Chapitre 12 : Structures algébriques usuelles

1 Lois de composition interne

Définition 1 (Loi de composition interne).

*Une **loi de composition interne ou opération interne** sur un ensemble E est une application de $E \times E$ vers E.*
Notation : $E \times E \longrightarrow E$, $(x, y) \mapsto x * y$. Un ensemble muni d'une opération interne $(E, *)$ est appelé un magma.

▶ Exemple : : $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \times)$, $(\mathbb{R}^3, \wedge)$, $(\mathbb{R}^3, +)$, ... Mais $\times$ n'est pas une loi externe sur $\mathbb{R}^-$ car le produit de deux nombres réels négatifs n'est pas un nombre réel négatif.

Définition 2 (Partie stable pour $*$).

*On dit que A est **stable** pour $*$ ssi $\forall (a, a') \in A^2,\ a * a' \in A$.*
*La restriction à A de la loi $*$ est une loi de composition interne sur A, appelée loi de composition interne **induite** par $*$ sur A.*

▶ Exemple : : Dans $(\mathbb{Z}, +)$, $\mathbb{N}$ est stable.
Dans $(\mathbb{Z}, \times)$, $\mathbb{N}$ est stable alors que $\mathbb{Z}^-$ ne l'est pas.

Définition 3 (Loi produit).

*Soient $(E, *)$ et $(F, \perp)$ deux magmas. On appelle **loi de composition interne produit sur** $E \times F$ la loi de composition définie par :*

$$(E \times F)^2 \longrightarrow E \times F,\ ((x, y), (x', y')) \mapsto (x * x', y \perp y').$$

▶ Exemple : : $(\mathbb{R}^{+*} \times \mathbb{R})^2 \longrightarrow \mathbb{R}^{+*} \times \mathbb{R},\ ((r, \theta), (r', \theta')) \mapsto (rr', \theta + \theta')$.

2 Propriétés éventuelles

Soit $(E, *)$ un magma.

Définition 4 (Commutativité).

*On dit que $*$ est **commutative** sur E lorsque $\forall (x, y) \in E^2,\ x * y = y * x$.*

▶ Exemple : : $+$ dans $\mathbb{R}$, $\times$ dans $\mathbb{R}$.
Non commutativité : $\exists (x, y) \in E^2,\ x * y \neq y * x$.

Définition 5 (Associativité).

*On dit que $*$ est **associative** sur E lorsque $\forall (x, y, z) \in E^3,\ (x * y) * z = x * (y * z)$.*

▶ Exemple : : $+$ et $\times$ dans $\mathbb{C}$.
$\wedge$ n'est pas associatif dans $\mathbb{R}^3$.

Définition 6 (Elément neutre).

*Soit $e \in E$, e est **élément neutre** pour $*$ dans E ssi $\forall x \in E,\ e * x = x = x * e$.*

▶ Exemple : : 0 est élément neutre pour $+$ dans $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$. 1 est élément neutre pour $\times$ dans $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

Propriété 1 (Unicité de l'élément neutre).

Si $(E, *)$ possède un élément neutre, celui-ci est unique.

Définition 7 (Elément inversible).

*Soit $(E, *)$ un magma tel que $*$ soit une loi associative et possédant un élément neutre e. Soit $x \in E$, x est **symétrisable ou inversible pour $*$ dans E** ssi $\exists y \in E,\ x * y = e = y * x$. y est appelé **symétrique ou inverse** de x et noté en général x^{-1}.*

▶ Exemple : : Dans $(\mathbb{R}, +)$ tout élément x possède un symétrique : $x^{-1} = -x$, appelé opposé.
Dans $(\mathbb{R}, \times)$ tout élément x non nul possède un symétrique : $x^{-1} = \dfrac{1}{x}$, appelé inverse.
Dans $(\mathbb{Z}, \times)$ les éléments symétrisables sont 1 et -1.
Dans $(\mathbb{N}, +)$ l'élément symétrisable est 0.

Propriété 2 (Inversibilité et inverse du produit de deux éléments inversibles).

Soit $(E, *)$ un magma tel que $*$ est associative et possédant un élément neutre e. Soit $(x, y) \in E^2$, $x * y$ est symétrisable et $(x * y)^{-1} = y^{-1} * x^{-1}$.

Remarque 1. *L'élément neutre s'il existe est toujours symétrisable et $e = e^{-1}$.*

Définition 8 (Elément idempotent).

*Soit $x \in E$, x est **idempotent** ssi $x * x = x$. $\forall n \in \mathbb{N}^*,\ x^n = ((x * x) * \cdots) \cdots) * x = x$. La loi est dite idempotente ssi tout élément est idempotent, ssi $\forall x \in E, x * x = x$.*

Remarque 2. *Si l'élément neutre existe, il est idempotent.*

Définition 9 (Distributivité).

Soit E muni de deux lois de composition interne $*$ et $\perp$.
*$*$ est **distributive par rapport à $\perp$** ssi*
$\forall (x, y, z) \in E^3,\ x * (y \perp z) = (x * y) \perp (x * z)$ (distributivité à gauche) et
$(y \perp z) * x = (y * x) \perp (z * x)$ (distributivité à droite).

▶ Exemple : : Soit E un ensemble. Sur $\mathcal{P}(E)$, vérifier que $\cup$ et $\cap$ sont des lois de composition interne et étudier leurs propriétés.

3 Groupes

Définition 10 (Groupe).

*Soit E un ensemble. $(E, *)$ est un **groupe** ssi*
- *$*$ est une loi de composition interne dans E,*
- *$*$ est associative,*
- *E possède un élément neutre e pour $*$,*
- *tout élément de E est symétrisable.*

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

▶ Exemple : : $(\mathbb{Z}, +), (\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes abéliens (groupes additifs usuels).
$(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}_+^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{U}, \times)$, $(\mathbb{U}_n, \times)$ sont des groupes abéliens (groupes multiplicatifs

usuels).

$(\mathbb{N},+)$ n'est pas un groupe.
$(\mathbb{R},\times)$ n'est pas un groupe.
$(\mathbb{R}^*,+)$ n'est pas un groupe.

Propriété 3.

Soit $(E,*)$ un groupe et e son élément neutre.

1. *Soit $x\in E$, le symétrique de x est unique.*
2. *Soit $x\in E$, x^{-1} est également symétrisable et $(x^{-1})^{-1}=x$.*
3. *Soit $(x,y)\in E^2$, $x*y$ est symétrisable et $(x*y)^{-1}=y^{-1}*x^{-1}$.*

Itéré d'un élément : dans un groupe additif on note $x*x*\cdots*x=nx$ alors que dans un groupe multplicatif on note $x*x*\cdots*x=x^n$.

Définition 11 (Groupe des permutations).

Si X est un ensemble, on appelle groupe des permutations de X (ou groupe symétrique de X) l'ensemble des bijections de X vers X. On le note S_X. $(S_X,\circ)$ est un groupe.

Cas particulier : lorsque $X=\{1,2,\cdots,n\}$, on note $S_X=S_n$ et S_n a n! éléments. C'est l'étude par Galois du groupe des permutations des racines d'un polynômme qui a conduit à la définition abstraite de groupe.

Définition 12 (Groupe produit).

Soient $(E,*)$ et $(F,\perp)$ deux groupes. On définit sur $E\times F$ la loi de composition $\otimes$: $(x,y)\otimes(x',y')=(x*x',y\perp y')$. $(E\times F,\otimes)$ est un groupe appelé groupe produit.

Définition 13 (Sous-groupe).

Soit H une partie de G. On dit que $(H,*)$ est un ***sous-groupe*** *de $(G,*)$ lorsque :*
— *H est stable par $*$,*
— *$(H,*)$ a une structure de groupe.*

Remarque 3. *Si $*$ est associative dans E alors son application induite l'est encore sur A.*
Si $*$ est commutative dans E alors son application induite l'est encore sur A.
Sous-groupe trivial.

▶ Exemple : Soit $n\in\mathbb{N}$. $(n\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$. $(\mathbb{U},\times)$ est un sous-groupe de $(\mathbb{C}^*,\times)$.

Propriété 4.

Soit $(G,*)$ un groupe et $H\subset G$. Alors $(H,*)$ est un sous-groupe de $(G,*)$ ssi

1. *H est stable par $*$,*
2. *$e\in H$ (où e est l'élément neutre de $(G,*)$)*
3. *$\forall x\in H\quad x^{-1}\in H$ (où x^{-1} est le symétrique de x pour $*$ dans G)*

Propriété 5.

Soit $(G,*)$ un groupe et $H\subset G$. Alors $(H,*)$ est un sous-groupe de $(G,*)$ ssi

1. *$H\neq\emptyset$*
2. *$\forall x,y\in H,\quad x*y^{-1}\in H$.*

4 Anneaux

4.1 Définition

Définition 14.

Soit A un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $(A,+,\times)$ est un anneau lorsque :
- *$(A,+)$ est un groupe commutatif (son élément neutre pour $+$ est noté 0_A et le symétrique de $a\in A$ pour $+$ est noté $-a$),*
- *$\times$ est associative et distributive par rapport à $+$,*
- *A possède un élément neutre pour $\times$ (noté 1_A).*

De plus, si $\times$ est commutative on dit que $(A,+,\times)$ est un anneau commutatif.

▶ Exemples :
- $(\mathbb{Z},+,\times)$,
- $(\mathbb{Q},+,\times)$,
- $(\mathbb{R},+,\times)$,
- $(\mathbb{C},+,\times)$,
- $(\mathbb{R}^{\mathbb{N}},+,\times)$

sont des anneaux commutatifs.
- Si I est un ensemble non vide, on définit sur $\mathcal{F}(I,\mathbb{R})$ deux lois de composition interne par : si $(f,g)\in(\mathcal{F}(I,\mathbb{R}))^2$, $f+g$ est l'élément de $\mathcal{F}(I,\mathbb{R})$ défini par : $\forall x\in I,(f+g)(x)=f(x)+g(x)$ et fg est l'élément de $\mathcal{F}(I,\mathbb{R})$ défini par : $\forall x\in I,(fg)(x)=f(x)g(x)$.
  $(\mathcal{F}(I,\mathbb{R}),+,\times)$ est un anneau commutatif. L'élément neutre pour $+$ est $0 : I\longrightarrow\mathbb{R},\ x\mapsto 0$. L'élément neutre pour $\times$ est $1 : I\longrightarrow\mathbb{R},\ x\mapsto 1$.
- Si A et B sont des anneaux alors $A\times B$ muni des lois produit est un anneau.
- Muni de l'addition et de la multiplication, l'ensemble des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif. On le démontrera le temps voulu.

4.2 Calculs dans un anneau

Notations :

↬ On note $x.y$ ou xy à la place de $x\times y$.

↬ **Notation additive** :
- La somme des n éléments $x_1,...,x_n$ est notée $\sum_{1\leqslant p\leqslant n} x_p$ ou $\sum_{p=1}^{n} x_p$.
- n^{ieme} itéré additif. Soit $x\in A$ et $n\in\mathbb{N}^*$, on note nx l'élément de A défini par $\sum_{1\leqslant p\leqslant n} x$(somme de n termes tous égaux à x) ; et pour $n\in\mathbb{Z}_-$, on note nx aussi pour $\sum_{1\leqslant p\leqslant -n} -x$ (somme de $-n$ termes tous égaux à $-x$). Si $n=0,\ nx=0_A$.
  On a alors : $\forall(p,q)\in\mathbb{Z}^2,\ (p+q)\,x=px+qx$ et $p\,(qx)=(pq)\,x$.

↬ **Notation multiplicative** :
- Le produit des n éléments $x_1,...,x_n$ est noté $\prod_{1\leqslant p\leqslant n} x_p$ ou $\prod_{p=1}^{n} x_p$.
- n^{ieme} itéré multiplicatif. Soit $x\in A$ et $n\in\mathbb{N}$, on note x^n l'élément de A défini par $\prod_{1\leqslant p\leqslant n} x$ (produit de n facteurs tous égaux à x) ; et pour $n\in\mathbb{Z}_-$, lorsque x admet un symétrique x^{-1} pour $\times$ dans A, on note x^n aussi pour $\prod_{1\leqslant p\leqslant -n}\left(x^{-1}\right)$ (produit de $-n$ facteurs tous égaux à x^{-1}). Si $n=0$, $x^0=1_A$. En particulier $0^0=1_A$.
  On a alors : $\forall(p,q)\in\mathbb{Z}^2,\ x^{p+q}=x^p\times x^q$ et $x^{pq}=(x^p)^q$

Propriété 6.

Soit $(A,+,\times)$ un anneau
- *0_A est un élément absorbant, c'est-à-dire, $\forall x\in A\quad 0_A\times x=x\times 0_A=0_A$*
- *$\forall(x,y)\in A^2\quad (-x)\,y=x\,(-y)=-(xy)$*

Remarque 4. *Si dans un anneau A on a $0_A = 1_A$, alors $A = \{0_A\}$. Dans toute la suite de ce chapitre on considère que A a au moins deux éléments.*

Propriété 7.

$$\forall a \in A, \quad \forall n \in \mathbb{N}^* \quad \forall (x_1, ..., x_n) \in A^n \quad \sum_{i=1}^{n} a x_i = a \left(\sum_{i=1}^{n} x_i \right) \text{ et } \sum_{i=1}^{n} x_i a = \left(\sum_{i=1}^{n} x_i \right) a.$$

Démonstration : par récurrence sur n.

Propriété 8 (Distributivité généralisée).

Soit $(a_i)_{i\in I}$ et $(b_j)_{i\in J}$ deux familles finies d'éléments de l'anneau $(A, +, \times)$

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

Démonstration : par récurrence sur le nombre d'éléments de I. Lorsque I a un élément, pour démontrer H_1 on fait une récurrence sur le nombre d'éléments de J en utilisant la distributivité.

Propriété 9 (Identités remarquables dans un anneau).

Soient a et b deux éléments d'un anneau tels que a et b commutent (ab=ba).

1. *Soit $n \in \mathbb{N}^*$* $a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$
2. *Soit $p \in \mathbb{N}$* $a^{2p+1} + b^{2p+1} = (a+b) \sum_{k=0}^{2p} (-1)^k a^k b^{2p-k}$
3. *Binôme de Newton : Pour tout entier naturel n,* $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$, *où* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Démonstration : 1. et 2. directement, 3. par récurrence. Retenir le rôle essentiel de la commutativité de a et b.

4.3 Diviseurs de zéro :

Il existe des anneaux contenant des éléments non nuls a et b vérifiant $ab = 0_A$. Par exemple dans $(\mathbb{R}^2, +, \times)$, $(0,1) \times (1,0) = (0,0)$. Soit $(A, +, \times)$ un anneau **commutatif**. On note $A^* = A \setminus \{0_A\}$.

Définition 15.

- *On dit que $a \in A^*$ est un diviseur de zéro lorsque $\exists x \in A^*$ $ax = 0_A$.*
- *L'anneau $(A, +, \times)$ est appelé intègre lorsqu'il est commutatif, distinct de $\{0_A\}$ et sans diviseur de zéro.*

▶ Exemple : $(\mathbb{Z}, +, \times)$ est un anneau intègre mais $\left(\mathbb{R}^2, +, \times\right)$ et $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ ne sont pas intègres.

Propriété 10.

Dans un anneau intègre A, on a $ab = 0_A \Rightarrow a = 0_A$ ou $b = 0_A$.

4.4 Sous-anneau :

Définition 16.

Soit $(A,+,\times)$ un anneau. Un sous-anneau de A est une partie non vide de A qui, munie de la restriction des lois $+$ et $\times$, est un anneau. On montre que $(B,+,\times)$ est un sous-anneau de $(A,+,\times)$ si
- *$(B,+)$ est un sous-groupe de $(A,+)$,*
- *B est stable par $\times$ ($\forall x,y\in B \quad x\times y\in B$),*
- *$1_A\in B$.*

Propriété 11.

Soit $(A,+,\times)$ un anneau et B une partie de A.
$(B,+,\times)$ est un sous-anneau de $(A,+,\times)$ si et seulement si
- *$\forall (x,y)\in B^2 \quad x-y\in B$*
- *$\forall (x,y)\in B^2 \quad xy\in B$*
- *$1_A\in B$*

Remarque 5. *On en déduit que H est un sous groupe de G si et seulement si H non vide et $\forall x,y\in H \quad x-y\in H$.*

▶ Exemples :
- $(\mathbb{Z},+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$ mais $(\{0\},+,\times)$ n'en est pas un (il ne contient pas 1).
- L'ensemble des suites convergentes d'éléments de $\mathbb{K}$ muni de l'addition et de la multiplication usuelles est un sous-anneau de l'ensemble des suites d'éléments de $\mathbb{K}$.
- L'ensemble des restrictions à l'intervalle I des fonctions polynômiales à valeurs dans $\mathbb{R}$ est un sous-anneau de $(\mathcal{F}(I,\mathbb{R}),+,\times)$.
- L'ensemble des polynômes à coefficients dans $\mathbb{K}$ de degré inférieur ou égal à n (noté $\mathbb{K}_n[X]$) n'est pas un sous-anneau de $K[X]$, ensemble des polynômes à coefficients dans $\mathbb{K}$ (l'ensemble n'est pas stable par $\times$).
- $\mathcal{C}(I)$ est un sous-anneau de $\mathcal{F}(I,\mathbb{R})$ (c'est aussi un sous-espace vectoriel) car une combinaison linéaire et un produit de fonctions continues sur I sont des fonctions continues sur I.

4.5 Groupe des inversibles d'un anneau

Propriété 12 (groupe des inversibles d'un anneau).

Soit $(A,+,\times)$ un anneau. Soit I l'ensemble des éléments inversibles de A. $(I,\times)$ est un groupe.

4.6 Corps

Définition 17.

On dit que $(\mathbb{K},+,\times)$ est un corps si $(\mathbb{K},+,\times)$ est un anneau commutatif non réduit à $\{0\}$ et dont tous les éléments non nuls sont inversibles.

Les corps sont commutatifs.

▶ Exemples :
- $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps mais $(\mathbb{Z},+,\times)$ n'en est pas un.
- Un corps commutatif est un anneau intègre.
- $(\mathcal{F}(X,\mathbb{R}),+,\times)$, où X est un ensemble ayant au moins deux éléments, est un anneau qui n'est pas un corps car il n'est pas intègre.

Notation : Soit $\mathbb{K}$ un corps commutatif. Lorsque $(a,b)\in\mathbb{K}^2$ et $b\neq 0$, on note $\dfrac{a}{b}$ pour ab^{-1}.

⇝ **Règles de calculs dans un corps**

Ce sont celles que l'on connaît dans $\mathbb{Q}$. Pour a, b, a', b' et x cinq éléments d'un corps $\mathbb{K}$ avec $b\neq 0$, $b'\neq 0$ et $x\neq 0$, on a :

1. $\dfrac{a}{b}=\dfrac{a'}{b'}\iff ab'=a'b$
2. $\dfrac{ax}{bx}=\dfrac{a}{b}$

3. $\frac{a}{b}+\frac{a'}{b'}=\frac{ab'+ba'}{bb'}$
4. $\frac{a}{b}\times\frac{a'}{b'}=\frac{aa'}{bb'}$
5. Si $\frac{a}{b}=\frac{a'}{b'}$ alors $\forall(\alpha,\beta)\in\mathbb{K}^2$ tels que $\alpha b+\beta b'\neq 0$, on a $\frac{a}{b}=\frac{\alpha a+\beta a'}{\alpha b+\beta b'}$
6. Si $a\neq 0$, $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$
7. Si $a\neq 1$, $\quad\forall n\in\mathbb{N}\quad\sum_{k=0}^{n}a^k=\frac{1-a^{n+1}}{1-a}$

Définition 18.

Soit $\mathbb{K}$ un corps. On appelle sous-corps de $\mathbb{K}$ un sous-anneau de $\mathbb{K}$ qui est un corps.

▶ Exemples :
— $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont trois sous-corps de $\mathbb{C}$.
— $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$.

5 Morphismes

Le mot morphisme vient du grec ancien $\mu o\rho\varphi\eta$, morphè, qui signifie "forme". Un morphisme est une application entre deux ensembles munis d'un même type de structure algébrique, qui respecte cette structure. Le mot se décline en iso-, endo- et auto-morphisme ($\iota\sigma o\varsigma$, isos, "égal" ; $\epsilon\nu\delta o\nu$, endon, "dedans" (idée d'intérieur) ; $\alpha\upsilon\tau o\varsigma$, autos, "soi-même").

Définition 19 (Morphisme).

Soient $(E,*)$ et $(F,\perp)$ deux magmas. Soit φ une application de E dans F.
*φ est un **morphisme ou homomorphisme** de $(E,*)$ dans $(F,\perp)$ ssi $\forall(x,y)\in E^2$, $\varphi(x*y)=\varphi(x)\perp\varphi(y)$.*
*Si $(E,*)=(F,\perp)$, on dit que φ est un **endomorphisme**.*
*Si φ est un morphisme bijectif de $(E,*)$ dans $(F,\perp)$, on dit que φ est un **isomorphisme**.*
*Si φ est un endomorphisme bijectif, on dit que c'est un **automorphisme**.*

▶ Exemple : : exp est un morphisme de $(\mathbb{R},+)$ vers $(\mathbb{R},\times)$.
▶ Exemple : : ln est un isomorphisme de $(\mathbb{R}^{+*},\times)$ vers $(\mathbb{R},+)$.
▶ Exemple : : L'application conjugaison est un automorphisme de $(\mathbb{C},+)$.
▶ Exemple : : L'application conjugaison est un automorphisme de $(\mathbb{C},\times)$.

5.1 Morphisme de groupes

Définition 20.

Soient $(G,*)$ et (G',∇) deux groupes. On appelle morphisme de groupes de $(G,*)$ dans (G',∇) une application de $(G,*)$ dans (G',∇) qui est un morphisme.
On étend à ce cas la terminologie d'isomorphisme, d'endomorphisme et d'automorphisme vue précédemment (définition 19).

▶ Exemples :
— La fonction logarithme est un isomorphisme de groupes de $\left(\mathbb{R}_+^*,\times\right)$ sur $(\mathbb{R},+)$.
— $(r,\theta)\longmapsto re^{i\theta}$ est un morphisme du groupe produit $\left(\mathbb{R}_+^*\times\mathbb{R},\otimes\right)$ dans $(\mathbb{C}^*,\times)$ avec $(r,\theta)\otimes(r',\theta')=(rr',\theta+\theta')$.

Propriété 13.

Soit f un morphisme de groupes de $(G,*)$ sur (G',∇). Si e est l'élément neutre de $(G,*)$ et e' l'élément neutre de (G',∇), on a :
- *$f(e)=e'$ (un morphisme de groupes transporte l'élément neutre).*
- *$\forall x\in G,\quad f\left(x^{-1}\right)=(f(x))^{-1}$ (un morphisme de groupes transporte la notion de symétrique).*
- *$\forall x\in G,\ \forall n\in\mathbb{Z},\quad (f(x))^n=f(x^n)$. L'itéré n-ième de l'image est l'image de l'itéré n-ième.*

▶ Exemple : appliquer cette propriété à la fonction ln.

Définition 21 (Groupes isomorphes).

Lorsqu'il existe un isomorphisme d'un groupe $(G,*)$ sur un groupe (G',∇), on dit que $(G,*)$ et (G',∇) sont isomorphes.

Propriété 14 (Transfert de la structure de groupe).

L'image d'un sous-groupe par un morphisme est un sous-groupe. Plus précisément, si f un morphisme de groupes de $(G,*)$ sur (G',∇) et si $(H,*)$ est un sous-groupe de $(G,*)$ alors $(f(H),\nabla)$ est un sous-groupe de (G',∇).
L'image réciproque d'un sous-groupe par un morphisme aussi. Plus précisément, si f un morphisme de groupes de $(G,*)$ sur (G',∇) et si (H',∇) est un sous-groupe de (G',∇) alors $\left(f^{-1}(H),*\right)$ est un sous-groupe de $(G,*)$.

5.2 Image et noyau d'un morphisme de groupes

5.2.1 Image

Définition 22 (Image de f).

Soient $(G,*)$ et (G',∇) deux groupes et soit $f:(G,*)\to(G',\nabla)$ un morphisme de groupes.
On appelle image de f et on note $\mathrm{Im}f$ l'image directe de G par f :

$$\mathrm{Im}f=f(G)=\{y\in G'\ ;\ \exists x\in G\mid y=f(x)\}\subset G'$$

.

Propriété 15.

- *$\mathrm{Im}f$ est un sous-groupe de (G',∇).*
- *$\mathrm{Im}f=G'$ si et seulement si f est surjective.*

★ Exercice : Soit $f:(\mathbb{R},+)\to(\mathbb{C}^*,\times),\quad \theta\longmapsto e^{i\theta}$. Quelle est l'image de ce morphisme ?

5.2.2 Noyau

Définition 23.

Soit $f:(G,*)\to(G',\nabla)$ un morphisme de groupes. On appelle noyau de f l'image réciproque de $\{e'\}$ par f :

$$\ker f=f^{-1}(\{e'\})=\{x\in G\ ;\ f(x)=e'\}\subset G.$$

Propriété 16.

- *$\ker f$ est un sous-groupe de $(G,*)$.*
- *$\ker f=\{e\}\iff f$ est injectif.*

★ Exercice : Soit $f:(\mathbb{R},+)\to(\mathbb{C}^*,\times),\quad \theta\longmapsto e^{i\theta}$. Quel est le noyau de ce morphisme ?
★ Exercice : Montrer que $(T(E),\circ)$, où $T(E)$ est l'ensemble des translations sur E, et $(E,+)$ sont isomorphes.

5.3 Morphisme d'anneaux

Définition 24.

Soient $(A,+,.)$ et $(B,\oplus,\odot)$ deux anneaux et $f : A \to B$ une application. On dit que f est un morphisme d'anneau lorsque :

- $\forall (x,y) \in A^2\ f(x+y) = f(x) \oplus f(y)$
- $\forall (x,y) \in A^2\ f(x.y) = f(x) \odot f(y)$
- $f(1_A) = 1_B$

Remarque 6.

- *On est obligé de rajouter le dernier point puisque $f(1_A) = (f(1_A))^2$ n'entraîne pas $f(1_A) = 1_B$.*
- *Les morphismes d'anneaux sont en particulier des morphismes de groupes. Ils en ont les mêmes propriétés et on utilise la même terminologie (vocabulaire de la définition ??).*

★ Exercice Montrer que l'identité est l'unique endomorphisme d'anneau de $\mathbb{Z}$ sur lui-même.
★ Exercice L'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe 0 est-elle un morphisme d'anneaux ?

Propriété 17.

L'image d'un sous-anneau de A par un morphisme d'anneau de A dans B est un sous-anneau de B.