

AL.5 Groupes – Anneaux - Corps

I. Groupes

Définition 1 :

On dit qu'un ensemble non vide G muni d'une l.c.i. $*$ est un **groupe** si :

- la loi $*$ est associative
- G admet un élément neutre pour la loi $*$
- tout élément de G admet un symétrique pour la loi $*$.

Remarque : Un groupe est un monoïde dans lequel tout élément est symétrisable.

Définition 2 :

On qualifie d'**abélien** (ou **commutatif**) tout groupe dont la loi est commutative.

Conventions :

- Dans le cas d'un groupe multiplicatif (G, \cdot) l'élément neutre sera noté 1 (plutôt que e), et le symétrique sera dit inverse : x^{-1} .
- De même, dans le cas d'un groupe additif $(G, +)$ l'élément neutre sera noté 0 , et le symétrique sera dit opposé : $-x$.

Remarques : Soit $(G, *)$ un groupe

- L'existence de l'élément neutre entraîne la non vacuité de G .
- L'élément neutre de G est unique.
- Tout élément de G admet un unique symétrique et est régulier (c-a-d. $x*y = x*z \Rightarrow y = z$).
- L'équation $a*x = b$ (Resp. $x*a = b$) admet dans G la solution unique $a^{-1}*b$ (Resp. $b*a^{-1}$).
- Enfin si G est un groupe additif abélien, on dispose de la règle des signes : $x-(y+z) = x-y-z$.

II. Morphismes de groupes

Définition : Soient $(G, *)$ et (G', \perp) deux groupes et $f : G \rightarrow G'$.

- On appelle **homomorphisme** de groupes, toute application $f : G \rightarrow G'$ telle que :
 $\forall (x, y) \in G^2, f(x * y) = f(x) \perp f(y)$.
- Un homomorphisme de $(G, *)$ dans $(G, *)$ est appelé **endomorphisme**,
- Un homomorphisme bijectif est appelé **isomorphisme**,
- Un endomorphisme bijectif est appelé **automorphisme**.

Proposition : Soit $f : (G, *) \rightarrow (G', \perp)$ un homomorphisme de groupes. Alors :

- $f(e) = e'$ (où e et e' sont respectivement les éléments neutres de G et G').
- $\forall x \in G, f(x^{-1}) = (f(x))^{-1}$.
- $\forall x \in G, \forall n \in \mathbb{Z}, f(x^n) = (f(x))^n$.

III. Sous-groupes

Définition 1 : Soient $(G, *)$ un groupe et $H \subset G$. On dit que H est un **sous-groupe** de G si :

- $\forall (x, y) \in H^2, x * y \in H$ (H stable pour la loi $*$)
- $e \in H$
- $\forall x \in H, x^{-1} \in H$ (x^{-1} symétrique de x).

Remarque : Un sous-groupe est un groupe.

Proposition 1 : Soient $(G, *)$ un groupe et $H \subset G$. Pour que H soit un sous-groupe de $(G, *)$ il faut et il suffit que l'on ait :

- $H \neq \emptyset$
- $\forall (x, y) \in H^2, x * y^{-1} \in H$

Définition 2 : Soit $f : (G, *) \rightarrow (G', \perp)$ un homomorphisme de groupes.

- On appelle **noyau** de f , noté $\text{Ker } f$, l'ensemble défini par :

$$\text{Ker } f = \{x \in G / f(x) = e'\} = f^{-1}(\{e'\}).$$
- On appelle **image** de f , noté $\text{Im } f$, l'ensemble défini par :

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

Proposition 2 : Soit $f : (G, *) \rightarrow (G', \perp)$ un homomorphisme de groupes. Alors :
 $\text{Ker } f$ et $\text{Im } f$ sont respectivement des sous groupes de $(G, *)$ et (G', \perp) .

Proposition 3 : Soit $f : (G, *) \rightarrow (G', \perp)$ un homomorphisme de groupes.

- f injectif $\Leftrightarrow \text{Ker } f = \{e\}$
- f surjectif $\Leftrightarrow \text{Im } f = G'$.

IV. Structure d'anneau

a) Notion d'anneau

Définition : Soit $(A, +, \cdot)$ un ensemble muni de 2 l.c.i. notées $+$ et \cdot .

On dit que $(A, +, \cdot)$ est un **anneau** si :

- $(A, +)$ est un groupe commutatif d'élément neutre 0
- la loi \cdot est associative et possède un élément neutre, noté 1 .
- la loi \cdot est distributive par rapport à la loi $+$

Remarque : si de plus la loi \cdot est commutative on dit que $(A, +, \cdot)$ est un anneau commutatif.

Remarque : on dispose des règles valables dans tout groupe abélien, et des propriétés qui tiennent au caractère associatif de la loi \cdot (possibilité de définir x^n).

b) Sous-anneau

Définition :

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

- B sous-groupe de $(A, +)$
- B stable pour la loi \cdot ($\forall (x, y) \in B^2, x \cdot y \in B$)
- $1_A \in B$

Remarque : Un sous-anneau de $(A, +, \cdot)$ est un anneau pour les lois induites par celles de A .

Proposition : Soit B une partie d'un anneau $(A, +, \cdot)$.

B est un **sous-anneau** de A si et seulement si :

- $\forall (a, b) \in B^2, a - b \in B$
- $a \cdot b \in B$
- $1_A \in B$.

c) Anneau intègre

Définition : Soient $(A, +, \cdot)$ un anneau et $a \in A / a \neq 0_A$. On dit que :

- a est diviseur de zéro à gauche si $\exists b \in A, b \neq 0_A, a \cdot b = 0_A$
- a est diviseur de zéro à droite si $\exists c \in A, c \neq 0_A, c \cdot a = 0_A$
- a est diviseur de zéro si a est diviseur de zéro à droite et à gauche

Définition :

Un anneau est dit **intègre** s'il est commutatif et s'il n'admet pas de diviseurs de zéro.

V. Structure de corps

a) Généralités

Définition :

On appelle corps tout anneau non nul dont tout élément non nul est inversible.

Remarques :

- i) On qualifie de commutatif tout corps dont la multiplication est commutative.
- ii) Un corps ne possède pas de diviseur de zéro.
- iii) Dans un corps K , l'équation $a \cdot x + b = 0$ où $(a, b) \in K^* \times K$ admet une solution unique : $x = -b \cdot a^{-1}$.

Définition : On appelle morphisme de corps (resp. d'anneau) toute application du corps (resp. anneau) $(A, +, \cdot)$ dans le corps (resp. anneau) $(B, +, \cdot)$ tel que :

- $\forall (a, b) \in A^2, f(a + b) = f(a) + f(b)$
- $\forall (a, b) \in A^2, f(a \cdot b) = f(a) \cdot f(b)$
- $f(1_A) = 1_B$

Proposition : Tout morphisme de corps est injectif.

b) Sous-corps

Définition : Soient $(K, +, \cdot)$ un corps et $L \subset K$. On dit que L est **sous-corps** de K si :

- L est un sous-anneau
- $\forall x \in L \setminus \{0\}, x^{-1} \in L$

Remarque : tout sous-corps est un corps.

Proposition : L est un sous-corps de $(K, +, \cdot)$ si et seulement si :

- $\forall (x, y) \in L^2, x - y \in L$
- $\forall (x, y) \in L^2, x \cdot y \in L$
- $1_K \in L$
- $\forall x \in L \setminus \{0\}, x^{-1} \in L$