Université Constantine 2 Abdelhamid Mehri — Département MI

Chapitre 5 : Structures algébriques

A. Kitouni — module : Algèbre 1

2015–2016

Définition (Loi de composition interne)

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

$$\begin{aligned} * \colon E \times E &\to E \\ (x, y) &\mapsto x * y \end{aligned}$$

$x * y$ s'appelle composé de x et y.

Une lci est notée $*$, $\top$, $\oplus$, $\otimes$,... et très souvent $+$ ou $\cdot$.

Si la lci est notée $+$ elle est dite additive, et si elle est notée $\cdot$, elle est dite multiplicative.

Soit E un ensemble, et $*$ une lci sur E.

Définition (associativité)

On dit que $*$ est associative si

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

Soit E un ensemble, et $*$ une lci sur E.

Définition (associativité)

On dit que $*$ est associative si

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

Définition (commutativité)

- On dit que deux éléments x et y de E commutent (ou sont permutables) si $x * y = y * x$.
- On dit que $*$ est commutative si

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

Soit E un ensemble, et $*$ et $\top$ deux lci dans E.

Définition (Distributivité)

On dit que $\top$ est distributive *sur*, *pour* ou *par rapport à* $*$ si

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

Soit E un ensemble muni d'une lci $*$.

Définition (Elément neutre)

Soit $e \in E$. On dit que e est un élément neutre pour $*$ si

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

Soit E un ensemble muni d'une lci $*$.

Définition (Elément neutre)

Soit $e \in E$. On dit que e est un élément neutre pour $*$ si

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

Proposition

Si e et e' sont deux éléments neutres de $*$ dans E alors $e = e'$.

Soit E un ensemble muni d'une lci $*$ admettant un élément neutre e.

Définition (Eléments symétrisable)

Un élément x de E est dit symétrisable pour $*$ s'il existe un élément y de E tel que : $x * y = y * x = e$.

Un tel élément y est appelé un symétrique de x pour $*$.

Soit E un ensemble muni d'une lci $*$ admettant un élément neutre e.

Définition (Eléments symétrisable)

Un élément x de E est dit symétrisable pour $*$ s'il existe un élément y de E tel que : $x * y = y * x = e$.

Un tel élément y est appelé un symétrique de x pour $*$.

Proposition (unicité du symétrique)

Supposons que $*$ est associative et soit $x \in E$.

Si x est symétrisable pour $*$ alors x admet un seul symétrique pour $*$.

Remarque

Si x un élément symétrisable de E alors le symétrique de x est noté x', $sym(x)$ ou x^{-1}.

Lorsque la loi est notée $+$, le symétrique de x (s'il existe) est noté $-x$ et appelé opposé de x.

Si x est un élément symétrisable pour une loi associative, alors il peut être simplifié.

Remarque

Si x un élément symétrisable de E alors le symétrique de x est noté x', $sym(x)$ ou x^{-1}.

Lorsque la loi est notée $+$, le symétrique de x (s'il existe) est noté $-x$ et appelé opposé de x.

Si x est un élément symétrisable pour une loi associative, alors il peut être simplifié.

Proposition (symétrique du composé)

Supposons que $*$ est associative et soit $x, y \in E$.

Si x et y sont symétrisables pour $*$ alors $x * y$ est symétrisable pour $*$ et

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

Exercice

Soit les lci $\oplus$ et $\otimes$ définies sur $\mathbb{R}$ par :

$$\forall x \in \mathbb{R} : x \oplus y = x + y - 1$$

$$\forall x \in \mathbb{R} : x \otimes y = x + y - xy$$

1. Les loi $\oplus$ et $\otimes$ sont-elles associatives ?
2. Les loi $\oplus$ et $\otimes$ sont-elles commutatives ?
3. Montrer que $\otimes$ est distributive par rapport à $\oplus$.
4. Quels sont les éléments neutres pour $\oplus$ et $\otimes$?
5. Quels sont les éléments symétrisables pour chacunes de ces lois ?

Groupes

Définition (Groupe)

On dit qu'un ensemble G muni d'une lci $*$ est un groupe si et seulement si :

- $*$ est associative ;
- G admet un neutre pour $*$;
- tout élément de G admet un symétrique pour $*$.

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

Définition (Sous-groupe)

Soit $(G, *)$ un groupe. Une partie H non-vide de G est appelée un sous-groupe de G si la restriction de $*$ à H lui confère une structure de groupe.

Définition (Sous-groupe)

Soit $(G, *)$ un groupe. Une partie H non-vide de G est appelée un sous-groupe de G si la restriction de $*$ à H lui confère une structure de groupe.

Remarque

L'élément neutre de tout sous-groupe H de G coïncide avec celui de G.

Proposition

Soit $(G, *)$ un groupe et H un sous-ensemble *non-vide* de G, alors H est un sous-groupe de G si et seulement si

- $\forall x, y \in H : x * y \in H$;
- $\forall x \in H : x^{-1} \in H$.

Proposition

Soit $(G, *)$ un groupe et H un sous-ensemble *non-vide* de G, alors H est un sous-groupe de G si et seulement si

- $\forall x, y \in H : x * y \in H$;
- $\forall x \in H : x^{-1} \in H$.

Ce qui est aussi équivalent à

- $\forall x, y \in H : x * y^{-1} \in H$.

Proposition

Soit G un groupe et H_1 et H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Proposition

Soit G un groupe et H_1 et H_2 deux sous-groupes de G. Alors $H_1 \cap H_2$ est un sous-groupe de G.

Remarque

Ce résultat reste valable pour un nombre quelconque de groupes.

Morphismes de groupes

Définition

Soit $(G, *)$ et $(G', \perp)$ deux groupes.

- On appelle *morphisme* (ou *homomorphisme*) de groupes de $(G, *)$ dans $(G', \perp)$ toute application $f : G \to G'$ telle que

$$\forall (x, y) \in G : f(x * y) = f(x) \perp f(y).$$

Morphismes de groupes

Définition

Soit $(G, *)$ et $(G', \perp)$ deux groupes.

- On appelle *morphisme* (ou *homomorphisme*) de groupes de $(G, *)$ dans $(G', \perp)$ toute application $f : G \to G'$ telle que

$$\forall (x, y) \in G : f(x * y) = f(x) \perp f(y).$$

- On appelle *isomorphisme* tout morphisme bijectif.

Morphismes de groupes

Définition

Soit $(G, *)$ et $(G', \perp)$ deux groupes.

- On appelle *morphisme* (ou *homomorphisme*) de groupes de $(G, *)$ dans $(G', \perp)$ toute application $f : G \to G'$ telle que

$$\forall (x, y) \in G : f(x * y) = f(x) \perp f(y).$$

- On appelle *isomorphisme* tout morphisme bijectif.
- On appelle *endomorphisme* de $(G, *)$ tout morphisme de $(G, *)$ dans $(G, *)$.

Morphismes de groupes

Définition

Soit $(G, *)$ et $(G', \perp)$ deux groupes.

- On appelle *morphisme* (ou *homomorphisme*) de groupes de $(G, *)$ dans $(G', \perp)$ toute application $f : G \to G'$ telle que

$$\forall (x, y) \in G : f(x * y) = f(x) \perp f(y).$$

- On appelle *isomorphisme* tout morphisme bijectif.
- On appelle *endomorphisme* de $(G, *)$ tout morphisme de $(G, *)$ dans $(G, *)$.
- On appelle *automorphisme* tout endomorphisme bijectif.

Proposition

Soit deux groupes $(G, *)$ et $(G', \perp)$, et $f : G \to G'$ un morphisme de groupes.

Si e est l'élément neutre de G et e' l'élément neutre de G' alors $f(e) = e'$, et pour tout élément x de G, on a $f(x^{-1}) = [f(x)]^{-1}$.

Noyau et image d'un morphisme

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

Définition

- On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre e' de G'.

$$\ker(f) = \{x \in G \mid f(x) = e'\}$$

Noyau et image d'un morphisme

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

Définition

- On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre e' de G'.

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

Noyau et image d'un morphisme

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

Définition

- On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre e' de G'.

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

- On appelle image de f l'ensemble des images, $f(G)$. On note :

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

Noyau et image d'un morphisme

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

Définition

- On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre e' de G'.

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

- On appelle image de f l'ensemble des images, $f(G)$. On note :

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

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

Proposition

- Le noyau de f est un sous-groupe de G.
- L'image de f est un sous-groupe de G'.

Théorème

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

- f *est une injection si et seulement si* $\ker f = \{e\}$.
- f *est une surjection si et seulement si* $\operatorname{Im} f = G'$.

Théorème (Transfert de la structure de groupe)

Soit $(G, *)$ *un groupe et* G' *un ensemble muni d'une lci* $\perp$.

S'il existe une application bijective $f : G \to G'$ *telle que*

$$\forall x, y \in G : f(x * y) = f(x) \perp f(y)$$

alors $(G', \perp)$ *est un groupe.*

Définition

Soit A un ensemble muni de deux lois de composition internes $*$ et $\top$.

On dit que $(A, *, \top)$ est un anneau si :

- $(A, *)$ est un groupe commutatif.
- $\top$ est associative.
- $\top$ est distributive par rapport à $*$.

Définition

Soit A un ensemble muni de deux lois de composition internes $*$ et $\top$.

On dit que $(A, *, \top)$ est un anneau si :

- $(A, *)$ est un groupe commutatif.
- $\top$ est associative.
- $\top$ est distributive par rapport à $*$.

Si $\top$ est commutative, ont dit que l'anneau est commutatif, et si elle a un élément neutre on dit que l'anneau est unitaire.

Remarque

Dans un anneau, on note habituellement la première loi additivement et la seconde multiplicativement.

Dans ce cas, on note 0 l'élément neutre de la première loi et 1 l'élément neutre de la deuxième loi (s'il existe).

Remarque

Dans un anneau, on note habituellement la première loi additivement et la seconde multiplicativement.

Dans ce cas, on note 0 l'élément neutre de la première loi et 1 l'élément neutre de la deuxième loi (s'il existe).

Définition (Sous-anneau)

Soit $(A, +, .)$ un anneau et H une partie *non vide* de A, alors H est un sous-anneau de A si et seulement si :

- $\forall x, y \in H : x - y \in H$,
- $\forall x, y \in H : xy \in H$.

Définition

Soit A un anneau tel que $A \neq \{0\}$. S'il existe deux éléments a et b de A tels que :

$$a \neq 0 \quad \text{et} \quad b \neq 0 \quad \text{et} \quad ab = 0,$$

alors on dit que a et b sont des diviseurs de zéro.

Définition

Soit A un anneau tel que $A \neq \{0\}$. S'il existe deux éléments a et b de A tels que :

$$a \neq 0 \quad \text{et} \quad b \neq 0 \quad \text{et} \quad ab = 0,$$

alors on dit que a et b sont des diviseurs de zéro.

Définition (Anneau intégre)

On dit qu'un anneau est intègre s'il est distinct de $\{0\}$ et s'il ne possède pas de diviseurs de zéro.

Définition

Soit $\mathbb{K}$ un ensemble muni de deux lois de composition internes $*$ et $\top$.

On dit que $(\mathbb{K}, *, \top)$ est un corps si

1. $(\mathbb{K}, *, \top)$ est un anneau unitaire,
2. tous les éléments de $\mathbb{K}$ sauf le neutre de $*$ sont symétrisables pour $\top$.