123. Corps finis. Applications.

(ou pourquoi les polynômes cyclothymiques sont irrésistibles sur $\mathbb{Q}$)

1 Structure des corps finis

1.1 Caractéristique

Définition 1. Soit K un corps quelconque. On appelle *sous-corps premier* de K le plus petit sous-corps de K.

Définition 2. Le morphisme d'anneaux $n \mapsto n \cdot 1_K$ a pour noyau l'idéal premier $p\mathbb{Z}$. On appelle *caractéristique* de K le nombre p premier ou nul, noté $\text{car}(K)$.

Remarque 3. Si $\text{car}(K) = 0$, K est infini et de sous-corps premier $\mathbb{Q}$.

Remarque 4. Si K est fini, $\text{car}(K) = p > 0$ et son sous-corps premier est $\mathbb{Z}/p\mathbb{Z}$ aussi noté $\mathbb{F}_p$.

Remarque 5. La réciproque n'est pas vraie, $\mathbb{F}_p(X)$ est un corps infini de caractéristique $p > 0$.

Proposition 6. Si F est un sous-corps de K alors K est un F-espace vectoriel.

Remarque 7. Si $F \subseteq K$ sont deux corps finis et $\dim_F K = n$ alors $|K| = |F|^n$.

Application 8. Le cardinal d'un corps fini est un nombre primaire, c'est-à-dire une puissance d'un nombre premier.

1.2 Caractérisation

Définition 9. Soit $P \in K[X]$ un polynôme irréductible. On appelle *corps de rupture* de P sur K une extension $L = K(\alpha)$ où $P(\alpha) = 0$.

Théorème 10. Il existe un corps de rupture de P sur K unique à isomorphisme près.

Définition 11. Soit $P \in K[X]$ un polynôme. On appelle *corps de décomposition* de P sur K la plus petite extension L de K où P est scindé.

Théorème 12. Il existe un corps de décomposition de P sur K unique à isomorphisme près.

Définition 13 (Endomorphisme de Frobenius)**.** Soit K un corps de caractéristique $p > 0$. L'application $x \mapsto x^p$ est un morphisme d'anneaux.

Remarque 14. Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, c'est l'identité.

Théorème 15. Soit p un nombre premier et k un entier. On pose $q = p^k$. Il existe un corps à q éléments noté $\mathbb{F}_q$, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Remarque 16. $\mathbb{F}_q$ est unique à isomorphisme près.

Application 17. $Q \in \mathbb{F}_q[X] \Leftrightarrow Q(X^q) = (Q(X))^q$.

Application 18. Les racines d'un polynôme de $\mathbb{F}_q[X]$ sont stables par l'application $x \mapsto x^q$.

Application 19. Soit P un polynôme irréductible sur $\mathbb{F}_q$ de degré m et α une racine de P. Alors m est le plus petit entier tel que $\alpha^{p^m} = \alpha$ et P est associé à $(X-\alpha)(X-\alpha^p)\dots(X-\alpha^{p^{m-1}})$.

Application 20. Si P est un polynôme irréductible sur $\mathbb{F}_q$, alors son corps de rupture coïncide avec son corps de décomposition.

Application 21. Deux polynômes de même degré irréductibles sur $\mathbb{F}_q$ ont le même corps de décomposition.

Définition 22. Un corps K est dit *parfait* si tous les polynômes irréductibles sur K n'admettent que des racines simples.

Proposition 23. Tout corps fini est parfait.

Théorème 24. Soit $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ une extension de corps finis. L'application :

$$\begin{array}{ccc} \left\{ \begin{array}{c} k \text{ sous-corps de } \mathbb{F}_{q^m} \text{ contenant } \mathbb{F}_q \\ \mathbb{F}_q \subseteq k \subseteq \mathbb{F}_{q^m} \end{array} \right\} & \to & \{\text{diviseurs de } m\} \\ k & \mapsto & [k : \mathbb{F}_q] \end{array}$$

est une bijection de réciproque :

$$d \mapsto \{\text{racines de } X^{q^d} - X \text{ sur } \mathbb{F}_{q^m}\}.$$

Corollaire 25. $\mathbb{F}_{q^m}$ a un unique sous-corps de cardinal q^k où k divise m.

1.3 $\mathbb{F}_q^*$

Théorème 26. $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$.

Application 27 (Caractérisation des carrés de $\mathbb{F}_q$)**.** On suppose $p > 2$.
$x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

Application 28. $-1 \in \mathbb{F}_q^2 \Leftrightarrow q \equiv 1 \pmod 4$.

Application 29. Il existe une infinité de nombres premiers de la forme $4m+1$.

2 Polynômes de $\mathbb{F}_q[X]$

2.1 Cyclotomie

Définition 30. Soit $n \in \mathbb{N}^*$. On appelle *n-ième polynôme cyclotomique* le polynôme $\Phi_n(X)$ défini par :

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2\pi i k/n}).$$

Exemple 31. $\Phi_6(X) = X^2 - X + 1$.

Remarque 32. $\deg \Phi_n = \varphi(n)$.

Proposition 33. $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

Application 34 (Wedderburn)**.** Tout corps fini est commutatif.

Théorème 35 (Gauss)**.** Pour tout $n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Q}$.

Théorème 36. Soit n un entier positif premier à q et r l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$. Alors Φ_n se décompose sur $\mathbb{F}_q$ en produit de polynômes unitaires irréductibles de degré r, tous différents.

Corollaire 37. Si q engendre $(\mathbb{Z}/n\mathbb{Z})^*$, Φ_n est irréductible sur $\mathbb{F}_q$.

Corollaire 38. Sur $\mathbb{F}_q$, Φ_{q^r-1} est produit de polynômes unitaires irréductibles de degré r, tous différents.

Exemple 39. $\Phi_7 = 1 + X + \ldots + X^6$ est irréductible sur $\mathbb{Q}$ mais en tant que polynôme de $\mathbb{F}_2[X]$ se factorise en $(1 + X + X^3)(1 + X^2 + X^3)$.

2.2 Irréductibilité

Application 40. Pour tout nombre premier p et tout entier $n > 0$, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p$.

Exemple 41. $X^q - X + 1$ est irréductible sur $\mathbb{F}_q$.

Application 42. Un corps fini n'est jamais algébriquement clos.

Théorème 43. Soit A un anneau factoriel, K son corps de fractions et I un idéal premier de A. On note $B = A/I$, c'est un sous-anneau intègre de A. Soit $P \in A[X]$ et $\overline{P}$ sa réduction modulo I. Alors si $\deg_A P = \deg_B P$ et $\overline{P}$ est irréductible sur B, alors P est irréductible sur K.

Proposition 44. $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais est réductible sur $\mathbb{F}_p$.

Théorème 45. Soit $P \in k[X]$ de degré n. P est irréductible sur k si et seulement si P n'a pas de racines dans les extensions K de k vérifiant $[K : k] \leqslant n/2$.

Théorème 46. Soit $P \in k[X]$ un polynôme irréductible de degré n et soit K une extension de degré m où $m \wedge n = 1$. Alors P est encore irréductible sur K.

2.3 Critères algorithmiques

Proposition 47. Soit $n \in \mathbb{N}^*$. $X^{p^n} - X$ est le produit de tous les polynômes unitaires irréductibles sur $\mathbb{F}_p$ de degré divisant n.

Corollaire 48. Soit $m_n(p)$ le nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_p$. Alors :

$$\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leqslant m_n(p) \leqslant \frac{p^n}{n}.$$

Application 49. Un polynôme unitaire de grand degré n choisi au hasard a environ une chance sur n d'être irréductible.

Application 50. P est irréductible sur $\mathbb{F}_p$ si et seulement si P divise $X^{p^n} - X$ et pour tout facteur premier q de n, P est premier à $X^{p^{n/q}} - X$.

Application 51. Si P est un polynôme irréductible de degré n sur $\mathbb{F}_p$, $\mathbb{F}_p[X]/(P)$ est un corps à $q = p^n$ éléments.

Exemple 52. $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$.

Définition 53. P est dit *sans facteurs multiples* si les facteurs irréductibles de P apparaissent tous avec multiplicité 1.

Proposition 54. P et P' sont premiers entre eux si et seulement si P est sans facteurs multiples.

Algorithme 55 (Berlekamp)**.** Soit P un polynôme réductible de $\mathbb{F}_p[X]$ sans facteurs multiples et Q un polynôme non constant modulo P vérifiant $Q^p \equiv Q \pmod P$. Alors :

$$P = \prod_{\alpha \in \mathbb{F}_p} \operatorname{pgcd}(P, Q - \alpha)$$

est une décomposition non triviale de P.

Algorithme 56 (Berlekamp probabiliste)**.** Soit P un polynôme réductible de $\mathbb{F}_p[X]$ sans facteurs multiples et Q un polynôme non constant modulo P vérifiant $Q^p \equiv Q \pmod P$. Alors :

$$P = \operatorname{pgcd}(P, Q) \operatorname{pgcd}(P, Q^{(p-1)/2} + 1) \operatorname{pgcd}(P, Q^{(p-1)/2} - 1)$$

est une décomposition non triviale de P avec probabilité $> 1/2$.

Algorithme 57 (Cantor-Zassenhaus)**.** Soit P un polynôme réductible de $\mathbb{F}_p[X]$. Alors $P_r = \operatorname{pgcd}(P, X^{p^r} - X)$ est produit de polynômes irréductibles de degré r exactement et si Q est tiré aléatoirement parmi les polynômes unitaires irréductibles de degré $< 2r$, alors :

$$P_r = \operatorname{pgcd}(P, Q) \operatorname{pgcd}(P, Q^{(p^r-1)/2} - 1) \operatorname{pgcd}(P, Q^{(p^r-1)/2} + 1)$$

est une décomposition non triviale de P avec probabilité $> 1/2$.

3 Codes correcteurs

3.1 Codes linéaires cycliques

Définition 58. On appelle *code linéaire* sur $\mathbb{F}_q$ de paramètres (n, k, d) (de longueur n, de dimension k) un sous-espace vectoriel C de dimension k de $\mathbb{F}_q^n$. On appelle *poids* d'un mot $m \in \mathbb{F}_q^n$ le nombre de composantes non nulles de m. La *distance minimale* d du code est donnée par :

$$d = \min_{m,m' \in C} w(m - m') = \min_{m \in C} w(m).$$

Exemple 59 (Code de Hamming de longueur 7, de paramètres (7, 4, 3))**.**

$$\gamma(a_0, a_1, a_2, a_3) = a_0(1101000) + a_1(0110100) + a_2(0011010) + a_3(0001101)$$

$$\begin{array}{ll}
\gamma(0000) = (0000000) & \gamma(1000) = (1101000) \\
\gamma(0100) = (0110100) & \gamma(0010) = (0011010) \\
\gamma(0001) = (0001101) & \gamma(1100) = (1011100) \\
\gamma(1010) = (1110010) & \gamma(1001) = (1100101) \\
\gamma(0110) = (0101110) & \gamma(0101) = (0111001) \\
\gamma(0011) = (0010111) & \gamma(1110) = (1000110) \\
\gamma(1101) = (1010001) & \gamma(1011) = (1111111) \\
\gamma(0111) = (0100011) & \gamma(1111) = (1001011)
\end{array}$$

Proposition 60. Si C est de distance minimale d, on peut détecter l'existence d'une erreur e telle que $w(e) < d$ et corriger une erreur telle que $w(e) < d/2$. Si $2t < d$, le code permet de corriger une erreur e telle que $w(e) \leqslant t$, il est dit *t-correcteur*.

Définition 61. On note $B(m, t)$ la boule de rayon t centrée en m :

$$B(m, t) = \{m' \in \mathbb{F}_q^n, w(m - m') \leqslant t\}.$$

C est t-correcteur si les q^k boules sont deux à deux disjointes. C est dit *parfait* si ces boules forment une partition de $\mathbb{F}_q^n$.

Exemple 62. Le code de Hamming est parfait.

Proposition 63 (Borne de Singleton)**.** $d \leqslant n + 1 - k$.

Définition 64. Un code linéaire C est dit *cyclique* s'il est stable par tous les décalages circulaires : si σ est le décalage circulaire à droite sur $\mathbb{F}_q^n$ et $m \in C$, alors $\sigma(m) \in C$.

Définition 65. Pour tout mot m, il existe un plus petit code linéaire cyclique qui le contient, on l'appelle le code cyclique *engendré* par m.

Proposition 66. À chaque vecteur $m = (m_0, \ldots, m_{n-1}) \in \mathbb{F}_q^n$ on fait correspondre le polynôme $m(X) = m_0 + m_1 X + \ldots + m_{n-1} X^{n-1} \in \mathbb{F}_q[X]$. Alors $\sigma(m)(X) \equiv Xm(X) \pmod{X^n - 1}$.

Proposition 67. Soit $g(X) = a_0 + \ldots + a_{n-k} X^{n-k}$ $(a_{n-k} = 1)$ un diviseur unitaire de $X^n - 1$ dans $\mathbb{F}_q[X]$ et $m = (a_0, \ldots, a_{n-k})$ le mot correspondant. Alors $(m, \sigma(m), \ldots, \sigma^{k-1}(m))$ est une base d'un code cyclique de dimension k. Réciproquement, tout code cyclique de longueur n s'obtient par cette construction.

Définition 68. On dit que g est le *générateur* du code cyclique C.

3.2 Classes cyclotomiques

Remarque 69. Soit $\mathbb{F}_q$ un corps, K le corps de décomposition de $X^n - 1$ sur $\mathbb{F}_q$. $X^n - 1 = \prod_{i=0}^{n-1}(X - \alpha^i)$ donc si g_Σ est un diviseur de $X^n - 1$ alors $g_\Sigma = \prod_{i \in \Sigma}(X - \alpha^i)$.

Proposition 70. g_Σ est à coefficients dans $\mathbb{F}_q$ si et seulement si Σ est stable par multiplication par q.

Définition 71. Les parties stables minimales $\Sigma_j = \{j, qj, \ldots, q^{s-1} j\}$ où s est l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$ sont appelées les *classes cyclotomiques*.

Code 72 (Hamming)**.** On choisit $q = 2$ et $n = 2^r - 1$. Le code ayant pour générateur le polynôme correspondant à la classe cyclotomique $\Sigma = \{1, 2, \ldots, 2^{r-1}\}$ est de paramètres $(2^r - 1, 2^r - r - 1, 3)$. Il est 1-correcteur et parfait.

Code 73 (Reed-Solomon)**.** On choisit $q > 2$, $n = q - 1$, k tel que $1 \leqslant k \leqslant q - 1$ et α un générateur de $\mathbb{F}_q^*$. On pose $g = \prod_{i=1}^{q-1-k}(X - \alpha^i) \in \mathbb{F}_q[X]$. Alors g est le générateur d'un code cyclique de paramètres $(q - 1, k, q - k)$.

Code 74 (BCH)**.** On choisit $n = q^m - 1$, δ un paramètre supplémentaire (*distance assignée*) tel que $1 < \delta \leqslant q^m - 1$ et Σ la plus petite partie de $\mathbb{Z}/(q^m - 1)\mathbb{Z}$ contenant $\{1, \ldots, \delta - 1\}$ et stable par multiplication par q. On a $|\Sigma| \leqslant m(\delta - 1)$, $k \geqslant q^m - 1 - m(\delta - 1)$ et la distance minimale de ce code est supérieure ou égale à δ.

Code 75 (BCH binaire)**.** On choisit $q = 2$, $n = 2^m - 1$, $\delta = 2t + 1$ tel que $1 < \delta \leqslant 2^m - 1$ et Σ la plus petite partie de $\mathbb{Z}/(2^m - 1)\mathbb{Z}$ contenant $\{1, \ldots, \delta - 1\}$ et stable par multiplication par 2. On a $|\Sigma| \leqslant mt$, la dimension $k \geqslant 2^m - 1 - mt$ et la distance minimale de ce code est impaire et supérieure ou égale à δ.

Développements

Algorithme de Berlekamp
Algorithme de décodage des codes BCH

Références

$Demazure_{Knuth}(Perrin)$

Jill-Jênn Vie – `agreg-cachan.fr`