

Fiche de cours Structures algébriques usuelles

Lois de composition interne, groupes, sous-groupes, morphismes, anneaux, corps

définitions · théorèmes et hypothèses · méthodes · démonstrations exigibles

1 LOIS DE COMPOSITION INTERNE

Définition. Soit E un ensemble. Une **loi de composition interne** sur E est une application $\star : E \times E \rightarrow E$; on note $x \star y$ l'image du couple (x, y) . Le fait que $x \star y$ appartienne à E fait partie de la définition : on dit que E est **stable** pour $\star$.

Définition. Soit $\star$ une loi sur E . On dit que $\star$ est

- **associative** si $\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$;
- **commutative** si $\forall (x, y) \in E^2, x \star y = y \star x$.

Un élément $e \in E$ est **neutre** pour $\star$ si $\forall x \in E, x \star e = e \star x = x$. Si $\star$ admet un neutre, celui-ci est **unique**.

Idée de preuve (unicité du neutre). Si e et e' sont neutres, $e \star e'$ vaut e (car e' est neutre) et e' (car e est neutre), donc $e = e'$.

Définition. Soit $\star$ une loi associative sur E , de neutre e . Un élément $x \in E$ est **inversible** (ou **symétrisable**) s'il existe $y \in E$ tel que $x \star y = y \star x = e$. Un tel y est alors **unique**, appelé **symétrique** (ou **inverse**) de x ; on le note x^{-1} en notation multiplicative, $-x$ en notation additive.

Idée de preuve (unicité du symétrique). Si y et y' conviennent, $y = y \star e = y \star (x \star y') = (y \star x) \star y' = e \star y' = y'$: c'est l'associativité qui donne l'unicité.

Propriété — inverse d'un produit. Si x et y sont inversibles pour une loi associative, alors $x \star y$ l'est, $(x^{-1})^{-1} = x$ et $(x \star y)^{-1} = y^{-1} \star x^{-1}$ (attention à l'ordre), car $(x \star y) \star (y^{-1} \star x^{-1}) = x \star (y \star y^{-1}) \star x^{-1} = e$, et de même de l'autre côté.

Définition. Soient $+$ et $\times$ deux lois sur E . On dit que $\times$ est **distributive** sur $+$ si, pour tous $x, y, z \in E$, $x(y + z) = xy + xz$ et $(y + z)x = yx + zx$: les deux égalités sont à exiger tant que $\times$ n'est pas supposée commutative.

Définition. Une partie $F \subset E$ est **stable** pour $\star$ si $\forall (x, y) \in F^2, x \star y \in F$. La loi $\star$ induit alors une loi sur F , appelée **loi induite**; elle hérite automatiquement de l'associativité et de la commutativité, mais pas du neutre ni de l'inversibilité.

✖ ATTENTION — neutre $\neq$ absorbant

Un élément a est **absorbant** si $a \star x = x \star a = a$ pour tout x : dans $\mathbb{R}$, 0 est neutre pour $+$ et absorbant pour $\times$. De même $\mathbb{N}$ est stable pour $+$, mais 2 n'y est pas inversible : la stabilité ne dit rien des inverses.

Notation — table de composition. Pour une loi sur un ensemble fini, la case (ligne x , colonne y) de la table contient $x \star y$. On y lit la commutativité (symétrie par rapport à la diagonale), le neutre (une ligne et une colonne recopiant les en-têtes) et les inverses (la présence de e); l'associativité, elle, ne se lit pas sur la table.

2 GROUPES

Définition. Un **groupe** est un couple $(G, \star)$ où $\star$ est une loi de composition interne sur G telle que (i) $\star$ est associative; (ii) $\star$ admet un élément neutre e ; (iii) tout élément de G est inversible pour $\star$. Si de plus $\star$ est commutative, le groupe est dit **abélien** (ou commutatif). Un groupe est toujours non vide, puisqu'il contient e .

Notation — puissances. En notation multiplicative, $x^0 = e$, $x^{n+1} = x^n x$ ($n \in \mathbb{N}$) et $x^{-n} = (x^n)^{-1} = (x^{-1})^n$; alors, pour $m, n \in \mathbb{Z}$, $x^{m+n} = x^m x^n$, $(x^m)^n = x^{mn}$, et $(xy)^n = x^n y^n$ **seulement si** $xy = yx$. En notation additive : $(m+n)x = mx + nx$, $n(mx) = (nm)x$, $n(x+y) = nx + ny$.

Propriété — régularité. Dans un groupe, tout élément a est **régulier** : $ax = ay \implies x = y$ et $xa = ya \implies x = y$ (multiplier par a^{-1} du bon côté); l'équation $ax = b$ a l'unique solution $x = a^{-1}b$.

Propriété — exemples usuels — à connaître.

■ FORMULAIRE

- **Groupes additifs** : $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont abéliens. $(\mathbb{N}, +)$ **n'est pas** un groupe.

- **Groupes multiplicatifs** : $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$ et $(\mathbb{U}_n, \times)$ ($n \geq 1$) sont abéliens. $(\mathbb{R}, \times)$ **n'est pas** un groupe (0 n'est pas inversible).
- **Groupe des permutations** : pour X non vide, l'ensemble $\mathfrak{S}_X$ des bijections de X sur X , muni de $\circ$, est un groupe de neutre id_X , l'inverse étant la bijection réciproque ; on note $\mathfrak{S}_n = \mathfrak{S}_{[1;n]}$. Il n'est pas abélien dès que $\text{Card } X \geq 3$.
- **Groupe produit** : $G \times H$ muni de $(x, y) \cdot (x', y') = (x \star x', y \star y')$ est un groupe, de neutre (e_G, e_H) et d'inverse (x^{-1}, y^{-1}) ; il est abélien si et seulement si G et H le sont.

3 SOUS-GROUPES

Définition. Soit $(G, \star)$ un groupe. Une partie $H \subset G$ est un **sous-groupe** de G si H est stable pour $\star$ et si $(H, \star)$ est lui-même un groupe (pour la loi induite).

Théorème — caractérisation d'un sous-groupe — démonstration exigible. Soit $H \subset G$. Alors H est un sous-groupe de G si et seulement si

$$(1) H \neq \emptyset \quad (\text{en pratique : } e \in H), \quad (2) \forall (x, y) \in H^2, x \star y \in H, \quad (3) \forall x \in H, x^{-1} \in H.$$

Ces trois conditions se condensent en : $e \in H$ et $\forall (x, y) \in H^2, x \star y^{-1} \in H$.

Idée de preuve. La condition (2) donne la loi induite, (3) les inverses ; (1) et (3) donnent $e = x \star x^{-1} \in H$, et l'associativité est héritée. Le neutre de H est nécessairement celui de G : si $e_H \star e_H = e_H$, la régularité dans G donne $e_H = e$.

Propriété. Les sous-groupes $\{e\}$ et G sont dits **triviaux**. Une intersection de sous-groupes de G est un sous-groupe de G ; une réunion, en général, n'en est pas un.

Théorème — les sous-groupes de $(\mathbb{Z}, +)$ — démonstration exigible. Les sous-groupes de $(\mathbb{Z}, +)$ sont exactement les ensembles

$$n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}, \quad n \in \mathbb{N},$$

et l'entier $n \in \mathbb{N}$ est déterminé de façon unique par le sous-groupe.

Idée de preuve. Chaque $n\mathbb{Z}$ est un sous-groupe. Réciproquement, soit H un sous-groupe. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon H contient un élément non nul, donc, par passage à l'opposé, un élément de $\mathbb{N}^*$: la partie non vide $H \cap \mathbb{N}^*$ de $\mathbb{N}$ admet un plus petit élément n , et $n\mathbb{Z} \subset H$ par stabilité. Inversement, pour $x \in H$, la division euclidienne $x = nq + r$ ($0 \leq r < n$) donne $r = x - nq \in H$; si $r > 0$, cela contredit la minimalité de n : donc $r = 0$ et $x \in n\mathbb{Z}$. L'unicité vient de $n\mathbb{Z} = m\mathbb{Z} \implies n \mid m$ et $m \mid n$.

Remarque. C'est, dans le langage des groupes, le raisonnement par division euclidienne du chapitre 11 (Bézout par le plus petit élément positif de $a\mathbb{Z} + b\mathbb{Z}$). On en déduit $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

4 MORPHISMES DE GROUPES

Définition. Soient $(G, \star)$ et $(H, *)$ deux groupes. Une application $f : G \rightarrow H$ est un **morphisme de groupes** si

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

Un morphisme *bijectif* est un **isomorphisme** ; deux groupes sont **isomorphes** s'il existe un isomorphisme de l'un sur l'autre. Un morphisme de G dans G est un **endomorphisme**, un isomorphisme de G sur G un **automorphisme**.

Propriété. Soit $f : G \rightarrow H$ un morphisme de groupes. Alors

$$f(e_G) = e_H, \quad \forall x \in G, f(x^{-1}) = f(x)^{-1}, \quad \forall n \in \mathbb{Z}, f(x^n) = f(x)^n.$$

La composée de deux morphismes est un morphisme ; la bijection réciproque d'un isomorphisme est un isomorphisme.

Idée de preuve. $f(e) = f(e \star e) = f(e) * f(e)$, et la régularité dans H donne $f(e) = e_H$; puis $f(x) * f(x^{-1}) = f(x \star x^{-1}) = f(e_H)$.

✗ ATTENTION

$f(e_G) = e_H$ est une *conséquence*, pas une hypothèse : inutile de l'exiger dans la définition. En revanche, pour montrer qu'une application n'est pas un morphisme, calculer $f(e_G)$ est souvent le test le plus rapide.

Théorème — image, image réciproque. Soit $f : G \rightarrow H$ un morphisme.

- Si K est un sous-groupe de G , alors $f(K)$ est un sous-groupe de H ; en particulier $\text{Im } f = f(G)$ est un sous-groupe de H .
- Si L est un sous-groupe de H , alors $f^{-1}(L)$ est un sous-groupe de G ; en particulier $\text{Ker } f = f^{-1}(\{e_H\}) = \{x \in G, f(x) = e_H\}$ est un sous-groupe de G .

Idée de preuve (exigible pour Ker et Im). $e_G \in \text{Ker } f$ car $f(e_G) = e_H$; si $x, y \in \text{Ker } f$, $f(x \star y^{-1}) = f(x) \star f(y)^{-1} = e_H$, donc $x \star y^{-1} \in \text{Ker } f$. Pour $\text{Im } f$: $e_H = f(e_G) \in \text{Im } f$, et $f(x) \star f(y)^{-1} = f(x \star y^{-1}) \in \text{Im } f$.

Théorème — critère d'injectivité — démonstration exigible. Un morphisme de groupes $f : G \rightarrow H$ est injectif si et seulement si $\text{Ker } f = \{e_G\}$. Il est surjectif si et seulement si $\text{Im } f = H$.

Idée de preuve. Si f est injective et $x \in \text{Ker } f$, alors $f(x) = e_H = f(e_G)$ donne $x = e_G$. Réciproquement, si $\text{Ker } f = \{e_G\}$ et $f(x) = f(y)$, alors $f(x \star y^{-1}) = e_H$, donc $x \star y^{-1} = e_G$, soit $x = y$.

Propriété — morphismes usuels — à connaître.

■ FORMULAIRE

- $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \times)$ est un isomorphisme, de réciproque $\ln$; $\text{Ker } \exp = \{0\}$.
- $t \mapsto e^{it}$ est un morphisme surjectif de $(\mathbb{R}, +)$ sur $(\mathbb{U}, \times)$, de noyau $2\pi\mathbb{Z}$.
- $z \mapsto |z|$ est un morphisme surjectif de $(\mathbb{C}^*, \times)$ sur $(\mathbb{R}_+^*, \times)$, de noyau $\mathbb{U}$.
- pour $n \geq 1$, $z \mapsto z^n$ est un morphisme surjectif de $(\mathbb{C}^*, \times)$ sur lui-même, de noyau $\mathbb{U}_n$.
- pour G un groupe et $x \in G$, $\varphi_x : (\mathbb{Z}, +) \rightarrow G, k \mapsto x^k$, est un morphisme, de noyau de la forme $n\mathbb{Z}$.

Remarque — hors programme — pour aller plus loin. L'entier n tel que $\text{Ker } \varphi_x = n\mathbb{Z}$ s'appelle l'ordre de x , et $\text{Im } \varphi_x$ le sous-groupe engendré par x : ces notions, comme les groupes *monogènes* et *cycliques*, ne sont pas au programme de MPSI (voir la feuille d'approfondissement).

5 ANNEAUX

Définition. Un **anneau** est un triplet $(A, +, \times)$ où

- $(A, +)$ est un groupe abélien, de neutre noté 0_A ;
- $\times$ est associative, admet un élément neutre noté 1_A , et est distributive sur $+$.

Dans ce programme, tout anneau est unitaire : l'existence de 1_A fait partie de la définition. L'anneau est **commutatif** si $\times$ l'est. L'anneau **nul** est $\{0\}$, le seul où $1_A = 0_A$.

Propriété — règles de calcul. Dans un anneau A , pour tous $a, b \in A$ et $n \in \mathbb{N}$:

■ FORMULAIRE

- $0 \times a = a \times 0 = 0$; $(-a)b = a(-b) = -(ab)$; $(-a)(-b) = ab$; $(na)b = n(ab)$ pour $n \in \mathbb{Z}$;
- **formule du binôme** : $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ si et seulement si l'on sait que $ab = ba$;
- **identité géométrique** : $a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$ ($n \geq 1$), là encore sous l'hypothèse $ab = ba$; en particulier

$$1 - a^n = (1 - a) \sum_{k=0}^{n-1} a^k$$
 sans aucune hypothèse, puisque a commute avec 1.

Idée de preuve de $0 \times a = 0$. $0a = (0 + 0)a = 0a + 0a$, et l'on simplifie dans le groupe $(A, +)$.

✖ ATTENTION

Sans l'hypothèse $ab = ba$, $(a + b)^2 = a^2 + ab + ba + b^2$ et rien de plus : pas de « $2ab$ ». L'anneau non commutatif de référence, $\mathcal{M}_n(\mathbb{K})$, est étudié au chapitre 13 : c'est là que ce piège coûte le plus cher.

Définition. Un élément $a \in A$ est **inversible** (on dit aussi : est une **unité**) s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des inversibles de A est noté $A^\times$ (ou $\mathcal{U}(A)$).

Théorème. $(A^\times, \times)$ est un groupe, appelé **groupe des inversibles** de A . Ce n'est presque jamais un sous-anneau de A (il ne contient pas 0).

Définition. Soit A un anneau. Un élément $a \in A$ est un **diviseur de zéro** s'il est non nul et s'il existe $b \neq 0$ tel que $ab = 0$ ou $ba = 0$. L'anneau A est **intègre** s'il est commutatif, non nul, et sans diviseur de zéro :

$$\forall (a, b) \in A^2, \quad ab = 0 \implies (a = 0 \text{ ou } b = 0).$$

Propriété. Dans un anneau intègre, tout élément non nul est régulier ($ab = ac$ et $a \neq 0$ entraînent $b = c$); un inversible n'est jamais diviseur de zéro.

Définition. Une partie $B \subset A$ est un **sous-anneau** de A si B est un sous-groupe de $(A, +)$, stable pour $\times$, et contient 1_A .

Théorème — caractérisation. $B \subset A$ est un sous-anneau de A si et seulement si $1_A \in B$ et $\forall (x, y) \in B^2, x - y \in B$ et $xy \in B$.

Définition. Soient A et B deux anneaux. Une application $f : A \rightarrow B$ est un **morphisme d'anneaux** si, pour tous $x, y \in A$, $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1_A) = 1_B$. Un morphisme bijectif est un **isomorphisme**. L'image d'un morphisme d'anneaux est un sous-anneau de B , et f envoie un inversible sur un inversible, avec $f(a^{-1}) = f(a)^{-1}$.

✗ ATTENTION

La condition $f(1_A) = 1_B$ est à **exiger** : elle ne découle pas des deux autres. Ainsi $f : \mathbb{R} \rightarrow \mathbb{R}^2, x \mapsto (x, 0)$, est additive et multiplicative pour les lois composante par composante, mais $f(1) = (1, 0) \neq (1, 1)$: ce n'est pas un morphisme d'anneaux. Noter aussi que $\text{Ker } f$ n'est pas un sous-anneau : c'est un idéal, notion hors programme.

Propriété — exemples usuels.

■ FORMULAIRE

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux commutatifs intègres; $\mathbb{Z}^\times = \{-1, 1\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$, $\mathbb{R}^\times = \mathbb{R}^*$, $\mathbb{C}^\times = \mathbb{C}^*$.
- $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ (**entiers de Gauss**) et $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}, (a, b) \in \mathbb{Z}^2\}$ sont des sous-anneaux de $\mathbb{C}$ et de $\mathbb{R}$.
- $\mathbb{R}^\mathbb{R}$ (fonctions de $\mathbb{R}$ dans $\mathbb{R}$), muni de $(f + g)(x) = f(x) + g(x)$ et $(fg)(x) = f(x)g(x)$, est un anneau commutatif *non intègre*, d'inversibles les fonctions qui ne s'annulent pas; idem pour $\mathbb{R}^\mathbb{N}$.
- Le **produit** $A \times B$ de deux anneaux, muni des lois composante par composante, est un anneau de neutres $(0_A, 0_B)$ et $(1_A, 1_B)$; il n'est *jamais* intègre si A et B sont non nuls, car $(1, 0)(0, 1) = (0, 0)$.

6 CORPS

Définition. Un **corps** est un anneau commutatif $\mathbb{K}$ tel que $1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ et dont tout élément non nul est inversible, c'est-à-dire $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$. Dans ce programme, les corps sont commutatifs.

Propriété. Tout corps est intègre : si $ab = 0$ avec $a \neq 0$, alors $b = a^{-1}(ab) = a^{-1} \times 0 = 0$. Un **sous-corps** de $\mathbb{K}$ est un sous-anneau L de $\mathbb{K}$ tel que tout élément non nul de L ait son inverse dans L .

Propriété — exemples. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps, et $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, lui-même sous-corps de $\mathbb{C}$; $\mathbb{Z}$ **n'est pas** un corps (2 n'y est pas inversible), ni $\mathbb{R}^\mathbb{R}$. Enfin $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{R}$, avec $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$.

► SAVOIR-FAIRE

- Vérifier qu'une loi est associative / commutative, trouver son neutre et ses inversibles; lire une table. Montrer qu'une partie est un sous-groupe par la caractérisation (*non-vacuité d'abord*), ou l'infirmier par un contre-exemple; déterminer les sous-groupes de $(\mathbb{Z}, +)$, calculer $n\mathbb{Z} \cap m\mathbb{Z}$ et $n\mathbb{Z} + m\mathbb{Z}$.
- Vérifier qu'une application est un morphisme, calculer $\text{Ker } f$ et $\text{Im } f$, en déduire injectivité et surjectivité; construire un isomorphisme.
- Montrer qu'une partie est un sous-anneau ou un sous-corps; déterminer $A^\times$; exhiber un diviseur de zéro; calculer dans un anneau (binôme et identité géométrique *après avoir vérifié la commutation*, inverse de $1 - a$ lorsque $a^n = 0$).

✗ PIÈGES

- Oublier $H \neq \emptyset$ (ou $e \in H$) : $\emptyset$ vérifie (2) et (3) sans être un sous-groupe. Vérifier la stabilité par la loi et oublier celle par passage à l'inverse : $\mathbb{N}$ dans $(\mathbb{Z}, +)$, $\mathbb{Z}$ dans $(\mathbb{Q}^*, \times)$.
- Appliquer le binôme ou $a^n - b^n$ dans un anneau sans avoir écrit « a et b commutent »; confondre neutre et élément absorbant; croire qu'une partie stable hérite du neutre ou des inverses.
- Croire que $\text{Ker } f$ est un sous-anneau, oublier $f(1_A) = 1_B$, dire « A est un corps » sans vérifier $1 \neq 0$ ($\mathbb{Z}, \mathbb{R}^\mathbb{R}$), ou utiliser $\mathbb{Z}/n\mathbb{Z}$ et les ensembles quotients (*hors programme* : on calcule avec les congruences du chapitre 11).