Structures algébriques

Par
Rabah Bououden
Centre Universitaire Abdelhafid Boussouf - Mila.

1er mars 2021

Contents

Definition

Soit E un ensemble non vide.

1. On appelle **loi de composition interne** sur E une application de $E \times E$ dans E. Si T désigne cette application, alors l'image du couple $(x, y) \in E \times E$ par T s'écrit xTy .
2. On appelle **ensemble structuré** tout couple (E, T) où E est un ensemble non vide et T une loi de composition interne sur E.

Example

Les lois de compositions internes les plus courantes sont :

1. $+$ dans $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. et mais pas sur $\mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$
2. $-$ dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
3. $\times$ dans $\mathbb{N}, \mathbb{N}^*, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
4. $/$ dans $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$.
5. 0 (composition des applications) dans l'ensemble des applications de $\mathbb{E}$ dans E.
6. La loi $\oplus$définie sur $\mathbb{R}^2$ par $(x_1, y_1) \oplus (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$.
7. La loi T définie sur $\mathbb{R}$ par $xTy = x + y - xy$.
8. Les lois $\cup$, $\cap$ (union, intersection) définies sur $P(E)$ (ensemble des parties d'un ensemble E).

Definition

(Propriétés des lois)
Soit (E, T) un ensemble structuré.

1. La loi T est dite associative sur E si $(xTy)Tz = xT(yTz)$ pour tous x, y, z appartenant à E.
2. La loi T est dite commutative sur E si $xTy = yTx$ pour tous x, y appartenant à E.

Example

L'addition et la multiplication sont associatives et commutatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definition

(Propriétés des lois)
Soit (E, T) un ensemble structuré.

1. La loi T est dite associative sur E si $(xTy)Tz = xT(yTz)$ pour tous x, y, z appartenant à E.
2. La loi T est dite commutative sur E si $xTy = yTx$ pour tous x, y appartenant à E.

Example

L'addition et la multiplication sont associatives et commutatives sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Definition

(Propriétés des lois)
Soit (E, T) un ensemble structuré.

1. Un élément e de E est dit neutre pour la loi T si, pour tout $x \in E$,
$$xTe = eTx = x$$
.
2. Si (E, T) possède un élément neutre e alors un élément x de E est dit symétrisable pour la loi T s'il existe un élément x' de E tel que
$$xTx' = x'Tx = e$$
.
L'élément x' est alors appelé élément symétrique de x pour la loi T.

Proposition

Soit (E, T) un ensemble structuré. Si l'élément neutre de E pour la loi T existe, alors il est unique.

Proposition

Soit (E, T) un ensemble structuré pour lequel la loi T est associative et admet un élément neutre.

1. *Si $x \in E$ est symétrisable, alors son symétrique est unique.*
2. *Si $x \in E$ et $y \in E$ sont symétrisables alors xTy est symétrisable et son symétrique $(xTy)'$ est donné par $(xTy)' = y'Tx'$ où x' désigne le symétrique de x et y' celui de y.*

Proposition

Soit (E, T) un ensemble structuré. Si l'élément neutre de E pour la loi T existe, alors il est unique.

Proposition

Soit (E, T) un ensemble structuré pour lequel la loi T est associative et admet un élément neutre.

1. *Si $x \in E$ est symétrisable, alors son symétrique est unique.*
2. *Si $x \in E$ et $y \in E$ sont symétrisables alors xTy est symétrisable et son symétrique $(xTy)'$ est donné par $(xTy)' = y'Tx'$ où x' désigne le symétrique de x et y' celui de y.*

Definition

Soit (G, T) un ensemble structuré.

1. On dit que (G, T) est un groupe si
   1. la loi T est associative sur G,
   2. il existe un élément neutre pour la loi T dans G,
   3. tout élément de G est symétrisable pour la loi T.

   On dit aussi que l'ensemble G possède une structure de groupe pour la loi T.
2. On dit que le groupe (G, T) est commutatif (ou abélien) si la loi T est commutative sur G.

Example

On fournit d'abord des exemples de groupes

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de la somme.
2. $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ munis du produit.

Example

Pour diverses raisons (à déterminer), les couples suivants ne sont pas des groupes :

1. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.
2. $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

Example

On fournit d'abord des exemples de groupes

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munis de la somme.
2. $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$ munis du produit.

Example

Pour diverses raisons (à déterminer), les couples suivants ne sont pas des groupes :

1. $(\mathbb{N}, +)$, $(\mathbb{R}, \times)$.
2. $(\mathcal{P}(E), \cup)$, $(\mathcal{P}(E), \cap)$.

Definition

(Sous groupes)
Un sous-groupe d'un groupe $(G, *)$ est une partie non vide H de G telle que :

1. $*$ induit sur H une loi de composition interne.
2. Muni de cette loi, H est un groupe. On note alors : $H < G$.

Proposition

L'ensemble $H \subset G$ est un sous-groupe d'un groupe $(G, *)$ si et seulement si

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y \in H$,
3. $\forall x \in H,\ x' \in H$.

Definition

(Sous groupes)
Un sous-groupe d'un groupe $(G, *)$ est une partie non vide H de G telle que :

1. $*$ induit sur H une loi de composition interne.
2. Muni de cette loi, H est un groupe. On note alors : $H < G$.

Proposition

L'ensemble $H \subset G$ est un sous-groupe d'un groupe $(G, *)$ si et seulement si

1. $H \neq \varnothing$,
2. $\forall (x, y) \in H^2,\ x * y \in H$,
3. $\forall x \in H,\ x' \in H$.

Example

1. Soit $(G, *)$ un groupe. Alors G et $\{e_G\}$ sont des sous groupes de G.
2. $(\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{R}, +)$.

Proposition

L'ensemble $H \subset G$ est un sous-groupe d'un groupe $(G, *)$ si et seulement si

1. $H \neq \emptyset$,
2. $\forall (x, y) \in H^2,\ x * y' \in H$,

Proposition

L'intersection quelconque de sous groupes d'un groupe $(G, *)$ est un sous groupe de $(G, *)$.

Proposition

L'ensemble $H \subset G$ est un sous-groupe d'un groupe $(G, *)$ si et seulement si

1. $H \neq \emptyset$,
2. $\forall (x, y) \in H^2,\ x * y' \in H$,

Proposition

L'intersection quelconque de sous groupes d'un groupe $(G, *)$ est un sous groupe de $(G, *)$.

Remarque

L'union quelconque de sous groupes d'un groupe $(G, *)$, n'est pas nécessairement un sous groupe de $(G, *)$.

Example

Soit T la loi de composition intèrne défini sur $\mathbb{R}^2$ par

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1) T (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

On a $(\mathbb{R}^2, T)$ est un groupe, $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ sont deux sous groupes de $(\mathbb{R}^2, T)$ mais $\mathbb{R} \times \{0\} \bigcup \{0\} \times \mathbb{R}$ ne forme pas un sous-groupe de $(\mathbb{R}^2, T)$.

Remarque

L'union quelconque de sous groupes d'un groupe $(G, *)$, n'est pas nécessairement un sous groupe de $(G, *)$.

Example

Soit T la loi de composition intèrne défini sur $\mathbb{R}^2$ par

$$\forall (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2, \quad (x_1, y_1) T (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

On a $(\mathbb{R}^2, T)$ est un groupe, $\mathbb{R} \times \{0\}$ et $\{0\} \times \mathbb{R}$ sont deux sous groupes de $(\mathbb{R}^2, T)$ mais $\mathbb{R} \times \{0\} \bigcup \{0\} \times \mathbb{R}$ ne forme pas un sous-groupe de $(\mathbb{R}^2, T)$.

Proposition

L'union de deux sous-groupes A et B d'un même groupe $(G, *)$,est un sous-groupe $(A \bigcup B < G)$ si, et seulement si, $A \subset B$ ou $B \subset A$.

Il est d'abord clair que si n est un entier que l'on peut supposer positif et non nul, l'ensemble $n\mathbb{Z}$ des entiers relatifs de la forme nk, k décrivant $\mathbb{Z}$, est un sous-groupe additif de $(\mathbb{Z}, +)$: ensemble des multiples de n.

Proposition

Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$.

Il est d'abord clair que si n est un entier que l'on peut supposer positif et non nul, l'ensemble $n\mathbb{Z}$ des entiers relatifs de la forme nk, k décrivant $\mathbb{Z}$, est un sous-groupe additif de $(\mathbb{Z}, +)$: ensemble des multiples de n.

Proposition

Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$.

Démonstration.

Soit S un sous-groupe de $\mathbb{Z}$ autre que $\{0\}$ et $\mathbb{Z}$. S ne contient donc pas 1. L'ensemble des entiers positifs de S, noté S^+, admet un plus petit élément n au moins égal à 2 (ensemble dénombrable, borné inférieurement). Tout élément de $\mathbb{Z}$ de la forme kn, k entier naturel, est un élément de S (évident par récurrence car $kn = n + n + ... + n$). Donc S contient $n\mathbb{Z}$. Par division euclidienne, tout entier de S^+ qui n'est pas de la forme kn s'écrit $a = kn + r$, $0 < r < n$. On a alors $r = a - kn > 0$. Mais a et kn sont dans S^+, donc r aussi. Voilà un entier de S strictement plus petit que son plus petit élément (Pas possible), donc $r = 0$. Ce qui montre que $S = n\mathbb{Z}$. □

On montre très facilement que la relation de congruence modulo n, $n \in \mathbb{N}$, due à Gauss notée $\equiv$:

$$\forall x, y \in \mathbb{Z} \quad x \equiv y[n] \Leftrightarrow \quad (x-y) \in n\mathbb{Z} \Leftrightarrow \quad \exists k \in \mathbb{N} / \quad y = x - nk.$$

Démonstration.

Soit S un sous-groupe de $\mathbb{Z}$ autre que $\{0\}$ et $\mathbb{Z}$. S ne contient donc pas 1. L'ensemble des entiers positifs de S, noté S^+, admet un plus petit élément n au moins égal à 2 (ensemble dénombrable, borné inférieurement). Tout élément de $\mathbb{Z}$ de la forme kn, k entier naturel, est un élément de S (évident par récurrence car $kn = n + n + ... + n$). Donc S contient $n\mathbb{Z}$. Par division euclidienne, tout entier de S^+ qui n'est pas de la forme kn s'écrit $a = kn + r$, $0 < r < n$. On a alors $r = a - kn > 0$. Mais a et kn sont dans S^+, donc r aussi. Voilà un entier de S strictement plus petit que son plus petit élément (Pas possible), donc $r = 0$. Ce qui montre que $S = n\mathbb{Z}$. □

On montre très facilement que la relation de congruence modulo n, $n \in \mathbb{N}$, due à Gauss notée $\equiv$:

$$\forall x, y \in \mathbb{Z} \quad x \equiv y[n] \Leftrightarrow \quad (x-y) \in n\mathbb{Z} \Leftrightarrow \quad \exists k \in \mathbb{N}/ \quad y = x - nk.$$

($x \equiv y[n]$ on lit « x est congru à y modulo n » est une relation d'équivalence définie dans $(Z, +)$. L'ensemble quotient est fini et peut ainsi s'écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, ..., \widehat{n-1}\}.$$

Par exemples : $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$ et $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

($x \equiv y[n]$ on lit « x est congru à y modulo n » est une relation d'équivalence définie dans $(Z, +)$. L'ensemble quotient est fini et peut ainsi s'écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, ..., \widehat{n-1}\}.$$

Par exemples : $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$ et $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

($x \equiv y[n]$ on lit « x est congru à y modulo n » est une relation d'équivalence définie dans $(Z, +)$. L'ensemble quotient est fini et peut ainsi s'écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\dot{0}, \dot{1}, ..., \overset{\bullet}{n-1}\}.$$

Par exemples : $\mathbb{Z}/2\mathbb{Z} = \{\dot{0}, \dot{1}\}$, $\mathbb{Z}/3\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\}$, $\mathbb{Z}/4\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}\}$ et $\mathbb{Z}/6\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}\}$.

- L'addition quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{+} \dot{y} = \dot{\overbrace{x + y}}.$$

- La multiplication quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{\times} \dot{y} = \dot{\overbrace{x \times y}}.$$

Proposition

L'ensemble $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est un groupe additif commutatif, groupe quotient de Z par la relation de congruence.

- L'addition quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{+} \dot{y} = \dot{\overbrace{x + y}}.$$

- La multiplication quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{\times} \dot{y} = \dot{\overbrace{x \times y}}.$$

Proposition

L'ensemble $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est un groupe additif commutatif, groupe quotient de Z par la relation de congruence.

- L'addition quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{+} \dot{y} = \widehat{x + y}.$$

- La multiplication quotient sur $\mathbb{Z}/n\mathbb{Z}$ induite par celle de $\mathbb{Z}$, est :

$$\forall x, y \in \mathbb{Z}/n\mathbb{Z} \quad \dot{x} \dot{\times} \dot{y} = \widehat{x \times y}.$$

Proposition

L'ensemble $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est un groupe additif commutatif, groupe quotient de Z par la relation de congruence.

Definition

(Homomorphismes de groupes)
Soient $(G, *)$ et (H, T) deux groupes. Une application f de G dans H est un **Homomorphisme de groupes** lorsque :

$$\forall x,\ y \in G, \quad f(x * y) = f(x) T f(y).$$

De plus

1. Si $G = H$ et $* = T$, on parle d'endomorphisme.
2. Si f est bijective, on parle d'isomorphisme.
3. Si f est un endomorphisme bijectif, on parle d'automorphisme.

Example

$x \longmapsto 2x$ réalise un automorphisme de $(R, +)$.

Definition

(Homomorphismes de groupes)
Soient $(G, *)$ et (H, T) deux groupes. Une application f de G dans H est un **Homomorphisme de groupes** lorsque :

$$\forall x,\ y \in G, \quad f(x * y) = f(x) T f(y).$$

De plus

1. Si $G = H$ et $* = T$, on parle d'endomorphisme.
2. Si f est bijective, on parle d'isomorphisme.
3. Si f est un endomorphisme bijectif, on parle d'automorphisme.

Example

$x \longmapsto 2x$ réalise un automorphisme de $(R, +)$.

Proposition

(Quelques propriétés élémentaires des Homomorphismes de groupes)
f est ici un Homomorphisme de $(G,*)$ dans (H,T)

1. $f(e_G) = e_H$.
2. $\forall x \in G \quad f(x') = (f(x))'$ *(x' est le symétrique de x dans G et $(f(x))'$ est le symétrique de $f(x)$ dans H)*
3. *Si f est un isomorphisme, alors son application réciproque f^{-1} réalise un isomorphisme de (H,T) sur $(G,*)$.*
4. $G_1 < G$, *alors* $f(G_1) < H$.
5. $H_1 < H$, *alors* $f^{-1}(H_1) < G$.

Definition

Soit f un Homomorphisme de G dans H.

1. Le noyau de f, noté $Ker(f)$ est l'ensemble des antécédents par f de e_H :

$$Ker(f) = \{x \in G, \quad f(x) = e_H\} = f^{-1}\{e_H\}$$

(attention, f n'est pas supposée bijective ; il n'est donc pas question de la bijection réciproque de f).

2. L'image de f, noté $Im(f)$ est $f(G)$ (ensemble des images par f des éléments de G).

Remarque

D'après les deux derniers points de la proposition (9), le noyau et l'image de f sont des sous-groupes respectifs de G et H.

Definition

Soit f un Homomorphisme de G dans H.

1. Le noyau de f, noté $Ker(f)$ est l'ensemble des antécédents par f de e_H :

$$Ker(f) = \{x \in G, \quad f(x) = e_H\} = f^{-1}\{e_H\}$$

(attention, f n'est pas supposée bijective ; il n'est donc pas question de la bijection réciproque de f).

2. L'image de f, noté $Im(f)$ est $f(G)$ (ensemble des images par f des éléments de G).

Remarque

D'après les deux derniers points de la proposition (9), le noyau et l'image de f sont des sous-groupes respectifs de G et H.

Proposition

Soit f un Homomorphisme de $(G, *)$ dans (H, T). Alors f est injectif si et seulement si $Ker(f) = \{e_G\}$.

Definition

Un anneau est un ensemble muni de deux LCI $(A, *, T)$ tels que :

1. $(A, *)$ est un groupe commutatif d'élément neutre noté 0_A.
2. La loi T est une LCI sur A associative et distributive à gauche et à droite par rapport à $*$:

   $$\forall x,\ y,\ z \in A, \quad xT(y*z) = xTy*xTz \ \text{ et } \ (x*y)Tz = xTz*yTz.$$

3. La loi T admet un élément neutre différent de 0_A, noté 1_A.

Example

$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux bien connus.

Definition

Un anneau est un ensemble muni de deux LCI $(A, *, T)$ tels que :

1. $(A, *)$ est un groupe commutatif d'élément neutre noté 0_A.
2. La loi T est une LCI sur A associative et distributive à gauche et à droite par rapport à $*$:

$$\forall x,\ y,\ z \in A, \quad xT(y*z) = xTy*xTz \ \text{ et } \ (x*y)Tz = xTz*yTz.$$

3. La loi T admet un élément neutre différent de 0_A, noté 1_A.

Example

$(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux bien connus.

Remarque

1. *Si la loi T est commutative, l'anneau est dit commutatif ou abélien.*
2. *L'ensemble $A - \{0_A\}$ est noté A^*.*
3. *Par souci de simplification, nous laissons de côté (provisoirement) les notations T et $*$ des deux lois internes définies sur A au profit des notations additive ($+$) et multiplicative ($\times$). Donc on dit l'anneau $(A, +, \times)$ au lieu de $(A, *, T)$.*

Definition

1. Un anneau commutatif $(A, +, \times)$ est dit intègre s'il est
   1. différent de l'anneau nul (autrement dit : si $1_A \neq 0_A$),
   2. $\forall (x, y) \in A^2, \quad x.y = 0 \quad \Rightarrow \quad (x = 0 \quad ou \quad b = 0)$.
2. Lorsqu'un produit $a \times b$ est nul alors que ni a, ni b ne le sont, on dit que a et b sont des diviseurs de zéro.

Example

1. $(\mathbb{Z}, +, \times)$ des entiers relatifs est intègre : il ne possède aucun diviseur de zéro.
2. L'anneau $\mathbb{Z}/6\mathbb{Z}$ des classes résiduelles modulo 6 n'est pas intègre puisque $\dot{2} \times \dot{3} = \dot{6}$, donc $\dot{2} \times \dot{3} = \dot{0}$. De même $\mathbb{Z}/4\mathbb{Z}$.

Definition

1. Un anneau commutatif $(A, +, \times)$ est dit intègre s'il est
   1. différent de l'anneau nul (autrement dit : si $1_A \neq 0_A$),
   2. $\forall (x, y) \in A^2, \quad x.y = 0 \quad \Rightarrow \quad (x = 0 \quad ou \quad b = 0)$.
2. Lorsqu'un produit $a \times b$ est nul alors que ni a, ni b ne le sont, on dit que a et b sont des diviseurs de zéro.

Example

1. $(\mathbb{Z}, +, \times)$ des entiers relatifs est intègre : il ne possède aucun diviseur de zéro.
2. L'anneau $\mathbb{Z}/6\mathbb{Z}$ des classes résiduelles modulo 6 n'est pas intègre puisque $\dot{2} \times \dot{3} = \dot{6}$, donc $\dot{2} \times \dot{3} = \dot{0}$. De même $\mathbb{Z}/4\mathbb{Z}$.

Proposition

Les règles de calcul dans les anneaux sont les suivantes :

Soit $(A, +, \times)$ *un anneau alors :*

1. $x.0_A = 0_A.x = 0_A$. *L'élément* 0_A *est alors dit absorbant pour la loi* $\times$*).*
2. $\forall (x, y) \in A^2, \quad (-x)y = x(-y) = -(xy).$
3. $\forall x \in A, \quad (-1_A)x = -x.$
4. $\forall (x, y) \in A^2, \quad (-x)(-y) = xy.$
5. $\forall (x, y, z) \in A^3, \quad x(y - z) = xy - xz$ *et* $(y - z)x = yx - zx.$

Definition

Soit $(A, *, T)$ un anneau. Une partie non vide A_1 de A est un sous-anneau de A lorsque :

1. $1_A \in A_1$;
2. les lois $*$ et T induisent des LCI sur A_1, et, muni de ces lois, $(A_1, *, T)$ est un anneau.

Proposition

Une partie A_1 de A est un sous-anneau si et seulement si

1. *$(A_1, *)$ est un sous-groupe de $(A, *)$;*
2. *$1_A \in A_1$;*
3. *$\forall (x, y) \in A_1^2 \quad xTy \in A_1$ (T induit une LCI sur A_1).*

Definition

Soit $(A, *, T)$ un anneau. Une partie non vide A_1 de A est un sous-anneau de A lorsque :

1. $1_A \in A_1$;
2. les lois $*$ et T induisent des LCI sur A_1, et, muni de ces lois, $(A_1, *, T)$ est un anneau.

Proposition

Une partie A_1 de A est un sous-anneau si et seulement si

1. $(A_1, *)$ *est un sous-groupe de* $(A, *)$;
2. $1_A \in A_1$;
3. $\forall (x, y) \in A_1^2 \quad xTy \in A_1$ *(T induit une LCI sur A_1).*

Example

$(\mathbb{Z},\ *,\ T)$ est un sous anneau de $(\mathbb{Q},\ *,\ T)$ qui est un sous anneau de $(\mathbb{R},\ *,\ T)$ qui est un sous anneau de $(\mathbb{C},\ *,\ T)$

Definition

Soient $(A, +_A, \times_A)$ et $(B, +_B, \times_B)$ deux anneaux. Un homomorphisme d'anneaux de A vers B est une application de A vers B telle que :

1. $f(1_A) = 1_B$;
2. pour tout $x,\ y \in A,\quad f(x +_A y) = f(x) +_B f(y) \quad et \quad f(x \times_A y) = f(x) \times_B f(y)$.

Soit $(A, +, \times)$ un anneau commutatif

Definition

(Idéal)
Une partie I de A est un idéal d'un anneau $(A, +, \times)$ si

1. $(I, +)$ est un sous-groupes de $(A, +)$,
2. Pour tout $a \in A$, on a $aI \subset I$. En d'autres termes $\forall a \in A, \forall x \in I : ax \in I$.

Proposition

Une partie I de A est un idéal d'un anneau $(A, +, \times)$ ssi

1. *I contient l'élément zéro 0_A,*
2. *pour tous $x, y \in I : x - y \in I$,*
3. *$\forall a \in A, \forall x \in I : ax \in I$.*

Soit $(A, +, \times)$ un anneau commutatif

Definition

(Idéal)
Une partie I de A est un idéal d'un anneau $(A, +, \times)$ si

1. $(I, +)$ est un sous-groupes de $(A, +)$,
2. Pour tout $a \in A$, on a $aI \subset I$. En d'autres termes $\forall a \in A, \forall x \in I : ax \in I$.

Proposition

Une partie I de A est un idéal d'un anneau $(A, +, \times)$ ssi

1. *I contient l'élément zéro 0_A,*
2. *pour tous $x, y \in I : x - y \in I$,*
3. *$\forall a \in A, \forall x \in I : ax \in I$.*

Example

1. Tout anneau non trivial a au moins deux idéaux, l'idéal trivial $\{0\}$ et A lui-même. Les idéaux de A distincts de A sont dits propres.
2. Tout élément x de A permet de définir un idéal principal :

$$< x >= xA = \{ax/a \in A\}$$

. C'est le plus petit idéal qui contient a, on dit qu'il est engendré par a. Si a est inversible (et seulement dans ce cas), $aA = A$.

3. Plus généralement, si $x_1, ..., x_n \in A$, le plus petit idéal contenant $x_1, ..., x_n$ est :

$$< x_1, ..., x_n >= x_1A + ... + x_nA = \{a_1x_1 + ... + a_nx_n/a_1, ..., a_n \in A\}$$

Definition

Corps

1. Un corps est un anneau commutatif dans lequel tout élément non nul est inversible.
2. Si, de plus, la seconde loi $\times$ est commutative sur K alors on dit que le corps $(K, +, \times)$ est commutatif.

Example

$(\mathbb{Q}, +, \times)$ et $(\mathbb{R}, +, \times)$ sont des corps commutatif.

Definition

Corps

1. Un corps est un anneau commutatif dans lequel tout élément non nul est inversible.
2. Si, de plus, la seconde loi $\times$ est commutative sur K alors on dit que le corps $(K, +, \times)$ est commutatif.

Example

$(\mathbb{Q},\ +,\ \times)$ et $(\mathbb{R},\ +,\ \times)$ sont des corps commutatif.

Definition

Sous corps

Soit $(K, +, \times)$ un corps et soit K_1 un sous partie non vide de K. On dit que K_1 est un sous corps de K si K_1 est stable pour $+$ et $\times$ de K et K_1 muni des lois induites par celles de K est lui-même un corps

Example

$(\mathbb{Q}, +, \times)$ et un sous corps de$(\mathbb{R}, +, \times)$.

Definition

Sous corps

Soit $(K, +, \times)$ un corps et soit K_1 un sous partie non vide de K. On dit que K_1 est un sous corps de K si K_1 est stable pour $+$ et $\times$ de K et K_1 muni des lois induites par celles de K est lui-même un corps

Example

$(\mathbb{Q},\ +,\ \times)$ et un sous corps de$(\mathbb{R},\ +,\ \times)$.

Proposition

Soit $(K, +, \times)$. Un sous partie K_1 de K est un sous corps si et seulement si

1. *$(K_1, +)$ soit un sous-groupe de K,*
2. *pour tous x et y de K_1, $x \times y \in K_1$ (stabilité de K_1 pour la loi $\times$),*
3. *K_1 contient l'élément unité de K et l'inverse de tout x de K_1 dans $(K, \times)$ est élément de K_1.*