123 Corps finis. Applications.

Refs : [Perr] Perrin Cours d'algèbre
[Serre] Serre, cours d'arithmétique
[Goz] Gozard Théorie de Galois
[Dem] Demazure Cours d'Algèbre

Devt :
34 Réciprocité quadratique [Serre]
45 46 Polys irred $\mathbb{F}_q$ [Goz]
56 57 Chevalley Warning + EGZ [Zav]

I. Généralités sur les corps finis.

1) Caractéristique, sous corps premier.

[Perr] 72 73

Def 1 : Soit K un corps, on appelle sous corps premier de K l'intersection de tous ses sous corps non nuls.

Ex 2 : Le sous corps premier de $\mathbb{R}$ ou $\mathbb{C}$ est $\mathbb{Q}$.

Prop def 3 : Soit A un anneau unitaire, il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \to A$ (unitaire). Le générateur positif de $\ker \varphi$ est appelé caractéristique de A, notée $car(A)$.

Prop 4 : Si $A = K$ est un corps, sa caractéristique est nulle ou est un nombre premier.

Cor 5 : Si $car(K) = 0$, K est infini, mais la réciproque est fausse (ex, $\mathbb{F}_2(X)$ est de caractéristique 2).

Théo 6 : Soit $k \subseteq K \subseteq L$ des extensions de corps, alors L (resp K) est un K (resp k)-espace vectoriel, si $(b_i)_{i\in I}$ est une k base de K et $(a_j)_{j\in J}$ est une K base de L, alors $(a_j b_i)_{i\in I\times J}$ est une k base de L.

Cor 7 : Si $k \subset K$ est une extension et k, K sont finis, alors $|K| = k^m$ où $m = [K:k]$ est la dimension de K comme k-ev.

Théo 8 : Si K est un corps fini de caractéristique p, alors le sous corps premier de K est $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Ainsi $|K| = p^m$ est une puissance de p.

Ex 9 : Il n'existe pas de corps de cardinal 57.

Prop 10 : Si $car(K) = p$, alors l'application $F : K \to K$ associant x^p à x est un morphisme de corps, dit morphisme de Frobenius. Si K est fini, c'est un automorphisme, identité si $K = \mathbb{F}_p$.

Cor 11 : (Théorème de Fermat) Soit $p \in \mathbb{Z}$ premier, pour $a \in \mathbb{Z}$, on a $a^p \equiv a\,[p]$, et $a^{p-1} \equiv 1\,[p]$ si $a \notin p\mathbb{Z}$.

2) Existence et unicité des corps finis, construction.

[Goz] 59 60

Def 12 : Soit K un corps et E une extension de K. Pour $P \in K[X]$ de degré ≥ 1 on dit que E est un corps de décomposition pour P si : P est scindé dans $E[X]$ et si : E est minimal (parmi les extensions intermédiaires) avec cette propriété.

Ex 13 : Si P est scindé K en est un corps de décomposition.
$\mathbb{C}$ est le corps de décomposition de X^2+1 sur $\mathbb{R}$.

[Goz] 60

Théo 14 : Soit K un corps, $P \in K[X]$ de degré ≥ 1, Il existe un corps E de décomposition pour P, avec $[E:K] \leq n!$. De plus, deux corps de décomposition pour P sont K-isomorphes.

Théo 15 : Soient p premier, et $n \in \mathbb{N}^*$, on pose $q = p^n$. Il existe un corps à q éléments, défini comme corps de décomposition du polynôme $X^q - X \in \mathbb{F}_p[X]$. De plus ce corps est unique à isomorphisme près, on le note $\mathbb{F}_q$.

Théo 16 : Soient $n, m \in \mathbb{N}^*$, on a une inclusion $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$ si et seulement si $n | m$.

Ex 17 : Les sous corps de $\mathbb{F}_{16}$ sont $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$

3) Structure de $\mathbb{F}_q^*$

[Perr] 73 74

Théo 18 : Soit K un corps, tout sous groupe fini de K^* est cyclique. En particulier, le groupe $\mathbb{F}_q^*$ est cyclique.

Rq 19 : On ne sait pas en général trouver un générateur de $\mathbb{F}_q^*$

Ex 20 : $\mathbb{F}_8^* \simeq \mathbb{Z}/7\mathbb{Z}$, tout élément différent de 1 dans $\mathbb{F}_8^*$ en est un générateur.

88.

Théo 21 : Élément primitif pour les corps finis. On considère l'extension $\mathbb{F}_{q^n} - \mathbb{F}_q$! Il existe $\alpha \in \mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

II. Les carrés dans $\mathbb{F}_q$.

1) Définition et caractérisations

$q = p^m$ est fixé.

[Perr] 74 75

Def 22 : On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \mid y^2 = x\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \setminus \{0\}$.

Prop 23 : Par le morphisme de Frobenius, si $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$.

Prop 24 : Si $p \neq 2$ on considère le morphisme $\mathbb{F}_q^* \to \mathbb{F}_q^{*2}$ associant x^2 à x, on obtient alors $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.
On a en fait une suite exacte courte $\{\pm 1\} \hookrightarrow \mathbb{F}_q^* \twoheadrightarrow \mathbb{F}_q^2$

Prop 25 : On a une suite exacte courte $\mathbb{F}_q^{*2} \hookrightarrow \mathbb{F}_q^* \twoheadrightarrow \{\pm 1\}$ où la flèche est donnée par $x \mapsto x^{\frac{q-1}{2}}$ en particulier.
On a $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$, et $\mathbb{F}_q^{*} \simeq \mathbb{F}_q^{*}/\{\pm 1\}$ (ce qui est assez clair en se rappelant que ce sont des groupes cycliques).

[Perr] 74-75

Cor26 : Soit $p>2$ est premier, on pose $q=p^n$. Alors -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1[4]$.

Ex27 : 2 est un carré dans $\mathbb{F}_7$, contrairement à -1 et 3.

Appli28 : Il existe une infinité de nombres premiers de la forme $4m-1$.

58

Appli29 (Théorème des deux carrés) Soit $n \geq 2$, on décompose n en produit de facteurs premiers $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$. Alors n est somme de deux carrés si et seulement si ($\forall p \in \mathbb{P}$, $p \equiv 3[4] \Rightarrow v_p(n)$ est pair).

2) Symboles de Legendre et de Jacobi.

[Perrin] 14-18

Def30 : Soit $p>2$ un nombre premier et soit $x \in \mathbb{F}_p^*$. On appelle symbole de Legendre de x, noté $\left(\frac{x}{p}\right)$ l'entier ± 1 congru à $x^{\frac{p-1}{2}} \in \mathbb{F}_p$.

Rq31 : Ce symbole s'étend à $\mathbb{F}_p$ en posant $\left(\frac{0}{p}\right)=0$, et à $\mathbb{Z}$ en posant $\left(\frac{n}{p}\right) := \left(\frac{\overline{n}}{p}\right)$.
On a donc $\left(\frac{k}{p}\right)=1$ ssi $k \in \mathbb{F}_p^*$ est un carré.

Prop32 : Pour $k, k' \in \mathbb{Z}$, on a $\left(\frac{k}{p}\right)\left(\frac{k'}{p}\right)=\left(\frac{kk'}{p}\right)$ [Le symbole de Legendre est un caractère sur $\mathbb{F}_p^*$].

Prop33 : On a $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$ où $\omega(p) = \frac{p^2-1}{8}[2] = \begin{cases} 0 \text{ si } p = \pm 1[8] \\ 1 \text{ si } p = \pm 5[8] \end{cases}$.

Théo34 : Soient p et q deux nombres premiers impairs distincts, on a

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

DVP

Rq35 : Ce résultat est utilisé pour calculer des symboles de Legendre par réductions successives : $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

On souhaite aussi étendre le symbole de Legendre à un cas plus général.

[Dem] 122 123

Def36 : Si $n = p_1 \cdots p_r$, pour $m \in \mathbb{Z}$, on pose $\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_r}\right)$ où les $\left(\frac{m}{p_i}\right)$ sont des symboles de Legendre, c'est le symbole de Jacobi. (n impair)

Rq37 : Si m et n ne sont pas premiers entre eux $\left(\frac{m}{n}\right) = 0$, sinon il vaut ± 1. Il ne dépend que de la classe de m modulo n. Et on a
$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$ $\left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right)$

Prop38 : On a $\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$ si n, m sont impairs positifs premiers entre eux.

Prop39 : Si m est $\in \mathbb{F}_n^{*2}$, $\left(\frac{m}{n}\right) = 1$ mais la réciproque est fausse : $\left(\frac{14}{51}\right) = 1$.

III. Polynômes sur un corps fini.

1) Polynômes irréductibles

Prop40 : Un corps fini n'est pas algébriquement clos : $\prod_{a \in K}(X-a)+1$ est sans racines dans K.

[Goz] 86

Prop41 : Pour toute application $f : \mathbb{F}_q \to \mathbb{F}_q$, il existe un unique polynôme de degré au plus $q-1$ tel que f soit la fonction polynomiale associée à P. (interpolation de Lagrange).

Théo42 : La clôture algébrique de $\mathbb{F}_q$ s'écrit comme $\bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{q^{n}}$ (limite inductive).

[Goz] 87 90

Théo43 : Pour p premier et $n \in \mathbb{N}^*$, $q := p^n$, alors $\mathbb{F}_q \simeq \mathbb{F}_p/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Cor44 : Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$.
Si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, alors P divise $X^{p^n}-X$ dans $\mathbb{F}_p[X]$ donc est scindé dans $\mathbb{F}_q[X]$: son corps de rupture $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition.

Théo45 : Soient $p \in \mathbb{P}$ et q une puissance de p. Pour $j \in \mathbb{N}^*$, on note $K(q,j)$ l'ensemble des polynômes irréductibles de degré j sur $\mathbb{F}_p$. Alors $X^q - X = \prod_{d|n}\prod_{Q \in K(q,d)} Q(X)$

Cor46 : En notant $I(q,n) = |K(q,n)|$ et μ la fonction de Möbius, on a

$$I(q,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \underset{n \to \infty}{\sim} \frac{p^n}{n}.$$

DVP

[Perr] 77 78

Appli47 : (réduction). Soit A un anneau factoriel et $K = \mathrm{Fr}\, A$, $I \trianglelefteq A$ un idéal premier et $B = A/I$, $L = \mathrm{Fr}\, B$. Soit $P(X) = a_n X^n + \ldots + a_0 \in A[X]$ et $\overline{P}$ sa réduction modulo I. On suppose $\overline{a_n} \neq 0$ dans B. Alors si $\overline{P}$ est irréductible dans B ou L, P est irréductible dans K.

Ex48 : Pour $A = \mathbb{Z}$, $I = (p)$ et $B = L = \mathbb{F}_p$, par exemple $p=2$ donne que $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$.

Cor49 : Soit $p \in \mathbb{P}$ alors $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$ et sur $\mathbb{Z}$.

Théo50 : Si $P \in \mathbb{F}_q[X]$ de degré $n > 0$. Alors P est irréductible dans $\mathbb{F}_q[X]$ ssi il n'admet aucune racine dans $\mathbb{F}_{q^m}$ où $m \leqslant \frac{n}{2}$.

2) Cyclotomie.

[Perr] 80 82

Def 51: Pour K un corps, et $n \in \mathbb{N}$, on considère $P_n = X^n - 1$, K_n son corps de décomposition sur K. On pose $\mu_n^*(K) = \{\xi \in K_n \mid o(\xi) = n \text{ dans } K_n\}$ les racines primitives de l'unité, on pose enfin $\phi_{k,n} = \prod_{\xi \in \mu_n^*(K)} (X - \xi) \in K_n[X]$, le n-ème polynôme cyclotomique sur K.

Prop 52: On a $X^n - 1 = \prod_{d \mid n} \phi_{k,d}(X)$. Cette formule permet de calculer $\phi_{k,d}$ par récurrence.

Prop 53: On a $\phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. Et si $\varphi : \mathbb{Z} \to K$ est l'unique morphisme d'anneaux unitaires, alors $\phi_{n,k}(X) = \varphi(\phi_{n,\mathbb{Q}}(X))$.

Théo 54: Soit $q = p^\alpha$, n non divisé par p. On note k l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Les facteurs irréductibles de $\phi_{n,\mathbb{F}_q}$ sont tous de degré k.

Appli 55: (Wedderburn) Tout corps fini est commutatif.

3) Polynômes à plusieurs variables.

[Serre] 13.

Théo 56: Soit $q = p^r$, $r \geq 1$ et A un ensemble fini, $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \dots, X_n]$ tels que $\sum_{\alpha \in A} \deg f_\alpha < n$, et soit V l'ensemble de leurs zéros communs dans $\mathbb{F}_q^n$, on a $|V| \equiv 0 [p]$ (Chevalley Warning)

DVP

Cor 57 (Erdős Ginzburg Ziv) Soit $n \in \mathbb{N}$, $a_1 \dots a_{2n-1}$ des entiers, on peut en choisir n parmi ceux-ci dont la somme est divisible par n.

Appl 58: Toute forme quadratique sur $\mathbb{F}_q$ d'au moins trois variables admet un vecteur isotrope non trivial.

IV Algèbre linéaire et bilinéaire.

1) Groupes linéaires sur $\mathbb{F}_q$.

[Perr] 105

Def 59: Soit K un corps, le centre de $GL_n(K)$ est donné par les matrices scalaires et celui de $SL_n(K)$ par $Z(SL_n(K)) = SL_n(K) \cap Z(GL_n(K))$ (donc les matrices scalaires d'une racine n-ème de l'unité). On définit $PGL_n(K)$ et $PSL_n(K)$ comme les quotients respectifs de $GL_n(K)$ et $SL_n(K)$ par leurs centres.

Prop 60: Sur $\mathbb{F}_q$ tous les groupes considérés sont finis, on peut donc calculer
- $|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} (q-1)(q^2-1) \dots (q^n - 1)$.
- $|SL_n(\mathbb{F}_q)| = N = (q^n - 1) \dots (q^n - q^{n-2}) q^{n-1}$.
- $|PGL_n(\mathbb{F}_q)| = N$
- $|PSL_n(\mathbb{F}_q)| = N/d$ où $d = \operatorname{pgcd}(n, q-1)$.

[Perr] 105 106

Appl 61: $GL_n(\mathbb{F}_p)$ admet un sous-groupe de Sylow d'ordre $p^{\frac{n(n-1)}{2}}$ donné par les matrices triangulaires supérieures de diagonale $= 1$.
Ainsi tout groupe fini d'ordre un multiple de p admet des p-sous-groupes de Sylow.

Prop 62: On a les isomorphismes exceptionnels de groupe suivants
- $GL_2(\mathbb{F}_2) \simeq SL_2(\mathbb{F}_2) \simeq PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$
- $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$
- $PGL_2(\mathbb{F}_4) \simeq PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$
- $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

Rq 63: Connaissant les résultats de simplicité du groupe projectif spécial linéaire, on retrouve que $\mathfrak{A}_5$ est simple.

2) Formes quadratiques sur $\mathbb{F}_q$.

[Perr] 130

Prop 64: L'équation $ax^2 + by^2 = 1$, $a, b \in \mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$.

Prop 65: Sur $\mathbb{F}_q$ de caractéristique non 2, E un $\mathbb{F}_q$-ev de dim n, $\alpha \in \mathbb{F}_q^\times$ tq $\alpha \notin \mathbb{F}_q^{\times 2}$. Il y a exactement deux classes de similitudes de formes quadratiques non dégénérées sur E. Deux représentants respectifs de ces classes sont I_n et $\begin{pmatrix} I_{n-1} & 0 \\ 0 & \alpha \end{pmatrix}$.