CHAPITRE 12

STRUCTURES ALGÉBRIQUES

1. Groupes

Définition 1.1

Soit G un ensemble muni d'une loi **interne** notée $*$. On dit que $(G, *)$ est un *groupe* si

(1) $*$ est associative ;

(2) $*$ possède un élément neutre e dans G ;

(3) Tout élément de G possède un symétrique dans G.

Définition 1.2

Soit $(G, *)$ un groupe. On dit que $(G, *)$ est un groupe *commutatif* ou que c'est un groupe *abélien* si $*$ est commutative.

Remarque 1.3

En général, les groupes sont notés *multiplicativement* : on note xy à la place de $x * y$, le neutre est noté 1_G, le symétrique de x est appelé *inverse* et noté x^{-1}.

En revanche, si G est abélien, on utilise plutôt une notation *additive* : la loi est notée $+$, le neutre 0_G, le symétrique de x est appelé *opposé* de x et noté $-x$.

Définition 1.4

Soit $(G, *)$ un groupe d'élément neutre e et $H \subset G$. On dit que H est un *sous-groupe* de G si

(1) $e \in H$;

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

(3) $\forall x \in H,\ x^{-1} \in H$.

Proposition 1.5

Soit H un sous-groupe de $(G, *)$. Alors $(H, *)$ est un groupe.

Proposition 1.6

Soit $(G, *)$ un groupe et $H \subset G$. Alors H est un sous-groupe de $(G, *)$ si et seulement si H est non vide et

$$\forall x, y \in H,\ x * y^{-1} \in H.$$

Définition 1.7

Soient $(G, *)$ et (H, Δ) deux groupes, et $f : G \to H$ une application. On dit que f est un *homomorphisme (ou plus simplement un morphisme) de groupes* si

$$\forall x, y \in G,\ f(x * y) = f(x) \Delta f(y)$$

.

Proposition 1.8

Soient $(G, *)$ et (H, Δ) deux groupes et $f : G \to H$ un morphisme de groupes. On note e le neutre de G et ε celui de H. Alors :

(1) $f(e) = \varepsilon$;

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

Remarque 1.9

Dans la proposition ci-dessus, $f(x)^*$ est le symétrique de $f(x)$ pour la loi Δ, alors que x^* est le symétrique de x pour la loi $*$.

Proposition 1.10

La composée de deux morphismes de groupes est encore un morphisme de groupes.

Définition 1.11

Soit $f : G \to H$ un morphisme de groupes. On dit que f est un

— *endomorphisme* de groupes si $H = G$;

— *isomorphisme* de groupes si f est bijectif ;

— *automorphisme* de groupes si f est à la fois un endomorphisme et un isomorphisme.

Notation 1.12

Soit G un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Proposition 1.13

$(\mathrm{Aut}(G), \circ)$ est un groupe.

Proposition 1.14

Soit $f : G \to H$ un morphisme de groupes, G' un sous-groupe de G et H' un sous-groupe de H. Alors

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

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

Définition 1.15

Soit $f : G \to H$ un morphisme de groupes. On note ε l'élément neutre de H. Le *noyau* de f est

$$\ker(f) = \{x \in G \mid f(x) = \varepsilon\}$$

C'est un sous-groupe de G.

Théorème 1.16

Soit $f : G \to H$ un morphisme de groupes. On note e l'élément neutre de G. Alors f est injective si et seulement si $\ker(f) = \{e\}$.

2. Anneaux

Définition 2.1

Soit A un ensemble muni de deux lois de composition **internes** notées $+$ et $*$. On dit que $(A, +, *)$ est un *anneau* si

(1) $(A, +)$ est un groupe commutatif ;

(2) la loi $*$ vérifie les propriétés suivantes :

  (a) $*$ est associative ;

  (b) $*$ a un élément neutre 1_A dans A ;

(3) (a) $\forall (a, b, c) \in A^3,\ a * (b + c) = (a * b) + (a * c)$;

  (b) $\forall (a, b, c) \in A^3,\ (a + b) * c = (a * c) + (b * c)$.

On dit que A est *commutatif* si $*$ est commutative.

Remarque 2.2

Soit $(A, +, *)$ un anneau. On utilise une notation additive pour $+$, donc le neutre de $+$ est noté 0_A et le symétrique pour $+$ d'un élément x est noté $-x$.

Proposition 2.3

Soit $(A, +, *)$ un anneau. Alors 0_A est *absorbant* :

$$\forall x \in A,\ x * 0_A = 0_A * x = 0_A.$$

Définition 2.4

Soit $(A, +, *)$ un anneau et $x \in A$. On dit que x est un *diviseur de zéro* s'il existe $y \in A \setminus \{0_A\}$ tel que $x * y = 0_A$.

Proposition 2.5

Un diviseur de zéro ne peut pas être inversible.

Définition 2.6

Un anneau est dit *intègre* si

(1) $0_A \neq 1_A$;

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

Définition 2.7

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

(1) B est un sous-groupe de $(A, +)$;

(2) $1_A \in B$;

(3) $\forall x, y \in B,\ x * y \in B$.

Proposition 2.8

Soit $(A, +, *)$ un anneau et B un sous-anneau de A. Alors $(B, +, *)$ est un anneau.

Proposition 2.9

Soient $(A, +, *)$ et $(B, +, *)$ deux anneaux, et $f : A \to B$ une application. On dit que f est un *homomorphisme (ou plus simplement un morphisme) d'anneaux* si

(1) $\forall x, y \in A,\ f(x + y) = f(x) + f(y)$;

(2) $\forall x, y \in A,\ f(x * y) = f(x) * f(y)$;

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

Remarque 2.10

Dans la définition précédente, on a noté de la même façon les lois de A et de B mais il n'y a aucune raison que ce soient les mêmes !

Proposition 2.11

L'image directe ou réciproque d'un sous-anneau par un morphisme d'anneaux est pas un sous-anneau.

Définition 2.12

Soit $f : A \to B$ un morphisme d'anneaux. Le *noyau* de f est

$$\ker(f) = \{x \in A \mid f(x) = 0_B\}.$$

Remarque 2.13

Le noyau d'un morphisme d'anneaux n'est pas un sous-anneau en général.

3. Corps

Définition 3.1

Soit $\mathbb{K}$ un ensemble muni de deux lois de composition **internes**. On dit que $(\mathbb{K}, +, *)$ est un *corps* si

(1) $(\mathbb{K}, +, *)$ est un anneau commutatif ;

(2) $0_{\mathbb{K}} \neq 1_{\mathbb{K}}$;

(3) tout élément non nul de $\mathbb{K}$ possède un inverse dans $\mathbb{K}$.

Remarque 3.2

Soit $(\mathbb{K}, +, *)$ un corps. Alors $(\mathbb{K}, +)$ et $(\mathbb{K} \setminus \{0_A\}, *)$ sont des groupes abéliens.

Remarque 3.3

On peut trouver dans certains ouvrages une définition différente de la notion de corps : ils peuvent ne pas être commutatifs.

Définition 3.4

Soit $(\mathbb{K}, +, *)$ un corps et $\mathbb{L} \subset \mathbb{K}$. On dit que $\mathbb{L}$ est un *sous-corps* de $\mathbb{K}$ si

(1) $\forall x, y \in \mathbb{L},\ x - y \in \mathbb{L}$;

(2) $\forall x, y \in \mathbb{L} \setminus \{0_{\mathbb{K}}\},\ x * y^{-1} \in \mathbb{L}$.

Proposition 3.5

Soit $\mathbb{L}$ un sous-corps de $(\mathbb{K}, +, *)$. Alors $(\mathbb{L}, +, *)$ est un corps.

Définition 3.6

Soient $(\mathbb{K}, +, *)$ et $(\mathbb{L}, +, *)$ deux corps, et $F : \mathbb{K} \to \mathbb{L}$ une application. On dit que f est un *homomorphisme (ou plus simplement un morphisme) de corps* si

(1) $\forall x, y \in \mathbb{K},\ f(x + y) = f(x) + f(y)$;

(2) $\forall x, y \in \mathbb{K},\ f(x * y) = f(x) * f(y)$.

Remarque 3.7

Un morphisme de corps est aussi un morphisme d'anneaux.

Proposition 3.8

Un morphisme de corps est toujours injectif.