

Remarques sur les racines primitives dans les extensions finies des corps finis

Robert Rolland

17 Octobre 2001

R. Rolland, C.N.R.S. Institut de Mathématiques de Luminy
Luminy Case 930, F13288 Marseille CEDEX 9
e-mail : rolland@iml.univ-mrs.fr

Résumé

On étudie les relations entre les racines primitives et les polynômes primitifs d'un corps fini, et ceux d'une extension finie de ce corps.

Mots clés : corps finis, extensions finies, racines primitives, polynômes primitifs.

1 Introduction - Notations

Soit $q = p^n$ une puissance d'un nombre premier p . Soit \mathbb{F}_q le corps fini à q éléments. Si m est un entier ≥ 2 , le corps fini \mathbb{F}_{q^m} est une extension de degré m de \mathbb{F}_q .

Soit alors α un élément primitif de \mathbb{F}_{q^m} et $P(X) \in \mathbb{F}_p[X]$ le polynôme primitif (de degré mn) qui est le polynôme minimal sur \mathbb{F}_p de α .

Posons $\gamma = 1 + q + \dots + q^{m-1}$. Ainsi

$$q^m - 1 = (q - 1)\gamma.$$

Remarquons que $\mathbb{F}_{q^m} = \mathbb{F}_p(\alpha)$. On a donc aussi $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$. Mais en raison de la relation sur les dimensions relatives, la dimension de l'extension algébrique simple $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$ sur \mathbb{F}_q est m . Par suite $(1, \alpha, \dots, \alpha^{m-1})$ est une base de \mathbb{F}_{q^m} sur \mathbb{F}_q .

2 Lien entre racines primitives

Posons $\beta = \alpha^\gamma$. Alors,

$$\beta^{q-1} = 1,$$

et donc $\beta \in \mathbb{F}_q$.

Proposition 2.1 β est un élément primitif de \mathbb{F}_q .

Preuve. Il suffit de voir que si $0 < v < q - 1$ alors $0 < \gamma v < q^m - 1$, et donc $\beta^v \neq 1$. \square

3 Polynômes q -primitifs

Rappelons que $P(X) \in \mathbb{F}_p[X]$ est le polynôme primitif (de degré mn) associé à α .

Notons alors $\Pi(X) \in \mathbb{F}_q(X)$ le polynôme minimal de α dans l'extension \mathbb{F}_{q^m} de \mathbb{F}_q .

Un tel polynôme sera appelé q -**primitif**. La question est de savoir quels sont les liens entre $P(X)$ et $\Pi(X)$.

Il ya en tout $\phi(q^m - 1)$ éléments primitifs dans \mathbb{F}_{q^m} . Il y a donc

$$\frac{\phi(q^m - 1)}{mn}$$

polynômes primitifs et

$$\frac{\phi(q^m - 1)}{m}$$

polynômes q -primitif.

Rappelons que si u est racine dans un corps fini \mathbb{F}_s d'un polynôme $N(X) \in \mathbb{F}_s[X]$, alors u^s est aussi racine de $N(X)$.

En conséquence les racines de $P(X)$ sont

$$\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{mn-1}}.$$

Les racines de $\Pi(X)$ sont

$$\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}.$$

Posons alors

$$\Pi_1(X) = \Pi(X) = (X - \alpha) \cdots (X - \alpha^{q^{m-1}}),$$

$$\Pi_2(X) = (X - \alpha^p) \cdots (X - \alpha^{pq^{m-1}}),$$

$$\Pi_j(X) = (X - \alpha^{p^{j-1}}) \cdots (X - \alpha^{p^{j-1}q^{m-1}}),$$

$$\Pi_n(X) = (X - \alpha^{p^{n-1}}) \cdots (X - \alpha^{p^{n-1}q^{m-1}}).$$

Avec ces notations on obtient donc

$$P(X) = \Pi_1(X)\Pi_2(X) \cdots \Pi_n(X).$$

Remarquons que $\Pi_j(X)$ est le polynôme q -primitif associé à l'élément primitif $\alpha^{p^{j-1}}$.

Les polynômes q -primitifs (de degré m) se regroupent donc par paquets de n pour reconstituer les polynômes primitifs (de degré mn).