RAMM ALGEBRA CENTER

L3 Mathématiques

Mathématiques : THEORIE DES CORPS

Elisabeth REMM- Michel GOZE

Chapitre 1

Généralités sur les corps : Résumé

1. Définition d'un corps

1.1. **Définition.**

Définition 1. *Un corps $\mathbb{K}$ est un ensemble non vide muni de deux lois de composition (deux opérations), notées $+$ et $\times$ vérifiant les conditions suivantes :*

(1) La loi de composition $+$ vérifie :

(a) Elle est associative $(x+y)+z = x+(y+z)$, $\forall x, y, z \in \mathbb{K}$,

(b) Elle est commutative : $X + y = y + x$, $\forall x, y \in \mathbb{K}$,

(c) $\mathbb{K}$ possède un élément neutre 0 : $x + 0 = x$, $\forall x \in \mathbb{K}$,

(d) Tout élément x de $\mathbb{K}$ possède un symétrique $(-x)$ par rapport à 0 : $x+(-x) = 0$, $\forall x \in \mathbb{K}$.

(2) La loi de composition $\times$ vérifie :

(a) Elle est associative $(x \times y) \times z = x \times (y \times z)$, $\forall x, y, z \in \mathbb{K}$,

(b) Elle est distributive par rapport à la loi $+$: $x \times (y + z) = x \times y + x \times z$, $\forall x, y, z \in \mathbb{K}$,

(c) $\mathbb{K}$ possède un élément neutre e pour $\times$: $x \times e = e \times x = x$, $\forall x \in \mathbb{K}$,

(d) Tout élément $x \neq 0$ de $\mathbb{K}$ possède un inverse (x^{-1}) par rapport à e : $x \times (x^{-1}) = (x^{-1}) \times x = e$, $\forall x \in \mathbb{K}$.

Exemples de corps

(1) L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$ sont des corps commutatifs.

(2) Le corps des Quaternions défini comme l'ensemble $\mathbb{H}$ des matrices complexes de la forme

$$\begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix}$$

(3) Le corps des fractions d'un anneau intègre. C'est comme cela que l'on construit $\mathbb{Q}$ comme le corps des fractions de l'anneau $\mathbb{Z}$.

(4) Soit A un anneau commutatif unitaire et $\mathfrak{m}$ un idéal maximal de A. Alors l'anneau quotient $A/\mathfrak{m}$ est un corps.

(5) Soit $P \in \mathbb{K}[X]$ un polynôme à coefficients dans $\mathbb{K}$ à une indéterminée X. Si ce polynôme est irréductiblle, alors l'idéal (P) de l'anneau $\mathbb{K}[X]$ engendré par P est maximal et l'anneau quotient $\mathbb{K}[X]/(P)$ est un corps, appelé le corps de rupture de P. Ce corps jouera un rôle important dans la suite.

1.2. **Sous-corps. Sous-corps premier.**

Définition 2. *On appelle sous-corps d'un corps $\mathbb{K}$ un sous-ensemble de $\mathbb{K}$ qui est lui même un corps par rapport à l'addition et à la multiplication de $\mathbb{K}$.*

Ainsi un sous-ensemble $\mathbb{L}$ de $\mathbb{K}$ est un sous-corps si $\mathbb{L}$ est un sous-groupe additif de $\mathbb{K}$ (pour l'addition de $\mathbb{K}$) et si $\mathbb{L}^* = \mathbb{L} - \{0\}$ est un sous-groupe multiplicatif de $\mathbb{K}^*$. Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$, on dit que $\mathbb{K}$ est un surcorps de $\mathbb{L}$. Toute intersection de sous-corps du corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$. Notons $\Pi(\mathbb{K})$ l'intersection des sous-corps de $\mathbb{K}$. Il n'admet aucun sous-corps autre que lui même.

Définition 3. *On appelle sous-corps premier du corps $\mathbb{K}$ le sous-corps $\Pi(\mathbb{K})$ obtenu comme l'intersection des sous-corps de $\mathbb{K}$. On dit qu'un corps Π est un corps premier, s'il est le sous-corps premier d'un corps.*

1.3. **Homomorphismes de corps.**

Définition 4. *Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps. Une application $f : \mathbb{K}_1 \to \mathbb{K}_2$ est un homomorphisme de corps si elle vérifie*
(1) f(x+y)=f(x)+f(y) ,
(2) f(xy)=f(x)f(y)
pour tout $x, y \in \mathbb{K}_1$.

Tout homomorphisme de corps non nul est injectif.

2. Caractéristique d'un corps

2.1. **Définition.**

Définition 5. *Soit $\mathbb{K}$ un corps et soit (e) le groupe monogène engendré par l'élément neutre de $\mathbb{K}$ noté e. Alors si le sous-groupe (e) est cyclique d'ordre fini n_e on dit que $\mathbb{K}$ est de caractéristique n_e sinon $\mathbb{K}$ est dit de caractéristique* 0.

Si $\mathbb{K}$ est de caractéristique p, $p \neq 0$, alors

$$pe = 0.$$

Proposition 1. *Soit $\mathbb{K}$ un corps de caractéristique p avec $p \neq 0$. Alors p est un nombre premier.*

Proposition 2. *Tout corps fini $\mathbb{K}$ est de caractéristique p avec $p \neq 0$. Il existe alors un entier q tel que la cardinalité de ce corps fini soit égale à p^q.*

Proposition 3. *Soit $\mathbb{K}$ un corps de caractéristique p, $p \neq 0$. L'application*

$$F : \mathbb{K} \to \mathbb{K}$$

définie par

$$F(x) = x^p$$

est un homomorphisme de corps. Il est appelé l'homomorphisme de Frobenius.