Projet de Master :
Factorisation de polynômes sur des corps finis

Daniel RESENDE

2013/2014

Table des matières

Chapitre 1

Introduction

Ce projet a pour but d'étudier la factorisation d'un polynôme en facteurs irréductibles sur des corps finis à l'aide d'algorithmes de factorisation.

1.1 Historique

La théorie des corps finis, notamment l'étude des congruences, sur des entiers et sur des polynômes, se développe à partir du 19ième siècle. Puis en 1967, Elwyn Berlekamp développa le premier algorithme de factorisation de polynômes sur un corps. Tandis qu'en 1981 avec l'algorithme de Cantor-Zassenhaus, on a l'apparition d'algorithme plus performant.

1.2 Quelques propriétés fondamentales d'un corps fini

Définition 1.2.1 (Polynôme irréductible)
Soient K un corps et $P \in K[X]$. On dit que P est irréductible (dans $K[X]$) si P n'est pas constant et si ses seuls diviseurs sont les polynômes constants et les polynômes associés à P, ie de la forme λP avec $\lambda \in K^*$.

Théorème 1.2.1 (Wedderburn)
Tout corps fini est commutatif.

Preuve. Soit K un corps fini non nécessairement commutatif de caractéristique $p > 0$.
On pose $Z = Z(K) = \{x \in K \mid \forall y \in K, xy = yx\}$ le centre de K. Il est clair que Z est un sous-corps fini commutatif de K, donc de caractéristique p. Par conséquent, K est le sous-corps premier de $\mathbb{F}_p$. Ainsi on a que Z est un $\mathbb{F}_p$-espace vectoriel de dimension r et K un Z-espace vectoriel de dimension n. Si on défini $q = card(Z)$, on a alors que $q = p^r$ et $card(K) = q^n$.

Soit $x \in K^*$, on note $C_x = \{y \in K \mid xy = yx\}$ le centralisateur de x dans K. On a clairement que $C_x \supset Z$ est un sous-corps de K, alors $\exists d(x) \in N^*$ tel que $card(C_x) = q^{d(x)}$. Comme C_x^* est un sous-groupe de K^*, on que $card(C_x^*) \mid card(K^*)$, ie. $q^{d(x)} - 1 \mid q^n - 1$

On veut ainsi montrer que $d(x) = n = 1$. On applique la division euclidienne de n par $d(x)$,ie. $n = s(x)d(x) + t(x)$. Il en suit :

$$\begin{aligned} q^n - 1 &= \left((q^{d(x)})^{s(x)} - 1\right) q^{t(x)} + q^{t(x)} - 1 \\ &= (q^{d(x)} - 1) \left(\sum_{i=0}^{s(x)-1} q^{id(x)+t(x)} \right) + q^{t(x)} - 1. \end{aligned}$$

Par conséquent, $q^{d(x)} - 1 \mid q^{t(x)} - 1$. Comme $q \geq 2$ et $0 \leq t(x) < d(x)$, d'où $t(x) = 0$, donc on a $d(x) \mid n$.

Soit $n > 1$, on suppose par l'absurde que K est non commutatif. On considère l'action du groupe K^* sur lui-même par conjugaison ; on obtient donc une partition de K^* telle que $\mathscr{P}(K^*) = \bigcup_{x_i \in K^*} \vartheta_{x_i}$ l'union disjointe finie d'orbites. Ceci nous donne l'équation aux classes suivante :

$$q^n - 1 = q - 1 + \sum_{x \in \mathscr{P}(K^*) et x \notin Z} \frac{q^n - 1}{q^{d(x)} - 1}. \tag{1.1}$$

Soit ϕ_m le polynôme cyclotomique, on a d'après les propriétés de ϕ_m que :

$$q^n - 1 = \prod_{m|n} \phi_m(q), \tag{1.2}$$

$$q^d - 1 = \prod_{m|d} \phi_m(q) \tag{1.3}$$

On remarque que si $d \mid n$ et $d < n$, on a $\phi_n(q) \mid \frac{q^n-1}{q^d-1}$. Alors, d'après (**??**), $\phi_n(q) \mid q - 1$, donc $|\phi_n(q)| \leq q - 1$.

Soit $\xi \in U_n^*(\mathbb{C})$. Comme $n > 1$, on a $\xi \neq 1$, d'où $|q - \xi| > q - 1$. On en déduit que $\phi_n(q)$ ne divise pas $q - 1$ dans $\mathbb{Z}$, d'où la contradiction. Par conséquent, $n = 1$, $K = Z$ et K est commutatif.

Proposition 1.2.1
Soient K un corps fini caractéristique $p > 0$ un nombre premier $p > 0$. On a :

1. *$Card(K) = q = p^n$ avec un entier $n \geq 1$.*
2. *Le groupe $(K^*, \times)$ est cyclique d'ordre $q - 1$.*
3. *$\forall x \in K^*$, $x^{q-1} = 1$ et $\forall x \in K$, $x^q = x$*

Proposition 1.2.2
Le groupe $(K, +)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^n$.

Chapitre 2

Existence et unicité d'un corps fini à q éléments

Dans cette section, nous allons démontrer l'existence et l'unicité (à isomorphisme près) d'un corps fini à $p^n = q$ éléments.

Proposition 2.0.1 (Existence)
Soit $q = p^n$, il existe $\mathbb{F}_q$ un corps de décomposition du polynôme $X^q - X$ sur le corps premier $\mathbb{F}_p$ à q éléments. De plus, tout élément de $\mathbb{F}_q$ est racine de ce polynôme.

Preuve. Soit $q = p^n$ et soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_q$. On pose que $\mathbb{F}_q$ est un corps de décomposition dans $\overline{\mathbb{F}_p}$du polynôme $X^q - X$ sur $\mathbb{F}_p$. Comme son polynôme dérivé est égale à -1 toutes ses racines sont simples. Par conséquent, il y a q racines distinctes de $X^q - X$ dans $\mathbb{F}_q$.

Montrons alors que celles-ci forment un corps.

On pose $\alpha, \beta \in \mathbb{F}_q$ deux racines de $X^q - X$, on a alors :

$$(\alpha+\beta)^q - (\alpha+\beta) = \alpha^q + \beta^q - \alpha - \beta = \alpha + \beta - \alpha - \beta = 0$$

et

$$(-\alpha)^q - (-\alpha) = (-1)^q \alpha^q + \alpha =$$

– si p pair : $-1 = 1$ dans $\mathbb{Z}/2\mathbb{Z}$ et α est une racine simple.
– sinon p impair : $(-1)^q = -1$ et $-\alpha$ est une racine simple.

Par ailleurs,

$$(\alpha\beta)^q - \alpha\beta = \alpha^q \beta^q - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

et

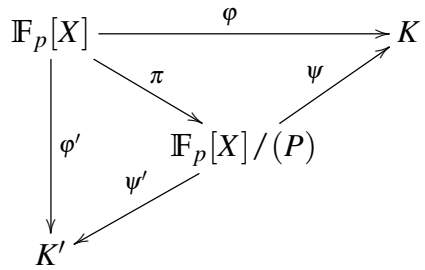
$$(\alpha^{-1})^q - \alpha^{-1} = (\alpha^q)^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0 \text{ avec } \alpha \neq 0.$$

Les racines du polynôme $X^q - X$ forment un corps de décomposition sur $\mathbb{F}_p$ et engendre un corps à q éléments qui est $\mathbb{F}_q$.

Théorème 2.0.2 (Unicité)
Tout corps K fini à $q = p^n$ éléments est isomorphe à $\mathbb{F}_q$.

Preuve. Nous allons montrer que tout corps K fini à q éléments est unique à isomorphisme près, ie. isomorphe à $\mathbb{F}_q$. D'après la proposition (1.2.1), nous connaissons l'existence d'un générateur $x \in K^*$.

Soient $\begin{array}{rccc} \varphi : & \mathbb{F}_p[X] & \longrightarrow & K \\ & X & \longmapsto & x \end{array}$ l'homomorphisme surjectif, P le polynôme minimal de x sur $\mathbb{F}_p[X]$ et $\psi : \mathbb{F}_p[X]/(P) \longrightarrow K$ la factorisation de φ par la projection canonique $\pi : \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]/(P)$. On obtient le diagramme suivant :



D'après ce diagramme, ψ est donc un isomorphisme.

Comme x est d'ordre $q-1$, x est racine $X^{q-1}-1$, par conséquent $P \mid X^{q-1}-1$. Soit K' un corps à p^r éléments. Les $q-1$ éléments de K'^* sont racines de $X^{q-1}-1$. Comme P n'est pas le polynôme constant, il existe au moins $y \in K'^*$ une racine de P, d'où $\begin{array}{rccc} \varphi' : & \mathbb{F}_p[X] & \longrightarrow & K' \\ & X & \longmapsto & y \end{array}$ cet homomorphisme. Comme $\varphi'(P) = 0$, $\exists \psi' : \mathbb{F}_p[X]/(P) \longrightarrow K'$ telle que $\varphi = \psi'\pi \circ \psi'$ est injective, donc c'est un isomorphisme car $\mathbb{F}_p[X]/(P)$ et K' ont q éléments. Finalement, on a que $\psi'\psi^{-1}$ est un isomorphisme de K sur K'.

Chapitre 3

Extension galoisienne d'un corps fini

3.1 Extension d'un corps fini

Proposition 3.1.1
Soient K et L deux corps finis de caractéristique p. On pose $\mid K \mid = q = p^n$ *avec* $n \geq 1$.

1. *Si L est une extension de K,* $\exists s \geq 1$, *tel que* $\mid K \mid = q^{sn} = p^n$. *Tout élément de L est algébrique sur K, de degré inférieur à ou égal à s.*
2. *Si* $\exists s \geq 1$, *tel que* $\mid L \mid = q^s = p^{sn}$, *alors il existe un unique un sous-corps L isomorphe à K.*

Proposition 3.1.2
Soient K un corps fini et L une extension fini de degré s de K à q^s *éléments.*

On a que L est un corps de décomposition du polynômes $X^{q^s} - X$ *sur K et est une extension galoisienne de K.*

Preuve. Soit $P \in K[X]$ un polynôme irréductible.

Si P possède une racine x dans L, alors $P \mid X^{q^s} - X$ et donc se factorise en un produit de polynômes de degrés un dans $L[X]$. De plus, P a des racines simples qui sont les conjugués de x sur K donc dans L.

3.2 Groupe de Galois d'un corps fini

Proposition 3.2.1
Soient K et L deux corps finis avec $K \subset L$ *tout deux de caractéristique q. On pose* $|K| = q = p^n$ *et* $|L| = q^s$ *avec* $n, s \geq 1$.

On a que le groupe de Galois $G = Gal(L \mid K)$ *est cyclique d'ordre s et engendré par l'automorphisme de Frobenius*

$$\begin{array}{rccc} \varphi_q : & \mathbb{F}_q & \longrightarrow & \mathbb{F}_{11}[X] \\ & x & \longmapsto & x^q \end{array} .$$

.

Preuve. Par construction, on a que l'extension L/K est galoisienne de degré s. Soit φ_q l'automorphisme de Frobenius de L et G le groupe engendré par φ_q. On a $\varphi_q^s(x) = x^{q^s} = x$, $\forall x \in L$, d'où $\varphi_q^s = id_L$. D'autre part, si $1 \leq k \leq s-1$, on a que $\varphi_q^s \neq id_L$ sinon pour tout $x \in L^*$ est d'ordre au plus $q^k - 1$. Or L^* est cyclique, il possède ainsi un élément d'ordre $q^s - 1$.

On a que G possède donc au moins s éléments, si x engendre L, ses s images par les puissances de F sont distinctes comme conjugués de x sur K. Puisque $[L:K] = s$ cela exclut l'existence d'autres éléments de G, car x ne peut avoir d'autres conjugués. Par conséquent, $|G| = s$.

Chapitre 4

Algorithme de factorisation

Dans la littérature, il existe deux algorithmes majeurs de factorisation de polynômes en facteurs irréductibles sur un corps fini.

4.1 Réduction au cas sans facteur carré

Afin de pouvoir factoriser un polynôme quelconque, on doit le décomposer en facteur carrés avant de pourvoir utiliser un algorithme de factorisation. On pose $P = P_1^{\alpha_1} \dots P_s^{\alpha_s} \in \mathbb{F}_p[X]$ polynôme quelconque où les P_i sont irréductibles (deux à deux distincts) et les $\alpha_i \geq 1$.

Définition 4.1.1
Soit $P \in \mathbb{F}_p[X]$ un polynôme. On dit que P est sans carré s'il n'existe pas de polynôme non constant $Q \in \mathbb{F}_p[X]$ tel que $Q^2 \mid P$.

Lemme 4.1.1
Soit $P \in \mathbb{F}_p[X]$. La dérivée P' vaut 0 si et seulement si P s'écrit sous la forme Q^p, $Q \in \mathbb{F}_p[X]$.

Preuve. Si $P = Q^p$, on a bien que $P' = Q^{p-1} p Q' = 0$.
Réciproquement, si $P' = 0$, $P = \sum_i q_i X^{pi} = \sum_i q_i^p X^{pi} = \sum_i (q_i X^i)^p = \left(\sum_i q_i X^{pi}\right)^p = Q^p$.

Proposition 4.1.1
Soit $P \in \mathbb{F}_p[X]$. P est sans facteur carré si et seulement si $pgcd(P,P') = 1$ avec P' la dérivée de P.

Preuve. Soit $P = P_1^{\alpha_1} \dots P_s^{\alpha_s} \in \mathbb{F}_p[X]$ où les P_i sont irréductible et les $\alpha_i \geq 1$. On obtient en dérivant P :

$$P' = \sum_{i=1}^{s} \alpha_i P_i' \frac{P}{P_i}.$$

Si on P admet un facteur carré, il existe au moins un $\alpha_i \geq 2$ où $P_i \mid P_i' \frac{P}{P_i}$. Alors $P_i \mid P_i' \frac{P}{P_j}$, $\forall i \neq j$, il divise P' de sorte que $pgcd(P,P') \neq 1$.

Réciproquement, comme les P_i sont irréductibles, d'après le lemme 4.1.1 alors on sait que leur dérivées sont non nulles. On suppose donc que $pgcd(P,P') \neq 1$. Par conséquent, il existe

un $P_i \mid P'$. En effet, il divise tout les autres $\frac{P}{P_j}$, et ainsi divise $\alpha_i P_i' \frac{P}{P_i}$. Ainsi P_i' est non nul, donc $P_i \mid \alpha_i P_i \frac{P}{P_i}$.

Si $\alpha_i \not\equiv 0\ [p]$, on a $P_i \mid P_i' \frac{P}{P_i}$ et $pgcd(P,P') = 1$, donc, d'après le lemme de Gauss, finalement $P_i^2 \mid P$.

Sinon si $\alpha_i \equiv 0\ [p]$, on a $p \mid \alpha_i$, donc finalement $\alpha_i \neq 1$.

Maintenant, on récrit $P = Q_1 Q_2^2 \dots Q_s^s$ tel que Q_1 le produit des P_i apparaissant à la puissance $1, \dots,$ Q_s le produit des P_i apparaissant à la puissance s. On appelle alors $Q_1 Q_2 \dots Q_s$ la partie sans facteur carré de P.

Proposition 4.1.2
Si $p > s$, alors la partie sans carré de P est $P / pgcd(P,P')$.

Preuve. On obtient en dérivant $P = Q_1 Q_2^2 \dots Q_s^s$:

$$P' = (Q_2 \dots Q_s^{s-1})(Q_1' Q_2^2 \dots Q_s^s + \dots + s Q_1 Q_2^2 \dots Q_{s-1}').$$

Les Q_i' ne sont pas nuls d'après le lemme 4.1.1. Comme $\forall 1 \leq i \leq s,\ i \not\equiv 0\ [p]$, le membre de droite est donc premier avec tous les Q_i, donc avec P. Donc $pgcd(P,P') = Q_2 \dots Q_s^{s-1}$.

Proposition 4.1.3
On a

$$\frac{P}{pgcd(P,P')} = \prod_{i \text{ non multiple de } p} Q_i^i.$$

Preuve. Comme la preuve précédente, on remarque que

$$pgcd(P,P') = (Q_2 \dots Q_s^{s-1}) \cdot \prod_{i \text{ multiple de } p} Q_i^i.$$

Proposition 4.1.4
Soient $n = deg(P)$, $U = pgcd(P,P')$ et $V = P/U$.
On pose $W = pgcd(U, V^n)$. Alors

$$U/W = \prod_{i \text{ multiple de } p} Q_i^i.$$

Preuve. D'après la proposition précédente,

$$V^n = \prod_{i \text{ non multiple de } p} Q_i^n$$

et

$$U = (Q_2 \dots Q_s^{s-1}) \cdot \prod_{i \text{ multiple de } p} Q_i.$$

Comme n est la plus grande multiplicité, on a par conséquent que

$$W = \prod_{i \text{ non multiple de } p} Q_i^{i-1}.$$

Algorithme 1 Calculer la partie sans facteur carré d'un polynôme

Require: $P \in \mathbb{F}_p[X]$ un polynôme quelconque.
Ensure: La partie sans facteur carré de P.
$U = pgcd(P,P')$;
$V = P/U$;
$W = pgcd(U,V^n)$;
Calculer la racine p-ième W_0 de W ;
Calculer récursivement la partie sans facteur carré S de W_0 ;
return VS.

Voici donc l'algorithme de décomposition sans facteur carré :

Proposition 4.1.5
L'algorithme a une complexité en $O(M(n)log(n))$ où M est une fonction de multiplication.

Démonstration. Les calculs de *pgcd* se font en $O(M(n)log(n))$ opérations ; remarquer qu'il suffit de calculer V^n *mod* U, et que cela se fait en $O(log(n))$ multiplications modulo U par exponentiation binaire. Ensuite, W_0 s'obtient sans calcul ; son degré est au plus égal à n/p. Par conséquent, le temps de calcul $T(n)$ satisfait la récurrence

$$T(n) \leq T\left(\frac{n}{p}\right) + CM(n)(log(n))$$

avec C une constante.

4.2 Cas d'un polynôme sans facteur carré (Algorithme de Berlekamp)

On étudie d'abord l'algorithme de Berlekamp, car celui-ci est le plus générale. On suppose $P \in \mathbb{F}_p[X]$ un polynôme sans facteur carré de degré n, tel que $P = P_1 \dots P_s$ avec P_i irréductibles. On a que $n = \sum_1^s i$.

Théorème 4.2.1 (Restes chinois)
Soit $P = P_1 \dots P_m$ avec $P_1, \dots, P_m$ m polynômes irréductibles de $A = K[X]$ un corps deux à deux premiers entre eux. On pose (P_i) l'idéal engendré par P_i, alors $A/(P)$ est isomorphe à $A/(P_1) \times \dots \times A/(P_m)$.

D'après le théorème des restes chinois, on a $\mathbb{F}_p/(P) = \mathbb{F}_p/(P_1) \times \dots \times \mathbb{F}_p/(P_s)$ avec $\mathbb{F}_p/(P_i) \cong \mathbb{F}_{p^{deg(P_i)}}$.

Proposition 4.2.1
Soit $N \in ker(M_{\varphi_p} - I_p)$ un polynôme non constant.
On a

$$P = \prod_{j \in \mathbb{F}_p} pgcd(P, N - j)$$

et cette factorisation est non triviale.

Preuve. En remplaçant N dans l'équation suivante,

$$X^p - X = \prod_{j \in \mathbb{F}_p} (X - j),$$

d'où

$$N^p - N = \prod_{j \in \mathbb{F}_p} (N - j).$$

De plus, comme $P \mid X^p - X$, on a alors

$$P = \prod_{j \in \mathbb{F}_p} pgcd(P, N - j).$$

On montre ensuite, par l'absurde, que la factorisation est non triviale. Si la factorisation est triviale, alors $\exists j$ telle que $P \mid N - j$, d'où N constant modulo P. Ce qui absurde d'après l'énoncé.

Voici donc l'algorithme de Berlekamp :

Algorithme 2 Berlekamp

Require: $P \in \mathbb{F}_p[X]$ un polynôme sans facteurs carré de degré n.
Ensure: La factorisation de P.

```
On construit la matrice M_{φ_p} engendrée par φ_p l'endomorphisme de Frobenius dans la base
(1, x, ..., x^{n-1}) avec x l'image projective X par la projection canonique ;
if rg(M_{φ_p} − I_p) ≥ n then
    return P est irréductible ;
else
    On calcule le ker(M_{φ_p} − I_p) à l'aide d'un algorithme classique d'algèbre linéaire (par
    exemple un pivot de Gauss) ;
    On calcule le sous-espace propre associé à 1 et on choisit des éléments de N celui-ci ;
    i ← 0 ;
    j ← 1 ;
    F ← 1 ;
    while i ≤ dim(ker(M_{φ_p} − I_p)) and j < p do
        if pgcd(P, Q − j) premier à F then
            F ← F · pgcd(P, N − j) ;
            i++ ;
        end if
        j++ ;
    end while
end if
return F ;
```

Proposition 4.2.2
L'algorithme a une complexité en $O(n^\tau + nM(n)log(n)p)$ avec τ dépendant du choix de l'algorithme de résolution de système linéaire.

Preuve. Tout d'abord, on commence par construire la matrice M_{φ_p}. On commence par calculer X^p *mod* P : soit $O(log(p))$ opérations *mod* P, soit $O(M(n)log(p))$ opérations dans $\mathbb{F}_p$. Ensuite, il faut calculer $(X^2)^p = (X^p)^2, (X^3)^p = (X^p)^3, \ldots$, ce qui se fait en n multiplications mod P, soit $O(nM(n))$ opérations en tout.

La résolution du système linéaire d'un algorithme l'algèbre linéaire (tel un pivot de Gauss) coûte n^τ.

Une fois obtenu un vecteur du noyau, pour chaque essai de *pgcd* un coûte $O(M(n)log(n))$ opérations avec un maximum de de p.

Pour trouver la factorisation complété, il suffit de réitérer le procédé ce qui entraîne a priori un surcoût de n. En fait, il n'y a pas besoin de refaire de l'algèbre linéaire, de sorte que le coût total de la factorisation est $O(n^\tau + nM(n)log(n)p)$.

4.3 Application de l'Algorithme de Berlekamp

Dans cette section, on étudie une application de l'algorithme de Berlekamp sur un exemple concret.

On choisi par exemple le polynôme

$$P = X^6 + 7 \in \mathbb{F}_{11}$$

et on cherche à le factoriser sur $\mathbb{F}_{11}$. On note x l'image projective X par la projection canonique de $\mathbb{F}_{11}$ dans $\mathbb{F}_{11}/(P)$ et

$$\begin{array}{rccc} \varphi_{11} : & \mathbb{F}_{11}[X] & \longrightarrow & \mathbb{F}_{11}[X] \\ & t & \longmapsto & t^{11} \end{array} .$$

On a :

$$\left\{ \begin{array}{rcl} \varphi_{11}(1) & \equiv & 1\ [P] \\ \varphi_{11}(x) & \equiv & 4x^5\ [P] \\ \varphi_{11}(x^2) & \equiv & -2x^4\ [P] \\ \varphi_{11}(x^3) & \equiv & x^3\ [P] \\ \varphi_{11}(x^4) & \equiv & 5x^2\ [P] \\ \varphi_{11}(x^5) & \equiv & 3x\ [P] \end{array} \right.$$

On peux ensuite construire la matrice associée à φ_{11}, on obtient ainsi

$$M_{\varphi_{11}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 0 \end{pmatrix}$$

et

$$M_{\varphi_{11}} - I_{11} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 3 \\ 0 & 0 & -1 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & -1 & 0 \\ 0 & 4 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

On peux remarquer que $rg(M_{\varphi_{11}} - I_{11}) = 2$, par conséquent il y a quatre facteurs irréductibles et le noyau de $ker(M_{\varphi_{11}} - I_{11}) = \langle 1, x^3, 5x^2 + x^4, 3x + x^5 \rangle$ (grâce à un algorithme d'algèbre linéaire). On a :

$$pgcd(X^6 + 7, 3XX^5 + 1) = X^2 + 4X + 5,\ pgcd(X^6 + 7, 3X + X^5 + 2) = X + 4,$$

$$pgcd(X^6 + 7, 3X + X^5 + 9) = X + 7,\ pgcd(X^6 + 7, 3X + X^5 + 10) = X^2 + 7X + 5.$$

On obtient donc une factorisation de P modulo 11, d'où

$$P = (X^2 + 7X + 5)(X^2 + 4X + 5)(X + 7)(X + 4).$$

Chapitre 5

Conclusion

Nous avons pu voir que la factorisation d'un polynôme en facteurs irréductibles est assez simple pour p assez petit grâce à l'algorithme de Berlekamp, mais cette recherche de factorisation devient assez vite fastidieuse pour p grand. Ceci est dû à sa complexité polynomiale. Par conséquent pour faire face à ce problème, on utilise d'autres algorithmes probabilistes avec toujours une complexité polynomiale, cependant plus rapide que la méthode d'algèbre linéaire. Malheureusement, on ne connaît pas encore d'algorithme déterministe avec une complexité linéaire ou quasi-linéaire dans des corps finis.

Grâce à cette factorisation dans $\mathbb{F}_p$, on peux trouver une factorisation dans Z à l'aide d'algorithme de remontée de Hensel linéaire ou quadratique. On peux retrouver une autre utilisation de la factorisation dans des corps fini de polynômes dans les systèmes de calculs formels, en cryptographie notamment dans le calcul de logarithme discret, ...

Bibliographie

[1] M. Demazure. *Cours d'algèbre (seconde édition)*. Cassini.

[2] J.-P. Escofier. *Théorie de Galois*. Dunod.

[3] D. Guin and T. Hausberger. *Algèbre I : Groupes, corps et théorie de Galois*. EDP Sciences.

[4] D. Madore. Factorisation de polynômes sur les corps finis.

[5] R. Ollivier. Résolution d'un système linéaire par l'algorithme de wiedermann.

[6] S. Roman. *Field theory (Second edition)*. Springer, décembre 2007.

[7] E. Schost. Factorisation des polynômes. STIX, Ecole polytechnique, novembre 2004.

[8] J. Stern. Polynômes à une variable. Algorithme et programmation (cours avancé à l'ENS), janvier 2011.

[9] P. Tauvel. *Corps commutatifs et théorie de Galois*. Calvage et Mounet.