123 - Corps finis. Applications

Cadre : K corps fini de cardinal $q \in \mathbb{N}$, commutatif en vertu du théorème de Wedderburn.

I - STRUCTURE DES CORPS FINIS

1) Caractéristique et cardinal

[GOZ-PER]

Rque 1 : $\varphi : \begin{cases} \mathbb{Z} \to K \\ n \mapsto n.1 \end{cases}$ alors $\operatorname{Ker}\varphi = p\mathbb{Z}$ où p premier est appelé caractéristique de K, noté car(K).
$\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$, le sous-corps premier de K est $\simeq$ à $\mathbb{F}_p$.

Propo 2 Il existe $n \in \mathbb{N}^*$ tel que $\#K = p^n$.

Conseq 3 Il n'y a pas de corps fini à 6 éléments.

Propo/déf 4 : $F : \begin{cases} K \to K \\ x \mapsto x^p \end{cases}$ est un automorphisme de corps, dit de Frobenius. Si $K = \mathbb{F}_p$ alors $F = \mathrm{Id}$.

Cor 5 [Fermat] p premier. Alors $\forall a \in \mathbb{Z}$, $a^p \equiv a [p]$.

[DMZ]

App 6 Test de non primalité : s'il existe $1 < a < n$ avec $a^{n-1} \not\equiv 1 [n]$ alors n est composé.

2) Existence et unicité des corps finis

Ici, $q = p^n$.

DEV 1

Thm 7 (i) Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.
(ii) K est unique à isomorphisme près, noté $\mathbb{F}_q$.

Cor 8 [Wilson] $n \in \mathbb{N}$, $n \geq 2$.
n est premier $\Leftrightarrow (p-1)! \equiv -1 [p]$.

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

[GOZ]

Thm 9 $\mathbb{F}_q^\times$ est cyclique : $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.

Rque 10 Plus précisément, tout sous-groupe de $\mathbb{F}_q^\times$ est cyclique.

Ex 11

p	2	3	5	7	11
générateur de $\mathbb{F}_p^\times$	1	2	2	3	2

Propo 12 Soit a un générateur de $\mathbb{F}_q^\times$. Alors $\mathbb{F}_q = \mathbb{F}_p(a) = \mathbb{F}_p[a]$ et $(1, a, \dots, a^{n-1})$ est une base du $\mathbb{F}_p$-ev $\mathbb{F}_q$.

Conseq 13 [Critère de Lehmer] Soit $n > 1$ entier impair tel qu'on connaisse les facteurs premiers de $n-1$. [DMZ]
n est premier $\Leftrightarrow$ il existe un entier a tq $a^{n-1} \equiv 1 [n]$ et $\forall q$ facteur premier de $n-1$, $a^{(n-1)/q} \not\equiv 1 [n]$

App 14 [Test de Pocklington-Lehmer]
On écrit $n-1 = uv$, les facteurs premiers de u sont connus : $u = q_1^{e_1} \dots q_r^{e_r}$. Si $\forall i \in [\![1, r]\!]$ il existe un entier a_i tel que $a_i^{q_i^{e_i}} \equiv 1 [n]$ et $(a_i^{q_i^{e_i - 1}} - 1 \wedge n) = 1$
Alors les facteurs premiers de n sont $\equiv 1 [n]$. Si de plus $v \leq u+1$ alors n est premier.

Rque 15 Nombres de Fermat $F_n = 2^{2^n} + 1$. [DMZ]
F_n est premier $\Leftrightarrow \exists a$, $a^{(F_n - 1)/2} \equiv -1 [F_n]$.

4) Automorphismes de $\mathbb{F}_q$

[DMZ]

Propo 16 Soit $\alpha \in \mathbb{F}_q$ et $r = \min\{n > 0 \mid \alpha^{p^n} = \alpha\}$. Alors $\mathbb{F}_p(\alpha)$ a p^r éléments et $\operatorname{Min}_{\mathbb{F}_p}(\alpha) = (X - \alpha) \dots (X - \alpha^{p^{r-1}})$.

Cor. $\operatorname{Aut}(\mathbb{F}_q)$ est cyclique d'ordre n, engendré par F.

5) Sous-corps de $\mathbb{F}_q$

[GOZ]

Thm 17 Les sous-corps de $\mathbb{F}_q$ sont les corps à p^d éléments de $\mathbb{F}_q$ où $d \mid n$. Ils sont uniques et isomorphes aux $\mathbb{F}_{p^d}$, $d \mid n$.

[PER]

II – LES CARRÉS DANS $\mathbb{F}_q$

1) Définition et caractérisation

Notations $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists a \in \mathbb{F}_q\ x = a^2\}$, $\mathbb{F}_q^{\times 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\times$

Propo 18 1) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

2) Pour $p > 2$ $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$

Propo 19 [Caractérisation]

$p > 2$, $x \in \mathbb{F}_q^{\times 2} \iff x^{\frac{q-1}{2}} = 1$

Ex 20 3 n'est pas un carré dans $\mathbb{F}_7$.

Cor 21 $-1 \in \mathbb{F}_q^{\times 2} \iff q \equiv 1\,[4]$.

Applications 22 • théorème des 2 carrés

• Il existe une infinité de nbs premiers de la forme $4m+1$.

[S-P]

2) Résidus quadratiques (p premier ≥ 3)

déf [Symbole de Legendre] $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0\,[p] \\ 1 \text{ si } a \text{ est un carré modulo } p \\ -1 \text{ sinon} \end{cases}$$

Propriétés 23 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Rque 24 : $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\,[p]$.

Thm [Réciprocité quadratique] q premier ≥ 3

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right).$$

Rque 25 Pour $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, on définit le symbole de Jacobi par, pour $a \in \mathbb{Z}$, $\left(\frac{a}{n}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right)^{\alpha_i}$

⚠ $\left(\frac{2}{15}\right) = 1$ mais 2 n'est pas un carré dans $\mathbb{Z}/15\mathbb{Z}$.

On a une loi de réciprocité quadratique pour m, n impairs,

Ex 26 $\left(\frac{6547}{8731}\right) = -\left(\frac{2184}{6547}\right) = -\left(\frac{8}{6547}\right)\left(\frac{273}{6547}\right) = +\left(\frac{268}{273}\right) = \dots = -1$

Rque 27 $\left(\frac{\cdot}{p}\right)$ est l'unique mφ non trivial de $\mathbb{F}_p^\times \longrightarrow \{-1, +1\}$

[OA]

App 28 [Frobenius-Zolotarev] V $\mathbb{F}_p$-ev de dim finie $\forall u \in GL(V)$, $\varepsilon(u) = \left(\frac{\det u}{p}\right)$.

Propo 29 Soit $n \in \mathbb{Z}$ composé et impair. Alors il existe $b \in \mathbb{Z}$, $b \wedge n = 1$ tel que $\left(\frac{b}{n}\right) \not\equiv b^{\frac{n-1}{2}}\,[n]$.

App 30 Test de non primalité de Solovay-Strassen.

III – POLYNÔMES SUR UN CORPS FINI

[GOZ-FER-SP]

1) Polynômes irréductibles

Notation $\mathrm{Irr}_q(\delta) = \{$polynômes irréductibles de deg δ sur $\mathbb{F}_q\}$

Thm 31 Soit $\pi \in \mathrm{Irr}_p(n)$. Alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$.

Cor 32 Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.

Ex 33 $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$, $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

Ex 34 $X^p - X - 1 \in \mathrm{Irr}_p(p)$.

[PER]

Thm 35 Soit $P \in\ [X]$, de degré n. Alors $P \in \mathrm{Irr}\ (n)$ $\iff$ P n'a pas de racines dans les extensions K de telles que $[K :\ ] \leq \frac{n}{2}$.

App 36 $X^4 + X + 1 \in \mathrm{Irr}_2(4)$.

[SP]

Thm 37 $X^q - X = \prod_{d \mid n}\left(\prod_{P \in \mathrm{Irr}_p(\delta)} P\right)$.

Conseq 38 $p^n = \sum_{d \mid n} d\,\#\mathrm{Irr}_p(d)$ et via la formule d'inversion de Möbius $\#\mathrm{Irr}_p(d) \underset{d \to \infty}{\sim} \frac{p^d}{d}$

[OA]

2) Factorisation : algorithme de Berlekamp

(DEV 2)

$P \in \mathbb{F}_q[X]$ sans facteurs carrés. Soit $x = X \bmod P$ et considérons la base $\mathcal{B} = (1, x, \dots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$.

Algorithme entrée : P sortie : $P_1, \dots, P_r$ avec $P = P_1 \dots P_r$

① Calculer $\mathrm{mat}_{\mathcal{B}}(S_P - \mathrm{Id})$ puis passer au 2, où $S_P : Q(X) \bmod P \mapsto Q(X^q) \bmod P$.

② $r = \dim(\mathrm{Ker}(S_p - Id)) = \deg P - rg(S_p - Id)$
Si $r=1$ alors P irréductible : on renvoie P.
Sinon, on passe en 3.
③ Calculer V non congru mod P à un polynôme constant de $\mathbb{F}_q[X]$, tel que V mod P $\in \mathrm{Ker}(S_p - Id)$
Alors $P = \prod_{x\in\mathbb{F}_q} \mathrm{pgcd}(P, V-x)$.
Retourner en 1 avec chacun des facteurs non triviaux.

[SER]

3) Equations sur un corps fini

lem 39 $n\in\mathbb{N}$. $S(X^n) := \sum_{x\in\mathbb{F}_q} x^n = \begin{cases} -1 & \text{si } n\geq 1 \text{ et } q-1|n \\ 0 & \text{sinon}\end{cases}$

Thm 40 [Chevalley-Warning]
Soient $f_\alpha \in K[X_1,\dots,X_n]$ (K corps à q él., $\alpha \in I$ finie) tels que $\sum \deg(f_\alpha) < n$ et V l'ensemble de leurs zéros communs dans K^n. Alors $\#V \equiv 0 \mod p$.

Cor 41 Si les f_α sont sans termes constants, $\sum \deg f_\alpha < n$ alors ils ont un zéro commun non trivial.

[SP-DMZ]

4) Polynômes et codes correcteurs

But : Détecter, voire corriger les erreurs liées aux canaux de transmission. Ici, $n \wedge q = 1$.

déf 42 : $C \subset \mathbb{F}_q^n$. La distance de Hamming de deux mots $m, m' \in C$ est le nb de positions en lesquels ils diffèrent : $d(m,m') = w(m-m')$.
Distance minimale de C : $d = \inf_{\substack{(m,m')\in C \\ m\neq m'}} w(m-m')$.

déf 43 Un code linéaire de type $[n,k,d]$ est un sev C de $\mathbb{F}_q^n$, de dimension k et distance minimale d.

ex 44 Le code de parité $\mathcal{C} = \{(c_1,\dots,c_n)\in\mathbb{F}_2^n \mid c_n \equiv \sum_1^{n-1} c_i\ [2]\}$ est un code $[n, n-1, 2]$ sur $\mathbb{F}_2$

déf 45 Un code linéaire $\mathcal{C}$ est cyclique si $\forall (c_1,\dots,c_n)\in\mathcal{C}$, $(c_n, c_1,\dots,c_{n-1})\in\mathcal{C}$.

Propo 46 Un code linéaire $\mathcal{C}$ de longueur n est cyclique ssi le sev qu'il constitue est un idéal de $\mathbb{F}_q[X]/(X^n-1)$ (on identifie $(c_1,\dots,c_n)$ à $c_1 + c_2X + \dots + c_nX^{n-1} \mod X^n-1$)

Rque 47 Cet idéal est alors principal, engendré par un diviseur g de X^n-1.

Ex $\mathcal{H}$ $[7,4,3]$ sur $\mathbb{F}_2$, de base $\begin{pmatrix}1\\1\\0\\1\\0\\0\\0\end{pmatrix} \begin{pmatrix}0\\1\\1\\0\\1\\0\\0\end{pmatrix} \begin{pmatrix}0\\0\\1\\1\\0\\1\\0\end{pmatrix} \begin{pmatrix}0\\0\\0\\1\\1\\0\\1\end{pmatrix}$.
est engendré par X^3+X+1

Rque 48 Si $\rho_1,\dots,\rho_r$ sont les racines de g dans un corps de décomposition. Alors $c\in\mathcal{C}$ ssi $c(\rho_i)=0\ \forall i\in\{1,\dots,r\}$.

Pb : déterminer les diviseurs de X^n-1.
Soit α une racine dans une extension de $\mathbb{F}_q$.

Propo 49 Soit $\Sigma \subseteq [\![0,n-1]\!]$ et $g_\Sigma = \prod_{i\in\Sigma}(X-\alpha^i)$.
Alors $g_\Sigma \in \mathbb{F}_q[X] \iff \Sigma$ est stable par $\times q$.

Propo 50 Si $a+1,\dots,a+s\in\Sigma$ alors $d\geq s+1$.

IV - Algèbre linéaire et bilinéaire

[PER]

1) Groupes linéaires

Propo 51 [Cardinaux des groupes linéaires sur $\mathbb{F}_q$]
$|GL_n(q)| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$
$|SL_n(q)| = |GL_n(q)|/q-1$
$|PGL_n(q)| = |SL_n(q)|$.

Ex 52 $PGL_2(3)\simeq S_4$.

2) Formes quadratiques sur $\mathbb{F}_q$ ($p\neq 2$)

Thm 53 Soit E un k-ev de dim n,
Soit $\alpha\in\mathbb{F}_q^\times\setminus\mathbb{F}_q^{\times 2}$. Il y a deux classes d'équivalence de f.q non dégénérées sur E, de matrices
$Q_1 = I_n$, $Q_2 = \begin{pmatrix}1 & & \\ & \ddots & \\ & & \alpha\end{pmatrix}$

~~férences~~ PERRIN
GOZARD
Saux-Picart (Corps finis)
Demazure
Serre
OA

velopements possibles

- Existence & unicité des corps finis
- Théorème de Frobenius-Zolotarev
- Réciprocité quadratique
- Polynômes irréductibles sur $\mathbb{F}_q$ & inversion de Möbius
- Berlekamp
- Chevalley-Warning