Chapitre IV - Corps finis

Définition

Un corps fini est un corps $(K, 0, +, *, e)$ tel que $\mathrm{card}(K) = q \in \mathbb{N}$.

1. Extensions de corps
2. Structure des corps (commutatifs) finis
3. Les polynômes irréductibles de $\mathbb{F}_p[X]$
4. Théorème de Wedderburn

Précision : On suppose que les corps sont commutatifs. Cette hypothèse est superflue pour les corps finis : le théorème de Wedderburn montre que les corps finis sont commutatifs.

1. Extensions de corps

1. Polynôme minimal d'un élément algébrique
2. Caractéristique et corps premiers
3. Construction d'un corps fini
4. L'endomorphisme de Frobenius

Notation : $\mathbb{P} = \{2; 3; 5; 7; \ldots\}$ désigne l'ensemble des nombres premiers.

1. Polynôme minimal d'un élément algébrique

Soit une extension de corps commutatifs.

$$K \overset{j}{\hookrightarrow} L$$

- L est muni d'une structure de K-espace vectoriel par

$$\begin{array}{rcl} \cdot : K \times L & \longrightarrow & L \\ (a, x) & \longmapsto & a \cdot x \overset{\text{déf}}{=} j(a)x \overset{\text{notation}}{=} ax \end{array}$$

Définition (degré d'une extension finie)

Si L est un K-espace vectoriel de dimension finie $\dim_K(L) < \infty$, on dit que l'extension L/K est finie, de degré $[L : K] = \dim_K(L)$.

- Soit $\alpha \in L$. S'il existe $P \in K[X]$ tel que $P \neq 0$ et $P(\alpha) = 0$ on dit que α est algébrique sur K. Sinon, on dit qu'il est transcendant sur K.

Polynôme minimal d'un élément algébrique (2)

• Soit $\alpha \in L$ algébrique sur K. L'unique morphisme de K-algèbre $\varphi_\alpha : K[X] \to L$ tel que $\varphi_\alpha(X) = \alpha$ se factorise selon :

$$\begin{array}{ccc} K[X] & \xrightarrow{\varphi_\alpha} & L \\ \pi \downarrow & & \uparrow \\ K[X]/\mathrm{Ker}(\varphi_\alpha) & \xrightarrow{\widetilde{\varphi_\alpha}} & \mathrm{Im}(\varphi_\alpha) \end{array}$$

• $\boxed{\mathrm{Ker}(\varphi_\alpha) = \{P \in K[X] : \ P(\alpha) = 0\}}$
est un idéal premier non nul de $K[X]$ (car $\mathrm{Im}(\varphi_\alpha)$ intègre).

Polynôme minimal d'un élément algébrique (3)

• De plus, $\mathrm{Ker}(\varphi_\alpha)$ est principal (car $K[X]$ est principal). Il existe donc un unique polynôme $P_\alpha \in K[X]$, de cœfficient dominant égal à 1, tel que

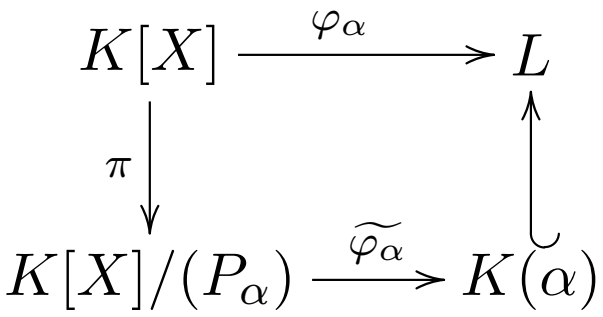
$$\mathrm{Ker}(\varphi_\alpha) = (P_\alpha)$$

Définition (polynôme minimal d'un élément algébrique)

P_α s'appelle le polynôme minimal de α sur K.

• $P_\alpha \in K[X]$ est premier non nul, donc irréductible. Et comme $K[X]$ est principal, (P_α) est un idéal maximal.
• $K[X]/\mathrm{Ker}(\varphi) = K[X]/(P_\alpha)$ est donc un corps, de même que $\mathrm{Im}(\varphi_\alpha)$ qui lui est isomorphe.
• Par ailleurs, $\mathrm{Im}(\varphi_\alpha) = K[\alpha]$, le plus petit sous-anneau de L contenant K et α. Comme c'est un corps, c'est aussi $K(\alpha)$, le plus petit sous-corps de L contenant K et α.

Polynôme minimal d'un élément algébrique (4)



- On a donc une extension $K \hookrightarrow K(\alpha)$.

Comme $K(\alpha)$ est isomorphe à $K[X]/(P_\alpha)$, la famille des α^k pour $k \in [\![0, \deg(P_\alpha) - 1]\!]$ constitue une base du K-espace vectoriel $K(\alpha)$, et donc :

$$[K(\alpha) : K] = \deg(P_\alpha)$$

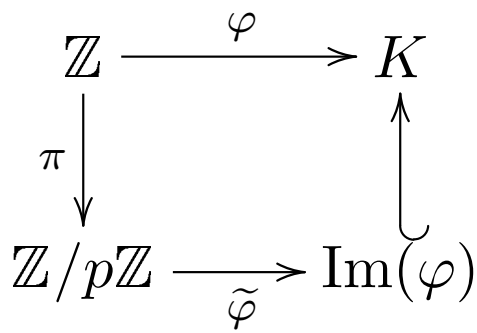
Définition (élément primitif d'une extension)

Soit une extension $K \hookrightarrow L$. On dit que $\alpha \in L$ est primitif sur K si $L = K(\alpha)$.

2. Caractéristique et corps premiers

Soit $(K, 0, +, *, e)$ un corps commutatif.

Rappel :
Il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \to K$ qui se factorise en :



avec $\boxed{\mathrm{car}(K) \overset{\text{déf}}{=} p} \in \{0\} \cup \mathbb{P}$ (car $\mathrm{Im}(\varphi)$ intègre).

Exercices :

1. $\mathrm{card}(K) < \infty \implies \mathrm{car}(K) \in \mathbb{P}$
2. $\mathrm{car}(K) = 0 \implies \mathrm{card}(K) = \infty$
3. $\mathrm{car}(K) \neq 0 \implies \mathrm{Im}(\varphi)$ est le plus petit sous-corps de K.

sous-corps premier et corps premiers

Définitions (sous-corps premier, corps premiers)

1. On appelle sous-corps premier d'un corps K, et on note $\mathrm{SCP}(K)$, le plus petit sous-corps de K : c'est le sous-corps de K engendré par $\{0; e\}$.
2. Les corps premiers sont : $\mathbb{Q}$ et les $\mathbb{F}_p \overset{\text{déf}}{=} \mathbb{Z}/p\mathbb{Z}$ pour $p \in \mathbb{P}$.

Remarque : Les corps premiers sont commutatifs.

Lemme (caractéristique et sous-corps premier)

1. *Un corps premier coïncide avec son sous-corps premier.*
2. *Si* $K \overset{j}{\hookrightarrow} L$ *, alors* K *et* L *ont des sous-corps premiers isomorphes, donc* $car(K) = car(L)$.

caractéristique et cardinal des corps finis

Lemme (caractéristique et sous-corps premier)

Soit un corps K. Son sous-corps premier $SCP(K)$ est isomorphe à un corps premier et :

$$car(K) = 0 \iff SCP(K) \text{ isomorphe à } \mathbb{Q}$$
$$car(K) = p \in \mathbb{P} \iff SCP(K) \text{ isomorphe à } \mathbb{F}_p$$

Théorème (caractéristique et cardinal des corps finis)

Soit K un corps fini de cardinal $card(K) = q$ et de caractéristique $car(K) = p$.

1. *Son sous-corps premier est isomorphe à $\mathbb{F}_p$.*
2. *K est une extension de $\mathbb{F}_p$ de degré $\boxed{[K : \mathbb{F}_p] = n}$ fini, et donc $q = p^n$.*

Exercice : démontrer les lemmes et le théorème ci-dessus.

3. Construction d'un corps fini

Soit $p \in \mathbb{P}$.
$\mathbb{F}_p[X]$ est un anneau principal (car $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps).
Soit, s'il en existe, $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré $\deg(P) = n$.

$$\begin{array}{ccc} & & \mathbb{F}_p[X] \\ & & \Big\downarrow \pi \\ K & \overset{\text{déf}}{=} & \mathbb{F}_p[X]/(P) \end{array}$$

Exercices :

1. $\mathbb{F}_p \hookrightarrow K$ est une extension de degré $[K : \mathbb{F}_p] = \deg(P) = n$.
2. $\mathrm{car}(K) = p$ et $\mathrm{card}(K) = p^n$.
3. Posons $\boxed{\alpha \overset{\text{déf}}{=} \pi(X)} \in K$. Montrer que $P(\alpha) = 0$. Quel est le polynôme minimal de α ?
4. En déduire $K = \mathbb{F}_p(\alpha)$.

4. L'endomorphisme de Frobenius

Soit K un corps (commutatif) de caractéristique $\mathrm{car}(K) = p \in \mathbb{P}$.

$$\begin{array}{rccc} \mathrm{Frob}_K : & K & \longrightarrow & K \\ & a & \longmapsto & a^p \end{array}$$

Proposition (endomorphisme de Frobenius)

$Frob_K$ est un morphisme de corps et de $\mathbb{F}_p$-algèbre. En particulier,

1. $(\forall x \in \mathbb{F}_p) \qquad x^p = x$
2. $(\forall a, b \in K) \qquad (a+b)^p = a^p + b^p$

Si de plus $card(K) < \infty$, alors $Frob_K$ est un automorphisme.

Démonstration :

1. petit Fermat.
2. p premier donc : $(\forall k \in [\![1, p-1]\!]) \qquad p \Big| \binom{p}{k} = \dfrac{p!}{k!(p-k)!}$. (exercice)
3. Frob_K est un morphisme de corps, donc injectif (le seul idéal $\neq K$ est $\{0\}$). Si $\mathrm{card}(K) < \infty$, il est donc bijectif. □