L 112

Corps finis. Applications.

On suppose les corps commutatifs en vertu du théorème de Wedderburn.

I. Structure des corps finis

1) Caractéristique et cardinal.

Déf caractéristique Soit $\varphi : \mathbb{Z} \to K ; n \mapsto \underbrace{1+\dots+1}_{n \text{ fois}}$

Ker φ est un idéal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$, $p \in \mathbb{N}$

[PER] et $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im}\varphi$ donc $p\mathbb{Z}$ est premier donc $p = 0$ ou p est premier.

p est appelé caractéristique de K, notée $\operatorname{car}(K)$.

Prop : Si K est fini :

[PER] . $\operatorname{car}(K) = p > 0$, p premier.

. $\mathbb{Z}/p\mathbb{Z}$, noté $\mathbb{F}_p$, est le plus petit sous-corps de K, appelé sous-corps premier de K.

Rq Si K est une extension de $\mathbb{F}_p$ alors K est un $\mathbb{F}_p$-ev donc $|K| = q = p^n$.

[PER] Le cardinal d'un corps fini est une puissance d'un nombre premier.

2) Construction.

Lem Soit K un corps avec $\operatorname{car}(K) = p > 0$. L'application

[PER] $F : K \to K ; x \mapsto x^p$ est un automorphisme de corps, appelé automorphisme de Frobénius.

Thm : existence. Soit p premier, soit $n \in \mathbb{N}$. On pose $q = p^n$.

[PER] Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.

Thm : unicité Deux corps à q éléments sont isomorphes.

[PER] On note un représentant $\mathbb{F}_q$.

Ex . $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ sont des corps finis.

. un anneau fini et intègre est un corps.

Dans la suite on notera $q = p^n$ avec p premier et $n \in \mathbb{N}$.

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

[PER] Thm Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique. (isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$)

Cor : théorème de l'élément primitif

[GOZ] Quel que soit q, il existe $\alpha \in \mathbb{F}_q^*$ tq $\mathbb{F}_q = \mathbb{F}_p(\alpha)$.

App° représentation des corps finis (agréable pour la multiplication)

Ex $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$

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

Thm Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre

[PER] $n = [\mathbb{F}_q : \mathbb{F}_p]$. Il est engendré par l'automorphisme de Frobénius.

5) Sous-corps et clôture algébrique

[GOZ] Thm K est un sous-corps de $\mathbb{F}_q \iff$ il existe d diviseur de n tq $\operatorname{car}(K) = p^d$.

[GOZ] Prop $\mathbb{F}_q$ n'est jamais algébriquement clos.

6) Carrés de $\mathbb{F}_q$

Prop Pour $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

[PER] et Pour p premier, $p > 2$, il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$

$x \in \mathbb{F}_q^2 \iff x^{\frac{q-1}{2}} = 1$.

Cor p premier, $p > 2$. Alors -1 est un carré dans $\mathbb{F}_q$

[PER] ssi $q \equiv 1 \ [4]$

App°. Il existe une infinité de nombres premiers de la

[PER] forme $4m + 1$.

[PER] . théorème des deux carrés : soit p un nombre premier. p est somme de deux carrés ssi $p = 2$ ou $p \equiv 1 \ [4]$.

Prop : résidus quadratiques

Caractère quadratique $\left(\frac{\alpha}{\mathbb{F}_q}\right) = \begin{cases} 0 & \text{si } \alpha = 0 \\ 1 & \text{si } \alpha \text{ carré dans } \mathbb{F}_q^* \\ -1 & \text{sinon} \end{cases}$

[MIG] Cela correspond au symbole de Legendre quand $n = 1$

$\left(\frac{\alpha}{\mathbb{F}_p}\right) = \left(\frac{\alpha}{p}\right)$

Prop p premier. $\left(\frac{\alpha\beta}{\mathbb{F}_q}\right) = \left(\frac{\alpha}{\mathbb{F}_q}\right)\left(\frac{\beta}{\mathbb{F}_q}\right)$; $\left(\frac{\alpha}{\mathbb{F}_q}\right) = \alpha^{\frac{q-1}{2}}$

$\left(\frac{2}{\mathbb{F}_q}\right) = (-1)^{\frac{q^2-1}{8}}$

Prop : loi de réciprocité quadratique (cas particulier)
Soient ℓ et p premiers impairs distincts.
[HIG] $\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{\ell-1}{2}\cdot\frac{p-1}{2}}$

II. Corps finis et polynômes

1) Polynômes irréductibles sur $\mathbb{F}_q$

Intérêt : représentation des corps $\mathbb{F}_q$.

Thm Soit Π un polynôme de degré n sur $\mathbb{F}_p$, irréductible
[GOZ] Alors $\mathbb{F}_q = \mathbb{F}_p[X]/(\Pi)$

Ex. $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$
Si on note α la classe de X, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$
→ on a une représentation agréable pour l'addition

Question Existe-il des polynômes irréductibles de tout degré sur $\mathbb{F}_p$?

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

On a même le résultat :

Thm On note $I(n,q)$ le nombre de polynômes irréductibles de degré n sur $\mathbb{F}_q$.
Alors $I(n,q) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$
[FG] avec μ définie par :
$\mu(1) = 1$
$\mu(p_1 \dots p_k) = (-1)^k$ si les p_i sont premiers distincts
$\mu(n) = 0$ sinon.
μ est la fonction de Möbius [DVPT]

Thm : algorithme de Berlekamp

Soit $P \in \mathbb{F}_q[X]$ un polynôme dont la décomposition en polynômes irréductibles est sans facteurs carrés.
[D.A] Définissons $\alpha = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$, et considérons la base $\mathcal{B} = (1, \alpha, \dots, \alpha^{\deg(P)-1})$ de $\mathbb{F}_q[X]/(P)$.
Alors le processus suivant s'arrête au bout d'un nb fini d'étapes et donne la décomposition en facteurs irréductibles de P.

1) Soit $S_p : \mathbb{F}_q[X]/(P) \to \mathbb{F}_q[X]/(P)$ (bien définie et linéaire). $Q(X) \bmod P \mapsto Q(X^q) \bmod P$
On calcule $S_p - Id$ dans $\mathcal{B}$ puis on passe au 2).

2) Le nb de facteurs irréductibles de P est :
$r = \dim(\ker(S_p - Id)) = \deg(P) - \operatorname{rg}(S_p - Id)$
Si $r = 1$, P irréductible et on arrête l'algorithme.
Sinon on passe au 3),

3) On calcule un polynôme V non congru à un polynôme constant modulo P et tq $V \bmod P \in \ker(S_p - Id)$.
Avec l'algorithme d'Euclide on calcule ensuite les $PGCD(P, V-\alpha)$. On a alors $P = \prod_{\alpha \in \mathbb{F}_q} PGCD(P, V-\alpha)$
On retourne au 1) avec chacun de ses facteurs non triviaux. [DVPT]

Rq On peut en déduire un algorithme de décomposition pour les polynômes quelconques.

2) Critères d'irréductibilité des polynômes

Idée : regarder des polynômes modulo p pour en déduire des informations sur l'irréductibilité sur le corps initial.

Thm réduction modulo p. Soient $P \in \mathbb{Z}[X]$ et $\bar{P}$ sa réduction
[PER] modulo p. On suppose $\bar{a}_n \neq 0$ dans $\mathbb{F}_p$ (a_n coefficient dominant). Alors si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, le polynôme P
[GOZ] est irréductible sur $\mathbb{Q}$, et même sur $\mathbb{Z}$ si P est unitaire.

Ex. $X^3 + 462X^2 + 2433X - 69691$ est irréductible sur $\mathbb{Z}$.
(mod 2 on a X^2+X+1)

App $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Thm Soit $P \in K[X]$ de degré $n > 0$. Alors P est irréductible
[PER] sur K ssi P n'a pas de racines dans les extensions L de K qui vérifient : $[L:K] \leq n/2$.

Ex. $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Rq Il n'y a pas de réciproque à la méthode de réduction : X^4+1 irréductible sur $\mathbb{Z}$, mais réductible sur $\mathbb{F}_p$, p premier.

3) Polynômes cyclotomiques et applications

Déf racine primitive Soit k un corps et $n \in \mathbb{N}$. On considère $P_n(X) = X^n - 1$, et soit K_n le corps de décomposition de P_n sur k. Une racine n-ème primitive de 1 est un élément ζ de K_n tq $\zeta^n = 1$ et $\zeta^d \neq 1$ pour $d < n$. Leur ensemble sera noté $\mu_n^*(K_n)$.

[PER] Déf polynôme cyclotomique Le n-ème polynôme cyclotomique $\Phi_{n,k} \in K_n[X]$ est donné par :

$$\Phi_{n,k}(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$$

Rq $\Phi_{n,k}$ est unitaire de degré $\varphi(n)$

[PER] Prop On a la formule : $X^n - 1 = \prod_{d \mid n} \Phi_{d,k}(X)$.

App° . théorème de Wedderburn : Tout corps fini est commutatif.

[PER] . cas particulier du théorème de Dirichlet :

[GOZ] il existe une infinité de nb premiers de la forme $\lambda n + 1$, $\lambda \in \mathbb{N}^*$.

. Pour $k = \mathbb{F}_p$.

théorème : . les générateurs de $\mathbb{F}_q^*$ sont les zéros de $\Phi_{q-1, \mathbb{F}_p}(X)$.

[GOZ] . les polynômes irréductibles des générateurs de $\mathbb{F}_q^*$ sont les diviseurs irréductibles de $\Phi_{q-1, \mathbb{F}_q}(X)$ dans $\mathbb{F}_p[X]$ et sont appelés polynômes primitifs de $\mathbb{F}_q$. Ils sont de degré n et chacune de leurs racines engendre $\mathbb{F}_q^*$.

III. Applications géométriques

1) Groupe linéaire sur $\mathbb{F}_q$

Prop Les cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont :

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

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

3) $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)| = N$

4) $|PSL_n(\mathbb{F}_q)| = N/d$ où $d = PGCD(n, q-1)$

Dans le cas des corps de petits cardinaux on a :

Prop 1) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

[PER] 2) $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$; $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$.

3) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$

4) $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$; $PSL_2(\mathbb{F}_5) \simeq \mathcal{A}_5$.

2) Formes quadratiques sur les corps finis.

Thm Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2 et E un $\mathbb{F}_q$-ev de dim° m. Soit $\alpha \in \mathbb{F}_q^*$, $\alpha \notin \mathbb{F}_q^{*2}$.

Il y a deux classes d'équivalences de formes quadratiques

[PER] non dégénérées sur E, de matrices :

$$Q_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \quad \text{et} \quad Q_2 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \alpha \end{pmatrix}$$

Une forme quadratique Q est de l'un ou l'autre type suivant que son déterminant $\delta(Q)$ est un carré ou non de $\mathbb{F}_q^*$.

3) Nombre de solutions d'équations dans $\mathbb{F}_q$

Thm : Chevalley-Warning Soit $\mathbb{F}_q$ un corps fini de caractéristique p. Si $P \in \mathbb{F}_q[x_1, \dots, x_n]$ avec $\deg(P) < n$

[HIN] alors $\operatorname{card}\{x \in \mathbb{F}_q^n \mid P(x) = 0\} \equiv 0 \bmod p$

En particulier, si P est homogène de degré $d < n$, alors P possède un zéro non trivial (i.e distinct de 0).

Thm Soit Q une forme quadratique en n variables, non

[HIN] dégénérée, à coefficient dans $\mathbb{F}_p$ où $p \neq 2$. Alors

$$\operatorname{card}\{x \in (\mathbb{F}_p)^n \mid Q(x) = 0\} = p^{n-1} + \varepsilon(p-1)p^{\frac{n}{2}-1}$$

avec $\varepsilon = \begin{cases} 0 \text{ si } n \text{ impair} \\ \left(\frac{(-1)^{n/2}\delta(Q)}{p}\right) \text{ si } n \text{ pair.} \end{cases}$

Rq Il existe une généralisation dans $\mathbb{F}_q$.

Réf :

Marc Hindry	Arithmétique	[HIN]
Ivan Gozard	Théorie de Galois	[GOZ]
Daniel Perrin	Cours d'Algèbre.	[PER]
V. Beck	Objectif Agrégation	[OA]
Maurice Mignotte	Algèbre Concrète.	[MIG]

⊕ Serre, cours d'arithmétique ⊕ Cohen

On aurait pu parler de :

- codes correcteurs (cf leçon de l'an dernier)
- tests de primalité
- géométrie projective.

Autres développements :

- Chevalley - Warning
- Somme de Gauss et nb de vecteurs isotropes d'une forme quadratique non dégénérée sur $\mathbb{F}_p$. (dernier thm).

- Complexité de Berlekamp ?
- Somme des puissances $n^{ième}$ des elts d'un corps finis.

$$\sum_{a \in \mathbb{F}_q} a^m$$

si $m = 0$ ça fait $\sum_{\mathbb{F}_q} 1 = q = 0$

si $m = 0 \to 0$

Si $m | q$ (distinguer les cas si m est ...)

$q | m \to -1$

... L Chambert

- $X^4 + 1$ irred sur $\mathbb{Z}$ ms red sur $\mathbb{F}_p$ $\forall p$.

Généralisation ?

$X^4 + 1$ est cyclotomique déjà.

Peut-on dire que ts les pol cyclo vérifient ça ?

↳ difficile..

- 2 pol irred sur $\mathbb{F}_7$

$X^2 - 2X + 3$ $\quad \mathbb{F}_7/\langle\rangle$

$X^2 + 3X + 1$ $\quad \mathbb{F}_7/\langle\rangle$

↳ expliciter l'isom. ($\mathbb{F}_{49}$ ds les 2 cas).

Rq

- dvp Berlekamp : raccourcir le début ⊕ donner un ex détailler les étapes de l'algo.
- plan : bien.
- Les carré c'est incontournable symbole de Legendre et tout
- on peut faire ⊕ de géom. (prop sur les corps fini par ex)
- pol cyclo : pas trop s'éloigner du sujet ⚠
- savoir la complexité de l'algo qu'on présente !
- On peut parler du corps de Conway !