

Leçon 123: Corps finis et applications

I - Corps finis: construction

a - Généralités sur les extensions de corps M, L, K corps commutatifs

Def. 1: Si $K \subset L$, on dit que L est une extension de K (noté L/K)

Rmq. 2: Si L/K , alors L est un K -ev.

Prop. Def. 3: Soit L/K . L est un K -ev. Si $\dim_K L < \infty$ on note $\dim_K L = [L:K]$ appelé degré de L sur K .

Thm. 4: (base télescopique) Soient $M/L/K$, $(e_i)_{i \in I}$ une base de L sur K , $(f_j)_{j \in J}$ base de M sur L alors $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K .

Si les extensions sont de degrés finis on a $[M:K] = [M:L][L:K]$

Def. 5: Soit L/K et $A \subset L$ on dit que A engendre L sur K (et on note $L = K(A)$) si L est la plus petite extension de K contenant K et A . L est dite monogène si il existe $\alpha \in L$ tq $L = K(\alpha)$.

Def. 6: Soit L/K , $\alpha \in L$. Si $\exists P \in K[X] \setminus \{0\}$ tq $P(\alpha) = 0$, on dit alors que α est algébrique sur K . Dans le cas contraire α est dit transcendant.

Def. 7: Si $\alpha \in L$ est algébrique sur K , alors $\{P \in K[X] \mid P(\alpha) = 0\}$ est un idéal non nul donc admet un unique générateur (P_α, K) appelé polynôme minimal de α sur K .

Thm./def. 8: Soient L/K , $\alpha \in L$. les ASE:

- (i) α est algébrique sur K (iii) $\dim_K K(\alpha) < \infty$
- (ii) $K(\alpha) = K(\alpha)$

Si $P_{\alpha, K}$ est le pol. min de α sur K alors $\dim_K K(\alpha) = \deg(P_{\alpha, K})$

Def. 9: L/K est dite finie si $[L:K] < \infty$.

L/K est dite algébrique si $\forall \alpha \in L$, α est algébrique sur K .

Rmq. 10: Toute extension finie est algébrique

Thm. 11: L'ensemble des éléments algébrique sur K est un corps de L .

b - Corps de rupture et décomposition

Def. 12: Soit $P \in K[X]$ irréductible. On dit que L est un corps de rupture de P sur K si $\exists \alpha \in L$ tq $P(\alpha) = 0$ et $L = K(\alpha)$.

Thm. 13: Soit $P \in K[X]$ irréductible. Le corps $\frac{K[X]}{(P)}$ est l'unique corps de rupture de P à isomorphisme près.

Def. 14: Soit $P \in K[X]$ de deg. n . On appelle corps de décomposition de P sur K une extension L/K tq:

- Dans $L[X]$ P est produit de facteurs de deg. 1.
- L est minimal pour cette prop.

Thm. 15: $\forall P \in K[X]$, il existe un unique (à isomorphisme près) corps de décomposition de P sur K . On le note $D_K(P)$.

c - Caractéristique d'un corps

Def. 16: On appelle sous corps premier de K le plus petit sous corps de K contenant 1_K .

Def. 17: $\varphi: \mathbb{Z} \rightarrow K$, $n \mapsto n \cdot 1_K$. Le générateur de $\text{Ker}(\varphi)$ est appelé caractéristique de K noté $\text{car}(K)$.

Prop. 18: $\text{car}(K)$ est soit nulle soit un nombre premier. Si $\text{car}(K) = 0$ alors K est infini et contient $\mathbb{Q}$.

Rmq. 19: Si $\text{car}(K) = p$ on a $p \cdot 1_K = 0$ donc $\forall x \in K$ $px = 0$.

d - Existence, unicité et structure des corps finis

Def. 20: On dit qu'un corps est fini si $|K| < \infty$.

Ex. 21: $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps fini.

Prop. 22: Si K est fini, on a $\text{car}(K) = p$. Le sous corps premier de K est $\mathbb{F}_p$.

Prop. 23: Si K est fini alors le cardinal de K est une puissance de p .

CPER
p. 65
-67

CPER
p. 70-72

CPER
p. 72

ZPER3
p-72
-73

$(p = \text{car}(K))$.

Prop. 24: Soit $\text{car}(K) = p$. $f: K \rightarrow K$ est appelé morphisme de Frobenius.

Si K est fini c'est un automorphisme.

Si $K = \mathbb{F}_p$ c'est l'identité.

Thm. 25: Il existe un corps K à q éléments, c'est $\mathbb{F}_q(X^q - X)$.

Rmq. 26: D'après Thm. 15 ce corps est unique à isomorphisme près.

Prop. 27: $\text{Aut}(\mathbb{F}_q) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. $\text{Aut}(\mathbb{F}_q)$ est un groupe abélien fini de cardinal $\phi(m)$.

Thm. 28: $\text{Aut}(\mathbb{F}_q)$ est un groupe cyclique (engendré par le morphisme de Frobenius).

ZPER3
p-24
-25

Thm. 29: (Wedderburn) Tout corps fini est commutatif.

Prop. 30: $\mathbb{F}_q$ contient (à isomorphisme près) un unique corps à p^m éléments avec $m|m$. Avec un abus de notation on a $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$.

Rmq. 31: On peut faire des tours d'extensions (cf fig 1)

c- Groupe multiplicatif $\mathbb{F}_q^\times$

Prop. 32: $\forall n \in \mathbb{N}^*$, $m = \sum_{d|n} \phi(d)$

Thm. 33: $\mathbb{F}_q^\times$ est un groupe cyclique (donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$).

Rmq. 34: En général on ne sait pas trouver des générateurs de $\mathbb{F}_q^\times$.

Thm. 35: (Élément primitif sur un corps fini). K corps fini, L/K extension finie de K . Alors L est monogène.

Thm. 36: Soit $P \in \mathbb{F}_p[X]$ irr. de deg. n . $\mathbb{F}_q \cong \mathbb{F}_p[X]/(P)$

Cor. 37: Dans un corps fini, corps de rupture et decomp. coïncident.

ZG023
p-85 et 87
à voir si c'est pas autre chose.

II. Polynômes irréductibles et corps finis

Thm. 38: (Eisenstein) Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$

Soit $p \in \mathbb{Z}$ premier. Si:

- $p \nmid a_n$
- $p \mid a_i \quad \forall i \in \{0, \dots, n-1\}$
- $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$. Si $\text{pgcd}(a_i, p) = 1$ alors P est irr. dans $\mathbb{Z}[X]$.

Thm. 39: Soit p premier, $P \in \mathbb{Z}[X]$. Soit $\bar{P}$ sa réduction sur $\mathbb{F}_p$. Si $\text{deg}(\bar{P}) \neq 0$ dans $\mathbb{F}_p$.

Si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, P est irréductible sur $\mathbb{Q}[X]$.

Rmq. 40: Ces théorèmes se généralisent en considérant un anneau factoriel, un idéal premier et le corps des fractions de cet anneau.

Thm. 41: Soit $P \in K[X]$ de deg. n . P est irréductible si P n'a pas de racines dans tout L/K tq $[L:K] \leq \frac{n}{2}$.

Thm. 42: $P \in K[X]$ irréductible de deg. n et soit L/K de degré m tq $\text{pgcd}(m, n) = 1$ alors P est irr. sur K .

Rmq. 43: la connaissance de pol. irréductibles est utile pour la construction de corps finis (cf. thm. 36)

III. Dénombrément dans les corps finis

a- Dénombrément des polynômes irréductibles sur $\mathbb{F}_q$

On prend $m \in \mathbb{N}^*$ et $m = \prod_{i=1}^r p_i^{a_i}$ sa décomposition en facteurs.

Def. 44: On appelle fonction de Möbius $\mu(m) = \begin{cases} 1 & \text{si } m=1 \\ (-1)^r & \text{si } m \text{ est produit de } r \text{ facteurs premiers} \\ 0 & \text{sinon} \end{cases}$

Prop. 45: (Inversion de Möbius) Soient $u, v \in \mathbb{N}^{\mathbb{N}^*}$
 $\forall m \in \mathbb{N}^*, u(m) = \sum_{d|m} v(d)$ si $\forall m \in \mathbb{N}^* v(m) = \sum_{d|m} \mu(d) u(\frac{m}{d})$

Thm. 46: $X^q - X$ est sans facteur carré dans $\mathbb{F}_p[X]$ et
 $X^q - X = \prod_{d|q} \prod_{P \in \mathcal{U}_d(p)} P$ où $\mathcal{U}_d(p)$ est l'ensemble des pol. unitaires irr. de deg. d sur $\mathbb{F}_p[X]$.

ZPER3
p-76
-79

ZG013
p-325
-332

[KOM]
p.423
-424
DEV1

Cor. 47: $\forall n \in \mathbb{N}^*$, $I_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$ où $I_n = |U_n(p)|$

b. Carrés dans un corps fini $q = p^n$

[ZPERS]
p.75

Def. 48: On note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \text{ tq } x^2 = y\}$

$$\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$$

Prop. 49: $\mathbb{F}_2^2 = \mathbb{F}_2$ et si $p > 2$ $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Thm. 50: Si $p > 2$, on a: $x \in \mathbb{F}_q^{*2}$ si $x^{\frac{q-1}{2}} = 1$.

Cor. 51: $p > 2$. -1 est carré dans $\mathbb{F}_q$ si $q \equiv 1 \pmod{4}$.

Rmq. 52: Avec ce corollaire on peut montrer que $x^2 + 1$ est irréductible dans $\mathbb{F}_q$ pour q qui n'est pas congru à 1 mod. 4.

c. Matrices à coefficients dans un corps fini E en $\mathbb{F}_q$ -ev. de dim. $n \in \mathbb{N}^*$

[ZPERS]
p.105

Prop. 53 $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$

$|SL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-2}) q^{n-1}$

[KOM]
p.151

Def. 54: On note $DP(E)$ l'ensemble des automorphismes de E diagonalisables

DEV2

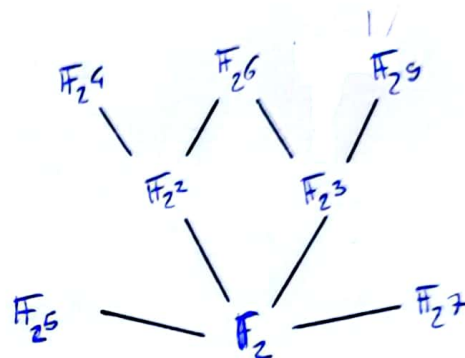
Thm. 55: $|DP(E)| = \sum_{\substack{n_1, \dots, n_q \in \mathbb{N} \\ n_1 + \dots + n_q = n}} \frac{|GL_{n_1}(\mathbb{F}_q)| \dots |GL_{n_q}(\mathbb{F}_q)|}{|GL_n(\mathbb{F}_q)|}$

[ZPERS]
p.63

Def. 56: On note $D(E)$ l'ensemble des endomorphismes de E diagonalisables.

Thm. 57: $|D(E)| = \sum_{\substack{n_1, \dots, n_q \in \mathbb{N} \\ n_1 + \dots + n_q = n}} \frac{|GL_{n_1}(\mathbb{F}_q)| \dots |GL_{n_q}(\mathbb{F}_q)|}{|GL_n(\mathbb{F}_q)|}$

Annexe 1:



Références:

[ZPERS]: Perrin, cours d'algèbre.

[GOZ]: Gossard, théorie de Galois.

[KOM]: Rombaldi, algèbre géométrie.

[CVAS]: Caldero, Carnet de voyage en algèbre.