Leçon n°123 : Corps finis. Applications.

I/ Construction des corps finis.

A/ Prérequis sur les extensions de corps. [PER]

Définition 1 : Degré d'une extension.

Théorème 2 : Base télescopique.

Définition 3 : Corps de rupture.

Théorème 4 : Existence et unicité des corps de rupture.

Remarque 5 : Construction explicite du corps de rupture.

Définition 6 : Corps de décomposition.

Théorème 7 : Existence et unicité du corps de décomposition.

B/ Construction théorique [PER]

Définition 8 : Caractéristique et sous-corps premier.

Corollaire 9 : Si $\mathbb{K}$ est infini alors $\mathrm{car}(\mathbb{K}) = 0$.

Corollaire 10 : Tout corps fini est de cardinal la puissance d'un nombre premier.

Remarque 11 : Il n'existe donc pas de corps de cardinal 6.

Lemme 12 : Morphismes de Frobenius.

Théorème 13 : Existence et unicité des corps finis.

Théorème 14 : Théorème de Wedderburn.

C/ Construction explicite [ROM]

Développement 1

Théorème 15 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_n(p)} P$ et dénombrement des polynômes irréductibles de degré donné avec équivalent.

Corollaire 16 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 17 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

D/ Éléments de structure. [PER] [ROM]

Proposition 18 : Inclusion des $\mathbb{F}_{p^n}$: $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \equiv n|m$.

Proposition 19 : $\mathbb{F}_q^\times$ est cyclique.

Corollaire 20 : Théorème de l'élément primitif pour les corps finis.

Remarque 21 : On retrouve le fait qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$ en écrivant $\mathbb{F}_q = \mathbb{F}_p[a]$ et en prenant le polynôme minimal de a.

Théorème 22 : Le groupe des $\mathbb{F}_p$-automorphismes de $\mathbb{F}_q$ est cyclique engendré par le morphisme de Frobenius.

II/ Les carrés d'un corps fini. [ROM 428-431]

Proposition 23 : Nombre de carrés de $\mathbb{F}_q^\times$ et $\mathbb{F}_q$.

Proposition 24 : Critère d'Euler pour les carrés.

Corollaire 25 : Produit de deux carrés et produit d'un carré et d'un non-carré.

Corollaire 26 : $ax^2 + by^2 = c$ admet des solutions dans $(\mathbb{F}_p)^2$.

Remarque 27 : Si on prend $a = 1$ et $b = 1$, tout élément de $\mathbb{F}_q$ s'écrit comme somme de deux carrés.

Définition 28 : Symbole de Legendre.

Proposition 29 : Le symbole de Legendre est l'unique morphisme de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Corollaire 30 : Théorème de Frobenius-Zolotarev.

Proposition 31 : Le nombre de solutions de $ax^2 = 1$ est $1 + \left(\frac{a}{p}\right)$

Théorème 32 : Loi de réciprocité quadratique.

Proposition 33 : Calculs de $\left(\frac{-1}{p}\right)$ et $\left(\frac{2}{p}\right)$.

Remarque 34 : On peut donc calculer tous les symboles de Legendre.

Exemple 35 : Exemple du calcul de $(\frac{13}{31}) = -1$.

III/ Applications des corps finis.

A/ Sur les polynômes. [PER] [OBJ]

Théorème 36 : Critère d'Eisenstein.

Exemple 37 : Polynôme cyclotomique pour p premier et $Y - X(X-1)(X+1)$ dans $\mathbb{K}[X,Y]$.

Théorème 38 : Réduction mod p des polynômes.

Exemple 39 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 40 : $P \in \mathbb{F}_p[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{F}_p$.

Corollaire 41 : $X^4 + 1$ réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

Développement 2

Algorithme 42 : Algorithme de Berlekamp.

B/ Dénombrement et isomorphismes exceptionnels. [CAL]

Définition 43 : Définition des groupes projectifs.

Proposition 44 : L'action sur les droites est transitive.

Proposition 45 : Dénombrement des différents groupes.

Théorème 46 : Isomorphismes exceptionnels.

Références :

- [PER] Perrin p. 65-82
- [ROM] Rombaldi Algèbre 2nd éd. p. 421 et p. 425
- [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244
- [CAL] Caldéro Histoires hédonistes tome 1 p. 250