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.

- L'addition, la soustraction, la multiplication sont des lois de composition internes de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, et de $\mathbb{C}$.
- La soustraction n'est pas une loi de composition interne de $\mathbb{N}$.
- La division n'est pas une loi de composition interne de $\mathbb{Z}$, ni de $\mathbb{R}$, mais de $\mathbb{R}^*$.
- Pour tout ensemble E, l'intersection et l'union sont des lois de composition internes de $\mathscr{P}(E)$.
- Le PGCD ($\wedge$) et le PPCM ($\vee$) sont des lois de composition internes de $\mathbb{Z}$ et de $\mathbb{N}$.
- 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 $\mathscr{M}_{np}(\mathbb{K})$.

  La multiplication des matrices est une loi de composition interne de $\mathscr{M}_n(\mathbb{K})$.
- Soit X un ensemble. La loi $\circ$ est une loi de composition interne de l'ensemble $\mathscr{F}(X, X)$ des fonctions de X dans X.

Définitions

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

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

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

Exemple 1 (suite). Parmi les lois données en exemples,

les lois non commutatives sont :

les lois non associatives sont :

Définition

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

$$\forall (x,y,z) \in E^3 \qquad x \nabla (y \Delta z) = (x \nabla y) \Delta (x \nabla z)$$
$$\text{et} \quad (y \Delta z) \nabla x = (y \nabla x) \Delta (z \nabla x)$$

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. Symétriques et itérés

Définition

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

$$\forall x \in E \qquad x * e = e * x = x$$

Exemples.

- 0 est élément neutre pour la loi $+$ dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- 1 est élément neutre pour la loi $\times$ dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- Les lois $-$ et $/$ n'admettent pas d'élément neutre.
- Les lois $\cap$ et $\cup$ de $\mathscr{P}(E)$ admettent pour éléments neutres :
- La matrice nulle 0_{np} est élément neutre pour l'addition de $\mathscr{M}_{np}(\mathbb{K})$.
  La matrice identité I_n est élément neutre pour la multiplication de $\mathscr{M}_n(\mathbb{K})$.
- Id_X est élément neutre pour la loi $\circ$ de $\mathscr{F}(X)$.

Proposition

Si une loi de composition admet un élément neutre alors celui-ci est unique.

Démonstration. Supposons qu'il existe deux éléments neutres e et e' pour une loi de composition interne $*$.

Définition

Soit E un ensemble muni d'une loi de composition interne $*$ associative admettant un élément neutre.

Un élément x de E est dit *symétrisable* si :

$$\exists y \in E \qquad x * y = y * x = e$$

Cet élément y est alors unique, il est appelé *symétrique* de x.

▷ **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 $\mathbb{R}$ est symétrisable pour la loi $\times$ si et seulement s'il est non-nul. On note x^{-1} son symétrique, et on l'appelle *inverse* de x.
- Les seuls éléments de $\mathbb{Z}$ symétrisables pour la loi $\times$ sont 1 et -1.
- Tout élément de $\mathbb{Z}$ et de $\mathbb{R}$ est symétrisable pour la loi $+$, on note $-x$ son symétrique et on l'appelle *opposé* de x.
- De même pour les matrices, la matrice $-M$, opposée de M, est la symétrique de M pour l'addition des matrices.

  La symétrique d'une matrice inversible A pour la loi $\times$ 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 est symétrisable 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 symétrisable si et seulement si elle est bijective, sa symétrique est alors sa réciproque, elle est notée f^{-1}.

Notation

Le symétrique de x est noté x^{-1}, sauf pour la loi $+$ auquel cas il est noté $-x$.

▷ **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 symétrisables alors $x * y$ est symétrisable.

Son symétrique est $(x * y)^{-1} = y^{-1} * x^{-1}$.

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

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

Par définition $x * y$ est symétrisable de symétrique $y^{-1} * x^{-1}$. □

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 est symétrisable alors on note x^{-n} le symétrique de x^n pour tout $n \in \mathbb{N}$.

Proposition

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

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

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

Démonstration. On démontre ces deux formules par récurrence sur n en fixant m.

Les extensions aux entiers relatifs s'en déduisent en passant au symétrique. □

Notation

Pour la loi $+$ on note nx au lieu de x^n. La propriété ci-dessus s'écrit :

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

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 $\mathscr{P}(A)$ est une partie de $\mathscr{P}(E)$ stable par $\cap$ et $\cup$.
- $\mathscr{D}_n(\mathbb{K})$, $\mathscr{T}_n(\mathbb{K})$, $\mathscr{T}'_n(\mathbb{K})$ sont des parties de $\mathscr{M}_n(\mathbb{K})$ stables par addition et produit.
  $\mathscr{S}_n(\mathbb{K})$ et $\mathscr{A}_n(\mathbb{K})$ sont stables par addition mais pas par produit.
- L'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ est une partie de $\mathscr{F}(\mathbb{R})$ 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.

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x * y \end{aligned}$$

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

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

II. Groupes

A. Définition et exemples

Définition

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

(G_1) La loi $*$ est une loi de composition interne de G.

(G_2) La loi $*$ est associative.

(G_3) G contient un élément neutre pour $*$.

(G_4) Tout élément de G possède un symétrique pour la loi $*$.

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

(G_5) La loi $*$ est commutative.

Exemples.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathscr{M}_{np}(\mathbb{K}), +)$ sont des groupes abéliens.
  Leurs éléments neutres respectifs sont $0_{\mathbb{Z}} = 0_{\mathbb{Q}} = 0_{\mathbb{R}} = 0_{\mathbb{C}}$ et $0_{n,p}$.
- $(\mathbb{N}, +)$ n'est pas un groupe, car tout élément n'admet pas d'opposé.
- $(\mathbb{Z}, -)$ n'est pas un groupe car sa loi de composition interne n'est pas associative.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes abéliens. Leur élément neutre est 1.
- $(\mathbb{Z}^*, \times)$ n'est pas un groupe, car par exemple 2 n'a pas d'inverse dans $\mathbb{Z}$.
- Soit $G = \{\pm 1\}$. Alors $(G, \times)$ est un groupe.
- Soit X un ensemble. On note S_X ou $\mathscr{B}(X)$ 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 2. Description de $(S_X, \circ)$ si $X = \{1, 2\}$.

Définition

Les groupes munis d'une loi d'addition $+$ sont appelés *groupe additifs*.

- Ils sont toujours commutatifs par convention.
- Leur élément neutre est noté 0_G.
- Le symétrique d'un élément x est noté $-x$ et appelé *opposé* de x.
- Les itérés de x sont notés nx avec $n \in \mathbb{Z}$.
- On note aussi $x - y$ au lieu de $x + (-y)$.

Proposition

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

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

<u>Démonstration</u>. En effet, tout élément x de G admet un symétrique x^{-1}, et la loi $*$ est associative, donc :

Remarque. Soit $(G, *)$ un groupe fini.

On peut construire la *table de composition* de $(G, *)$. La proposition ci-dessous montre que tout élément de G apparaît une et une seule fois dans chaque ligne et chaque colonne.

Exemple 3.

(i) Table de composition d'un groupe G à deux éléments, en notant $G = \{e, a\}$.

(ii) Table de composition d'un groupe G à trois éléments, en notant $G = \{e, a, b\}$.

▷ **Exercice 3.**

Proposition - Définitions

Soit $(G, *)$ et $(G', *')$ deux groupes, d'éléments neutres respectifs e et e'.

- La *loi produit* des lois $*$ et $*'$ est la loi définie sur $G \times G'$ par :

$$\forall ((x, x'), (y, y')) \in (G \times G')^2 \qquad (x, x') \cdot (y, y') = (x * y, x' *' y')$$

  Il s'agit d'une loi de composition interne de $G \times G'$.
- De plus $(G \times G', \cdot)$ est un groupe, appelé *groupe produit* de $(G, *)$ et $(G', *')$.
  Son élément neutre est (e, e').
  Le symétrique d'un élément (x, x') est $(x, x')^{-1} = \left(x^{-1}, x'^{-1}\right)$.
- On définit de même le produit de plusieurs groupes.

Démonstration. Les propriétés (G_1) à (G_4) sont toutes vérifiées. □

Exemple. L'ensemble $\mathbb{R}^2$ est un groupe additif avec la loi :

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

L'élément neutre est $0_{\mathbb{R}^2} = (0, 0)$. L'opposé de (x, y) est $-(x, y) = (-x, -y)$.

B. Sous-groupes

Définition

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

(SG_1) H est inclus dans G.

(SG_2) H est non-vide.

(SG_3) H est stable par $*$: $\quad \forall (x, y) \in H^2 \quad x * y \in H$

(SG_4) H est stable par passage au symétrique : $\quad \forall x \in H \quad x^{-1} \in H$

En d'autres termes, un sous-groupe de G est un sous-ensemble de G non-vide, stable par sa loi de composition interne et par passage au symétrique.

Exemples.

- Si $(G, *)$ est un groupe, alors $\{e\}$ et G sont des sous-groupes de $(G, *)$.
- $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$, qui est un sous-groupe de $(\mathbb{R}, +)$, qui est un sous-groupe de $(\mathbb{C}, +)$.
- $(\{\pm 1\}, \times)$ est un sous-groupe de $(\mathbb{Q}^*, \times)$, qui est un sous-groupe de $(\mathbb{R}^*, \times)$, qui est un sous-groupe de $(\mathbb{C}^*, \times)$.
- $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$, mais $\mathbb{R}_-^*$ n'en est pas un.
- L'ensemble $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$.
- $\mathscr{D}_n(\mathbb{K})$, $\mathscr{T}_n(\mathbb{K})$, $\mathscr{T}'_n(\mathbb{K})$, $\mathscr{S}_n(\mathbb{K})$, $\mathscr{A}_n(\mathbb{K})$ sont des sous-groupes de $(\mathscr{M}_n(\mathbb{K}), +)$.

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.

(G_1) La loi induite est une loi de composition interne de H car H stable par $*$.

(G_2) Elle est associative car la loi $*$ de G l'est.

(G_3) Démontrons que H contient l'élément neutre e de G.

D'après le point (SG_2) H est non-vide donc il contient au moins un élément x.

D'après le point (SG_4) H est stable par inversion donc x^{-1} appartient aussi à H.

D'après le point (SG_3) H stable par la loi $*$ donc il contient aussi $x * x^{-1} = e$.

(G_4) D'après le point (SG_4) tout élément de H admet un symétrique dans H, c'est son symétrique dans G.

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

Méthode

- Pour vérifier qu'un couple $(G, *)$ est un groupe, on peut démontrer que c'est un sous-groupe d'un groupe plus gros $(G', *)$.
- Pour démontrer qu'il est non-vide on montre qu'il contient l'élément neutre.

▷ **Exercices 4, 5.**

C. 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

- Un *homomorphisme* est un morphisme.
- Un *endomorphisme* est un morphisme de $(E, *)$ dans lui-même.
- Un *isomorphisme* est un morphisme bijectif.
- Un *automorphisme* est un endomorphisme bijectif.

Exemple 4.

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

Proposition

La composée de deux morphismes est un morphisme.

Démonstration. Soit $f : (E, *) \to (E', *')$ et $g : (E', *') \to (E'', *'')$ deux morphismes.
Alors :

Donc $g \circ f$ est un morphisme. □

Proposition

La réciproque d'un isomorphisme est un isomorphisme.

Démonstration.

Définition

Un *morphisme de groupes* est un morphisme d'un groupe vers un autre, *i.e.*, un morphisme de $(G,*)$ dans $(G',*')$ où $(G,*)$ et $(G',*')$ sont deux groupes.

Exemple 5.

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

Cadre

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

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 5 (suite). Dans le cas du logarithme, ces propriétés s'écrivent :

$$\ln 1 = 0 \qquad \forall x \in \mathbb{R}_+^* \quad \ln\left(\frac{1}{x}\right) = -\ln x \qquad \forall (x,n) \in \mathbb{R}_+^* \times \mathbb{Z} \quad \ln(x^n) = n \ln x$$

▷ **Exercice 6.**

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.

(SG_1) $f(H)$ est inclus dans G', car $H \subseteq G$ et f va de G dans G'.

(SG_2) Comme H est un sous-groupe de G alors il contient e, donc $f(H)$ contient $f(e) = e'$, *i.e.*, $e' \in f(H)$.

(SG_3) 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 $*$.

(SG_4) 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'.

(SG_1) Comme $f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ alors $f^{-1}(H') \subseteq G$.

(SG_2) Comme H' est un sous-groupe de G' alors il contient son élément neutre e'.

Comme $f(e) = e'$ alors $e \in f^{-1}(H')$.

(SG_3) 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 $*$.

(SG_4) 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. $\square$

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 5 (suite). Déterminer le noyau et l'image de $f : \begin{array}{rcl} (\mathbb{R}, +) & \longrightarrow & (\mathbb{C}^*, \times) \\ \theta & \longmapsto & e^{i\theta} \end{array}$

Théorème

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

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

(ii) f est injectif si et seulement si $\ker f = \{e\}$.

Démonstration.

(i) Par définition le morphisme f est surjectif si et seulement si :

$$\forall x' \in G' \qquad \exists x \in G \qquad f(x) = x'.$$

Ceci signifie exactement $G' \subseteq \operatorname{im} f$, donc $\operatorname{im} f = G'$ car l'inclusion réciproque est immédiate.

(ii)

▷ **Exercice 6 (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 :

(A_1) $(A, +)$ est un groupe abélien.

(A_2) La loi $\times$ est associative.

(A_3) A possède un élément neutre pour $\times$.

(A_4) La loi $\times$ est distributive par rapport à la loi $+$.

Un *anneau commutatif* est un anneau dans lequel :

(A_5) La loi $\times$ est commutative.

Remarques.

- On omet souvent de noter le signe $\times$: $xy = x \times y$.
- On note 0_A l'élément neutre pour la loi $+$ de A. On l'appelle *élément nul* de A.
- On note 1_A l'élément neutre pour la loi $\times$ de A. On l'appelle *unité* de A.
- On appelle *inverse* d'un élément x de A l'inverse de x pour la loi $\times$.

  Les éléments d'un anneau admettent tous un opposé mais pas tous un inverse.

Exemples.

- $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux. Tous sont commutatifs.
  On remarque que 2 n'a pas d'inverse dans $\mathbb{Z}$.
- $(\mathbb{R}^2,+,\times)$ 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.
- 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.
- 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.
- 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.
- L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif.

▷ **Exercice 7.**

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. Dans un anneau on peut avoir $xy = 0_A$ 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.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intègres.
- $(\mathbb{R}^2, +, \times)$ n'est pas intègre. En effet $(1, 0)$ et $(0, 1)$ ne sont pas nuls, alors que leur produit est nul.
- L'anneau $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ des suites réelles n'est pas intègre.
- $(\mathcal{M}_n(\mathbb{K}), +, \times)$ 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 8.**

Propositions

- (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 $n \in \mathbb{N}$:

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

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

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \quad = (a-b)\sum_{k=0}^{n-1} a^{n-1-k} b^k$$

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, appelé *groupe des inversibles* de A.

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

(G_1) 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.

(G_2) La loi $\times$ d'un anneau est associative donc la loi $\times$ de A^* est associative.

(G_3) 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 $\times$.

(G_4) 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.

- Le groupe des inversible de l'anneau $(\mathbb{R},+,\times)$ est $(\mathbb{R}^*,\times)$.
  De même pour $\mathbb{C}$ et $\mathbb{Q}$.
- Le groupe des inversibles de $(\mathbb{Z},+,\times)$ est $(\{\pm 1\},\times)$.
  Il est incorrect de noter $\mathbb{Z}^*$ pour $\mathbb{Z}\setminus\{0\}$.
- Le groupe des inversible de $\mathscr{M}_n(\mathbb{K})$ 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.

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

- $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.
- $\mathbb{Z}$ n'est pas un corps, par exemple car 2 n'est pas inversible dans $\mathbb{Z}$.
- 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 :

(SA_1) $(B,+)$ est un sous-groupe de $(A,+)$.

(SA_2) 1_A appartient à B.

(SA_3) B est stable par $\times$.

Propositions

- Si B est un sous-anneau de A alors B est un anneau.
- 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.

- $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.
- $\mathscr{D}_n(\mathbb{K})$, $\mathscr{T}_n(\mathbb{K})$, $\mathscr{T}'_n(\mathbb{K})$ sont des sous-anneaux de $\mathscr{M}_n(\mathbb{K})$.
- $\{0_A\}$ 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 9.**

E. Morphismes d'anneaux

Soit A et A' deux anneaux.

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 :

(MA$_1$) $\forall (a,b) \in A^2 \qquad f(a+b) = f(a) + f(b)$

(MA$_2$) $\forall (a,b) \in A^2 \qquad f(ab) = f(a)f(b)$

(MA$_3$) $f(1_A) = 1_{A'}$

Remarques.

- On définit également les isomorphismes, endomorphismes et automorphismes d'anneaux.
- Un morphisme d'anneaux $f : A \to A'$ est en particulier un morphisme de groupes de $(A,+)$ dans $(A',+)$.
- 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.
- On a toujours l'équivalence, pour un morphisme d'anneaux :

$$f \text{ injectif} \qquad \Longleftrightarrow \qquad \ker f = \{0_A\}$$