123 : Corps finis . Applications .

I Notions de corps finis

A Définitions et propriétés Per

On considère $\mathbb{K}$ un corps fini

Définition 1 : On appelle sous corps premier de $\mathbb{K}$ le plus petit sous corps de $\mathbb{K}$.

Exemple 2 : Le sous corps premier de $\mathbb{R}$ est $\mathbb{Q}$.

Définition 3 : La caractéristique de $\mathbb{K}$ est l'entier $\text{car}(\mathbb{K}) = p$ tel que $\ker\varphi = p\mathbb{Z}$ avec $\varphi(n) = n.1_{\mathbb{K}}$ morphisme d'anneaux.

Remarque 4 : La caractéristique d'un corps est donc soit 0, soit un nombre premier.
Si $\text{car}(\mathbb{K}) = 0$, $\varphi(\mathbb{Z}) \subset \mathbb{K}$ donc $\mathbb{K}$ est infini.
Si $\mathbb{K}$ est fini on a $\text{car}(\mathbb{K}) = p > 0$. Le sous corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$.
Le cardinal d'un corps fini est une puissance d'un nombre premier : sa caractéristique.

Exemple 5 : Il n'existe pas de corps de cardinal $6 = 3 \times 2$.

Proposition 6 : Soit $\mathbb{K}$ de caractéristique $p > 0$. L'application $F : \mathbb{K} \to \mathbb{K}$ définie par $F(x) = x^p$ est un homomorphisme de corps appelé homomorphisme de Frobenius.
Si $\mathbb{K}$ est fini, c'est un automorphisme.

Exemple 7 : Si $\mathbb{K} = \mathbb{F}_p$ alors $F = id_{\mathbb{K}}$.

B Existence et unicité Romb Per

On considère $q = p^n$ avec $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$.

Définition 8 : On note $\mathcal{U}_n(P)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = \text{card}(\mathcal{U}_n(p))$.

Proposition 9 : Soit $P \in \mathcal{U}_n(p)$, alors $\mathbb{F}_p[X]/(P)$ est une $\mathbb{F}_p$ algèbre de dimension n de base $(\overline{X}^k)_{0 \le k \le n-1}$ et c'est un corps fini de cardinal p^n.

Exemple 10 : $\forall \lambda \in \mathbb{F}_p$, $P(X) = X - \lambda$ est unitaire de degré 1 et irréductible dans $\mathbb{F}_p[X]$ donc $I_1(p) = p$. Tous ces corps $\mathbb{F}_p[X]/(X-\lambda)$ sont isomorphes à $\mathbb{F}_p$.

Lemme 11 : En notant $P_n = X^q - X \in \mathbb{F}_p[X]$, tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement pour tout d diviseur de n, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

Théorème 12 : Le polynôme P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en facteurs irréductibles :

$$X^q - X = \prod_{d \mid n} \prod_{P \in \mathcal{U}_d(p)} P$$

Théorème 13 : À isomorphisme près, il n'existe qu'un seul corps à p^n éléments. C'est le corps $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_n(p)$.

Exemple 14 : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$

C Inclusion entre corps finis Dos

Lemme 15 : Soit $a > 1$, $n, s > 0$ des entiers, alors $a^s - 1 \mid a^n - 1$ si et seulement si $s \mid n$.

Proposition 16 : Soit $n > 1$, $s > 0$ des entiers, alors $X^s - 1 \mid X^n - 1$ dans $\mathbb{K}[X]$ si et seulement $s \mid n$.

Théorème 17 : Soit p premier et $n \in \mathbb{N}^*$, alors il existe une bijection entre les sous corps de $\mathbb{F}_{p^n}$ et l'ensemble des diviseurs de n, plus précisément $\mathbb{F}_{p^s}$ est un sous corps de $\mathbb{F}_{p^n}$ si et seulement si $s \mid n$.

Théorème 18 (base télescopique) : Soit $K \subset L \subset M$ des corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de M sur L. Alors la famille $(e_i f_j)_{(i,j) \in I \times J}$ est une base de M sur K. Ainsi $[M:K] = [M:L][L:K]$.

Corollaire 19 : Soit $s \mid n$, alors $[\mathbb{F}_{p^n} : \mathbb{F}_{p^s}] = \frac{n}{s}$.

Exemple 20 : Les sous corps de $\mathbb{F}_{1024}$ sont $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_{32}$ et $\mathbb{F}_{1024}$.

Théorème 21 (Théorème de l'élément primitif pour les corps finis) : Il existe $\alpha \in \mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$.

Exemple 22 : $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$, alors en notant a l'image de $X \in \mathbb{F}_2[X]$ dans le quotient $\mathbb{F}_4$, alors $\mathbb{F}_4 = \mathbb{F}_2(a)$.

II Notions de groupes liés au corps

A Groupe des inversibles

Définition 22 : On note $\mathbb{F}_q^*$ le groupe des inversibles de $\mathbb{F}_q$ donc $\mathbb{F}_q \setminus \{0\}$. On a ainsi $|\mathbb{F}_q^*| = q-1$.

Théorème 23 : Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique (et $\mathbb{F}_q^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$).

Lemme 24 : On note φ l'indicatrice d'Euler. Alors $\varphi(m) = \sum_{d|m} \varphi(d)$, $m \in \mathbb{N}^*$.

Remarque 25 : On ne sait pas, en général, trouver explicitement un générateur de $\mathbb{F}_q^*$.

B Groupe des automorphismes 13-6 Rom

Définition 26 : $\mathrm{Aut}(\mathbb{F}_q)$ est le groupe des automorphismes du corps $\mathbb{F}_p$ linéaire.

Exemple 27 :
- $\mathrm{id}_{\mathbb{F}_{p^n}} \in \mathrm{Aut}(\mathbb{F}_{p^n})$ et il s'agit du neutre pour la loi du groupe qui est la composition.
- Le morphisme de Frobenius définit précédemment $F \in \mathrm{Aut}(\mathbb{F}_{p^n})$.

Proposition 28 : En notant $\mathbb{K} = \mathbb{F}_p[X]/(P)$ avec $P \in \mathcal{U}_n(p)$, l'application $\varphi : \mathrm{Aut}(\mathbb{K}) \to \mathbb{K}$, $\gamma \mapsto \gamma(\bar{X})$ réalise une injection entre $\mathrm{Aut}(\mathbb{K})$ et l'ensemble des racines dans $\mathbb{K}$ de P.

Corollaire 29 : Le groupe $\mathrm{Aut}(\mathbb{F}_{p^n})$ est cyclique d'ordre n, engendré par l'automorphisme de Frobenius F.

III Carrés dans $\mathbb{F}_q$

A Propriétés de $\mathbb{F}_q^2$ Per

Notation 30 : On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 31 :
i) pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$
ii) Pour $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Proposition 32 : On suppose que $p > 2$. Alors on a :
$x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Corollaire 33 : Soit $p > 2$ premier, alors -1 est un carré dans $\mathbb{F}_q \iff q \equiv 1 [4]$

Application 34 : Il existe une infinité de nombres premiers $p \equiv 1 [4]$

B Symbole de Legendre Rom Calderon

Définition 35 : Soit $p > 2$ premier. On définit le symbole de Legendre $\left(\frac{x}{p}\right)$ pour $x \in \mathbb{F}_p^*$ comme suit :
$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon} \end{cases}$$

Exemple 36 : $4^2 \equiv 1 [5]$ donc $4 \in \mathbb{F}_5^{*2}$.

Théorème 37 : i) Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^*$.
ii) L'application $\mathbb{F}_p^* \to \{-1, 1\}$, $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

Exemple 38 : $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1 [5]$ donc $2 \notin \mathbb{F}_5^{*2}$

Corollaire 39 : Si $n = \pm \prod_{i=0}^{\hat{}} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=0}^{\hat{}} \left(\frac{p_i}{p}\right)^{\alpha_i}$

Théorème 40 (réciprocité quadratique) : Pour tout nombre premier impair $q \neq p$, on a : $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Exemple 41 : $\left(\frac{23}{59}\right) = (-1)^{11 \cdot 29}\left(\frac{59}{23}\right) = \ldots = \left(\frac{2}{5}\right) = -1$

Lemme 42 : pour tout $p > 2$ premier, 8 divise $p^2 - 1$.

Proposition 43 : Pour tout $p > 2$ premier on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

IV Racines de l'unité et polynômes cyclotomiques

A Racines de l'unité Per

Définition 44 : On note $\mu_n(\mathbb{K})$ l'ensemble des racines n ième de l'unité dans $\mathbb{K}$, $\mu_n(\mathbb{K}) = \{u \in \mathbb{K}, u^n = 1\}$.

Définition 45 : Une racine $n$ième primitive de 1 est un élément $u \in \mu_n(\mathbb{K})$ tel que $u^n = 1$, $u^d \neq 1$ pour $d < n$. Autrement dit, u est un générateur du groupe μ_n, de sorte qu'il y ait $\varphi(n)$ racines primitives de 1. On note $\mu_n^*(\mathbb{K})$

Définition 46 : Le $n$ième polynôme cyclotomique sur $\mathbb{K}$ est défini par :

$$\Phi_n(X) = \prod_{u \in \mu_n^*(\mathbb{K})} (X - u)$$

Remarque 47 : i) Si u est une racine $n$ième de l'unité primitive, les autres sont les u^m avec $m \wedge n = 1$.
ii) Le polynôme Φ_n est unitaire de degré $\varphi(n)$.

B Etude de Φ_n. Per

Proposition 48 : On a : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

Remarque 49 : En comparant les degrés, on retrouve que $n = \sum_{d \mid n} \varphi(d)$.

Exemple 50 : $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$

Développement (Théorème de Wedderburn) [Annexe I]
Tout corps fini est commutatif.

Conséquence : dans un corps fini, on peut toujours utiliser la formule du binôme de Newton.

C Irréductibilité de Φ_n sur $\mathbb{Z}$. Per

Théorème 51 : (Critère d'Eisenstein)
Soit $P \in \mathbb{Z}[X]$, $P = \sum a_i X^i$ et p premier tel que :
i) $p \nmid a_n$
ii) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$
iii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus P est unitaire, alors P est aussi irréductible dans $\mathbb{Z}[X]$.

Application 52 : Soit $p \in \mathcal{P}$, $\Phi_p(X)$ est irréductible sur $\mathbb{Z}[X]$.

Théorème 53 : Soit $p \in \mathcal{P}$, $P = \sum_0^n a_i X^i \in \mathbb{Z}[X]$ et $\bar{P}$ sa réduction modulo p telle que $\bar{a_n} \neq 0$.
Alors $\bar{P}$ est irréductible sur $\mathbb{Z}_p$ et P est irréductible sur $\mathbb{Q}$.

Exemple 54 : pour p premier, $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Développement Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$

Références :

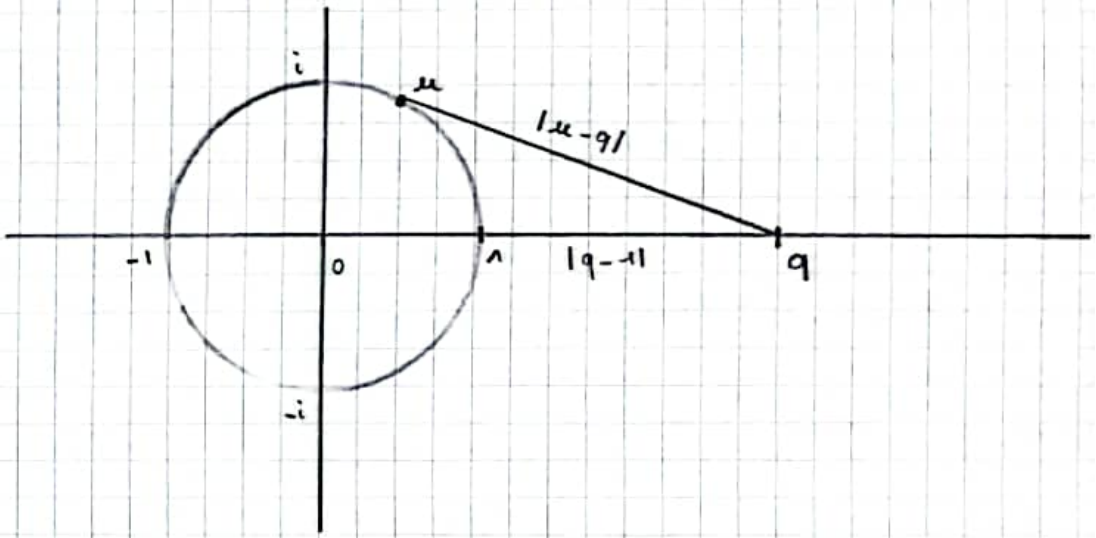
Daniel Perrin Cours d'Algèbre.

Rombaldi Mathématiques pour l'agrégation

Extensions de corps Josette Calais

Annexe :

Théorème de Wedderburn.



Sur le schéma, on voit bien que $|u-q| > |q-1|$.