NOMBRES ET STRUCTURES ALGEBRIQUES

1 Nombres entiers naturels.

1.1 Loi de composition interne.

Définition

Soit E un ensemble, une opération ou une loi de composition interne - en abrégé une l.c.i. - sur E est une application de $E \times E$ dans E.

Exemples

α. $+$ et $\times$ sont des l.c.i. sur $\mathbb{N}$.

β. Pour tout ensemble E, la réunion et l'intersection sont des l.c.i. sur $\mathcal{P}(E)$.

γ. Soient X et E deux ensembles. On suppose E muni d'une l.c.i., notée $*$. On peut munir E^X d'une l.c.i., encore notée $*$, définie par :

$$\forall (f,g) \in E^X, \qquad \begin{array}{rccc} f*g & : & X & \to & E \\ & & x & \mapsto & f(x)*g(x) \end{array}$$

et appelée extension à E^X de la l.c.i. $*$ de E.

δ. Soient E et F deux ensembles munis de l.c.i. T et $\perp$ respectivement. Alors on peut munir $E \times F$ d'une l.c.i. $*$ définie par :

$$\forall (x,y) \in E \times F, \quad \forall (x',y') \in E \times F, \qquad (x,y)*(x',y') = (xTx', y \perp y').$$

1.2 Associativité et commutativité.

Définitions : une l.c.i. $*$ dans un ensemble E est dite

associative si et seulement si

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

commutative si et seulement si

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

Exemples

α. $+$ et $\times$ de $\mathbb{N}$ sont associatives et commutatives.

β. Soit E un ensemble. La loi de composition est associative et non commutative sur $\mathcal{F}(E,E)$.

γ. La loi sur $\mathbb{N}$ définie par

$$\forall (x,y) \in \mathbb{N}^2, \qquad x*y = x^y$$

n'est pas associative.

1.3 Elément neutre.

Définition

Soit E une ensemble muni d'une l.c.i. $*$. On dit que $e \in E$ est neutre pour $*$ si et seulement si

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

Exemples

α. 0 est neutre pour $+$ dans $\mathbb{N}$ et 1 est neutre pour $\times$ dans $\mathbb{N}$.

β. Soit E un ensemble. Id_E est neutre pour la loi de composition sur $\mathcal{F}(E,E)$.

γ. La loi sur $\mathbb{R}_+^*$ définie par

$$\forall (x,y) \in \mathbb{N}^2, \qquad x * y = x^y$$

n'a pas d'élément neutre.

Proposition

Soit E un ensemble muni d'une l.c.i.. Si e et e' sont neutres pour cette loi dans E alors $e = e'$.

2 Nombres entiers relatifs.

2.1 $\mathbb{Z}$ et la structure de groupe.

2.1.1 Symétrie.

Définitions soit E un ensemble muni d'une loi de composition interne $*$ associative et telle que $*$ possède un élément neutre e.

Un élément x de E est dit symétrisable pour $*$ si et seulement s'il existe un élément y de E tel que $x * y = y * x = e$. Un tel élément y (s'il existe) est appelé un symétrique de x pour $*$.

Exemples

α. Dans $\mathbb{N}$, tout élément de $\mathbb{N}^*$ n'est pas symétrisable pour $+$. En revanche, dans $\mathbb{Z}$, c'est vrai.

β. Soit E un ensemble. Soit $f \in \mathcal{F}(E,E)$. f est symétrisable pour $\circ$ dans $\mathcal{F}(E,E)$ si et seulement si f est bijective.

Proposition

Soit E un ensemble muni d'une l.c.i. $*$ associative et d'élément neutre e. Soit $x \in E$, symétrisable pour $*$. Alors x admet un et un seul symétrique pour $*$.

Remarque : soit E un ensemble muni d'une l.c.i. $*$ associative et d'élément neutre e. Soit $x \in E$, symétrisable pour $*$. Le symétrique de x est noté x^{-1} et est appelé aussi inverse de x. Lorsque la loi est notée $+$, le symétrique de x est noté $-x$ et est appelé opposé de x.

Proposition

Soit E un ensemble muni d'une l.c.i. $*$ associative et d'élément neutre e. Soient x et y dans E, symétrisables pour $*$. Alors $x * y$ est symétrisable pour $*$ et

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

2.1.2 Structure de groupe.

Définitions

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

(i) $*$ est associative,

(ii) $*$ possède un élément neutre e,

(iii) tout élément de G est symétrisable pour $*$.

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

Exemples

α. $(\mathbb{Z},+)$ est un groupe abélien.

β. Soient (E,T) et $(F,\perp)$ deux groupes. Alors $E\times F$ muni de la loi produit est un groupe.

γ. Soit X un ensemble. Soit $(E,*)$ un groupe. Alors $(E^X,*)$ est un groupe.

2.1.3 Sous-groupes.

Définition

Soit $(G,*)$ un groupe d'élément neutre e. Soit $H\in\mathcal{P}(G)$. On dit que H est un sous-groupe de G si et seulement si :

(i) $\forall (x,y)\in H^2$, $x*y\in H$,

(ii) $e\in H$,

(iii) $\forall x\in H$, $x^{-1}\in H$.

Exemples

α. Pour tout $n\in\mathbb{Z}$, $n\mathbb{Z}=\{na \mid a\in\mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z},+)$. On peut démontrer que ce sont les seuls.

β. L'ensemble des suites bornées dans $\mathbb{K}$ est un sous-groupe de $(\mathbb{K}^{\mathbb{N}},+)$.

Proposition

Soient $(G,*)$ un groupe et $H\in\mathcal{P}(G)$. Pour que H soit un sous-groupe de $(G,*)$, il faut et il suffit que l'on ait :

(i) H stable par $*$ (i.e. $\forall (x,y)\in H^2$, $x*y\in H$),

(ii) H est un groupe pour la loi induite par la loi $*$ de G (i.e. $H\times H\to H$, $(x,y)\mapsto x*y$).

Proposition

Soient $(G,*)$ un groupe et $H\in\mathcal{P}(G)$. Pour que H soit un sous-groupe de $(G,*)$, il faut et il suffit que l'on ait :

(i) H non vide,

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

2.1.4 Morphismes de groupes.

Définitions

Soient $(G,*)$ et (G',T) deux groupes d'éléments neutres respectifs e et e'. Soit $f\in\mathcal{F}(G,G')$. On dit que f est un morphisme de groupes de $(G,*)$ dans (G',T) lorsque :

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

Un endomorphisme de groupe de $(G,*)$ est un morphisme de groupes de $(G,*)$ vers $(G,*)$.

Un isomorphisme de groupes de $(G,*)$ dans (G',T) est un morphisme de groupes bijectif de $(G,*)$ vers (G',T).

Un automorphisme de groupe de $(G,*)$ est un isomorphisme de groupes de $(G,*)$ vers $(G,*)$ (ou un endomorphisme bijectif de $(G,*)$).

Exemple

Soit $f : (\mathbb{Z},+) \to (\mathbb{Z},+)$, $x \mapsto 2 \times x$. Alors f est un endomorphisme de groupe de $(\mathbb{Z},+)$.

Proposition

Soit f : $(G,*) \to (G',T)$ un morphisme de groupes. On note e et e' les éléments neutres respectifs de $(G,*)$ et (G',T) respectivement. Alors

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

(ii) $\forall x \in G$, $f(x^{-1}) = (f(x))^{-1}$.

Définitions

Soient $(G,*)$ et (G',T) deux groupes d'éléments neutres respectifs e et e'. Soit f un morphisme de groupes de $(G,*)$ dans (G',T). On appelle

(i) noyau de f et on note $\ker(f)$ l'ensemble :

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

(ii) image de f et on note $\mathrm{Im}(f)$ l'ensemble :

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

Proposition

Soit f : $(G,*) \to (G',T)$ un morphisme de groupes. $\ker(f)$ est un sous-groupe de $(G,*)$ et $\mathrm{Im}(f)$ est un sous-groupe de (G',T).

Proposition

Soit f : $(G,*) \to (G',T)$ un morphisme de groupes, d'éléments neutres respectifs e et e'. f est injectif si et seulement si $\ker(f) = \{e\}$.

Définition

Soient $(G,*)$ et (G',T) deux groupes. On dit que $(G,*)$ est isomorphe à (G',T) si et seulement s'il existe un isomorphisme de groupes de $(G,*)$ vers (G',T).

2.2 $\mathbb{Z}$ et la structure d'anneau.

2.2.1 Structure d'anneau.

Définition

Soit E un ensemble muni de deux l.c.i., notées $*$ et T. On dit que T est distributive sur $*$ si et seulement si :

$$\forall (x,y,z) \in E^3, \quad xT(y*z) = (xTy)*(xTz) \quad \text{et} \quad (y*z)Tx = (yTx)*(zTx).$$

Exemple

Pour tout ensemble E, chacune des lois $\cap$ et $\cup$ est distributive sur les deux lois $\cap$ et $\cup$ dans $\mathcal{P}(E)$.

Définitions

Soit A un ensemble muni de deux l.c.i. notées $+$ et $\times$. On dit que $(A,+,\times)$ est un anneau si et seulement si

(i) $(A,+)$ est un groupe abélien,

(ii) $\times$ est associative.

(iii) $\times$ est distributive sur $+$.
(iv) A admet un élément neutre pour $\times$.
Si de plus, $\times$ est commutative, alors $(A, +, \times)$ est un anneau commutatif.

Exemples
α. $(\mathbb{Z}, +, \times)$ est un anneau commutatif.
β. Soit $(E, *)$ un groupe abélien. $(E^E, *, \circ)$ n'est pas un anneau.

2.2.2 Sous-anneaux

Définition
Soit $(A, +, \times)$ un anneau. Soit $B \in \mathcal{P}(A)$. On dit que B est un sous-anneau de $(A, +, \times)$ si et seulement si :
(i) B est un sous-groupe de $(A, +)$,
(ii) $\forall (x, y) \in B^2$, $x \times y \in B$,
(iii) $1 \in B$ (on a noté 1 le neutre de $\times$ dans A).

2.2.3 Morphismes d'anneaux

Définitions
Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. Soit $f : A \to B$. On dit que f est un morphisme d'anneaux de $(A, +_A, \times_A)$ dans $(B, +_B, \times_B)$ lorsque :
(i) $\forall (x, y) \in A^2$, $f(x +_A y) = f(x) +_B f(y)$,
(ii) $\forall (x, y) \in A^2$, $f(x \times_A y) = f(x) \times_B f(y)$,
(iii) $f(1_A) = 1_B$, où on a noté 1_A et 1_B les éléments neutres respectifs de A et B pour leurs deuxièmes lois.

3 Les nombres rationnels.

3.1 Inverses dans un anneau.

Définition
Soit $(A, +, \times)$ un anneau. On note A^* l'ensemble des éléments inversibles pour $\times$ dans A.

Exemple
$\mathbb{Z}^* = \{-1, 1\}$.

Proposition
Soit $(A, +, \times)$ un anneau. $(A^*, \times)$ est un groupe.

3.2 Structure de corps.

Définitions
Un ensemble K muni de deux lois $+$ et $\times$ est appelé un corps si et seulement si :
(i) $(K, +, \times)$ est un anneau,
(ii) $0_K \neq 1_K$.
(iii) Tout élément de $K \setminus \{0\}$ admet un inverse pour $\times$ dans K.
Si de plus $\times$ est commutative, on dit que $(K, +, \times)$ est un corps commutatif.

Exemple
$(\mathbb{Q}, +, \times)$ est un corps commutatif.

3.3 Sous-corps.

Définition

Soit $(K, +, \times)$ un corps. Soit L une partie de K. On dit que L est un sous-corps de K si et seulement si :

(i) L est un sous-anneau de $(K, +, \times)$,

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

4 Les nombres réels.

$(\mathbb{R}, +, \times)$ est un corps commutatif.
$(\mathbb{R}_+^*, \times)$ est un groupe.
L'exponentielle est un isomorphisme de groupes de $(\mathbb{R}, +)$ vers $\mathbb{R}_+^*, \times)$.
$(\mathbb{R}_+^*, \times)$ est isomorphe à $(\mathbb{R}, +)$ car ln est un isomorphisme de groupes de $(\mathbb{R}_+^*, \times)$ sur $(\mathbb{R}, +)$.
$\mathbb{Z}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.
$2\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{Q}, +, \times)$.
$\mathbb{Q}$ est un sous-corps de $(\mathbb{R}, +, \times)$.

5 Les nombres complexes.

$(\mathbb{C}, +, \times)$ est un corps commutatif.
$(\mathbb{C}^*, \times)$ est un groupe abélien.
$(\mathbb{U}, \times)$ est un groupe abélien.
Pour tout $n \in \mathbb{N}^*$, $(\mathbb{U}_n, \times)$ est un groupe abélien.
$\theta \mapsto e^{i\theta}$ est un morphisme surjectif de $(\mathbb{R}, +)$ sur $(\mathbb{U}, \times)$ de noyau $2\pi\mathbb{Z}$.
$z \mapsto e^z$ est un morphisme surjectif de $(\mathbb{C}, +)$ sur $(\mathbb{C}^*, \times)$, de noyau $2i\pi\mathbb{Z}$.
$\mathbb{R}$ est un sous-corps de $(\mathbb{C}, +, \times)$.