Arithmetique | CM: 3

Par Lorenzo

20 septembre 2024

Définition 0.1. *Soient $(G, *)$ et $(H, \square)$ deux groupes.*
*On appelle **morphisme de groupes** toute application $f : G \to H$ vérifiant*

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

Proposition 0.1.

Si $f : G \to H$ est un morphisme de groupe, alors $f(e_G) = e_H$

Démonstration 0.1.

$f(e_G) = f(e_G * e_G) = f(e_G) \square f(e_G)$
$f(e_G) = f(e_G) \square e_H$
$f(e_G) \square f(e_G) = f(e_G) \square e_H \implies f(e_G) = e_H$

□

Proposition 0.2.

Si $f : G \to H$ est un morphisme de groupe, alors $\forall x \in G, f(x^{-1}) = f(x)^{-1}$

Démonstration 0.2.

$f(x^{-1}) = f(x^{-1}) \square f(x) \square f(x)^{-1} = f(x^{-1} * x) \square f(x)^{-1} = f(x)^{-1}$

□

0.1 Anneaux et Corps

Définition 0.2. *Un **anneau** est $(A, +, \times)$ où A est un ensemble, $+$ et x sont deux l.c.i sur A vérifiant les axiomes suivants*

- *$(A, +)$ est un groupe abélien (on note 0_A sont élément neutre)*
- *$\times$ est associative*
- *$\times$ est distributive sur $+$*

Remarques 0.1. *On dit que $(A, +, \times)$ est un anneau commutatif si, de plus $\times$ est commutative.*
Un élément $x \in A$ est dit inversible dans A lorsqu'il adment un symétrique pour $\times$.

Proposition 0.3.

Soit $(A, +, \times)$ un anneau alors
$\forall x \in A,\ 0_A \times x = 0_A$

Démonstration 0.3.

$$\begin{aligned} 0_A \times x &= (0_A + 0_A) \times x \\ &= 0_A \times x + 0_A \times x \implies 0_A = 0_A \times x \text{ (par soustraction de } 0_A \times x) \end{aligned}$$

□

Proposition 0.4.

Soient $x, y, z \in A$, Si $x \times z = y \times z$ et z est inversible alors $x = y$

Démonstration 0.4.

$$\begin{aligned} x \times z = y \times z &\implies (x \times z) \times z^{-1} = (y \times z) \times z^{-1} \\ &\implies x \times (z \times z^{-1}) = y \times (z \times z^{-1}) \\ &\implies x \times 1_A = y \times 1_A \\ &\implies x = y \end{aligned}$$

□

Définition 0.3. *Un **corps** est la donnée d'un triplet $(\mathbb{k}, +, \times)$ où $\mathbb{k}$ est un ensemble, $+$ et $\times$ sont deux l.c.i sur $\mathbb{k}$ vérifiant les axiomes suivants:*

- *$(\mathbb{k}, +, \times)$ est un anneau commutatif*
- *$(\mathbb{k}^*, \times)$ est un groupe abélien (de neutre noté $1_{\mathbb{k}}$).*

Remarques 0.2. *De manière équivalente, un corps est un anneau commutatif avec un élément neutre pour $\times$ où tout élément non-nul est inversible.*

1 Arithmétique des entiers

1.1 Rappels sur $\mathbb{N}$ et $\mathbb{Z}$

Théorème 1.1. *(propriétés de $+$ et $\times$ sur $\mathbb{N}$)*

(a) *$+$ et $\times$ sont associative et commutative sur $\mathbb{N}$*

(b) *0 est élement neutre pour $+$ tandis que 1 est neutre pour $\times$*

(c) *Il y a une distributivité de $\times$ sur $+$*

(d) *$\forall x, y, m \in \mathbb{N},\ x + m = y + m \implies x = y$*

Théorème 1.2. *(propriétés de $\leq$ sur $\mathbb{N}$)*

1) *(relation d'ordre total) $\forall m, n, p \in \mathbb{N}$*

(a) *$n \leq n$*

(b) $m \leq n \wedge n \leq m \iff m = n$

(c) $m \leq n \wedge n \leq p \implies m \leq p$

(d) $m \leq n \vee n \leq m$

2) *Les opérations* $+$ *et* $\times$ *sont compatibles avec la relation d'ordre*
$\forall n, m, p \in \mathbb{N},\ n \leq m \implies (n + p \leq m + p) \wedge (n \times p \leq m \times p)$

3) $\forall n \in \mathbb{N},\ 0 \leq n$

4) $\forall n, m \in \mathbb{N}, \forall p \in \mathbb{N}^*,\ n \leq m \implies n \times p \leq m \times p$

Théorème 1.3.

1. *Toute partie finie de* $\mathbb{N}$ *admet un plus grand élément.*

2. *Toute partie non vide de* $\mathbb{N}$ *admet un plus petit élément.*

3. *Toute partie non vide et majorée de* $\mathbb{N}$ *admet un plus grand élément.*

4. $\mathbb{N}$ *n'admet pas de plus grand élément.*

Théorème 1.4. *(propriétés de* $+$ *et* $\times$ *sur* $\mathbb{Z}$*)*

(a) $+$ *et* $\times$ *sont associative et commutative sur* $\mathbb{Z}$

(b) *0 est élement neutre pour* $+$ *tandis que 1 est neutre pour* $\times$

(c) *Il y a une distributivité de* $\times$ *sur* $+$

(d) *Tout* $m \in \mathbb{Z}$ *admet un symétrique (élément inverse),* $-m \in \mathbb{Z}$ *pour* $+$

Théorème 1.5. *(propriétés de* $\leq$ *sur* $\mathbb{Z}$*)*

1) $\leq$ *est une relation d'ordre totale sur* $\mathbb{Z}$.

2) *Soient* $n, m, p \in \mathbb{Z}$

(a) $n \leq m \iff n + p \leq m + p$

(b) $\forall p \in \mathbb{Z}_+^*, n \leq m \iff np \leq mp$

(c) $\forall p \in \mathbb{Z}_-^*, n \leq m \iff mp \leq np$

(d) $\forall p \in \mathbb{Z}^*, m = n \iff mp = np$