b \cdot 1_A) = 0_A$.
Ce qui implique que $f(ab) = 0_A$.
Donc $f(a) \cdot f(b) = 0_A$.
Comme A est intègre, on a $f(a) = 0_A$ ou $f(b) = 0_A$.
Cela signifie que soit $a \in \mathrm{Ker}(f)$, soit $b \in \mathrm{Ker}(f)$.
Donc que $a \cdot 1_A = 0_A$ ou $b \cdot 1_A = 0_A$. Contradiction.
On conclut que $c = 0$ ou c est premier. ■

Fin du Chapitre X.