L14 - Structures algébriques usuelles

Plan

I. Lois de composition interne

1. Propriétés des lois de composition interne

Def. 1 On appelle **loi de composition interne** (en abrégé lci) sur un ensemble E toute application de $E \times E$ dans E.

Exemple 1

- L'addition et la multiplication sont des lois de composition interne dans les ensembles usuels de nombres $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$;
- Pour tout ensemble X, la réunion et l'intersection sont des lois de composition interne dans $E = \mathcal{P}(X)$;
- Dans $E = X^X$ (ensemble des applications de X dans X), la composition des applications, notée $\circ$, est une loi de composition interne.

Notations : une lci sur E est souvent notée $*$, $\top$, $\perp$, $+$, $\cdot$, $\circ$, ...
On écrit par exemple : $* : \begin{array}{ccc} E \times E & \longrightarrow & E \\ (x,y) & \longmapsto & x * y \end{array}$.

Def. 2 Une lci $*$ dans un ensemble E est dite **associative** si et seulement si :

$$\forall (x,y,z) \in E^3,\ (x*y)*z = x*(y*z).$$

Exemple 2

- L'addition et la multiplication sont associatives dans les ensembles usuels de nombres.

- La loi $* : \begin{array}{ccc} \mathbb{Q}\times\mathbb{Q} & \longrightarrow & \mathbb{Q} \\ (x,y) & \longmapsto & x*y=\dfrac{x+y}{2} \end{array}$ n'est pas associative.

  $\big((-1)*0\big)*1=\big(\dfrac{-1+0}{2}\big)*1=\dfrac{-1}{2}*1=\dfrac{\frac{-1}{2}+1}{2}=\dfrac{1}{4}$ et

  $(-1)*(0*1)=(-1)*\dfrac{1}{2}=\dfrac{-1+\frac{1}{2}}{2}=-\dfrac{1}{4}$.

- Dans $\mathcal{P}(X)$ la réunion et l'intersection sont associatives.
- Sur X^X, la composition des applications est associative : $(f\circ g)\circ h=f\circ(g\circ h)$.

Def. 3 Une lci $*$ dans un ensemble E est dite **commutative** si et seulement si :

$$\forall (x,y)\in E^2,\quad x*y=y*x.$$

Lorsque $x*y=y*x$, on dit que x et y **commutent**.

Exemple 3

- L'addition et la multiplication sont commutatives dans les ensembles usuels de nombres.
- La soustraction n'est pas commutative dans les ensembles usuels de nombres.
- Dans $\mathcal{P}(X)$ la réunion et l'intersection sont commutatives.

Remarque : La notation $+$ n'est généralement utilisée que pour une loi commutative.

Def. 4 Soit $*$ et $\top$ deux lois de composition interne sur E.
On dit que $*$ est **distributive** sur $\top$ si et seulement si :

$$\forall (x,y,z)\in E^3,\ x*(y\top z)=(x*y)\top(x*z)\ \text{ et }\ (x\top y)*z=(x*z)\top(y*z).$$

Exemple 4

- Dans $\mathbb{R}$, la multiplication est distributive sur l'addition.
- Dans $\mathbb{R}$, l'addition n'est pas distributive sur la multiplication :

$$2+(1\times 3)=2+3=5\quad\text{et}\quad(2+1)\times(2+3)=3\times 5=15.$$

- Dans $\mathcal{P}(X)$, l'intersection et la réunion sont chacune distributives par rapport à l'autre :

$$\forall A,B,C\in\mathcal{P}(X),\quad \begin{cases} A\cap\big(B\cup C\big)=\big(A\cap B\big)\cup\big(A\cap C\big)\\ A\cup\big(B\cap C\big)=\big(A\cup B\big)\cap\big(A\cup C\big)\end{cases}$$

2. Propriétés des éléments

Soit $*$ une loi de composition interne sur un ensemble E. On note aussi $(E,*)$ pour désigner E muni de la loi $*$.

Def. 5 Soit $e\in E$.
On dit que e est un **élément neutre** pour $*$ si et seulement si :

$$\forall x\in E,\ x*e=e*x=x.$$

Prop. 1 **Unicité de l'élément neutre** (s'il existe)
Si e et e' sont des éléments neutres pour $*$ dans E, alors $e = e'$.

Démo. 1

Exemple 5

- Sur $\mathbb{R}$, 0 est l'élément neutre pour l'addition et 1 est l'élément neutre pour la multiplication.
- Sur $\mathcal{P}(X)$, X est l'élément neutre pour l'intersection et $\emptyset$ est l'élément neutre pour la réunion.
- Sur X^X, l'application id_X est l'élément neutre pour la composition de fonctions.

Def. 6 Soit E muni d'une lci $*$ et possédant un élément neutre e.
Un élément x de E est dit **symétrisable** si et seulement si :

$$\exists y \in E, \quad x * y = y * x = e.$$

Un tel élément y est appelé un symétrique de x.

Prop. 2 Soit E muni d'une lci $*$ **associative**, possédant un élément neutre e.
Si x est symétrisable pour $*$, alors x admet un unique symétrique pour $*$.

Démo. 2

Remarques :

- lorsque la loi est notée multiplicativement, le symétrique de x est noté x^{-1} et appelé **inverse** de x. On dit aussi que x est **inversible**.
- lorsque la loi est notée additivement, le symétrique de x est noté $-x$ et appelé **opposé** de x.
- Si $(E, *)$ admet un élément neutre e, alors e est symétrisable et son symétrique est lui même.

Exemple 6

- Pour l'addition dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, tout élément admet un opposé.
- Pour la multiplication dans $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, tout élément non nul admet un inverse.
- Dans $(X^X, \circ)$ les éléments symétrisables sont les bijections. On parle aussi d'inverse de f notée f^{-1}.

Prop. 3 Soit E muni d'une lci $*$ associative et possédant un élément neutre e.

Si a et b sont symétrisables pour $*$, alors $a * b$ est symétrisable et :

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

Démo. 3

Exemple 7 Si f et g sont deux bijections de X^X, alors $f \circ g$ est bijective et $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Exemple 8 Si E est muni d'une lci $*$ associative et possède un élément neutre e, soit x symétrisable, alors :

$$\forall (a,b) \in E^2, \begin{cases} x * a = x * b \Longrightarrow a = b \\ \text{et} \\ a * x = b * x \Longrightarrow a = b \end{cases}$$

Def. 7 - Prop. 4 **Itérés d'un élément**

Soit E muni d'une lci associative $*$ et possédant un élément neutre e.

• Soit $x \in E$ et $n \in \mathbb{N}$. On définit l'itéré $n-$ième de x par récurrence :

$$x^0 = e \quad \text{et} \quad x^{n+1} = x * (x^n) = (x^n) * x.$$

• Si x est inversible alors, pour tout $n \in \mathbb{N}$, x^n est inversible et son inverse est $(x^{-1})^n$ que l'on note x^{-n}.

Démo. 4

Prop. 5 Soit $x \in E$.

$$\forall (p,q) \in \mathbb{N}^2, \quad x^{p+q} = x^p * x^q \quad \text{et} \quad (x^p)^q = x^{pq}.$$

Démo. 5

Remarque : $p + q = q + p$, donc les itérés de x commutent deux à deux.

3. Partie stable, loi induite

Def. 8 Soit E un ensemble muni d'une lci $*$ et F une partie de E.
On dit que F est **stable** par $*$ lorsque : $\forall (x,y) \in F^2$, $x * y \in F$.

On définit alors une loi de composition interne sur F par $\begin{array}{ccc} F \times F & \longrightarrow & F \\ (x,y) & \longmapsto & x * y \end{array}$,
appelée **loi induite** par $*$ sur F.

Exemple 9

- $\mathbb{R}^*$ et $\mathbb{C}^*$ sont stables pour les multiplications respectives de $\mathbb{R}$ et $\mathbb{C}$;
- $\mathbb{U}$ est stable pour la multiplication de $\mathbb{C}$;
- L'ensemble des injections et l'ensemble des surjections de X dans X sont des parties stables de X^X pour $\circ$.

II. Groupes et sous-groupes

1. Structure de groupe

Def. 9 Soit G un ensemble muni d'une loi de composition interne $*$.
On dit que $(G, *)$ est un groupe si :

1) la loi $*$ est associative, et il y a un élément neutre e.

2) tout élément de G possède un symétrique pour la loi $*$.

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

Remarques :

- Par définition, un groupe est non vide car il possède au moins l'élément neutre.
- Si la loi est notée $+$, on dit que G est un groupe additif. Le neutre est noté 0, $+$ est toujours supposée commutative, et on note $-x$ l'opposé de x, pour tout $x \in G$.
- Si la loi est notée $\times$, on dit que $(G, \times)$ est un groupe multiplicatif.

Notations :

- Pour un groupe multiplicatif, on note $x^n = xx \cdots x$ (n fois) ;
- Pour un groupe additif, on note $nx = x + x + \cdots + x$ (n fois).

Exemple 10 - Groupes usuels

- Les ensembles $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes abéliens.
- Les ensembles $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}^{+*}, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}^{+*}, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes multiplicatifs.
- Les ensembles $(\mathbb{U}, \times)$ et $(\mathbb{U}_n, \times)$ sont des groupes multiplicatifs.

Exemple 11 Soit $n \in \mathbb{N}^*$. On munit $E = \mathbb{R}^n$ de la loi *somme* définie par :

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n).$$

Alors, $(E, +)$ est un groupe commutatif. Le neutre est $e = (0, \cdots, 0)$ et l'opposé de $(x_1, \cdots, x_n)$ est $(-x_1, \cdots, -x_n)$.

Def. 10 - Prop. 6 Soit E un ensemble. On note $\mathcal{S}_E$ l'ensemble des bijections de E dans E (ensemble des **permutations** de E dans E).
$\mathcal{S}_E$ est un groupe pour la loi de composition des applications $\circ$, appelé **groupe des permutations** de E.

Démo. 6

Remarques :

- L'élément neutre de $\mathcal{S}_E$ est Id_E.
- Si E possède au moins trois éléments distincts, le groupe $\mathcal{S}_E$ est non commutatif.

Def. 11 - Prop. 7 **Groupe produit**
Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes, d'éléments neutres respectifs e_1 et e_2. On définit une loi de composition interne $*$ sur $G_1 \times G_2$ en posant :

$$\forall\big((x,y),(x',y')\big) \in \big(G_1 \times G_2\big)^2,\ (x,y) * (x',y') = (x *_1 x', y *_2 y').$$

Alors $(G_1 \times G_2, *)$ est un groupe, appelé **groupe produit**, d'élément neutre (e_1, e_2) et tel que :

$$\forall (x,y) \in G_1 \times G_2,\ (x,y)^{-1} = (x^{-1}, y^{-1}).$$

Démo. 7

2. Sous-groupes

Def. 12 Soit $(G, *)$ un groupe. Une partie H de G est un **sous-groupe** de G si :

1) H est non vide ;

2) H est stable pour la loi $*$: $\forall (x,y) \in H^2,\ x * y \in H$;

3) H est « stable par passage à l'inverse » : $\forall x \in H,\ x^{-1} \in H$.

Exemple 12 Soit $n \in \mathbb{N}$, l'ensemble $n\mathbb{Z} = \{nk \,/\, k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Prop. 8 Soit H un sous-groupe de $(G, *)$. Alors H muni de la loi induite par $*$ est un groupe.

Démo. 8

Méthode

Méthode la plus rapide pour prouver qu'un ensemble est un groupe : prouver que c'est un sous-groupe d'un groupe de référence.

Prop. 9 **Caractérisation des sous-groupes**
Soit $(G, *)$ un groupe et H une partie de G. Les assertions suivantes sont équivalentes :

1) H est un sous-groupe de $(G, *)$.

2) H est non vide, stable pour la loi $*$ et par passage à l'inverse :

$$\forall (x,y) \in H^2, x * y \in H \text{ et } x^{-1} \in H.$$

3) H est non vide et $\forall (x,y) \in H^2,\ x * y^{-1} \in H$.

Démo. 9

Remarques :

1) Pour montrer que H est non vide, on prouve généralement que e (neutre de G) est dans H.

2) Si on a un groupe additif, les différentes caractérisations peuvent avec $x+y$ ou $x-y$ à la place de $x*y$ ou $x*y^{-1}$.

Exemple 13

- Si $(G,*)$ est un groupe, alors $\{e\}$ et G sont deux sous-groupes de G. On parle de *sous-groupes triviaux.*
- $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Q},+)$, $(\mathbb{Q},+)$ est un sous-groupe de $(\mathbb{R},+)$ et $(\mathbb{R},+)$ est un sous-groupe de $(\mathbb{C},+)$.
- $(\{-1,1\},\times)$ est un sous-groupe de $(\mathbb{Q}^*,\times)$, etc ...
- $(\mathbb{U},\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$, $(\mathbb{U}_n,\times)$ est un sous-groupe de $(\mathbb{U},\times)$.

Prop. 10 Soit $(G,*)$ un groupe et $(G_i)_{i\in I}$ une famille de sous-groupes de G.
Alors $\displaystyle\bigcap_{i\in I} G_i$ est un sous-groupe de G.

Démo. 10

Remarque : en général, la réunion d'une famille de sous-groupes n'est pas un sous-groupe.

3. Morphismes de groupes

Def. 13 Soit $(G,*)$ et $(G',\times)$ deux groupes, et f une fonction de G dans G'.
On dit que f est un **morphisme de groupes** lorsque :

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

Si $G=G'$, on dit que f est un **endomorphisme** de groupes.

Un morphisme de groupes bijectif est appelé **isomorphisme** de groupes.
Un endomorphisme bijectif est appelé **automorphisme** de groupes.

Prop. 11 Soit G et G' deux groupes, d'éléments neutres respectifs e et e', et f un morphisme de groupe de G dans G'. On a :

- $f(e)=e'$,
- $\forall x\in G,\ \big(f(x)\big)^{-1}=\big(f(x^{-1})\big)$,
- $\forall x\in G,\ \forall n\in\mathbb{Z},\ \big(f(x)\big)^n=f\big(x^n\big)$.

Démo. 11

Prop. 12
- La composée de deux morphismes de groupes est un morphisme de groupes.
- La bijection réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

Démo. 12

Exemple 14 exp : $(\mathbb{R},+) \to (\mathbb{R}_+^*,\times)$ et ln : $(\mathbb{R}_+^*,\times) \to (\mathbb{R},+)$ sont deux isomorphismes de groupes.

Prop. 13 Si on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de groupe de G, alors $(\mathrm{Aut}(G),\circ)$ est un groupe.

Démo. 13 - Sous-groupe de $\mathcal{S}_G$.

4. Noyau, image

Soit G et G' deux groupes, d'éléments neutres respectifs e et e', et f un morphisme de groupe de G dans G'.

Prop. 14 **Image et image réciproque d'un sous-groupe par un morphisme**
- si H est un sous-groupe de G, alors $f(H)$ est un sous-groupe de G'.
- si H' est un sous-groupe de G', alors $f^{-1}(H')$ est un sous-groupe de G.

Démo. 14

Def. 14 - Prop. 15
- L'ensemble $f(G)$, appelé **image de** f, est un sous-groupe de G'. On le note $\mathrm{Im}(f)$.
- L'ensemble $f^{-1}\big(\{e'\}\big)$, appelé **noyau de** f, est un sous-groupe de G. On le note $\mathrm{Ker}(f)$.

Démo. 15

Exemple 15 L'application $\mathbb{R} \to \mathbb{U}$, $\theta \mapsto e^{i\theta}$ est un morphisme de groupes.
Son noyau est $2\pi\mathbb{Z}$.

Exemple 16 L'application exp : $\mathbb{C} \to \mathbb{C}^*$ est un morphisme de groupes.
Son noyau est $2i\pi\mathbb{Z}$.

Prop. 16 f est injective si et seulement si $\mathrm{Ker}(f) = \{e\}$.
f est surjective si et seulement si $\Im(f) = G'$.

Démo. 16

Preuve de f injective

Si f est un morphisme de groupe, pour montrer l'injectivité de f, il suffit de vérifier :

$$\forall x \in G,\ f(x) = e' \Longrightarrow x = e.$$

Exercice 1 **Exercice type**

Soit G un groupe, $g \in G$, on note γ_g l'application définie par :

$$\gamma_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g * x \end{array}$$

1) Montrer que γ_g est une bijection de G. On l'appelle translation à gauche.

2) Montrer que $G \to \mathcal{S}_G$, $g \mapsto \gamma_g$ est un morphisme injectif de groupe.

3) Montrer que G est isomorphe à un sous-groupe de $\mathcal{S}_G$.

5. Calculs dans un groupe

- Soit $g \in G$. On introduit les applications γ_g et δ_g, respectivement appelées translation à gauche et translation à droite :

$$\gamma_g : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & g * x \end{array} \quad \text{et} \quad \delta_g \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x * g \end{array}$$

  γ_g et δ_g sont bijectives, d'applications réciproques respectives $\gamma_{g^{-1}}$ et $\delta_{g^{-1}}$.

- Dans un groupe G, **tout élément est simplifiable** :

$$\forall (x, y, z) \in G^3, \begin{cases} x * y = x * z & \Longrightarrow & y = z \\ y * x = z * x & \Longrightarrow & y = z \end{cases}$$

  On a en fait des équivalences, les implications réciproques étant toujours vraies et triviales.

- **Résolution d'équation dans un groupe** :
  Soit a et b dans G.
  L'équation $a * x = b$ d'inconnue x, possède une solution unique $x = a^{-1} * b$.
  L'équation $x * a = b$ d'inconnue x, possède une solution unique $x = b * a^{-1}$.

III. Anneaux et corps

1. Structure d'anneau

Def. 15 Soit A un ensemble muni de deux lois de composition internes, notées $+$ et $\times$.
On dit que $(A, +, \times)$ est un **anneau** si :

1) $(A, +)$ est un groupe commutatif ;

2) A possède un élément neutre pour $\times$;

3) $\times$ est associative et distributive par rapport à $+$.

On dit que l'anneau est **commutatif** si $\times$ est commutative.

Notations usuelles - Dans un anneau A :

- on note 0, ou 0_A, l'élément neutre pour la loi $+$;
- on note 1, ou 1_A, l'élément neutre pour la loi $\times$;

- on note couramment $x.y$ ou xy à la place de $x \times y$;
- on utilise simultanément les deux notations :
  - $n.a$ ou na avec $n \in \mathbb{Z}$ pour l'itéré additif ;
  - a^n avec $n \in \mathbb{N}$ (ou $n \in \mathbb{Z}$ si a est inversible) pour l'itéré multiplicatif.

Remarque : $\forall x \in A$, $x^0 = 1_A$, et en particulier $0_A^0 = 1_A$.

Exemple 17 Exemples usuels : $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des anneaux commutatifs pour l'addition et la multiplication usuelles.

2. Calculs dans un anneau

Prop. 17 Soit A un anneau. On a les propriétés suivantes :
- 0 est absorbant : $\forall a \in A$, $0 \times a = a \times 0 = 0$.

- Règle des signes : $\forall (a,b) \in A^2$, $(-a) \times b = a \times (-b) = -(a \times b)$.

Démo. 17

Remarque : soit A un anneau tel que $0_A = 1_A$.
Pour tout $x \in A$, $x = 1_A.x = 0_A.x = 0_A$. Donc $A = \{0_A\}$.
Un tel anneau est appelé **anneau nul**, ou **anneau trivial**.

Prop. 18 Si $(a_i)_{i\in I}$ est une famille **finie** d'éléments d'un anneau A, on a :

$$\forall x \in A, \quad x\Big(\sum_{i\in I} a_i\Big) = \sum_{i\in I} x a_i \quad \text{et} \quad \Big(\sum_{i\in I} a_i\Big)x = \sum_{i\in I} a_i x.$$

Démo. 18 - Récurrence sur le nombre d'éléments de I, utilisation de la distributivité.

Prop. 19 **Distributivité généralisée**
Si $(a_i)_{i\in I}$ et $(b_j)_{j\in J}$ sont deux familles d'éléments d'un anneau A, indexées par des ensembles **finis** I et J :

$$\Big(\sum_{i\in I} a_i\Big)\Big(\sum_{j\in J} b_j\Big) = \Big(\sum_{(i,j)\in I\times J} a_i b_j\Big).$$

Démo. 19 - Récurrence sur le nombre d'éléments de I, l'ensemble J étant fixé.

Application : développement du carré d'une somme dans un anneau.

$$(a1 + \cdots + a_n)^2 = \sum_{k=1}^{n} a_k^2 + \sum_{1\ \leq i\neq j\leq n} a_i a_j.$$

Si l'anneau est commutatif, ou si les termes de la somme commutent deux à deux, on obtient :

$$(a1 + \cdots + a_n)^2 = \sum_{k=1}^{n} a_k^2 + 2 \sum_{1\ \leq i<j\leq n} a_i a_j.$$

Prop. 20 Soit a et b deux éléments d'un anneau A tels que $ab = ba$. On a alors :

- **Formule du binôme de Newton**

$$\forall n \in \mathbb{N},\, (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

- **Factorisation de $a^n - b^n$**

$$\forall n \in \mathbb{N}^*,\, a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k} b^k.$$

Démo. 20

Exemple 18 Cas particuliers dans $\mathbb{R}$ ou $\mathbb{C}$:

- $a^2 - b^2 = (a-b)(a+b)$
- $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$

Exemple 19 Dans un anneau le neutre 1_A commute avec tous les éléments de A.
On a la factorisation :

$$\forall n \in \mathbb{N}^*,\, \forall a \in A,\, 1 - a^n = (1-a)\sum_{k=0}^{n-1} a^k = (1-a)(1 + a + a^2 + \cdots + a^{n-1}).$$

Def. 16 **Anneau intègre**
Un anneau intègre est un anneau commutatif, différent de $\{0\}$, et tel que :

$$\forall (a,b) \in A^2,\, ab = 0 \Longrightarrow (a = 0 \,\mathrm{ou}\, b = 0).$$

Autre formulation : A anneau commutatif tel que $0_A \neq 1_A$ et sans diviseur de 0.

3. Sous-anneaux

Def. 17 Soit un anneau $(A, +, \times)$ et B une partie de A. On dit que B est un sous-anneau de A lorsque :

1) $1_A \in B$;

2) $\forall (x,y) \in B^2,\, x - y \in B$;

3) $\forall (x,y) \in B^2, x \times y \in B$.

Autre formulation : B est un sous-groupe de $(A, +)$ contenant 1_A et stable par $\times$.

Remarques :

- Si B est un sous-anneau de A, alors B est un anneau pour les lois induites par $+$ et $\times$.
- Si B est un sous anneau de $(A, +, \times)$ alors c'est un sous-groupe de $(A, +)$.

Exemple 20 $\mathbb{Z}$ est un sous-anneau de $(\mathbb{C},+,\times)$.
Si A est un sous-anneau de $(\mathbb{C},+,\times)$ alors $\mathbb{Z}\subset A$.

Exemple 21 L'ensemble noté $\mathbb{Z}[i]=\{a+ib,\ (a,b)\in\mathbb{Z}^2\}$, ensemble des entiers de Gauss, est un sous-anneau de $\mathbb{C}$.

4. Morphismes d'anneaux

Def. 18 Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux. On dit que $f:A\to B$ est un morphisme d'anneaux lorsque :

1) $\forall (x,y)\in A^2,\ f(x+y)=f(x)+f(y)$;

2) $\forall (x,y)\in A^2,\ f(x\times y)=f(x)\times f(y)$;

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

Remarques :

- Si f est un morphisme d'anneaux alors f est un morphisme de groupes de $(A,+)$ dans $(B,+)$.
- On conserve le vocabulaire : endomorphisme (cas $A=B$), isomorphisme (cas f bijective), automorphisme (f bijective et $A=B$).
- On peut parler du noyau de f et on a toujours : $\mathrm{Ker}(f)=\{0_A\}\Leftrightarrow f$ est injectif.

Prop. 21 Soit $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f:A\to B$ un morphisme d'anneaux. On a :

$$\forall a\in A,\ \forall n\in\mathbb{Z},\ f(n.a)=n.f(a).$$

$$\forall a\in A,\ \forall\in\mathbb{N},\ f\big(a^n\big)=\big(f(a)\big)^n.$$

Soit $a\in A$. Si a est inversible alors $f(a)$ est inversible et :

$$\forall n\in\mathbb{Z},\ f\big(a^n\big)=\big(f(a)\big)^n.$$

Démo. 21

Prop. 22 La composée de deux morphismes d'anneaux est un morphisme d'anneaux.
Si f est un isomorphisme d'anneau alors f^{-1} est un isomorphisme d'anneaux.

Démo. 22

5. Éléments inversibles, unités

Def. 19 On appelle **inversible**, ou **unité**, de A, tout élément de A inversible pour la multiplication (loi $\times$).
On note A^* l'ensemble des éléments inversibles de A.

Rappel : sous réserve d'existence, il y a unicité de l'inverse de a qui est noté a^{-1}.

Prop. 23 **Groupe des éléments inversibles d'un anneau**
Soit $(A, +, \times)$ un anneau.
L'ensemble des éléments de A qui sont inversibles pour le produit est un groupe pour la loi $\times$.

Démo. 23

Exemple 22

- Le groupe des inversibles de l'anneau $(\mathbb{Z}, +, \times)$ est l'ensemble $\{-1, 1\}$.
- Le groupe des inversibles de l'anneau $(\mathbb{R}, +, \times)$ est l'ensemble de tous les réels non nuls.

6. Corps

Def. 20 Un corps est un anneau commutatif non trivial $(\mathbb{K}, +, \times)$ dont tous les éléments non nuls sont inversibles.

Exemple 23 $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
$\mathbb{Z}$ n'est pas un corps.

Prop. 24 Un corps est un anneau intègre :

$$\forall (a, b) \in \mathbb{K}^2,\ ab = 0 \Longrightarrow (a = 0 \,\text{ou}\, b = 0).$$

Démo. 24

Def. 21 Soit $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L}$ une partie de $\mathbb{K}$. On dit que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ lorsque :

1) $\mathbb{L}$ est un sous-anneau de $\mathbb{K}$;

2) $\forall x \in \mathbb{L} \setminus \{0\},\ x^{-1} \in \mathbb{L}$.

Remarques :

- $(\mathbb{L}, +, \times)$ est alors un corps pour les lois induites.
- Si $\mathbb{K}$ est un sous-corps de $\mathbb{C}$, alors $\mathbb{Q} \subset \mathbb{K}$.