LEÇ 114 : CORPS FINIS. APPLICATIONS

I GÉNÉRALITÉS [PER]

Déf Un corps est un anneau commutatif unitaire dans lequel tout élément non nul est inversible.

TH (WEDDERBURN) : Toute algèbre à division finie est un corps.

Soit K un corps fini, $\varphi : \mathbb{Z} \longrightarrow K$, $n \longmapsto n \cdot 1_K$ morphisme de noyau $p\mathbb{Z}$ (p premier).

Défs a) Caractéristique de K : nombre premier p tq $\ker \varphi = p\mathbb{Z}$.

b) Sous-corps premier de K : plus petit sous-corps de K contenant 1_K.

Notation : $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Prop : a) Si K est un corps fini de caractéristique p, alors le sous-corps premier de K est $\mathbb{F}_p$.

b) Si K est un corps fini, alors $\mathrm{car}\, K \neq 0$.

TH K un corps fini, alors $\exists n \in \mathbb{N}$, $\mathrm{Card}\, K = (\mathrm{car}\, K)^n$.

Morphisme de Frobenius :

$\Psi : K \longrightarrow K$, $x \longmapsto x^p$ est un automorphisme de K. (K corps fini, $\mathrm{car}(K) = p$)

De plus si $K = \mathbb{F}_p$, alors $\Psi \equiv Id$

Application : petit th. de fermat : $\forall p \in \mathcal{P}(\text{nbres. } 1^{\text{ers}})$, $x^p \equiv x \ [p]$.

II STRUCTURE DES CORPS FINIS

1) Théorème d'existence

TH Soit $p \in \mathcal{P}$, $n \in \mathbb{N}^*$, on pose $q = p^n$. Alors :

Il existe un corps K à q éléments.

(i) C'est le corps décomposition de $X^q - X$ sur $\mathbb{F}_q$; c'est aussi son corps de rupture.

(ii) Ce corps est unique à isomorphisme non unique près.

On note ce corps $\mathbb{F}_q$.

c) Le groupe multiplicatif $\mathbb{F}_q^*$

TH $\mathbb{F}_q^*$ est cyclique, et $\mathbb{F}_q^* \sim \mathbb{Z}/(q-1)\mathbb{Z}$

Ex : $\mathbb{F}_5^* = \langle 2 \rangle$, $\mathbb{F}_7^* = \langle 3 \rangle$... en général il n'est pas commode de trouver un générateur de $\mathbb{F}_q$.

TH de CHEVALLEY-WARNING : [SER]

Soit K un corps fini, $\mathrm{car}(K) = p$; soient $(P_1, \dots, P_r)$ des polynômes de $K[X_1, \dots, X_n]$ tq $\sum_{i=1}^{r} \deg P_i < n$, soit $V = \{ x \in K^n \text{ tq } \forall i \in [\![1, r]\!],\ P_i(x) = 0 \}$

Alors $\#V \equiv 0 \ [p]$.

III POLYNÔMES SUR UN CORPS FINI

1) Polynômes irréductibles

Th: Soit $q = p^n$. Alors $X^q - X = \prod_{\substack{\deg P / n \\ P \text{ irred} \\ P \in \mathbb{F}_p[X]}} P(X)$.

Csq: En s'intéressant aux degrés, on écrit

$$p^n = \sum_{d|n} I_p^d \cdot d \quad \text{où } I_p^d \text{ est le nombre de}$$

poly. irred. de degré d sur $\mathbb{F}_p$. En appliquant la formule d'inversion de Möbius, on voit que $\forall n \in \mathbb{N}$, $\forall p \in \mathcal{P}$, $I_p^n \geq 1$.

Th de réduction : Soit $P(X) = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$, $p \in \mathcal{P}$, tel que $a_n \not\equiv 0 [p]$, $\overline{P}$ la classe de P dans $\mathbb{F}_p[X]$. Si $\overline{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$ et donc sur $\mathbb{Z}$ si $\gcd(a_i) = 1$.

Rq: La réciproque est fausse : $X^4 + 1$ est irréd. sur $\mathbb{Z}[X]$, mais il est réductible sur tous les $\mathbb{F}_p$ pour $p \in \mathcal{P}$.

Ex: $\forall p \in \mathcal{P}$, $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

2) Construction des corps finis non triviaux

Prop Tout corps fini à q éléments est isomorphe à $\mathbb{F}_p[X]/(P)$ où P est de degré n, irréductible sur $\mathbb{F}_p$ ($q = p^n$)

Ex: $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$

Applications: Calcul dans $\mathbb{F}_q$!

IV POLYNÔMES CYCLOTOMIQUES [DEV]

Déf n-ième polynôme cyclotomique : $\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$ où $\mu_n^* = \{ \zeta \in \mathbb{C} \text{ tq } \zeta^n = 1 \text{ et } \forall d < n, \zeta^d \neq 1 \}$.

Propson a $X^n - 1 = \prod_{d|n} \Phi_d(X)$

2) $\Phi_n(X) \in \mathbb{Z}[X]$

3) $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$ (Gauss)

Th Soit $n \in \mathbb{N}^*$, $n \wedge q = 1$. Soit r le plus petit entier tq $q^r \equiv 1 [n]$. Alors $\Phi_n(X)$ se décompose sur $\mathbb{F}_q[X]$ en polynômes irréductibles unitaires de degré r, tous $\neq$.

Ex: $q = 3$, $n = 11$, $r = 5$: Φ_{11} se décompose dans $\mathbb{F}_3$ en produit de 2 polynômes irréd. unitaires de deg 5.

Cor : 1) Φ_n irréd. sur $\mathbb{F}_q \iff q$ engendre $(\mathbb{Z}/n\mathbb{Z})^*$

2) Dans $\mathbb{F}_p[X]$, $\Phi_{p^r - 1}$ est un produit de polynômes unitaires irréd. de deg r, tous différents.

C'est ce dernier corollaire qui va nous permettre de construire de manière explicite les corps finis. En effet, quand $q = p^n$, on fabrique $\mathbb{F}_q$ en considérant $\mathbb{F}_p[X]/(P(X))$ où P est un facteur irréductible de Φ_{q-1}. $\alpha = \overline{X}$ est alors un générateur de $\mathbb{F}_q^*$.

Ex: Dans $\mathbb{F}_{16}$, $\Phi_{15}(X) = X^8 + X^7 + X^5 + X^4 + X^3 + X + 1$
$= (X^4 + X + 1)(X^4 + X^3 + 1)$ [2]

Donc $\mathbb{F}_{16} = \mathbb{F}_2[X]/(X^4 + X + 1)$, et on peut écrire la table de multiplication dans le corps, et ainsi calculer dans $\mathbb{F}_{16}$.

V APPLICATIONS

1) Codes correcteurs [DEM]

On cherche à transmettre un mot codé comprenant n lettres qui sont des éléments de $\mathbb{F}_2$.

Defs - code C : partie de $\mathbb{F}_2^n$
- vecteur d'erreur : $E = R - C$ où R est le mot effectivement reçu

On veut corriger les erreurs de transmission, dont le nombre correspond au nombre de 1 dans E.

Codes cycliques : BCH

Def : - Un code linéaire de longueur n et de dimension k sur $\mathbb{F}_q$ ($k \leq n$) est un sev de dimension k de $\mathbb{F}_q^n$.
On s'intéresse aux codes binaires ($q = 2$).

- Un code cyclique de longueur n est un code linéaire stable par $T : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$
$(x_1, \dots, x_n) \mapsto (x_2, \dots, x_n, x_1)$

On identifie $\mathbb{F}_2^n$ à $\mathbb{F}_2[X]/(X^n - 1)$ par $(x_1, \dots, x_n) \mapsto x_1 X^{n-1} + \dots + x_n$

On identifie donc un code cyclique à un idéal de $\mathbb{F}_2[X]/(X^n - 1)$.
A un code cyclique on associe donc un polynôme g, générateur de l'idéal, qui est un facteur de $\phi_n \in \mathbb{F}_2[X]$ de degré n.

Def Code cyclique BCH de longueur n et de distance prescrite $\delta \in \mathbb{N}$, $\delta \leq n$
$\Longleftrightarrow$ Code cyclique de polynôme générateur
$g_\Sigma = \prod_{i \in \Sigma} (X - \alpha^i)$

où $\begin{cases} \alpha \text{ est une racine primitive } n^{\text{ième}} \text{ de } 1 \\ \Sigma \subset \mathbb{Z}/n\mathbb{Z} \text{ contenant } 1, 2, \dots, \delta - 1 \text{ et stable} \\ \text{par multiplication par } 2 \end{cases}$

$\Rightarrow \left(c \in C \Longrightarrow c(\alpha) = c(\alpha^2) = \dots = c(\alpha^{\delta - 1}) = 0 \right)$

Prop Si C est un code BCH de longueur n et de distance prescrite $2t + 1$, alors il est possible de corriger t erreurs de transmission.

Rq Dans ce cas, il existe une méthode effective pour retrouver le mot codé.

2) Algorithme de Berlekamp [DEM] [CHI]

TH Soit $f \in \mathbb{F}_p[X]$ de degré $d > 1$, soit $g \in \mathbb{F}_p[X]$ de degré $\leq d$ tq f divise $(g(x))^p - g(x))$. Alors $f = \prod_{k=0}^{p-1} \operatorname{pgcd}(f, g(X) - k)$ et c'est une factorisation non triviale de f.

Cet algorithme ramène le problème de la factorisation de polynômes dans $\mathbb{F}_p$ à un problème d'algèbre linéaire.

Refs : [DEM] Demasure
[CHI] Childs
[PER] Perrin
[SER] Serre

Faire démonstration sur un corps fini.