Théorie de l'information et codage **2010/2011**

Cours 10 — 3 mai

Enseignant: Marc Lelarge *Scribe: Rémi Varloot*

Pour information

- Page web du cours
  `http://www.di.ens.fr/~lelarge/info11.html`

10.1 Corps finis

Théorème 10.1.1 *Si $\pi(x)$ est irréductible sur $\mathbf{F}(p)$ et a degré m. Alors l'ensemble des polynômes de degré $\leq m-1$ à coefficients dans $\mathbf{F}(p)$ avec les opérations modulo $\pi(x)$ forme un corps d'ordre p^m.*

On note α la classe d'équivalence du polynôme x. Par construction $\pi(\alpha) = 0$. $\mathbf{F}(p^m)$ est constitué de tous les polynômes en α de degré $\leq m-1$ à coefficients dans $\mathbf{F}(p)$.

10.1.1 Introduction

Définition 10.1.1 *La caractéristique d'un corps fini $\mathbf{F}$ est le plus petit entier p tel que* $1+1+\ldots+1 = 0$ *(où* 1 *apparaît p fois).*

Remarque : Soit $\mathbf{F}$ de caractéristique p (premier) et de cardinal q. Si $p = q$ alors $\mathbf{F} = \mathbf{F}(p)$, et si $q > p$, alors on peut choisir un ensemble maximal $\{\beta_0 = 1, \ldots \beta_{m-1}\}$ d'éléments de $\mathbf{F}$ linéairement indépendants sur $\mathbf{F}(p)$.

$\mathbf{F}$ est un e.v. de dimension m sur $\mathbf{F}(p)$ et contient $q = p^m$ éléments. On note $\mathbf{F}^\star$ les $q-1$ éléments non nuls de $\mathbf{F}$.

Théorème 10.1.2 *$\mathbf{F}^\star$ est un groupe multiplicatif cyclique d'ordre $p^m - 1$.*

Démonstration. Par définition, $\mathbf{F}^\star$ est un groupe multiplicatif.
Soit $\alpha \in \mathbf{F}^\star$. Comme $|\mathbf{F}^\star| = p^m - 1$, α^i a au plus $p^m - 1$ valeurs différentes. Il existe donc r, $1 \leq r \leq p^m - 1$, tel que $\alpha^r = 1$. Le plus petit r vérifiant cette propriété est appelé l'ordre de α.
Soit α un élément de $\mathbf{F}^\star$ d'ordre r maximal. Montrons que l'ordre l de tout élément β de $\mathbf{F}^\star$ divise r.

Soit π premier tel que $r = \pi^a r'$ et $l = \pi^b l'$ avec $\text{pgcd}(r', \pi) = \text{pgcd}(l', \pi) = 1$.
α^{π^a} a pour ordre r' et $\beta^{l'}$ a pour ordre π^b, donc $\alpha^{\pi^a}\beta^{l'}$ a pour ordre $\pi^b r'$.
Par conséquent, $\pi^b r' \leq r = \pi^a r'$, soit $b \leq a$.
Cela montre que l divise r.
Pour tout $\beta \in \mathbf{F}^\star$, β est donc solution de $X^r - 1 = 0$.
$\prod_{\beta \in \mathbf{F}^\star}(X - \beta)$ divise $X^r - 1$, donc $r \geq p^m - 1$, et donc $r = p^m - 1$ et $\mathbf{F}^\star$ est cyclique. □

Corollaire 10.1.1 (Petit théorème de Fermat) *Tout élément β d'un corps $\mathbf{F}$ d'ordre p^m satisfait l'identité $\beta^{p^m} = \beta$, donc $X^{p^m} - X = \prod_{\beta \in \mathbf{F}}(X - \beta)$.*

Un élément α de $\mathbf{F}$ est dit primitif si son ordre est $p^m - 1$.

Théorème 10.1.3 *Tout corps fini a un élément primitif.*

Démonstration. Il suffit de prendre un élément générant $\mathbf{F}^\star$. □

10.1.2 Polynômes minimaux

Définition 10.1.2 *Le polynôme minimal sur $\mathbf{F}(p)$ de β est le polynôme unitaire M de degré minimal, à coefficients dans $\mathbf{F}(p)$, tel que $M(\beta) = 0$.*

Propriétés des polynômes minimaux

Soit $M(X)$ polynôme minimal de β dans $\mathbf{F}(p^m)$.

(M1) $M(X)$ est irréductible.

(M2) Si $f(X)$ est un polynôme à coefficients dans $\mathbf{F}(p)$ tel que $f(\beta) = 0$, alors $M(X)$ divise $f(X)$.

Démonstration. On écrit la division euclidienne de f par M :

$$f(X) = a(X)M(X) + r(X) \qquad \deg r \leq \deg M - 1$$

$$0 = 0 + r(\beta) \Rightarrow r(\beta) \equiv 0$$

Donc r est le polynôme nul. □

(M3) $M(X)$ divise $X^{p^m} - X$.

(M4) $\deg M(X) \leq m$.

Démonstration. $\mathbf{F}(p^m)$ est un espace vectoriel de dimension m sur $\mathbf{F}(p)$. □

(M5) Le polynôme minimal d'un élément primitif de $\mathbf{F}(p^m)$ a pour degré m. Un tel polynôme est appelé polynôme primitif.

Démonstration. Soit β un élément primitif de polynôme minimal $M(X)$ de degré d. On peut utiliser $M(X)$ pour générer $\mathbf{F}$ d'ordre p^d (comme dans le Théorème 10.1.1), $\mathbf{F}$ contient β et donc tout $\mathbf{F}(p^m)$ donc $d \geq m$. □

Remarque : si un polynôme irréductible π est utilisé pour construire $\mathbf{F}(p^m)$, et si α dans $\mathbf{F}(p^m)$ est racine de $\pi(X)$, alors $\pi(X)$ est le polynôme minimal de α.

Théorème 10.1.4 *Tous les corps finis d'ordre p^m sont isomorphes.*

Démonstration. Soient F, G deux corps d'ordre p^m et soit α un élément primitif de F de polynôme minimal $M(x)$. Par (M3), $M(x)$ divise $x^{p^m} - x$. Par le petit théorème de Fermat, il existe $\beta \in G$ qui a pour polynôme minimal $M(x)$. Il est ensuite facile de voir que l'application $\alpha \leftrightarrow \beta$ s'étant en une fonction bijective de F dans G qui préserve l'addition et la multiplication. □

Exemple 10.1.1:
On se place dans $\mathbf{F}(2^3)$ défini soir par $x^3 + x + 1$ soit par $x^3 + x^2 + 1$.

$X^3 + X + 1$	$X^3 + X^2 + 1$
$000 = 0$	$000 = 0$
$100 = 1$	$100 = 1$
$010 = \alpha$	$010 = \gamma$
$001 = \alpha^2$	$001 = \gamma^2$
$110 = \alpha^3$	$101 = \gamma^3$
$011 = \alpha^4$	$111 = \gamma^4$
$111 = \alpha^5$	$110 = \gamma^5$
$101 = \alpha^6$	$011 = \gamma^6$

Isomorphisme :

$$\alpha \leftrightarrow \gamma^3$$

Théorème 10.1.5 *Pour tout nombre premier p et entier $m \geq 1$, il existe un corps d'ordre p^m qui est noté $\mathbf{F}(p^m)$.*

Démonstration. Pour $m = 1$, il s'agit de $\mathbf{Z}/p\mathbf{Z}$.
Pour $m > 1$, on construit $\mathbf{F}_1 = \mathbf{F}(p), \mathbf{F}_2, \ldots, \mathbf{F}_r$ jusqu'à contenir tous les zéros de $X^{p^m} - X$ dans $\mathbf{F}_r$, qui est alors d'ordre p^m. Soit $f(x)$ un facteur irréductible de degré ≥ 2 de $X^{p^m} - X$ sur $\mathbf{F}(p) = \mathbf{F}_1$. On l'utilise pour obtenir une extension $\mathbf{F}_2$ de $\mathbf{F}_1$... □

Théorème 10.1.6
– $\mathbf{F}(p^r)$ *contient un sous-corps* $\mathbf{F}(p^s)$ *si et seulement si* s *divise* r.
– $\beta \in \mathbf{F}(p^r)$ *est dans* $\mathbf{F}(p^s)$ *si et seulement si* $\beta^{p^s} = \beta$.

Exemple 10.1.2:
$\mathbf{F}(4)$ et $\mathbf{F}(8)$ sont deux extensions de $\mathbf{F}(2)$. $\mathbf{F}(16)$ a comme sous corps $\mathbf{F}(4)$ et $\mathbf{F}(2)$, mais pas $\mathbf{F}(8)$. $\mathbf{F}(64)$ a comme sous corps $\mathbf{F}(8)$, $\mathbf{F}(4)$, $\mathbf{F}(2)$, mais pas $\mathbf{F}(16)$ ni $\mathbf{F}(32)$.

(M6) Conjugués et classes cyclotomiques : β et β^p ont même polynôme minimal. En particulier, dans $\mathbf{F}(2^m)$, β et β^2 ont même polynôme minimal.

Exemple 10.1.3:
Soit $\beta \in \mathbf{F}\left(2^4\right)$ de polynôme minimal $X^4 + X^3 + 1$. Alors

$$\left(\beta^2\right)^4 + \left(\beta^2\right)^3 + 1 = \left(\beta^4 + \beta^3 + 1\right)^2 = 0$$

Donc par (M2) le polynôme minimal de β^2 divise $X^4 + X^3 + 1$. Mais $\left(\beta^2\right)^8 = \beta$ et donc on peut utiliser le même argument pour montrer que le polynôme minimal de β divise celui de β^2.

Deux éléments ayant le même polynôme minimal sont dits conjugués.

Exemple 10.1.4:
On se place dans $\mathbf{F}\left(2^4\right)$. Les éléments suivants (sur chaque ligne) ont même polynôme minimal :

$$\begin{array}{llllll} \alpha, & \alpha^2, & \alpha^4, & \alpha^8, & \alpha^{16} = \alpha & \\ \alpha^3, & \alpha^6, & \alpha^{12}, & \alpha^{24} = \alpha^9, & \alpha^{18} = \alpha^3 & \\ \alpha^5, & \alpha^{10}, & \alpha^{20} = \alpha^5 & & & \\ \alpha^7, & \alpha^{14}, & \alpha^{28} = \alpha^{13}, & \alpha^{26} = \alpha^{11}, & \alpha^{22} = \alpha^7 & \end{array}$$

Les puissances de α tombent dans des ensembles disjoints. Ce sont les classes cyclotomiques.

Définition 10.1.3 *L'opération de multiplier par p divise les entiers modulo $p^m - 1$ en ensembles appelés classes cyclotomiques modulo $p^m - 1$. Classe cyclotomique contenant s :* $\left\{sp^k : 0 \leq k \leq m_s - 1, m_s = \min\left(\left\{j : sp^j \equiv s\,[p^m - 1]\right\}\right)\right\}$

Exemple 10.1.5:
Pour p=2 et $m = 4$, les classes cyclotomiques modulo 15 sont :

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8\} \\ C_3 &= \{3, 6, 12, 9\} \\ C_5 &= \{5, 10\} \\ C_7 &= \{7, 14, 13, 11\} \end{aligned}$$

Dans l'exemple précédent, les éléments $1, 2, 5, 7$ sont des représentants de classe.

Définition 10.1.4 *Soit $M^{(i)}(X)$ le polynôme minimal de α^i dans $\mathbf{F}(p^m)$. Par (M6), on a :*

$$M^{(pi)}(X) = M^{(i)}(X)$$

Si i est dans la classe cyclotomique C_s, alors $\prod_{j \in C_s}\left(X - \alpha^j\right)$ divise $M^{(i)}(X)$ dans $\mathbf{F}(p^m)$.

(M7) Pour tout i dans C_s, $M^{(i)}(X) = \prod_{j \in C_S}\left(X - \alpha^j\right)$.
De plus, $X^{p^m-1} = \prod_s M^{(s)}(X)$ où s parcoure l'ensemble des représentants de classe.

10.1.3 Comment trouver des polynômes irréductibles

Théorème 10.1.7 *Pour tout corps $\mathbf{F}(q)$, $X^{q^m} - X$ est le produit de tous les polynômes unitaires irréductibles sur $\mathbf{F}(q)$ dont le degré divise m.*

Application: On prend $q = 2$.

$$m = 1 \quad : \quad X^2 + X = X(X + 1)$$

et X est le polynôme minimal de 0 tandis que $X + 1$ est celui de 1 dans $\mathbf{F}(2)$.

$$m = 2 \quad : \quad X^4 + X = X(X + 1)\left(X^2 + X + 1\right)$$

On a $M^{(0)}(X) = X + 1$ et $M^{(1)}(X) = M^{(2)}(X) = X^2 + X + 1$ ayant pour racines α et α^2.

$$m = 3 \quad : \quad X^8 + X = X(X+1)\left(X^3 + X + 1\right)\left(X^3 + X^2 + 1\right)$$

Dans $\mathbf{F}(2^3)$ défini par $\alpha^3 + \alpha + 1 = 0$, on a : $M^{(1)}(X) = M^{(2)}(X) = M^{(4)}(X) = X^3 + X + 1$ et $M^{(3)}(X) = M^{(6)}(X) = M^{(5)}(X) = X^3 + X^2 + 1$.

Définition 10.1.5 *Le polynôme réciproque de $f(X)$ est $X^{\deg f} f\left(X^{-1}\right)$.*

Les polynômes $X^3 + X + 1$ et $X^3 + X^2 + 1$ sont réciproques. Plus généralement le polynôme réciproque de

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

est

$$a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n.$$

Si $a_0 \neq 0$, les racines du polynôme réciproque sont les inverses des racines du polynôme. Le réciproque d'un polynôme irréductible est irréductible.

$$m = 4 \quad : \quad X^{16} + X = X(X+1)\left(X^2 + X + 1\right)\left(X^4 + X + 1\right)\left(X^4 + X^3 + 1\right)\left(X^4 + X^3 + X^2 + X + 1\right)$$

Eléments de $\mathbf{F}(2^4)$ défini par $\alpha^4 + \alpha + 1 = 0$:

0000	0	0
1000	1	1
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$1 + \alpha$	α^4
0110	$\alpha + \alpha^2$	α^5
0011	$\alpha^2 + \alpha^3$	α^6
1101	$1 + \alpha + \alpha^3$	α^7
1010	$1 + \alpha^2$	α^8
0101	$\alpha + \alpha^3$	α^9
1110	$1 + \alpha + \alpha^2$	α^{10}
0111	$\alpha + \alpha^2 + \alpha^3$	α^{11}
1111	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
1011	$1 + \alpha^2 + \alpha^3$	α^{13}
1001	$1 + \alpha^3$	α^{14}

Les classes cyclotomiques ont été calculées dans l'exemple précédent et on a :

$$\begin{aligned} M^{(1)}(X) &= X^4 + X + 1 \\ M^{(3)}(X) &= X^4 + X^3 + X^2 + X + 1 \\ M^{(5)}(X) &= X^2 + X + 1 \\ M^{(7)}(X) &= X^4 + X^3 + 1 \end{aligned}$$