Cadre : Tous les corps considérés seront supposés commutatif (sauf en théorème de Wedderburn)

Corps finis. Applications.

123

I) Construction des corps finis

A] Caractéristique, sous-corps premier

Def 1 : Soit K un corps. On appelle sous-corps premier de K son plus petit sous-corps contenant 1.

Prop 2 : Soit $K \hookrightarrow L$ une extension de corps. Alors L est un K-espace vectoriel.

Thm 3 : (de la base télescopique) Soient $k \hookrightarrow K$ et $K \hookrightarrow L$ deux extensions finies. Alors $k \hookrightarrow L$ est finie et $[L:k] = [L:K][K:k]$

Def 4 : Soit K un corps. On pose $\varphi : \mathbb{Z} \to K$, $n \mapsto n.1$. On appelle caractéristique de K l'unique générateur positif de $\ker\varphi$. On le note $\mathrm{car}\, K$.

Prop 5 : La caractéristique d'un corps est nulle ou première.

Thm 6 : Soit K un corps.
- Si $\mathrm{car}\, K = 0$, $\mathbb{Q} \hookrightarrow K$ est son sous-corps premier.
- Si $\mathrm{car}\, K = p \neq 0$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est son sous-corps premier.

Rem 7 : Si K est fini, $\mathrm{car}\, K \neq 0$.

Cor 8 : Soit K un corps fini. Alors, si $p = \mathrm{car}\, K$, $\exists n \in \mathbb{N}$, $|K| = p^n$. Tout corps fini est donc de cardinal une puissance d'un nombre premier.

Prop 9 : Soit K corps de caractéristique $p > 0$. L'application $F : K \to K$, $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius

Rem 10 : Si K est fini, F est un automorphisme.

Thm 11 : (de Fermat) Si $K = \mathbb{F}_p$, $F = \mathrm{id}_{\mathbb{F}_p}$. Donc $\forall x \in \mathbb{Z}$, $x^p \equiv x\ [p]$.

B] Construction et premières propriétés

Thm 12 : Soient K un corps et $P \in K[X]$. Alors il existe un corps de décomposition de P sur K, unique à isomorphisme près.

Thm 13 : Soit $p \in \mathbb{N}$ premier. Soit $n \in \mathbb{N}^*$. Il existe un unique corps à p^n éléments qui est le corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_{p^n}$.

Prop 14 : Soient $\mathbb{F}_q$ et $\mathbb{F}_{q'}$ deux corps finis. Alors $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q'}$ si et seulement si $\exists n \in \mathbb{N}$, $q' = q^n$.

Lem 15 : Soient $n > 1$ et $d \mid n$, $d \neq n$. Alors $(X^d - 1) \mid (X^n - 1)$ et $\Phi_n \mid \frac{X^n - 1}{X^d - 1}$ où Φ_n est le n-ième polynôme cyclotomique

Thm 16 : (de Wedderburn) Soit K un corps fini, non supposé commutatif. Alors K est effectivement commutatif

Rem 17 : Ceci valide notre supposition faite au départ.

Thm 18 : Soit K un corps fini. Alors K^* est cyclique.

Rem 19 : Il n'est pas exigé, en général, d'en trouver un générateur explicite.

II) Etude des carrés dans $\mathbb{F}_q$

Soient $p \in \mathbb{N}$ premier, $n \in \mathbb{N}^*$ et $q = p^n$.

A] Caractérisation des carrés

Def 20 : Soit $x \in \mathbb{F}_q$. On dit que x est un carré

si $\exists y \in \mathbb{F}_q$, $x = y^2$. On note $\mathbb{F}_q^2$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \setminus \{0\}$.

Ex 21 : 0 et 1 sont bien sûr des carrés.

Thm 22 : Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$. En particulier, tout élément de $\mathbb{F}_q$ est un carré.

On suppose maintenant $p > 2$.

Thm 23 : $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$. Donc $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

Thm 24 : $\forall x \in \mathbb{F}_q^*$, $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

Ex 25 : 2 est un carré modulo 7, contrairement à 3.

Cor 26 : $(-1) \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1 [4]$.

App 27 : Il existe une infinité de nombres premiers congrus à 1 modulo 4.

App 28 : (Théorème des deux carrés de Fermat) Soit $n \in \mathbb{N}^*$. n est somme de deux carrés si et seulement si pour tout nombre premier p tel que $p | n$ et $p \equiv 3 [4]$, alors $v_p(n)$ est pair.

B] Symbole de Legendre

On suppose toujours $p > 2$.

Def 29 : Soit $x \in \mathbb{F}_p$. On définit son symbole de Legendre, noté $\left(\frac{x}{p}\right)$ par : $\left(\frac{x}{p}\right) = \begin{cases} 0 \text{ si } x = 0 \\ 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ -1 \text{ si } x \notin \mathbb{F}_p^2 \end{cases}$

Rem 30 : On étend par quotient cette définition aux entiers relatifs. On dit alors que $n \in \mathbb{N}$ premier avec p est un résidu quadratique modulo p si $\left(\frac{n}{p}\right) = 1$.

Prop 31 : $\forall x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.

Cor 32 : $\mathbb{F}_p^* \to \{\pm 1\}$, $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de groupe.

Thm 33 : (DEV 1) (loi de réciprocité quadratique) Soit $q \in \mathbb{N}$ premier impair. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Prop 34 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Rem 35 : Ces relations permettent ainsi le calcul du symbole de Legendre par réduction successives.

Ex 36 : $\left(\frac{23}{59}\right) = -1$.

III) Polynômes

A] Recherche de la clôture algébrique de $\mathbb{F}_q$

Prop 37 : Un corps algébriquement clos est nécessairement infini.

Prop 38 : $\forall n \in \mathbb{N}^*$, $\mathbb{F}_p$ et $\mathbb{F}_{p^n}$ ont même clôture algébrique, notée $\overline{\mathbb{F}_p}$.

Prop 39 : $\forall n \leq m$, $\mathbb{F}_{p^n}! \hookrightarrow \mathbb{F}_{p^m}!$

Rem 40 : On peut donc munir $\bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^n}!$ d'une structure de corps.

Thm 41 : $\overline{\mathbb{F}_p} = \bigcup_{n \geq 0} \mathbb{F}_{p^{n!}}$

B] Polynômes irréductibles

Thm 42 : $\mathbb{F}_q \simeq \frac{\mathbb{F}_p[X]}{(\pi)}$ où π est un polynôme irréductible quelconque de degré n, sur $\mathbb{F}_p[X]$.

Cor 43 : $\forall n \in \mathbb{N}^*$, il existe $\pi \in \mathbb{F}_p[X]$ irréductible

de degré n.

[1] **Thm 44 :** Soit $P \in \mathbb{F}_q[X]$ de degré $n \in \mathbb{N}^*$. P est irréductible si et seulement si il n'admet aucune racine dans les corps $\mathbb{F}_{q^m}$ avec $m \leq \frac{n}{2}$.

[3] **Thm 45 : (DEV 2) (Algorithme de Berlekamp)** Soit $P \in \mathbb{F}_q[X]$ non irréductible et sans facteur carré. Alors il existe $V \in \mathbb{F}_q[X]$ non constant modulo (P) tel que : $P = \prod_{\alpha \in \mathbb{F}_q} PGCD(P, V - \alpha)$

Rem 46 : Ceci donne un algorithme permettant de trouver la décomposition en irréductibles de P.

IV) Algèbre linéaire et multilinéaire

A] Groupe de matrices

Prop 47 : Soient k un corps et $n \in \mathbb{N}^*$. Le centre de $GL_n(k)$ est formé des homothéties. Celui de $SL_n(k)$ est formé des homothéties de rapports $\mu_n(k) = \{\lambda \in k \mid \lambda^n = 1_k\}$.

Prop 48 : $|\mu_n(\mathbb{F}_q)| = PGCD(n, q-1)$

[7] **Cor 49 :** On a les égalités suivantes :

$$|GL_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i)$$

$$|SL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| = q^{n-1} \prod_{i=0}^{n-2} (q^n - q^i)$$

$$|PSL_n(\mathbb{F}_q)| = \frac{|SL_n(\mathbb{F}_q)|}{PGCD(n, q-1)}$$

Prop 50 : $S_n \hookrightarrow GL_n(\mathbb{F}_p)$

App 51 : (Théorème de Sylow) Soit G un groupe fini et soit $p \mid |G|$ premier. Alors G admet un p-Sylow.

B] Formes quadratiques

Soit k un corps fini, avec $\mathrm{car}\, k \neq 2$. Soit E un k-espace vectoriel de dimension finie.

Def 52 : On appelle forme quadratique sur E toute application $q : E \to k$ obtenue par $\varphi : E \times E \to k$ bilinéaire symétrique avec $\forall x \in E, q(x) = \varphi(x, x)$.
Deux formes quadratiques q et q' sont dites équivalentes si $\exists u \in GL(E) / q' = q \circ u$.

[7] **Thm 53 : (de classification)** Soit $\alpha \in k^*, \alpha \notin k^2$. Alors il existe deux classes d'équivalence des formes quadratiques non dégénérées sur E données par :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$$

En particulier, une forme quadratique non dégénérée appartient à l'une ou l'autre de ses classes suivant si son discriminant est un carré ou non.

App 54 : On démontre à l'aide du déterminant la loi de réciprocité quadratique via ce théorème.

Références :

- Cours d'algèbre, Perrin [1]
- Théorie de Galois, Gozard [2]
- Objectif agrégation, Beck [3]