Arithmetique | CM: 2

Par Lorenzo

13 septembre 2024

1 Structures algébriques

1.1 Lois de compositions internes

Définition 1.1. *Soit E un ensemble. On appelle **loi de composition interne** (l.c.i) sur E une opération binaire.*

On parle d'application $E \times E \to E$

Définition 1.2. *Soit $*$ une l.c.i sur E. On dit que $*$ est*

associative *si* $\forall x, y, z \in E,\ x * (y * z) = (x * y) * z$

commutative *si* $\forall x, y \in E,\ x * y = x * y$

identitaire *(a un **élement neutre** $e \in E$) si* $\forall x \in E, x * e = e * x = x$

1.2 Groupes

Définition 1.3. *Soit G un ensemble et $*$ une l.c.i sur G. On dit que $(G, *)$ est un **groupe** lorsque les axiomes suivants sont vérifiés.*

- *$*$ est associative*
- *$*$ admet un élement neutre $e \in G$*
- *$\forall x \in G, \exists x' \in G$ tel que $x * x' = x' * x = e$ (on dit que x' est l'élement inverse ou symétrique de x pour $*$)*

Remarques 1.1. *Si de plus $*$ est commutative, alors le groupe est dit **abélien** (ou commutatif).*

Example 1.1. *Si X est un ensemble, notons $Bij(X)$, l'ensemble des application de X dans X admettant une application réciproque*

$$\forall\, f\colon X \to X,\ \exists\, g\colon X \to X,\ g \circ f = f \circ g = \mathrm{Id}_X : \begin{cases} X & \to X \\ x & \mapsto x \end{cases}$$

Ainsi $(Bij(X), \circ)$ est un groupe.

Proposition 1.1.

Si $(G, *)$ est un groupe alors

(a) *L'élement neutre de G est unique*

(b) *Chaque $x \in G$ admet un unique élement inverse*

(c) *Si $x, y, z \in G$ tel que $x * y = z * y$ alors $x * y$ (indépendament de l'ordre)*

Démonstration 1.1.

(a) *Soient e, e' des élements neutres de G par *, $e * e' = e' * e = e = e'$*

(b) *Soient x', x" des élements inverse de $x \in G$,*
$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$

(c) *Posons $x^{-1} * (x * y) = x^{-1} * (x * z) \implies (x^{-1} * x) * y = (x^{-1} * x) * z \implies e * y = e * z \implies y = z$*

$\square$

Remarques 1.2. *Lorsqu'il n'y a pas d'ambiguïtés, l'inverse d'un élement x sera noté x^{-1}. Notons que $(x^{-1})^{-1} = x$*

Définition 1.4. *Soit (G, *) un groupe. Soit $H \subset G$, on dit que H est un* ***sous-groupe*** *de G lorsque les condtions suivantes sont vérifiées.*

- *$\forall x, y \in H,\ x * y \in H$. On dit que H est stable par $*$*
- *Muni de $*$, H est un groupe*

Proposition 1.2.

Soit $(G, *)$ un groupe et $H \subset G$. Les conditions suivantes sont équivalentes.

(a) *H est un sous groupe de G*

(b) *$H \neq \emptyset$, H est stable par $*$ et par passage au symétrique ($\forall x \in H,\ x^{-1} \in H$)*

(b) *$H \neq \emptyset$ et $\forall x, y \in H,\ x * y^{-1} \in H$*

Démonstration 1.2.

• *Démontrons que $(a) \implies (b)$.*

◇ *H est un sous groupe donc doit admettre un élement neutre (e_H) donc $H \neq \emptyset$. Montrons que $e_H = e_G$, on a $e_H * e_H = e_H = e_G + e_H = e_G$.*

◇ *La stabilité par * fait partie de la définition de sous groupe.*

◇ *Soit $x \in H$, soit s' son symétrique dans H. x' est aussi un symétrique dans G. Dans G par unicité du symétrique $x^{-1} = x' \in H$.*

• *Démontrons que $(b) \implies (c)$.*

◇ *Soient $x, y \in H$. Alors $y^{-1} \in H$ et encore par $x * x^{-1} \in H$.*

• *Démontrons que $(c) \implies (a)$.*

◇ *l'associativité est montré par $\forall x, y, z \in H, x, y, z \in G, x * (y * z) = (x * y) * z$*

$\diamond$ *l'élement neutre par* $\exists x \in H, e = x * x^{-1} \in G$, *ainsi* $\forall x \in H, x \in G$

$\diamond$ *l'élement inverse par* $x \in H$, *prenons* $y = e$, *ainsi* $x^{-1} * e = x^{-1}$, *ici* x^{-1} *est le symétrique de* x *dans* H.

$\diamond$ *la stabilité par* $*$ *dans* H *par* $x, y \in H$, *posons* $z = y^{-1}$, *ainsi* $x * y = x * z^{-1} \in H$.

> *Finalement par implication circulaire nous avons démontré que*
> $(a) \iff (b) \iff (c)$

$\square$