La factorisation de $x^{p^l} - x \in F\_p[x]$ selon la trace

Roland Bacher

La factorisation de $x^{p^l} - x \in \mathbb{F}_p[x]$ selon la trace

Roland Bacher

Résumé: Nous décrivons quelques factorisations de polynômes sur des corps finis. Ces factorisation sont liées à la trace, aux compositions de polynômes et aux coefficients binomiaux. Comme conséquence nous obtenons la description des polynômes irréductibles $Q \in \mathbb{F}_2[x]$ tels que les polynômes $Q(1+x+x^2)$ (ou $Q(x+x^2)$) sont également irréductibles.

Abstract: We present a few factorizations of polynomials over finite fields. These factorizations are related to traces, compositions of polynomials and binomial coefficients. As a corollary we obtain a description of all irreducible polynomials $Q \in \mathbb{F}_2[x]$ such that $Q(1+x+x^2)$ (or $Q(x+x^2)$) remain irreducible.

1 Résultats principaux

Pour p un nombre premier, les racines du polynôme $x^{p^l} - x \in \mathbb{F}_p[x]$ sont les éléments du corps fini $\mathbb{F}_{p^l} = \mathbb{F}_p[x]/(R)$ à $q = p^l$ éléments où $R \in \mathbb{F}_p[x]$ est un polynôme irréductible de degré l. Rappelons la définition de la *trace relative* $\mathrm{tr}_l(\rho) = \sum_{k=0}^{l-1} \rho^{p^k} \in \mathbb{F}_p$ d'un élément $\rho \in \mathbb{F}_{p^l}$. C'est donc la trace de l'application $x \longmapsto \rho x$, considérée comme endomorphisme $\mathbb{F}_p-$linéaire de $\mathbb{F}_{p^l}$. Pour $F = \sum_{j=0}^{d} \alpha_j x^j \in \mathbb{F}_p[x]$ un polynôme irréductible de degré d divisant l nous posons $\mathrm{tr}_l(F) = \mathrm{tr}_l(\rho) = -\frac{l}{d}\frac{\alpha_{d-1}}{\alpha_d}$ pour définir sa trace relative où $\rho \in \mathbb{F}_{p^l}$ est une racine de F.

Dans la suite, on identifiera généralement deux diviseurs F, G d'un polynôme $P \in \mathbb{F}_p[x]$ si $G = \lambda F$ pour $\lambda \in \mathbb{F}_p^*$. L'ensemble des diviseurs d'un polynôme P sera défini comme l'ensemble des polynômes moniques divisant P.

Le résultat suivant est, au moins partiellement, bien connu, voir par exemple la proposition 3.4.7 dans [1].

Théorème 1.1 *(i) Le polynôme*

$$-\alpha + \sum_{k=0}^{l-1} x^{p^k} \in \mathbb{F}_p[x]$$

est le produit de tous les facteurs irréductibles F divisant $x^{p^l} - x$ dont la trace relative est $tr_l(F) = \alpha$.

(ii) Pour $\alpha \in \mathbb{F}_p$ et d un diviseur de $l = df$, le polynôme

$$-\alpha + \sum_{k=0}^{f-1} x^{p^{dk}} \in \mathbb{F}_p[x]$$

divise $-d\alpha + \sum_{k=0}^{l-1} x^{p^k} \in \mathbb{F}_p[x]$.

Notre preuve démontre une légère généralisation du théorème 1.1 : On peut remplaçer le corps primaire $\mathbb{F}_p$ par le corps fini $\mathbb{F}_q$ à $q = p^e$ éléments.

La factorisation partielle

$$X^{p^l} - X = \prod_{\alpha=0}^{p-1} \left(-\alpha + \sum_{k=0}^{l-1} X^{p^k} \right) \in \mathbb{F}_p[X]$$

est l'ingrédient principal de l'algorithme 3.4.8 dans [1] permettant la factorisation dans $\mathbb{F}_2[x]$. La caractérisation des diviseurs irréductibles de $-\alpha + \sum_{k=0}^{l-1} x^{p^k} \in \mathbb{F}_p[x]$ en fonction de leurs traces simplifie légèrement l'étude de cet algorithme.

Avant de passer en caractéristique 2, mentionnons encore le résultat suivant (probablement bien connu) qui est valable pour un corps commutatif quelconque.

Proposition 1.2 *Considérons deux polynômes $Q, R \in K[x]$ à coefficients dans un corps commutatif K. Supposons Q irréductible. Alors son degré $\deg(Q)$ divise le degré de tout facteur irréductible $F \in K[x]$ du polynôme composé $Q \circ R \in K[x]$.*

La proposition 1.2 associe donc à une paire de polynômes $Q, R \in K[x]$ avec Q irréductible une partition $\sum_{j=1}^{a} r_j$ du degré de R obtenue en considérant les degrés $(r_j \deg(Q)) = \deg(F_j)$ des a facteurs irréductibles (pas nécessairement distincts) du polynôme composé $Q \circ R = F_1 \cdots F_a$. Un cas particulier amusant est la partition associée à $Q \circ Q$ pour $Q \in K[x]$ irréductible. Y-a-t-il des restrictions sur les partitions obtenues à partir de $Q \circ Q$? (Cela semble être le cas sur le corps $\mathbb{F}_2$: Les partitions $l = 1+1+\ldots+1$ n'apparaissent pas pour $Q \in \mathbb{F}_2[x]$ irréductible de degré $l \in \{2, \ldots, 8\}$.) On peut également se poser des questions sur les fréquences (asymptotiques) des partitions associées à $Q \circ Q$ (respectivement $Q \circ R$) pour Q irréductible et Q (respectivement R) de degré grand etc.

Pour $P, Q \in \mathbb{F}_q[x]$ à coefficients dans le corps fini à $q = p^e$ éléments, Q irréductible de degré l, le nombre de facteurs irréductibles distincts $F \in \mathbb{F}_q[x]$ divisant $Q \circ R$ de degré un diviseur de dl est évidemment donné par le nombre de facteurs irréductible du plus grand diviseur commun entre $Q \circ R$ et $x^{q^{dl}} - x \pmod{Q} \circ R$.

Le premier cas non-trivial, obtenu en choisissant R parmi les polynômes $x+x^2, 1+x+x^2 \in \mathbb{F}_2$ de degré 2 à coefficients dans $\mathbb{F}_2$ admet une description plus simple, donnée par le résultat suivant. (Les cas $Q(x^2) = (Q(x))^2$ et $Q(1+x^2) = (Q(1+x))^2 \in \mathbb{F}_2[x]$ sont sans intérêt.)

Théorème 1.3 *Si $Q = x^{2m} + \sum_{j=0}^{2m-1} \alpha_j x^j \in \mathbb{F}_2[x]$ est irréductible de degré pair $l = 2m$, alors les polynômes $Q(x+x^2), Q(1+x+x^2) \in \mathbb{F}_2[x]$ sont irréductibles de degré $2l$ si la trace $tr_l(Q) = \alpha_{2m-1}$ de Q vaut 1 et les deux polynômes $Q(x+x^2), Q(1+x+x^2) \in \mathbb{F}_2[x]$ se décomposent en un produit de deux polynômes irréductibles de degré l et de même trace sinon.*

Si $Q = x^{2m+1} + \sum_{j=0}^{2m} \alpha_j x^j \in \mathbb{F}_2[x]$ est irréductible de degré impair $l = 2m+1$, alors le polynôme $Q(1+\alpha_{2m}+x+x^2) \in \mathbb{F}_2[x]$ est irréductible de degré $2l$ et le polynôme $Q(\alpha_{2m}+x+x^2) \in \mathbb{F}_2[x]$ se décompose en un produit de deux polynômes irréductibles de degré l et de traces différentes.

Le théorème 1.3 est relié à une jolie factorisation de $x^{2^{2^n}-1}+1 \in \mathbb{F}_2[x]$ qui semble nouvelle. Nous l'appellerons la *factorisation de Pascal* car elle fait intervenir la réduction modulo 2 des coefficients binomiaux $\binom{m}{k} = \frac{m!}{k!(m-k)!}$ constituant le triangle de Pascal.

Théorème 1.4 *On a*

$$\prod_{k=0}^{2^n-1} \left(1 + \sum_{j=0}^{k} \binom{k}{j} x^{2^j} \right) = x^{2^{2^n}-1} + 1 \in \mathbb{F}_2[x] \ .$$

L'outil principal pour prouver les théorèmes 1.3 et 1.4 est un monoïde décrit dans le chapitre 3. On l'obtient en considérant un certain sous-espace vectoriel $\subset \mathbb{F}_p[x]$ qui est stable pour la composition des polynômes.

2 Preuves du théorème 1.1 et de la proposition 1.2

Preuve du théorème 1.1: En posant $X = \sum_{k=0}^{l-1} x^{p^k}$ dans l'identité triviale $X \prod_{\alpha=1}^{p-1}(X-\alpha) = X^p - X \in \mathbb{F}_p[X]$ on a

$$\prod_{\alpha=0}^{p-1} \left(-\alpha + \sum_{k=0}^{l-1} x^{p^k} \right) = \sum_{k=1}^{l} x^{p^k} - \sum_{k=0}^{l-1} x^{p^k} = x^{p^l} - x \ .$$

Le polynôme $-\alpha + \sum_{k=0}^{l-1} x^{p^j}$ divise donc $x^{p^l} - x$ dans $\mathbb{F}_p[x]$.

Par définition de la trace relative $\mathrm{tr}_l(F) = \sum_{k=0}^{l-1} \rho^{p^k}$ d'un diviseur irréductible F de $-\alpha + \sum_{k=0}^{l-1} x^{p^k}$, la racine $\rho \in \mathbb{F}_{p^l}$ de F est également une racine de $-\mathrm{tr}_l(F) + \sum_{k=0}^{l-1} x^{p^k}$. Le polynôme irréductible $F \in \mathbb{F}_p[x]$ divise donc $-\mathrm{tr}_l(F) + \sum_{k=0}^{l-1} x^{p^k} \in \mathbb{F}_p[x]$. Ceci démontre l'assertion (i).

Posons $q = p^d$ et considérons le corps $\mathbb{F}_q$ à $q = p^d$ éléments. Les arguments utilisés dans la preuve de l'assertion (i) montrent qu'on a également

$$\prod_{\alpha\in\mathbb{F}_q}\left(-\alpha+\sum_{k=0}^{f-1}x^{q^k}\right)=x^{q^f}-x=x^{p^l}-x\in\mathbb{F}_p[x]\ .$$

La trace $\mathrm{tr}_{f,\mathbb{F}_q}(F)=\sum_{k=0}^{f-1}\rho^{q^k}\in\mathbb{F}_q$ (où $F(\rho)=0$ pour $\rho\in\mathbb{F}_{q^f}$) d'un diviseur irréductible $F=\sum_j\alpha_j x^j\in\mathbb{F}_q[x]$ de $-\alpha+\sum_{k=0}^{f-1}x^{q^k}$ est donc également donnée par $\alpha\in\mathbb{F}_q$. Le produit $\prod_{s=0}^{d-1}\left(\sum_j\alpha_j^{p^s}x^j\right)$ est une puissance (d'exposant un diviseur d) d'un polynôme irréductible $G\in\mathbb{F}_p[x]$ divisible par F. Sa trace $\mathrm{tr}_l(G)=\sum_{k=0}^{l-1}\rho^{p^k}=\sum_{k=0}^{f-1}\left(\rho^{p^{dk}}+\rho^{p^{dk+1}}+\ldots+\rho^{p^{dk+(d-1)}}\right)=\alpha+\alpha^p+\ldots+\alpha^{p^{d-1}}$ vaut donc $d\alpha$ pour $\alpha\in\mathbb{F}_p$. L'assertion (ii) découle maintenant de l'assertion (i). □

Preuve de la proposition 1.2: Soit ρ une racine d'un diviseur irréductible F de $Q\circ R\in K[x]$. Le corps $K[\rho]=K[x]/(F)$ contient donc le sous-corps $K[R(\rho)]$ qui est une extension de degré $\deg(Q)$ de K car $R(\rho)$ est une racine du polynôme irréductible $Q\in K[x]$. □

3 Le monoïde de composition

Lemma 3.1 *Pour* $A=\epsilon_A+\sum_{k=0}^{a}\alpha_k x^{p^k}$ *et* $B=\epsilon_B+\sum_{k=0}^{b}\beta_k x^{p^k}\in\mathbb{F}_p[x]$ *avec* $\epsilon_A,\alpha_0,\ldots,\alpha_a,\epsilon_B,\beta_0,\ldots,\beta_b\in\mathbb{F}_p$ *on a*

$$A\circ B=\epsilon_C+\sum_{k=0}^{a+b}\gamma_k x^{p^k}\in\mathbb{F}_p[x]$$

avec $\epsilon_C=\epsilon_A+\epsilon_B\sum_{k=0}^{a}\alpha_k$ *et* $\sum_{k=0}^{a+b}\gamma_k x^k=\left(\sum_{k=0}^{a}\alpha_k x^k\right)\left(\sum_{k=0}^{b}\beta_k x^k\right)$.

Preuve: Un calcul facile montre le résultat pour le cas particulier $A=\epsilon_A+x^{p^a}$. Le cas général s'en déduit par linéarité. □

Associons au polynôme $A=\epsilon_A+\sum_{k=0}^{a}\alpha_k x^{p^k}\in\mathbb{F}_p[x]$ (avec $\epsilon_A,\alpha_0,\ldots,\alpha_a\in\mathbb{F}_p$) le symbole $(\epsilon_A,\sum_{k=0}^{a}\alpha_k x^k)\in\mathbb{F}_p\times\mathbb{F}_p[x]$. Par le lemme 3.1, le polynôme composé $A\circ B$ de deux tels polynômes de symboles (ϵ_A,α) et (ϵ_B,β) correspond au symbole $(\epsilon_A+\alpha(1)\epsilon_B,\alpha\beta)$. Ce produit munit donc l'ensemble $\mathcal{M}_p=\mathbb{F}_p\times\mathbb{F}_p[x]$ de ces symboles d'une structure de monoïde associative et distributive à gauche pour la structure d'espace vectoriel évidente $(\epsilon_A,\alpha)+\lambda(\epsilon_B,\beta)=(\epsilon_A+\lambda\epsilon_B,\alpha+\lambda\beta)$ sur $\mathcal{M}_p$. Nous appellerons $\mathcal{M}_p$ le *monoïde de composition*. La projection sur le deuxième facteur $\mathbb{F}_p[x]$ de $\mathcal{M}_p$ est un morphisme de monoïde sur le monoïde commutatif multiplicatif $\mathbb{F}[x]$. La section $\alpha\longmapsto(0,\alpha)\in\mathcal{M}_p$ réalise $\mathbb{F}_p[x]$ comme sous-anneau de l'espace vectoriel $\mathcal{M}_p$. Un autre sous-anneau commutatif (qui n'est cependant pas

de type fini) est défini par le sous-ensemble $\mathbb{F}_p \times (x-1)\mathbb{F}_p[x]$ du monoïde $\mathcal{M}_p$, augmenté de sa structure d'espace vectoriel. L'élément $(0,1) \in \mathcal{M}_p$ est une identité bilatère tandis que la multiplication (à gauche ou à droite) par $(0,x)$ correspond à l'action de l'automorphisme de Frobenius. Le sous-ensemble $\mathbb{F}_p \times \mathbb{F}_p^* \subset \mathcal{M}_p$ est un sous-monoïde isomorphe au groupe affine du corps $\mathbb{F}_p$. Mentionnons également que le monoïde $\mathcal{M}_p$ possède des quotients commutatifs finis de la forme $\mathbb{F}_p \times (\mathbb{F}_p[x]/(G))$ pour $G \in \mathbb{F}_p[x]$ un polynôme divisible par $x-1$.

Remarque 3.2 *Toutes les définitions et propriétés énoncées dans ce chapitre restent valable en remplaçant p partout par une même puissance $q = p^e$ d'un nombre premier et en travaillant sur le corps fini $\mathbb{F}_q$ à q éléments.*

4 Preuves des théorèmes 1.3 et 1.4

Preuve du théorème 1.3: Considérons d'abord $Q \in \mathbb{F}_2[x]$ irréductible de degré pair $l = 2m$. Comme $(Q_1Q_2) \circ R = (Q_1 \circ R)(Q_2 \circ R)$, par l'assertion (i) du théorème 1.1 il suffit de montrer que le polynôme $\left(\sum_{k=0}^{2m-1} x^{2^k}\right) \circ (\epsilon + x + x^2)$ divise $x^{2^{2m}} + x$ et que le polynôme $\left(1 + \sum_{k=0}^{2m-1} x^{2^k}\right) \circ (\epsilon + x + x^2)$ est premier à $x^{2^{2m}} + x$ (il divisera alors $x^{2^{4m}} + x$ par la proposition 1.2) pour $\epsilon \in \mathbb{F}_2$. En travaillant dans le monoïde $\mathcal{M}_2$, on obtient $(0, \sum_{k=0}^{2m-1} x^k)(\epsilon, 1+x) = (2m\epsilon, 1+x^{2m}) = (0, 1+x^{2m})$ correspondant à $x + x^{2^{2m}}$ dans le premier cas. Le deuxième cas, $(1, \sum_{k=0}^{2m-1} x^k)(\epsilon, 1+x) = (1, 1+x^{2m})$, correspond à $1+x+x^{2^{2m}}$ qui est premier à $x+x^{2^{2m}}$. La proposition 1.2 (ou la factorisation $(1+x+x^{2^{2m}})(1+(1+x+x^{2^{2m}})^{2^{2m}-1}) = (1+x+x^{2^{2m}}) + (1+x+x^{2^{2m}})^{2^{2m}} = x + x^{2^{4m}}$) termine la preuve pour Q irréductible de degré pair $l = 2m$. Nous laissons au lecteur le cas similaire où Q est irréductible de degré impair. □

Preuve du théorème 1.4: Considérons le polynôme $P_h = 1 + \sum_{k=0}^{h} \binom{h}{k} x^{2^k} \in \mathbb{F}_2[x]$ correspondant au symbole $(1, (1+x)^h) \in \mathcal{M}_2$. Les identités faciles $(1, 1+x)(1, (1+x)^h) = (1, (1+x)^h)(0, 1+x) = (1, (1+x)^{h+1}) \in \mathcal{M}_2$ pour $h \in \mathbb{N}$ montrent qu'on a $P_1 \circ P_h = P_h \circ (x + x^2) = P_{h+1}$ pour tout $h \in \mathbb{N}$. En itérant l'identité $P_1 \circ P_h = 1 + P_h + P_h^2 = P_{h+1}$ on obtient

$$\begin{aligned} P_{h+1} &= 1 + P_h(1 + P_h) = 1 + P_h P_{h-1}(1 + P_{h-1}) = \dots \\ &= 1 + P_h P_{h-1} \dots P_1 P_0 (1 + P_0) = 1 + x \prod_{k=0}^{h} P_k \ . \end{aligned}$$

Pour $h + 1 = 2^n$, on a donc l'égalité

$$P_{2^n} = 1 + x + x^{2^{2^n}} = 1 + x \prod_{k=0}^{2^n - 1} P_k$$

qui démontre le théorème. □

Remarque 4.1 *Le produit*

$$P_{2^{n-1}} \cdots P_{2^n-1} = \frac{x^{2^{2^n}-1}+1}{x^{2^{2^{n-1}}-1}+1} \in \mathbb{F}_2[x]$$

s'identifie au produit de tous les polynômes irréductibles distincts de degré 2^n *dans* $\mathbb{F}_2[x]$. *Le théorème 1.1 appliqué à* $P_{2^{n-1}} = 1 + \sum_{k=0}^{2^n-1} x^{2^k}$ *(ou le théorème 1.3 appliqué aux identités* $P_{h+1} = P_h \circ (x + x^2)$*) montre qu'un tel polynôme irréductible* $F = \sum_{k=0}^{2^n} \alpha_k x^k$ *divise le dernier facteur* $P_{2^{n-1}}$ *si et seulement si sa trace* $tr_{2^n}(F) = \alpha_{2^n-1}$ *vaut* 1. *Mentionnons également que les formules* $P_{h+1} = P_h \circ P_1 = P_h \circ (x+x^2)$ *pour* $h \geq 1$ *illustrent et précisent le théorème 1.3.*

Remarque 4.2 *Pour* p *un premier quelconque (ou plus généralement pour* $q = p^e$ *une puissance d'un premier), les polynômes*

$$P_{h,\alpha} = -\alpha + \sum_{k=0}^{h} \binom{h}{k} x^{p^k} \in \mathbb{F}_p[x]$$

ont également des propriétés intéressantes: $P_{h,\alpha}$ *divise* $P_{h+1,2\alpha}$ *car*

$$\begin{aligned} 0 &= \left(-\alpha + \textstyle\sum_k \binom{h}{k}\rho^{p^k}\right) + \left(-\alpha + \textstyle\sum_k \binom{h}{k}\rho^{p^k}\right)^p \\ &= -\alpha + \textstyle\sum_k \binom{h}{k}\rho^{p^k} - \alpha + \textstyle\sum_k \binom{h}{k-1}\rho^{p^k} = P_{h+1,2\alpha} \end{aligned}$$

pour $\rho \in \overline{\mathbb{F}}_p$ *une racine de* $P_{h,\alpha}$. *Le polynôme* $P_{h,\alpha}$ *divise donc* $P_{p^n,2^{p^n-h}\alpha}$ *pour* $h \leq p^n$. *Il divise donc également* $x^{p^{2p^n}} - x$ *en appliquant le théorème 1.1 à* $P_{p^n,2^{p^n-h}\alpha} = 2^{p^n-h}\alpha + x + x^{p^{p^n}}$. *L'ensemble des polynômes* $P_{h,\alpha}$ *correspond au sous-monoïde* $\mathbb{F}_p \times (1+x)^{\mathbb{N}}$ *de* $\mathcal{M}_p$. *Il est donc fermé pour la composition et on a* $P_{h,\alpha} \circ P_{m,\beta} = P_{h+m,\alpha+2^h\beta}$.

References

[1] H. Cohen, A Course in Computational Algebraic Number Theory, 3-rd corr. print. Berlin ; Heidelberg ; New York : Springer, 1996.

Institut Fourier, Laboratoire de Mathématiques, UMR 5582 (UJF-CNRS), 100, rue des Mathématiques, BP 74, 38402 St MARTIN D'HÈRES Cedex, France

Adresse courriel: Roland.Bacher@ujf-grenoble.fr