Chapitre 9 : structures algébriques

Table des matières

1 Groupes

1.1 Définitions

Définition 1 Soit E un ensemble. On appelle ***loi de composition interne*** (en abrégé LCI), toute application de $E \times E$ dans E. Si $\star$ est une LCI sur E, on note pour tout $(a, b) \in E^2$, $\star(a, b) = a \star b$.

Définition 2 Soit $(G, \star)$ un ensemble G muni d'une LCI $\star$ [on dit que G est un ***magma***]. On dit que $(G, \star)$ est un ***groupe*** (ou que la LCI $\star$ munit l'ensemble G d'une structure de groupe) si :
- la LCI $\star$ est ***associative*** : $\forall (a, b, c) \in G^2$, $a \star (b \star c) = (a \star b) \star c$; [on dit alors que G est un ***monoïde***]
- la LCI $\star$ admet un ***élément neutre*** : $\exists e \in G$, $\forall a \in G$, $a \star e = e \star a = a$; [on dit que G est ***unifère***]
- tout élément $g \in G$ admet un ***inverse*** (ou un ***symétrique***) pour la LCI $\star$: $\exists h \in G$, $h \star g = g \star h = e$. [on dit que tous les éléments de G sont ***symétrisables***]

Proposition 1 Si $(G, \star)$ est un groupe, il existe un unique élément neutre noté e et pour tout élément g de G, il existe un unique inverse h noté $h = g^{-1}$.

Définition 3 Soit $(G, \star)$ un groupe. On dit que le groupe est ***commutatif*** ou ***abélien*** si : $\forall (a, b) \in G^2$, $a \star b = b \star a$.

Exemple 1 • Les ensembles $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs d'élément neutre $e = 0$ et d'inverse $x^{-1} = -x$.

• Les ensembles $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes commutatifs d'élément neutre $e = 1$ et d'inverse $x^{-1} = \dfrac{1}{x}$.

• Soit E un ensemble. L'ensemble $Bij(E)$ des bijections de E dans E muni de la LCI $\star = \circ$ (la composition) forme un groupe en général non commutatif d'élément neutre $e = \mathrm{id}_E$ et d'inverse $f^{-1} = f^{-1}$ la fonction réciproque de la fonction bijective f.

Proposition 2 Soient $(G, \star)$ un groupe, puis $g_1, \cdots, g_n$, n éléments de ce groupe. Alors :

$$(g_1 \star \cdots \star g_n)^{-1} = g_n^{-1} \star \cdots \star g_1^{-1}.$$

Remarque 1 Si $(G, \star)$ est un groupe, $g \in G$ et $n \in \mathbb{Z}$ est un entier, on note g^n l'itéré $n^{\text{ème}}$ de g :
$\longrightarrow$ si $n \in \mathbb{N}^*$, $g^n = g \star \cdots \star g \quad (n \text{ fois})$
$\longrightarrow$ si $n \in \mathbb{Z} \setminus \mathbb{N}$, $g^n = g^{-1} \star \cdots \star g^{-1} \quad ((-n) \text{ fois})$
$\longrightarrow$ si $n = 0$, $g^0 = e$ l'élément neutre.
On en déduit que dans un groupe $(G, \star)$,

$$\forall g \in G,\ \forall (p, q) \in \mathbb{Z}^2,\ \left(g^{\star p}\right) \star \left(g^{\star q}\right) = g^{\star (p+q)} \text{ et } \left(g^{\star p}\right)^{\star q} = g^{\star (pq)}.$$

Une somme vide est l'élément neutre pour l'addition et vaut 0. Un produit vide est l'élément neutre pour la multiplication et vaut 1. Un produit de composition vide vaut id.

1.2 Sous-groupes

Définition 4 Soit $(G, \star)$ un groupe. On dit qu'une partie H de G est un ***sous-groupe*** de G si $(H, \star)$ est un groupe.

Méthode : Comment montrer que H est un groupe ?

Pour montrer que $(H, \star)$ est un groupe :
- trouver un groupe connu $(G, \star)$ contenant H
- montrer que le neutre e de G appartient à H
- montrer que si x et y sont dans H, alors $x \star y^{-1} \in H$.

Exemple 2 • L'ensemble $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ est un groupe multiplicatif, ainsi que les racines $n^{ème}$ de l'unité.
- L'intersection de sous-groupes d'un groupe G est encore un sous-groupe.
- Montrer que si H et K sont deux sous-groupes d'un groupe G, alors :

$$H \cup K \text{ est un sous-groupe} \iff H \subset K \text{ ou } K \subset H.$$

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

Théoréme 1 Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles de la forme $a \cdot \mathbb{Z} = \{a \cdot p \in \mathbb{Z} \mid p \in \mathbb{Z}\}$, où $a \in \mathbb{Z}$.
De plus, si H est un sous-groupe de $(\mathbb{Z}, +)$, il existe un seul entier naturel a tel que $H = a \cdot \mathbb{Z}$. Cet entier s'appelle le ***générateur positif du sous-groupe*** H.

Exemple 3 • Si $H = 12\mathbb{Z}$ et $K = 15\mathbb{Z}$, montrer que $H \cap K$ et $H + K$ sont deux-sous-groupes de $(\mathbb{Z}, +)$.
- Quel est le générateur positif de $H \cap K$?
- Quel est le générateur positif de $H + K$?

1.4 Morphismes de groupes

Définition 5 Soient $(G, \star)$ et $(G', \perp)$ deux groupes. Soit $f : G \longrightarrow G'$ une fonction. On dit que f est un ***morphisme de groupes*** si :

$$\forall (x, y) \in G^2, \quad f(x \star y) = f(x) \perp f(y).$$

On appelle ***isomorphisme de groupes*** tout morphisme de groupes bijectif.
On dit que deux groupes sont ***isomorphes*** s'il existe un isomorphisme de groupes entre les deux.

Exemple 4 • L'application ln est un isomorphisme entre les groupes $(]0, +\infty[, \times)$ et $(\mathbb{R}, +)$.
- L'application $z \longmapsto |z|$ est un morphisme de groupes entre $(\mathbb{C}^*, \times)$ et $(\mathbb{R}_+^*, \times)$.
- L'application $\theta \longmapsto e^{i\theta}$ est un morphisme de groupes surjectif de $(\mathbb{R}, +)$ dans $(\mathbb{U}, \times)$.

Proposition 3 • La composée de deux morphismes de groupes est encore un morphisme de groupes.
- Si $f : G \longrightarrow G'$ est un isomorphisme de groupes, alors la fonction réciproque f^{-1} également.

Proposition 4 Soit $f : G \longrightarrow G'$ un morphisme de groupes. On note e le neutre dans G et e' le neutre dans G'.
Alors, $f(e) = e'$ et pour tout $x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

Définition 6 Soit $f : G \longrightarrow G'$ un morphisme de groupes. On appelle ***noyau*** de f et on note $\mathrm{Ker} f$, l'ensemble :

$$\mathrm{Ker} f = f^{[-1]}(\{e'\}) = \{x \in G \mid f(x) = e'\}.$$

On appelle ***image*** de f et on note $\mathrm{Im} f$, l'ensemble $\mathrm{Im} f = f(G)$.

Proposition 5 Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors $\mathrm{Ker} f$ est un sous-groupe de $(G, \star)$ et $\mathrm{Im} f$ est un sous-groupe de $(G', \perp)$.

Proposition 6 Soit $f : G \longrightarrow G'$ un morphisme de groupes. Alors :
- la fonction f est injective si et seulement si $\mathrm{Ker} f = \{e\}$.
- la fonction f est surjective si et seulement si $\mathrm{Im} f = G'$.

Exemple 5 • La fonction $\exp : \mathbb{C} \to \mathbb{C}^*$ est un morphisme de groupes. Expliciter $\mathrm{Ker}(\exp)$ et $\mathrm{Im}(\exp)$.
- Si G est un groupe et $a \in G$, l'application $\varphi : g \longmapsto a^{-1} \star g \star a$ est un isomorphisme de groupes.

Exemple 6 [théorème de Lagrange]
Soit G un groupe commutatif fini de cardinal p. On pose $x = \prod_{a \in G} a$ le prduit de tous les éléments de G.

1. Montrer que pour tout $g \in G$, $x = \prod_{a \in G} (a \star g)$.
2. En déduire que pour tout $g \in G$, $g^{\star p} = e$.

2 Anneaux

2.1 Premières définitions

Définition 7 Soit A un ensemble muni de deux LCI notées $+$ et $\times$. On dit que $(A, +, \times)$ est un ***anneau*** si :
- l'ensemble $(A, +)$ forme un groupe abélien. On note 0_A ou 0 l'élément neutre de ce groupe et on l'appelle ***élément nul*** de l'anneau
- la LCI $\times$ est ***associative*** : $\forall (a, b, c) \in A^3$, $a \times (b \times c) = (a \times b) \times c$
- la LCI $\times$ est ***distributive*** sur $+$: $\forall (a, b, c) \in A^3$, $a \times (b + c) = a \times b + a \times c$ et $(a + b) \times c = a \times c + b \times c$

- la LCI $\times$ admet un élément neutre noté 1_A ou encore 1 différent de l'élément nul 0_A : $\forall a \in A$, $a \times 1_A = 1_A \times a = a$. Cet élément neutre est appelé ***élément unité*** de l'anneau.

Remarque 2 • L'élément unité est unique.
• L'élément nul est ***absorbant*** : $\forall a \in A$, $a \times 0_A = 0_A \times a = 0_A$
• On dit que l'anneau $(A, +, \times)$ est ***commutatif*** si la LCI $\times$ est commutative : $\forall (a, b) \in A^2$, $a \times b = b \times a$.

2.2 Autres définitions

Définition 8 Soit $(A, +, \times)$ un anneau. Soit $a \in A$.
- On dit que a est ***inversible*** s'il existe $b \in A$ tel que $a \times b = b \times a = 1_A$.
- On dit que a est ***irréductible*** dans A si :

$$\forall (x, y) \in A^2, \quad a = x \times y \Longrightarrow \Big[x \in A^* \text{ ou } y \in A^*\Big].$$

- On dit que l'anneau est ***intègre*** si :

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

- Lorsque A est commutatif, on dit que a ***divise*** b si :

$$\exists \alpha \in A, \quad b = a \times \alpha.$$

Proposition 7 L'ensemble des éléments inversibles est noté A^*. L'ensemble $(A^*, \times)$ forme un groupe d'élément neutre 1_A.

Exemple 7 Étudier les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}^{\mathbb{R}}, +, \times)$ et $(\mathscr{P}(E), \triangle, \cap)$.

2.3 Sous-anneaux

Définition 9 Soit $(A, +, \times)$ un anneau. Soit B une partie de A. On dit que B est un ***sous-anneau*** de A si $(B, +, \times)$ est un anneau.

Méthode : Comment montrer que B est un sous-anneau de A ?
▶ montrer que $1_A \in B$
▶ montrer que si x et y sont dans B, alors $x - y \in B$ et $x \times y \in B$.

Exemple 8 Le seul sous-anneau de $(\mathbb{Z}, +, \times)$ est $\mathbb{Z}$ lui-même.

2.4 Morphisme d'anneaux

Définition 10 Soient $(A,+,\times)$ et $(A',+,\times)$ deux anneaux. Soit $f : A \longrightarrow A'$, une application. On dit que f est un ***morphisme d'anneaux*** si :

$$\forall (x,y) \in A^2, \quad f(x+y) = f(x) + f(y), \quad f(x \times y) = f(x) \times f(y) \text{ et } f(1_A) = 1_{A'}.$$

On appelle ***isomorphisme d'anneaux*** tout morphisme d'anneaux bijectif.
On appelle ***automorphisme d'anneaux***, tout isomorphisme d'un anneau dans lui-même.

Exemple 9 • L'application id_A est un automorphisme d'anneau.
• Il n'existe que deux automorphismes du corps $\mathbb{C}$: $\mathrm{id}_{\mathbb{C}}$ et la conjugaison $z \longmapsto \overline{z}$.

2.5 Formules de sommation dans un anneau

Proposition 8 (formule du binôme de Newton)
Soit $(A,+,\times)$ un anneau. Soient a et b deux éléments qui commutent dans l'anneau (c'est-à-dire $a \times b = b \times a$). Alors, pour tout $n \in \mathbb{N}$, on a :

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

Proposition 9 (formule de factorisation géométrique)
Soit $(A,+,\times)$ un anneau. Soient a et b deux éléments qui commutent dans l'anneau. Alors, pour tout $n \in \mathbb{N}$, on a :

$$a^n - b^n = (a-b) \times \sum_{k=0}^{n-1} a^k \times b^{n-1-k}.$$

3 Corps

Définition 11 Soit $(A,+,\times)$ un anneau commutatif. On dit que A est un ***corps*** si tous les éléments non nuls de A sont inversibles (c'est-à-dire que $A^* = A \setminus \{0_A\}$).

Exemple 10 Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.