123 - Corps finis - Applications

Tous les corps sont considérés comme commutatifs.

I. Corps finis : existence et unicité

1) Généralités sur les corps

Déf. / Prop. ①: Soit K un corps. $\sigma : \mathbb{Z} \to K$, $n \mapsto n.1_K$ est un morphisme d'anneaux bien défini.

Si $\operatorname{Ker} \sigma = \{0\}$, on dit que K est de caractéristique nulle, noté $\operatorname{car}(K) = 0$ et que $\mathbb{Q}$ est le sous corps premier de K.

Sinon $\operatorname{Ker} \sigma = p\mathbb{Z}$ où p est premier, on dit que $\operatorname{car}(K) = p$ et que $\mathbb{F}_p$ est le sous-corps premier de K.

Ex. ②: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique nulle.

Rq ③: Si K est un corps fini, il existe $p \in \mathbb{N}$ premier tel que $\mathbb{F}_p \subset K$. Il existe alors $n \in \mathbb{N}^*$ tel que $|K| = p^n$.

Th. ④: (*base télescopique*)

Soient $K \subset L \subset M$ des corps, $(e_i)_{i\in I}$ une base du K-ev L, $(f_j)_{j\in J}$ une base du L-ev M. Alors, $(e_i f_j)_{I\times J}$ est une base du K-ev M.

Coro. ⑤: En notant $[L:K] = \dim_K L$, on a $[M:K] = [M:L]\,[L:M]$

Coro ⑥: Soit L un corps fini, $p = \operatorname{car}(L)$ et $|L| = p^n$.

Si $K \subset L$ est un sous-corps de L, alors K est fini, $\operatorname{car}(K) = p$ et $|K| = p^r$ où $r \in \mathbb{N}^*$ et $r \mid n$.

Déf. / Prop. ⑦: Soit K un corps de caractéristique $p > 0$. Alors, $F : K \to K$, $x \mapsto x^p$ est un morphisme de corps appelé morphisme de Frobenius.

Si K est fini, c'est un automorphisme.

Si $K = \mathbb{F}_p$, c'est l'identité.

2) Existence et "unicité" des corps finis

Th. ⑧: Soit $q = p^n$, p premier et $n \in \mathbb{N}^*$.

Il existe un corps fini à q éléments, noté $\mathbb{F}_q$, unique à isomorphisme près. C'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Th. ⑨: Soit $P \in \mathbb{F}_p[X]$ irréductible de degré $n \geq 1$.

Alors $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_q$ où $q = p^n$

Ex. ⑩: $P = X^4 + X^3 + X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$.

On a donc $\mathbb{F}_2[X]/(P) \simeq \mathbb{F}_{2^4} = \mathbb{F}_{16}$.

Rq ⑪: On souhaiterait connaître l'existence de polynômes irréductibles de tout degré sur $\mathbb{F}_p$, et éventuellement pouvoir tester l'irréductibilité d'un polynôme sur $\mathbb{F}_p$ (voir III).

II. Structure de $\mathbb{F}_q$.

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

1) Sous-ensembles de $\mathbb{F}_q$

Prop. ⑫: Le théorème de structure des groupes abéliens finis appliqué à $(\mathbb{F}_q, +)$ est : $\mathbb{F}_q \simeq (\mathbb{Z}/p\mathbb{Z})^n$

Prop. ⑬: $(\mathbb{F}_q^*, \cdot)$ est cyclique de cardinal $q-1$.

On a donc $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$.

Ex ⑭: $\mathbb{F}_8^* \simeq \mathbb{Z}/7\mathbb{Z}$, donc tout élément différent de 1 dans $\mathbb{F}_8^*$ en est un générateur

Rq ⑮: On ne sait pas, en général, trouver un générateur de $\mathbb{F}_q^*$

Prop. (16): Soit $r \mid n$. Alors $\mathbb{F}_q$ admet un sous-corps de cardinal p^r : c'est l'ensemble des racines de $X^{p^r} - X$ dans $\mathbb{F}_q$.

Coro (17): Soient p, p' premiers et $r, n \in \mathbb{N}^*$.

$$\mathbb{F}_{p^r} \subset \mathbb{F}_{p'^n} \iff p = p' \text{ et } r \mid n$$

Ex. (18):
$$\begin{tikzcd} & \mathbb{F}_{p^2} \arrow[d, "\times"] \arrow[dr] & \\ \mathbb{F}_p \arrow[ur] \arrow[dr] & \mathbb{F}_{p^3} \arrow[r] & \mathbb{F}_{p^6} \end{tikzcd}$$

2) Carrés dans $\mathbb{F}_q$ (Rappel : $q = p^n$)

Déf. (19): On note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q,\ x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^* \cap \mathbb{F}_q^2$

Prop. (20): 1) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$

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

Prop. (21): Si $p > 2$, et $x \in \mathbb{F}_q$.

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

Ex. (22): 2 est un carré dans $\mathbb{F}_7$.

[H2G2] **Déf./Prop. (23)**: On suppose $p > 2$. Soit $a \in \mathbb{F}_p$.

302 Alors : $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*2} \\ -1 & \text{si } a \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2} \\ 0 & \text{si } a = 0 \end{cases}$

$\left(\frac{a}{p}\right)$ est appelé symbole de Legendre de a par rapport à p.

Prop. (24): Si $p > 2$, $a, b \in \mathbb{F}_p$. Alors $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

303

DVP 1 **Prop. (25)**: Si $p > 2$ et $a \in \mathbb{F}_p^*$, alors $|\{x \in \mathbb{F}_p,\ ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$

Th. (26): (*loi de réciprocité quadratique*) 304

Soient p et q deux nombres premiers impairs distincts. DVP 1

Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}$

Exercice (27): Calculer $\left(\frac{19}{43}\right)$

III. Polynômes sur les corps finis

1) Polynômes irréductibles

Rq (27): Un corps fini $\mathbb{F}_q$ n'est jamais algébriquement clos, prendre par exemple $\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) + 1 \in \mathbb{F}_q[X]$.

Lemme (28): Soient $r, n \in \mathbb{N}^*$ et $q \geq 2$. Alors [Dem]

$$q^r - 1 \mid q^n - 1 \iff r \mid n$$ 220

Th. (29): Soit $\mathbb{F}_q$ un corps fini, et $n \in \mathbb{N}$, $n \geq 1$. DVP 2

Alors, $X^{q^n} - X \in \mathbb{F}_q[X]$ est exactement le produit des polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$.

De plus, si on note m_n leur nombre, on a $m_n \sim \frac{q^n}{n}$ quand $n \to +\infty$

Coro (30): Soit $P \in \mathbb{F}_q[X]$ unitaire, $\deg P = n \geq 1$. Alors,

P irréductible sur $\mathbb{F}_q \iff$ 1) $P \mid X^{q^n} - X$

2) $\forall r \mid n$, r premier, $P \wedge X^{q^{\frac{n}{r}}} - X = 1$

Th. (31): (*algorithme de Berlekamp*) [Beck

Soit $P \in \mathbb{F}_q[X]$ sans facteur carré, $\deg P = n \geq 1$. Alors il existe $V \in \mathbb{F}_q[X]$ tq :

i) V est non constant modulo P 244

ii) $P = \prod_{\alpha \in \mathbb{F}_q} \operatorname{pgcd}(P, V - \alpha)$ DVP3

iii) Si P n'est pas irréductible, au moins deux des facteurs du produit précédent sont non triviaux

Exercice (32) : Appliquer l'algorithme de Berlekamp à $X^2 - a \in \mathbb{F}_p[X]$ où $a \in \mathbb{F}_p^*$, et retrouver la prop. (23).

Th. (33) : Soit $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $p \in \mathbb{N}$ un nombre premier. On suppose $\bar{a}_n \neq \bar{0}$ dans $\mathbb{F}_p$.
Si $\bar{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$.

Appli. (34) : Montrer que $X^p - X - 1$ est irréductible sur $\mathbb{Z}$ pour tout p premier.

Rq (35) : Dans le th. (33), P n'est pas nécessairement irréductible sur $\mathbb{Z}$ (prendre $P = 2X$ et $p = 3$).

2) Polynômes cyclotomiques

Notations (36) : Soit $n \in \mathbb{N}^*$. On notera $\mu_n \subset \mathbb{C}$ (resp. μ_n^*) l'ensemble des racines (resp. racine primitives) n-ièmes de l'unité dont on supposera connues les principales propriétés.

Déf/Prop (37) : $n \geq 1$. On appelle n-ième polynôme cyclotomique $\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi) \in \mathbb{C}[X]$. On a alors $X^n - 1 = \prod_{d \mid n} \Phi_d$

Ex. (38) : $\Phi_1 = X - 1$; $\Phi_2 = X + 1$; $\Phi_3 = X^2 + 1$; $\Phi_p = X^{p-1} + \dots + X + 1$ p premier.

Th. / Déf. (39) : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$. Pour p premier, en notant $\sigma : \mathbb{Z} \to \mathbb{F}_p$ la projection canonique, on pose $\Phi_{n, \mathbb{F}_p} = \sigma(\Phi_n)$.

Rq (40) : Si $p \nmid n$, alors $X^n - 1$ est à racines simples sur son corps de décomposition.

Th. (41) : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

Appli. (42) : (théorème de Wedderburn)
Soit A un anneau intègre tel que $A^\times = A \setminus \{0\}$ et A fini. Alors, A est un corps.

Appli. (43) : (théorème de Dirichlet (faible))
Soit $n \in \mathbb{N}$, $n \geq 1$. Alors il existe une infinité de nombres premiers congrus à 1 modulo n.

[FGN1] p31 DVPH

IV. Un résultat d'algèbre linéaire

Soit $K = \mathbb{F}_q$ un corps fini, car$(K) \neq 2$ et E un K-ev de dimension finie $n \geq 1$.

Déf. (44) : Soit q une forme quadratique sur E. Le discriminant de q est $\delta(q) = \det(q) \bmod \mathbb{F}_q^{*2}$, où $\det(q)$ est pris dans une base quelconque de E.

Th. (45) : Soit $\alpha \in \mathbb{F}_q^*$, $\alpha \notin \mathbb{F}_q^{*2}$. Il y a deux classes d'équivalence de formes quadratiques non dégénérées sur E de matrices : $\underbrace{Q_1 = I_n}_{\text{si } \delta(q) \in \mathbb{F}_q^{*2}}$ ou $\underbrace{Q_2 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & 1 & \\ 0 & & \alpha \end{pmatrix}}_{\text{si } \delta(q) \notin \mathbb{F}_q^{*2}}$

Appli. (46) : voir Th. (26).

Références :

- [Per] Perrin, Cours d'algèbre (+80%)
- [H2G2] Caldero, Nouvelles ....
- [FGN1] Francinou, Algèbre 1
- [Beck] Beck, Objectif agrégation
- [Demz] Demazure, Cours d'algèbre