Leçon 123 : Corps finis. Applications

Références : Perrin, Gozard, Berhuy, Francinou 1, Caldero (CVA)

I - Construction des corps finis

1) Caractéristique d'un corps, extension de corps
2) Existence et unicité des corps finis
3) Le groupe multiplicatif $\mathbb{F}_q^\times$

II - Polynômes et corps finis

1) Critères d'irréductibilité
2) Polynômes irréductibles de $\mathbb{F}_q[X]$

III - Dénombrement dans les corps finis

1) Carrés dans un corps fini
2) Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$
3) Matrices à coefficients dans $\mathbb{F}_q$

DEV 1 : Théorème de Wedderburn

DEV 2 : Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$.

Leçon 123 : Corps finis. Applications.

I - Construction des corps finis

[PER] 1) Caractéristique d'un corps et extension de corps

Soient K, L des corps commutatifs.

DEF 1 : Si $K \subset L$, on dit que L est une extension de K et on la note L/K. On dit aussi que K est un sous-corps de L.

REM 2 : Si K est un sous-corps de L, alors L est un K-espace vectoriel.

DEF 3 : Si $\dim_K(L)$ est finie, on pose $[L:K] = \dim_K(L)$ et cet entier s'appelle le degré de L sur K.

THM 4 : Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une K-base de L et $(f_j)_{j\in J}$ une L-base de M. Alors $(e_i f_j)_{(i,j)\in I\times J}$ est une K-base de M.

COR 5 : Dans ce cas, si les degrés sont finis, on a $[M:K] = [M:L][L:K]$

DEF 6 : Soit L/K une extension et $A \subset L$. On dit que A engendre L sur K et on écrit $L = K(A)$ si L est le plus petit sous-corps de L contenant A et K. L'extension est dite monogène lorsqu'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

DEF 7 : Soit L/K une extension. Soit $\alpha \in L$. Soit $\varphi : \begin{array}{l} K[T] \longrightarrow L \\ P \longmapsto P(\alpha) \end{array}$

- Si φ est injectif, on dit que α est transcendant sur K
- Sinon, on dit que α est algébrique sur K. L'idéal $I = \ker(\varphi)$ est non nul et principal donc engendré par μ_α appelé polynôme minimal de α sur K.

EX 8 : $\sqrt{2}$; i ; $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$.

THM 9 : Soit L/K une extension et $\alpha \in L$. LASSE :

- α est algébrique sur K
- On a $K[\alpha] = K(\alpha)$
- On a $\dim_K(K[\alpha]) < \infty$. Dans ce cas, μ_α est irréductible et $\dim_K(K[\alpha]) = \deg(\mu_\alpha)$.

DEF 10 : Soit $P \in K[X]$ irréductible. Une extension L/K est appelée corps de rupture de P sur K si $L = K(\alpha)$ avec $P(\alpha) = 0$.

THM 11 : Soit $P \in K[X]$. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

DEF 12 : Soit $P \in K[X]$. On appelle corps de décomposition de P sur K une extension L/K telle que P est scindé dans L et L est minimal pour cette propriété.

THM 13 : Pour tout $P \in K[X]$, il existe un corps de décomposition de P sur K, unique à isomorphisme près. On le note $D_K(P)$.

EX 14 : $D_{\mathbb{Q}}(X^3-2) = \mathbb{Q}(\sqrt[3]{2}, j)$, $D_{\mathbb{Q}}(X^4-2) = \mathbb{Q}(i, \sqrt[4]{2})$.

DEF 15 : On appelle sous-corps premier de K le plus petit sous-corps de K.

PROP 16 : Soit $\varphi : \begin{array}{l} \mathbb{Z} \longrightarrow K \\ m \longmapsto m\cdot 1 \end{array}$. Alors $\ker(\varphi) = \{0\}$ ou $\ker(\varphi) = p\mathbb{Z}$ avec p un nombre premier.

DEF 17 : Le nombre p, générateur de $\ker(\varphi)$ est appelé caractéristique du corps K noté $\mathrm{car}(K)$.

REM 18 : Si $p \neq 0$, $p = \mathrm{car}(K)$, alors $p \cdot 1_K = 0$.

PROP 19 : Si $\mathrm{car}(K) = p$, alors $f : x \in K \mapsto x^p \in K$ est un morphisme de corps.

2) Existence et unicité des corps finis [PER] [GOZ]

PROP 20 : Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps commutatif noté $\mathbb{F}_p$.

REM 21 : Si L est un corps fini, alors L est un $\mathbb{F}_p$-espace vectoriel, donc $\#L = p^n$ où $n = [L:\mathbb{F}_p]$ où $p = \mathrm{car}(L)$

DEV 1

THM 22 : (Wedderburn) Tout corps fini est commutatif

THM 24 : Soit p un nombre premier et $n \in \mathbb{N}^*$, $q = p^n$. Il existe un corps K à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.

EX 25 : Il n'existe pas de corps à 6 éléments. Par contre $\mathbb{F}_{25} = \mathbb{F}_{5^3}$ existe c'est $D_{\mathbb{F}_5}(X^{25}-X)$ à isomorphisme près.

THM 26: Soient p premier, $n \in \mathbb{N}^*$, $q = p^n$.
- Soit K un sous-corps de $\mathbb{F}_q$. Alors il existe $d | n$ tel que $\#K = p^d$.
- Pour tout $d | n$, $\mathbb{F}_q$ a un et un seul sous-corps de cardinal p^d. Ce sous-corps est isomorphe à $\mathbb{F}_{p^d}$.

COR 27: $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n} \Leftrightarrow d | n$

REM 28: On dessine en annexe le treillis de $\mathbb{F}_2$.

3) Le groupe multiplicatif $\mathbb{F}_q^*$ [BERH] [GOZ]

DEF 29: Soit G un groupe. On dit que G est d'exposant fini lorsqu'il existe $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$. On appelle alors exposant de G le plus petit entier $n \geq 1$ vérifiant cette propriété.

LEMME 30: Soit G un groupe d'exposant fini. Alors $\exp(G) = \text{ppcm}(o(x), x \in G)$. De plus, si G est fini, $\exp(G) | \#G$

PROP 31: Soit G un groupe abélien d'exposant fini. Alors : $\exists x \in G, o(x) = \exp(G)$.

COR 32: Soit G abélien fini. Alors $\exp(G) = \#G$ si et seulement si G est cyclique.

EX 33: L'exemple de $\mathfrak{S}_3$ montre que ce résultat est faux en général si G n'est pas abélien.

THM 34: Soit K un corps. Alors tout sous-groupe fini de K^* est cyclique.

COR 35: $\mathbb{F}_q^*$ est cyclique, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

THM 36: Soit ξ un générateur de $\mathbb{F}_q^*$. Alors $\mathbb{F}_q = \mathbb{F}_p(\xi)$. ξ est un élément primitif.

THM 37: Soient p premier, $q = p^n$, $n \in \mathbb{N}^*$. Soit π un polynôme irréductible sur $\mathbb{F}_p$ de degré n. Alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$.

EX 38: X^2+X+1 est irréductible sur $\mathbb{F}_2$ donc : $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$
De même, $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$

II - Polynômes et corps finis

1) Critères d'irréductibilité [PER]

THM 39 (Eisenstein): Soit A un anneau factoriel, $K = \text{Frac}(A)$ son corps des fractions. Soit $P(X) = a_n X^n + \dots + a_0$, $a_i \in A$. Soit $p \in A$ irréductible. On suppose :
- $p \nmid a_n$
- $\forall i \in [\![0; n-1]\!]$, $p | a_i$
- $p^2 \nmid a_0$

Alors, P est irréductible dans $K[X]$ et dans $A[X]$ si $\text{pgcd}(a_i) = 1$.

THM 40 (Réduction modulo p): Soient A un anneau factoriel, p un élément premier de A et $B = A/(p)$ et $K = \text{Frac}(A)$. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo p. On suppose $\bar{a}_n \neq \bar{0}$ dans B. Alors, si $\bar{P}$ est irréductible dans B ou $L = \text{Frac}(B)$, alors P est irréductible dans K.

REM 41: On applique ce théorème avec $A = \mathbb{Z}$ et $B = \mathbb{F}_p$.

EX 42: $X^n - 2$ est irréductible dans $\mathbb{Z}$

2) Polynômes irréductibles de $\mathbb{F}_q[X]$ [GOZ] [PER]

THM 43: Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.
Si π est un polynôme irréductible de degré n sur $\mathbb{F}_p$ alors $\pi(X)$ divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$, donc est scindé sur $\mathbb{F}_{p^n}$ donc son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(\pi)$ est aussi son corps de décomposition.

THM 44: Soit $P \in \mathbb{F}_q[X]$. Alors P est irréductible si et seulement si P est sans racines dans toute extension de degré au plus $\frac{\deg(P)}{2}$.

THM 45 : Soit $P \in K[X]$ irréductible de degré n et $\mathbb{L}$ une extension de degré m avec $n \wedge m = 1$. Alors P est encore irréductible sur $\mathbb{L}$.

EX 46 : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$. Donc on a aussi $X^4 + 8X^2 + 17X - 1$ irréductible sur $\mathbb{Z}$.

PROP 47 : $X^4 + 1$ est irréductible sur $\mathbb{Z}$ (donc sur $\mathbb{Q}$) mais est réductible sur tout corps $\mathbb{F}_p$ pour tout p.

III - Dénombrement dans les corps finis

1) Carrés dans un corps fini [PER]

DEF 48 : On note $\mathbb{F}_q^2 = \{ y \in \mathbb{F}_q \mid y = x^2, x \in \mathbb{F}_q \}$ et $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^2 \setminus \{0\}$.

PROP 49 : Pour $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$.
Pour $p > 2$, $\#\mathbb{F}_q^2 = \frac{q+1}{2}$ et $(\mathbb{F}_q^*)^2 = \frac{q-1}{2}$.

PROP 50 : On suppose $p > 2$. Alors on a :
$$x \in (\mathbb{F}_q^*)^2 = x^{\frac{q-1}{2}} = 1$$

COR 51 : $-1 \in (\mathbb{F}_q^*)^2 \iff q \equiv 1 \bmod 4$.

EX 52 : Si $q = 7$, $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, on a $\frac{q-1}{2} = 3$ et $2^3 = 8 = 1 \bmod 7$ donc 2 est un carré, 3 n'est pas un carré dans $\mathbb{F}_7$.

COR 53 : Le produit de deux carrés ou de deux non carrés est un carré. Le produit d'un carré et d'un non carré est un non carré.

2) Dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ [FRA 1]

DEF 54 : On définit la fonction de Möbius par :
$$\mu : \mathbb{N}^* \longrightarrow \{-1; 0; 1\}$$
$$n \longmapsto \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \text{ contient un facteur carré} \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ avec les } p_i \text{ 2 à 2 distincts} \end{cases}$$

DEV 2

LEMME 55 : $\forall n \geq 2$, $\sum_{d \mid n} \mu(d) = 0$

PROP 56 : (Inversion de Möbius) Soit $f : \mathbb{N}^* \to \mathbb{R}$ et $g : n \in \mathbb{N}^* \mapsto \sum_{d \mid n} f(d)$. Alors, pour tout $n \in \mathbb{N}^*$,
$$f(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right)$$

THM 57 : Soit $A(n,q)$ l'ensemble des polynômes irréductibles de degré n unitaires sur $\mathbb{F}_q$. Alors :
$$X^{q^n} - X = \prod_{d \mid n} \prod_{P \in A(d,q)} P(X)$$

THM 58 : Soit $I(n,q) = \# A(n,q)$. Alors on a la formule :
$$I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d \text{ et } I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}.$$

3) Matrices à coefficients dans un corps fini [CAL] [CVA]

PROP 59 : Les ensembles $\mathcal{M}_n(\mathbb{F}_q)$, $GL_n(\mathbb{F}_q)$ et $SL_n(\mathbb{F}_q)$ sont finis et on a : $\# \mathcal{M}_n(\mathbb{F}_q) = q^{n^2}$; $\# GL_n(\mathbb{F}_q) = \prod_{i=0}^{n-1} (q^n - q^i)$ et $\# SL_n(\mathbb{F}_q) = \prod_{i=0}^{n-2} (q^n - q^i) q^{n-1}$

Soit E un $\mathbb{F}_q$-espace vectoriel de dimension $n \in \mathbb{N}^*$.

LEMME 60 : (Fitting) Soit $u \in \mathcal{L}(E)$. Les suites $(\ker(u^k))_{k \in \mathbb{N}}$ et $(\mathrm{Im}(u^k))_{k \in \mathbb{N}}$ sont respectivement croissante et décroissante et stationnent à partir d'un même rang $n_0 \in \mathbb{N}^*$. On a $E = \ker(u^{n_0}) \oplus \mathrm{Im}(u^{n_0})$ et $v = u_{|\ker(u^{n_0})}$ est nilpotent, $w = u_{|\mathrm{Im}(u^{n_0})}$ est bijectif.

DEF 61 : La donnée de $((F,G), v, w)$ avec $E = F \oplus G$, $v \in \mathcal{L}(F)$ nilpotent, $w \in \mathrm{Aut}(G)$ est appelée décomposition de Fitting.

THM 62 : Soit $\mathcal{N}_n(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes sur $\mathbb{F}_q$, de taille n. Alors $\# \mathcal{N}_n(\mathbb{F}_q) = q^{n(n-1)}$.