123

Corps finis - Applications

I Construction des corps finis

1) Premiers résultats

Déf : Soit un corps K supposé commutatif.
Soit le morphisme d'anneau $\varphi\begin{pmatrix} \mathbb{Z} \to K \\ n \mapsto n \cdot 1_K \end{pmatrix}$
Alors $\ker(\varphi)$ est un idéal de $\mathbb{Z}$ donc de la forme $p\mathbb{Z}$ où $p \in \mathbb{Z}$.
Cet entier p est appelé la caractéristique du corps K et on la note $car(K)$.

Ppté : $p \in \mathbb{P}$ ou $p = 0$ (car $K \simeq \mathbb{Z}/p\mathbb{Z}$ et K est un corps)

Désormais tous les corps sont supposés commutatifs et finis

Ppté : $car(K) \in \mathbb{P}$ (car sinon $K \simeq \mathbb{Z}$ infini)

Rq : La réciproque est fausse ! Prendre $\mathbb{F}_p(X)$.

Ppté : $|K| = p^n$ où $p \in \mathbb{P}$, $n \in \mathbb{N}$ (pas de corps à 6 éléments)
(K est un $\mathbb{Z}/car(K)\mathbb{Z}$ - ev de dim finie n d'où $|K| = p^n$)

Déf : $F\begin{pmatrix} K \to K \\ x \mapsto x^p \end{pmatrix}$ est un morphisme de corps appelé l'automorphisme de Frobenius

Rq : C'est un automorphisme et si $K = \mathbb{Z}/p\mathbb{Z}$, $F = Id$

2) Existence et unicité des corps finis

Déf : Pour $P \in K[X]$, le corps de décomposition de P sur K est une extension L de K tq
- P est produit de facteurs de degré 1 dans $L[X]$
- L est un corps minimal pour cette propriété (il est unique à iso près)

Th : Soit $p \in \mathbb{P}$ et soit $n \in \mathbb{N}^*$ et on pose $q = p^n$
- Il existe un corps K a q éléments : le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$ convient
- Ce corps est unique à isomorphisme près (1)

Notation : On le note $\mathbb{F}_q$

Ex : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(1+X+X^2)$ et $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^8-X)$
$\simeq \mathbb{F}_2[X]/(X^4-X)$ $\simeq \mathbb{F}_2[X]/(X$

3) Théorème de Wedderburn

DEV 1

Th : Tout anneau fini non réduit à $\{0\}$ dans lequel tout élément non nul est inversible est un corps.

Rq : On avait pas besoin de supposer K fini et commutatif

II Propriétés des corps finis

1) Le groupe $\mathbb{F}_q^*$ et les sous-corps de $\mathbb{F}_q$

Th : Le groupe multiplicatif de tout corps fini est cyclique
càd $\forall p \in \mathbb{P}$, $\forall n \in \mathbb{N}$, $\mathbb{F}_{p^n}^*$ est cyclique (2)

Cor : Tout sous-groupe de K^* où K corps quelconque est cyclique.

Rq : Il reste difficile de déterminer des générateurs pour $\mathbb{F}_q$
En particulier $\mathbb{F}_{p^n}^* \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}$

Th : Soient $p \in \mathbb{P}$ et $n \in \mathbb{N}^*$. Alors : (3)
$\mathbb{F}_{p^s}$ est un sous-corps de $\mathbb{F}_{p^n}$ si et ssi $s \mid n$

col

Coro : $\mathbb{F}_{p^n}$ est ~~le~~ corps de décomposition du polynôme $X^{p^n} - X$ sur $\mathbb{F}_p$.

Rq : On peut voir $\mathbb{F}_{p^n}$ de plusieurs façons !

Coro : Tout générateur de $\mathbb{F}_{p^n}^*$ est un élément primitif de $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ pour -s(m c.a.d $\mathbb{F}_{p^n} = \mathbb{F}_p(\omega)$ tq(?) et en particulier $\mathbb{F}_{p^n} = \mathbb{F}_p(\omega)$ (le th de l'élt primitif assure son existence !)

Rq : La réciproque est fausse !

Ex : $\mathbb{F}_8^* \simeq \mathbb{Z}/7\mathbb{Z}$ donc $\forall \omega \in \mathbb{F}_8^*$, $\mathbb{F}_8 = \mathbb{F}_2(\omega)$

2) Polynômes à coefficients dans $\mathbb{F}_q$ (4)

Rq : $\mathbb{F}_q$ n'est pas algébriquement clos (5)

Prop : Soit $q = p^d$. Soient $\mathcal{I}_n(n,q) = \{P \in \mathbb{F}_q[X] \mid d°(P) = n$, P unitaire et P irréductible$\}$ et $I(n,q) = |\mathcal{I}_n(n,q)|$.

Alors :

DEV2
- $X^{p^n} - X = \prod_{d|n} \prod_{P \in \mathcal{I}(d,q)} P$
- $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$ où μ fct de Möbius
- $I(n,q) \geq 1 \quad \forall n \in \mathbb{N}^*$
- $I(n,q) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$ qd n tend vers $+\infty$

(Rq : Si $x = q^n$, on obtient $I(x,q) \sim \frac{x}{\log_q(x)}$ un analogue (6) au th des nombres premiers (i.e. un th des nbr pour les polynômes))

Soit n tq $n \wedge q = 1$ et $K = \mathbb{F}_q$, $q = p^d$

Def : Soit $P_n(X) = X^n - 1 \in K[X]$ et $K_n \simeq K[X]/(P_n)$ un corps de décomposition de P_n sur K.

Soit $\mu_n(K_n)$ le sous-groupe (fini) de $(K_n^*, \times)$ formé des racines de P_n (il est de cardinal n) et soit $\mu_n^*(K_n)$ l'ensemble des générateurs de $\mu_n(K_n)$ (il est de cardinal $\varphi(n)$) et ses éléments sont appelés racines primitives $n$ième de l'unité)

Def : Le $n$ième polynôme cyclotomique sur K est défini par
$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*(K_n)} (X - \zeta)$$

Ppté : $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Prop : Les facteurs irréductibles de $\Phi_n(X)$ de $\mathbb{F}_q[X]$ sont tous de même degré, égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$ (7)

3) Etude des carrés de $\mathbb{F}_q$ (8)

Def : Soit $q = p^n$, $n \in \mathbb{N}^*$, $p \in \mathcal{P}$. Un carré x de $\mathbb{F}_q$ est un élément de $\mathbb{F}_q$ tq : $\exists y \in \mathbb{F}_q$ tq $y^2 = x$

Prop : Dans $\mathbb{F}_2$, tous les éléments sont des carrés.
Dans $\mathbb{F}_q$, $q > 2$, il y a autant de carrés que de non carrés et il y en a $\frac{q+1}{2}$. (9)

Def : Pour $p \in \mathcal{P} \setminus \{2\}$ et pour $a \in \mathbb{Z}$, on définit le symbole de Legendre par $\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & \text{si } a \text{ est un carré de } \mathbb{F}_p^* \\ -1 & \text{sinon} \end{cases}$

($\left(\frac{0}{p}\right) = 0$ et $\left(\frac{1}{p}\right) = 1$)

Th : Pour $p \in \mathcal{P} \setminus \{2\}$ et $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$

Rq : Par définition, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Loi de réciprocité quadratique : Soient p, p' éléments de $\mathcal{P} \setminus \{2\}$.
Alors $\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{p-1}{2}\frac{p'-1}{2}}$

Prop : Pour $p \in \mathcal{P} \setminus \{2\}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Def : Pour m impair avec $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, on définit pour $a \in \mathbb{Z}$ le symbole de Jacobi par $\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{\alpha_i}$

Si $\left(\frac{a}{m}\right)$ vaut 1, a est un carré dans $\mathbb{F}_m$

Propos : Les énoncés se généralisent au symbole de Jacobi.

Coro : -1 est un carré de $\mathbb{F}_p$ ssi $\begin{cases} p=2 \\ \text{ou} \\ p\equiv 1\ [4] \end{cases}$

Ex : $\left(\frac{11}{123}\right) = \left(\frac{123}{11}\right) \times (-1)^{5\times 61} = -\left(\frac{3}{11}\right)\left(\frac{41}{11}\right) = -\left(\frac{3}{11}\right)\left(\frac{8}{11}\right) = 1$

Donc 11 est un carré modulo 123

III Applications des corps finis

1) Une version faible de Dirichlet

Th : Soit $n \in \mathbb{N}$; il existe une infinité de nombres premiers congrus à 1 modulo n

Rq : La version forte est qu'il existe une infinité de nombres premiers congrus à a modulo b où $a \wedge b = 1$

Utilise la réduction du polynôme cyclotomique Φ_n dans $\mathbb{F}_p[X]$

2) Théorème des deux carrés

Th : Soit $n \in \mathbb{N} \setminus \{0,1\}$ avec $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

Alors n est la somme de deux carrés si $\forall i \in [\![1,r]\!]$ tel que $p_i \equiv 3\ [4]$, α_i est pair

En particulier, $p \in \mathcal{P}$ est somme de deux carrés si et ssi $p=2$ ou $p \equiv 1\ [4]$

Rq : On montre que $p \in \mathcal{P}$ somme de deux carrés si et ssi -1 est un carré dans $\mathbb{F}_p$ ce qu'on a déduit précédemment

3) Premier théorème de Sylow

Pté : $|GL_n(\mathbb{F}_p)| = \prod_{k=0}^{n-1} (p^n - p^k)$ pour $n \in \mathbb{N}^*$ et $p \in \mathcal{P}$ (1)

$= p^{\frac{n(n-1)}{2}} \times m$ où $m \nmid p$

Rq : Pour G un groupe fini de cardinal $p^\alpha m$ où $m \nmid p$ un p-sous-groupe de Sylow de G est un sous-groupe de G de cardinal p^α.

Pté : $GL_n(\mathbb{F}_p)$ admet un p-sous-groupe de Sylow (2)

Th : Soit G un groupe fini, soit $p \in \mathcal{P}$ tq $p \mid |G|$

Alors G possède un p-sous-groupe de Sylow

Rq : On utilise le résultat sur $GL_n(\mathbb{F}_p)$ en plongeant G dans $S_{|G|}$ puis dans $GL_n(\mathbb{F}_p)$

4) Formes quadratiques sur $\mathbb{F}_q$

Références : PERRIN
CALAIS (Anneaux)
CALDERO - GERMONI

(1) $\mathbb{Z}/p\mathbb{Z}[X]/(X^q - X)$ a bien q éléments car ces éléments sont toutes les racines de $X^q - X$ qui sont toutes distinctes (distinctes par dérivation) et de nombre $= d°(X^q - X) = q$
+ propriété du corps de déc qui assure que ces éléments forment $\mathbb{F}_q$

(2) Utiliser la notion d'exposant et le fait que $x^q = 1$ a q solutions distinctes

(3) Utiliser le lemme d'arithmétique $X^s - 1 \mid X^n - 1 \iff s \mid n$

(4) Étude justifiée par le critère de réductibilité qui rapporte la réductibilité des polynômes dans $\mathbb{Z}$ modulo p + résultat

(5) Étude $X^{p^{n+1}} - X$ dans $\mathbb{F}_{p^n}$

On a $(X^{p^{n+1}} - X)$ à racines simples car
$(X^{p^{n+1}} - X)' = p^{n+1} X^{p^{n+1}-1} - 1 = -1$ (car $\mathrm{car}\,\mathbb{F}_{p^n} = p$)
et si $\mathbb{F}_{p^n}$ scindé, on aurait $X^{p^{n+1}} - X$ polynôme scindé avec p^{n+1} racines distinctes $> |\mathbb{F}_{p^n}|$!

(6) Analogue au th des nombres premiers
+ Interprétation à la question : si je tire un polynôme unitaire de degré n dans $\mathbb{F}_q$, proba qu'il soit irréductible ? $= 1/n$!

(7)

8) Permet l'étude des irréductibles des anneaux $\mathbb{Z}[i\sqrt{d}]$

(9) $f\left(\begin{array}{ccc}\mathbb{F}_q^* & \to & \mathbb{F}_q^* \\ x & \mapsto & x^2\end{array}\right)$ morphisme de groupes et $\ker(f) = \{\pm 1\}$ donc si $q > 2$: $\mathrm{Im}(f) = \frac{|\mathbb{F}_q^*|}{|\ker(f)|} = \frac{q-1}{2}$
+ 1 dans $\mathbb{F}_q$ car on rajoute 0

(11) On a $p^n - 1$ choix puis $p^n - p$ (col de (1) etc.) Σ de suite arit.
et $\prod_{k=0}^{n-1} p^n - p^k = \ldots p \times p^2 \ldots \times p^{n-1} \times \pi = p^{\frac{n(n-1)}{2}} \pi$

(11) Prendre $H = \left\{ \begin{pmatrix} 1 & a_{ij} \\ 0 & 1 \end{pmatrix}, a_{ij} \in \mathbb{F}_p \right\} < GL_n(\mathbb{F}_p)$
et $|H| = p^{\frac{n(n-1)}{2}}$!