Chapitre B6
Structures algébriques

I. Lois de composition internes

A. Définition, propriétés

Définition. Soit E un ensemble. Une loi de composition interne de E est une application de $E \times E$ dans E :

Pour tous x et y dans E on note $x * y$ au lieu de $*(x, y)$.

Exemple 1.

(i) L'addition, la soustraction, la multiplication sont des lois de composition internes de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et de $\mathbb{C}$.

(ii) La soustraction n'est pas une loi de composition interne de $\mathbb{N}$.

(iii) La division n'est pas une loi de composition interne de $\mathbb{Z}$, ni de $\mathbb{R}$, mais de $\mathbb{R}^*$.

(iv) Pour tout ensemble E, l'intersection et l'union sont des lois de composition internes de $\mathcal{P}(E)$.

(v) Le PGCD et le PPCM sont des lois de composition internes de $\mathbb{Z}$ et de $\mathbb{N}$.

(vi) Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, n et p deux entiers strictement positifs.
L'addition des matrices est une loi de composition interne de $\mathcal{M}_{np}(\mathbb{K})$.
La multiplication des matrices est une loi de composition interne de $\mathcal{M}_n(\mathbb{K})$.

(vii) Soit X un ensemble. La loi $\circ$ est une loi de composition interne de l'ensemble $\mathcal{F}(X, X)$ des fonctions de X dans X.

Définitions. Soit $*$ une loi de composition interne. On dit que la loi $*$ est :

- commutative si :
- associative si :

Remarque. Si $x * y = y * x$ on dit que x et y commutent, ou que x commute avec y.

Exemple 1 (suite). Parmi toutes les lois de composition internes données en exemple ci-dessus, déterminer celles qui sont commutatives et celles qui sont associatives.

Définition. Soit ∇ et Δ deux lois de composition internes d'un ensemble E. On dit que ∇ est distributive par rapport à Δ si :

Exemples.

- La multiplication est distributive par rapport à l'addition.
- L'intersection est distributive par rapport à l'union.
- L'union est distributive par rapport à l'intersection.

B. Inverse et itérés

Définition. Soit $*$ une loi de composition interne d'un ensemble E. Un élément neutre de $*$ est un élément e de E tel que :

Exemples.

- La loi $+$ de $\mathbb{Z}$ admet un élément neutre noté 0.
- La loi $\times$ de $\mathbb{R}$ admet un élément neutre noté 1.
- Les lois $-$ et $/$ n'admettent pas d'élément neutre.
- Les lois $\cap$ et $\cup$ de $\mathcal{P}(E)$ admettent pour éléments neutres :

- La matrice nulle 0_{np} est élément neutre pour l'addition de $\mathcal{M}_{np}(\mathbb{K})$.
  La matrice identité I_n est élément neutre pour la multiplication de $\mathcal{M}_n(\mathbb{K})$.
- La loi $\circ$ de $\mathcal{F}(X)$ admet pour élément neutre Id_X.

Proposition. *Si la loi $*$ admet un élément neutre alors celui-ci est unique.*

Démonstration. Supposons qu'il existe deux éléments neutres e et e'.

Définition. Soit E un ensemble muni d'une loi de composition interne $*$ associative admettant un élément neutre.
Un élément x de E est dit inversible si :

Cet élément y est alors unique, il est appelé inverse de x et noté x^{-1}.

▷ **Exercice 1.**

Remarque. Si la loi $*$ est commutative, il suffit de vérifier $x * y = e$. De même pour l'élément neutre il suffit de vérifier que $x * e = x$ pour tout $x \in E$.

Exemples.

- Un élément de $\mathbb{R}$ admet un inverse pour la loi $\times$ si et seulement s'il est non-nul, on le note bien x^{-1}, et on l'appelle inverse sans préciser la loi.
- Les seuls éléments de $\mathbb{Z}$ qui admettent un inverse pour la loi $\times$ sont 1 et -1.
- Tout élément de $\mathbb{Z}$ et de $\mathbb{R}$ admet un inverse pour la loi $+$, mais on le note $-x$ et on l'appelle opposé de x.
- De même pour les matrices, la matrice $-M$, opposée de M, est l'inverse de M pour l'addition des matrices.
  L'inverse d'une matrice inversible A est la matrice inverse A^{-1}.
- Soit X un ensemble et f un élément de $\mathcal{F}(X)$, c'est-à-dire une application de X dans X. Alors f admet un inverse pour la loi $\circ$ si et seulement si il existe $g : X \to X$ telle que $f \circ g = \mathrm{Id}_X$ et $g \circ f = \mathrm{Id}_X$.
  Ainsi une application de X dans X est inversible si et seulement si elle est bijective, son inverse est alors sa réciproque, elle est bien notée f^{-1}.

▷ **Exercice 2.**

Proposition. *Soit E un ensemble muni d'une loi de composition interne $*$ associative, et d'un élément neutre e.*
Si x et y sont inversibles alors $x * y$ est inversible et son inverse est $(x * y)^{-1} = y^{-1} * x^{-1}$.

Démonstration. L'associativité de la loi $*$ permet d'écrire :

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = e$$
$$\text{et} \qquad (y^{-1} * x^{-1}) * (x * y) = y^{-1} * (x^{-1} * x) * y = y^{-1} * e * y = e$$

Par définition $x * y$ est inversible d'inverse $y^{-1} * x^{-1}$. □

Définition. Soit $*$ une loi de composition interne associative sur un ensemble E.
Pour tout x de E les puissances ou itérés de x sont définies par récurrence par $x^1 = x$ puis pour tout $n \in \mathbb{N}^* : \quad x^{n+1} = x * x^n$.
Si E possède un élément neutre e pour $*$ alors on pose $x^0 = e$.
Si de plus x admet un inverse alors on note x^{-n} l'inverse de x^n pour tout $n \in \mathbb{N}$.

Proposition. *On garde les hypothèses de la définition ci-dessus. Alors pour tout $x \in E$:*

$$\forall (m, n) \in (\mathbb{N}^*)^2 \qquad x^{m+n} = x^m * x^n \qquad \textit{et} \qquad (x^m)^n = x^{mn}$$

Si E admet un élément neutre ces formules sont valables pour tout $(m, n) \in \mathbb{N}^2$, si x est inversible elles sont valables pour tout $(m, n) \in \mathbb{Z}^2$.

Démonstration. La première formule se démontre par récurrence sur n en fixant m. La seconde s'en déduit.

Les extensions aux entiers relatifs s'en déduisent également en passant à l'inverse. □

Notation. Pour la loi $+$ on note nx au lieu de x^n. La propriété ci-dessus donne alors :

$$(m + n)x = mx + nx \qquad \text{et} \qquad m(nx) = (mn)x$$

C. Stabilité

Définition. Soit E un ensemble muni d'une loi de composition interne $*$. Une partie F de E est dite stable par $*$ si :

Exemples.

- $\mathbb{Z}$ est une partie de $\mathbb{R}$ stable par $+$ et $\times$.
- $\{\pm 1\}$ est une partie de $\mathbb{Z}$ stable par $\times$ mais pas par $+$.
  Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z}$ est une partie de $\mathbb{Z}$ stable par $+$ et par $\times$.
- $\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ et par $\times$.
  $i\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ mais pas par $\times$.
  $\mathbb{U}$ est une partie de $\mathbb{C}$ non stable par $+$ mais stable par $\times$.
- Si $A \subseteq E$ alors $\mathcal{P}(A)$ est une partie de $\mathcal{P}(E)$ stable par $\cap$ et $\cup$.
- $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$ sont des parties de $\mathcal{M}_n(\mathbb{K})$ stables par addition et produit.
  $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont stables par addition mais pas par produit.
- L'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ est une partie de $\mathcal{F}(\mathbb{R})$ stable par $\circ$.

Définition. Soit E un ensemble muni d'une loi de composition interne $*$. Soit A une partie de E stable par $*$. Alors la restriction de $*$ à $A \times A$ est une loi de composition interne de A.

On dit qu'elle est induite par la loi $*$ de E.

Remarque. Si $*$ est associative ou commutative alors la loi induite $*$ l'est également.

D. Morphismes

Définition. Soit E et E' deux ensembles, $*$ une loi de composition interne de E et $*'$ une loi de composition interne de E'.

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lois de composition internes, *i.e.,* telle que :

Définitions.

(i) Un morphisme est aussi appelé homomorphisme.

(ii) Un morphisme de $(E, *)$ dans lui-même est appelé endomorphisme.

(iii) Un morphisme bijectif est appelé isomorphisme.

(iv) Un endomorphisme bijectif est appelé automorphisme.

Exemple 2.

(i) L'application $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & e^x \end{array}$ est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}, \times)$.

(ii) L'application $\begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln x \end{array}$ est un morphisme de $\left(\mathbb{R}_+^*, \times\right)$ dans $(\mathbb{R}, +)$.

C'est un isomorphisme.

(iii) Soit $a \in \mathbb{R}$. Alors l'application $f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & ax \end{array}$ est un morphisme de $(\mathbb{R}, +)$ dans lui-même, donc un endomorphisme de $(\mathbb{R}, +)$.

C'est un isomorphisme si et seulement si a est non-nul.

(iv) Soit $n \in \mathbb{Z}$. L'application $f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ x & \longmapsto & nx \end{array}$ est un endomorphisme de $(\mathbb{Z}, +)$.

C'est un automorphisme si et seulement si $n = \pm 1$.

(v) Soit $x \in \mathbb{R}$. L'application $f : \begin{array}{ccc} \mathbb{N} & \longrightarrow & \mathbb{R} \\ n & \longmapsto & x^n \end{array}$ est un morphisme de $(\mathbb{N}, +)$ dans $(\mathbb{R}, \times)$.

(vi) L'application Id_E est un automorphisme de $(E, *)$.

Proposition. *La composée de deux morphismes est un morphisme.*

Démonstration.

Proposition. *La réciproque d'un isomorphisme est un isomorphisme.*

Démonstration. Soit $f : (E, *) \to (E', *')$ un isomorphisme. Alors $f : E \to E'$ est bijective, donc elle admet une réciproque f^{-1}, qui est elle aussi bijective.

Montrons que f^{-1} est un morphisme.

Soit (x', y') deux éléments de E'. Soit $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Alors $x' = f(x)$ et $y' = f(y)$ donc :

car f est un morphisme et $f^{-1} \circ f = \mathrm{Id}_E$.

Ceci montre que f^{-1} est un morphisme, donc c'est un isomorphisme. □

II. Groupes

A. Définition et exemples

Définition. Un groupe $(G, *)$ est un ensemble G muni d'une loi $*$ vérifiant les propriétés :

(i) La loi $*$ est une loi de composition interne de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un inverse.

Un groupe commutatif ou groupe abélien est un groupe $(G, *)$ tel que :

(v) La loi $*$ est commutative.

Exemples.

(i) $(\mathbb{Z}, +)$ est un groupe abélien. Son élément neutre est 0.

(ii) $(\mathbb{N}, +)$ n'est pas un groupe, car tout élément n'admet pas d'inverse.

(iii) $(\mathbb{Z}, -)$ n'est pas un groupe car sa loi de composition interne n'est pas associative.

(iv) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes abéliens.

(v) $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes abéliens. Leur élément neutre est 1.

(vi) $(\mathbb{Z}^*, \times)$ n'est pas un groupe, car par exemple 2 n'a pas d'inverse dans $\mathbb{Z}$.

(vii) Soit $G = \{\pm 1\}$. Alors $(G, \times)$ est un groupe.

(viii) $(\mathbb{R}^2, +)$ est un groupe abélien, avec la loi + définie par :

$$\forall ((x, x'), (y, y')) \in (\mathbb{R}^2)^2 \qquad (x, x') + (y, y') = (x + y, x' + y').$$

L'élément neutre est $(0, 0)$, l'inverse d'un élément (x, y) est $-(x, y) = (-x, -y)$.

(ix) $(\mathcal{M}_{np}(\mathbb{K}), +)$ est un groupe abélien.

$(\mathcal{M}_n(\mathbb{K}), \times)$ n'est pas un groupe car tous les éléments ne sont pas inversibles.

(x) Soit X un ensemble. On note S_X ou $\mathcal{B}(X)$ l'ensemble des applications bijectives de X dans X. Alors $(S_X, \circ)$ est un groupe. L'élément neutre est Id_X.

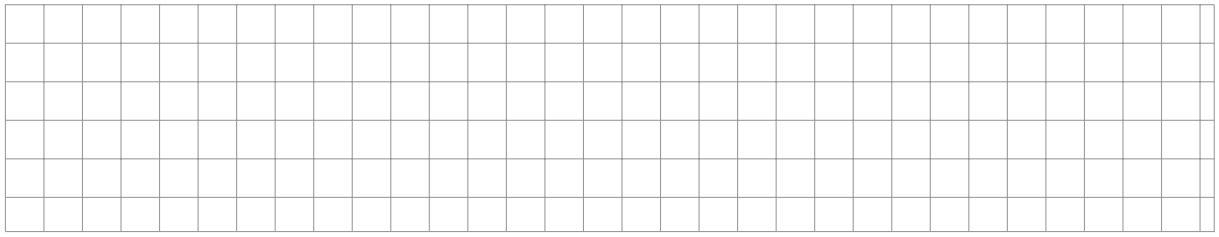
Il n'est pas commutatif dès que X contient au moins trois éléments.

Exemple 3. Description de $(S_X, \circ)$ si $X = \{1, 2\}$.

Proposition. *Dans un groupe tout élément est régulier,* i.e., *simplifiable à gauche et à droite :*

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

Démonstration. En effet, tout élément x de G admet un inverse x^{-1}, et la multiplication est associative, donc :



Remarques.

(i) Si la loi de G est la loi $+$ alors on dit que G est un groupe additif. Par convention les groupes additifs sont toujours commutatifs, leur élément neutre est noté 0_G, l'inverse est appelé opposé et noté $-x$, les itérés sont notés nx avec $n \in \mathbb{Z}$.

(ii) Si la loi de G est la loi $\times$ alors on dit que G est un groupe multiplicatif.
Par exemple $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{R}_+^*$ et $\mathbb{U}$ sont des groupes multiplicatifs.

Notation. Soit G un groupe additif. Pour tous x et y dans G on note $x - y = x + (-y)$.

B. Sous-groupes

Définition. Soit $(G, *)$ un groupe. Un ensemble H est un sous-groupe de G si :

(i) H est inclus dans G.

(ii) H est non-vide.

(iii) H est stable par $*$: $\forall (x, y) \in H^2 \quad x * y \in H$

(iv) H est stable par passage à l'inverse : $\forall x \in H \quad x^{-1} \in H$

Exemples.

(i) Si $(G, *)$ est un groupe, alors $\{e\}$ et G sont des sous-groupes de $(G, *)$.

(ii) $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$, qui est un sous-groupe de $(\mathbb{C}, +)$.

(iii) $(\{\pm 1\}, \times)$ est un sous-groupe de $(\mathbb{Q}^*, \times)$, qui est un sous-groupe de $(\mathbb{R}^*, \times)$, qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

(iv) $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$, mais $\mathbb{R}_-^*$ n'en est pas un.

(v) L'ensemble $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$.

(vi) $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}_n'(\mathbb{K})$, $\mathcal{S}_n(\mathbb{K})$, $\mathcal{A}_n(\mathbb{K})$ sont des sous-groupes de $(\mathcal{M}_n(\mathbb{K}), +)$.

Proposition. *Si H est un sous-groupe de $(G, *)$ alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.*

Démonstration. On vérifie les quatre points de la définition d'un groupe.

(i) La loi induite est une loi de composition interne de H car H stable par $*$.

(ii) Elle est associative car la loi $*$ de G l'est.

(iii) Démontrons que H contient l'élément neutre e de G.
D'après le point *(ii)* H est non-vide donc elle contient au moins un élément x.
D'après le point *(iv)* H est stable par inversion donc x^{-1} appartient aussi à H.
D'après le point *(iii)* H stable par la loi $*$ donc elle contient aussi $x * x^{-1} = e$, et donc elle contient l'élément neutre de G, qui est aussi un élément neutre pour la loi $*$ induite.

(iv) D'après le point *(iv)* tout élément de H admet un inverse, c'est son inverse dans G.

Ces quatre propriétés montrent que le couple $(H, *)$ est un groupe. □

Remarque. Dans la pratique, pour vérifier qu'un couple $(G, *)$ est un groupe, il est souvent plus rapide de démontrer que c'est un sous-groupe d'un groupe plus gros $(G', *)$.
De plus, pour démontrer qu'il est non-vide il est en général simple de montrer qu'il contient l'élément neutre.

▷ **Exercices 3, 4.**

C. Morphismes de groupes

Dans toute cette partie on note $(G, *)$ et $(G', *')$ deux groupes, et e, e' leurs éléments neutres respectifs.

Définition. Un morphisme de groupes est une application $f : G \to G'$ telle que :

Remarque. On conserve également les définitions d'isomorphisme, endomorphisme, automorphisme de groupes.

Exemple 4.

(i) L'application $\begin{array}{ccc} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln x \end{array}$ est un isomorphisme de groupes de $\left(\mathbb{R}_+^*, \times\right)$ dans $(\mathbb{R}, +)$.

(ii) L'application $\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ \theta & \longmapsto & e^{i\theta} \end{array}$ est un morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.

Proposition. *Soit $f : (G, *) \to (G, *')$ un morphisme de groupes. Alors :*

(i) $f(e) = e'$.

(ii) Pour tout $x \in G$: $f(x^{-1}) = f(x)^{-1}$

(iii) Pour tout $x \in G$ et tout $n \in \mathbb{Z}$: $f(x^n) = (f(x))^n$

Démonstration.

(iii) On démontre la propriété pour tout $n \in \mathbb{N}^*$ par récurrence, puis pour $n = 0$ grâce au *(i)*, et pour tout $n \in \mathbb{Z}_-$ grâce au *(ii)*, car x^{-n} est l'inverse de x^n. □

Exemple 4 (suite). Dans le cas du logarithme, les propriétés *(i)* et *(ii)* s'écrivent :

$$\ln 1 = 0 \qquad \text{et} \qquad \forall x \in \mathbb{R}_+^* \quad \ln\left(\tfrac{1}{x}\right) = -\ln x$$

▷ **Exercice 5.**

D. Noyau et image

Proposition. *Soit $f : G \to G'$ un morphisme de groupes.*

- *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.*

Démonstration. Soit H un sous-groupe de G. On vérifie les quatre points de définition d'un sous groupe.

(i) $f(H)$ est inclus dans G', car $H \subseteq G$ et f va de G dans G'.

(ii) Comme H est un sous-groupe de G alors il contient e, donc $f(H)$ contient $f(e) = e'$, *i.e.,* $e' \in f(H)$.

(iii) Soit x' et y' deux éléments de $f(H)$. Alors il existe x et y dans H tels que $x' = f(x)$ et $y' = f(y)$.
Comme H est un sous-groupe de G alors il est stable par $*$ donc $x * y \in H$.
Or $f(x) *' f(y) = f(x * y)$ donc $f(x) *' f(y) \in f(H)$, puis $x' *' y' \in f(H)$.
Ceci montre que $f(H)$ est stable par $*$.

(iv) Soit x' un élément de $f(H)$. Alors il existe $x \in H$ tel que $x' = f(x)$.
Comme H est un sous-groupe de G alors il est stable par passage à l'inverse, donc $x^{-1} \in H$. Ainsi $f(x^{-1}) \in f(H)$. Or $f(x^{-1}) = f(x)^{-1}$, donc $(x')^{-1} \in f(H)$.
Ceci montre que $f(H)$ est stable par passage à l'inverse.

Les quatre points ci-dessus montrent que $f(H)$ est un sous-groupe de G'.

Soit maintenant H' un sous-groupe de G'.

(i) Comme $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ alors $f^{-1}(H') \subseteq G$.

(ii) Comme H' est un sous-groupe de G' alors il contient son élément neutre e'.
Comme $f(e) = e'$ alors $e \in f^{-1}(H')$.

(iii) Soit x et y deux éléments de $f^{-1}(H')$. Alors $f(x)$ et $f(y)$ appartiennent à H'.
Comme H' est un sous-groupe de G' alors il est stable par $*'$ donc $f(x) *' f(y) \in H'$.
Comme f est un morphisme de groupes alors $f(x)*'f(y) = f(x*y)$, donc $f(x*y) \in H'$, ce qui montre que $x * y \in f^{-1}(H')$.
Ainsi $f^{-1}(H')$ est stable par $*$.

(iv) Soit x un élément de $f^{-1}(H')$. Alors $f(x) \in H'$.
Comme H' est un sous-groupe de G' alors il est stable par passage à l'inverse, donc $f(x)^{-1} \in H'$. Or $f(x)^{-1} = f(x^{-1})$ donc $f(x^{-1}) \in H'$, ce qui montre que $x^{-1} \in f^{-1}(H')$, et donc $f^{-1}(H')$ est stable par passage à l'inverse.

Les quatre points ci-dessus montrent que $f^{-1}(H')$ est un sous-groupe de G. □

Exemples. On sait que $\{e\}$ est un sous-groupe de G et G' est un sous-groupe de G'. Or :

$f(\{e\}) =$ $\qquad\qquad$ $f^{-1}(G') =$

Ce sont bien des sous-groupes respectivement de G' et de G.

Définitions. Soit $f : G \to G'$ un morphisme de groupes.

On appelle image de f et on note $\operatorname{im} f$ l'ensemble :

On appelle noyau de f et on note $\ker f$ l'ensemble :

Proposition. *L'image de f est un sous-groupe de G', le noyau de f est un sous-groupe de G.*

Remarque. Caractérisation des éléments de l'image et du noyau.

Exemple 4 (suite). Déterminer le noyau et l'image de $f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}^*, \times)$, $\theta \longmapsto e^{i\theta}$

Théorème. *Soit $f : G \to G'$ un morphisme de groupes. Alors :*

(i) f est injective si et seulement si $\ker f = \{e\}$.

(ii) f est surjective si et seulement si $\operatorname{im} f = G'$.

Démonstration.

▷ **Exercice 5 (suite).**

III. Anneaux et corps

A. Anneaux

Définition. Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de composition internes $+$ et $\times$ telles que :

(i) $(A, +)$ est un groupe abélien.

(ii) La loi $\times$ est associative.

(iii) A possède un élément neutre pour $\times$.

(iv) La loi $\times$ est distributive par rapport à la loi $+$.

Un anneau commutatif est un anneau dans lequel :

(v) La loi $\times$ est commutative.

Remarques.

(i) On omet souvent de noter le signe $\times$: $xy = x \times y$.

(ii) On note 0 ou 0_A l'élément neutre pour la loi $+$ de A. On l'appelle élément nul de A.

(iii) On note 1 ou 1_A l'élément neutre pour la loi $\times$ de A. On l'appelle unité de A.

(iv) On appelle inverse d'un élément x de A l'inverse de x pour la loi $\times$. L'inverse d'un élément d'un anneau n'existe pas toujours.

Exemples.

(i) $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux. Tous sont commutatifs. On remarque que l'entier 2 n'a pas d'inverse dans $\mathbb{Z}$.

(ii) $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, muni des lois :

$$\forall ((x,y),(x',y')) \in (\mathbb{R}^2)^2 \qquad \begin{array}{rcl} (x,y)+(x',y') & = & (x+x', y+y') \\ (x,y)\times(x',y') & = & (xx', yy') \end{array}$$

On vérifie que tous les axiomes sont satisfaits.

Les éléments neutres sont $(0,0)$ et $(1,1)$.

L'opposé de (x,y) est $-(x,y) = (-x,-y)$.

Le couple (x,y) est inversible si et seulement si x et y sont non-nuls, son inverse est alors $(x,y)^{-1} = (x^{-1}, y^{-1})$.

Démontrons par exemple la distributivité. Soit $u = (x,y)$, $v = (x',y')$ et $w = (x'',y'')$ trois éléments de $\mathbb{R}^2$. Alors :

$$\begin{aligned} (u+v)\times w &= [(x,y)+(x',y')]\times(x'',y'') \\ &= (x+x', y+y')\times(x'',y'') \\ &= ((x+x')x'', (y+y')y'') \\ &= (xx''+x'x'', yy''+y'y'') \\ &= (xx'', yy'') + (x'x'', y'y'') \\ &= (x,y)\times(x'',y'') + (x',y')\times(x'',y'') = u\times w + v\times w \end{aligned}$$

Comme la loi $\times$ est commutative, la distributivité dans l'autre sens est aussi vérifiée.

(iii) Soit X un ensemble quelconque et $A = \mathcal{F}(X, \mathbb{R})$. On munit A des lois $+$ et $\times$ suivantes : Si f et g sont deux éléments de A, alors $f + g$ et $f \times g$ sont les fonctions définies par :

$$\forall x \in X \qquad (f+g)(x) = f(x) + g(x) \qquad \text{et} \qquad (f \times g)(x) = f(x)g(x)$$

Alors $(A, +, \times)$ est un anneau, il est commutatif.

L'élément nul est la fonction nulle, *i.e.,* la fonction constante égale à 0, et l'unité est la fonction constante égale à 1.

(iv) L'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites indexées par $\mathbb{N}$ muni de l'addition et de la multiplication usuelles est un anneau.

L'élément nul est la suite nulle, l'unité est la suite constante égale à 1.

(v) L'ensemble $\mathcal{M}_n(\mathbb{K})$ muni de l'addition et de la multiplication matricielles est un anneau. Il n'est pas commutatif.

L'élément nul est la matrice nulle 0_n, l'unité est la matrice identité I_n.

(vi) L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif.

▷ **Exercice 6.**

B. Propriétés

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

Proposition. *Pour tout $x \in A$:* $0_A \times x = 0_A = x \times 0_A$ *(0_A est dit élément absorbant).*

Démonstration.

Remarque. On peut avoir dans un anneau $xy = 0_A$ alors que ni x ni y n'est nul.
En d'autres termes l'implication

$$(x = 0_A \quad \text{ou} \quad y = 0_A) \quad \Longrightarrow \quad xy = 0_A$$

n'est pas une équivalence.

Définition. Un anneau A est dit intègre s'il est commutatif et :

Exemples.

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intègres.

(ii) $(\mathbb{R}^2, +, \times)$ n'est pas intègre. En effet $(1,0)$ et $(0,1)$ ne sont pas nuls, alors que leur produit est nul.

(iii) L'anneau $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ des suites réelles n'est pas intègre.

(iv) $(\mathcal{M}_n(\mathbb{K}), +, \times)$ n'est pas intègre car non seulement il n'est pas commutatif, mais en plus il existe des matrices non-nulles dont le produit est nul.

▷ **Exercice 7.**

Propositions.

*(i) (Formule du binôme de Newton) Soit a et b deux éléments de A tels que $ab = ba$ (*i.e., *a et b commutent). Alors pour tout $n \in \mathbb{N}$:*

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

(ii) Soit a et b deux éléments de A tels que $ab = ba$. Alors pour tout $n \in \mathbb{N}$:

$$\begin{aligned} a^n - b^n &= (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}) \\ &= (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k \end{aligned}$$

Notation. Soit $(A, +, \times)$ un anneau. On note A^* l'ensemble des éléments inversibles de A, *i.e.,* des éléments inversibles pour la loi $\times$.

Proposition - Définition. *Le couple $(A^*, \times)$ est un groupe.*
Ce groupe est appelé groupe des inversibles de A.

Démonstration. On vérifie les quatre points de la définition d'un groupe.

(i) Le produit de deux éléments inversibles est inversible, donc A^* est stable par la loi $\times$. Ainsi la loi $\times$ de A^* est induite par celle de A. C'est donc une loi de composition interne.

(ii) La loi $\times$ d'un anneau est associative donc la loi $\times$ de A^* est associative.

(iii) L'anneau A contient un élément neutre pour la loi $\times$. Cet élément est inversible (d'inverse lui-même) donc il appartient à A^*. Ainsi A^* possède un élément neutre pour sa loi $\times$.

(iv) Si x appartient à A^* alors x est inversible. Son inverse x^{-1} est inversible d'inverse x, ce qui montre que x^{-1} appartient à A^*.
Ainsi tout élément de A^* possède un inverse dans A^*.

Tout ceci montre que $(A^*, \times)$ est un groupe. □

Exemples.

(i) Le groupe des inversible de l'anneau $(\mathbb{R}, +, \times)$ est $(\mathbb{R}^*, \times)$.
De même pour $\mathbb{C}$ et $\mathbb{Q}$.

(ii) Le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est $(\{\pm 1\}, \times)$.
Il est incorrect de noter $\mathbb{Z}^*$ pour $\mathbb{Z} \setminus \{0\}$.

(iii) Le groupe des inversible de $\mathcal{M}_n(\mathbb{K})$ est $\mathrm{GL}_n(\mathbb{K})$, appelé $n^{\text{ème}}$ groupe linéaire de $\mathbb{K}$.

C. Corps

Définition. Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Remarques.

(i) Un anneau commutatif K non-nul est donc un corps si et seulement si : $K^* = K \setminus \{0\}$

(ii) Si x est un élément non-nul de K alors on note $\frac{1}{x} = x^{-1}$ et $\frac{y}{x} = y \times \frac{1}{x}$.

Exemples.

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(ii) $\mathbb{Z}$ n'est pas un corps, par exemple car 2 n'est pas inversible dans $\mathbb{Z}$.

(iii) L'ensemble des polynômes $\mathbb{R}[X]$ n'est pas un corps.
En effet ses éléments inversibles sont les polynômes non-nuls de degré 0.

Proposition. *Un corps est intègre.*

Démonstration.

D. Sous-anneaux

Définition. Soit A un anneau. Un ensemble B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Propositions.

(i) Si B est un sous-anneau de A alors B est un anneau.

(ii) Si B est une partie de A contenant 1_A, stable par $+$, $\times$, et passage à l'opposé alors B est un sous-anneau de A.

Exemples.

(i) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

(ii) $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$ sont des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$.

(iii) $\{0_A\}$ est un sous-groupe de $(A, +)$, il est stable par $\times$, mais ce n'est pas un sous-anneau de A, car il ne contient par 1_A.

▷ **Exercice 8.**

E. Morphismes d'anneaux

Soit A et A' deux anneaux.

Dans la suite on note de la même façon les additions et les multiplications de A et de A' pour alléger les notations.

Définition. Un morphisme d'anneaux est une application $f : A \to A'$ vérifiant :

Remarques.

(i) On définit également les isomorphismes, endomorphismes et automorphismes d'anneaux.

(ii) Un morphisme d'anneaux $f : A \to A'$ est un morphisme de groupes de $(A, +)$ dans $(A', +)$.

(iii) Le noyau $\ker f = f^{-1}(\{0_{A'}\})$ et l'image $\operatorname{im} f = f(A)$ sont toujours définis.
L'image de f est un sous-anneau de A' mais en général le noyau de f n'est pas un sous-anneau de A. En effet il ne contient pas obligatoirement 1_A.

(iv) On a toujours l'équivalence, pour un morphisme d'anneaux :

$$f \text{ injectif} \iff \ker f = \{0_A\}$$