Corps finis. Applications.

123

I - Des corps finis

A- Prérequis sur les extensions de corps

Soit $L/M/K$ une tour d'extensions de corps (commutatifs).

[P] 65 **Def/Prop 1** : L est un K-espace vectoriel, sa dimension est appelée *degré* de L/K, et est notée $[L:K]$.

[P] 65 **Thm 2** (de la base téléscopique) : Soient $(e_i)_{i\in I}$ une K-base de M et $(f_j)_{j\in J}$ une M-base de L. En particulier, $[L:K] = [L:M]\times[M:K]$ (dans $\mathbb{N}\cup\{+\infty\}$).

[P] 70 **Def 3** : Soit $P\in K[X]$ non constant.

- Supposons P irréductible sur K. On dit que L est un *corps de rupture* (CDR) de P sur K s'il existe $\alpha\in L$ tel que $P(\alpha)=0$ et $L=K(\alpha)$.
- On dit que L est un *corps de décomposition* (CDD) de P sur K s'il existe $(\alpha_1,\dots,\alpha_n)\in L^n$ tel que $L=K(\alpha_1,\dots,\alpha_n)$ et P est scindé sur L.

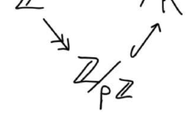
[P] 70-71 **Thm 4** :
- P admet un unique corps de rupture à K-isomorphisme près. Plus précisément, $\frac{K[X]}{\langle P\rangle}$ est un corps de rupture de P sur K.
- P admet un unique corps de décomposition D à K-isomorphisme près. Celui-ci vérifie $[D:K]\leq \deg(P)!$.

B- Construction des corps finis : existence et unicité

Ex 5 : Soit p un nombre premier. L'anneau $(\mathbb{Z}/p\mathbb{Z},+,\times)$ est un corps fini commutatif. On le note $\mathbb{F}_p$.

Dans ce paragraphe, K désigne un corps fini commutatif.

[P] 72 **Thm/Def 6** : Il existe un nombre premier p rendant le diagramme ci-contre commutatif. L'entier p est appelé *caractéristique* de K notée $\mathrm{car}(K)$, et $\mathbb{F}_p$ est appelé *sous-corps premier* de K.



C'est le plus petit sous-corps de K. On notera p la caractéristique de K.

Cor 7 : $\#K = p^{[K:\mathbb{F}_p]}$.

[P] 72

Rq 8 : Il n'existe pas de corps fini commutatif à 6 éléments !

[P] 73 **Lemme/Def 9** : $Fr : K\longrightarrow K,\ x\longmapsto x^p$ est un morphisme de corps, appelé *morphisme de Frobenius*.

[P] 73 **Thm 10** : Soient $r\in\mathbb{N}^*$, p premier et $q=p^r$. Il existe un corps fini commutatif à q éléments. Un tel corps est un CDD de X^q-X. En particulier, les classes d'isomorphisme de corps finis commutatifs sont caractérisées par le cardinal de ces-derniers. On note $\mathbb{F}_q$ un représentant de la classe d'isomorphisme des corps finis commutatifs à q éléments.

[P] 82 **Thm 11** (de Wedderburn) : Tout corps fini est commutatif.

Ex 12 : $\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{\langle X^2+X+1\rangle} = \{0,1,\bar{X},1+\bar{X}\}$, $\mathbb{F}_9 = \frac{\mathbb{F}_3[X]}{\langle X^3+X^2+X+1\rangle}$

C- Propriétés des corps finis

Soient p un nombre premier, $r\in\mathbb{N}^*$ et $q=p^r$.

Prop 13 : $\forall (m,n)\in(\mathbb{N}^*)^2,\ \mathbb{F}_{p^n}\subseteq\mathbb{F}_{p^m} \iff n\mid m$ FIGURE 1

Prop 14 :
- $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}^*}\mathbb{F}_{p^n}$ est une clôture algébrique de $\mathbb{F}_p$.
- Si K est une extension de $\mathbb{F}_q$, alors $\mathbb{F}_q = \{x\in K \mid x^q = x\}$.

[P] ~73

En particulier, $\mathbb{F}_q$ est l'unique sous-corps de $\overline{\mathbb{F}_p}$ de cardinal q.

[P] 74 **Thm 15** : $\mathbb{F}_q^\times$ est cyclique.

[P] 73 **Prop 16** : Fr est un automorphisme de $\mathbb{F}_q$.

[Rb] 425 **Thm 17** : Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre r, engendré par Fr.

Rq 18 : Pour tout $\theta\in\mathbb{F}_q$, il existe $d\in\mathbb{N}^*$ tel que $Fr^d(\theta)=\theta^{p^d}=\theta$. Le polynôme minimal de θ sur $\mathbb{F}_p$ est $\prod_{k=1}^{d}(X-Fr^k(\theta))$

Ex 19 : Soit $\beta=\bar{X}^2+\bar{X}\in\frac{\mathbb{F}_2[X]}{\langle X^4+X+1\rangle}$. On a $P_{\beta,\mathbb{F}_2} = X^2+X+1$,

II - Carrés dans un corps fini

Soient p un nombre premier impair, $r \in \mathbb{N}^*$ et $q = p^r$. On pose $c : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^2$ et $\ell : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^{\frac{q-1}{2}}$.

Prop 20 : $\mathrm{Im}(\ell) = \mathrm{Ker}(c) = \{\pm 1\}$ et $\mathrm{Ker}(\ell) = \mathrm{Im}(c) = \{x^2 : x \in \mathbb{F}_q^\times\}$.

[P 75] **Cor 21** (critère d'EULER) : $x \in \mathbb{F}_q^\times$ est un carré si, et seulement si $x^{\frac{q-1}{2}} = 1$

[P 74] **Cor 22** : Il y a $\frac{q-1}{2}$ carrés inversibles dans $\mathbb{F}_q$ (et $\frac{q+1}{2}$ carrés).

[P 74] **Prop 23** : Tous les éléments de $\mathbb{F}_{2^r}$ sont des carrés.

[P 75] **Prop 24** : -1 est un carré dans $\mathbb{F}_p$ si, et seulement si $p \equiv 1\ [4]$.

[P 56] **Appli 25** : p est somme de deux carrés si, et seulement si $p = 2$ ou $p \equiv 1\ [4]$.

[Rb 428] **Def 26** : Le symbole de LEGENDRE de $a \in \mathbb{Z}$ modulo p est :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \in p\mathbb{Z} \\ 1 & \text{si } a \text{ est un carré inversible modulo } p \\ -1 & \text{sinon} \end{cases}$$

[Rb 428] **Prop 27** : $\forall a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$. En particulier, $\left(\frac{\cdot}{p}\right)$ est un morphisme du groupe $\mathbb{F}_p^\times$.

Prop 28 : Soit $a \in \mathbb{F}_p^\times$. L'équation de $ax^2 = 1$ a $1 + \left(\frac{a}{p}\right)$ solutions dans $\mathbb{F}_p$.

[Rb 431-434] **Thm 29** (loi de réciprocité quadratique) : Soient p et q deux nombres premiers impairs distincts.

DEV 1 (*)

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

(*) : par les formes quadratiques

Appli 30 : $\left(\frac{11}{23}\right) = \left(\frac{23}{11}\right)(-1)^{11 \cdot 5} = -\left(\frac{1}{11}\right) = -1$ donc 11 n'est pas un carré modulo 23.

[Rb ~438 C 307] **Prop 31** : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Prop 32 : Soit $(a,b,c) \in \mathbb{F}_q^3$ avec $a \neq 0$. L'équation $ax^2 + bx + c = 0$ dans $\mathbb{F}_q$ a des solutions si, et seulement si $b^2 - 4ac$ est un carré dans $\mathbb{F}_q$. Le cas échéant, si $\delta \in \mathbb{F}_p$ vérifie $\delta^2 = b^2 - 4ac$, alors les solutions de cette équation sont $\frac{-b \pm \delta}{2a}$.

Rq 33 : Dans $\mathbb{F}_{2^r}$, l'équation $ax^2 + bx + c = 0$ est bien plus difficile à résoudre, en dehors des cas triviaux !

III - Algèbre (bi)linéaire sur les corps finis

Soient p un nombre premier impair, $r \in \mathbb{N}^*$, $q = p^r$ et $n \in \mathbb{N}$.

[Rb 155] **Prop 34** : ▸ $\#GL_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} (q^k - 1)$

▸ $\#SL_n(\mathbb{F}_q) = \#GL_n(\mathbb{F}_q) / (q-1)$

[C 50] **Thm 35** :

$$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré mod } q \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

DEV 2

Rq 36 : $SO_2(\mathbb{F}_{2^r}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \mathbb{F}_{2^r}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, puis $SO_2(\mathbb{F}_{2^r}) \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^r$.

Soit E un $\mathbb{F}_q$-espace vectoriel de dimension finie.

[Rb 463] **Def 37** : Le discriminant d'une forme quadratique f sur E est l'image de son déterminant dans une base quelconque modulo les carrés de $\mathbb{F}_q^\times$.

[Rb ~482] **Thm 38** : Il y a deux classes d'équivalence de formes quadratiques non dégénérées sur E. Plus précisément, soient $a \in \mathbb{F}_q^\times$ qui n'est pas un carré, et f une forme quadratique sur, de matrice M dans la base canonique.

- Si $\det(M)$ est un carré dans $\mathbb{F}_p^\times$, alors M est congruente à $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.
- Sinon, M est congruente à $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$.

Appli 39 : Loi de réciprocité quadratique (Thm 29).

IV - Polynômes et corps finis

[P] 76

Thm 40 (critère d'EISENSTEIN) : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Soit p un nombre premier. Si $p \nmid a_n$, si $\forall k \in [\![0, n-1]\!]$, $p \mid a_k$ et $p^2 \nmid a_0$, alors P est irréductible dans $\mathbb{Q}[X]$.

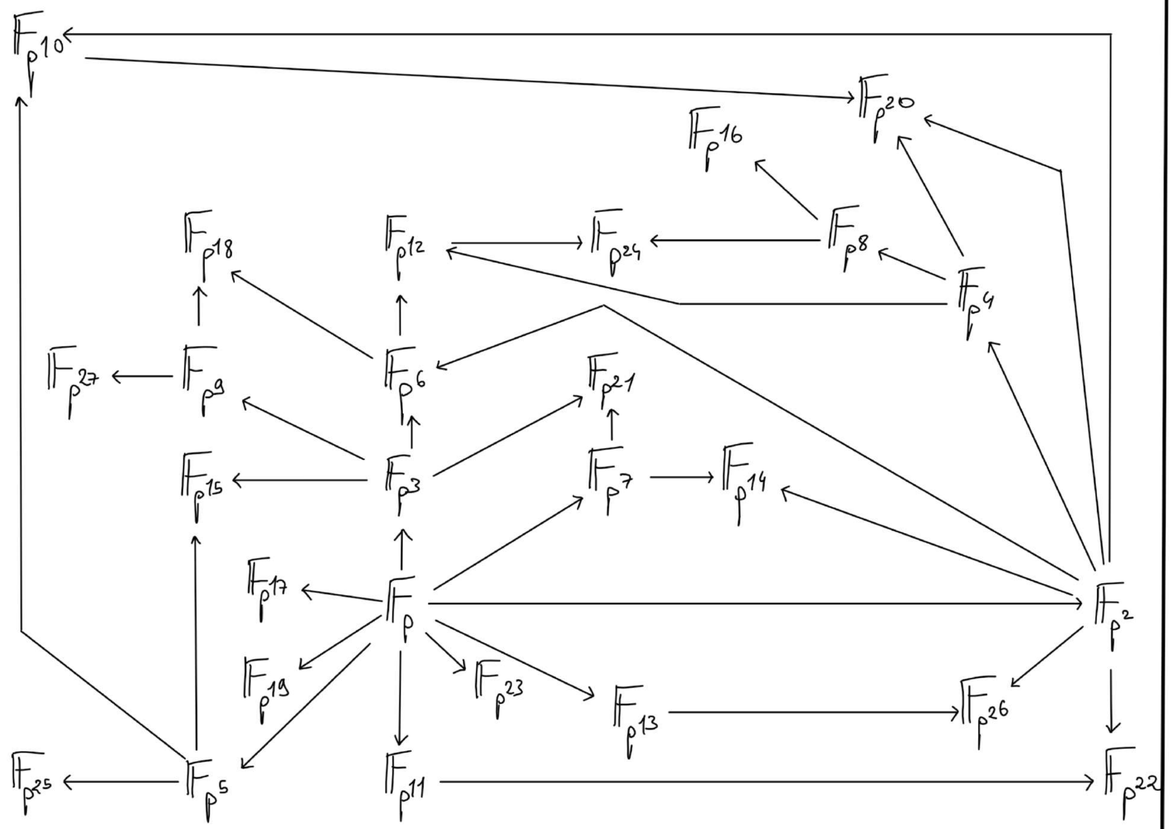
Ex 41 : Pour tout p premier, $\Phi_p = X^{p-1} + \cdots + X + 1$ est irréductible sur $\mathbb{Q}$.

[P] 77

Thm 42 : Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, $n \geq 1$, $a_n \neq 0$. Soit $p \in \mathbb{Z}$ premier. Si $p \nmid a_n$ et si l'image $\bar{P}$ de P dans $\mathbb{F}_p[X]$ est irréductible, alors P est irréductible sur $\mathbb{Z}$.

Rq 43 : La réciproque est fausse : considérer $X^4 + 1$

FIGURE 1



RÉFÉRENCES

[P] Perrin

[Rb] Rombaldi

[C] NH_2G_2 I