Fiche : Structures Algébriques

1 Monoïdes

Définition 1.1. (L.C.I)

Soit E un ensemble.
On appelle **loi de composition interne** une application $*$ de $E \times E$ dans E.

Définition 1.2. (Magma)

Un ensemble muni d'une *loi de composition interne* est appelé un **magma**.

Définition 1.3. (Associativité)

Soit $(E, *)$ un magma.
On dit que $*$ est **associative** lorsque :

$$\forall a, b, c \in E, (a * b) * c = a * (b * c)$$

Définition 1.4. (Elément neutre)

Soit $(E, *)$ un magma.
On dit qu'un élément e de E est **neutre** lorsque :

$$\forall a \in E, a * e = e * a = a$$

Si le neutre existe, il est unique.

Définition 1.5. (Monoïde)

Un magma dont la loi est associative et qui possède un élément neutre est appelé un **monoïde**.

Définition 1.6 (Itéré)

Soit $(E, *)$ un monoïde. Soit n un entier naturel.
On appelle **n-ième itéré** d'un élément a de E l'élément de E défini par :

$a^0 = 1_E$ et $a^n = a * \cdots * a$ (Si la loi est notée multiplicativement)

$0a = 0_E$ et $na = a + \cdots + a$ (Si la loi est noté additivement)

Définition 1.7. (Symétrisabilité)

Soit $(E, *)$ un monoïde.
Un élément a de E est dit **symétrisable** lorsqu'il existe $a^{-1} \in E$ tel que :

$$a * a^{-1} = a^{-1} * a = e$$

Si a^{-1} existe, il est unique.

Définition 1.8. (Elément simplifiable)

Soit $(E, *)$ un monoïde.
Un élément a de E est dit **symplifiable ou régulier** lorsque :

$$\forall x, y \in E, (a * x = a * y) \Rightarrow (x = y)$$

et,

$$\forall x, y \in E, (x * a = y * a) \Rightarrow (x = y)$$

Définition 1.9. (Commutativité)

Soit $(E, *)$ un monoïde.
On dit que deux éléments a et b de E **commutent** lorsque :

$$a * b = b * a$$

On dit que $*$ est **commutative** lorsque tous les éléments de E commutent.

Définition 1.9. (Distributivité)

Soit E un ensemble muni de deux lois $*$ et $\bullet$.
On dit que $*$ est **distributive** sur $\bullet$ lorsque :

$$\forall a, b, c \in E, a * (b \bullet c) = (a * b) \bullet (a * c)$$

et,

$$\forall a, b, c \in E, (b \bullet c) * a = (b * a) \bullet (c * a)$$

Définition 1.10. (Loi induite)

Soit $(E, *)$ un monoïde et F une partie de E.
Si F est stable pour $*$ c'est à dire si :

$$\forall a, b \in F, a * b \in F$$

on obtient sur F une L.C.I dite **loi induite** qui fait de $(F, *)$ un magma.

Définition 1.11. (Sous-monoïde)

Soit $(E, *)$ un monoïde et F une partie de E telle que $(F, *)$ est un magma.
Si $e \in F$ alors $(F, *)$ est un monoïde. On dit que c'est un **sous-monoïde** de E.

Proposition 1.1. (Caractérisation des sous-monoïdes)

$F \subset E$ est un sous-monoïde de E si, et seulement si, on a :

(a) $e \in F$

(b) $\forall a, b \in F, a * b \in F$

Remarque. On peut construire d'autres lois que la loi induite (*Cf. Cours*). Parmi elles :
— La loi produit
— Loi fonctionnelle
— Loi ensembliste

2 Groupes

Définition 2.1. (Groupe)

Un **groupe** $(G, *)$ est un monoïde dans lequel tout élément est symétrisable, c'est à dire que :

(a) G est stable par $*$

(b) $*$ est associative

(c) $*$ admet un élément neutre e

(d) $\forall g \in G, \exists! g^{-1} \in G, g * g^{-1} = g^{-1} * g = e$

Lorsque $*$ est commutative, on dit que $(G, *)$ est un **groupe abélien**.

Définition 2.2. (Sous-groupe)

Soit $(G, *)$ un groupe.
Soit H une partie de G qui est stable par la loi $*$.
On dit que H est un **sous-groupe** de G lorsque $(H, *)$ est un groupe.

Proposition 2.1. (Caractérisation des sous-groupes)

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

(a) $H \subset G$

(b) $e_G \in H$

(c) $\forall h_1, h_2 \in H, h_1 * h_2 \in H$

(d) $\forall h \in H, h^{-1} \in H$

De plus, (a) et (b) sont équivalentes à la *stabilité par produit twisté* :

(e) $\forall h_1, h_2 \in H, h_1 * {h_2}^{-1} \in H$

Définition 2.3. (Morphisme de groupes)

Soient $(G, *)$ et $(G', \bullet)$ deux groupes.
On appelle **morphisme de groupes** de G vers G' une application $\varphi : G \to G'$ telle que :

$$\forall g_1, g_2 \in G, \varphi(g_1 * g_2) = \varphi(g_1) \bullet \varphi(g_2)$$

i.e telle que l'image d'un produit est le produit des images.

Vocabulaire.

(a) Un morphisme de groupes de G vers lui-même est appelé un **endomorphisme** de G.

(b) Un morphisme de groupes qui est bijectif est appelé un **isomorphisme**.

(c) Un morphisme de groupes qui est bijectif d'un groupe G dans lui-même est appelé un **automorphisme** de G.

(d) L'ensemble des automorphisme de G est noté $Aut(G)$.

Définition 2.4. (Noyau et Image d'un morphisme de groupes)

Soient $(G, *)$ et $(G', \bullet)$ deux groupes.
Soit $\varphi : G \to G'$ un morphisme.

(a) On appelle **noyau** de φ noté $Ker(\varphi)$ le sous-groupe de G défini par :

$$Ker(\varphi) = \varphi^{-1}(\{e_{G'}\}) = \{g \in G | \varphi(g) = e_{G'}\}$$

(b) On appelle **image** de φ noté $Im(\varphi)$ le sous-groupe de G' défini par :

$$Im(\varphi) = \varphi(G) = \{g' \in G' | \exists g \in G, g' = \varphi(g)\}$$

3 Anneaux

Définition 3.1. (Anneau)

Un **anneau** $(A, +, \times)$ est un ensemble A muni de deux L.C.I notées $+$ et $\times$ telles que :

(a) $(A, +)$ est un groupe abélien dont l'élément neutre est noté 0_A

(b) $(A, \times)$ est un monoïde dont l'élément neutre est noté 1_A

(c) $\times$ est distributive sur $+$

Lorsque $\times$ est commutative, on dit que $(A, +, \times)$ est un **anneau commutatif**.

Définition 3.2. (Diviseurs de zéro, nilpotence)

Soit $(A, +, \times)$ un anneau.
On dit que $a \in A$ est un **diviseur de zéro** lorsque $a \neq 0_A$ et il existe $b \in A^*$ tel que :

$$ab = 0_A \text{ ou } ba = 0_A$$

Si a est un diviseur de zéro, il est possible qu'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0_A$. On dit alors que a est **nilpotent**.

Définition 3.3. (Intégrité)

Soit $(A, +, \times)$ un anneau.
On dit que A est **intègre** lorsque A ne possède pas de diviseurs de zéro, c'est à dire que :

$$\forall a, b \in A, (ab = 0_A) \Rightarrow (a = 0_A \text{ ou } b = 0_A)$$

Notation. On note $U(A)$ l'ensemble des éléments inversibles de A, i.e :

$$U(A) = \{a \in A | a^{-1} \text{ existe}\}$$

Définition 3.4. (Sous-anneau)

On dit que B est un **sous-anneau** de $(A, +, \times)$ lorsque :

(a) $B \subset A$

(b) B est stable par $+$ et $\times$

(c) $(B, +, \times)$ est un anneau

(d) $1_A \in B$

Proposition 3.1. (Caractérisation des sous-anneaux)

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

(a) $B \subset A$

(b) $1_A \in B$

(c) $\forall b_1, b_2 \in B, b_1 - b_2 \in B$

(d) $\forall b_1, b_2 \in B, b_1 \times b_2 \in B$

Définition 3.5. (Idéal)

Soit $(A, +, \times)$ un anneau *commutatif*. On dit que I est un **idéal** de A lorsque :

(a) $I \subset A$

(b) $(I, +)$ est un sous-groupe de (A,+)

(c) $\forall i \in I, \forall a \in A, ia \in I$ (Hyperstabilité)

Proposition 3.2. (Caractérisation des idéaux)

I est un idéal de $(A, +, \times)$ si, et seulement si, on a :

(a) $I \subset A$

(b) $0_A \in I$

(c) $\forall i_1, i_2 \in I, i_1 - i_2 \in I$

(d) $\forall i \in I, \forall a \in A, ia \in I$

Définition 3.6. (Morphisme d'anneaux)

On dit que $\varphi : A \to A'$ est un **morphisme d'anneaux** lorsque :

(a) $\forall a_1, a_2 \in A, \varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$

(b) $\forall a_1, a_2 \in A, \varphi(a_1 \times a_2) = \varphi(a_1) \times \varphi(a_2)$

(c) $\varphi(1_A) = 1_{A'}$

Vocabulaire.

(a) Un morphisme d'anneaux de A vers lui-même est appelé un **endomorphisme** de A.

(b) Un morphisme d'anneaux qui est bijectif est appelé un **isomorphisme**.

(c) Un morphisme d'anneaux qui est bijectif d'un anneau A dans lui-même est appelé un **automorphisme** de A.

Définition 3.7. (Noyau et Image d'un morphisme d'anneaux)

Soit $\varphi : A \to A'$ un morphisme d'anneaux.

(a) On a :
$$Ker(\varphi) = \varphi^{-1}(\{0_{A'}\}) = \{a \in A | \varphi(a) = 0_{A'}\}$$

(b) On a :
$$Im(\varphi) = \varphi(A) = \{a' \in A' | \exists a \in A, a' = \varphi(a)\}$$

Remarque. (Structure de $Ker(\varphi)$ et $Im(\varphi)$)

(a) $Ker(\varphi)$ est un idéal de A.

(b) $Im(\varphi)$ est un sous-anneau de A'

4 Corps

Définition 4.1. (Corps)

Un **corps** K est un anneau (différent de l'anneau nul $\{0\}$) dans lequel tous les éléments non-nuls sont inversibles i.e. $U(K) = K^*$.

Définition 4.2. (Sous-corps)

Un **sous-corps** L du corps K est une partie de K qui est stable pour $+$ est $\times$ telle que $(L, +, \times)$ est un corps.

Proposition 4.1. (Caractérisation des sous-corps)

L est un sous-corps de K si, et seulement si :

(a) $L \subset K$

(b) $1_K \in L$

(c) $\forall x, y \in L, x - y \in L$

(d) $\forall x \in L, \forall y \in L^*, xy^{-1} \in L$

Définition 4.3. (Morphisme de corps)

Un **morphisme de corps** est un morphisme d'anneaux entre deux anneaux qui sont des corps. Tout ce qui a été vu dans le contexte des anneaux se généralise au contexte des corps.