Mathématiques

Chapitre B6
Structures algébriques

MPSI – Lycée Bellevue – Toulouse

Année 2024-2025

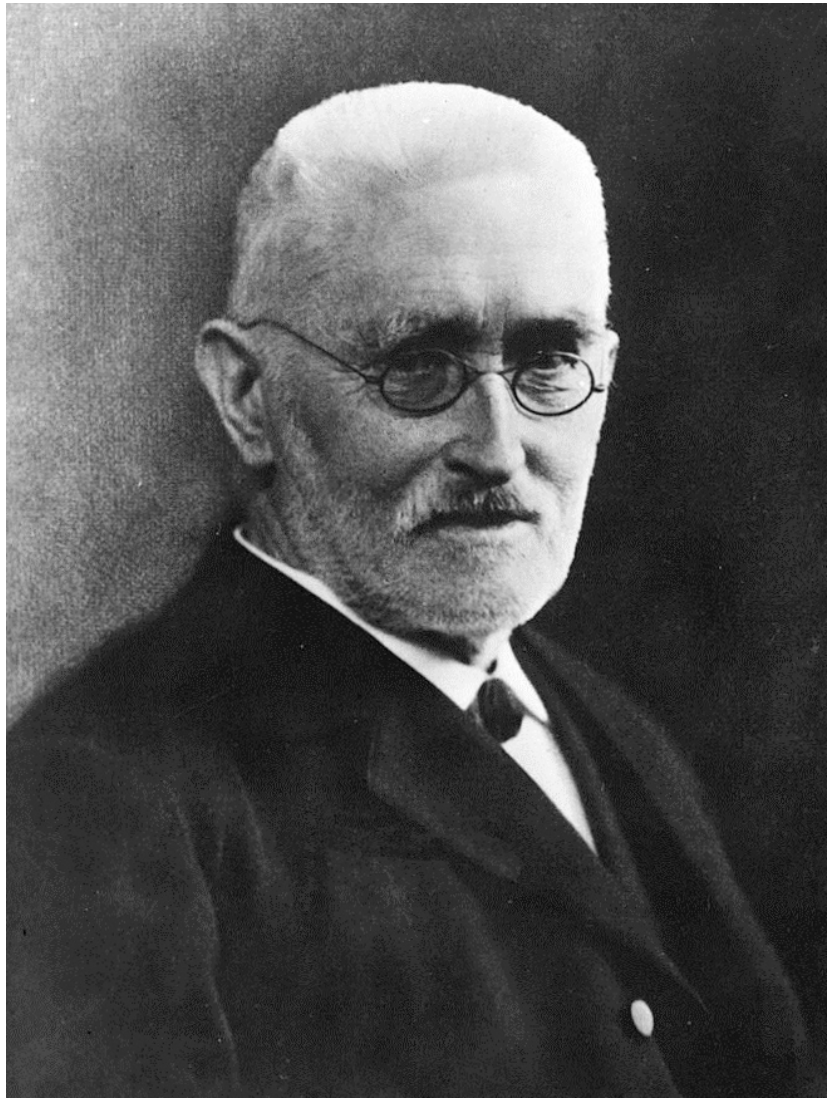
Évariste Galois (France) 1811 – 1832

Niels Abel (Norvège) 1802 – 1829

Johann Dirichlet (Allemagne) 1805 – 1859

Leopold Kronecker (Allemagne) 1823 – 1891

Richard Dedekind (Allemagne) 1831 – 1916



Chapitre B6. Structures algébriques

I. Lois de composition internes

Chapitre B6. Structures algébriques

Chapitre B6. Structures algébriques

Chapitre B6. Structures algébriques

Définition

Soit E un ensemble.

Une loi de composition interne est une application de $E \times E$ dans E :

$$\begin{aligned} * : E \times E &\longrightarrow E \\ (x, y) &\longmapsto x * y \end{aligned}$$

On note $x * y$ au lieu de $*(x, y)$.

Exemple 1

(i) L'addition, la soustraction, la multiplication sont des lci de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Exemple 1

(i) L'addition, la soustraction, la multiplication sont des lci de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) La soustraction n'est pas une lci de $\mathbb{N}$.

Exemple 1

(i) L'addition, la soustraction, la multiplication sont des lci de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) La soustraction n'est pas une lci de $\mathbb{N}$.

(iii) La division n'est pas une lci de $\mathbb{Z}$, ni de $\mathbb{R}$, mais de $\mathbb{R}^*$.

Exemple 1

(i) L'addition, la soustraction, la multiplication sont des lci de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) La soustraction n'est pas une lci de $\mathbb{N}$.

(iii) La division n'est pas une lci de $\mathbb{Z}$, ni de $\mathbb{R}$, mais de $\mathbb{R}^*$.

(iv) L'intersection et l'union sont des lci de $\mathcal{P}(E)$.

Exemple 1

(i) L'addition, la soustraction, la multiplication sont des lci de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(ii) La soustraction n'est pas une lci de $\mathbb{N}$.

(iii) La division n'est pas une lci de $\mathbb{Z}$, ni de $\mathbb{R}$, mais de $\mathbb{R}^*$.

(iv) L'intersection et l'union sont des lci de $\mathcal{P}(E)$.

(v) Le PGCD et le PPCM sont des lci de $\mathbb{Z}$ et $\mathbb{N}$.

Exemple 1

(v) L'addition des matrices (n, p) et la multiplication des matrices (n, n) sont des lci, de $\mathcal{M}_{np}(\mathbb{K})$ et de $\mathcal{M}_n(\mathbb{K})$ respectivement.

Exemple 1

(v) L'addition des matrices (n,p) et la multiplication des matrices (n,n) sont des lci, de $\mathcal{M}_{np}(\mathbb{K})$ et de $\mathcal{M}_n(\mathbb{K})$ respectivement.

(vi) La loi $\circ$ est une lci de $\mathcal{F}(X,X)$.

Définitions

Une lci $*$ est :

- commutative si :

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

- associative si :

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

Définitions

Une lci $*$ est :

- commutative si :

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

- associative si :

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

Remarque

Si $x * y = y * x$ alors on dit que x et y commutent
ou que x commute avec y.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) La division dans $\mathbb{R}^*$.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) La division dans $\mathbb{R}^*$.

(iv) L'intersection et l'union dans $\mathcal{P}(E)$.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) La division dans $\mathbb{R}^*$.

(iv) L'intersection et l'union dans $\mathcal{P}(E)$.

(v) Le PGCD et le PPCM dans $\mathbb{Z}$ et $\mathbb{N}$.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) La division dans $\mathbb{R}^*$.

(iv) L'intersection et l'union dans $\mathcal{P}(E)$.

(v) Le PGCD et le PPCM dans $\mathbb{Z}$ et $\mathbb{N}$.

(vi) L'addition des matrices, La multiplication des matrices.

Exemple 1 (suite)

Quelles sont les lci commutatives et associatives ?

(i) L'addition, la soustraction, la multiplication dans $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(iii) La division dans $\mathbb{R}^*$.

(iv) L'intersection et l'union dans $\mathcal{P}(E)$.

(v) Le PGCD et le PPCM dans $\mathbb{Z}$ et $\mathbb{N}$.

(vi) L'addition des matrices, La multiplication des matrices.

(vii) La composition dans $\mathcal{F}(X, X)$.

Définition

Soit ∇ et Δ deux lci sur E.

∇ est distributive par rapport à Δ si :

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

$$x \nabla (y \Delta z) = (x \nabla y) \Delta (x \nabla z)$$

et $$(y \Delta z) \nabla x = (y \nabla x) \Delta (z \nabla x)$$

Exemples

- La multiplication est distributive par rapport à l'addition.
- L'intersection est distributive par rapport à l'union.
- L'union est distributive par rapport à l'intersection.

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$: élément neutre 0

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$: élément neutre 0
- Loi $\times$ de $\mathbb{R}$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$: élément neutre 0
- Loi $\times$ de $\mathbb{R}$: élément neutre 1

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$: élément neutre 0
- Loi $\times$ de $\mathbb{R}$: élément neutre 1
- Lois $-$ et $/$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathbb{Z}$: élément neutre 0
- Loi $\times$ de $\mathbb{R}$: élément neutre 1
- Lois $-$ et $/$: pas d'élément neutre.

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Lois $\cap$ et $\cup$ de $\mathcal{P}(E)$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Lois $\cap$ et $\cup$ de $\mathcal{P}(E)$: éléments neutres

  E pour $\cap$ et $\varnothing$ pour $\cup$

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Lois $\cap$ et $\cup$ de $\mathcal{P}(E)$: éléments neutres

  E pour $\cap$ et $\varnothing$ pour $\cup$

- (De même, $\wedge$ et $\vee$ admettent pour éléments neutres respectifs 0 et 1.)

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$: élément neutre 0_{np}

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$: élément neutre 0_{np}
- Loi $\times$ de $\mathcal{M}_n(\mathbb{K})$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$: élément neutre 0_{np}
- Loi $\times$ de $\mathcal{M}_n(\mathbb{K})$: élément neutre I_n

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$: élément neutre 0_{np}
- Loi $\times$ de $\mathcal{M}_n(\mathbb{K})$: élément neutre I_n
- Loi $\circ$ de $\mathcal{F}(X)$:

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Exemples

- Loi $+$ de $\mathcal{M}_{np}(\mathbb{K})$: élément neutre 0_{np}
- Loi $\times$ de $\mathcal{M}_n(\mathbb{K})$: élément neutre I_n
- Loi $\circ$ de $\mathcal{F}(X)$: élément neutre Id_X

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Proposition

L'élément neutre est unique.

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Proposition

L'élément neutre est unique.

Démonstration. Supposons qu'il existe deux éléments neutres e et e'.

Définition

Élément neutre de $*$: $e \in E$ tel que :

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

Proposition

L'élément neutre est unique.

Démonstration. Supposons qu'il existe deux éléments neutres e et e'.

□

Définition

E muni d'une lci $*$ associative, admettant un élément neutre.

$x \in E$ est symétrisable si :

$$\exists y \in E \qquad x * y = y * x = e$$

Définition

E muni d'une lci $*$ associative, admettant un élément neutre.

$x \in E$ est symétrisable si :

$$\exists y \in E \qquad x * y = y * x = e$$

y est unique, il est appelé symétrique de x.

Définition

E muni d'une lci $*$ associative, admettant un élément neutre.

$x \in E$ est symétrisable si :

$$\exists y \in E \qquad x * y = y * x = e$$

y est unique, il est appelé symétrique de x.

▷ Exercice 1.

Démontrer l'unicité du symétrique.

Remarque

Si la loi $*$ est commutative :

$$\begin{aligned} x * y = e \quad &\Longrightarrow \quad y * x = e \\ &\Longrightarrow \quad x * y = y * x = e \end{aligned}$$

Il suffit de vérifier un seul sens.

Remarque

Si la loi $*$ est commutative :

$$\begin{aligned} x * y = e \quad &\Longrightarrow \quad y * x = e \\ &\Longrightarrow \quad x * y = y * x = e \end{aligned}$$

Il suffit de vérifier un seul sens.

De même pour l'élément neutre :

$$\begin{aligned} \forall x \in E \quad x * e = x \quad &\Longrightarrow \quad e * x = x \\ &\Longrightarrow \quad x * e = e * x = x \end{aligned}$$

Il suffit de vérifier que $x * e = x$ pour tout $x \in E$.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x * y = y * x = e$$

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x \times y = y \times x = 1$$

Exemples

- $x \in \mathbb{R}$ est symétrisable pour $\times$ ssi $x \neq 0$.
  On note x^{-1} son symétrique, on l'appelle inverse de x.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x \times y = y \times x = 1$$

Exemples

- $x \in \mathbb{R}$ est symétrisable pour $\times$ ssi $x \neq 0$.
  On note x^{-1} son symétrique, on l'appelle inverse de x.
- Les seuls éléments de $\mathbb{Z}$ symétrisables pour $\times$ sont 1 et -1.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x + y = y + x = 0$$

Exemples

- Tout élément de $\mathbb{Z}$ et de $\mathbb{R}$ admet un symétrique pour $+$.
  On le note $-x$ et on l'appelle opposé de x.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x + y = y + x = 0$$

Exemples

- Toute matrice de $\mathcal{M}_{np}(\mathbb{K})$ admet un symétrique pour $+$.
  On le note $-M$ est on l'appelle opposée de M.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x \times y = y \times x = 1$$

Exemples

- Toute matrice de $\mathcal{M}_{np}(\mathbb{K})$ admet un symétrique pour $+$.
  On le note $-M$ est on l'appelle opposée de M.
- Une matrice A de $\mathcal{M}_n(\mathbb{K})$ est symétrisable pour $\times$ si elle est inversible. Son inverse est A^{-1}.

Définition

$x \in E$ est inversible si :

$$\exists y \in E \qquad x * y = y * x = e$$

Exemples

- $f : X \to X$ est symétrisable pour $\circ$ ssi :

$$\exists g : X \to X \qquad f \circ g = g \circ f = \mathrm{Id}_X$$

Donc f est symétrisable ssi elle est bijective.
Son symétrique est sa réciproque, notée f^{-1}.

▷ Exercice 2.

Soit E un ensemble.

Quels sont les éléments symétrisables de $\mathcal{P}(E)$

- pour la loi $\cap$?
- Pour la loi $\cup$?

Proposition

E ensemble muni

- d'une lci $*$ associative,
- d'un élément neutre e.

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

Proposition

E ensemble muni

- d'une lci $*$ associative,
- d'un élément neutre e.

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

Son symétrique est :

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

Démonstration. Par associativité :

$$\begin{aligned}(x*y)*(y^{-1}*x^{-1}) &= x*(y*y^{-1})*x^{-1}\\ &= x*e*x^{-1}\\ &= e\end{aligned}$$

$$\begin{aligned}(y^{-1}*x^{-1})*(x*y) &= y^{-1}*(x^{-1}*x)*y\\ &= y^{-1}*e*y\\ &= e\end{aligned}$$

Donc $x*y$ est symétrisable de symétrique $y^{-1}*x^{-1}$.

□

Définition

Soit $*$ une lci associative sur E.

Les puissances ou itérés de x sont définies par :

$$x^1 = x \qquad \forall n \in \mathbb{N}^* \quad x^{n+1} = x * x^n$$

Définition

Soit $*$ une lci associative sur E.

Les puissances ou itérés de x sont définies par :

$$x^1 = x \qquad \forall n \in \mathbb{N}^* \quad x^{n+1} = x * x^n$$

Si E possède un élément neutre e pour $*$:

$$x^0 = e$$

Définition

Soit $*$ une lci associative sur E.

Les puissances ou itérés de x sont définies par :

$$x^1 = x \qquad \forall n \in \mathbb{N}^* \quad x^{n+1} = x * x^n$$

Si E possède un élément neutre e pour $*$:

$$x^0 = e$$

Si x est symétrisable :

$$\forall n \in \mathbb{N} \qquad x^{-n} = (x^n)^{-1}$$

Proposition

Pour tout $x \in E$ et $(m,n) \in (\mathbb{N}^*)^2$:

$$x^{m+n} = x^m * x^n \qquad \text{et} \qquad (x^m)^n = x^{mn}$$

Si E admet un élément neutre ces formules sont valables pour tout $(m,n) \in \mathbb{N}^2$.
Si x est symétrisable elles sont valables pour tout $(m,n) \in \mathbb{Z}^2$.

Proposition

Pour tout $x \in E$ et $(m,n) \in (\mathbb{N}^*)^2$:

$$x^{m+n} = x^m * x^n \qquad \text{et} \qquad (x^m)^n = x^{mn}$$

Si E admet un élément neutre ces formules sont valables pour tout $(m,n) \in \mathbb{N}^2$.
Si x est symétrisable elles sont valables pour tout $(m,n) \in \mathbb{Z}^2$.

Démonstration. La première formule se démontre par récurrence sur n en fixant m.

Proposition

Pour tout $x \in E$ et $(m,n) \in (\mathbb{N}^*)^2$:

$$x^{m+n} = x^m * x^n \qquad \text{et} \qquad (x^m)^n = x^{mn}$$

Si E admet un élément neutre ces formules sont valables pour tout $(m,n) \in \mathbb{N}^2$.
Si x est symétrisable elles sont valables pour tout $(m,n) \in \mathbb{Z}^2$.

Démonstration. La première formule se démontre par récurrence sur n en fixant m.
La seconde s'en déduit.

Proposition

Pour tout $x \in E$ et $(m,n) \in (\mathbb{N}^*)^2$:

$$x^{m+n} = x^m * x^n \qquad \text{et} \qquad (x^m)^n = x^{mn}$$

Si E admet un élément neutre ces formules sont valables pour tout $(m,n) \in \mathbb{N}^2$.
Si x est symétrisable elles sont valables pour tout $(m,n) \in \mathbb{Z}^2$.

Démonstration. Les extensions aux entiers relatifs s'en déduisent également en passant au symétrique.
□

Notation

Pour la loi $+$ on note nx au lieu de x^n.

La propriété devient :

$$(m+n)x = mx + nx \qquad \text{et} \qquad m(nx) = (mn)x$$

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{Z}$ est une partie de $\mathbb{R}$ stable par $+$ et $\times$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{Z}$ est une partie de $\mathbb{R}$ stable par $+$ et $\times$.
- $\{\pm 1\}$ est une partie de $\mathbb{Z}$ stable par $\times$ mais pas par $+$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{Z}$ est une partie de $\mathbb{R}$ stable par $+$ et $\times$.
- $\{\pm 1\}$ est une partie de $\mathbb{Z}$ stable par $\times$ mais pas par $+$.
  $n\mathbb{Z}$ est une partie de $\mathbb{Z}$ stable par $+$ et par $\times$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ et par $\times$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ et par $\times$.
  $i\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ mais pas par $\times$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ et par $\times$.
  $i\mathbb{R}$ est une partie de $\mathbb{C}$ stable par $+$ mais pas par $\times$.
  $\mathbb{U}$ est une partie de $\mathbb{C}$ non stable par $+$ mais stable par $\times$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- Si $A \subseteq E$ alors $\mathcal{P}(A)$ est une partie de $\mathcal{P}(E)$ stable par $\cap$ et $\cup$.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$ sont des parties de $\mathcal{M}_n(\mathbb{K})$ stables par addition et produit.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$ sont des parties de $\mathcal{M}_n(\mathbb{K})$ stables par addition et produit.
  $\mathcal{S}_n(\mathbb{K})$ et $\mathcal{A}_n(\mathbb{K})$ sont stables par addition mais pas par produit.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- L'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ est une partie de $\mathcal{F}(\mathbb{R})$ stable par $\circ$.

Démonstration.

Définition

Soit E muni d'une lci $*$.

Une partie F de E est stable par $*$ si :

$$\forall (x,y) \in F^2 \qquad x * y \in F$$

Exemples

- L'ensemble des fonctions affines de $\mathbb{R}$ dans $\mathbb{R}$ est une partie de $\mathcal{F}(\mathbb{R})$ stable par $\circ$.

Démonstration. □

Définition

Soit A une partie de E **stable par** $*$.

Alors la restriction de $*$ à $A \times A$ est une lci de A.

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x * y \end{aligned}$$

On dit qu'elle est induite par la loi $*$ de E.

Définition

Soit A une partie de E **stable par** $*$.

Alors la restriction de $*$ à $A \times A$ est une lci de A.

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x * y \end{aligned}$$

On dit qu'elle est induite par la loi $*$ de E.

Remarque

Si $*$ est associative

alors la loi induite $*$ est associative.

Définition

Soit A une partie de E **stable par** $*$.

Alors la restriction de $*$ à $A \times A$ est une lci de A.

$$\begin{aligned} * : A \times A &\longrightarrow A \\ (x, y) &\longmapsto x * y \end{aligned}$$

On dit qu'elle est induite par la loi $*$ de E.

Remarque

Si $*$ est commutative

alors la loi induite $*$ est commutative.

Chapitre B6. Structures algébriques

II. **Groupes**

A. Définition et exemples

B. Sous-groupes

C. Morphismes

D. Noyau et image

Définition

Un groupe $(G, *)$ est un ensemble G muni d'une loi $* : G \times G \to G$ vérifiant les propriétés :

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif ou groupe abélien est un groupe $(G, *)$ tel que :

(v) La loi $*$ est commutative.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(i) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
sont des groupes abéliens, d'élément neutre 0.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(i) $(\mathcal{M}_{np}(\mathbb{K}), +)$ est un groupe abélien.
Son élément neutre est 0_{np}.

Remarque

Si la loi de G est $+$ alors on dit que G est un groupe additif.

Remarque

Si la loi de G est $+$ alors on dit que G est un groupe additif.

Les groupes additifs sont toujours commutatifs,
leur élément neutre est noté 0_G,
le symétrique est appelé opposé et noté $-x$,
les itérés sont notés nx avec $n \in \mathbb{Z}$.

Remarque

Si la loi de G est $+$ alors on dit que G est un groupe additif.

Les groupes additifs sont toujours commutatifs,
leur élément neutre est noté 0_G,
le symétrique est appelé opposé et noté $-x$,
les itérés sont notés nx avec $n \in \mathbb{Z}$.

Par exemple $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^2$, $\mathcal{M}_{np}(\mathbb{K})$ sont des groupes additifs.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(ii) $(\mathbb{N}, +)$

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(ii) $(\mathbb{N}, +)$ n'est pas un groupe.
Tout élément n'admet pas d'opposé.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(iii) $(\mathbb{Z}, -)$

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(iii) $(\mathbb{Z}, -)$ n'est pas un groupe.
Sa lci n'est pas associative.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(iv) $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(iv) $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ sont des groupes abéliens. Leur élément neutre est 1.

Remarque

Si la loi de G est $\times$ alors on dit que G est un groupe multiplicatif.

Remarque

Si la loi de G est $\times$ alors on dit que G est un groupe multiplicatif.

Le symétrique est appelé inverse.

Remarque

Si la loi de G est $\times$ alors on dit que G est un groupe multiplicatif.

Le symétrique est appelé inverse.

Par exemple $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{R}_+^*$ et $\mathbb{U}$ sont des groupes multiplicatifs.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(v) $(\mathbb{Z}^*, \times)$

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(v) $(\mathbb{Z}^*, \times)$ n'est pas un groupe.
2 n'a pas d'inverse.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Un groupe commutatif est un groupe tel que :

(v) La loi $*$ est commutative.

Exemples

(vi) Soit $G = \{\pm 1\}$.
Alors $(G, \times)$ est un groupe.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Exemples

(vii) $S_X = \mathcal{B}(X) = \{\text{bijections } X \to X\}$
$(S_X, \circ)$ est un groupe, d'élément neutre Id_X.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Exemples

(vii) $S_X = \mathcal{B}(X) = \{\text{bijections } X \to X\}$
$(S_X, \circ)$ est un groupe, d'élément neutre Id_X.
Il n'est pas commutatif dès que X contient au moins trois éléments.

Définition : Groupe

(i) La loi $*$ est une lci de G.

(ii) La loi $*$ est associative.

(iii) G contient un élément neutre pour $*$.

(iv) Tout élément de G possède un symétrique.

Exemple 2

Description de $(S_X, \circ)$ si $X = \{1, 2\}$.

Proposition

Dans un groupe tout élément est régulier, *i.e.*, simplifiable à gauche et à droite :

$$\forall (x,y,z) \in G^3 \qquad \begin{aligned} x*y = x*z &\implies y = z \\ y*x = z*x &\implies y = z \end{aligned}$$

Proposition

Dans un groupe tout élément est régulier, *i.e.*, simplifiable à gauche et à droite :

$$\forall (x,y,z) \in G^3 \qquad \begin{aligned} x*y = x*z &\implies y = z \\ y*x = z*x &\implies y = z \end{aligned}$$

Démonstration.

- Tout élément x de G admet un inverse x^{-1}.
- La multiplication est associative.

Proposition

Dans un groupe tout élément est régulier, *i.e.*, simplifiable à gauche et à droite :

$$\forall (x,y,z) \in G^3 \qquad \begin{aligned} x*y = x*z &\implies y = z \\ y*x = z*x &\implies y = z \end{aligned}$$

Démonstration.

- Tout élément x de G admet un inverse x^{-1}.
- La multiplication est associative. □

II. **Groupes**

A. Définition et exemples

B. Sous-groupes

C. Morphismes

D. Noyau et image

Définition

Soit $(G, *)$ un groupe et H un ensemble.
H est un sous-groupe de G si :

(i) H est inclus dans G : $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$:

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

(iv) H est stable par passage au symétrique :

$$\forall x \in H \qquad x^{-1} \in H$$

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(i) Si $(G, *)$ est un groupe, alors $\{e\}$ et G sont des sous-groupes de $(G, *)$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(ii) $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$,
qui est un sous-groupe de $(\mathbb{R}, +)$,
qui est un sous-groupe de $(\mathbb{C}, +)$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(iii) $(\{\pm 1\}, \times)$ est un sous-groupe de $(\mathbb{Q}^*, \times)$,
qui est un sous-groupe de $(\mathbb{R}^*, \times)$,
qui est un sous-groupe de $(\mathbb{C}^*, \times)$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(iv) $\mathbb{R}_+^*$ est un sous-groupe de $(\mathbb{R}^*, \times)$,
mais $\mathbb{R}_-^*$ n'en est pas un.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(v) L'ensemble $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Exemples

(vi) $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$, $\mathcal{S}_n(\mathbb{K})$, $\mathcal{A}_n(\mathbb{K})$ sont des sous-groupes de $(\mathcal{M}_n(\mathbb{K}), +)$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Proposition

Soit H un sous-groupe de $(G, *)$.
Alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Démonstration. $(H, *)$ **est un groupe.**

(i) La loi induite est une lci car H stable par $*$.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Démonstration. $(H, *)$ **est un groupe.**

(i) La loi induite est une lci car H stable par $*$.

(ii) Elle est associative car la loi $*$ de G l'est.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Démonstration. $(H, *)$ **est un groupe.**

(i) La loi induite est une lci car H stable par $*$.

(ii) Elle est associative car la loi $*$ de G l'est.

(iii) H contient l'élément neutre e de G.

Définition

H est un sous-groupe de $(G, *)$ si :

(i) $H \subseteq G$

(ii) H est non-vide.

(iii) H est stable par $*$.

(iv) H est stable par passage au symétrique.

Démonstration. $(H, *)$ **est un groupe.**

(ii) Elle est associative car la loi $*$ de G l'est.

(iii) H contient l'élément neutre e de G.

(iv) Tout élément de H admet un inverse. □

Proposition

Soit H un sous-groupe de $(G, *)$.
Alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.

Remarque

Pour vérifier qu'un couple $(G, *)$ est un groupe, il est souvent plus rapide de démontrer que c'est un sous-groupe d'un groupe plus gros $(G', *)$.

Proposition

Soit H un sous-groupe de $(G, *)$.
Alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.

Remarque

Pour vérifier qu'un couple $(G, *)$ est un groupe, il est souvent plus rapide de démontrer que c'est un sous-groupe d'un groupe plus gros $(G', *)$.

Pour démontrer qu'il est non-vide on montre qu'il contient l'élément neutre.

Proposition

Soit H un sous-groupe de $(G, *)$.
Alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.

▷ Exercice 3.

Démontrer que l'ensemble $\mathbb{U}$ muni de la multiplication est un groupe.
Démontrer que pour tout $n \in \mathbb{N}^*$ l'ensemble $\mathbb{U}_n$ muni de la multiplication est un groupe.

Proposition

Soit H un sous-groupe de $(G, *)$.
Alors $(H, *)$ est un groupe, où $*$ est la loi de composition de H induite par $*$.

▷ Exercice 4.

Soit $(\mathcal{B}(\mathbb{R}), \circ)$ le groupe des bijections de $\mathbb{R}$.
Démontrer que l'ensemble Aff des applications affines $x \mapsto ax + b$ avec $a \neq 0$ est un sous-groupe de $\mathcal{B}(\mathbb{R})$.
Est-il commutatif ?

II. Groupes

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Définitions

(i) Un morphisme est aussi appelé homomorphisme.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Définitions

(ii) Un morphisme de $(E, *)$ dans lui-même est appelé endomorphisme.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Définitions

(ii) Un morphisme de $(E, *)$ dans lui-même est appelé endomorphisme.

(iii) Un morphisme bijectif est appelé isomorphisme.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Définitions

(ii) Un morphisme de $(E, *)$ dans lui-même est appelé endomorphisme.

(iii) Un morphisme bijectif est appelé isomorphisme.

(iv) Un endomorphisme bijectif est appelé automorphisme.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(i) $$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto e^x \end{aligned}$$

est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}, \times)$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(ii) $$\begin{array}{rcl} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln x \end{array}$$

est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(ii) $$\begin{array}{rcl} \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln x \end{array}$$

est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

C'est un isomorphisme.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(iii) $$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto ax \end{aligned}$$

est un endomorphisme de $(\mathbb{R}, +)$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(iii) $$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto ax \end{aligned}$$

est un endomorphisme de $(\mathbb{R}, +)$.

C'est un automorphisme ssi $a \neq 0$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(iv) $$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto nx \end{aligned}$$

est un endomorphisme de $(\mathbb{Z}, +)$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(iv) $$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto nx \end{aligned}$$

est un endomorphisme de $(\mathbb{Z}, +)$.

C'est un automorphisme ssi $n = \pm 1$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(v) $$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{R} \\ n &\longmapsto x^n \end{aligned}$$

est un morphisme de $(\mathbb{N}, +)$ dans $(\mathbb{R}, \times)$.

Définition

Un morphisme de $(E, *)$ dans $(E', *')$ est une application $f : E \to E'$ compatible avec les lci :

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

Exemple 3

(vi) $$\begin{aligned} \mathrm{Id}_E : E &\longrightarrow E \\ x &\longmapsto x \end{aligned}$$

est un automorphisme de $(E, *)$.

Proposition

La composée de deux morphismes est un morphisme.

Proposition

La composée de deux morphismes est un morphisme.

Démonstration.

Soit $f : (E, *) \to (E', *')$

et $g : (E', *') \to (E'', *'')$ deux morphismes.

Alors :

Proposition

La composée de deux morphismes est un morphisme.

Démonstration.

Soit $f : (E, *) \to (E', *')$

et $g : (E', *') \to (E'', *'')$ deux morphismes.

Alors :

□

Proposition

La réciproque d'un isomorphisme est un isomorphisme.

Proposition

La réciproque d'un isomorphisme est un isomorphisme.

Démonstration.

Proposition

La réciproque d'un isomorphisme
est un isomorphisme.

Démonstration.

□

Remarque

Dans toute la suite on note :

- $(G, *)$ et $(G', *')$ deux groupes,
- e, e' leurs éléments neutres respectifs.

Définition

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

Définition

Un morphisme de groupes est une application $f : G \to G'$ telle que :

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Définition

Un morphisme de groupes est une application $f : G \to G'$ telle que :

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Remarque

On conserve également les définitions de :

- isomorphisme de groupes,
- endomorphisme de groupes,
- automorphisme de groupes.

Définition

Un morphisme de groupes est une application $f : G \to G'$ telle que :

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Exemple 4

(i) $$\begin{aligned} \mathbb{R}_+^* &\longrightarrow \mathbb{R} \\ x &\longmapsto \ln x \end{aligned}$$

morphisme de groupes de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

Définition

Un morphisme de groupes est une application $f : G \to G'$ telle que :

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Exemple 4

(ii) $$\begin{aligned} \mathbb{R} &\longrightarrow \mathbb{C}^* \\ \theta &\longmapsto e^{i\theta} \end{aligned}$$

morphisme de groupes de $(\mathbb{R}, +)$ dans $(\mathbb{C}^*, \times)$.

Définition

Morphisme de groupes : $f : G \to G'$ telle que

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Proposition

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

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

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

(iii) $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = (f(x))^n$

Définition

Morphisme de groupes : $f : G \to G'$ telle que

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Proposition

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

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

Démonstration.

(i)

Définition

Morphisme de groupes : $f : G \to G'$ telle que

$$\forall (x, y) \in G^2 \qquad f(x * y) = f(x) *' f(y)$$

Proposition

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

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

Démonstration.

(i)

(ii)

Proposition

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

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

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

(iii) $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = (f(x))^n$

Démonstration.

(iii) Par récurrence tout $n \in \mathbb{N}^*$

Pour $n = 0$ grâce au *(i)*,

Pour tout $n \in \mathbb{Z}_-$ grâce au *(ii)*. □

Proposition

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

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

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

(iii) $\forall x \in G \quad \forall n \in \mathbb{Z} \quad f(x^n) = (f(x))^n$

Exemple 4

Dans le cas du logarithme :

$$\ln 1 = 0 \quad \text{et} \quad \forall x \in \mathbb{R}_+^* \quad \ln\left(\frac{1}{x}\right) = -\ln x$$

▷ Exercice 5.

a. Justifier que les applications suivantes sont des morphismes de groupes.

$$\begin{aligned} f_1 : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 3n \end{aligned}$$

$$\begin{aligned} f_2 : (\mathbb{Z}, +) &\longrightarrow (\mathbb{C}^*, \times) \\ n &\longmapsto j^n \end{aligned}$$

$$\begin{aligned} f_3 : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z| \end{aligned}$$

II. **Groupes**

A. Définition et exemples

B. Sous-groupes

C. Morphismes

D. Noyau et image

Proposition

Soit $f : G \to G'$ un morphisme de groupes.

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Proposition

Soit $f : G \to G'$ un morphisme de groupes.

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.

Démonstration. Soit H un sous-groupe de G.

(i) $f(H) \subseteq G'$

(ii) $e' \in f(H)$

(iii) $\forall (x', y') \in f(H)^2 \qquad x' *' y' \in f(H)$

(iv) $\forall x' \in f(H) \qquad (x')^{-1} \in f(H)$.

Proposition

Soit $f : G \to G'$ un morphisme de groupes.

- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Démonstration. Soit H' un sous-groupe de G'.

(i) $f^{-1}(H') \subseteq G$.

(ii) $e \in f^{-1}(H')$

(iii) $\forall (x, y) \in f^{-1}(H')^2 \qquad x * y \in f^{-1}(H')$

(iv) $\forall x \in f^{-1}(H') \qquad x^{-1} \in f^{-1}(H')$.

Proposition

Soit $f : G \to G'$ un morphisme de groupes.

- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Démonstration. Soit H' un sous-groupe de G'.

(i) $f^{-1}(H') \subseteq G$.

(ii) $e \in f^{-1}(H')$

(iii) $\forall (x, y) \in f^{-1}(H')^2 \qquad x * y \in f^{-1}(H')$

(iv) $\forall x \in f^{-1}(H') \qquad x^{-1} \in f^{-1}(H')$. □

Proposition

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Exemples

$\{e\}$ sous-groupe de G, G' sous-groupe de G'. Or :

$$f(\{e\}) = \qquad\qquad f^{-1}(G') =$$

Proposition

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Exemples

$\{e\}$ sous-groupe de G, G' sous-groupe de G'. Or :

$$f(\{e\}) = \{e'\} \qquad f^{-1}(G') =$$

Proposition

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Exemples

$\{e\}$ sous-groupe de G, G' sous-groupe de G'. Or :

$$f(\{e\}) = \{e'\} \qquad f^{-1}(G') = G$$

Proposition

- Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G'.
- Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G.

Exemples

$\{e\}$ sous-groupe de G, G' sous-groupe de G'. Or :

$$f(\{e\}) = \{e'\} \qquad f^{-1}(G') = G$$

Ce sont bien des sous-groupes respectivement de G' et de G.

Définitions

$f : G \to G'$ morphisme de groupes.

Image de f :

$$\operatorname{im} f = f(G) = \{ f(x) \mid x \in G \}$$

Noyau de f :

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

Définitions

$f : G \to G'$ morphisme de groupes.

Image de f :

$$\operatorname{im} f = f(G) = \{ f(x) \mid x \in G \}$$

Noyau de f :

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

Proposition

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

Définitions

$$\operatorname{im} f = f(G) = \{ f(x) \mid x \in G \}$$

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

Remarque (Caractérisations)

$\forall x' \in G'$

$$x' \in \operatorname{im} f \iff \exists x \in G \quad f(x) = x'$$

$\forall x \in G$

$$x \in \ker f \iff f(x) = e'$$

Définitions

$$\operatorname{im} f = f(G) = \{ f(x) \mid x \in G \}$$

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

Exemple 4 (suite)

Déterminer le noyau et l'image de :

$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathbb{C}^*, \times) \\ \theta &\longmapsto e^{i\theta} \end{aligned}$$

Théorème

Soit $f : G \to G'$ un morphisme de groupes. Alors :

(i) f est injective ssi $\ker f = \{e\}$.

(ii) f est surjective ssi $\operatorname{im} f = G'$.

Théorème

Soit $f : G \to G'$ un morphisme de groupes. Alors :

(i) f est injective ssi $\ker f = \{e\}$.

(ii) f est surjective ssi $\operatorname{im} f = G'$.

Démonstration.

(ii) f est surjective ssi $f(G) = G'$

Théorème

Soit $f : G \to G'$ un morphisme de groupes. Alors :

(i) f est injective ssi $\ker f = \{e\}$.

(ii) f est surjective ssi $\operatorname{im} f = G'$.

Démonstration.

(ii) f est surjective ssi $f(G) = G'$

(i) f est injective ssi

$$\forall (x, y) \in G^2 \quad f(x) = f(y) \quad \Longrightarrow \quad x = y$$

Théorème

Soit $f : G \to G'$ un morphisme de groupes. Alors :

(i) f est injective ssi $\ker f = \{e\}$.

(ii) f est surjective ssi $\operatorname{im} f = G'$.

Démonstration.

(ii) f est surjective ssi $f(G) = G'$

(i) f est injective ssi

$$\forall (x, y) \in G^2 \quad f(x) = f(y) \quad \Longrightarrow \quad x = y$$

□

▷ Exercice 5. (suite)

$$\begin{aligned} f_1 : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Z}, +) \\ n &\longmapsto 3n \end{aligned}$$

$$\begin{aligned} f_2 : (\mathbb{Z}, +) &\longrightarrow (\mathbb{C}^*, \times) \\ n &\longmapsto j^n \end{aligned}$$

$$\begin{aligned} f_3 : (\mathbb{C}^*, \times) &\longrightarrow (\mathbb{R}^*, \times) \\ z &\longmapsto |z| \end{aligned}$$

b. Déterminer les noyaux et images de ces morphismes.
Lesquels sont injectifs, lesquels sont surjectifs ?

Chapitre B6. Structures algébriques

III. **Anneaux et corps**

Définition

Un anneau $(A, +, \times)$ est un ensemble A muni de deux lcis $+$ et $\times$ telles que :

(i) $(A, +)$ est un groupe abélien.

(ii) La loi $\times$ est associative.

(iii) A possède un élément neutre pour $\times$.

(iv) La loi $\times$ est distributive par rapport à la loi $+$.

Un anneau commutatif est un anneau dans lequel :

(v) La loi $\times$ est commutative.

Remarques

(i) On omet souvent de noter le signe $\times$:

$$xy = x \times y$$

Remarques

(i) On omet souvent de noter le signe $\times$:

$$xy = x \times y$$

(ii) On note 0 ou 0_A l'élément neutre pour $+$.
On l'appelle élément nul de A.

Remarques

(i) On omet souvent de noter le signe $\times$:

$$xy = x \times y$$

(ii) On note 0 ou 0_A l'élément neutre pour $+$.
On l'appelle élément nul de A.

(iii) On note 1 ou 1_A l'élément neutre $\times$.
On l'appelle unité de A.

Remarques

(i) On omet souvent de noter le signe $\times$:

$$xy = x \times y$$

(ii) On note 0 ou 0_A l'élément neutre pour $+$.
On l'appelle élément nul de A.

(iii) On note 1 ou 1_A l'élément neutre $\times$.
On l'appelle unité de A.

(iv) On appelle inverse d'un élément x de A l'inverse de x pour la loi $\times$.

Remarques

(i) On omet souvent de noter le signe $\times$:

$$xy = x \times y$$

(ii) On note 0 ou 0_A l'élément neutre pour $+$.
On l'appelle élément nul de A.

(iii) On note 1 ou 1_A l'élément neutre $\times$.
On l'appelle unité de A.

(iv) On appelle inverse d'un élément x de A l'inverse de x pour la loi $\times$.
L'inverse d'un élément d'un anneau n'existe pas toujours, mais tout élément admet un opposé.

Exemples

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

Tous sont commutatifs.

Exemples

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

Tous sont commutatifs.

On remarque que l'entier 2 n'a pas d'inverse dans $\mathbb{Z}$.

Exemples

(ii) $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, muni des lois :

$$\begin{aligned}(x,y)+(x',y') &= (x+x',y+y')\\ (x,y)\times(x',y') &= (xx',yy')\end{aligned}$$

Exemples

(ii) $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, muni des lois :

$$\begin{aligned}(x,y)+(x',y') &= (x+x',y+y')\\ (x,y)\times(x',y') &= (xx',yy')\end{aligned}$$

Les éléments neutres sont $(0,0)$ et $(1,1)$.
L'opposé de (x,y) est $-(x,y)=(-x,-y)$.

Exemples

(ii) $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, muni des lois :

$$\begin{aligned}(x,y)+(x',y') &= (x+x',y+y')\\ (x,y)\times(x',y') &= (xx',yy')\end{aligned}$$

Les éléments neutres sont $(0,0)$ et $(1,1)$.
L'opposé de (x,y) est $-(x,y)=(-x,-y)$.

(x,y) est inversible ssi x et y sont non-nuls, son inverse est alors $(x,y)^{-1}=(x^{-1},y^{-1})$.

Exemples

(ii) Démonstration de la distributivité :

$$\begin{aligned}
(u+v)w &= [(x,y)+(x',y')](x'',y'') \\
&= (x+x',y+y')(x'',y'') \\
&= ((x+x')x'',(y+y')y'') \\
&= (xx''+x'x'',yy''+y'y'') \\
&= (xx'',yy'')+(x'x'',y'y'') \\
&= (x,y)(x'',y'')+(x',y')(x'',y'') \\
&= uw+vw
\end{aligned}$$

Exemples

(ii) Démonstration de la distributivité :

$$\begin{aligned}
(u+v)w &= [(x,y)+(x',y')](x'',y'') \\
&= (x+x',y+y')(x'',y'') \\
&= ((x+x')x'',(y+y')y'') \\
&= (xx''+x'x'',yy''+y'y'') \\
&= (xx'',yy'')+(x'x'',y'y'') \\
&= (x,y)(x'',y'')+(x',y')(x'',y'') \\
&= uw+vw
\end{aligned}$$

La distributivité dans l'autre sens est aussi valable car la loi $\times$ est commutative.

Exemples

(ii) $(\mathbb{R}^2, +, \times)$ est un anneau commutatif, muni des lois :

$$\begin{aligned}(x,y)+(x',y') &= (x+x',y+y')\\ (x,y)\times(x',y') &= (xx',yy')\end{aligned}$$

Les éléments neutres sont $(0,0)$ et $(1,1)$.
L'opposé de (x,y) est $-(x,y)=(-x,-y)$.

(x,y) est inversible ssi x et y sont non-nuls, son inverse est alors $(x,y)^{-1}=(x^{-1},y^{-1})$.

Exemples

(iii) Soit $A = \mathcal{F}(X, \mathbb{R})$ muni des lois :

$$\forall x \in X \qquad \begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (f \times g)(x) &= f(x)g(x) \end{aligned}$$

Alors $(A, +, \times)$ est un anneau commutatif.

Exemples

(iii) Soit $A = \mathcal{F}(X, \mathbb{R})$ muni des lois :

$$\forall x \in X \qquad \begin{aligned}(f+g)(x) &= f(x) + g(x)\\ (f \times g)(x) &= f(x)g(x)\end{aligned}$$

Alors $(A, +, \times)$ est un anneau commutatif.

L'élément nul est la fonction nulle, l'unité est la fonction constante égale à 1.

Exemples

(iii) Soit $A = \mathcal{F}(X, \mathbb{R})$ muni des lois :

$$\forall x \in X \qquad \begin{aligned}(f+g)(x) &= f(x) + g(x)\\ (f \times g)(x) &= f(x)g(x)\end{aligned}$$

Alors $(A, +, \times)$ est un anneau commutatif.

L'élément nul est la fonction nulle, l'unité est la fonction constante égale à 1.

(iv) L'ensemble $\mathbb{R}^{\mathbb{N}}$ est un anneau.
L'élément nul est la suite nulle, l'unité est la suite constante égale à 1.

Exemples

(v) L'ensemble $\mathcal{M}_n(\mathbb{K})$ est un anneau.
Il n'est pas commutatif.
L'élément nul est la matrice nulle 0_n, l'unité est la matrice identité I_n.

Exemples

(v) L'ensemble $\mathcal{M}_n(\mathbb{K})$ est un anneau.
Il n'est pas commutatif.
L'élément nul est la matrice nulle 0_n, l'unité est la matrice identité I_n.

(vi) L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est un anneau commutatif.

▷ Exercice 6.

Soit $A = \mathcal{F}(\mathbb{R})$.

Pourquoi $(A, +, \circ)$ n'est-il pas un anneau ?

III. **Anneaux et corps**

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

Proposition

Pour tout $x \in A$:

$$0_A \times x = 0_A = x \times 0_A$$

i.e., 0_A est élément absorbant.

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

Proposition

Pour tout $x \in A$:

$$0_A \times x = 0_A = x \times 0_A$$

i.e., 0_A est élément absorbant.

Démonstration.

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

Proposition

Pour tout $x \in A$:

$$0_A \times x = 0_A = x \times 0_A$$

i.e., 0_A est élément absorbant.

Démonstration.

□

Proposition

Pour tout $x \in A$:

$$0_A \times x = 0_A = x \times 0_A$$

i.e., 0_A est élément absorbant.

Remarque

L'implication

$$(x = 0_A \text{ ou } y = 0_A) \quad \Longrightarrow \quad xy = 0_A$$

n'est pas une équivalence.

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x, y) \in A^2$$

$$x \times y = 0_A \quad \Longrightarrow \quad (x = 0_A \quad \text{ou} \quad y = 0_A)$$

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x, y) \in A^2$$

$$x \times y = 0_A \quad \Longrightarrow \quad (x = 0_A \quad \text{ou} \quad y = 0_A)$$

Exemples

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intègres.

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x, y) \in A^2$$

$$x \times y = 0_A \quad \Longrightarrow \quad (x = 0_A \quad \text{ou} \quad y = 0_A)$$

Exemples

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux intègres.

(ii) $(\mathbb{R}^2, +, \times)$ n'est pas intègre.

$$(1, 0) \times (0, 1) = (0, 0)$$

$$(1, 0) \neq (0, 0) \qquad (0, 1) \neq (0, 0)$$

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x, y) \in A^2$$

$$x \times y = 0_A \quad \Longrightarrow \quad (x = 0_A \quad \text{ou} \quad y = 0_A)$$

Exemples

(iii) $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ n'est pas intègre.

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x,y) \in A^2$$
$$x \times y = 0_A \quad \Longrightarrow \quad (x = 0_A \quad \text{ou} \quad y = 0_A)$$

Exemples

(iii) $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ n'est pas intègre.

(iv) $(\mathcal{M}_n(\mathbb{K}), +, \times)$ n'est pas intègre.
Il n'est pas commutatif, et il existe des matrices non-nulles dont le produit est nul.

Définition

Un anneau A est intègre s'il est commutatif et :

$$\forall (x,y) \in A^2 \qquad x \times y = 0_A \implies (x = 0_A \quad \text{ou} \quad y = 0_A)$$

▷ Exercice 7.

Démontrer que dans un anneau intègre A on peut simplifier par un élément non-nul :

Soit $a \in A \setminus \{0_A\}$. Alors :

$$\forall (x,y) \in A^2 \qquad ax = ay \implies x = y$$
$$\text{et} \qquad xa = ya \implies x = y$$

Propositions

$(a, b) \in A^2$ tel que $ab = ba$ (*i.e.*, a et b commutent.)
Alors pour tout $n \in \mathbb{N}$:

(i) (Formule du binôme de Newton)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

(ii) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$

$$= (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k$$

Notation

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

Notation

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

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Démonstration.

(i) A^* est stable par la loi $\times$.
La loi $\times$ de A^* est induite par celle de A.
C'est donc une lci.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Démonstration.

(i) La loi $\times$ est une lci de A^*.

(ii) La loi $\times$ est associative.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Démonstration.

(i) La loi $\times$ est une lci de A^*.

(ii) La loi $\times$ est associative.

(iii) A contient l'élément neutre 1_A pour $\times$.
1_A est inversible donc appartient à A^*.
Ainsi A^* admet un élément neutre pour sa loi $\times$.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Démonstration.

(i) La loi $\times$ est une lci de A^*.

(ii) La loi $\times$ est associative.

(iii) A^* admet un élément neutre pour sa loi $\times$.

(iv) Si $x \in A^*$ alors x est inversible.
x^{-1} est inversible donc appartient à A^*.
Ainsi tout élément de A^* possède un inverse dans A^*.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Démonstration.

(i) La loi $\times$ est une lci de A^*.

(ii) La loi $\times$ est associative.

(iii) A^* admet un élément neutre pour sa loi $\times$.

(iv) Tout élément de A^* possède un inverse.

Tout ceci montre que $(A^*, \times)$ est un groupe. □

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Exemples

(i) Le groupe des inversible de l'anneau $(\mathbb{R}, +, \times)$ est $(\mathbb{R}^*, \times)$.
De même pour $\mathbb{C}$ et $\mathbb{Q}$.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.

Ce groupe est appelé groupe des inversibles de A.

Exemples

(ii) Le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.

Ce groupe est appelé groupe des inversibles de A.

Exemples

(ii) Le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est $(\{\pm 1\}, \times)$.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Exemples

(ii) Le groupe des inversibles de $(\mathbb{Z}, +, \times)$ est $(\{\pm 1\}, \times)$.
Il est incorrect de noter $\mathbb{Z}^*$ pour $\mathbb{Z} \setminus \{0\}$.

Proposition - Définition

Le couple $(A^*, \times)$ est un groupe.
Ce groupe est appelé groupe des inversibles de A.

Exemples

(iii) Le groupe des inversible de $\mathcal{M}_n(\mathbb{K})$ est $\mathrm{GL}_n(\mathbb{K})$, appelé $n^{\text{ème}}$ groupe linéaire de $\mathbb{K}$.

III. **Anneaux et corps**

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Remarque

Si $1_A = 0_A$ alors $A = \{0_A\}$: il s'agit de l'anneau nul. Ce cas est écarté.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Remarques

(i) Un anneau commutatif K non-nul est un corps ssi :

$$K^* = K \setminus \{0\}$$

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Remarques

(ii) Soit $x \in K$. Si x est non-nul alors on note :

$$\frac{1}{x} = x^{-1} \qquad \text{et} \qquad \frac{y}{x} = y \times \frac{1}{x}$$

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Exemples

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Exemples

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(ii) $\mathbb{Z}$ n'est pas un corps.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Exemples

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(ii) $\mathbb{Z}$ n'est pas un corps.
Par exemple 2 n'a pas d'inverse.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Exemples

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(ii) $\mathbb{Z}$ n'est pas un corps.
Par exemple 2 n'a pas d'inverse.

(iii) $\mathbb{R}[X]$ n'est pas un corps.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Exemples

(i) $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps.

(ii) $\mathbb{Z}$ n'est pas un corps.
Par exemple 2 n'a pas d'inverse.

(iii) $\mathbb{R}[X]$ n'est pas un corps.
Par exemple X n'a pas d'inverse.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Proposition

Un corps est intègre.

$$\forall (x, y) \in K^2$$

$$xy = 0 \quad \Longrightarrow \quad x = 0 \quad \text{ou} \quad y = 0$$

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Proposition

Un corps est intègre.

$$\forall (x, y) \in K^2$$

$$xy = 0 \quad \Longrightarrow \quad x = 0 \quad \text{ou} \quad y = 0$$

Démonstration.

Définition

Un corps $(K, +, \times)$ est un anneau commutatif non réduit à 0 dans lequel tout élément non-nul est inversible.

Proposition

Un corps est intègre.

$$\forall (x, y) \in K^2$$

$$xy = 0 \quad \Longrightarrow \quad x = 0 \quad \text{ou} \quad y = 0$$

Démonstration. □

III. **Anneaux et corps**

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Propositions

(i) Si B est un sous-anneau de A alors B est un anneau.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Propositions

(ii) Si B est une partie de A

- contenant 1_A,
- stable par $+$, $\times$, et passage à l'opposé,

alors B est un sous-anneau de A.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Exemples

(i) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Exemples

(i) $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

(ii) $\mathcal{D}_n(\mathbb{K})$, $\mathcal{T}_n(\mathbb{K})$, $\mathcal{T}'_n(\mathbb{K})$ sont des sous-anneaux de $\mathcal{M}_n(\mathbb{K})$.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

Exemples

(iii) $\{0_A\}$ est un sous-groupe de $(A, +)$.
Il est stable par $\times$, mais ce n'est pas un sous-anneau de A, car il ne contient par 1_A.

Définition

B est un sous-anneau de A si :

(i) $(B, +)$ est un sous-groupe de $(A, +)$.

(ii) 1_A appartient à B.

(iii) B est stable par $\times$.

▷ Exercice 8.

Démontrer que le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

III. **Anneaux et corps**

Soit A et A' deux anneaux.

On note de la même façon les additions et les multiplications de A et de A'.

Définition

Un morphisme d'anneaux est une application $f : A \to A'$ vérifiant :

(i) $\forall (a,b) \in A^2 \quad f(a+b) = f(a) + f(b)$

(ii) $\forall (a,b) \in A^2 \quad f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$

Définition

Morphisme d'anneaux : $f : A \to A'$ vérifiant :

(i) $\forall (a,b) \in A^2 \quad f(a+b) = f(a) + f(b)$

(ii) $\forall (a,b) \in A^2 \quad f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$

Remarques

(i) On définit également les isomorphismes, endomorphismes et automorphismes.

Définition

Morphisme d'anneaux : $f : A \to A'$ vérifiant :

(i) $\forall (a,b) \in A^2 \quad f(a+b) = f(a) + f(b)$

(ii) $\forall (a,b) \in A^2 \quad f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$

Remarques

(i) On définit également les isomorphismes, endomorphismes et automorphismes.

(ii) Un morphisme d'anneaux $f : A \to A'$ est un morphisme de groupes de $(A, +)$ dans $(A', +)$.

Définition

Morphisme d'anneaux : $f : A \to A'$ vérifiant :

(i) $\forall (a,b) \in A^2 \quad f(a+b) = f(a) + f(b)$

(ii) $\forall (a,b) \in A^2 \quad f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$

Remarques

(iii) $\ker f = f^{-1}(\{0_{A'}\})$ et $\operatorname{im} f = f(A)$ sont toujours définis.

$\operatorname{im} f$ est un sous-anneau de A', $\ker f$ n'est pas un sous-anneau de A en général.

Définition

Morphisme d'anneaux : $f : A \to A'$ vérifiant :

(i) $\forall (a,b) \in A^2 \quad f(a+b) = f(a) + f(b)$

(ii) $\forall (a,b) \in A^2 \quad f(ab) = f(a)f(b)$

(iii) $f(1_A) = 1_{A'}$

Remarques

(iii) $\ker f = f^{-1}(\{0_{A'}\})$ et $\operatorname{im} f = f(A)$ sont toujours définis.

(iv) On a toujours l'équivalence :

$$f \text{ injectif} \iff \ker f = \{0_A\}$$

Prochain chapitre

Chapitre A8
Limites et continuité