Chapitre
Structures algébriques

I Loi de composition interne

Définition (Loi de composition interne)

On appelle **loi de composition interne** (l.c.i.) $*$ sur un ensemble E toute application $\begin{array}{ccc} E\times E & \to & E \\ (x,y) & \mapsto & x*y \end{array}$.

- $*$ est **associative** si: $\forall (x,y,z)\in E^3,\ (x*y)*z = x*(y*z)$
- $*$ est **commutative** si: $\forall (x,y)\in E^2,\ x*y=y*x$
- e est **élément neutre** pour $*$ si: $\forall x\in E,\ x*e=e*x=x$
- Si $*$ admet un neutre e, on dit que x est **inversible** pour $*$ si: $\exists y\in E \,/\, x*y=y*x=e$.
  y est alors un **inverse** de x.

L'ensemble E muni de $*$ est noté $(E,*)$.

Ensemble	Loi	Commutatif	Associatif	Neutre	Inverse
$\mathbb{N}$	$+$				
$\mathbb{N}$	$\times$				
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	$+$				
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	$\times$				
$\mathbb{Z}^*$					
$\mathbb{Z}^*$					
$\mathcal{P}(E)$	$\cup$				
$\mathcal{P}(E)$	$\cap$				
$\mathcal{F}(E,E)$	$\circ$				
$\mathcal{F}(I,\mathbb{R})$	$+$				
$\mathcal{F}(I,\mathbb{R})$	$\times$				
$\mathbb{R}^{\mathbb{N}}$	$+$				
$\mathbb{R}^{\mathbb{N}}$	$\times$				
$\mathbb{R}^2$	$+$				

Remarques

1) **Notation des lois**. La loi $*$ sera souvent notée $+$, $\times$, $\cdot$. Mais attention, dans ce cas ce ne seront pas forcément l'addition et la multiplication de $\mathbb{R}$.
La notation $+$ est réservée à des lois commutatives.

2) **Notation des neutres**. Lorsque la loi est notée $+$, le neutre est souvent noté 0_E. Lorsque la loi est notée $\times$ ou $\cdot$, le neutre est souvent noté 1_E.

3) **Notation des inverses**. Lorsque la loi est notée $+$, l'inverse de x est souvent noté $-x$ et est appelé l'opposé de x. Lorsque la loi est notée $\times$ ou $\cdot$, le neutre est souvent noté x^{-1}.

4) **Notation Σ et $\prod$**. Dans le cas d'une loi associative, si la loi est notée $+$ (respectivement $\times$), on définit
$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n \qquad \text{(resp. } \prod_{i=1}^{n} x_i = x_1 \times \cdots \times x_n \text{).}$$

✎ Méthode pratique ✎

- **Pour montrer que $*$ est associative.**
Soit $(x, y, z) \in E^3$, $\quad (x * y) * z = \dots\dots\dots = x * (y * z)$.

- **Pour montrer que $*$ est commutative.**
Soit $(x, y) \in E^2$, $\quad x * y = \dots\dots\dots = y * x$.

- **Pour montrer l'existence d'un neutre.** Si $e \in G$ est un candidat.
Soit $x \in E$, $\quad e * x = \dots\dots\dots = x \quad$ et $\quad x * e = \dots\dots\dots = x$.
Il faut les DEUX égalités. La deuxième est assurée si la loi est commutative.
Pour trouver un candidat, on peut résoudre l'équation $x * e = x$ ou procéder à une analyse.

- **Pour montrer l'inversibilité de $x \in E$.**
Pour montrer que x est inversible on trouve un candidat y à être l'inverse (par une analyse puis on prouve) : $x * y = \dots\dots\dots = e$ et $x * y = \dots\dots\dots = e$.
On peut aussi résoudre l'équation $x * y = e$ d'inconnue y.
Il faut les DEUX égalités. La deuxième est assurée si la loi est commutative.

Exercice.

1) Soit $\mathbb{R}^2$ muni de la loi $*$ définie par : $(x, y) * (x', y') = (xx' - yy', xy' + x'y)$.
Montrer que $*$ est bien une lci, commutative, associative, admettant un neutre. Déterminer les couples $(x, y) \in \mathbb{R}^2$ admettant un inverse.

2) Montrer que le produit vectoriel $\wedge$ sur $\overrightarrow{\mathcal{E}}$ est une lci non associative.

3) Soit $\mathbb{Q}$ muni de la loi $*$ définie par : $x * y = \dfrac{x + y}{2}$. Montrer que $*$ est une lci sur $\mathbb{Q}$ non associative.

Théorème (Unicité du neutre et de l'inverse)

Soit $(E, *)$ un ensemble muni d'une lci.

1) Si $(E, *)$ possède un neutre e, alors il est unique.

2) $\boxed{\text{Supposons } * \text{ est associative}}$. Si l'inverse de $x \in E$ existe alors il est unique.

Remarques (Simplification d'une égalité)

Dans $(E, *)$ avec $*$ associative, si x est inversible

- $a * x = b * x$ se simplifie en $a = b$

- $a * x = b$ permet d'isoler $a = b * x^{-1}$

Propriétés (du neutre et de l'inverse)

Soit $(E, *)$ un ensemble muni d'une lci.

1) L'élément neutre est son propre inverse.
2) Si $x \in E$ est inversible alors x^{-1} est inversible avec : $\quad (x^{-1})^{-1} = x$.
3) Supposons $*$ associative. Si $x \in E$, $y \in E$ sont inversibles alors $x * y$ est inversible avec :
$$(x * y)^{-1} = y^{-1} * x^{-1}.$$

Remarques

On retrouve le fait que :

- dans $(\mathbb{R}^*, \cdot)$, si $(x, y) \in (\mathbb{R}^*)^2$, $\qquad (xy)^{-1} = \dfrac{1}{xy} = \dfrac{1}{x}\dfrac{1}{y} = x^{-1}y^{-1} = y^{-1}x^{-1}$.
  Ici le produit est commutatif, on peut donc échanger x^{-1} et y^{-1}.
- dans $(\mathcal{F}(E, E), \circ)$, si f et g sont bijectives, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

II Groupes

II.1 Définitions et premières propriétés

Définition (Groupe)

- Un ensemble $(G, *)$ muni d'une lci $*$ est un **groupe** si:
  (i) $*$ est associative
  (ii) G admet un élément neutre pour $*$
  (iii) tout élément de G admet un inverse
- Si de plus $*$ est commutative, alors G est dit **groupe commutatif**.

Exemples (Groupes de référence)

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathcal{F}(I, \mathbb{R}), +)$ sont des groupes commutatifs.
2) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Q}_+^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{R}_+^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ sont des groupes commutatifs.
3) On note $\mathcal{S}_E$ l'ensemble des bijections de E dans E. Alors $(\mathcal{S}_E, \circ)$ est un groupe non commutatif. Ce groupe est appelé **groupe des permutations de** E.

Exercice. Montrer que l'ensemble des applications affines de $\mathbb{R}$ dans $\mathbb{R}$, $\left\{ \begin{array}{rccc} f_{a,b} : & \mathbb{R} & \rightarrow & \mathbb{R} \\ & x & \mapsto & ax + b \end{array} \; / \; (a, b) \in \mathbb{R}^* \times \mathbb{R} \right\}$ muni de la composition $\circ$ est un groupe non commutatif.

Propriétés (Notations a^n et na)

- Soit $(G, \cdot)$ un groupe (notation multiplicative).
  - Pour $n \in \mathbb{N}^*$, on note
$$a^n = a \cdot a \cdots a \qquad a^{-n} = (a^n)^{-1} \qquad a^0 = e.$$
  - Soient $(a,b) \in G^2$ et $(n,m) \in (\mathbb{Z}^*)^2$,

1) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
2) $a^n = (a^{-n})^{-1} = (a^{-1})^{-n}$
3) $a^{n+m} = a^n \cdot a^m$
4) $(a^n)^m = a^{nm}$

⚠ **Attention** ⚠ La propriété $(a \cdot b)^n = a^n \cdot b^n$ n'est valable que si la loi est commutative.

- Soit $(G, +)$ un groupe (notation additive).
  - Pour $n \in \mathbb{N}^*$, on note
$$na = a + a \cdots + a \qquad \forall n \in \mathbb{N}^*, \quad (-n)a = -(na) \qquad 0a = e.$$
  - Soient $(a,b) \in G^2$ et $(n,m) \in (\mathbb{Z}^*)^2$,

1) $-(a+b) = (-b) + (-a)$
2) $na = -(-na) = (-n)(-a)$
3) $(n+m)a = na + ma$
4) $n(ma) = (nm)a$

⚠ **Attention** ⚠ La propriété $n(a+b) = na+nb$ n'est valable que si la loi est commutative.

II.2 Sous-groupes

Définition (Sous-groupe)

Soit $(G, *)$ un groupe et H une partie de G.
On dit que H est un **sous-groupe** de G si $(H, *)$ est un groupe.

Théorème (Caractérisation des sous-groupes)

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

1) H est une partie de G
2) $H \neq \emptyset$ (ou $e_G \in H$)
3) **Stabilité**
   (i) H est stable par $*$: $\forall (x,y) \in H^2, \quad x * y \in H$.
   (ii) H est stable par l'inverse : $\forall x \in H, \quad x^{-1} \in H$.

Remarque : 3) (i) et (ii) peuvent être remplacées par : $\forall (x,y) \in H^2$, $x * y^{-1} \in H$

Remarques

Souvent, pour montrer qu'un ensemble muni de $*$ est un groupe, on montre qu'il est un sous-groupe d'un groupe de référence. Dans ce cas, on fait l'économie de l'associativité, et on n'a pas à vérifier l'existence du neutre, ni de l'inverse.

✎ Méthode pratique ✎ (Montrer qu'un ensemble est un sous-groupe)

Pour montrer que H est un sous-groupe de $(G, *)$.

1) On montre que $H \subset G$.
2) On montre que $H \neq \emptyset$ en montrant que $e_G \in H$.
3) Stabilité par $*$: soit $(x, y) \in H^2$, ..., alors $x * y \in H$.
4) Stabilité par inverse : soit $x \in H$, ..., alors $x^{-1} \in H$.

Remarque : $e_G \notin H$ donne une preuve immédiate et simple que H n'est pas un sous-groupe de G.

Exemples (Sous-groupes de référence)

1) $(\mathbb{U}, \cdot)$, $(\mathbb{U}_n, \cdot)$ sont des groupes commutatifs.
2) Si $(G, *)$ est un groupe. $(G, *)$ et $(\{e\}, *)$ sont des sous-groupes de E appelés sous-groupes triviaux de E.
3) Pour $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z} = \{na \,/\, a \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$.

Exercice.

1) Montrer que $2\mathbb{Z} + 1$ n'est pas un sous-groupe de Z.
2) Montrer que les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.
3) Montrer que l'intersection de sous-groupes est un sous-groupe. Application : quelle est l'intersection de $4\mathbb{Z}$ et $6\mathbb{Z}$?

II.3 Morphisme de groupes

Définition (Morphisme)

Soient $(G, *)$ et $(G', \top)$ deux groupes.

- L'application $f : (G, *) \longrightarrow (G', \top)$ est un **morphisme de groupes** si

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

- Vocabulaire :
  - ▶ f est un **isomorphisme** si f est un morphisme bijectif
  - ▶ f est un **endomorphisme** si $(G', \top) = (G, *)$
  - ▶ f est un **automorphisme** si f est un endomorphisme bijectif
  - ▶ deux groupes sont dits **isomorphes** s'il existe un isomorphisme du premier groupe vers le deuxième groupe.

☞ **Explication** ☜ Un morphisme de groupes est une façon de relier deux structures de groupes, le morphisme transforme les produits du groupe de départ en produit dans le groupe d'arrivée.

Exemples

1) L'application $\begin{array}{ccc} (\mathbb{R}, +) & \to & (\mathbb{R}_+^*, \cdot) \\ x & \mapsto & \mathrm{e}^x \end{array}$ est un isomorphisme de groupes.

2) L'application $\begin{array}{ccc} (\mathbb{R}_+^*, \cdot) & \to & (\mathbb{R}, +) \\ x & \mapsto & \ln x \end{array}$ est un isomorphisme de groupes.

3) Pour $z \in \mathbb{C}$, l'application $\begin{array}{ccc} (\mathbb{Z}, +) & \to & (\mathbb{C}^*, \cdot) \\ k & \mapsto & z^k \end{array}$ est un morphisme de groupes.

4) L'application module $\begin{array}{ccc} (\mathbb{C}^*, \cdot) & \to & (\mathbb{C}^*, \cdot) \\ z & \mapsto & |z| \end{array}$ est un endomorphisme de groupes.

5) Soient $\mathcal{P}$ un plan affine, $\overrightarrow{\mathcal{P}}$ le plan vectoriel associé et $\overrightarrow{u} \in \overrightarrow{\mathcal{P}}$. L'application $\varphi : \begin{array}{ccc} (\mathcal{P}, +) & \to & (\mathbb{R}, +) \\ \overrightarrow{x} & \mapsto & \overrightarrow{x} \cdot \overrightarrow{u} \end{array}$ est un morphisme de groupes.

Théorème (Transport du neutre, du symétrique)

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

1) **Transport du neutre**. Si e et e' désignent respectivement les neutres de G et G' alors $f(e) = e'$ (transport du neutre).

2) **Transport du symétrique**. Pour tout $x \in G$, $(f(x))^{-1} = f(x^{-1})$ (transport du symétrique).

Exemple On vérifie ces propriétés pour $\begin{array}{ccc} (\mathbb{R}, +) & \to & (\mathbb{R}_+^*, \cdot) \\ x & \mapsto & \mathrm{e}^x \end{array}$: $\mathrm{e}^0 = 1$ et pour tout $x \in \mathbb{R}$, $(\mathrm{e}^x)^{-1} = \mathrm{e}^{-x}$.

Théorème (Composition et réciproque)

1) La composée de deux morphismes de groupes est un morphisme de groupes.

2) La réciproque d'un isomoprhisme de groupes est un isomorphisme de groupes.

Exemple La réciproque de $\ln : (\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +)$ est $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$.

II.4 Noyau et image d'un morphisme

Théorème (Image directe et réciproque d'un sous-groupe)

Soient $f : (G, *) \to (G', \top)$ un morphisme de groupes, H un sous-groupe de G et H' un sous-groupe de G'. Alors :

1) $f(H)$ est un sous-groupe de G'

2) $\overleftarrow{f}(H')$ est un sous-groupe de G.

Comme conséquence de ce résultat, on obtient les définitions suivantes:

Définition (Noyau - Image)

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

- **noyau** de f, noté $\operatorname{Ker} f$ l'ensemble:

$$\operatorname{Ker} f = \{x \in G \;/\; f(x) = e'\} = \overleftarrow{f}\,(\{e'\}).$$

- **image** de f, noté $\operatorname{Im} f$ l'ensemble:

$$\operatorname{Im} f = f(G) = \{y \in G' \;/\; \exists x \in G \;/\; y = f(x)\} = \{f(x) \;/\; x \in G\}.$$

Les ensembles $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont des sous-groupes de G et G' respectivement (comme image directe et image réciproque de sous-groupes triviaux).

✎ **En pratique** ✎ On utilise: $x \in \operatorname{Ker} f \Leftrightarrow f(x) = e'$ $\quad$ $y \in \operatorname{Im} f \Leftrightarrow \exists x \in G \;/\; y = f(x)$.

Exemples

1) $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*)$ alors $\operatorname{Ker}(\exp) = \{0\}$ et $\operatorname{Im}(\exp) = \mathbb{R}_+^*$.

2) Soient $\overrightarrow{u} \in \overrightarrow{\mathcal{P}}$, $\overrightarrow{u} \neq \overrightarrow{0}$ et le morphisme $\varphi : \begin{array}{ccc} \overrightarrow{\mathcal{P}} & \to & \mathbb{R} \\ \overrightarrow{x} & \mapsto & \overrightarrow{u} \cdot \overrightarrow{x} \end{array}$.

   Déterminer $\operatorname{Ker} \varphi$.

3) Déterminer le noyau et l'image de l'endomorphisme module sur $\mathbb{C}^*$.

4) Soit $z \in \mathbb{C}^*$. Déterminer le noyau et l'image du morphisme $k \mapsto z^k$.

5) Soit $n \in \mathbb{N}$. Déterminer le noyau et l'image du morphisme $z \mapsto z^n$.

Théorème (Caractérisation de l'injectivité et de la surjectivité)

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

1) f est injectif $\Longleftrightarrow \operatorname{Ker} f = \{e\}$

2) f est surjectif $\Longleftrightarrow \operatorname{Im} f = G'$

Exemples

1) $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*)$ alors $\operatorname{Ker}(\exp) = \{0\}$ et $\operatorname{Im}(\exp) = \mathbb{R}_+^*$. On retrouve le fait que exp est injective et surjective donc bijective.

2) Soient $\overrightarrow{u} \in \overrightarrow{\mathcal{P}}$, $\overrightarrow{u} \neq \overrightarrow{0}$ et le morphisme $\varphi : \begin{array}{ccc} \overrightarrow{\mathcal{P}} & \to & \mathbb{R} \\ \overrightarrow{x} & \mapsto & \overrightarrow{u} \cdot \overrightarrow{x} \end{array}$.

   Étudier l'injectivité, la surjectivité de φ.

III Anneaux

III.1 Définitions et premières propriétés

Définition (Anneaux)

- Un ensemble A muni de deux lci $+$ et $\times$ est un **anneau** si :

  1) $(A, +)$ est un groupe commutatif de neutre noté 0_A
  2) $\times$ est associative
  3) $\times$ admet élément neutre noté 1_A
  4) $\times$ est **distributive** par rapport à $+$

$$\forall (x,y,z) \in A^3, \quad x \times (y+z) = x \times y + x \times z \qquad (y+z) \times x = y \times x + z \times x.$$

- Si de plus $\times$ est commutative, l'anneau est dit commutatif.

Remarques

1) Pour $x \in A$, l'inverse de x pour la loi $+$ est noté $-x$ et est appelé l'**opposé** de x.
   Si $(x,y) \in A^2$, on note également $x - y = x + (-y)$.
2) Par convention, pour tout $x \in A$, $x^0 = 1_A$.
3) Un élément $x \in A$ n'a pas forcément d'inverse pour la loi $\times$, x^{-1} n'a donc pas toujours de sens.

Exemples (Anneaux de référence)

1) $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
2) $(\mathbb{R}^I, +, \times)$ et $(\mathbb{C}^I, +, \times)$ sont des anneaux commutatifs.
3) $(\mathbb{R}^\mathbb{N}, +, \times)$ et $(\mathbb{C}^\mathbb{N}, +, \times)$ sont des anneaux commutatifs.

Définition (Morphisme d'anneaux)

Soient A et B deux anneaux. L'application $f : A \longrightarrow B$ est un **morphisme d'anneaux** si

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

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

(iii) $f(1_A) = 1_B$.

On définit également les notions d'**isomorphisme**, **endomorphisme**, **automorphisme**.

Remarques (Sur les morphismes)

1) Si f est un morphisme d'anneaux, alors f est un morphisme de groupe pour l'addition. Conséquence :

$$f(0_A) = 0_B \qquad \forall a \in A, \;\; f(-a) = -f(a).$$

Exemple Montrer que la conjugaison $z \mapsto \overline{z}$ est un automorphisme d'anneaux.

III.2 Sous-anneaux

Définition (Sous-anneau)

Soit $(A, +, \times)$ un anneau et B une partie de A.
On dit que B est un **sous-anneau** de A si

1) $1_A \in B$
2) $(B, +\times)$ est un anneau.

Théorème (Caractérisation des sous-anneaux)

Soit $(A, +, \times)$ un anneau. B est un sous-anneau de A si et seulement si :

1) B est une partie de A
2) $1_A \in B$
3) **Stabilité**
   (i) B est stable par $+$: $\quad \forall (b, b') \in B^2, \quad b + b' \in B$.
   (ii) B est stable par opposé : $\quad \forall b \in B, \quad -b \in B$.
   (iii) B est stable par $\times$: $\quad \forall (b, b') \in B^2, \quad bb' \in B$.

   Remarque : 3) (i) et (ii) peuvent être remplacées par : $\quad \forall (b, b') \in B^2,\ b - b' \in B$

Remarques

Souvent, pour montrer qu'un ensemble muni de $+$ et $\times$ est un anneau, on montre qu'il est un sous-anneau d'un anneau de référence.

Exemples

1) L'ensemble $\{a + \mathrm{i}\, b \,/\, (a, b) \in \mathbb{Z}^2\}$ noté $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$, appelé l'anneau des entiers de Gauss.
2) Si $(A, +, \times)$ est un anneau. $(A, +, \times)$ et $(\{1_A, 0_A\}, +, \times\})$ sont des sous-anneaux de A appelés sous-anneaux triviaux de A.
3) L'ensemble $\mathcal{C}(\mathbb{R}, \mathbb{R})$ est un sous-anneau de $(\mathbb{R}^{\mathbb{R}}, +, \times)$.

III.3 Calcul dans les anneaux

Théorème (Règles de calculs)

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

1) $\forall x \in A, \quad 0_A \times x = x \times 0_A = 0_A$
2) $\forall x \in A, \quad (-1_A) \times x = x \times (-1_A) = -x$
3) $\forall (x, y) \in A^2, \quad (-x) \times y = x \times (-y) = -(xy)$ (on note $-xy$) $\quad$ et $\quad (-x)(-y) = xy$
4) $\forall (x, y, z) \in A^3, \quad (x - y) \times z = x \times z - y \times z \quad$ et $\quad z \times (x - y) = z \times x - z \times y$
5) Si $x \in A$ est inversible alors $-x$ est inversible avec : $\quad (-x)^{-1} = -x^{-1}$
6) Si $x \in A$, $y \in A$ sont inversibles alors $x \times y$ est inversible avec : $\quad (x \times y)^{-1} = y^{-1} \times x^{-1}$
7) **Généralisation de la distributivité**.
   $\forall n \in \mathbb{N}^*, \forall x \in A, \forall (x_1, \ldots, x_n) \in A^n, \quad \displaystyle\sum_{i=1}^{n} (x \times x_i) = x \times \sum_{i=1}^{n} x_i$ et $\displaystyle\sum_{i=1}^{n} (x_i \times x) = \left(\sum_{i=1}^{n} x_i\right) \times x$.

⚠ **Attention** ⚠

- $(A, \times)$ n'est pas un groupe car : .....
- Dans un anneau $x \times y = 0_A$ n'implique pas $x = 0_A$ ou $y = 0_A$. Contre-exemple :

Définition (Anneau intègre)

Soit un anneau $(A, +, \times)$ commutatif, non nul.
A est dit **intègre** si :
$$\forall (x, y) \in A^2, \quad x \times y = 0_A \Leftrightarrow x = 0_A \quad \text{ou} \quad y = 0_A.$$

Théorème (Groupe des inversibles d'un anneau)

Soit un anneau $(A, +, \times)$. On note A^* l'ensemble des éléments inversibles de A pour la loi $\times$:
$$A^* = \{x \in A \,/\, \exists x' \in A,\ x \times x' = x' \times x = 1_A\}.$$
L'ensemble $(A^*, \times)$ est un groupe appelé **groupe des inversibles de** A.

Exemples

1) Dans $(\mathbb{R}, +, \times)$ le groupe des inversibles est :
2) Dans $(\mathbb{Z}, +, \times)$ le groupe des inversibles est :
3) Dans $(\mathbb{R}^I, +, \times)$ le groupe des inversibles est :

Théorème (Trois formules)

Soit $(A, +, \times)$ un anneau. Soit $(x, y) \in A^2$ et $n \in \mathbb{N}$.

1) **Formule du binôme de Newton.** $\boxed{\text{Si } x.y = y.x}$, alors
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k . y^{n-k} \qquad \text{(on peut échanger les exposants)}$$

2) **Formule de factorisation de $x^n - y^n$.** $\boxed{\text{Si } x.y = y.x}$ et si $n \geqslant 1$, alors
$$\begin{aligned} x^n - y^n &= (x-y). \sum_{k=0}^{n-1} x^{n-1-k} y^k \qquad \text{(on peut échanger les exposants)} \\ &= (x-y).(x^{n-1} + x^{n-2}.y + \cdots + x.y^{n-2} + y^{n-1}) \end{aligned}$$

3) **Formule de factorisation $1_A - x^n$** Si $n \geqslant 1$,
$$1_A - x^n = (1_A - x). \sum_{k=0}^{n-1} x^k = (1_A - x).(1 + x + x^2 + \cdots + x^{n-1}).$$

IV Corps

Définition (Corps)

Un ensemble K muni de deux lci $+$ et $\cdot$ est un **corps** si

1) $(K, +, \cdot)$ est un anneau commutatif non réduit à $\{0_K\}$
2) tout élément de $K \setminus \{0_K\}$ admet un un inverse pour $\times$

Exemples (Corps de référence)

1) $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des corps.
2) $(\mathbb{Z}, +, \times)$ n'est pas un corps.

Remarques

Soit $(K, +, \times)$ un corps.

- L'ensemble des inversibles est $K^* = K \setminus \{0_K\}$.
- Si $x \times y = 0_K$ alors $x = 0_K$ ou $y = 0_K$ (contrairement à un anneau). On peut donc simplifier l'égalité suivante si $a \neq 0_K$,
$$a \times x = a \times y \Rightarrow x = y.$$