123 | Corps finis, applications

I - Construction et structure

1) Structure a priori

Def 1: On appelle corps fini tout corps K de cardinal fini.

Prop 2: (i) $K^\times$ le groupe multiplicatif de K est cyclique
(ii) Sa caractéristique est un nombre premier p
(iii) Son sous-corps premier est isomorphe à $\mathbb{F}_p$.
(iv) K est muni d'une structure de $\mathbb{F}_p$-espace vectoriel de dimension finie.

Coro (iv) 3: $\underbrace{|K|}_{=:q} = p^n$, $n \in \mathbb{N}^*$.

Ex 4: $\mathbb{Z}/p\mathbb{Z}$ avec p premier, $\mathbb{F}_p[X]/(P)$ où P est $\mathbb{F}_p$-irréductible

Def 5: $\sigma : \begin{array}{l} K \to K \\ x \mapsto x^p \end{array}$ est un morphisme de corps appelé ~~auto~~morphisme de Frobenius.

Prop 6: σ est un automorphisme (c-ex : $K = \mathbb{F}_p[X]$)

Prop 7: $\forall r \in \mathbb{N}$, $\mathrm{Fix}(\sigma^r)$ est un sous-corps de $\mathbb{F}_q = K$.

Prop 8: $\mathrm{Aut}(\mathbb{F}_q)$ est cyclique engendré par le Frobenius.

Thm 9: Un corps est fini de cardinal $q = p^n$ si et seulement si il est corps de décomposition sur $\mathbb{F}_p$ de $X^{p^n} - X$. En particulier, il est unique à $\mathbb{F}_p$-isomorphisme près.

2) Structure du groupe multiplicatif, élément primitif

Thm 10: Un sous groupe fini du groupe multiplicatif d'un corps est cyclique.

Coro 11: Le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique.

Ex 12: $\mathbb{F}_9 \simeq \dfrac{\mathbb{F}_3[X]}{\langle X^2+X-1\rangle}$ $\quad \overline{X}$ est générateur de $\mathbb{F}_9^\times$

Prop 13: Si θ engendre $\mathbb{F}_q^\times$ (un tel élément existe coro 11) alors $\mathbb{F}_q = \mathbb{F}_p[\theta]$.

Rem 14: La réciproque est fausse : $\mathbb{F}_9 \simeq \dfrac{\mathbb{F}_3[X]}{\langle X^2+X-1\rangle} \simeq \mathbb{F}_3[2+\alpha]$ et $2+\alpha$ d'ordre 4 ($\alpha := \overline{X}$).

Thm 15 (de l'élément primitif) : Soit K un corps fini. Soit L une extension de degré fini de K, alors il existe $\xi \in L$ tel que $L = K(\xi)$. Un tel élément est appelé élément primitif de L.

Prop 16: Si θ est élément primitif de $\mathbb{F}_q$ alors $(1, \theta, \dots, \theta^{n-1})$ est une $\mathbb{F}_p$-base de $\mathbb{F}_q$.

3) Sous-corps d'un corps fini

Thm 17 (de la base télescopique) : Soit K un corps, k sous corps de K, E un K-espace vectoriel de base $(e_i)_{i\in I}$ et $(\lambda_j)_{j\in J}$ une base de K en tant que k-espace vectoriel. Alors $(\lambda_j e_i)_{(i,j)\in I\times J}$ est une base de E en tant que k-ev.
Dans le cas des corps finis, $[E:k] = [E:K][K:k]$.

Lemme 18: $X^{p^n} - X \mid X^{p^m} - X$ si et seulement si $n \mid m$.

Prop 19: Il existe un sous-corps de $\mathbb{F}_{p^n}$ à p^r éléments ssi $r \mid n$, et dans ce cas il est égal à $\mathrm{Fix}(\sigma^r)$.

Ex 20: les sous corps de $\mathbb{F}_{2^{30}}$:

$$\begin{tikzcd}
 & \mathbb{F}_{2^{30}} & \\
\mathbb{F}_{2^{15}} \arrow[ur] & \mathbb{F}_{2^{6}} \arrow[u] & \mathbb{F}_{2^{10}} \arrow[ul] \\
\mathbb{F}_{2^{5}} \arrow[u] \arrow[urr] & \mathbb{F}_{2^{3}} \arrow[ul] \arrow[u] & \mathbb{F}_{2^{2}} \arrow[ul] \arrow[u] \\
 & \mathbb{F}_{2} \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

II - Polynômes

1) Constructions ~~pr~~ pratiques, calculs

Prop 21 : $\mathbb{F}_q / \mathbb{F}_p$ est finie donc algébrique, donc tout élément possède ~~le~~ un polynôme minimal qui est $\mathbb{F}_p$-irréductible.

Prop 22 : Si α est élément primitif et Π son polynôme minimal alors $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\Pi)$ et $q = p^{\deg \Pi}$.

Prop 23 : Soit $P \in \mathbb{F}_p[X]$ irréductible de degré d, alors $\mathbb{F}_p[X]/(P)$ est un corps à p^d éléments.

Rem 24 : $\overline{X}$ est élément primitif, et le polynôme minimal de $\overline{X}$ est P.

Prop 24 : Une base de $\mathbb{F}_p[X]/(P)$ est donnée par $(\overline{1}, \overline{X}, \dots, \overline{X}^{d-1})$

Ex 25 : $\mathbb{F}_4 \simeq \dfrac{\mathbb{F}_2[X]}{\langle X^2+X+1 \rangle} = (0, 1, \alpha, 1+\alpha)$ $\quad \alpha = \overline{X}$

Tables de calculs

+	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1		0	$1+\alpha$	α
α			0	1
$1+\alpha$				0

×	0	1	α	$1+\alpha$
0	0	0	0	0
1		1	α	$1+\alpha$
α			$1+\alpha$	1
$1+\alpha$				α

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

Prop 26 : ~~Soit~~ $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$ où P est le polynôme minimal d'un élément primitif de $\mathbb{F}_q$

Coro 27 : Il existe des polynômes irréductibles de tout degrés sur $\mathbb{F}_p$.

C-ex 28 : $K = \mathbb{R}$ ou $\mathbb{C}$, les irréductibles sont de degré ≤ 2.

Prop 29 : Si P est un polynôme irréductible de degré n sur $\mathbb{F}_p$, alors P divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ donc est scindé sur $\mathbb{F}_{p^n}$ et son corps de rupture $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(P)$ est aussi son corps de décomposition

Prop 30 : Facteurs irréductibles de $X^{p^n} - X$:

$$X^{p^n} - X = \prod_{d \mid n} \prod_{\substack{Q \text{ irréductible} \\ \text{de degré } d}} Q(X)$$

Application 31 : Générateur de $\mathbb{F}_9^* \simeq \left(\dfrac{\mathbb{F}_3[X]}{\langle X^2+X-1 \rangle}\right)^*$

$X^9 - X = X(X^8-1) = X(X^4-1)(X^4+1)$

$\varphi(8) = 4$ donc les générateurs sont les racines de X^4+1.

$(\mathbb{F}_9^\times = \{$ racines de $X^8-1\})$

Prop 32 (Algorithme de Berlekamp) Soit $P \in \mathbb{F}_q[X]$ dont la décomposition en irréductibles est sans facteurs carrés : $P = \prod_{i=1}^{r} P_i$.

(i) Le nombre de facteurs irréductibles de P est $r = \dim(\operatorname{Ker}(S_p - Id))$ où $S_p : \mathbb{F}_q[X]/(P) \to \mathbb{F}_q[X]/(P)$, $\overline{Q(X)} \mapsto \overline{Q(X^q)}$

(ii) $\exists V$ non congru modulo P à un polynôme constant de $\mathbb{F}_q[X]$ tel que $\overline{V} \in \operatorname{Ker}(S_p - Id)$ et $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$

Application 33 : Factorisation d'un polynôme $P \in \mathbb{F}_q[X]$.

1. Si P est constant, fin.
2. - si $\operatorname{pgcd}(P, P') = 1$, appliquer Berlekamp à P
   - si $\operatorname{pgcd}(P, P') = P$, calculer R tel que $R^p = P$, retourner en 1 avec $P = R$.
   - sinon ~~Revenir~~ Revenir en 1 avec $P_1 = \operatorname{pgcd}(P, P')$ et $P_2 = \dfrac{P}{P_1}$.

DEV1

III Carrés, formes quadratiques

1) étude de l'ensemble des carrés de $\mathbb{F}_q$

def 34 On note $\mathbb{F}_q^2 = \{x^2 / x \in \mathbb{F}_q\}$, $\mathbb{F}_q^{*2} = \{x^2 / x \in \mathbb{F}_q^*\}$

prop 35 Si $p = 2$, $q = 2^m$ $(m \geq 1)$ alors
$\forall x \in \mathbb{F}_q, \; x^{2^m} = x \Rightarrow x = (x^{2^{m-1}})^2$

prop 36 Si $p \geq 3$, $\mathbb{F}_q^{*2}$ est un sous groupe d'indice 2 de $\mathbb{F}_q^*$ et donc $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$

prop 37 $\forall x \in \mathbb{F}_q^*$, $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$ $\quad (p \neq 2)$

def 38 Symbole de Legendre : $\left(\frac{m}{p}\right) = \begin{cases} 1 \text{ si } m \text{ carré modulo } p \\ 0 \text{ si } p \mid m \\ -1 \text{ sinon} \end{cases}$

Si $\left(\frac{m}{p}\right) = 1$ on dit que m est résidu quadratique modulo p.

rmq 39 $\left(\frac{m}{p}\right) \equiv m^{\frac{p-1}{2}} [p]$ $\quad (p \geq 3)$

prop 40 $\forall m \in \mathbb{Z}, n \in \mathbb{Z}$, $\left(\frac{mp+n}{p}\right) = \left(\frac{n}{p}\right)$

$\forall m, n \in \mathbb{Z}$, $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$

prop 41 $\left(\frac{\cdot}{p}\right)$ est l'unique morphisme de groupe non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$

coro 42 $m \in \mathbb{Z}$ est résidu quadratique modulo $p \geq 3$
$\Leftrightarrow m^{\frac{p-1}{2}} \equiv 1 [p]$

coro 43 -1 est un carré ~~modulo~~ dans $\mathbb{F}_q^* \Leftrightarrow q \equiv 1 [4]$

thm 44 Loi de réciprocité quadratique $\forall p, q \in \mathbb{P}$, impairs
$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$

1ère loi complémentaire $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

2ème loi complémentaire $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

thm 45 théorème de Frobenius - Zolotarev — DEV ②
Si $p \in \mathbb{P}$, $p \geq 3$, $m \geq 1$, $q = p^m$; si $u \in GL(\mathbb{F}_q)$, alors
$\varepsilon(u) =$ ~~permut~~ signature de u en tant que permutation de $\mathbb{F}_q$
$= \left(\frac{\det u}{p}\right)$

46 application : calcul de $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$

exemples 47 : calculs de symboles de Legendre : $\left(\frac{12}{23}\right)$, par exemple

prop 48 si $p \equiv 3 [4]$, $a \in \mathbb{Z}$, alors $(a^{\frac{p+1}{4}})^2 = a\, a^{\frac{p-1}{2}} = a \left(\frac{a}{p}\right) [p]$
$\Rightarrow$ on peut calculer une racine de a ou $-a$ dans $\mathbb{Z}/p\mathbb{Z}$
(exemple 9 racine carrée de 12 mod 23)

rmq 49 le calcul d'une racine carrée mod p est un problème non trivial en général

prop 50 si $x^2 + ax + b = 0$ dans $\mathbb{F}_q$, alors cette équation possède des solutions ssi $(2^{-1}a)^2 - b$ est un carré dans $\mathbb{F}_q$ et dans ce cas elles sont données par $-2^{-1}a \pm \delta$ où $\delta^2 = (2^{-1}a)^2 - b$

2) classification des espaces quadratiques sur $\mathbb{F}_q$, q impair

rmq 51 On se place dans la suite sur $\mathbb{F}_q$, q impair

rappel 52 si (E, q) est un espace quadratique, il existe une base B qui soit q-orthogonale

rappel 53 si $A \subset \mathbb{F}_q^*$ système de représentants de $\mathbb{F}_q^* / \mathbb{F}_q^{*2}$ alors il existe une base B de E dans laquelle $[q]_B = \mathrm{Diag}(\lambda_1, \dots, \lambda_n)$, $\lambda_i \in A \cup \{0\}$

lemme 54 Si $a, b \in \mathbb{F}_q^*$, l'équation $ax^2 + by^2 = 1$ admet au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q$

thm 55 Si $a \in \mathbb{F}_q$ non carré ; q une forme quadratique non dégénérée sur $\mathbb{F}_q$ alors il existe une base B de E dans laquelle $[q]_B = \underbrace{\mathrm{Diag}(1, 1, \dots, 1)}_{\text{si } \det q \text{ est un carré}}$ ou $\underbrace{\mathrm{Diag}(1, 1, \dots, 1, a)}_{\text{si } \det q \text{ n'est pas un carré}}$

exemple 56 : $x^2 + 2xy + 2yz$ sur $\mathbb{F}_3$

def 57 $\delta(q) = \overline{\det q}$ = classe de $\det q$ dans $\mathbb{F}_q^* / \mathbb{F}_q^{*2}$
= discriminant de q

thm 58 q_1, q_2 2 formes quadratiques non dégénérées sur E alors (E, q_1), (E, q_2) sont isométriques ssi $\delta(q_1) = \delta(q_2)$

exemple 59 $x^2 + 2xy + 2yz$ et $x^2 + y^2 + z^2$ sur $\mathbb{F}_3$ ne sont pas isométriques