112 - Corps finis. Applications

On se donne K un corps fini, qu'on suppose dans un premier temps commutatif.

1 Généralités sur les corps finis

1.1 Caractéristique

Proposition-définition 1.1. *Soit K un corps et $\phi : \mathbb{Z} \longrightarrow K, n \longmapsto n.1_K$, morphisme d'anneaux. On appelle* ***caractéristique*** *de K, notée $car(K)$, le générateur positif de l'idéal $\ker\phi$. L'idéal $\ker\phi$ étant premier, la caractéristique d'un corps est soit nulle soit un nombre premier.*
Si K est fini, $car(K) = p > 0$. Le ***sous-corps premier*** *de K est $\mathbb{Z}/p\mathbb{Z}$, ce qui lui confère la structure de $\mathbb{Z}/p\mathbb{Z}$-e.v., d'où $card\,(K) = p^n$, où $n = [K : \mathbb{Z}/p\mathbb{Z}]$.*

Ainsi, le cardinal d'un corps fini est une puissance d'un nombre premier (sa caractéristique). En particulier, il n'existe pas de corps à 6 ou 10 éléments.

1.2 Groupe des inversibles

Remarque. *Tout polynôme $P \in K[X]$ de degré n a au plus n racines.*

Proposition 1.2. *Tout sous-groupe du groupe des inversibles d'un corps fini est monogène. En particulier si $|K| = q$, alors $K^* \simeq \mathbb{Z}/(q-1)\mathbb{Z}$.*

Application. $X^q - X = \prod_{\alpha\in K}(X - \alpha)$.

1.3 Structure des corps finis

Théorème 1.3 (Demazure p.198)**.** *Soit K un corps finis de caractéristique p et de cardinal p^n, $n \in \mathbb{N}^*$. Alors pour tout diviseur r de n, il existe un unique sous-corps de K de cardinal p^r, c'est l'ensemble des $\alpha \in K$, $\alpha^{p^r} = \alpha$.*

Corollaire 1.4. *Soit K un corps fini de caractéristique p. Si α un générateur de $K^\star$, alors $K = \mathbb{Z}/p\mathbb{Z}(\alpha)$ et, notant $n = [K : \mathbb{Z}/p\mathbb{Z}]$, $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de K sur $\mathbb{Z}/p\mathbb{Z}$.*

Théorème 1.5. *Soit p un nombre premier et $n \in \mathbb{N}_\star$. On note $q = p^n$.*
- *Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{Z}/p\mathbb{Z}$.*
- *En particulier, K est unique ? $\mathbb{Z}/p\mathbb{Z}$-isomorphisme près. On le note $\mathbb{F}_q$.*

Proposition 1.6. *$\bigcup_{n\in\mathbb{N}^*} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de tout corps fini de caractéristique p.*

1.4 Groupe des automorphismes d'un corps fini

Proposition 1.7. *Soit K un corps de caractéristique $p \neq 0$. L'application $F : x \longmapsto x^p$ est un endomorphisme de la $\mathbb{Z}/p\mathbb{Z}$-algèbre K, appelé* ***endomorphisme de Frobenius*** *de K.*
De plus, si K est fini, F est un automorphisme. En particulier, si $K = \mathbb{Z}/p\mathbb{Z}$, F est l'identité.

Proposition 1.8. *Soit K un corps fini de caractéristique p. Si $\alpha \in K$ est de degr ? r sur $\mathbb{F}_p$, alors r est le plus petit entier tel que $\alpha^{p^r} = \alpha$, les α^{p^i} sont distincts, pour $0 \leqslant i < r$, et le polynôme minimal de α sur $\mathbb{F}_p$ est $\prod_{1 \leqslant i < r} (X - \alpha^{p^i})$.*

Proposition 1.9. *Soit $q = p^n$, avec p premier. Le groupe des automorphismes de $\mathbb{F}_q$ est cyclique d'ordre n, engendré par l'automorphisme de Frobenius $F : x \longmapsto x^p$.*

1.5 Les carrés de $\mathbb{F}_q$

Soit q une puissance d'un nombre premier p.

Théorème 1.10.
- *Si $p = 2$, tout élément de $\mathbb{F}_q$ est un carré.*
- *Si $p \neq 2$, l'ensemble des carrés de $\mathbb{F}_q^\star$, not ? $\mathbb{F}_q^{\star 2}$, forme un sous-groupe d'indice 2 de $\mathbb{F}_q^\star$; précisément, ce sous-groupe est le noyau de l'homomorphisme $x \longmapsto x^{(q-1)/2}$, à valeurs dans $\{\pm 1\}$.*

Soit p un nombre premier impair.

Définition 1.11. *On appelle* ***symbole de Legendre*** *de $a \in \mathbb{Z}$ l'entier*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si\ p \mid a \\ 1 & si\ p \nmid a\ et\ a\ est\ un\ carr\ ?\ modulo\ p \\ -1 & sinon \end{cases}$$

Théorème 1.12. *Pour $a \in \mathbb{Z}$,*
- *$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$ et $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,*
- *$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ et $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$,*
- *si q est un nombre premier $\neq 2$, alors $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$ (loi de r ?ciprocit ? quadratique).*

Application. *La troisième égalité permet d'établir un cas particulier du théorème de la progression arithmétique de Dirichlet : il existe une infinité de nombres premiers de la forme $4m + 1$.*

Application. *Application Hindry.*

Théorème 1.13 (de Frobenius-Zolotarev)**.** *Soit p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension finie. Pour tout $u \in GL(V)$, $\epsilon(u) = \left(\frac{\det u}{p}\right)$.*

Application. *On peut déduire de ce théorème la signature de l'automorphisme de Frobenius $F : x \longmapsto x^p$ sur $\mathbb{F}_{p^n}$, pour p premier impair et $n \in \mathbb{N}_\star$: $\epsilon(F) = (-1)^{(p-1)(n+1)/2}$ (cf le fait que l'ensemble des automorphismes est engendré par le Frobénius).*

2 Primalité

2.1 Tests divers

Corollaire 2.1. *Le produit des éléments de $K^\star$ est égal à -1.*

Corollaire 2.2 (Théorème de Wilson)**.** *Soit $p \in \mathbb{N}, p \geqslant 2$. p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.*

Fermat, Carmichael.

Lemme 2.3. *Soit $H = \{a \in (\mathbb{Z}/n\mathbb{Z})^* / a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \ [n]\}$. Alors n est premier ssi $H = (\mathbb{Z}/n\mathbb{Z})^*$.*

Le test consiste alors à tester l'égalité du lemme pour des nombres aléatoires. Si n passe successivement k tests, on peut dire qu'il est premier avec une probabilité supérieure à $1 - 2^{-k}$.

2.2 RSA

Cf Hindry

3 Polynômes sur les corps finis

3.1 Polynômes irréductibles

Fixons un entier $q = p^r$, avec p premier et $r \in \mathbb{N}_\star$. On note $I(n,q)$, l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$.

Proposition 3.1. *Pour $n \in \mathbb{N}_\star$, on a l'égalité suivante dans $\mathbb{F}_q[X]$: $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P$*

Il existe donc des polynômes irréductibles de tout degré sur $\mathbb{F}_p$. Tout corps fini de cardianal $q = p^n$ peut ainsi être réalisé comme le corps de rupture sur $\mathbb{F}_p$ d'un polynôme irréductible de degré n. Par exemple, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.

Corollaire 3.2. *Soit $P \in \mathbb{F}_q[X]$ de degré $n \in \mathbb{N}_\star$. P est irréductible sur $\mathbb{F}_q$ si et seulement si P divise $X^{q^n} - X$ et si pour tout facteur premier r de n, P est premier ? $X^{q^{n/r}} - X$.*

Application. *$X^p - X - a$, avec $a \in \mathbb{F}_p^\star$, est irréductible sur $\mathbb{F}_p$.*

Proposition 3.3. *$X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$, car sans racine dans $\mathbb{F}_4$. On en déduit par exemple, par réduction modulo 2 que $X^4 + 8X^2 + 17X - 1$ est irréductible sur $\mathbb{Z}$.*

3.2 Polynômes cyclotomiques

Définition, premières propriétés.

Théorème 3.4 (de Wedderburn)**.** *Tout corps fini est commutatif.*

Irréductibilité, réduction sur $\mathbb{F}_q$, coro 8. 16 [Dem], application à la construction effective de corps finis.

3.3 Algorithme de Berlekamp

Soit p un nombre premier et $q = p^s$.

Lemme 3.5. *Pour $R \in \mathbb{F}_q[X]$, l'application $S_R : Q(X) \mod R \longmapsto Q(X^q) \mod R$ est un endomorphisme $\mathbb{F}_q$-linéaire de $\mathbb{F}_q[X]/(R)$ qui co ?ncide avec l'élévation à la puissance q dans $\mathbb{F}_q[X]/(R)$.*

Algorithme 1 (Algorithme de Berlekamp)**. Entrée :** *Un polyn ?me $P \in \mathbb{F}_q[X]$ sans facteur carr ?.*

Sortie : *La d ?composition en facteurs irr ?ductibles de P.*

1. *D ?terminer la matrice $S_P - Id$ dans la base $(1, x, \ldots, x^{\deg P - 1})$ de $\mathbb{F}_q[X]/(P)$, où $x = X \mod P$ et*
   calculer $r = \dim(\ker(S_P - Id)) = \deg(P) - rg(S_P - Id)$ (nombre de facteurs irr ?ductibles de P).
2. ***Si*** *$r = 1$, retourner P*
3. ***Sinon*** *Calculer $V \in \mathbb{F}_q[X]$ non constant modulo P et tel que $V \mod P ? \in \ker(S_P - Id)$.*
   $P = \prod_{\alpha \in \mathbb{F}_q} pgcd(P, V - \alpha)$ et appeler l'algorithme pour chacun des facteurs non triviaux du produit.

Il s'agit maintenant de savoir se ramener au cas d'un polyn ?me sans facteur carr ?.

Proposition 3.6. *Soit $P \in \mathbb{F}_q[X]$. Si Q est un facteur irréductible de P de multiplicité α, alors Q est un facteur irr ?ductible de $pgcd(P, P')$ de multiplicit ? $\alpha - 1$ si $p \nmid \alpha$ et α si $p \mid \alpha$.*

Ainsi $P \in \mathbb{F}_q[X]$ est sans facteur carré si et seulement si $\text{pgcd}(P, P') = 1$. Notons également que $\text{pgcd}(P, P') = P$ si et seulement s'il existe $R \in \mathbb{F}_q[X]$, tel que $P = R^p$, soit $P' = 0$.

Algorithme 2 (Factorisation d'un polynôme sur un corps fini)**. Entr ?e :** *Un polynôme $P \in \mathbb{F}_q[X]$.*

Sortie : *La décomposition en facteurs irréductibles de P.*

1. *Si P est constant retourner P.*
2. *Sinon calculer $pgcd(P, P')$:*
   - *si $pgcd(P, P') = 1$, appliquer l'algorithme de Berlekamp ? P,*
   - *si $pgcd(P, P') = P$, appeler l'algorithme sur R, tel que $R^p = P$,*
   - *sinon, appliquer l'algorithme aux deux facteurs non triviaux de P : $pgcd(P, P')$ et $P/pgcd(P, P')$.*

4 Codes correcteurs

On souhaite transmettre un message de a de k bits. Le m ?canisme de codage consiste ? associer ? chacun des 2^k mots possibles un mot du code de n bits, $n \geqslant k$. Le mot du code m d ?duit du message a est transmis. Le canal de transmission pouvant introduire des erreurs, on obtient en sortie un mot m'. Il s'agit alors de reconstruire m.

Fixons un corps fini $\mathbb{F}_q$, où $q = p^r$, et deux entiers k et n avec $0 \leqslant k \leqslant n$.

Définition 4.1. *On appelle* ***code linéaire*** *de* ***longueur*** n *et de* ***dimension*** k *sur* $\mathbb{F}_q$*, un sous-espace vectoriel* C *de dimension* k *de* $\mathbb{F}_q^n$*.*

On appelle ***code cyclique*** *de longueur* n*, un code linéaire* C *stable par d ?calage circulaire :*

$$\forall\, a = (a_0, \ldots, a_{n-1}) \in C, \quad \gamma(a) = (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

Définition 4.2. *La* ***distance de Hamming*** *entre deux mots* $x, y \in \mathbb{F}_q$ *est* $d(x,y) = w(x-y)$*, où* $w(x)$ *est le* ***poids*** *de* x*, i.e. le nombre de coordonn ?es non nulles de* x*.*

La ***distance minimale*** d *d'un code correcteur* C *est* $d = \min\{d(x,y)\ /?x, y \in C, x \neq y\}$*.* C *est alors* $\lfloor \frac{d-1}{2} \rfloor$***-correcteur****, i.e. capable de corriger* $\lfloor \frac{d-1}{2} \rfloor$ *erreurs de transmission.*

Proposition 4.3. *Soit* $g = a_{n-k}X^{n-k} + \cdots + a_0$ *un diviseur unitaire de* $X^n - 1$ *dans* $\mathbb{F}_q[X]$ *et le mot correspondant* $m = (a_0, \ldots, a_{n-k}, 0, \ldots, 0) \in \mathbb{F}_q^n$*. Les* k *mots* $m, \gamma(m), \ldots, \gamma^{k-1}(m)$ *forment une base d'un code cyclique sur* $\mathbb{F}_q$*.*

Réciproquement, tout code cyclique C *sur* $\mathbb{F}_q$ *s'obtient par la construction pr ?c ?dente, et le polyn ?me* g *est uniquement d ?termin ?. On l'appelle le* ***générateur*** *du code cyclique* C*.*

Références

[Dem] M. Demazure *Cours d'alg ?bre*

[Per] D. Perrin, *Cours d'alg ?bre*

[Beck] V. Beck, J. Malick, G. Peyr ? *Objectif agr ?gation*

D ?veloppements :

- Th ?or ?me de Frobenius-Zolotarev ([Beck], 104, 105, 110 ?, 112, 123)
- Algorithme de Berlekamp ([Beck], 110 ?, 112, 116, 118)
- D ?codage des codes BCH ([Dem], 109, 112, 113, 116)
- Th ?or ?me de Wedderburn ([Per], 101, 104, 112)