123 — Corps finis - Applications.

Go2 = Gozard, P = Perrin — Théorie de Galois — DEM = Demazure Cours d'algèbre — OA = Objectif agreg

Soit K un corps. + def du corps ← commutativité dans la def

I. GÉNÉRALITÉS SUR LES CORPS FINIS.

I. structure des corps finis

1. Caractéristique et cardinal

P p72

Def 1 = Soit $\varphi : \mathbb{Z} \to K$ le morphisme d'anneaux défini par $\varphi(n) = \underbrace{1 + \dots + 1}_{n \text{ fois}}$. L'idéal $\ker\varphi$ vérifie $\ker\varphi = p\mathbb{Z}$ où $p = 0$ ou p premier. Cet entier p est appelé la caractéristique de K. On la note $Car(K)$.

Rq 2 = Si K est fini alors $Car(K) > 0$ ⚠ Récip fausse : $\mathbb{F}_p(X)$

Def 3 = On appelle sous corps premier de K le plus petit sous corps de K.

Prop 4 = Si $Car(K) > 0$, le sous corps premier de K est $\mathbb{Z}/p\mathbb{Z}$. On le note $\mathbb{F}_p$.

Go2 p81

Prop 5 = Si K est fini de caractéristique p, alors il existe $n \in \mathbb{N}^*$ tel que $|K| = p^n$.

Ex 6 = Il n'existe pas de corps à 6 ou 12 éléments.

p85

Def 7 = Si K est de caractéristique $p > 0$, $F : K \to K$, $x \mapsto x^p$ est un $\mathbb{F}_p$-endomorphisme du corps K, appelé morphisme de Frobenius.

Prop 8 = • Si K est fini, F est un automorphisme
• Si $K = \mathbb{F}_p$, F est l'identité.

Coro 9 = Si K est fini de caractéristique p, tout élément de K admet exactement une racine p-ième.

2. Existence et unicité des corps finis

p85

def corps de décomposition

Thm 10 = Soient p un nombre premier, $n \in \mathbb{N}^*$. On note $q = p^n$. Il existe un corps fini à q éléments. Il est corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$. Il est de plus, unique à isomorphisme près. On le note $\mathbb{F}_{p^n}$.

3. Structure de $\mathbb{F}_q^\times$, $q = p^n$ + ex + corollaire G p86

p83

Prop 11 = Le groupe multiplicatif d'un corps fini est cyclique

Ex 12 = $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$

Prop 13 = Si K est un corps fini de caractéristique p et ξ un générateur de $K^\times$. Alors $K = \mathbb{F}_p(\xi) = \mathbb{F}_p[\xi]$.

Rq 14 = La réciproque est fausse
• On ne sait pas en général déterminer explicitement un générateur de $K^\times$.

4. Structure des corps finis ou sous corps d'un corps fini et gpe des auto.

P p91

Prop 15 = Si $q = p^n$, p premier, $n \in \mathbb{N}^*$. Pour chaque diviseur d de n, $\mathbb{F}_q$ a un unique sous corps de cardinal p^d. Ce sous corps est isomorphe à $\mathbb{F}_{p^d}$.

P p65

Prop 15* = Soient M/L et L/K des extensions de corps de degré fini. Alors M/K est une extension de degré fini et $[M:K] = [M:L][L:K]$.

Ex 16 = On a le diagramme :

$$\begin{tikzcd}
 & & & \mathbb{F}_{2^{12}} \\
 & & \mathbb{F}_{2^6} \arrow[ur] & \\
\mathbb{F}_{2^3} \arrow[urr] & & & \mathbb{F}_{2^4} \arrow[uu] \\
 & \mathbb{F}_2 \arrow[ul] \arrow[r] & \mathbb{F}_{2^2} \arrow[uu] \arrow[ur] &
\end{tikzcd}$$

Go7 p86

Thm 17 (Wedderburn) = Tout corps fini est commutatif (admis)

Prop 18 = Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre n. $Aut_{\mathbb{F}_p}(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$. Il est engendré par le morphisme de Frobenius.

II. CARRÉS DANS UN CORPS FINI

1. Définition et caractérisation. $q = p^n$ $n \in \mathbb{N}^*$ $p \in \mathcal{P}$

Go7 p93

Def 19 On pose $\mathbb{F}_q^2 = \{x^2, x \in \mathbb{F}_q\}$ et $\mathbb{F}_q^{\times 2} = \mathbb{F}_q^\times \cap \mathbb{F}_q^2$.
$\mathbb{F}_q^{\times 2}$ est l'image de $\mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $x \mapsto x^2$.

Prop 20 = • Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$ donc $\mathbb{F}_q^{\times 2} = \mathbb{F}_q^\times$.
• Si $p > 2$, $\mathbb{F}_q^{\times 2}$ est un sous groupe d'indice 2 de $\mathbb{F}_q^\times$ donc $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

Perrin p130

App 21 = L'équation d'inconnues x, y $ax^2 + by^2 = c$ avec $a, b, c \in \mathbb{F}_q^\times$ a des solutions dans $\mathbb{F}_q$.

Goz p93

Prop 22 : $-1 \in \mathbb{F}_q^{\times 2} \iff q \equiv 1\ [4]$

App 23 : Théorème des deux carrés

App 24 : Il existe une infinité de nombres premiers de la forme $4k+1$.

2- Symboles de Legendre et de Jacobi. p premier $p \neq 2$

Goz p153

Def 25 : On définit le symbole de Legendre $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p$ par
$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{ssi } x \in \mathbb{F}_p^{\times 2} \\ -1 & \text{ssi } x \notin \mathbb{F}_p^{\times 2} \\ 0 & \text{ssi } x = 0 \end{cases}$$

Ex 26 : $\left(\frac{2}{7}\right) = 1$ et $\left(\frac{3}{7}\right) = -1$.

Prop 27 (Critère d'Euler). $\forall x \in \mathbb{F}_p^\times$ $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$, $p \neq 2$

Ex 28 : $\left(\frac{7}{11}\right) = 7^5 \equiv -1\ [11]$.

Cor 29 : Le symbole de Legendre est multiplicatif : pour tout $x, y \in \mathbb{F}_p^\times$ $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$

Thm 30 (Loi de réciprocité quadratique)] DVLPT

Soient p, q deux nombres premiers impairs distincts. Alors
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Ex 31 : $\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{-1}{5}\right) = 1$ 5 est un carré dans $\mathbb{F}_{19}$.

DEM p112

Def 32 : On définit le symbole de Jacobi pour m, n entiers avec $n \geq 3$ impair par
$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_r}\right)$$
où $n = p_1 \cdots p_r$ décomposition en facteurs premiers.

où les $\left(\frac{m}{p_i}\right)$ sont les symboles de Legendre.

Prop 33 : Si m est un résidu quadratique modulo n, alors $\left(\frac{m}{n}\right) = 1$. La réciproque est vraie lorsque n est premier mais pas dans le cas général.

C-ex 34 : $\left(\frac{14}{51}\right) = 1$ mais 14 n'est pas un résidu quadratique modulo 51

III POLYNÔMES SUR UN CORPS FINI

1- Polynômes irréductibles sur les corps finis.

Goz p87

Thm 35 : Soient p premier, $n \in \mathbb{N}^\times$. Notons $q = p^n$. On a $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.

Ex 36 : $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3+X+1)$ + générateur etc

Coro 37 : • Il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$.

• Si P est un polynome irréductible de degré n sur $\mathbb{F}_p$, alors $P(X) \mid X^q - X$ dans $\mathbb{F}_p[X]$ donc P est scindé sur $\mathbb{F}_q$. Ainsi son corps de rupture $\mathbb{F}_q$ est aussi son corps de décomposition.

Thm 38 : On note $A(n,p)$ l'ensemble des polynômes de $\mathbb{F}_p[X]$ irréductibles unitaires de degré n. Alors
$$X^q - X = \prod_{d \mid n} \prod_{P \in A(n,p)} P(X).$$

Coro 39 : On a $q = \sum_{d \mid n} d\,|A(n,p)|$

Ex 40 : $|A(2,2)| = 1$. C'est X^2+X+1. + ex de $X^{2^3} - X$

si on rajoute Möbius, on peut calculer $|A(n,p)|$ formule

G p62

Prop 41 : Un corps fini n'est pas algébriquement clos.

Prop 42 : $\bigcup_{n \in \mathbb{N}^\times} \mathbb{F}_{p^n}$ est une clôture algébrique de $\mathbb{F}_p$

Perrin p78

Thm 43 : Soit $P \in \mathbb{F}_q[X]$ de degré $k > 0$. P est irréductible sur $\mathbb{F}_q$ ssi P n'a pas de racines dans les $\mathbb{F}_{p^m}$ avec $n \mid m$ et $\frac{m}{n} \leq \frac{k}{2}$.

Ex 44 : X^4+X+1 est irréductible sur $\mathbb{F}_2$.

Prop 45 : Le polynôme X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible sur $\mathbb{F}_p$ pour tout p premier.

OA p244

2- Algorithme $q = p^s$

a- Sans facteurs carrés.

DVLPT

Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés. $P = \prod_{i=1}^{r} P_i$ où les P_i sont des polynômes irréductibles premiers entre eux deux à deux.

Prop 46: On note $x = X \bmod P$ dans $\mathbb{F}_q[X]/(P)$. On considère la base $\mathcal{B} = (1, x, \dots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$. Alors le processus suivant s'arrête au bout d'un nombre fini d'étapes et donne la décomposition en facteurs irréductibles de P.

- On a $r = \dim(\mathrm{Ker}(S_p - id))$
  où $S_p = \begin{array}{ccc} \mathbb{F}_q[X]/(P) & \longrightarrow & \mathbb{F}_q[X]/(P) \\ Q(X) \bmod P & \longmapsto & Q(X^q) \bmod P \end{array}$
- $P = \prod_{\alpha \in \mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$ où $V \bmod P \in \mathrm{Ker}(S_p - id)$ et V non constant modulo P.
- On boucle sur l'ensemble des facteurs non triviaux du produit.

p248

b- Cas général.

Soit $P \in \mathbb{F}_q[X]$.

① Si P est constant on sort de l'algorithme

② $U = \mathrm{pgcd}(P, P')$

- Si $U = 1$ on applique l'algo de Berlekamp à P
- Si $U = P$, on calcule R tq $R^p = P$ et on retourne à ① avec R
- Sinon $V = \frac{U}{P}$, on retourne à ① avec U et V.

NB: Mettre beaucoup plus d'exemples = utiliser les exercices à la fin du chap de Gozard.