Arithmétique des corps de fonctions et ses applications à l'algorithmique et à la cryptologie

Alexander Gewirtz

Arithmétique des corps de fonctions et ses applications à l'algorithmique et à la cryptologie

Alexander Gewirtz

Remerciements

Tout d'abord, je tiens à remercier mes directeurs de thèse, Franck Leprévost et Alexei Pantchichkine, pour m'avoir suggéré l'étude des modules de Drinfeld ainsi que pour l'aide qu'ils m'ont apportée tout au long de mon travail.

Je remercie Serge Vladut et Eugénie Pankratiev d'avoir accepté de rapporter sur ma thèse et de participer à ce jury, ainsi que pour leurs commentaires qui m'ont permis d'améliorer le texte.

Je remercie également Michael Pohst d'avoir accepté de rapporter sur ma thèse et de participer à ce jury, ainsi que pour son invitation à faire un exposé à l'université de Berlin, la T.U. Berlin.

Je tiens également à remercier Rolland Gillard d'avoir accepté de participer à ce jury.

Je remercie également Hassan Oukhaba pour son invitation à faire un exposé au séminaire de théorie des nombres de Besançon.

Je suis reconnaissant à Bruno Anglès pour ses commentaires sur mon preprint ainsi que les suggestions qu'il m'a faites.

Je remercie également Gérard Vinel pour son aide très précieuse en ce qui concerne toute la partie informatique, ainsi qu'Arlette Guttin-Lombard pour son aide avec la présentation et les problèmes administratifs.

Je remercie également toute ma famille pour ses encouragements et son soutien.

Un grand merci à François Boisson pour ses conseils.

Enfin, je remercie Océane qui m'a soutenu et aidé tout au long de mon travail.

Table des matières

Chapitre 0

Introduction

Les objets principaux considérés dans cette thèse sont d'une part les polynômes irréductibles sur un corps fini - et plus précisément l'existence de pentanômiaux irréductibles sur $\mathbb{F}_2$ - et d'autre part, les modules de Drinfeld, où nous nous intéressons à l'étude de la torsion.

Les polynômes irréductibles jouent un rôle tout à fait crucial en mathématiques. D'un point de vue théorique, ils correspondent aux places finies de $\mathbb{F}_q(T)$, déterminent l'arithmétique des corps de fonctions (tout comme les nombres premiers déterminent l'arithmétique des corps de nombres) et sont les objets de base de la géométrie algébrique. D'un point de vue pratique, ils permettent de définir de manière concrète les corps finis, ce qui est particulièrement intéressant en cryptographie. Dans le premier chapitre, nous traitons l'aspect théorique des polynômes irréductibles. Plus précisément, nous rappelons les différents tests d'irréductibilité ainsi que des méthodes pour construire de tels polynômes, soit par composition, soit récursivement.

D'un côté pratique maintenant, ce sont les applications à la cryptologie qui sont intéressantes. Pour des raisons pratiques, on est amené à travailler sur les corps finis de caractéristique 2. Dans ce cadre, on est donc intéressé par la construction de polynômes irréductibles sur $\mathbb{F}_2$ les plus simples possibles, c'est-à-dire creux (ayant le moins de coefficients non nuls). Mais travaillant en caractéristique 2, les meilleurs candidats sont donc les trinômiaux (ayant uniquement trois coefficients non nuls) puis les pentanômiaux (ayant cinq coefficients non nuls). Dans le second chapitre, nous rappelons les résultats de Swan [40] (qui montrent en particulier que lorsque n est divisible par huit, il n'existe pas de trinômial irréductible sur $\mathbb{F}_2$ de degré n), puis nous étudions le cas des pentanômiaux et obtenons quelques résultats nouveaux. Pour être plus précis, les propositions **2.3.1** et **2.3.2** donnent des exemples de familles de pentanômiaux irréductibles, la proposition **2.3.3** et son corollaire **2.3.4** montrent qu'il existe toujours un pentanômial de degré n donné ayant un nombre impair de facteurs irréductibles sur $\mathbb{F}_2$ et enfin, nous présentons une liste de pentanômiaux irréductibles de degré compris entre 4 et 18000, ce qui constitue le record actuel. Pour

terminer avec cet aspect pratique, on peut remarquer que les polynômes bijectifs et irréductibles jouent un rôle central dans les applications algorithmiques de l'arithmétique des corps de fonctions, et que ceux qui sont intéressants proviennent de la théorie des modules de Drinfeld.

Pour leur part, les modules de Drinfeld jouent pour les corps globaux de caractéristique positive un rôle analogue à celui des courbes elliptiques pour la théorie des nombres algébriques. Etudiés pour la première fois par Carlitz, c'est dans les années 1970 que Drinfeld [5] a véritablement défini ce que sont les modules de Drinfeld et qu'il appelait à l'époque, modules elliptiques. C'est grâce à cette nouvelle théorie que Drinfeld a réussi à démontrer un analogue du théorème de Kronecker-Weber pour les corps de fonctions, ainsi qu'une partie des conjectures de Langlands pour GL(2). Bien que des définitions plus générales existent, nous nous intéressons dans cette thèse aux modules de Drinfeld sur $A = \mathbb{F}_q[T]$, c'est-à-dire aux morphismes d'anneaux $\varphi : A \mapsto L\{\tau\}$ (où $L\{\tau\}$ désigne l'anneau non commutatif des polynômes en $\tau : x \mapsto x^q$) vérifiant de plus que le terme constant de $\varphi(a)$ est a, pour tout a dans A. De plus, on appelle rang du module de Drinfeld l'entier $r = \deg_\tau(\varphi(T))$. Nous présentons, dans le troisième chapitre, les résultats généraux sur ceux-ci, notamment les analogies avec les courbes elliptiques.

Etant donné les fortes similitudes entre ces deux objets, il est naturel de se demander si certains résultats connus pour les courbes elliptiques se transposent aux modules de Drinfeld, en particulier le théorème de Mazur [24], qui donne les structures possibles pour les points de torsion rationnels, ainsi que l'ancienne conjecture de la borne uniforme, démontrée par Merel [26]. De façon plus précise, si φ est un module de Drinfeld à coefficients dans un corps L, on peut munir L d'une structure de A-module en posant $a.x = \varphi(a)(x)$, si on identifie un élément de $L\{\tau\}$ avec la fonction polynômiale. Pour cette nouvelle structure, on désigne par L^{φ}_{tor} le sous-module des points de torsion dans L. Dans certains cas, on peut donner une description explicite de la torsion des modules de Drinfeld : dans le quatrième chapitre, nous déterminons, par des méthodes élémentaires - à savoir en calculant les valuations possibles pour les points de torsion - toutes les structures possibles pour les points de torsion dans A :

Théorème 4.2.1 : Théorème de la borne uniforme dans le cas rationnel.
Pour tout module de Drinfeld A-rationnel de rang r, on a :

- (1) Si $q = 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q^2$. De plus, A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :

$$\{0\} \ , \ A/(T) \ , \ A/(T+1) \ , \ A/(T(T+1))$$

- (2) Si $q > 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q$. De plus, A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :

$$\{0\} \ , \ A/(T-\alpha) \text{ avec } \alpha \in \mathbb{F}_q$$

- (3) Enfin, si l'on fixe $r \geq 1$ ($r \neq 2$ si $q = 2$) et B l'un des modules cycliques précédents, il existe un module de Drinfeld de rang r dont la torsion est isomorphe à B.

Nous donnons également une borne uniforme pour la torsion dans les extensions finies entières de A :

Théorème 4.3.1 : Théorème de la borne uniforme dans le cas des extensions entières finies.

Soit $n \geq 1$ fixé. Alors pour tout anneau B entier et de type fini sur A vérifiant $[L : k] \leq n$ (où L désigne le corps de fractions de B) et pour tout module de Drinfeld B-rationnel φ, $\mid B_{tor}^{\varphi} \mid \leq \; q^{\frac{nq}{q-1}}$.

Enfin, nous retrouvons dans un cadre moins général les résultats de Poonen [35] sur la conjecture de la borne uniforme pour $r = 1$ (**corollaire 4.4.3**). Malheureusement, les techniques élémentaires employées ne permettent pas d'établir de véritable analogue du théorème de Merel tout simplement parce qu'on ne peut facilement borner inférieurement la valuation des points de torsion si ceux-si sont dans une extension de corps et non plus entiers.

Il existe par ailleurs une interprétation géométrique très intéressante des modules de Drinfeld admettant des points de torsion donné [41]. Les points rationnels qui correspondent à ces modules sont utilisés pour la construction de codes géométriques, fournissant ainsi une application pratique à ces objets théoriques. Dans le dernier chapitre, nous nous intéressons aux applications à la cryptologie, et plus précisément au cryptosystème développé dans [13]. Dans ce cadre, à savoir celui des modules de Drinfeld sur un corps fini, nous rappelons dans un premier temps la définition de la caractéristique d'Euler-Poincaré ainsi qu'une méthode pratique de calcul. Dans un second temps, nous étudions en détail le module de Carlitz et obtenons une méthode de calcul très simple pour la caractéristique d'Euler-Poincaré, puis sa généralisation aux modules de Drinfeld de rang 1 :

Proposition 5.2.5 : Proposition sur la caractéristique d'Euler-Poincaré associée au module de Carlitz.

Soit f irréductible unitaire et φ le module de Carlitz. Alors $f_{\varphi} = f - 1$.

Proposition 5.2.6 : Proposition sur la caractéristique d'Euler-Poincaré associée à un module de Drinfeld de rang 1.

Soit $\varphi_T = T + g\tau$ un module de Drinfeld de rang 1 avec $g \in A \setminus \{0\}$ et f un polynôme irréductible unitaire de degré n. Désignons par $\alpha \in \mathbb{F}_{q^n}$ une racine de f. Alors $f_{\varphi} = f - N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g(\alpha))$.

Nous en déduisons alors une égalité assez surprenante et contraire aux propriétés habituelles des déterminants :

Théorème 6.2.7 : Théorème sur une propriété d'additivité du déterminant.

Soit α un élément primitif de $\mathbb{F}_{q^n}/\mathbb{F}_q$ et σ le Frobienus. En désignant par m_{α} l'endomorphisme de multiplication par α, alors :

$$\det(m_{\alpha} + \sigma) = \det(m_{\alpha}) + \det(\sigma)$$

Enfin, pour terminer, après une brève énumération des différents protocoles existant en cryptographie, nous détaillons les applications pratiques des modules de Drinfeld à la cryptologie.

A ce jour, certaines questions que nous avons abordées dans cette thèse sont encore ouvertes :

Conjecture sur l'existence de pentanômiaux irréductibles : Pour tout entier $n \geq 4$, il existe au moins un pentanômial de degré n irréductible sur $\mathbb{F}_2$.

Ainsi que sa version moins forte mais plus intéressante pour les applications à la cryptologie :

Conjecture sur l'existence de trinômiaux ou de pentanômiaux irréductibles : Pour tout entier $n \geq 2$, il existe au moins un trinômial ou un pentanômial de degré n irréductible sur $\mathbb{F}_2$.

En ce qui concerne les modules de Drinfeld, on peut citer les deux conjectures suivantes :

Conjecture de la borne uniforme (forme forte) : Soit $r \geq 1$ et $n \geq 1$ deux entiers donnés. Alors il existe une constante $C(n, r)$, ne dépendant que de n et de r, telle que pour toute extension finie de $\mathbb{F}_q(T)$ de degré $\leq n$ et tout module de Drinfeld L-rationnel de rang r, $\mid L_{tor}^{\varphi} \mid \leq C(n, r)$.

Conjecture de la borne uniforme (forme faible) : Soit $r \geq 1$ et L une extension finie de $\mathbb{F}_q(T)$ donnés. Alors il existe une constante $C(L, r)$ ne dépendant que de L et de r, telle que pour tout module de Drinfeld L-rationnel de rang r, $\mid L_{tor}^{\varphi} \mid \leq C(L, r)$.

Questions ouvertes

Enfin, citons quelques problèmes qui méritent une attention particulière :

- Essayer d'établir un analogue de l'algorithme de Schoff pour calculer f_{φ}.
- Donner une interprétation modulaire des points de torsion dans les extensions finies de $\mathbb{F}_q(T)$ pour obtenir un véritable analogue du théorème de Merel.

Chapitre 1

Généralités sur l'arithmétique des corps de fonctions

Dans tout ce chapitre, p désigne un nombre premier et q une puissance de p.

1.1 Généralités sur les polynômes irréductibles sur $\mathbb{F}_q$

1.1.1 Existence et dénombrement

Proposition 1.1.1 *Pour tout entier $n \geq 1$, il existe au moins un polynôme irréductible sur $\mathbb{F}_q$ de degré n.*

En effet, tout sous-groupe fini de $K^\star$ où K est un corps commutatif est cyclique. Par suite, $\mathbb{F}_{q^n}^\star$ est cyclique. En prenant alors un générateur x de ce groupe, le polynôme minimal de x est irréductible sur $\mathbb{F}_q$ de degré n.

Ceci permet d'affirmer l'existence. Mais en fait, on peut dire beaucoup plus.

Lemme 1.1.2 *Soit n un entier positif et S l'ensemble des polynômes à coefficients dans $\mathbb{F}_q$, irréductibles unitaires de degré divisant n. Alors*

$$x^{q^n} - x = \prod_{P \in S} P$$

Preuve :

Soit $P \in S$. Montrons que P divise $x^{q^n} - x$.

On a $\mathrm{Dec}_{\mathbb{F}_q}(P) \simeq \mathbb{F}_{q^d}$ où d désigne le degré de P. Comme $d \mid n$, $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. Soit a une racine de P, alors $a \in \mathbb{F}_{q^n}$ donc a est une racine de $x^{q^n} - x$, ce qui permet de conclure que P divise $x^{q^n} - x$ (puisque P est irréductible, il est séparable car les corps finis sont parfaits) dans $\mathbb{F}_{q^d}$, soit $x^{q^n} - x = AP$ où $A \in \mathbb{F}_{q^d}[X]$. Maintenant si σ désigne le Frobienus, on a $A^\sigma P = AP$, ce qui

entraîne que $A^\sigma = A$, i.e. $A \in \mathbb{F}_q[X]$. Ce qui montre bien que P divise $x^{q^n} - x$ dans $\mathbb{F}_q[X]$.

Réciproquement, soit P irréductible unitaire divisant $x^{q^n} - x$ et a une racine de P. Comme $x^{q^n} - x$ est séparable, il suffit de montrer que $P \in S$. Alors $a \in \mathbb{F}_{q^n}$. Par conséquent,

$$[\mathbb{F}_{q^n} : \mathbb{F}_q(a)][\mathbb{F}_q(a) : \mathbb{F}_q] = n$$

Mais comme P est irréductible, $[\mathbb{F}_q(a) : \mathbb{F}_q] = \deg P$, d'où le résultat. On en déduit alors :

Proposition 1.1.3 *Soit $I(n,q)$ le nombre de polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ et μ la fonction de Möbius. Alors :*

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$$

Preuve :

D'après le lemme précédent, $q^n = \sum_{d|n} dI(d,q)$. On conclut alors en utilisant la première formule d'inversion de Möbius.

1.1.2 Tests d'irréductibilité

Il existe en fait très peu de méthodes pour tester la primalité d'un polynôme. Dans ce paragraphe, on présente deux techniques.

Théorème 1.1.4 *[25, p.60] Soit $f \in \mathbb{F}_q[X]$ un polynôme de degré n. Soit par ailleurs, $r_1, \ldots, r_t$ les diviseurs premiers distincts de n. Alors f est irréductible sur $\mathbb{F}_q$ si et seulement si :*

- *(i) $f(x) \mid x^{q^n} - x$*
- *(ii) $\forall i \in \{1, \ldots, t\}$, $pgcd(x^{q^{\frac{n}{r_i}}} - x, f(x)) = 1$*

Preuve :

- Supposons que f soit irréductible sur $\mathbb{F}_q$. Quitte à diviser f par son coefficient dominant, on peut supposer que f est unitaire. Alors d'après le lemme précédent, f divise $x^{q^n} - x$. Ce qui établit (i).
  Par ailleurs, soit $i \in \{1, \ldots, t\}$. Toujours d'après le lemme,

  $$x^{q^{\frac{n}{r_i}}} - x = \prod P$$

  le produit étant pris sur tous les polynômes irréductibles unitaires de degré divisant $\frac{n}{r_i}$. Mais comme f est irréductible de degré n ne divisant pas $\frac{n}{r_i}$, $f \not| x^{q^{\frac{n}{r_i}}} - x$. On en déduit donc (ii) puisque f est irréductible.
- Réciproquement, on suppose que f vérifie (i) et (ii). Montrons que f est irréductible. Par l'absurde. Ecrivons $f = \prod_{i=1}^{N} P_i$ où P_i est irréductible et supposons que $N > 1$. Soit $i \in \{1, \ldots, N\}$. Comme f vérifie (i), on en déduit en appliquant de nouveau le lemme que $\deg P_i = d_i$ divise n. Par ailleurs, comme on a supposé $N > 1$, $d_i \neq n$. Par conséquent, il existe

$j \in \{1, \ldots, t\}$ tel que $d_i \mid \frac{n}{r_j}$. Mais sous ces conditions, $P_i \mid x^{q^{\frac{n}{r_j}}} - x$ et $P_i \mid f$. Ce qui contredit (ii). Et donc f est bien irréductible.
Ce qui achève la démonstration du théorème.

Théorème 1.1.5 *[33] Soit $f \in \mathbb{F}_q[T]$. On suppose que f n'a pas de facteurs multiples. Soit $A = \frac{\mathbb{F}_q[T]}{(f)}$ et τ l'opérateur $\mathbb{F}_q$-linéaire qui à $a \in A$ associe a^q. Alors sont équivalents :*
- *(i) f est irréductible sur $\mathbb{F}_q$*
- *(ii) $rg(\tau - Id) = deg\ f - 1$*

Preuve :
Soit $f = \prod_{i=1}^{s} h_i$ la décomposition de f en facteurs irréductibles. Alors,

$$A \simeq \prod_{i=1}^{s} \frac{\mathbb{F}_q[T]}{(h_i)}$$

Par ailleurs, chaque $\frac{\mathbb{F}_q[T]}{(h_i)}$ contient le corps des constantes $\mathbb{F}_q$ caractérisé par $\mathbb{F}_q = \{a \in \frac{\mathbb{F}_q[T]}{(h_i)}, a^q = a\}$. On en déduit donc que

$$\mathrm{Ker}(\tau - Id) \simeq \mathbb{F}_q^s$$

On conclut alors par le théorème du rang.

1.2 Construction de polynômes irréductibles

1.2.1 Exemples de familles de polynômes irréductibles

Avant de donner quelques exemples de familles de polynômes irréductibles, on s'intéresse à une famille remarquable : les polynômes cyclotomiques.

Définition 1.2.1 *[21, p.61] Soit $\mathbb{F}_q$ un corps fini de caractéristique p, et n un entier non divisible par p. Soit ξ une racine primitive n-ième de l'unité dans une extension de $\mathbb{F}_q$. On appelle n-ième polynôme cyclotomique de $\mathbb{F}_q$, et on note Q_n, le polynôme défini par :*

$$Q_n(x) = \prod_{pgcd(s,n)=1} (x - \xi^s)$$

Il est facile de voir que cette définition ne dépend pas du choix de ξ. En effet, si ξ' est une autre racine primitive n-ième de l'unité, alors $\xi' = \xi^t$ avec $\mathrm{pgcd}(n, t) = 1$. Mais dans ce cas, l'application de $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\star$ dans lui même, qui à s fait correspondre st est une bijection. Ce qui montre bien que Q_n ne dépend pas du choix de la racine primitive.

Lemme 1.2.2 *[21, p.61] Soit $K = \mathbb{F}_q$ un corps de caractéristique p, et n un entier non divisible par p. Alors :*
- *(i) Q_n est de degré $\phi(n)$*

- (ii) $x^n - 1 = \prod_{d|n} Q_d(x)$
- (iii) $Q_n(x) \in \mathbb{F}_p[x]$

Preuve :
- (i) Découle de la définition de la fonction ϕ d'Euler.
- (ii) Comme n est premier à p, $x^n - 1$ est séparable, et mieux, ses racines sont les ξ^t, $1 \leq t \leq n$ où ξ est une racine primitive n-ième de l'unité. Il est alors clair que chaque racine de $x^n - 1$ est racine du polynôme Q_d où d est l'ordre de cette racine. Ceci montre que $x^n - 1$ divise $\prod_{d|n} Q_d(x)$ (dans $\bar{K}$). Par ailleurs, on a l'identité remarquable : $\sum_{d|n} \phi(d) = n$, ce qui montre que ces deux polynômes ont même degré. D'où l'égalité.
- (iii) On raisonne par récurrence sur n.
  - Cas $n = 1$
    On a $Q_1(x) = x - 1$. La propriété est vraie au rang 1.
  - On suppose la propriété vraie pour tout entier $0 \leq k < n$. Montrons qu'elle est vraie au rang n
    Posons $f(x) = \prod_{d|n, d<n} Q_d(x)$. L'hypothèse de récurrence entraîne que $f(x) \in \mathbb{F}_p[x]$. Par ailleurs, d'après (ii), on a $Q_n(x) = \frac{x^n-1}{f(x)}$. Il en résulte que $Q_n(x) \in \mathbb{F}_p(x) \cap \mathbb{F}_{q'}[x]$, (où $\mathbb{F}_{q'} = \mathrm{Dec}_{\mathbb{F}_p}(x^n - 1)$). Par suite $Q_n(x) \in \mathbb{F}_p[x]$. La propriété est donc vraie au rang n

  Ce qui achève la récurrence ainsi que la démonstration de (iii).

Théorème 1.2.3 *[21, p.62] Soit $K = \mathbb{F}_q$ un corps de caractéristique p, et n un entier non divisible par p. Pour d premier à p, $\tau(d)$ désigne l'ordre de q dans $\left(\frac{\mathbb{Z}}{d\mathbb{Z}}\right)^\star$. Alors :*
- (i) $[Dec_K(x^n - 1) : K] = \tau(n)$
- (ii) *$Q_n(x)$ a exactement $\frac{\phi(n)}{\tau(n)}$ facteurs irréductibles sur K*

Preuve :
- (i) Soit ξ une racine primitive n-ième de l'unité, $\mathrm{Dec}_K(x^n - 1) = K(\xi)$. De plus, on a les équivalences suivantes pour tout entier k :

$$\begin{aligned} \xi \in \mathbb{F}_{q^k} &\iff \xi^{q^k} = \xi \\ &\iff \xi^{q^k - 1} = 1 \\ &\iff n \mid q^k - 1 \text{ (car } \xi \text{ est une racine primitive)} \\ &\iff \tau(n) \mid k \end{aligned}$$

  Ceci démontre le point (i)
- (ii) Soit $g(x)$ un facteur irréductible de $Q_n(x)$ et α une racine de g. Alors α est une racine primitive n-ième de l'unité. Donc d'après la preuve de (i), $[K(\alpha) : K] = \tau(n)$. Mais comme g est irréductible, $\deg g = \tau(n)$.
  On conclut enfin en regardant les degrés et en remarquant que Q_n est séparable.

Maintenant, on a besoin d'un petit résultat d'arithmétique :

Lemme 1.2.4 *[21, p. 89] Soient $s, e \geq 2$ deux entiers premiers entre eux et soit m l'ordre de s modulo e. Soit $t \geq 2$. On suppose que t vérifie :*

– (i) $pgcd(t, \frac{s^m-1}{e}) = 1$
– (ii) *Chaque facteur premier de* t *divise* e
– (iii) *Si* $4 \mid t$, *alors* $4 \mid s^m - 1$

Alors l'ordre de s *modulo* te *est égal à* mt.

Preuve :

On va démontrer le lemme par récurrence sur n, le nombre de facteurs premiers (comptés avec multiplicités) de t.

– Cas $n = 1$:
On suppose donc que t est premier. En écrivant $d = \frac{s^m-1}{e}$, avec d premier avec t, on a $s^m = 1 + de$. Par suite,

$$\begin{aligned} s^{mt} &= (1+de)^t \\ &= 1 + \sum_{i=1}^{t-1} C_t^i d^i e^i + d^t e^t \end{aligned}$$

Comme t est premier, t divise C_t^i pour $1 \leq i \leq t-1$. De plus, d'après (ii), t divise e. Par suite, $s^{mt} \equiv 1\ [et]$. Il en découle que l'ordre de s modulo et divise mt. Par ailleurs, si s^k est congru à 1 modulo et, a fortiori s^k est congru à 1 modulo e. Ce qui montre que l'ordre de s modulo et est divisible par m. Comme t est premier, on en déduit que l'ordre en question vaut soit m soit mt. Si son ordre vaut m, alors $de \equiv 0\ [et]$ et donc t divise d, ce qui est absurde.
La propriété est donc vraie au rang 1.

– On suppose la propriété vraie pour tout entier t ayant un nombre de facteurs premiers (avec multiplicités) inférieur ou égal à n. Montrons qu'elle est encore vraie au rang $n+1$.
Soit donc t vérifiant $(i), (ii), (iii)$ ayant $n+1$ facteurs premiers. On écrit alors $t = rt'$, où r est un nombre premier. D'après le cas $n = 1$, on sait déjà que l'ordre de s modulo er est égal à mr. On remarque alors que si l'on montre que t' vérifient les hypothèses du lemme avec $e' = er$, $m' = mr$, alors par hypothèse de récurrence, s est d'ordre $m't'$ modulo $e't'$, i.e s est d'ordre mt modulo et, et la propriété sera vraie au rang $n+1$, ce qui achèvera la démonstration.
Soit p un nombre premier divisant t'. Comme chaque facteur premier de t divise e, il est clair que p divise e'. On écrit alors de nouveau $d = \frac{s^m-1}{e}$.
On a alors :

$$s^{mr} - 1 = c(s^m - 1) \text{ où } c = \sum_{i=0}^{r-1} s^{im}$$

Par suite, $d' = \frac{s^{mr}-1}{er} = \frac{cd}{r}$. De plus, comme s^m est congru à 1 modulo e et que r divise e, il s'ensuit que s^m est congru à 1 modulo r. En reportant dans la définition de c, on en déduit que $c \equiv r \equiv 0\ [r]$. Ce qui montre que $\frac{c}{r}$ est un entier. Puisque p ne divise pas d, il suffit de montrer que p ne divise pas $\frac{c}{d}$ pour montrer que p ne divise pas d'.

De même que précédemment, on a $s^m \equiv r\ [p]$. Deux cas se présentent alors : si $p \neq r$, alors r est inversible modulo p et donc $\frac{c}{r} \equiv 1\ [p]$. Maintenant, si $p = r$, alors $s^m = 1 + br\ [r^2]$ pour un entier b. Par suite :

$$\forall j \geq 0, s^{mj} \equiv (1 + br)^j \equiv 1 + jbr\ [r^2]$$

et donc,

$$c \equiv r + br \sum_{j=0}^{r-1} j \equiv r + br\frac{r(r-1)}{2}\ [r^2]$$

On en déduit alors que :

$$\frac{c}{r} \equiv 1 + b\frac{r(r-1)}{2}\ [r]$$

Si r est impair, alors $\frac{c}{r} \equiv 1\ [r]$, et donc $p = r$ ne divise pas $\frac{c}{d}$, ce qui est la conclusion souhaitée. Maintenant, si $p = r = 2$, alors 4 divise t et donc d'après (iii), 4 divise $s^m - 1$. Mais dans ce cas, comme $c = s^m + 1$, on en déduit que c est congru à 2 modulo 4 et donc que $\frac{c}{r}$ est congru à 1 modulo 2. Ce qui montre que 2 ne divise pas $\frac{c}{d}$.
En vertu de la remarque, on en déduit que la propriété est vraie au rang $n + 1$.

Ce qui achève la récurrence et la démonstration du lemme.

Ce lemme nous permet alors d'énoncer le théorème suivant :

Théorème 1.2.5 [25, p.40] [21, p.90-91] *(J.A.Serret) Soit $a \in \mathbb{F}_q^\star$ d'ordre e. Alors le polynôme $x^t - a$ est irréductible dans $\mathbb{F}_q[X]$ si et seulement si l'entier $t \geq 2$ vérifie les conditions suivantes :*

- *(i) pgcd$(t, \frac{(q-1)}{e}) = 1$*
- *(ii) Pour tout nombre premier p, $(p \mid t \Rightarrow p \mid e)$*
- *(iii) Si $4 \mid t$, alors $4 \mid (q-1)$*

Preuve :

- Supposons que $x^t - a$ est irréductible sur $\mathbb{F}_q$.
  Déjà, il est clair que $d = \text{pgcd}(t, \frac{q-1}{e}) = 1$. En effet, dans le cas contraire, on aurait la factorisation non triviale suivante : pour $t = dt'$, $\frac{q-1}{e} = de'$, et g un générateur de $\mathbb{F}_q^\star$:

$$x^t - a = x^{dt'} - g^{kde'} = (x^{t'} - g^{ke'})(\sum_{i=0}^{d-1} x^{it'} g^{(d-1-i)ke'})$$

  Ce qui établit le point (i).
  Soit α une racine de $P = x^t - a$ et soit ξ une racine primitive t-ième de l'unité. Alors les racines de P sont les $\xi^k\alpha$, $0 \leq k \leq t-1$. Maintenant, comme P est irréductible, toutes ses racines ont le même ordre. Par conséquent, t divise l'ordre de α (puisque $\xi^{w(\alpha)}\alpha^{w(\alpha)} = 1$, où $w(\alpha)$ désigne l'ordre de α). Posons alors $w(\alpha) = tu$. On a alors :

$$1 = \alpha^{w(\alpha)} = (\alpha^t)^u = a^u$$

Mais comme a est d'ordre e, e divise u et donc et divise l'ordre de α. De plus, $\alpha^{et} = 1$, ce qui montre qu'en fait, α est d'ordre exactement et, i.e. que α est une racine primitive et-ième de l'unité. En conservant les notations précédentes, α est racine de Q_{et} (et-ième polynôme cyclotomique sur $\mathbb{F}_q$). Par suite, $x^t - a$ divise Q_{et}. Le raisonnement fait ici ne dépend pas de l'élément d'ordre e choisi. On en déduit alors que :

$$\prod_{a \in \mathbb{F}_q^\star \text{ d'ordre } e} (x^t - a) \mid Q_{et}$$

Montrons alors que la divisibilité précédente est une égalité, i.e qu'on a obtenu la décomposition en facteurs irréductibles sur $\mathbb{F}_q$ de Q_{et}.
Soit β une racine de Q_{et}. Comme e divise $q-1$, on a $q = 1 + \lambda e$ pour un entier λ. Il s'ensuit que

$$(\beta^t)^q = \beta^{qt} = \beta^{t+\lambda et} = \beta^t$$

Par suite, $\beta^t \in \mathbb{F}_q$ et est d'ordre e. On en déduit alors que le polynôme minimal de β sur $\mathbb{F}_q$ est $x^t - \beta^t$. Par conséquent, on a bien comme annoncé $Q_{et} = \prod_a (x^t - a)$ (le produit étant pris sur tous les éléments d'ordre e). En regardant les degrés, on trouve :

$$\phi(et) = t\phi(e)$$

ce qui établit le point (ii), à savoir que tout nombre premier divisant t divise également e.
En ce qui concerne le point (iii), supposons que 4 divise t et que $q-1$ ne soit pas divisible par 4. Alors, nécessairement, $q \equiv 3$ [4] et $e \equiv 2$ [4]. De plus, comme a est d'ordre e, $a^{\frac{e}{2}} = -1$. Il s'ensuit que $x^t - a = x^t + a^d$ où $d = \frac{e}{2} + 1$ est pair. On a alors :

$$\begin{aligned} a^d &= 4(2^{-1}a^{\frac{d}{2}})^2 \\ &= 4(2^{-1}a^{\frac{d}{2}})^{q+1} \\ &= 4c^4 \text{ où } c = (2^{-1}a^{\frac{d}{2}})^{\frac{q+1}{4}} \end{aligned}$$

(la deuxième égalité provient du fait que si $y \in \mathbb{F}_q$, alors $y^q = y$ et donc $y^2 = y.y = y.y^q = y^{q+1}$)
Mais ceci conduit à la factorisation non triviale :

$$\begin{aligned} x^t - a &= x^{4t'} + 4c^4 \\ &= (x^{2t'} + 2cx^{t'} + 2c^2)(x^{2t'} - 2cx^{t'} + 2c^2) \end{aligned}$$

Ce qui contredit l'irréductibilité de $x^t - a$. D'où le résultat.

– Réciproquement, on suppose que les entiers e et t vérifient les conditions $(i), (ii)$ et (iii).
Soit θ une racine de $x^t - a$ et P son polynôme minimal sur $\mathbb{F}_q$. Déjà, P divise $x^t - a$. De plus, le degré de P est le plus petit entier d tel que

$\theta \in \mathbb{F}_{q^d}$, soit de manière équivalente, le plus petit entier tel que $\theta^{q^d-1} = 1$; soit encore d est l'ordre de q modulo l'ordre de θ.
Soit $w(\theta)$ l'ordre de θ. Alors clairement, $w(\theta)$ divise et. Soit p un nombre premier divisant t. Supposons que $\nu_p(w(\theta)) < \nu_p(t)$. Alors, $w(\theta)$ divise $\frac{et}{p}$. Mais $1 = \theta^{\frac{et}{p}} = (\theta^t)^{\frac{e}{p}} = a^{\frac{e}{p}}$. Or d'après (ii), p divise e et par hypothèse, a est d'ordre e, d'où la contradiction. Par suite, t divise $w(\theta)$. En écrivant alors $w(\theta) = tu$, on trouve que $1 = \theta^{tu} = a^u$. Comme a est d'ordre e, il s'ensuit que e divise u. Finalement, on a montré que θ est d'ordre et et par conséquent que d est l'ordre de q modulo et.
Mais d'après le lemme précédent, avec $s = q$, $e = e$, $m = 1$, l'ordre de q modulo et est t. Par suite, $d = t$. Ainsi P divise $x^t - a$, P est unitaire de degré t, donc $P = x^t - a$ et le théorème est entièrement démontré.

Corollaire 1.2.6 *[25, p.40] Soit r un facteur premier de $q-1$ et $a \in \mathbb{F}_q$ d'ordre e tel que r ne divise pas $\frac{q-1}{e}$. Supposons par ailleurs que $q \equiv 1$ [4] si $r = 2$ et $k \geq 2$. Alors pour tout entier k, $x^{r^k} - a$ est irréductible sur $\mathbb{F}_q$.*

Exemple 1 *[25, p.41] En appliquant ce corollaire, il est facile de constater que pour tout entier $k \geq 0$:*
- *(a) $x^{2^k} + 2$ et $x^{2^k} - 2$ sont irréductibles sur $\mathbb{F}_5$*
- *(b) $x^{3^k} \pm 3$ et $x^{3^k} \pm 2$ sont irréductibles sur $\mathbb{F}_7$*
- *(c) $x^{3^k} + a$ est irreductible sur $\mathbb{F}_4$ pour $a \in \mathbb{F}_4 \setminus \mathbb{F}_2$*
- *(d) $x^{2 \cdot 3^k} + x^{3^k} + 1$ est irreductible sur $\mathbb{F}_2$*

Le (d) découle du fait que $x^{2 \cdot 3^k} + x^{3^k} + 1 = (x^{3^k} + a)(x^{3^k} + a^2)$ est la décomposition en facteurs irréductibles dans $\mathbb{F}_4$.

Lemme 1.2.7 *Soit n et m deux entiers, $d = pgcd(n, m)$ et $s = ppcm(n, m)$. Alors :*

$$\begin{aligned} \mathbb{F}_{q^n} \cap \mathbb{F}_{q^m} &= \mathbb{F}_{q^d} \\ \mathbb{F}_{q^n}.\mathbb{F}_{q^m} &= \mathbb{F}_{q^s} \end{aligned}$$

Preuve :

(1) Il est clair que $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n} \cap \mathbb{F}_{q^m}$ (puisque d divise n et m). Par ailleurs, si on pose $\mathbb{F}_{q^n} \cap \mathbb{F}_{q^m} = \mathbb{F}_{q^a}$, alors a divise n et m (en effet, par multiplicativité du degré, $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_{q^a}][\mathbb{F}_{q^a} : \mathbb{F}_q]$ et idem en remplacant n par m). Donc a divise d et $\mathbb{F}_{q^a} \subset \mathbb{F}_{q^d}$.

(2) On pose de même $\mathbb{F}_{q^n}.\mathbb{F}_{q^m} = \mathbb{F}_{q^a}$. Il est clair que $\mathbb{F}_{q^a} \subset \mathbb{F}_{q^s}$ puisque $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^s}$ et $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^s}$. Par ailleurs, comme $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^a}$, n divise a. De même, m divise a. On conclut alors que s divise a, ce qui montre l'inclusion $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^a}$.

Lemme 1.2.8 *[21, p.99] Soit $f \in \mathbb{F}_q[X]$ un polynôme irréductible de degré n, $k \geq 1$ et $d = pgcd(n, k)$. Alors f est le produit de d polynômes irréductibles sur $\mathbb{F}_{q^k}$, chacun de degré $\frac{n}{d}$.*

Preuve :

Soit g un facteur irréductible de f sur $\mathbb{F}_{q^k}$ et soit x une racine de g (a fortiori, c'est une racine de f). Alors $\mathbb{F}_q(x) \simeq \mathbb{F}_{q^n}$ (puisque f est irréductible sur $\mathbb{F}_q$). Par ailleurs, $\mathbb{F}_{q^k}(x) = \mathbb{F}_{q^s}$, où $s = \text{ppcm}(n,k)$ d'après le lemme précédent. On en déduit alors que $\deg g = [\mathbb{F}_{q^s} : \mathbb{F}_{q^k}] = \frac{s}{k} = \frac{n}{d}$. Ce qui montre que tous les facteurs irréductibles de f sur $\mathbb{F}_{q^k}$ sont de degré $\frac{n}{d}$. On conclut en regardant les degrés.

Corollaire 1.2.9 *[21, p.100] Soit $f \in \mathbb{F}_q[X]$ un polynôme irréductible de degré n, $k \geq 1$ et $d = pgcd(n,k)$. Alors f est irréductible sur $\mathbb{F}_{q^k}$ si et seulement si $pgcd(n,k) = 1$*

Les corollaires 1.2.6 et 1.2.9 permettent donc de construire des polynômes irréductibles de degré r divisant $q-1$, sauf si $q \equiv 3$ [4] et $r = 2$. Pour ce cas, on a besoin du théorème suivant :

Théorème 1.2.10 *[25, p.41] Soit p premier tel que $p \equiv 3$ [4] et posons $p+1 = 2^\gamma s$ avec s impair. Alors, pour tout entier $k \geq 1$, $x^{2^k} - 2a_\gamma x^{2^{k-1}} - 1$ est irréductible sur $\mathbb{F}_p$, et donc irréductible sur $\mathbb{F}_{p^m}$ pour tout entier impair m, où a_γ est obtenu par récurrence de la manière suivante :*

- *(i)* $a_1 = 0$
- *(ii)* $\forall j \in \{2, \ldots, \gamma - 1\},\ a_j = \left(\frac{a_{j-1}+1}{2}\right)^{\frac{(p+1)}{4}}$
- *(iii)* $a_\gamma = \left(\frac{a_{\gamma-1}-1}{2}\right)^{\frac{(p+1)}{4}}$

Lemme 1.2.11 *[25, p.42] Soit P un polynôme $\mathbb{F}_p$-linéaire. On suppose que P n'admet que 0 comme racine dans $\mathbb{F}_q$. Alors pour tout $b \in \mathbb{F}_q$, $P - b$ admet un facteur irréductible de degré 1.*

Preuve :

Tout endomorphisme injectif d'un espace vectoriel de dimension finie est surjectif.

Théorème 1.2.12 *[25, p.42] Le polynôme trinômial $x^p - x - b$ où $b \in \mathbb{F}_q$ et $q = p^m$ est irréductible sur $\mathbb{F}_q$ si et seulement si $Tr_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$*

Preuve :

On rappelle que la trace d'un élément b de $\mathbb{F}_q$ sur $\mathbb{F}_p$, notée $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$, est la trace de l'application $\mathbb{F}_p$-linéaire de $\mathbb{F}_q$ dans lui-même, obtenue par multiplication par b. On montre que cette trace est égale à la somme des conjugués de b, c'est-à-dire à la somme des b^{p^i} pour $0 \leq i \leq m-1$.

Soit θ une racine de $x^p - x - b$. Montrons par récurrence sur n que

$$\theta^{p^n} = \theta + \sum_{i=0}^{n-1} b^{p^i}$$

.

– $n = 1$
Découle du fait que θ est une racine de $x^p - x - b$. La propriété est donc vraie au rang 1.
– Passage de n à $n+1$
Supposons la propriété vraie au rang n, alors

$$\theta^{p^n} = \theta + \sum_{i=0}^{n-1} b^{p^i}$$

On obtient alors en élevant cette égalité à la puissance p :

$$\begin{aligned}
\theta^{p^{n+1}} &= \left(\theta + \sum_{i=0}^{n-1} b^{p^i}\right)^p \\
&= \theta^p + \sum_{i=0}^{n-1} b^{p^{i+1}} \\
&= \theta + b + \sum_{i=1}^{n} b^{p^i} \\
&= \theta + \sum_{i=0}^{n} b^{p^i}
\end{aligned}$$

La propriété est donc vraie au rang $n+1$. Ce qui achève la récurrence.
En particulier, $\theta^q = \theta + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$.
On en déduit donc que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) = 0$ si et seulement si $\theta^q = \theta$, c'est-à-dire si et seulement si toutes les racines de $x^p - x - b$ sont dans $\mathbb{F}_q$. Ceci démontre que si $x^p - x - b$ est irréductible sur $\mathbb{F}_q$ alors $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$.
Réciproquement, si $\tau = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b) \neq 0$, alors $\tau \in \mathbb{F}_p$ et on a :

$$\forall i \in \mathbb{N},\ \theta^{q^i} = \theta + i\tau$$

En particulier ceci montre que θ a p $\mathbb{F}_q$-conjugués distincts, et donc que son polynôme minimal sur $\mathbb{F}_q$ est de degré p, et donc est égal à $x^p - x - b$. Ce qui démontre la réciproque.

Corollaire 1.2.13 [*25, p.43*] *Soient $a, b \in \mathbb{F}_q^\star$. Alors, les deux propriétés suivantes sont équivalentes :*
– *(i) $x^p - ax - b$ est irréductible sur $\mathbb{F}_q$*
– *(ii) $\exists A \in \mathbb{F}_q,\ a = A^{p-1}$ et $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\frac{b}{A^p}) \neq 0$*

Preuve :
D'après le lemme concernant les polynômes linéaires, si $x^p - ax - b$ est irréductible alors $x^{p-1} - a$ a une racine dans $\mathbb{F}_q$. En effet, supposons que $x^{p-1} - a$ n'ait pas de racine non nulle dans $\mathbb{F}_q$. Alors $x^p - ax$ n'a pas de racine non nulle. On conclut alors grâce au lemme 1.2.11 que $x^p - ax - b$ a une racine dans $\mathbb{F}_q$, et donc ne peut être irréductible.
Soit donc A une racine de $x^{p-1} - a$. Il s'ensuit que

$$x^p - ax - b = A^p \left(\left(\frac{x}{A}\right)^p - \left(\frac{x}{A}\right) - \frac{b}{A^p} \right) \quad (1)$$

On conclut alors grâce au théorème.

La réciproque étant immédiate en partant de (1). Ceci termine la preuve du corollaire.

1.2.2 Composition

Après cette courte énumération de polynômes irréductibles sur un corps fini, il est intéressant de voir comment, à partir d'un ou plusieurs polynômes irréductibles, on peut en construire de nouveaux, de degré plus élevé. Une méthode consiste à s'intéresser aux compositions, et plus précisement aux polynômes de la forme :

$$P(\tfrac{f}{g}) = g^n(x) P(\tfrac{f(x)}{g(x)})$$

où $P, f,$ et g sont des polynômes. C'est l'objet de ce paragraphe.

Théorème 1.2.14 *[25, p.44] Soit $f, g, P \in \mathbb{F}_q[x]$. Supposons que $P = \sum_{i=0}^{n} c_i x^i$ est irréductible de degré n. Alors $P(\frac{f}{g})$ (défini comme ci-dessus) est irréductible sur $\mathbb{F}_q$ si et seulement si $f - \lambda g$ est irréductible sur $\mathbb{F}_{q^n}$ pour au moins une racine λ de P dans $\mathbb{F}_{q^n}$.*

Preuve :

Le cas $n = 1$ étant trivial, on peut supposer $n > 1$. Dans ce cas, $P(\frac{f}{g})$ est de degré hn où $h = max(\deg f, \deg g)$. Ceci est clair lorsque les degrés de f et g sont distincts et s'ils sont égaux à s, si a désigne le coefficient dominant de f et b celui de g, le coefficient du terme en x^{ns}, c, de $P(\frac{f}{g})$ est égal à

$$\sum_{i=0}^{n} c_i a^i b^{n-i} = b^n P(\frac{a}{b}).$$

Mais comme $b \neq 0$ par définition et que P est irréductible sur $\mathbb{F}_q$ (a fortiori n'a pas de racines dans $\mathbb{F}_q$), il s'ensuit que $c \neq 0$.

Soit γ une racine de $P(\frac{f}{g})$. Alors γ est une racine de $f - \lambda g$, où λ est une racine de P. On a donc :

$$\begin{aligned} P(\frac{f}{g}) \text{ irréductible sur } \mathbb{F}_q \quad &\iff \quad [\mathbb{F}_q(\gamma) : \mathbb{F}_q] = hn \\ &\iff \quad [\mathbb{F}_q(\gamma) : \mathbb{F}_q(\lambda)] = h \ (\text{car } [\mathbb{F}_q(\lambda) : \mathbb{F}_q] = n) \\ &\iff \quad f - \lambda g \text{ irréductible sur } \mathbb{F}_{q^n} \end{aligned}$$

Ce qui complète la démonstration du théorème.

On peut alors s'intéresser à des formes particulières de f et g :

Corollaire 1.2.15 *[25, p.44] Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré n. Alors pour tout $a, b, c, d \in \mathbb{F}_q$ tels que $ad - bc \neq 0$,*

$$(cx + d)^n P\left(\tfrac{ax+b}{cx+d}\right) \text{ est irréductible sur } \mathbb{F}_q$$

Théorème 1.2.16 *[25, p.44] Soit t un entier et $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré n et d'exposant e (c'est-à-dire toutes les racines de P sont d'ordre e). Alors $P(x^t)$ est irréductible sur $\mathbb{F}_q$ si et seulement si les trois conditions suivantes sont vérifiées :*

- *(i) $pgcd(t, \frac{q^n-1}{e}) = 1$*
- *(ii) Pour tout nombre premier p, $(p \mid t \Rightarrow p \mid e)$*
- *(iii) si $4 \mid t$ alors $4 \mid (q^n - 1)$*

Preuve :

D'après le théorème précédent, $P(x^t)$ est irréductible sur $\mathbb{F}_q$ si et seulement si $x^t - \lambda$ est irréductible sur $\mathbb{F}_{q^n}$ pour une racine λ de P. On applique alors le théorème 1.2.5.

Définition 1.2.17 *Si f est un polynôme de degré n, on appelle polynôme réciproque de f, et on note $f^\star$, le polynôme défini par*

$$f^\star(x) = x^n f(\tfrac{1}{x})$$

Remarque 1.2.18 *On peut constater d'une part que $(f^\star)^\star = f$ et d'autre part que f est irréductible sur $\mathbb{F}_q$ si et seulement si $f^\star$ l'est. En effet, il suffit d'appliquer le corollaire 1.2.15 avec ici $a = d = 0$ et $c = b = 1$. Cette petite remarque sera particulièrement intéressante dans le chapitre suivant, puisque le nombre de facteurs irréductibles de $T^n + T^k + 1$ est le même d'après ce qui précède que celui de $T^n + T^{n-k} + 1$, permettant ainsi de réduire le nombre de cas à considérer.*

En caractéristique 2, on dispose du théorème suivant :

Théorème 1.2.19 *[25, p.45] Soit $q = 2^m$ et $P = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ irréductible de degré n. Alors*

- *(i) $x^n P(x + x^{-1})$ est irréductible sur $\mathbb{F}_q$ si et seulement si $Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_1}{c_0}) \neq 0$*
- *(ii) $x^n P^\star(x + x^{-1})$ est irréductible sur $\mathbb{F}_q$ ssi $Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) \neq 0$*

Preuve :

On démontre (i), la démonstration de (ii) étant identique. D'après le théorème 1.2.14, $x^n P(x + x^{-1})$ est irréductible sur $\mathbb{F}_q$ si et seulement si $x^2 - ax - 1$ est irréductible sur $\mathbb{F}_{q^n}$, pour une racine a de P. Mais en appliquant le corollaire 1.2.13, $x^2 - ax + 1$ est irréductible sur $\mathbb{F}_{q^n}$ si et seulement si $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a^{-2}) \neq 0$. Or,

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a^{-2}) = \left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a^{-1})\right)^2 = \left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a^{-1}))\right)^2.$$

Mais a est une racine de P ($a \neq 0$) donc a^{-1} est une racine de $P^\star$ qui est irréductible sur $\mathbb{F}_q$. On en déduit donc que $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(a^{-1}) = -\frac{c_1}{c_0}$ (puisque le polynôme minimal de a^{-1} sur $\mathbb{F}_q$ est $c_0^{-1} P^\star$).

Ceci achève la démonstration de ce théorème.

Théorème 1.2.20 *[25, p.45] Soit p premier impair et $q = p^m$. Soit P un polynôme irréductible sur $\mathbb{F}_q$, de degré n. Alors sont équivalents :*

- *(i) $x^n P(x + x^{-1})$ est irréductible sur $\mathbb{F}_q$*
- *(ii) $P(2)P(-2)$ n'est pas un carré dans $\mathbb{F}_q$*

Preuve :

En appliquant le théorème 1.2.14, $x^n P(x+x^{-1})$ est irréductible sur $\mathbb{F}_q$ si et seulement si $x^2 - ax + 1$ est irréductible sur $\mathbb{F}_{q^n}$, où a est une racine de P. Ce qui est clairement équivalent à la condition $a^2 - 4$ n'est pas un carré dans $\mathbb{F}_{q^n}$.

$$\begin{aligned}
a^2 - 4 \notin \mathbb{F}_{q^n}^2 &\iff (a^2-4)^{\frac{q^n-1}{2}} = -1 \\
&\iff [(a-2)(a+2)]^{\frac{q^n-1}{2}} = -1 \\
&\iff \{[(2-a)(-2-a)]^{\frac{q^n-1}{q-1}}\}^{\frac{q-1}{2}} = -1 \\
&\iff \{[(2-a)(-2-a)]^{\sum_{i=0}^{n-1} q^i}\}^{\frac{q-1}{2}} = -1 \\
&\iff \left(\prod_{i=0}^{n-1} (2-a)^{q^i}(-2-a)^{q^i}\right)^{\frac{q-1}{2}} = -1 \\
&\iff \left(\prod_{i=0}^{n-1} (2-a^{q^i})(-2-a^{q^i})\right)^{\frac{q-1}{2}} = -1 \\
&\iff (P(2)P(-2))^{\frac{q-1}{2}} = -1 \\
&\iff P(2)P(-2) \text{ n'est pas un carré dans } \mathbb{F}_q,
\end{aligned}$$

ce qui achève la démonstration du théorème.

Théorème 1.2.21 *[25, p.46] Soit $P = \sum_{i=0}^{n-1} c_i x^i + x^n$ un polynôme irréductible sur $\mathbb{F}_q$ et $b \in \mathbb{F}_q$. Soit p la caractéristique de $\mathbb{F}_q$. Alors sont équivalents :*

- *(i) $P(x^p - x - b)$ est irréductible sur $\mathbb{F}_q$*
- *(ii) $Tr_{\mathbb{F}_q/\mathbb{F}_p}(nb - c_{n-1}) \neq 0$*

Preuve :

En appliquant le théorème 1.2.14, $P(x^p - x - b)$ est irréductible sur $\mathbb{F}_q$ si et seulement si $x^p - x - b - a$ est irréductible sur $\mathbb{F}_{q^n}$ pour une racine a de P. Mais alors, d'après le théorème 1.2.12, ceci est équivalent à ce que la trace de $a + b$ sur $\mathbb{F}_p$ soit non nulle. On conclut alors par transitivité de la trace.

Ceci fournit quelques critères d'irréductibilité.

1.2.3 Construction récursive

En se servant des critères d'irréductibilité établis dans le paragraphe précédent, il s'agit à présent de donner quelques méthodes pour construire récursivement des polynômes irréductibles de degré arbitrairement élevé. Bien entendu, ces méthodes sont assez limitées dans la mesure où elles ne permettent que de construire des familles précises. Elles ne fournissent pas de technique générale pour construire un polynôme irréductible de degré donné. Néanmoins, elles sont tout de même intéressantes puisqu'on obtient ainsi facilement des polynômes irréductibles de degré arbitrairement élevé.

Théorème 1.2.22 *[25, p.49-50] Soit p premier et $f(x) = x^n + \sum_{i=0}^{n-1} c_i x^i$ un polynôme irréductible sur $\mathbb{F}_p$. Supposons qu'il existe $a \in \mathbb{F}_p^\star$ tel que $(na + c_{n-1})f'(a) \neq 0$. On pose alors :*

$$\begin{aligned} g(x) &= x^p - x + a \\ f_0(x) &= f(g(x)) \\ f_k(x) &= f_{k-1}^\star(g(x)) \text{ pour } k \geq 1 \end{aligned}$$

Alors pour tout $k \geq 0$, f_k est irréductible sur $\mathbb{F}_p$, de degré np^{k+1}.

Preuve :

L'idée est de démontrer le résultat par récurrence sur k en utilisant le théorème 1.2.21. Par conséquent, on démontre par récurrence sur k que le coefficient du terme en x dans f_k est non nul, que $f_k'(a) \neq 0$, que f_k est irréductible sur $\mathbb{F}_p$ de degré np^{k+1}. On note $[x]f_k(x)$ le coefficient du terme x dans f_k.

- Cas $k = 0$

  D'après le théorème 1.2.21, on sait que f_0 est irréductible sur $\mathbb{F}_p$ si et seulement si $Tr_{\mathbb{F}_p/\mathbb{F}_p}(na + c_{n-1}) \neq 0$. C'est-à-dire si et seulement si $na + c_{n-1} \neq 0$; ce qui est le cas par hypothèse. Ainsi, f_0 est irréductible sur $\mathbb{F}_p$, de degré np. Par ailleurs,

$$\begin{aligned} [x]f_0(x) &= [\frac{d}{dx} f_0(x)]_{x=0} \\ &= [\frac{d}{dx}\left(\sum_{i=0}^{n} c_i g(x)^i\right)]_{x=0} \\ &= \sum_{i=0}^{n} i c_i g'(0) g(0)^{i-1} \\ &= -\sum_{i=0}^{n} i c_i a^{i-1} \\ &= -f'(a) \end{aligned}$$

  Ce qui montre bien que ce coefficient est non nul. De manière identique, on trouve $f_0'(a) = f'(a)$ qui est de nouveau non nul par hypothèse. Ceci montre que la propriété est vraie au rang 0.

- Passage de k à $k+1$

  Supposons à présent que f_k est irréductible sur $\mathbb{F}_p$ de degré np^{k+1}, que son coefficient en x, $[x]f_k(x) \neq 0$ et que $f_k'(a) \neq 0$. Montrons alors que la propriété est vraie au rang $k+1$.

  f_k est irréductible, en particulier 0 n'est pas une racine de f_k. Par suite, le polynôme $f_k^\star$ est irréductible (d'après le théorème 1.2.14) de degré np^{k+1}. Si on transforme $f_k^\star$ en un polynôme unitaire, alors son coefficient du terme en $x^{np^{k+1}-1}$ vaut $\frac{[x]f_k(x)}{f_k(0)}$. Il est donc non nul par hypothèse de récurrence. On en déduit alors en appliquant de nouveau le théorème 1.2.21 que f_{k+1} est irréductible sur $\mathbb{F}_p$ (puisque $Tr_{\mathbb{F}_p/\mathbb{F}_p}(np^{k+1}a + \frac{[x]f_k(x)}{f_k(0)}) = \frac{[x]f_k(x)}{f_k(0)} \neq 0$), de degré np^{k+2}.

Maintenant, si $f_k(x) = \sum_{i=0}^{n_k} u_i x^i$ (où $n_k = np^{k+1}$) alors on a :

$$f_{k+1} = \sum_{i=0}^{n_k} u_i g(x)^{n_k - i}$$

Ce qui conduit à :

$$\begin{aligned} f'_{k+1}(x) &= \sum_{i=0}^{n_k} (n_k - i) u_i g'(x) g(x)^{n_k - i - 1} \\ &= -\sum_{i=0}^{n_k} (n_k - i) u_i g(x)^{n_k - i - 1} \end{aligned}$$

Mais comme g est constant sur $\mathbb{F}_p$, il en est de même pour f_k et f'_k. Par conséquent,

$$[x] f_{k+1}(x) = f'_{k+1}(0) = a^{n_k - 2} f'_k(a^{-1}) = a^{n_k - 2} f'_k(a)$$

Il est donc non nul par hypothèse de récurrence. De manière identique, $f'_{k+1}(a) = a^{n_k - 2} f'_k(a) \neq 0$.

La propriété est donc vraie au rang $k+1$.

On a donc montré par récurrence que f_k est irréductible sur $\mathbb{F}_p$ et le théorème est entièrement démontré.

Dans le cas particulier où $p = 2$ et $q = 2^m$ (cas particulièrement intéressant en cryptographie), on a la construction récursive suivante fondée sur le thèorème 1.2.19.

Théorème 1.2.23 *[25, p.51] Soit $f(x) = \sum_{i=0}^{n} c_i x^i$ un polynôme irréductible sur $\mathbb{F}_q$ de degré n. On suppose que les deux propriétés suivantes sont vérifiées :*

$$\begin{aligned} Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_1}{c_0}) &\neq 0 \\ Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_{n-1}}{c_n}) &\neq 0 \end{aligned}$$

On définit alors les polynômes a_k et b_k récursivement comme suit :

$$\begin{aligned} a_0(x) &= x \\ b_0(x) &= 1 \\ a_{k+1}(x) &= a_k(x) b_k(x) \text{ pour } k \geq 0 \\ b_{k+1}(x) &= a_k^2(x) + b_k^2(x) \text{ pour } k \geq 0 \\ f_k(x) &= (b_k(x))^n f(\frac{a_k(x)}{b_k(x)}) \text{ pour } k \geq 0 \end{aligned}$$

Alors pour tout $k \geq 0$, f_k est irréductible sur $\mathbb{F}_q$ de degré $2^k n$.

Preuve :

On constate pour commencer que pour tout $k \geq 0$, $\frac{a_{k+1}(x)}{b_{k+1}(x)} = \frac{\frac{a_k(x)}{b_k(x)}}{1+\left(\frac{a_k(x)}{b_k(x)}\right)^2}$. On en déduit alors facilement par récurrence sur $k \geq 0$ que :

$$\frac{a_k(\frac{x}{1+x^2})}{b_k(\frac{x}{1+x^2})} = \frac{\frac{a_k(x)}{b_k(x)}}{1+\left(\frac{a_k(x)}{b_k(x)}\right)^2}$$

Posons $y = \frac{x}{1+x^2}$ et $c_k(x) = \frac{b_{k+1}(x)}{b_k(y)}$ pour $k \geq 0$. Montrons alors que $\forall k \geq 0$, $c_{k+1} = c_k^2$. Soit $k \geq 0$. On a alors :

$$\begin{aligned}
c_{k+1}(x) &= \frac{b_{k+2}(x)}{b_{k+1}(y)} \\
&= \frac{a_{k+1}(x)^2 + b_{k+1}(x)^2}{b_{k+1}(y)} \\
&= \frac{b_{k+1}(x)^2}{b_{k+1}(y)}\left(1+\frac{a_{k+1}(x)}{b_{k+1}(x)}\right)^2 \\
&= \frac{b_{k+1}(x)^2}{b_{k+1}(y)}\left(1+\frac{a_k(y)}{b_k(y)}\right)^2 \\
&= \frac{b_{k+1}(x)^2}{b_k(y)^2}\frac{(a_k(y)^2 + b_k(y)^2)}{b_{k+1}(y)} \\
&= \left(\frac{b_{k+1}(x)}{b_k(y)}\right)^2 \\
&= c_k^2(x)
\end{aligned}$$

(Ces calculs sont licites puisqu'on est en caractéristique 2). Il en découle que

$$\forall k \geq 0, b_{k+1}(x) = (1+x^2)^{2^k} b_k(\frac{x}{1+x^2})$$

Il est alors aisé de vérifier que les f_k satisfont la relation de récurrence suivante :

$$\begin{aligned}
f_0(x) &= f(x) \\
f_{k+1}(x) &= (1+x^2)^{2^k n} f_k(\frac{x}{1+x^2}) \text{ pour } k \geq 0
\end{aligned}$$

Par ailleurs, pour $k \geq 0$ fixé,

$$\begin{aligned}
f_k^\star(x+x^{-1}) &= (x+x^{-1})^{2^k n} f_k((x+x^{-1})^{-1}) \\
&= \left(\frac{1+x^2}{x}\right)^{2^k n} f_k(\frac{x}{1+x^2}) \\
&= x^{-2^k n}(1+x^2)^{2^k n} f_k(\frac{x}{1+x^2})
\end{aligned}$$

Ce qui conduit à l'expression suivante pour f_{k+1} :

$$f_{k+1}(x) = x^{2^k n} f_k^\star(x + x^{-1})$$

Posons alors $n_k = 2^k n$ et $f_k(x) = \sum_{i=0}^{n_k} c_i^{(k)} x^i$ pour $k \geq 0$. En appliquant le théorème 1.2.19 (cas (ii)), on en déduit que si f_k est irréductible sur $\mathbb{F}_q$ alors f_{k+1} est irréductible si et seulement si :

$$Tr_{\mathbb{F}_q/\mathbb{F}_2}(\frac{c_{n_k-1}^{(k)}}{c_{n_k}^{(k)}}) \quad \neq \quad 0$$

Par ailleurs, comme $c_{n_0-1}^{(0)} = c_{n-1}$ et $c_{n_0}^{(0)} = c_n$, on voit que la dernière relation est vérifiée pour $k = 0$, ce qui montre que f_1 est irréductible. Donc pour démontrer que f_k est irréductible pour $k > 1$, il suffit de démontrer que :

$$\forall k \geq 1, c_{n_k}^{(k)} = c_0 \text{ et } c_{n_k-1}^{(k)} = c_1$$

Mais pour démontrer cette dernière relation, il suffit d'observer que si M est un polynôme arbitraire de $\mathbb{F}_q[x]$, $M(x) = \sum_{i=0}^{l} m_i x^i$, alors

$$(1+x^2)^l M(\frac{x}{1+x^2}) = \sum_{i=0}^{l} m_i x^i (1+x^2)^{l-i}$$

est auto-réciproque de degré $2l$, les coefficients des termes en x et x^{2l-1} étant égaux à m_1 et le coefficient dominant valant m_0. On achève alors la preuve avec une récurrence sur k.

Corollaire 1.2.24 *[25, p.52] Soit $a \in \mathbb{F}_{2^n}$ tel que $Tr_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a) \neq 0$. Alors pour tout entier $k \geq 0$, $a_k + ab_k$ est irréductible sur $\mathbb{F}_2$ de degré 2^k.*

Preuve :
On applique le théorème précédent avec $f(x) = x + a$.

Corollaire 1.2.25 *[25, p.53] Pour tout entier $k \geq 0$, $a_k + b_k$ est irréductible sur $\mathbb{F}_2$ de degré 2^k.*

Corollaire 1.2.26 *[25, p.53] Soit $f(x) = \sum_{i=0}^{n} c_i x^i$ un polynôme irréductible unitaire de degré n à coefficients dans $\mathbb{F}_2$ tel que $c_{n-1}c_1 \neq 0$. Alors*

$$\sum_{i=0}^{n} c_i a_k(x)^i b_k(x)^{n-i}$$

est irréductible sur $\mathbb{F}_2$ de degré $2^k n$ pour tout $k \geq 0$.

Preuve :
On applique le théorème précédent, sachant que dans le cas où $q = 2$, la trace d'un élément de $\mathbb{F}_q$ sur $\mathbb{F}_2$ n'est rien d'autre que l'élément en question (on sait que c_0 est non nul puisque f est irréductible).

Chapitre 2

Théorème de Swan : applications aux trinômiaux et pentanômiaux

Dans le paragraphe précédent, on a donné des exemples de familles de polynômes irréductibles, des méthodes de construction récursive ainsi que des tests d'irréductibilité. Les polynômes irréductibles sont très importants : d'un point de vue théorique, ils déterminent les places de $\mathbb{F}_q[T]$ et donc l'arithmétique des corps de fonctions ; d'un point de vue pratique, en cryptologie, on a besoin d'une description précise des corps finis (et plus particulièrement de $\mathbb{F}_2$). C'est une des raisons pour lesquelles les polynômes ayant le moins de monômes possible sont intéressants. Mais comme on s'intéresse plus particulièrement au cas $q = 2$, les polynômes en question sont donc les trinômiaux ou les pentanômiaux.

Dans ce chapitre, on commence par présenter les résultats de R. Swan qui permettent de donner une réponse partielle quant à l'existence de trinômiaux irréductibles de degré arbitraire donné. En particulier, on montrera que lorsque $n \equiv 0[8]$, il n'existe pas de trinômial irréductible. Dans un second temps, on montrera d'abord qu'il existe une infinité de pentanômiaux irréductibles sur $\mathbb{F}_2$, puis on appliquera le théorème de Swan aux pentanômiaux pour établir qu'il existe toujours un pentanômial de degré donné ayant un nombre impair de facteurs irréductibles. Enfin, on présentera les résultats des tests informatiques : une liste de pentanômiaux irréductibles de degré $4 \leq n \leq 18000$, ce qui constitue le record actuel.

2.1 Théorème de Swan

2.1.1 Propriétés des corps de nombres p-adiques

Le théorème de Swan, que l'on verra dans le paragraphe suivant, fait appel à des objets classiques : les corps de nombres p-adique. Sans pour autant exposer

toute la théorie, on rappelle ici les propriétés basiques qui seront utilisées dans la suite.

Lemme 2.1.1 *(Lemme de Hensel) [19, p.50] [15, p.169]*

Soit K un corps complet pour la topologie induite par une valuation discrète ν , O l'anneau de valuation associé, $\mathcal{P}$ l'unique idéal maximal de O et $k = O/\mathcal{P}$. Soit de plus $f \in O[x]$ un polynôme unitaire. Supposons qu'il existe $\mathcal{G}, \mathcal{H} \in k[x]$ premiers entre eux, $\mathcal{G}$ unitaire, et tels que

$$\bar{f}(x) = \mathcal{G}(x)\mathcal{H}(x)$$

où $\bar{f}$ désigne le polynôme obtenu à partir de f en réduisant chaque coefficient modulo $\mathcal{P}$. Alors il existe $g, h \in O[x]$, g unitaire tels que :

$$\begin{aligned} f(x) &= g(x)h(x) \\ \bar{g}(x) &= \mathcal{G}(x) \\ \bar{h}(x) &= \mathcal{H}(x) \\ deg(g) &= deg(\mathcal{G}) \end{aligned}$$

Preuve :

Notons $m = \deg(f)$ et $r = \deg(\mathcal{G})$. Par définition, il existe g_0 et h_0 dans $O[x]$ tels que $\bar{g_0} = \mathcal{G}$ et $\bar{h_0} = \mathcal{H}$. De plus, comme $\mathcal{G}$ est unitaire, on peut choisir g_0 unitaire de degré r et h_0 de degré plus petit ou égal à celui de $\mathcal{H}$, c'est-à-dire $\deg(h_0) \leq m - r$.

Soit π une uniformisante de K. Nous allons chercher les polynômes g et h sous la forme :

$$\begin{aligned} g &= g_0 + \sum_{i=1}^{\infty} \pi^i y_i \\ h &= h_0 + \sum_{i=1}^{\infty} \pi^i z_i \end{aligned}$$

où pour tout entier $i \geq 1$, $y_i, z_i \in O[x]$, vérifiant $\deg(y_i) < r$ et $\deg(z_i) \leq m - r$ sont à déterminer.

En posant $g_n = g_0 + \sum_{i=1}^{n} \pi^i y_i$ et $h_n = h_0 + \sum_{i=1}^{n} \pi^i z_i$, nous allons démontrer par récurrence sur n que l'on peut choisir y_i et z_i satisfaisant les conditions précédentes sur le degré, de façon à ce que :

$$f \equiv f_n g_n \bmod \mathcal{P}^{n+1}$$

- Pour $n = 0$, c'est vrai d'après ce qui précède (par choix de g_0 et h_0).
- Supposons la propriété vraie jusqu'au rang $n-1$. Comme $g_n = g_{n-1} + \pi^n y_n$ et $h_n = h_{n-1} + \pi^n z_n$, il faut et il suffit de montrer que l'on peut trouver y_n et z_n de degré inférieur strict à r et inférieur ou égal à $m-r$ respectivement et tels que :

$$f \equiv g_{n-1}h_{n-1} + \pi^n(g_{n-1}z_n + h_{n-1}y_n) \bmod \mathcal{P}^{n+1}$$

ce qui s'écrit également sous la forme $g_{n-1}z_n + h_{n-1}y_n \equiv f_n \bmod \mathcal{P}$ où $f_n = \frac{f - g_{n-1}h_{n-1}}{\pi^n} \in O[x]$ par hypothèse de récurrence. En prenant les classes modulo $\mathcal{P}$, il s'agit donc de montrer qu'il existe deux polynômes $\mathcal{Y}_n$ et $\mathcal{Z}_n$ dans $O/\mathcal{P}[x]$ tels que :

$$\mathcal{G}\mathcal{Z}_n + \mathcal{H}\mathcal{Y}_n = \mathcal{F}_n$$

où $\mathcal{F}_n = \bar{f_n}$ est de degré $\leq m$, $\deg(\mathcal{Y}_n) < r$ et $\deg(\mathcal{Z}_n) \leq m - r$.
Mais comme $\mathcal{G}$ et $\mathcal{H}$ sont premiers entre eux, il existe $\mathcal{U}, \mathcal{V}$ tels que $\mathcal{U}\mathcal{G} + \mathcal{V}\mathcal{H} = \mathcal{F}_n$. En effectuant la division euclidienne de $\mathcal{V}$ par $\mathcal{G}$, on a que $\mathcal{V} = \mathcal{Q}\mathcal{G} + \mathcal{R}$. On obtient ainsi le résultat en posant $\mathcal{Y}_n = \mathcal{R}$ et $\mathcal{Z}_n = \mathcal{U} + \mathcal{Q}\mathcal{H}$.
Ce qui achève la démonstration.

Corollaire 2.1.2 *Sous les hypothèses du lemme de Hensel, supposons que $\bar{f}$ soit séparable et possède une racine α. Alors f a une racine $\beta \in O$, telle que $\bar{\beta} = \alpha$.*

La séparabilité nous assure d'une factorisation $\bar{f} = (X - \alpha)g$ avec g premier à $(X - \alpha)$. On peut alors appliquer le lemme de Hensel. Sans cette hypothèse, on ne peut pas conclure à l'existence d'une racine pour f, comme le montre l'exemple suivant : $f(x) = x^2 + 1$ avec $O = \mathbb{Z}_2$. f n'a pas de racines dans $\mathbb{Z}_2$ alors que $\bar{f} = (x - 1)^2$.

Pour la démonstration des résultats de Swan, on aura besoin d'une description précise des extensions non ramifiées : c'est l'objet des résultats qui suivent.

Soit K un corps complet pour une valuation discrète et L une extension finie de K. On note O_L (respectivement O_K) l'anneau de valuation de L (respectivement K) , $\mathcal{P}_L$ (respectivement $\mathcal{P}_K$) son unique idéal maximal, $k(L)$ (respectivement $k(K)$) le corps résiduel de L (resp. de K) (i.e. $k(L) = O_L/\mathcal{P}_L$), e l'indice de ramification de L/K et f le degré résiduel.

Il s'agit à présent de donner une description des extensions non ramifiées en terme de corps de racines d'un polynôme :

Proposition 2.1.3 *[2, p.25]*

- *(i) Supposons L/K non ramifiée. Alors il existe un élément $x \in O_L$ tel que $k(L) = k(K)(\bar{x})$. De plus, si g désigne le polynôme minimal de x sur K, alors $O_L = O_K(x)$, $L = K(x)$, et $\bar{g}$ est irréductible dans $k(K)[X]$ et séparable.*
- *(ii) Soit g un polynôme unitaire à coefficients dans O_K tel que $\bar{g}$ est irréductible dans $k(K)[X]$ et séparable. Si x est une racine de g alors $L = K(x)$ est non ramifiée sur K et $k(L) = k(K)(\bar{x})$.*

Preuve :

- (i) Par définition de la non ramification, on a donc $e = 1$ et $k(L)/k(K)$ séparable. D'après le théorème de l'élément primitif, il existe $x \in O_L$ tel que $k(L) = k(K)(\bar{x})$. Pour un tel x, le polynôme minimal G de $\bar{x}$ est

irréductible sur $k(K)$ et séparable. De plus,

$$\begin{aligned}
[L:K] &\geq [K(x):K] \\
&\geq \deg g \text{ (car } g \text{ est irréductible)} \\
&\geq \deg G \text{ (car } G \text{ divise } \bar{g} \text{ et } \deg g = \deg \bar{g}) \\
&\geq [k(L):k(K)] \text{ (car } G \text{ est irréductible)} \\
&\geq [L:K] \text{ (car } L/K \text{ est non ramifiée)}
\end{aligned}$$

On conclut alors que $\bar{g} = G$, et donc que $\bar{g}$ est irréductible et séparable.

- (ii) Déjà, puisque $\bar{g}$ est irréductible, il s'ensuit que g est irréductible sur K. Par ailleurs, de la même façon que pour (i), on a :

$$\begin{aligned}
[L:K] &= \deg g \text{ (car } g \text{ est irréductible)} \\
&= \deg \bar{g} \text{ (puisque } g \text{ est unitaire)} \\
&= [k(K)(\bar{x}):k(K)] \text{ (puisque } \bar{g} \text{ est irréductible)} \\
&\leq [k(L):k(K)] \\
&\leq [L:K]
\end{aligned}$$

Par conséquent, $f = [L:K]$, i.e $e = 1$ et $k(L) = k(K)(\bar{x})$, c'est-à-dire $k(L)/k(K)$ séparable

Ce qui achève la démonstration de la proposition.

Théorème 2.1.4 *[2, p.26]*

Soit $\bar{k}$ une extension finie séparable de $k(K)$. Alors il existe un corps $L = L(\bar{k})$ tel que :

- *(i) L/K est finie séparable*
- *(ii) $\bar{k} \simeq k(L)$ ($k(K)$-isomorphisme)*
- *(iii) L/K est non ramifiée*
- *(iv) Les morphismes $Hom_K(L, L') \longrightarrow Hom_{k(K)}(k(L), k(L'))$ sont bijectifs pour tout L' contenant K*

De plus, les propriétés (i) et (ii) déterminent L de manière unique (à K-isomorphisme près).

Preuve :

D'après le théorème de l'élément primitif, $\bar{k} = k(K)(y)$ où $y \in \bar{k}$ est séparable sur $k(K)$. Soit G le polynôme minimal de y sur $k(K)$. Soit $g \in k(K)[X]$, unitaire tel que $\bar{g} = G$. Posons $L = K(x)$, où x est une racine de g. D'après la proposition précédente, L vérifie les propriétés $(i), (ii)$ et (iii). Montrons alors que L vérifie la propriété (iv).

Soit $w \in Hom_{k(K)}(k(L), k(L'))$. Alors $w(\bar{x})$ est une racine de $\bar{g}$ dans L'. En appliquant le lemme de Hensel, on en déduit que g a une racine y dans L' telle que $\bar{y} = w(\bar{x})$. De plus, comme $\bar{g}$ est séparable, on en déduit que l'élément y est unique. Mais alors il existe un unique morphisme $\sigma \in Hom_K(L, L')$ tel que $\sigma(x) = y$. Par construction, $\bar{\sigma} = w$. Ce qui montre la surjectivité.

Maintenant, si $\tau \in Hom_K(L, L')$ vérifie $\bar{\tau} = w$. Alors $\tau(x)$ est une racine de g vérifiant $\tau(x) = \bar{\tau}(\bar{x}) = w(\bar{x})$. Par unicité, $\tau(x) = y$ et donc $\tau = \sigma$, ce qui montre l'injectivité du morphisme en question.

Par conséquent, L' vérifie (iv).

Maintenant, si L' est non ramifiée sur K et w est un $k(K)$-isomorphisme de $k(L)$ sur $k(L')$. Alors, L et L' ont la même dimension en tant que K-espace vectoriel. Ce qui montre en appliquant (iv) que le relèvement σ de w à L est en fait un isomorphisme. Ainsi $L \simeq L'$. Ceci montre que les propriétés (i) et (ii) déterminent L de manière unique à K-isomorphisme près, et le théorème est entièrement démontré.

Grâce à ce théorème, on peut alors caractériser les sous-extensions de L non ramifiées sur K. En effet,

Théorème 2.1.5 *[2, p.27] Soit L/K une extension finie. On note $k(L)^s$ la clôture séparable de $k(K)$ dans $k(L)$ (dans le cas où L et K sont des extensions finies de $\mathbb{Q}_p$ la clôture séparable n'est rien d'autre que $k(L)$). Alors L a un sous-corps L_0 tel que pour tout $K \subset F \subset L$:*

$$F/K \text{ est non ramifiée} \iff F \subset L_0$$

De plus, $k(L_0) = k(L)^s$.

Preuve :

L'existence de L_0 découle du théorème précédent avec $k(L_0) = k(L)^s$. Par définition de la ramification, il est alors clair que tout sous-corps de L_0 est non ramifié sur K. Il s'agit donc de démontrer la réciproque.

Soit L' un sous-corps de L contenant K tel que L'/K soit non ramifiée. Alors, par définition de la non ramification, $k(L')/k(K)$ et séparable. Par conséquent, $k(L') \subset k(L)^s = k(L_0)$.

En appliquant alors le théorème précédent à $\bar{k} = k(L')$, on en déduit l'existence de $\sigma \in Hom_K(L', L_0)$ tel que $\bar{\sigma}$ soit l'inclusion. En appliquant alors le théorème de l'élément primitif à $k(L')$, on a $k(L') = k(K)(\bar{x})$ pour $x \in L'$. Mais dans ce cas, $\bar{x} = \bar{\sigma(x)}$. Si g désigne le polynôme minimal de x sur K, alors x et $\sigma(x)$ sont des racines de g. Comme $\bar{g}$ est séparable, on en déduit alors que $x = \sigma(x)$. En appliquant alors la proposition 2.1.3 à g, on conclut que $L' = K[x]$ et donc $L' \subset L_0$. Ce qui démontre la réciproque et achève la preuve du théorème.

Corollaire 2.1.6 *[2, p.28] Si L et L' sont deux extensions finies de K non ramifiées, alors $L.L'$ (compositum de L et L') est non ramifié sur K.*

Proposition 2.1.7 *Supposons que L/K soit galoisienne. Alors on a un morphisme de groupes :*

$$\begin{array}{rccc} \phi : & Gal(L/K) & \longrightarrow & Gal(k(L)/k(K)) \\ & \sigma & \longmapsto & \bar{\sigma} \end{array}$$

où $\bar{\sigma} : x + \mathcal{P}_L \longmapsto \sigma(x) + \mathcal{P}_L$.
De plus, ϕ est surjectif et si on note $I = I(L/K)$ (groupe d'inertie de L/K) le noyau de ϕ, alors I est de cardinal e et L^I/K est l'extension maximale incluse dans L non ramifiée.

Preuve :

Le fait que ϕ soit bien défini découle du fait qu'il existe une unique valuation ν_L sur L prolongeant celle de K. Par conséquent, si $\sigma \in Gal(L/K)$, $\nu_L \sigma = \nu_L$. Montrons que ϕ est surjectif.

Soit $w \in Gal(k(L)/k(K))$. Il existe $x \in L$, $k(L) = k(K)(\bar{x})$. Soit g le polynôme minimal de x sur K. Par la même argumentation que précédemment, il existe un unique élément y de L tel que y soit une racine de g et $\bar{y} = w(\bar{x})$. On en déduit alors qu'il existe un unique $\tau \in Hom_K(K(x), L)$ tel que $\tau(x) = y$. Maintenant, comme $L/K(x)$ est séparable, il existe $\sigma \in Hom(L, \bar{K})$ tel que $\sigma_{|K(x)} = \tau$. Mais comme L/K est normale, $\sigma \in Gal(L/K)$ et par construction $\phi(\sigma) = w$.

Le fait que L^I/K soit l'extension maximale incluse dans L non ramifiée découle alors du théorème 2.1.5, de $k(L^I) = k(L) = k(L)^s$ et de la transitivité de l'indice de ramification.

On s'intéresse à présent au cas où L et K sont des extensions finies de $\mathbb{Q}_p$. On peut alors décrire explicitement les extensions non ramifiées.

Théorème 2.1.8 *[43, p.323] Soient L et K deux extensions finies de $\mathbb{Q}_p$ telles que L/K soit non ramifiée. Alors :*

- *(a) L/K est galoisienne et $Gal(L/K)$ est cyclique.*
- *(b) $L = K(\xi_n)$ pour un entier n avec $p \not| n$.*

De plus, si K est donné et $m \geq 1$ fixé, il existe une unique extension L de K de degré m, non ramifiée. Cette extension est alors cyclique de degré m.

Preuve :

Supposons pour commencer que L/K soit galoisienne. Alors d'après la proposition 2.1.7,

$$Gal(L/K) \simeq Gal(k(L)/k(K))$$

Mais comme le membre de droite est le groupe de Galois d'une extension finie de corps finis, il est cyclique.

Maintenant, si L/K est quelconque. Soit M la clôture normale de L. Alors M/K est galoisienne finie. Soit M_0 l'extension maximale de K, incluse dans M et non ramifiée. Alors $L \subset M_0$. D'après les théorèmes précédents, si I désigne le groupe d'inertie de M/K, alors $M_0 = M^I$. De plus, comme I est un sous-groupe distingué de $Gal(M/K)$ (en tant que noyau d'un morphisme de groupes), M_0/K est galoisienne. D'après le cas galoisien, on en déduit que M_0/K est cyclique. Mais ceci entraîne que $Gal(M_0/L)$ est distingué dans $Gal(M_0/K)$ et donc par le théorème de correspondance de Galois, que L/K est galoisienne. Ceci démontre donc le point (a).

Pour (b), soit y un élément primitif de $k(L)/k(K)$. Alors y est une racine n-ième de l'unité, pour un entier n premier à p. Mais alors, le polynôme $X^n - 1$ a une racine dans $k(L)$. Donc, d'après le lemme de Hensel, il a une racine x dans L (puisque p ne divise pas n). Cette racine x engendre L sur K (conséquence de l'isomorphisme des groupes de Galois).

Enfin, soit ξ_n avec $p \not| n$ tel que $\bar{\xi_n}$ engendre une extension de degré m de $k(K)$. Alors $K(\xi_n)/K$ est non ramifiée (il suffit d'appliquer la proposition 2.1.3 à un relèvement du polynôme minimal de ξ_n dans O_K). L'isomorphisme des groupes de Galois démontre alors que $K(\xi_n)/K$ est cyclique de degré m. Par ailleurs, si L/K et L'/K sont deux extensions de degré m non ramifiées, alors leur compositum est encore non ramifié (corollaire 2.1.6), donc cyclique d'après

(a). Or $Gal(LL'/K)$ s'injecte dans $Gal(L/K) \times Gal(L'/K)$. Ce qui montre que tout élément de $Gal(LL'/K)$ est d'ordre divisant m. On conclut alors en regardant les degrés, que $L = L'$.

Ceci achève la démonstration du théorème.

2.1.2 Théorème de Swan

Théorème 2.1.9 *[40] Soit f un polynôme unitaire de degré n, à coefficients entiers dans un corps de nombres $\mathcal{P}$-adique F. Supposons que la réduction $\bar{f}$ de f modulo $\mathcal{P}$ soit séparable. Soit également r le nombre de facteurs irréductibles de $\bar{f}$ dans le corps résiduel. Alors $r \equiv n$ [2] si et seulement si $D(f)$ est un carré dans F.*

Preuve :

Soit K le corps résiduel de F. Alors on peut écrire $\bar{f} = \prod_{i=1}^{r} g_i$. Comme $\bar{f}$ est séparable, les g_i sont distincts. On en déduit donc par le lemme de Hensel qu'il existe $f_1, \ldots, f_r$,à coefficients dans F tels que

$$\forall i \in \{1, \ldots, r\}, \bar{f_i} = g_i$$
$$f = \prod_{i=1}^{r} f_i$$

Par ailleurs, puisque les g_i sont irréductibles (et séparables), il en est de même pour les f_i. Ainsi, en désignant par E_i le corps de rupture de f_i, on en déduit que E_i est non ramifié sur F (d'après la proposition 2.1.3). Mais on a vu qu'il existe une unique extension non ramifiée de F de degré donné et que cette extension est cyclique et donc E_i est cyclique, a fortiori galoisienne et donc finalement, E_i est le corps de décomposition de f_i.

Maintenant, si E désigne le corps de décomposition de f sur F, alors E est le compositum des E_i, donc est non ramifié sur F (puisque chaque E_i l'est). On conclut alors de même que précédemment que E est cyclique. Soit donc σ un générateur de $Gal(E/F)$. Maintenant, pour $j \in \{1, \ldots, r\}$ fixé, soit β_j une racine de f_j. Alors les racines de f_j sont les $\sigma^i(\beta_j)$,$0 \leq i \leq n_j - 1$ où n_j est le degré de f_j. En effet, ce sont clairement des racines de f_j et de plus, on a $Gal(E_j/F) \simeq \frac{Gal(E/F)}{Gal(E/E_j)}$, par suite si $\bar{\sigma}$ désigne la classe de σ modulo $Gal(E/E_j)$, c'est un générateur de $Gal(E_j/F)$, ce qui montre que les $\sigma^i(\beta_j)$,$0 \leq i \leq n_j - 1$ sont bien distincts.

Ainsi, les racines de f sont les $\sigma^i(\beta_j)$, $0 \leq j \leq r, 0 \leq i \leq n_j - 1$. On ordonne alors ces racines par $(i_1, j_1) < (i_2, j_2)$ si $j_1 < j_2$ ou $j_1 = j_2$ et $i_1 < i_2$ (où pour tout entier i, le symbole (i, j) désigne le couple (i', j) où $i' \equiv i$ $[n_j]$ et $0 \leq i' < n_j$). Maintenant, on a $D(f) = \delta(f)^2$ où

$$\delta(f) = \prod_{(i_1,j_1)<(i_2,j_2)} (\sigma^{i_1}(\beta_{j_1}) - \sigma^{i_2}(\beta_{j_2}))$$

Si on applique σ a $\delta(f)$, on obtient alors :

$$\sigma(\delta(f)) = \prod_{(i_1,j_1)<(i_2,j_2)} (\sigma^{i_1+1}(\beta_{j_1}) - \sigma^{i_2+1}(\beta_{j_2}))$$

On observe alors que les termes qui apparaissent dans cette expression sont les mêmes que ceux qui apparaissent dans $\delta(f)$, au signe près. En fait, $\sigma^{i_1}(\beta_{j_1}) - \sigma^{i_2}(\beta_{j_2})$ apparait dans $\delta(f)$ et $\sigma(\delta(f))$ avec le même signe si et seulement si $(i_1+1, j_1) < (i_2+1, j_2)$. Ceci est certainement vrai si $j_1 < j_2$ ou si $j_1 = j_2 = j$ et $i_2 < n_j - 1$. En revanche, si $j_1 = j_2 = j$ et $i_2 = n_j - 1$, alors $(i_2+1, j) = (0, j) < (i_1+1, j)$, $0 \leq i_1 \leq n_j - 2$. Ceci montre que $(i_1+1, j_1) < (i_2+1, j_2)$ si et seulement si $j_1 < j_2$ ou $j_1 = j_2 = j$ et $i_2 < n_j - 1$. Par conséquent, le nombre de termes qui apparaissent dans $\delta(f)$ et $\sigma(\delta(f))$ avec un signe opposé est égal au nombre de paires $((i_1, j), (n_j - 1, j))$ avec $0 \leq i_1 \leq n_j - 2$. Or a j fixé, il y a exactement $n_j - 1$ telles paires. Ainsi, le nombre total de termes qui apparaissent dans $\delta(f)$ et $\sigma(\delta(f))$ avec un signe opposé est égal à $\sum_{j=1}^{r}(n_j - 1) = n - r$. Ainsi, on a :

$$\sigma(\delta(f)) = (-1)^{n-r}\delta(f)$$

On en déduit donc les équivalences suivantes :

$$\begin{aligned} D(f) \text{ est un carré dans } F &\iff \delta(f) \in F \\ &\iff \sigma(\delta(f)) = \delta(f) \\ &\iff n \equiv r \ [2] \end{aligned}$$

Ce qui achève la démonstration du théorème.

Corollaire 2.1.10 *[40] Soient K un corps fini de caractéristique impaire, $g \in K[X]$ séparable de degré n et r le nombre de facteurs irréductibles de g dans K. Alors $r \equiv n \ mod\ 2$ si et seulement si $D(g)$ est un carré dans K.*

Preuve :

Quitte à diviser g par son coefficient dominant (ce qui ne modifie pas le nombre de facteurs irréductibles de g dans $K[X]$), on peut supposer que g est unitaire. Soit $p = Car(K) \geq 3$ et F un corps de nombres p-adique, de corps résiduel K. Soit par ailleurs $f \in F[X]$ unitaire, à coefficients entiers tels que $\bar{f} = g$ (où $\bar{f}$ désigne la classe de f modulo l'unique idéal maximal $\mathcal{P}$ de O_F). Alors $D(g) = D(\bar{f}) \bmod \mathcal{P}$.

D'après le théorème précédent, $r \equiv n \bmod 2$ si et seulement si $D(f)$ est un carré dans F.

Maintenant, il est clair que si $D(f)$ est un carré dans F alors $D(g)$ est un carré dans K. Réciproquement, supposons que $D(g)$ soit un carré dans F et considérons le polynôme $P = X^2 - D(f)$. Alors la réduction de P modulo $\mathcal{P}$ est $\bar{P} = X^2 - D(g)$. Mais puisque $D(g)$ est un carré dans K, $\bar{P} = (X-a)(X-b)$ avec $a, b \in K$. Par ailleurs, puisque $p \neq 2$, $\bar{P}$ est séparable, c'est-à-dire $a \neq b$. Par suite, $X - a$ et $X - b$ sont premiers entre eux et on peut appliquer le lemme

de Hensel, ce qui permet de conclure que P a une racine dans F. Ce qui montre que $D(f)$ est un carré dans F si et seulement si $D(g)$ est un carré dans K. Ce qui conclut la démonstration du corollaire.

Remarque 2.1.11 *Si $Car(K) = 2$, le dernier corollaire n'est plus valable. En effet, dans la démonstration du corollaire, un argument clé est que $D(f)$ est un carré dans F si et seulement si $D(g)$ est un carré dans K. Mais pour appliquer le lemme de Hensel comme dans la preuve du corollaire, il est nécessaire que $X^2 - D(g)$ soit séparable, ce qui n'est plus le cas lorsque $p = 2$.*

On cherche alors à s'affranchir de la condition $car(K) \neq 2$. On a alors besoin du lemme suivant :

Lemme 2.1.12 *[40] Soit a un entier $\mathcal{P}$-adique, premier à $\mathcal{P}$. Alors sont équivalents :*

- *(i) a est un carré $\mathcal{P}$-adique*
- *(ii) a est un carré mod $4\mathcal{P}$*

Preuve :

L'implication $(i) \Rightarrow (ii)$ est claire. Montrons la réciproque.

On suppose que a est un carré mod $4\mathcal{P}$. Montrons alors par récurrence sur n que a est un carré mod $4\mathcal{P}^n$

- $n = 1$
  C'est l'hypothèse (ii) et donc la propriété est vraie au rang 1.
- Passage de n à $n+1$
  On suppose la propriété vraie au rang n. Alors il existe un entier $\mathcal{P}$-adique b_n tel que $a \equiv b_n^2 \bmod 4\mathcal{P}^n$. Il existe alors un entier $\mathcal{P}$-adique c_n avec $c_n \in \mathcal{P}^n$ tel que $a = b_n^2 + 4c_n$. Mais puisque a est premier à $\mathcal{P}$, il en est de même pour b_n. Par conséquent, b_n est inversible. Posons alors $d_n = b_n^{-1}c_n$ et $b_{n+1} = b_n + 2d_n$. On a alors $a = b_n^2 + 4b_nd_n = (b_n + 2d_n)^2 - 4d_n^2 = b_{n+1}^2 - 4d_n^2$. Or, $d_n \equiv 0 \bmod \mathcal{P}^n$ (puisque $c_n \equiv 0 \bmod \mathcal{P}^n$ et b_n est premier à $\mathcal{P}$), donc $a \equiv b_{n+1}^2 \bmod 4\mathcal{P}^{n+1}$ (en fait modulo $4\mathcal{P}^{2n}$).
  La propriété est donc vraie au rang $n+1$

Ce qui montre par récurrence que $\forall n \geq 1, \exists b_n, a \equiv b_n^2 \bmod 4\mathcal{P}^n$.

Mais alors, pour tout entiers n et p, $(b_{n+p} - b_n) \in \mathcal{P}^n$, ce qui montre que (b_n) est une suite de Cauchy puisque les $(\mathcal{P}^n)$ forment une base de voisinage de 0, donc convergente. Soit b sa limite.

Soit $n \geq 1$ alors il existe n_0 tel que $\forall i \geq n_0, b_i^2 - b^2 \in \mathcal{P}^n$. On a alors $a - b^2 = (a - b_{n_0}^2) + (b_{n_0}^2 - b^2) \in \mathcal{P}^n$.

Ainsi, $(a - b^2) \in \cap_{n \geq 1}\mathcal{P}^n$, d'où $a = b^2$.

Ce qui démontre la réciproque et donc le lemme est entièrement démontré.

Corollaire 2.1.13 *Soit f un polynôme unitaire de degré n à coefficients entiers dans un corps de nombres $\mathcal{P}$-adique F. Supposons que $\bar{f}$ soit séparable. Soit alors r le nombre de facteurs irréductibles de $\bar{f}$ dans $K[X]$, K désignant le corps résiduel de F. Alors $r \equiv n$ [2] si et seulement si $D(f)$ est un carré modulo $4\mathcal{P}$.*

Preuve :

D'après le théorème, $r \equiv n$ [2] si et seulement si $D(f)$ est un carré dans F. Mais comme $D(f)$ est entier, on peut appliquer le lemme précédent, ce qui démontre le corollaire.

Corollaire 2.1.14 *[40] Soit $g \in \mathbb{F}_2[X]$ séparable de degré n et r le nombre de facteurs irréductibles de g sur $\mathbb{F}_2[X]$. Soit par ailleurs $f \in \mathbb{Z}_2[X]$ unitaire de degré n tel que $\bar{f} = g$. Alors $r \equiv n$ [2] si et seulement si $D(f) \equiv 1$ [8].*

Preuve :

Ceci découle du corollaire précédent et du fait que 1 est le seul carré impair modulo 8.

Exemple 2 *[40]* Soit $f \in \mathbb{F}_{2^n}[X]$ de degré k et tel que $f(0) \neq 0$. Soit g le polynôme défini par $g(x) = f(x)^8 + x^m$, où m est un entier impair. Posons $q = \deg g = \max(8k, m)$ (il y a bien égalité puisque m est impair donc ne peut valoir $8k$). Soit également E un corps de nombres p-adique de corps résiduel $\mathbb{F}_{2^n}$ et $F \in E[X]$ de degré k tel que $\bar{F} = f$. Alors $g = \bar{G}$ ou $G(x) = F(x)^8 + x^m$. Alors, comme $G'(x) \equiv mx^{m-1}$ [8], on a :

$$D(G) \equiv (-1)^{\frac{q(q-1)}{2}} \prod_{i=1}^{q} m\alpha_i^{m-1} \bmod 8$$

Mais $\prod \alpha_i = (-1)^q G(0) \equiv f(0)^8 \bmod \mathcal{P}$ (où $\mathcal{P}$ désigne l'unique idéal maximal de l'anneau des entiers de E). Par suite, $D(G) \not\equiv 0 \bmod \mathcal{P}$ et donc g est séparable. De plus, comme m est impair, $\prod_{i=1}^{q} \alpha_i^{m-1}$ est un carré. Ce qui montre que $D(G)$ est un carré modulo 8 si et seulement si $D' = (-1)^{\frac{q(q-1)}{2}} m^q$ est un carré.

- 1er cas : $q = 8k$
  Dans ce cas, D' est un carré, et par conséquent, $r \equiv q \equiv 0$ [2]. Ce qui montre que g a un nombre pair de facteurs irréductibles, donc est réductible.
- 2eme cas : $q = m$
  Alors $D' = (-1)^{\frac{m-1}{2}} m (-1)^{\frac{(m-1)^2}{2}} m^{m-1}$. Or $(m-1)^2 \equiv 0$ [4], ce qui montre que D' diffère d'un carré au terme $(-1)^{\frac{m-1}{2}} m$ près.
  Si $m \equiv \pm 3$ [8], alors $(-1)^{\frac{m-1}{2}} m \equiv 5$ [8], donc d'après le corollaire précédent, $r \not\equiv n \equiv 1$ [2]. Donc g est réductible.

En particulier, ceci montre que $x^{8k} + x^m + 1$ est réductible sur $\mathbb{F}_q$ si $m < 8k$ ou si $m > 8k$ et $m \equiv \pm 3$ [8].

Application 1 *[40] Loi de réciprocité quadratique.* Il s'agit ici de donner une démonstration de la loi de réciprocité quadratique, en appliquant le théorème précédent.

On rappelle que le discriminant du polynôme $x^n + a$ sur un corps quelconque K est donné par la relation :

$$D(x^n + a) = (-1)^{\frac{n(n-1)}{2}} n^n a^{n-1}$$

Considérons alors le polynôme $x^p - 1 = (x-1)Q_p(x)$, où p est un nombre premier impair. De même que dans l'exemple ci-dessus, son discriminant diffère d'un carré au terme $(-1)^{\frac{p-1}{2}} p$ près. Mais

$$\begin{aligned} (-1)^{\frac{p-1}{2}} p &\equiv 5 \ [8] \text{ si } p \equiv 3, 5 \ [8] \\ &\equiv 1 \ [8] \text{ si } p \equiv \pm 1 \ [8] \end{aligned}$$

On en déduit donc, d'après le dernier corollaire, que $x^p - 1$ a un nombre impair de facteurs irréductibles sur $\mathbb{F}_2$ si et seulement si $p \equiv \pm 1$ [8].

De la même façon, si $q \neq p$ est un nombre premier impair, alors $x^p - 1$ a un nombre impair de facteurs irréductibles sur $\mathbb{F}_q$ si et seulement si $(-1)^{\frac{p-1}{2}} p$ est un carré modulo q.

Maintenant, d'après l'étude des polynômes cyclotomiques, Q_p a exactement $\frac{\phi(p)}{\tau(p)}$, et donc $x^p - 1$ a exactement $1 + \frac{\phi(p)}{\tau(p)}$ facteurs irréductibles sur $\mathbb{F}_q$.

Par ailleurs, $\frac{\mathbb{Z}}{p\mathbb{Z}}^\star$ est cyclique de cardinal pair. Par conséquent, il possède un unique sous groupe d'indice 2, formé par les carrés modulo p. En effet, si g est un générateur de $\frac{\mathbb{Z}}{p\mathbb{Z}}^\star$, alors $< g^2 >$ est un sous-groupe d'indice 2. Si par ailleurs H est un sous-groupe d'indice 2, alors $g^2 \in H$, ce qui montre que $H =< g^2 >$. De plus, $< g^2 >$ est bien formé des carrés modulo p. Alors q est un carré modulo p si et seulement si le sous-groupe engendré par q est d'indice pair. Par ailleurs, cet indice vaut $\frac{\phi(p)}{\tau(p)}$. D'où on déduit que q est un carré modulo p si et seulement si $x^p - 1$ a un nombre impair de facteurs irréductibles sur $\mathbb{F}_q$. Ce qui conduit à

$$\begin{aligned} \left(\frac{q}{p}\right) &= \left(\frac{(-1)^{\frac{p-1}{2}} p}{q}\right) \text{ si } q \text{ est impair} \\ \left(\frac{2}{p}\right) &= 1 \text{ si et seulement si } p \equiv \pm 1 \ [8] \end{aligned}$$

Ces équations avec la formule $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ constituent la loi de réciprocité quadratique.

2.1.3 Calcul de discriminant d'un trinômial

Afin de pouvoir appliquer les résultats du paragraphe précédent, il est nécessaire de pouvoir calculer le discriminant. Dans ce paragraphe, on rappelle les propriétés élémentaires du résultant et du discriminant puis on donne une formule exacte pour le discriminant d'un trinômial.

Soit K un corps, f et g deux polynômes à coefficients dans K. Soient par ailleurs $\beta_1, \ldots, \beta_m$ les racines de g (comptées avec multiplicité) (dans une clôture algébrique fixée de K), b le coefficient dominant de g et n le degré de f.

Définition 2.1.15 *Le résultant de f et g, noté $R(f,g)$ est l'élément de K défini par :*

$$R(f,g) = b^n \prod_{i=1}^{m} f(\beta_i)$$

Remarque 2.1.16 *Il s'agit bien d'un élément de K puisque c'est une fonction symétrique des racines de g.*

Remarque 2.1.17 *Le discrimant de f, de racines $\alpha_1, \ldots, \alpha_n$ (comptées avec multiplicité) est défini par :*

$$D(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

Il s'ensuit que si f est unitaire, $D(f) = (-1)^{\frac{n(n-1)}{2}} R(f', f)$

Lemme 2.1.18 *[40]*

- *(1) $R(g,f) = (-1)^{degf.degg} R(f,g)$*
- *(2) Si $f = qg + r$, alors $R(f,g) = b^{degf - degr} R(r,g)$*
- *(3) Si a, b sont des constantes non toutes nulles, $R(a,b) = 1$*
- *(4) $R(f_1 f_2, g) = R(f_1, g) R(f_2, g)$*

Preuve :

On conserve les notations du début du paragraphe : f et g sont deux polynômes à coefficient dans K de degré n et m respectivement, de coefficient dominant a et b respectivement, de racines $\alpha_1, \ldots, \alpha_n$ et $\beta_1, \ldots, \beta_m$ respectivement .

- (1) Par définition du résultant de deux polynômes, on a :

$$\begin{aligned}
R(g,f) &= a^m \prod_{i=1}^{n} g(\alpha_i) \\
&= a^m \prod_{i=1}^{n} b \prod_{j=1}^{m} (\alpha_i - \beta_j) \\
&= b^n \prod_{j=1}^{m} a \prod_{i=1}^{n} (\alpha_i - \beta_j) \\
&= b^n \prod_{j=1}^{m} (-1)^n a \prod_{i=1}^{n} (\beta_j - \alpha_i) \\
&= b^n \prod_{j=1}^{m} (-1)^n f(\beta_j) \\
&= (-1)^{nm} R(f,g)
\end{aligned}$$

ce qui établit le point (1)

– (2) On suppose que $f = qg + r$, on a alors :

$$\begin{aligned} R(f,g) &= b^n \prod_{j=1}^{m} f(\beta_j) \\ &= b^n \prod_{j=1}^{m} (q(\beta_j)g(\beta_j) + r(\beta_j)) \\ &= b^n \prod_{j=1}^{m} r(\beta_j) \\ &= b^{\deg f - \deg r} R(r,g) \end{aligned}$$

ce qui établit le point (2)
– (3) est clair
– (4) On a pour f_1, f_2 et g trois polynômes fixés :

$$\begin{aligned} R(f_1 f_2, g) &= (b)^{\deg(f_1 f_2)} \prod_{j=1}^{m} f_1(\beta_j) f_2(\beta_j) \\ &= \left(b^{\deg f_1} \prod_{j=1}^{m} f_1(\beta_j) \right) \left(b^{\deg f_2} \prod_{j=1}^{m} f_2(\beta_j) \right) \\ &= R(f_1, g) R(f_2, g) \end{aligned}$$

Ce qui achève la démonstration du lemme.

Corollaire 2.1.19 *[40]*
– *(5)* $R(f, g_1 g_2) = R(f, g_1) R(f, g_2)$
– *(6) Si a est une constante,* $R(f, a) = R(a, f) = a^{degf}$
– *(7)* $R(f, x^m) = R(f, x)^m = f(0)^m$

Preuve :
– (5) Découle de (1) et (4)
– (6) Si g est constant, il est clair par définition du résultant que $R(f,g) = g^{degf}$. De même, si f est constant non nul, deg $f = 0$, par suite $R(f,g) = f^{degg}$.
– (7) La première égalité découle de (5). Pour la seconde, $R(f,x) = f(0)$ par définition du résultant.

On peut dès à présent calculer le discriminant d'un trinômial :

Lemme 2.1.20 *[40] Soient r, s deux entiers et $d = pgcd(r,s)$. Soient de plus r_1 et s_1 les entiers définis par $r = r_1 d$ et $s = s_1 d$. Soit encore α et β deux éléments d'un corps K fixé. Alors on a :*

$$R(x^r - \alpha, x^s - \beta) = (-1)^s [\alpha^{s_1} - \beta^{r_1}]^d$$

Preuve :

Tout d'abord, on observe que si la propriété est vraie pour un couple (r,s) elle l'est également pour le couple (s,r). En effet, supposons la propriété vraie pour un couple (r,s). Alors on a :

$$\begin{aligned} R(x^s-\beta,x^r-\alpha) &= (-1)^{rs}R(x^r-\alpha,x^s-\beta) \\ &= (-1)^{rs}(-1)^s[\alpha^{s_1}-\beta^{r_1}]^d \\ &= (-1)^{rs+s+r}(-1)^r[-(\beta^{r_1}-\alpha^{s_1})]^d \\ &= (-1)^{rs+s+r+d}(-1)^r[\beta^{r_1}-\alpha^{s_1}]^d \end{aligned}$$

Mais on a $rs+s+r+d\equiv 0\ [2]$. En effet, il suffit de regarder congruences modulo 2 de r et s, ce qui donne :

- 1er cas : $r\equiv s\equiv 0\ [2]$
  Dans ce cas $d\equiv 0\ [2]$ et donc $rs+s+r+d\equiv 0\ [2]$
- 2ème cas : exactement un parmi r et s est pair
  Dans ce cas, d est impair et le produit rs est pair.
  D'où $rs+r+s+d\equiv 0+1+0+1\equiv 0\ [2]$ et le résultat
- 3ème cas : $r\equiv s\equiv 1\ [2]$
  Dans ce cas $d\equiv 1\ [2]$ et de même que précédemment,
  $rs+r+s+d\equiv 1+1+1+1\equiv 0\ [2]$

Montrons alors le résultat par récurrence sur $n=r+s$ avec $r\geq s$.

- La propriété est trivialement vraie pour $n=0$
- Supposons la propriété vraie pour $r+s\leq n$ et montrons qu'elle est vraie au rang $n+1$.
  Soient donc r et s tels que $r\geq s$ et $r+s=n+1$. On peut écrire
  $$x^r-\alpha=x^{r-s}(x^s-\beta)+\beta x^{r-s}-\alpha$$
  Mais alors on a $R(x^r-\alpha,x^s-\beta)=R(\beta x^{r-s}-\alpha,x^s-\beta)$. Si $\beta=0$, le résultat est évident. On peut donc supposer $\beta\neq 0$. Dans ce cas, on peut encore écrire :

$$\begin{aligned} R(\beta x^{r-s}-\alpha,x^s-\beta) &= R(\beta,x^s-\beta)R(x^{r-s}-\frac{\alpha}{\beta},x^s-\beta) \\ &= \beta^s R(x^{r-s}-\frac{\alpha}{\beta},x^s-\beta) \end{aligned}$$

  On remarque alors que si $s\neq 0$, on peut appliquer l'hypothèse de récurrence au couple $(r-s,s)$. Le cas $s=0$ est évident puisqu'alors on a $d=r$, $s_1=0$, $r_1=1$ et d'après les propriétés du résultant rappelées dans la section précédente, si f est un polynôme non nul et a une constante, $R(f,a)=a^{\deg f}$. On suppose donc $s\neq 0$. On en déduit que :
  $$R(x^{r-s}-\tfrac{\alpha}{\beta},x^s-\beta)=(-1)^s[(\tfrac{\alpha}{\beta})^{s'_1}-\beta^{r'_1}]^{d'},$$
  où $d'=pgcd(r-s,s)$, $s=s'_1d'$, et $r-s=r'_1d'$.
  Mais il est clair que $d'=pgcd(r-s,s)=pgcd(r,s)=d$. On en déduit en conservant les notations du lemme que $s_1=s'_1$ et $r_1=r'_1+s'_1$. Par suite,

$$\begin{aligned} R(x^r-\alpha, x^s-\beta) &= \beta^s(-1)^s[(\frac{\alpha}{\beta})^{s_1}-\beta^{r_1-s_1}]^d \\ &= (-1)^s\beta^{s_1 d}[(\frac{\alpha}{\beta})^{s_1}-\beta^{r_1-s_1}]^d \\ &= (-1)^s[\alpha^{s_1}-\beta^{r_1}]^d \end{aligned}$$

La propriété est donc vraie au rang $n+1$, ce qui achève la récurrence et la démonstration du lemme.

Remarque 2.1.21 *Cette formule est assez intuitive. En effet, si a designe une racine de $x^r-\alpha$, b une racine de $x^s-\beta$, ξ_1 une racine primitive r-ième de l'unité et ξ_2 une racine primitive s-ième de l'unité, alors les racines de $x^r-\alpha$ (respectivement, $x^s-\beta$) sont les $\{\xi_1^n a\ ,\ 0\leq n\leq r-1\}$ (respectivement $\{\xi_2^m b\ ,\ 0\leq m\leq s-1\}$). On a alors,*

$$R(x^r-\alpha, x^s-\beta)=0 \iff \exists n,m\in\mathbb{N}, \xi_1^n a=\xi_2^m b$$

En élevant cette dernière égalité à la puissance $r_1 s_1 d$, on obtient :

$$R(x^r-\alpha, x^s-\beta)=0 \iff \alpha^{s_1}=\beta^{r_1}$$

Par ailleurs, si $\alpha^{s_1}=\beta^{r_1}$, alors $x^r-\alpha$ et $x^s-\beta$ ont une racine commune, ce qui se traduit par $\xi_1^n a=\xi_2^m b$. Mais alors, pour toute racine d-ième de l'unité ξ, $\xi\xi_1^n a=\xi\xi_2^m b$. Or, $\xi\xi_1^n a$ est encore une racine de $x^r-\alpha$ et de même, $\xi\xi_2^m b$ est encore une racine de $x^s-\beta$. Ce qui montre que ces deux polynômes ont alors d racines communes. Ce qui explique l'origine de la formule précédente.

Ce lemme permet alors de calculer le discriminant d'un trinôme. En effet,

Théorème 2.1.22 *[40] Soient $n>k>0$ deux entiers, a,b deux éléments d'un corps K, $d=pgcd(n,k)$ et n_1,k_1 les entiers définis par $n=n_1 d$ et $k=k_1 d$. Alors*
$D(x^n+ax^k+b)=(-1)^{\frac{n(n-1)}{2}}b^{k-1}[n^{n_1}b_{n_1-k_1}+(-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}a^{n_1}]^d$

Preuve :

On a par définition, pour tout polynôme f, $D(f)=(-1)^{\frac{n(n-1)}{2}}R(f',f)$. Par conséquent

$$\begin{aligned} D(x^n+ax^k+b) &= (-1)^{\frac{n(n-1)}{2}}R(nx^{n-1}+kax^{k-1}, x^n+ax^k+b) \\ &= (-1)^{\frac{n(n-1)}{2}}R(nx^{k-1}(x^{n-k}+\frac{ka}{n}), x^n+ax^k+b) \\ &= (-1)^{\frac{n(n-1)}{2}}R(n, x^n+ax^k+b)R(x^{k-1}, x^n+ax^k+b) \\ &\quad \times R(x^{n-k}+\frac{ka}{n}, x^n+ax^k+b) \\ &= (-1)^{\frac{n(n-1)}{2}}n^n(-1)^{n(k-1)}b^{k-1} \\ &\quad \times (-1)^{n(n-k)}R(x^n+ax^k+b, x^{n-k}+\frac{ka}{n}) \end{aligned}$$

Or $n(k-1)+n(n-k)=n^2-n\equiv 0$ [2] , par conséquent on a :

$$D(x^n+ax^k+b)=(-1)^{\frac{n(n-1)}{2}}n^n b^{k-1}R(x^n+ax^k+b,x^{n-k}+\tfrac{ka}{n})$$

Mais on a $x^n+ax^k+b=x^k(x^{n-k}+\frac{ka}{n})+a(1-\frac{k}{n})x^k+b$. Il s'ensuit alors que

$$\begin{aligned} R(x^n+ax^k+b,x^{n-k}+\frac{ka}{n}) &= R(a(1-\frac{k}{n})x^k+b,x^{n-k}+\frac{ka}{n}) \\ &= (a-\frac{ka}{n})^{n-k}R(x^k+\frac{b}{a(1-\frac{k}{n})},x^{n-k}+\frac{ka}{n}) \end{aligned}$$

Mais on peut alors appliquer le lemme précédent avec $r=k$, $\alpha=-\frac{b}{a-\frac{ka}{n}}$, $s=n-k$ et $\beta=-\frac{ka}{n}$, ce qui fournit en remarquant comme dans la preuve du lemme que $pgcd(n-k,k)=pgcd(n,k)$

$$R(x^k+\tfrac{b}{a(1-\frac{k}{n})},x^{n-k}+\tfrac{ka}{n})=(-1)^{n-k}[(\tfrac{-b}{(a-\frac{ka}{n})})^{n_1-k_1}-(\tfrac{-ka}{n})^{k_1}]^d$$

D'où en posant $R=R(a(1-\frac{k}{n})x^k+b,x^{n-k}+\frac{ka}{n})$, on obtient successivement :

$$\begin{aligned} R &= (a-\frac{ka}{n})^{n-k}(-1)^{n-k}[(\frac{-b}{(a-\frac{ka}{n})})^{n_1-k_1}-(\frac{-ka}{n})^{k_1}]^d \\ &= [(\frac{ka}{n}-a)^{n_1-k_1}]^d[(\frac{-b}{(a-\frac{ka}{n})})^{n_1-k_1}-(\frac{-ka}{n})^{k_1}]^d \\ &= [b^{n_1-k_1}+(-1)^{n_1+1}(a-\frac{ka}{n})^{n_1-k_1}(\frac{ka}{n})^{k_1}]^d \end{aligned}$$

En notant maintenant $D=D(x^n+ax^k+b)$, on obtient finalement :

$$\begin{aligned} D &= (-1)^{\frac{n(n-1)}{2}}n^{n_1 d}b^{k-1}[b^{n_1-k_1}+(-1)^{n_1+1}(a-\frac{ka}{n})^{n_1-k_1}(\frac{ka}{n})^{k_1}]^d \\ &= (-1)^{\frac{n(n-1)}{2}}b^{k-1}[n^{n_1}b^{n_1-k_1}+(-1)^{n_1+1}(n-k)^{n_1-k_1}a^{n_1}k^{k_1}]^d \end{aligned}$$

Ce qui achève la démonstration du théorème.

2.2 Application à la réductibilité des trinômiaux sur $\mathbb{F}_2$

Le théorème de la section précédente permet alors de donner une condition suffisante (mais non nécéssaire) pour qu'un polynôme trinomial soit réductible sur $\mathbb{F}_2$.

Corollaire 2.2.1 *[40] Soient $n>k>0$. On suppose qu'exactement un parmi n et k est pair. Alors le polynôme x^n+x^k+1 a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$ (et donc est réductible) dans les cas suivants :*

- *(a) n est pair, k impair, $n \neq 2k$ et $\frac{nk}{2} \equiv 0$ ou 1 [4]*
- *(b) n est impair, k est pair, $k \not| 2n$ et $n \equiv \pm 3$ [8]*
- *(c) n est impair, k est pair, $k \mid 2n$ et $n \equiv \pm 1$ [8]*

Dans tous les autres cas, x^n+x^k+1 a un nombre impair de facteurs irréductibles sur $\mathbb{F}_2$.

Remarque 2.2.2 *Le cas où n et k sont impairs se déduit du cas où n est impair et k pair en considérant le polynôme $x^n + x^{n-k} + 1$, qui a le même nombre de facteurs irréductibles que $x^n + x^k + 1$.*

Démonstration du corollaire :

Considérons les polynômes $g = x^n + x^k + 1 \in \mathbb{F}_q[X]$ et $f = x^n + x^k + 1 \in \mathbb{Z}_2[X] \subset \mathbb{Q}_2[X]$. Soit $\bar{f}$ la réduction de f modulo $2\mathbb{Z}_2$. En identifiant $\mathbb{Z}_2/2\mathbb{Z}_2$ à $\mathbb{F}_2$, on a donc $\bar{f} = g$.

De plus, d'après le théorème 2.1.22, $D(g) = (n^{n_1}+(n-k)^{n_1-k_1}k^{k_1})^d$ (puisque ici $a = b = 1$ et le corps de base est $\mathbb{F}_2$). Deux cas se présentent alors :

- 1er cas : $n \equiv 0$ [2] et $k \equiv 1$ [2]
  Alors $n^{n_1} \equiv 0$ [2] , $k^{k_1} \equiv 1$ [2] et $(n-k)^{n_1-k_1} \equiv 1$ [2]. Par conséquent, $D(g) = 1$.
- 2ème cas : $n \equiv 1$ [2] et $k \equiv 0$ [2]
  On trouve de même $D(g) = 1$

Ainsi dans les deux cas $D(g) = 1$ et donc g est séparable. On peut alors appliquer le corollaire 2.1.14 ; soit r le nombre de facteurs irréductibles de g sur $\mathbb{F}_2$ alors $r \equiv n$ [2] si et seulement si $D(f) \equiv 1$ [8].

- (a) On suppose n pair, k impair, $n \neq 2k$ et $\frac{nk}{2} \equiv 0$ ou 1 [4]. Dans ce cas, en conservant les notations de la section précédente, on trouve que :
  - $d = pgcd(n,k) \equiv 1$ [2]
  - $k_1 \equiv 1$ [2]
  - $n_1 \equiv 0$ [2]

  Mais on a également :

$$\begin{aligned} \frac{nk}{2} \equiv 0,1\ [4] \quad &\Longleftrightarrow \quad \frac{n_1 k_1 d^2}{2} \equiv 0,1\ [4] \\ &\Longleftrightarrow \quad \frac{n_1 k_1}{2} \equiv 0,1\ [4]\ (\text{ car } d^2 \equiv 1\ [4]) \end{aligned}$$

  - 1er sous-cas : $\frac{n_1}{2} \equiv 0$ [4]

$$\begin{aligned} \text{Alors } 8 \mid n \text{ et } D(f) &\equiv (-(-k)^{n_1-k_1}k^{k_1})^d\ [8] \\ &\equiv k^n(-1)^{(n_1-k_1+1)d}\ [8] \\ &\equiv k^n\ [8] \\ &\equiv 1\ [8] \end{aligned}$$

  (En effet, k étant premier à 8, $k \in (\mathbb{Z}/8\mathbb{Z})^\star$. Or $8 \mid n$, a fortiori $4 \mid n$; et donc $k^n \equiv 1$ [8]) Ainsi $D(f) \equiv 1$ [8].

Dans ce cas, $r \equiv n \equiv 0\ [2]$ et g a bien un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

- 2ème sous-cas : $\frac{n_1}{2} \equiv 1\ [4]$
  Dans ce cas, on a forcément $k_1 \equiv 1\ [4]$ (puisqu'il est supposé impair). Maintenant, il faut regarder les congruences possibles pour d, sachant que sous les hypothèses du cas (a), d est impair.
  - Si $d \equiv 1\ [4]$
    Alors $n \equiv 2\ [8]$, $k \equiv 1, 5\ [8]$ et $n_1 - k_1 \equiv 1\ [4]$. Par conséquent,

$$\begin{aligned} D(f) &\equiv (-1)[2^{n_1} - (2-k)k]^d\ [8] \\ &\equiv (-1)(2^{n_1} - (2-k)k)\ [8] \end{aligned}$$

    Maintenant si $n_1 = 2$ alors puisque $n_1 > k_1 > 0$, $k_1 = 1$. Mais alors $n = n_1 d = 2d = 2k_1 d = 2k$, ce qui contredit les hypothèses du cas (a). Par suite $n_1 > 2$ et $2^{n_1} \equiv 0\ [8]$ ce qui entraîne que $D(f) \equiv (2-k)k\ [8]$. Par ailleurs, comme $k \equiv 1, 5\ [8]$, on a dans les deux cas de figures $(2-k)k \equiv 1\ [8]$, et finalement, on trouve donc que $D(f) \equiv 1\ [8]$,ce qui permet de conclure à nouveau que $r \equiv n \equiv 0\ [2]$ et donc que g a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.
  - Si $d \equiv 3\ [4]$
    On a alors $n \equiv 6\ [8]$, $k \equiv 3, 7\ [8]$ et $n_1 - k_1 \equiv 1\ [4]$. Par conséquent,

$$\begin{aligned} D(f) &\equiv (-1)(6^{n_1} - (6-k)k)^d\ [8] \\ &\equiv ((6-k)k)^3\ [8] \end{aligned}$$

    (puisqu'ici encore le cas $n_1 = 2$ est impossible et donc $8 \mid 6^{n_1}$)
    Mais dans les deux cas $k \equiv 3$ ou $7\ [8]$, $((6-k)k)^3 \equiv 1\ [8]$. Ce qui montre une fois de plus que $r \equiv 0\ [2]$ et donc que g a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

  Ce qui achève le 2ème sous-cas.
- 3ème sous-cas : $\frac{n_1}{2} \equiv 2\ [4]$
  Dans ce cas, $2k_1 \equiv 0, 1\ [4]$ ce qui n'est pas possible car k_1 est impair et 2 n'est pas inversible dans $\mathbb{Z}/4\mathbb{Z}$.
- 4ème sous-cas : $\frac{n_1}{2} \equiv 3\ [4]$
  Alors nécessairement, $k_1 \equiv 3\ [4]$ (puisqu'il est impair et donc ne peut être divisible par 4). Il faut alors de nouveau distinguer les cas selon la valeur de d [4]. Mais on voit rapidement que :
  - Si $d \equiv 1\ [4]$
    Alors $n \equiv 6\ [8]$ et $k \equiv 3, 7\ [8]$, et donc de même que dans l'étude faîte dans le 2ème sous-cas, on a bien $D(f) \equiv 1\ [8]$, c'est-à-dire que g a de nouveau un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.
  - De même, si $d \equiv 3\ [4]$ alors on trouve de la même façon que $n \equiv 2\ [8]$ et $k \equiv 1, 5\ [8]$ et on conclut à nouveau que g a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

Ainsi, on a montré que si n est pair, k impair, $n \neq 2k$ et $\frac{nk}{2} \equiv 0,1$ [4] alors le polynôme $x^n + x^k + 1$ a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

- (b) n impair, k pair, $k \not| 2n$ et $n \equiv \pm 3$ [8]
  Déjà, on peut constater que nécessairement $k_1 > 2$. En effet, comme n est impair et k pair d est impair, ce qui montre pour commencer que $k_1 > 1$ (sinon k serait impair). De plus si $k_1 = 2$, alors $k = k_1 d = 2d \mid 2n_1 d = n$ ce qui contredit les hypothèses. Par suite $8 \mid k^{k_1}$. En reprenant l'expression de $D(f)$, on a donc :

$$\begin{aligned} D(f) &\equiv (-1)^{\frac{n(n-1)}{2}}(n^{n_1} + (3-k)^{n_1-k_1}k^{k_1})^d \ [8] \\ &\equiv (-1)^{\frac{n(n-1)}{2}}3^n \ [8] \end{aligned}$$

  - Si $n \equiv 3$ [8] alors
    $$D(f) \equiv (-1)3^3 \equiv 5 \ [8]$$
    Et donc $r \not\equiv n$ [2], c'est-à-dire que r est pair et g a bien un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.
  - Si $n \equiv 5$ [8] alors on a de même
    $$D(f) \equiv 5^n \equiv 5 \ [8]$$
    On conclut de la même façon que g a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

  Ce qui montre que sous les hypothèses du (b), à savoir n impair, k pair $k \not| 2n$ et $n \equiv 3,5$ [8], le polynôme $x^n + x^k + 1$ a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.
- (c) n est impair, k pair, $k \mid 2n$ et $n \equiv \pm 1$ [8]
  Déjà, on peut remarquer que $\frac{k}{2} \in (\mathbb{Z}/8\mathbb{Z})^\star$. On en déduit donc que $k \equiv 2,6$ [8]. Par ailleurs comme $k \mid 2n$, $2n_1 = ak_1$ où a est un entier. Distinguons alors les cas possibles :
  - 1er cas : $n \equiv 1$ [8] et $d \equiv 1$ [4]
    Alors on a $n_1 \equiv 1$ [4]. De plus en regardant les égalités précédentes modulo 4, on a : $ak_1 \equiv 2$ [4]. Or k_1 est pair, on en déduit donc que $k_1 \equiv 2$ [4]. On a alors :

$$\begin{aligned} D(f) &\equiv (1-(1-k)^{n_1-k_1}k^{k_1})^d \ [8] \\ &\equiv 1-(1-k)^3k^2 \ [8] \end{aligned}$$

    Mais dans les deux cas $k \equiv 2,6$ [8], on trouve $D(f) \equiv 5$ [8]. Ce qui montre que g a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.
  - 2ème cas : $n \equiv 1$ [8] et $d \equiv 3$ [4]
    Le même raisonnement fournit $n_1 \equiv 3$ [4] et $k_1 \equiv 2$ [4]. Par conséquent, $D(f) \equiv (1-(1-k)k^2)^3$ [8]. Là encore, une simple substitution avec $k \equiv 2,6$ [8] conduit à $D(f) \equiv 5$ [8].
  - 3ème cas : $n \equiv -1$ [8] et $d \equiv 1$ [4]

Alors $n_1 \equiv 3$ [4] , $k_1 \equiv 2$ [4] et $D(f) \equiv 1-(1-k)k^2$ [8]. Mais pour $k \equiv 2,6$ [8] , on a toujours en substituant $D(f) \equiv 5$ [8] et g a un nombre pair de facteurs irréductibles.

- 4ème cas : $n \equiv -1$ [8] et $d \equiv 3$ [4]
  Alors $n_1 \equiv 1$ [4] , $k_1 \equiv 2$ [4] et $D(f) \equiv (1-(1+k)^3k^2)^3$ [8]. Mais pour $k \equiv 2,6$ [8] , on a toujours en substituant $D(f) \equiv 5$ [8] et g a un nombre pair de facteurs irréductibles.

Ce qui montre que pour n impair, k pair, $k \mid 2n$ et $n \equiv \pm 1$ [8], x^n+x^k+1 a un nombre pair de facteurs irréductibles sur $\mathbb{F}_2$.

Maintenant, il s'agit de démontrer que dans tous les autres cas, x^n+x^k+1 a un nombre impair de facteurs irréductibles sur $\mathbb{F}_2$.

- (a) n est pair et k est impair
  - Si $n = 2k$
    Dans ce cas, $d = k$, $k_1 = 1$, et $n_1 = 2$. En revenant à la formule donnant le discriminant d'un trinôme, on trouve :
    $$D(f) = D(x^{2k}+x^k+1) = -(3k^2)^k$$
    - Si $k \equiv 1$ [4]
      Alors $D(f) \equiv 5k^2$ [8]. Mais comme $k \equiv 1$ [4], $k^2 \equiv 1$ [8] ce qui entraîne que $D(f) \equiv 5$ [8] et montre donc que $r \equiv 1$ [2].
    - Si $k \equiv 3$ [4]
      Alors $D(f) \equiv 5k^2$ [8]. Mais comme $k \equiv 3$ [4], $k^2 \equiv 1$ [8]. Finalement, $D(f) \equiv 5$ [8]. Ce qui montre de nouveau que $r \equiv 1$ [2].

  - Si $n \neq 2k$ et $\frac{nk}{2} \equiv 3,4$ [4]

    Déjà, $n_1 > 2$. En effet, comme n est pair et k impair, n_1 est pair donc différent de 1. Par ailleurs, si $n_1 = 2$, alors $n = 2d$. Mais comme $k < n$, on a alors $k_1 = 1$ et donc $n = 2k$, ce qui contredit les hypothèses de ce cas. Par suite, $n^{n_1} \equiv 0$ [8].
    - 1er cas : $k_1 \equiv 1$ [4]
      - Si $d \equiv 1$ [4]

$$\begin{aligned} D(f) &\equiv (-1)^{\frac{n(n-1)}{2}}[n^{n_1}+(-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d \text{ [8]} \\ &\equiv (-1)^{\frac{n(n-1)}{2}}[-(n-k)^{n_1-1}k]^d \text{ [8]} \end{aligned}$$

Or, $n_1 \equiv 4,6$ [8] et $d \equiv 1,5$ [8]. On en déduit donc que :

$$\begin{aligned} &\text{Si } n_1 \equiv 4 \text{ [8]} \quad , \quad D(f) \equiv -(4-k)^3k \text{ [8]} \\ &\text{Si } n_1 \equiv 6 \text{ [8]} \quad , \quad D(f) \equiv (6-k)k \text{ [8]} \end{aligned}$$

Mais sous les conditions $k_1 \equiv 1$ [4] et $d \equiv 1$ [4], alors nécéssairement, $k \equiv 1,5$ [8]. Et, dans tous les cas, on trouve $D(f) \equiv 5$ [8], ce qui montre que r est impair.

- Si $d \equiv 3$ [4]
  Alors, $D(f) \equiv (-1)^{\frac{n(n-1)}{2}}[-(n-k)^{n_1-1}k]^3$. Mais, comme dans le cas précédent, $n_1 \equiv 4, 6$ [8]. De plus, si $n_1 \equiv 4$ [8], alors nécéssairement $n \equiv 4$ [8] et de même, si $n_1 \equiv 6$ [8] alors $n_1 \equiv 2$ [8]. On en déduit donc que :

$$\begin{array}{rcl} \text{Si } n_1 \equiv 4 \text{ [8]} & , & D(f) \equiv -(4-k)k^3 \text{ [8]} \\ \text{Si } n_1 \equiv 6 \text{ [8]} & , & D(f) \equiv (2-k)^3k^3 \text{ [8]} \end{array}$$

  Mais une simple substitution en remarquant que sous ces conditions $k \equiv 3, 7$ [8], fournit $D(f) \equiv 5$ [8]. Ce qui démontre que r est impair.
- 2ème cas : $k_1 \equiv 3$ [4]
  - Si $d \equiv 1$ [4]
    Alors $D(f) \equiv (-1)^{\frac{n(n-1)}{2}}[-(n-k)^{n_1-3}k^3]$ [4].

$$\begin{array}{r} \text{si } n_1 \equiv 2 \text{ [8]}, \text{ alors } n \equiv 2 \text{ [8] et } D(f) \equiv (2-k)^3k^3 \text{ [8]} \\ \text{si } n_1 \equiv 4 \text{ [8]}, \text{ alors } n \equiv 4 \text{ [8] et } D(f) \equiv -(4-k)k^3 \text{ [8]} \end{array}$$

    Mais une fois de plus, sous les hypothèses de ce cas, $k \equiv 3, 7$ [8], et on trouve de nouveau que $D(f) \equiv 5$ [8]. Ce qui permet de conclure que r est impair.
  - Si $d \equiv 3$ [4]
    De même que précédemment, on trouve que :

$$\begin{array}{r} \text{si } n_1 \equiv 2 \text{ [8]}, \text{ alors } n \equiv 6 \text{ [8] et } D(f) \equiv (6-k)k \text{ [8]} \\ \text{si } n_1 \equiv 4 \text{ [8]}, \text{ alors } n \equiv 4 \text{ [8] et } D(f) \equiv -(4-k)^3k \text{ [8]} \end{array}$$

    Mais une fois de plus, sous les hypothèses de ce cas, $k \equiv 1, 5$ [8], et on trouve de nouveau que $D(f) \equiv 5$ [8]. Ce qui permet de conclure que r est impair.

- (b) n est impair, k pair, $k \not| 2n$ et $n \not\equiv \pm 3$ [8]
  Sous ces conditions, $n \equiv 1, 7$ [8]. De plus, si $k_1 \mid 2n_1$ alors $k \mid 2n$, ce qui contredit les hypothèses de ce cas. Par conséquent, $k_1 \not| 2n_1$. Maintenant, puisque k est pair et n impair, d est impair ; donc k_1 est pair et puisque $k_1 \not| 2n_1$, on en déduit que $k_1 > 2$.
  Dans ces conditions $k^{k_1} \equiv 0$ [8] et donc $D(f) \equiv (-1)^{\frac{n(n-1)}{2}}n^n$ [8]. Mais pour $n \equiv 1, 7$ [8], on obtient $D(f) \equiv 1$ [8].
  Ce qui permet de conclure que $r \equiv n$ [2], c'est-à-dire r est impair.

- (c) n impair, k pair, $k \mid 2n$ et $n \equiv 3, 5$ [8]
  Commençons par montrer que $k_1 = 2$.

Déjà, s'il existe p premier distinct de 2 divisant k_1 , alors, comme $k_1 \mid 2n_1$ et $p \neq 2$, $p \mid n_1$ et donc $p \mid \text{pgcd}(n_1, k_1) = 1$, ce qui est absurde. On en déduit donc pour commencer que k_1 est une puissance de 2.
Maintenant comme n_1 est impair et que $k_1 \mid 2n_1$ nécessairement $k_1 = 2$.
Ainsi, $k = 2d$ et $n = n_1 d$. On a donc :

$$\begin{aligned} D(f) &= (-1)^{\frac{n(n-1)}{2}}[n^{n_1} + (-1)^{n_1+1}(n-k)^{n_1-k_1}k^{k_1}]^d \\ &= (-1)^{\frac{n(n-1)}{2}}[n^{n_1} + (n-k)^{n_1-2}k^2]^d \\ &= (-1)^{\frac{n(n-1)}{2}} \sum_{i=0}^{d} C_d^i n^{(d-i)n_1}(n-k)^{i(n_1-2)}k^{2i} \end{aligned}$$

Mais ici, k est pair, donc si $i \geq 2$, $k^{2i} \equiv 0$ [8]. On en déduit donc l'expression suivante :

$$D(f) \equiv (-1)^{\frac{n(n-1)}{2}}[n^n + dn^{n_1(d-1)}(n-k)^{n_1-2}k^2] \text{ [8]}$$

- 1er cas : $d \equiv 1$ [4]
  Alors $D(f) \equiv (-1)^{\frac{n(n-1)}{2}}[n^n + d(n-k)^{n_1-2}k^2]$ [8]
  - Si $n \equiv 3$ [8]
    Dans ce cas, $n_1 \equiv 3$ [4] et donc $D(f) \equiv -[3 + d(3-k)k^2]$ [8]. On a alors,

$$\begin{aligned} d \equiv 1 \text{ [8]}, \text{alors } k \equiv 2 \text{ [8]}, D(f) \equiv -(3 + (3-k)k^2) \equiv 1 \text{ [8]} \\ d \equiv 5 \text{ [8]}, \text{alors } k \equiv 2 \text{ [8]}, D(f) \equiv -(3 + 5(3-k)k^2) \equiv 1 \text{ [8]} \end{aligned}$$

    Ce qui montre que r est impair.
  - Si $n \equiv 5$ [8]
    Dans ce cas, $n_1 \equiv 1$ [4] et donc

$$\begin{aligned} D(f) &\equiv [5 + d(5-k)^3k^2] \text{ [8]} \\ &\equiv 5 + 4d^2 \text{ [8]} \\ &\equiv 1 \text{ [8] (puisque } d^2 \equiv 1 \text{ [8])} \end{aligned}$$

- 2ème cas : $d \equiv 3$ [4]
  Alors $D(f) \equiv (-1)^{\frac{n(n-1)}{2}}[n^n + dn^{2n_1}(n-k)^{n_1-2}k^2]$ [8]
  - Si $n \equiv 3$ [8]
    Dans ce cas, $n_1 \equiv 1$ [4] et donc

$$\begin{aligned} D(f) &\equiv -[3 + 3^2d(3-k)^3k^2] \text{ [8]} \\ &\equiv -(3 + 4d^3) \text{ [8]} \\ &\equiv 1 \text{ [8] (puisqu'on est dans le cas } d \equiv 3 \text{ [4]} \end{aligned}$$

    Ce qui montre que r est impair.

– Si $n \equiv 5$ [8]
Dans ce cas, $n_1 \equiv 3$ [4] et donc

$$\begin{aligned} D(f) &\equiv [5 + d(5-k)k^2] \text{ [8]} \\ &\equiv 5 + 4d^3 \text{ [8]} \\ &\equiv 1 \text{ [8] (puisque } d^3 \equiv 3, 7 \text{ [8])} \end{aligned}$$

Ce qui montre de nouveau que r est impair.
Ceci achève la démonstration du corollaire.

Corollaire 2.2.3 *[40] Il n'existe pas de polynôme trinômial irréductible sur* $\mathbb{F}_2$ *de degré* $n \equiv 0$ [8].

Preuve :

En effet, si n est divisible par huit, d'après le dernier corollaire, cas (a), pour tout entier k impair , on a $n \neq 2k$ (car k est impair et n divisible par huit) et $\frac{nk}{2}$ est divisible par 4. Ce qui montre que $x^n + x^k + 1$ a un nombre pair de facteurs irréductibles, et donc est réductible.

De même, si k est pair, alors $x^n + x^k + 1 = (x^{\frac{n}{2}} + x^{\frac{k}{2}} + 1)^2$ est réductible.

2.3 Existence de polynômes pentanômiaux irréductibles sur $\mathbb{F}_2$

La section précédente a montré qu'il n'était pas toujours possible de trouver un trinômial irréductible sur $\mathbb{F}_2$. On peut alors se demander ce qu'il en est pour les pentanômiaux. La recherche sous Maple de pentanômiaux irréductibles de degré n pour $4 \leq n \leq 10000$ semble suggérer qu'il en existe toujours, mais cette question reste ouverte. De plus, il est surprenant de constater que même pour les valeurs de n relativement élevées, l'expérience montre que l'on peut toujours trouver $f = x^n + x^a + x^b + x^c + 1$ irréductible avec $a \leq 60$ (pour toutes les valeurs considérées). Dans cette partie, on montre dans un premier temps qu'il existe une infinité de pentanômiaux irréductibles en exhibant deux exmples de familles infinies. Puis, dans un second temps, on montre que contrairement aux trinômiaux, on peut toujours trouver un pentanômial de degré n fixé ayant un nombre impair de facteurs irréductibles. Enfin, pour terminer, on présente les résultats de la recherche faîte sous Maple qui nous a permis d'atteindre le record actuel du pentanômial de plus haut degré.

2.3.1 Famille de pentanômiaux irréductibles sur $\mathbb{F}_2$

Proposition 2.3.1 *Les polynômes* $x^{4.5^k} + x^{3.5^k} + x^{2.5^k} + x^{5^k} + 1$ *sont irréductibles sur* $\mathbb{F}_2$ *pour tout entier* k.

Preuve :

Le polynôme cyclotomique $Q_5 = x^4 + x^3 + x^2 + x + 1$ est irréductible sur $\mathbb{F}_2$ (en appliquant le théorème 1.2.3, 2 est primitif modulo 5). Ses racines sont toutes d'ordre 5 exactement. En appliquant alors le théorème 1.2.16 avec $q = 2$, $P = Q_5$, $n = 4$, $t = 5^k$ et $e = 5$, on déduit la proposition.

Proposition 2.3.2 *Les polynômes $x^{5.31^k} + x^{3.31^k} + x^{2.31^k} + x^{31^k} + 1$ sont irréductibles sur $\mathbb{F}_2$ pour tout entier k.*

Preuve : Comme dans le cas précédent, on applique le théorème 1.2.16 avec $q = 2$, $P = x^5 + x^3 + x^2 + x + 1$, $n = 5$, $e = 31$, et $t = 31^k$.

En utilisant ce procédé, il est aisé de construire des familles de pentanômiaux irréductibles sur $\mathbb{F}_2$. Mais cette méthode est très limitée puisqu'elle ne donne que des exemples et ne fournit pas de méthode générale pour construire un pentanômial irréductible de degré donné. En revanche, elle permet tout de même d'exhiber des familles infinies de pentanômiaux irréductibles.

2.3.2 Application du théorème de Swan au cas des pentanômiaux

La situation est bien plus compliquée pour les pentanômiaux. En effet, une des grandes applications du théorème de Swan est de montrer que lorsque n est divisible par 8, il n'existe pas de trinômial irréductible de degré n. Pour cela, on montre en fait que tous les trinômiaux de degré n ont un nombre pair de facteurs irréductibles. Cette méthode ne marche pas pour les pentanômiaux comme le montre la proposition suivante :

Proposition 2.3.3 *Pour tout entier n supérieur ou égal à 33, il existe au moins un pentanômial de degré n ayant un nombre impair de facteurs irréductibles.*

Preuve :

Dans ce qui suit, r désignera toujours le nombre de facteurs irréductibles du polynôme considéré sur $\mathbb{F}_2$.

- Si $n \equiv \pm 1$ [8]
  On considère $f(x) = x^n + x^{32} + x^{16} + x^8 + 1$. Alors $f'(x) \equiv nx^{n-1}$. On en déduit donc que : $D(f) \equiv (-1)^{\frac{n(n-1)}{2}} n^n \equiv 1$ [8]. Ce qui entraîne que $r \equiv n \equiv 1$ [8]
- Si $n \equiv \pm 3$ [8]
  On considère $f(x) = x^n + x^{n-2} + x^{16} + x^8 + 1$. On en déduit l'expression suivante, $D(f) \equiv (-1)^{\frac{n(n-1)}{2}} n^n f(\sqrt{\frac{2-n}{n}}) f(-\sqrt{\frac{2-n}{n}})$. Ce qui conduit à l'expression suivante :

$$\begin{aligned} D(f) \equiv & -(2-n)^n - 2n(2-n)^{n-1} - n^2(2-n)^{n-2} \\ & + n^{n-16}(2-n)^{16} + 2n^{n-12}(2-n)^{12} + 3n^{n-8}(2-n)^8 \\ & + 2n^{n-4}(2-n)^4 + n^n \end{aligned}$$

  On conclut alors que pour $n \equiv \pm 3$ [8], $D(f) \equiv 1$ [8], et le résultat.

– Si $n \equiv 0$ [8]
On considère $f(x) = x^n + x^{n-1} + x^{n-3} + x^8 + 1$. On a sous ces conditions, $f'(x) \equiv x^{n-4}((n-1)x^2 + n - 3)$. Ce qui conduit à l'expression suivante : $D(f) \equiv (n-1)^n f(\sqrt{\frac{3-n}{n-1}}) f(-\sqrt{\frac{3-n}{n-1}})$. Soit encore,

$$\begin{aligned} D(f) \equiv & -(n-1)(3-n)^{n-1} - 2(n-1)^2(3-n)^{n-2} \\ & -(n-1)^3(3-n)^{n-3} + 2(n-1)^n(\frac{3-n}{n-1})^{\frac{n+8}{2}} \\ & +2(n-1)^n(\frac{3-n}{n-1})^{\frac{n}{2}} + 2(n-1)^n(\frac{3-n}{n-1})^4 \\ & +(n-1)^n(\frac{3-n}{n-1})^8 + (n-1)^n + (3-n)^n \end{aligned}$$

(L'expression précédente a un sens puisque $n-1$ est inversible modulo 8, puisqu'il vaut -1).
En substituant, on obtient $D(f) \equiv 5$ [8]. Ce qui montre que $r \not\equiv n$ [2], et donc que f a un nombre impair de facteurs irréductibles.
– Si $n \equiv 2$ [8]
On considère alors $f(x) = x^n + x^{n-1} + x^{n-2} + x^8 + 1$. On a alors successivement $f'(x) \equiv nx^{n-1} + (n-1)x^{n-2}$ et $D(f) \equiv -n^n f(\frac{1-n}{n})$. Soit encore,

$$D(f) \equiv -\left((1-n)^n + n(1-n)^{n-1} + n^2(1-n)^{n-2}n^{n-8}(1-n)^8 + n^n\right)$$

Ce qui conduit en remplaçant par la valeur de n modulo 8 à $D(f) \equiv 5$ [8]. D'où le résultat.
– Si $n \equiv 4$ [8]
On pose alors $f(x) = x^n + x^{n-1} + x^{n-4} + x^8 + 1$. On conclut alors de la même façon que dans le cas précédent.
– Si $n \equiv 6$ [8]
On pose alors $f(x) = x^n + x^{n-1} + x^{n-6} + x^8 + 1$. On conclut alors de la même façon que dans le cas précédent.

Corollaire 2.3.4 *Pour tout entier $n \geq 4$, il existe au moins un pentanômial de degré n ayant un nombre impair de facteur irréductible sur $\mathbb{F}_2$.*

Preuve :
Si $n \geq 33$, c'est la proposition précédente. Les autres cas sont traités explicitement dans la table (qui donne mieux puisqu'elle fournit un pentanômial irréductible).

2.3.3 Conjecture sur les pentanômiaux

La question de savoir s'il existe toujours un pentanômial irréductible de degré donné est encore ouverte. Une recherche par ordinateur faîte sous Maple puis NTL fournit une indication quant à la réponse. En effet, pour $4 \leq n \leq 18000$, cette recherche a montré que l'on peut toujours en trouver un, avec une

première puissance x^a relativement faible (moins de 60 pour toutes les valeurs de n testées).

A titre d'exemple, les calculs ont montré que les polynômes suivants sont irréductibles sur $\mathbb{F}_2$: $x^{9694} + x^{50} + x^{18} + x^{17} + 1$, $x^{8123} + x^{47} + x^{22} + x^{18} + 1$, $x^{9683} + x^{46} + x^{37} + x^{21} + 1$, $x^{9472} + x^{45} + x^{40} + x^{15} + 1$ pour ceux ayant les puissances parmi les plus élevées et $x^{8226}+x^5+x^2+x+1$, $x^{8207}+x^5+x^4+x+1$, $x^{9992} + x^7 + x^4 + x^2 + 1$, $x^{9751} + x^9 + x^3 + x + 1$ sont parmi ceux qui ont les puissances les moins élevées.

En fait, la liste que nous avons calculé grace à l'aide très précieuse de Gérard Vinel établit le record actuel. Cette liste est disponible à l'adresse internet suivante : http ://fr.briefcase.yahoo.com/a_gewirtz.

En ce qui concerne la recherche informatique, pour les degrés $n \leq 5000$, les calculs ont été faits sous Maple. Le calcul de 50 pentanômiaux prenaient en moyenne quelques heures pour les petits degrés, 1 à 2 jours pour des degrés moyens (aux environs de 2000) puis 2 à 4 jours pour les degrés aux environs de 4000 (les moyennes ici ne sont pas précises et ne sont que des estimations).

En revanche, avec la programmation en C++ avec les bibliothèques GMP et NTL (developpé par Shoup), la recherche a été beaucoup plus efficace. Afin de déterminer une moyenne précise, nous avons effectué 50 fois la recherche de 50 pentanômiaux irréductibles et relevé les temps de calculs à chaque fois. Voici les moyennes observées en fonction des degrés n :

- pour $5000 \leq n \leq 5050$, le temps moyen observé est de 112 unités,
- pour $10000 \leq n \leq 10050$, le temps moyen observé est de 3332 unités,
- et enfin pour n de l'ordre de 15000, le temps moyen observé est de 6000 unités.

En ce qui concerne les ressources informatiques, les calculs ont été effectué sur plusieurs ordinateurs à la fois, chacun cherchant une liste donnée (par exemple de 5000 à 6000). Sous Maple, nous avons utilisé cinq ordinateurs, qui chacun travaillait par groupe de 50 degrés. Sous NTL, à partir de 10000, nous avons utilisé un seul ordinateur, une machine biprocesseur Xeon à 2Ghz avec 2Go de Ram. Les programmes utilisés sont eux aussi disponibles à l'adresse internet précédente.

Au vu des résultats des calculs informatiques, il est raisonable d'énoncer la conjecture suivante :

Conjecture 2.3.5 *Pour tout entier $n \geq 4$, il existe un pentanômial irréductible sur $\mathbb{F}_2$ de degré n.*

Du point de vue de la cryptologie, il est plus intéressant d'avoir des trinômiaux. On peut également citer une conjecture plus faible :

Conjecture 2.3.6 *Pour tout $n \geq 3$, il existe un trinômial ou un pentanômial de degré n irréductible sur $\mathbb{F}_2$.*

Chapitre 3

Généralités sur les modules elliptiques de Drinfeld

3.1 Analyse non-archimédienne et polynômes additifs sur $\mathbb{F}_q$

Il existe deux descriptions équivalentes des modules de Drinfeld : une description algébrique et une définition analytique. Avant de pouvoir donner la description analytique, il est nécessaire d'introduire un certain nombre de notions d'analyse non-archimédienne. Dans ce paragraphe, on rappelle d'une part les résultats d'analyse non-archimédienne dont on aura besoin au paragraphe suivant, notamment le théorème de factorisation des fonctions entières, et d'autre part, on rappelle également les caractérisations des polynômes additifs et $\mathbb{F}_q$-linéaire.

3.1.1 Série entière et rayon de convergence

Proposition 3.1.1 *[14] Soit K un corps complet pour une valuation ν. Soit $\bar{K}$ une clôture algébrique fixée de K muni du prolongement canonique de ν encore noté ν. Soit $\hat{\bar{K}}$ le complété de $\bar{K}$ pour ν. Alors $\hat{\bar{K}}$ est algébriquement clos.*

Remarque 3.1.2 *On rappelle que si (K, ν) est complet pour une valuation ν, alors la série de terme général a_n converge si et seulement si a_n converge vers 0.*

Remarque 3.1.3 *Dans tout ce qui suit, on supposera donc (K, ν) complet et algébriquement clos.*

Définition 3.1.4 *[38, p.283] Soit $f(x) = \sum_{n\geq 0} a_n x^n$ une série formelle sur K. On définit le rayon de convergence de f par :*

$$\rho(f) = -\liminf \frac{\nu(a_n)}{n}$$

Proposition 3.1.5 *[38, p.284] [14] Soit f une série formelle a coefficient dans K, de rayon de convergence $\rho(f)$. Soit $x \in K$, alors :*
- *(i) Si $\nu(x) > \rho(f)$, f converge en x.*
- *(ii) Si $\nu(x) < \rho(f)$, alors f diverge en x.*

Remarque 3.1.6 *On dit que f converge en x si la série de terme général $a_n x^n$ converge. Sinon on dit que f diverge en x.*

Preuve :

(i) On suppose $\nu(x) < \rho(f)$ (en particulier, on suppose $\rho(f) \neq -\infty$). On a alors :

$$\nu(a_n x^n) = n(\frac{\nu(a_n)}{n} + \nu(x))$$

Mais comme $\nu(x) < \rho(f)$, il existe une infinité d'indices n pour lesquels $\frac{\nu(a_n)}{n} + \nu(x) < 0$. En particulier, $a_n x^n$ ne converge pas vers zéro. D'après la remarque qui précède, on en déduit que f ne converge pas au point x.

(ii) Supposons à présent $\nu(x) > \rho(f)$ (en particulier, on suppose que $\rho(f) \neq +\infty$). Posons $\epsilon = \frac{\nu(x)-\rho(f)}{2}$ ($\epsilon > 0$). Il existe un entier n_0 tel que pour tout $n \geq n_0$, $-\epsilon < \inf_{k \geq n}(\frac{\nu(a_k)}{k} + \rho(f)) < \epsilon$. Pour un tel n_0, on en déduit que :

$$\forall n \geq n_0, \nu(a_n x^n) \geq n\frac{\nu(x) - \rho(f)}{2}$$

Par suite, $a_n x^n$ converge vers zéro et f converge en x. Ce qui achève la démonstration de la proposition.

3.1.2 Fonctions entières et théorème de factorisation

Définition 3.1.7 *[38, p.291] Soit f une série formelle de rayon de convergence $\rho(f) < +\infty$. Pour $r \in]\rho(f), +\infty[$, on pose $A_r(f) = \inf_{n \in \mathbb{N}}(\nu(a_n) + nr)$.*

On dit que r est régulier si la borne inférieure définissant $A_r(f)$ est atteinte pour un unique entier n.

On dit que r est critique si cette borne inférieure est atteinte pour au moins deux indices distincts.

Remarque 3.1.8 *La borne inférieure est bien atteinte. En effet, comme $r > \rho(f)$, d'après ce qui précède, $\nu(a_n) + nr$ tend vers $+\infty$. On est donc ramené à la borne inférieure d'un ensemble fini.*

Proposition 3.1.9 *[38, p.292] Avec les notations précédentes, on désigne par A la fonction qui à $r > \rho(f)$ associe le réel $A_r(f)$. Alors :*
- *(i) A est une fonction croissante continue.*
- *(ii) Pour tout $r > \rho(f)$, f a au plus un nombre fini de rayons critiques strictement plus grands que r.*

Preuve :

(i) Le fait que A soit croissante est évident. En ce qui concerne la continuité, soit $r > \rho(f)$ fixé et $\rho(f) < r' < r$. A partir d'un certain rang, tous les termes $\nu(a_n) + nr'$ sont strictement plus grands que $\nu(a_0)$. Par suite, $A_s(f) = \inf_{0 \leq n \leq N}(\nu(a_n) + ns)$ pour tout $s > r'$ (N étant un entier ne dépendant pas de s). Soit $\epsilon > 0$. Par continuité de chaque fonction $f_n(s) = \nu(a_n) + ns$ $(0 \leq n \leq N)$, on en déduit l'existence d'un réel δ tel que pour tout $s \in]r - \delta, r + \delta[$, pour tout entier $0 \leq n, k \leq N$,

$$-\epsilon \leq \nu(a_n) + ns - (\nu(a_k) + kr) \leq \epsilon$$

Ce qui montre que A est continue en r.

(ii) Soit $r > \rho(f)$. Alors $a_n r^n$ converge vers zéro. Par suite, il existe $n \in \mathbb{N}$ $A_r(f) = \nu(a_n) + nr$. Soit $s > r$ fixé et $N > n$, on a alors : $\nu(a_N) + Nr \geq \nu(a_n) + nr$. On en déduit donc que $\nu(a_N) - \nu(a_n) + (N - n)r \geq 0$. En particulier, on obtient que :

$$\forall N > n,\ \nu(a_N) + Ns > \nu(a_n) + ns$$

Par suite, à r fixé et $s > r$ fixé, seuls les termes de la forme $\nu(a_k) + ks$, $k \leq n$ peuvent être égaux. Ainsi les rayons critiques $s > r$ sont parmi les solutions des équations $(j - i)s = \nu(a_i) - \nu(a_j)$ pour $0 \leq i, j \leq n$, $i \neq j$. Ce qui montre bien que f a au plus un nombre fini de rayons critiques strictement plus grands que r et achève la preuve de la proposition.

Proposition 3.1.10 *Si $\nu(x) > \rho(f)$ et $f(x) = 0$ pour une série formelle f non identiquement nulle, alors $r = \nu(x)$ est un rayon critique de f.*

Preuve :

Supposons que r ne soit pas un rayon critique. Alors r est régulier. Par suite, il existe un unique entier n tel que :

$$\inf_{k \in \mathbb{N}}(\nu(a_k + kr)) = \nu(a_n) + nr$$

Mais alors, comme chaque terme $a_k x^k$ a une valuation strictement supérieure à celle de $a_n x^n$ pour k distinct de n, il s'ensuit que $\nu(f(x)) = \nu(a_n + nr)$. Mais x étant un zéro de f, on en déduit que $\nu(a_n) = +\infty$, c'est-à-dire, $a_n = 0$. Par suite, $a_k = 0$ pour tout entier k et f est identiquement nulle.

Ce qui achève la démonstration de la proposition.

Corollaire 3.1.11 *[38, p.307] [14] Considérons f une série formelle de rayon de convergence $\rho(f) < +\infty$ et non identiquement nulle. Alors f a un nombre fini de zéro dans tout disque fermé $\{\nu \geq r\}$ avec $r > \rho(f)$.*

Preuve :

D'après la proposition précédente, si x est un zéro de f, alors $r = \nu(x)$ est un rayon critique. Mais on a vu que f a un nombre au plus fini de rayons critiques strictement plus grands que $r > \rho(f)$ fixé.

Proposition 3.1.12 *[38, p.307] Soient $r_3 < r_2 < r_1$ trois rayons critiques consécutifs pour f. Désignons par α le plus petit entier n tel que la borne inférieure de $A_{r_2}(f)$ soit atteinte et β le plus grand. Alors :*

$$\begin{aligned} \nu(f(x)) &= \nu(a_\alpha) + \alpha\nu(x) \quad si\ r_2 < \nu(x) < r_1 \\ &= \nu(a_\beta) + \beta\nu(x) \quad si\ r_3 < \nu(x) < r_2 \end{aligned}$$

Preuve :

Soit $x \in K$ tel que $r_2 < \nu(x) < r_1$. Il existe un entier n_0 tel que pour tout $n \geq n_0$, $\nu(a_n) + ns > \nu(a_0)$ pour tout réel $s \geq r_2$ (si a_0 est nul on prend le plus petit entier tel que a_i est non nul et le résultat reste vrai). On en déduit que pour $s \geq r_2$, la borne inférieure de $A_s(f)$ est atteinte pour un entier n plus petit que n_0.

Comme r est régulier, il existe un unique entier k (inférieur ou égal à n_0 d'après ce qui précède), tel que la borne inférieure de $A_r(f)$ soit atteinte. Pour un tel k, considérons l'ensemble suivant :

$$O = \bigcap_{0 \leq n \leq n_0, n \neq k} \{s \in]r_2, r_1[, f_n(s) > f_k(s)\}$$

où f_n désigne la fonction qui à s associe $\nu(a_n) + ns$.

Comme chaque f_n est continue, il s'ensuit que O est ouvert non vide (contient r). De plus, il est clairement convexe ; par suite, $O =]a, b[$ pour $r_2 \leq a < b \leq r_1$. Montrons alors que a et b sont des rayons critiques.

En effet, comme $a \notin O$, il existe un entier n tel que $f_n(a) \leq f_k(a)$. Supposons que $f_n(a) < f_k(a)$. Par continuité de ces deux fonctions, il existe un réel $\epsilon > 0$ tel que pour tout $a' \in]a, a+\epsilon[$, $f_n(a') < f_k(a')$. Ce qui contredit le fait que a est la borne inférieure de O. Par conséquent, $f_n(a) = f_k(a)$. De plus, pour $p \neq k$, $p \leq n_0$, si $f_p(a) < f_n(a) = f_k(a)$, de la même façon que précédemment, on en déduit que a n'est pas la borne inférieure de O. Par suite, $f_p(a) \geq f_n(a) = f_k(a)$. Ceci montre que $A_a(f) = f_n(a) = f_k(a)$ et donc que a est un rayon critique.

Un raisonnement analogue démontre de même que b est un rayon critique. On en déduit alors que $a = r_2$ et $b = r_1$.

Mais au voisinage (à droite) de r_2, on a $f_\alpha(r_2^+) < f_n(r_2^+)$ pour tout entier n. Par suite, $k = \alpha$ ce qui démontre le premier cas.

La démonstration du deuxième cas est identique. Ceci achève la preuve de la proposition.

On est alors en mesure de démontré la réciproque de la proposition 3.1.10 :

Théorème 3.1.13 *[38, p.307] Si r est un rayon critique pour f alors f a un zéro sur la sphère $\{\nu = r\}$.*

Preuve :

Tout d'abord, désignons comme précédemment par α le plus petit entier tel que la borne inférieure $A_r(f)$ soit atteinte et par β le plus grand.

Comme ν est surjective, il existe $a \in K$ tel que $\nu(a) = r$. Posons alors $f_a(x) = f(ax)$ pour $\nu(x) > \rho(f) - r$. Alors f_a a un rayon critique en $s = 0$. On se ramène donc au cas où $r = 0$. On a alors $A_0(f) = \nu(a_\alpha) = \nu(a_\beta)$ (ce qui entraîne que a_α est non nul). Quitte à diviser f par a_α, on peut supposer que $\nu(a_\alpha) = \nu(a_\beta) = 0$. Enfin, quitte à multiplier f par un inversible de O_ν (anneau de valuation associé à ν), on peut supposer que $a_\alpha = 1$.

Ainsi, on se ramène au cas ou $r = 0$ est un rayon critique pour f (donc $f \in O_\nu[[X]]$), $a_\alpha = 1$, $\nu(a_\alpha) = \nu(a_\beta) = 0$. En particulier, $\nu(1) = 0 > \rho(f)$, donc f converge en 1, ce qui implique que a_n converge vers 0.

Etape 1 : troncature

Pour tout entier $\tau \geq 0$, on pose :

$$\begin{aligned} P_\tau &= \sum_{n \leq \tau} a_n x^n \\ g_\tau &= \sum_{n > \tau} a_n x^n \\ \text{donc } f &= P_\tau + g_\tau \end{aligned}$$

En particulier, si $\tau \geq \beta$, $A_0(g_\tau) = \inf_{n>\tau}(\nu(a_n)) > 0 = A_0(f) = A_0(P_\tau)$. Par continuité de $A(f), A(g_\tau)$:

$$\exists \epsilon' > 0, (\mid r \mid_{\mathbb{R}} < \epsilon' \Rightarrow A_r(g_\tau) > A_0(f))$$

De plus, comme les rayons critiques de f et g_τ sont en nombre fini dans toute boule de rayon strictement plus grand que leur ordre de convergence respectif, on en déduit l'existence de $0 < \epsilon'' < \epsilon'$ tel que f et g_τ n'aient pas de rayons critique autre que $r = 0$ dans l'intervalle $I =]-\epsilon'', \epsilon''[$. Alors :

$$\forall x \in K, \nu(x) \in I, \nu(g_\tau(x)) > \nu(f(x))$$

Par suite, $\nu(f(x)) = \nu(P_\tau(x))$ pour les x considérés ci-dessus.

Soit maintenant $\tau \geq \beta$ tel que $a_\tau \neq 0$ (possible car a_n converge vers zéro). On a alors $deg(P_\tau) = \tau$. Mais K étant supposé algébriquement clos, on a :

$$P_\tau = a_\tau \prod_\xi (X - \xi)$$

Considérons alors les trois ensembles suivants :

- $\Lambda = \Lambda_\tau$ l'ensemble des racines ξ de P_τ vérifiant $\nu(\xi) > 0$.
- $\Lambda' = \Lambda'_\tau$ l'ensemble des racines ξ de P_τ vérifiant $\nu(\xi) = 0$.
- $\Delta = \Delta_\tau$ l'ensemble des racines ξ de P_τ de valuation strictement négatives.

Soit alors $\epsilon = \inf(\epsilon'', \nu(xi), -\nu(\xi))$ (la borne inférieure étant prise pour les ξ racines de P_τ de valuation non nulle. Désignons par J l'intervalle réel centré en 0 de rayon ϵ et dressons le tableau donnant la valuation de $x - \xi$ selon les cas possibles :

	Λ	Δ	Λ'
$-\epsilon < \nu(x) < 0$	$\nu(x)$	$\nu(x)$	$\nu(\xi)$
$\nu(x) = 0$	0	$\nu(x-\xi)$	$\nu(\xi)$
$0 < \nu(x) < \epsilon$	$\nu(x)$	0	$\nu(\xi)$

On en déduit alors :

$$\begin{aligned}\nu(P_\tau(x)) &= \nu(a_\tau) + \mid \Lambda \mid \nu(x) + \sum_{\xi \in \Lambda'} \nu(\xi) \text{ pour } \nu(x) \in J^+ \\ &= \nu(a_\tau) + \mid \Lambda \mid \nu(x) + \sum_{\xi \in \Lambda'} \nu(\xi) + \mid \Delta \mid \nu(x) \text{ pour } \nu(x) \in J^-\end{aligned}$$

où J^+ (respectivement J^-) désigne l'intervalle $J \cap \mathbb{R}^{+\star}$ (resp. $J \cap \mathbb{R}^{-\star}$).

Or, d'après la proposition 3.1.12, on dispose également des relations suivantes :

$$\begin{aligned}\nu(f(x)) &= \alpha\nu(x) \text{ pour } 0 < \nu(x) < \epsilon \\ &= \beta\nu(x) \text{ pour } -\epsilon < \nu(x) < 0\end{aligned}$$

En comparant les résultats trouvés, sachant que $P_\tau(x)$ et $f(x)$ ont même valuation pour $x \in J$, on en déduit successivement que :

$$\begin{aligned}\alpha &= \mid \Lambda \mid \\ \nu(a_\tau) + \sum_{\xi \in \Lambda'} \nu(\xi) &= 0 \\ \delta = \mid \Delta \mid &= \beta - \alpha \\ \nu(P_\tau(x)) &= \sum_{\xi \in \Delta} \nu(x - \xi) \text{ pour } \nu(x) = 0\end{aligned}$$

On remarque que le cardinal de Δ ainsi que celui de Λ ne dépend pas de l'entier τ.

Etape 2 : convergence de la méthode

Si f est un polynôme, pour un entier τ, on a $f = P_\tau$. Comme $\delta > 0$, on en déduit que f a une racine dans la sphère de rayon $R = 0$ et le théorème est démontré.

Si f n'est pas un polynôme, il existe $\tau' > \tau$ tel que $P_{\tau'} = P_\tau + a_{\tau'} x^{\tau'}$ où $a_{\tau'} \neq 0$. On a alors pour tout $x \in K$ vérifiant $\nu(x) = 0$:

$$\nu(P_{\tau'}(x)) = \sum_{\xi' \in \Delta_{\tau'}} \nu(x - \xi')$$

En particulier, pour $x = \xi$ une racine de P_τ dans Δ, on obtient :

$$\begin{aligned}\sum_{\xi' \in \Delta'} \nu(\xi - \xi') &= \nu(P_\tau(\xi) + a_{\tau'}\xi^{\tau'}) \\ &= \nu(a_{\tau'}) \text{ (car } \nu(\xi) = 0)\end{aligned}$$

Par suite, il existe au moins un $\xi' \in \Delta'$ vérifiant :

$$\nu(\xi' - \xi) > \frac{\nu(a_{\tau'})}{\delta}$$

On construit ainsi par récurrence une suite croissante τ_n et une suite $\Delta_n \subset \{x \in K, \nu(x) = 0\}$ ainsi qu'une suite ξ_n vérifiant :

– $\forall n \in \mathbb{N}$, $\xi_n \in \Delta_n$

– $\forall n \in \mathbb{N}$, $\nu(\xi_{n+1} - \xi_n) > \frac{\nu(a_{\tau_{n+1}})}{\delta}$

Mais comme a_n converge vers zéro, il s'ensuit que la suite $(\xi_{n+1} - \xi_n)$ converge également vers zéro. Par suite, (ξ_n) converge. Soit ξ sa limite. Alors $\nu(\xi) = 0$ car $O_\nu^\star = \{x \in K, \nu(x) = 0\}$ est fermé.

De plus par construction,

$$\begin{aligned}f(\xi_n) &= \sum_{i > \tau_n} a_i \xi_n^i \\ \nu(f(\xi_n)) &\geq \inf_{i > \tau_n} (\nu(a_i))\end{aligned}$$

Comme a_n converge vers zéro, il s'ensuit que $f(\xi_n)$ converge vers zéro. Par continuité de f en ξ, on en déduit alors que :

$$f(\xi) = f(\lim_{n \to +\infty} \xi_n) = \lim_{n \to +\infty} f(\xi_n) = 0$$

Ce qui démontre que f a un zéro dans la sphère de rayon $R = 0$ et achève la démonstration du théorème.

Définition 3.1.14 *[14] Une série formelle $f(x) = \sum_{n \geq 0} a_n x^n$ est dîte entière sur K si $\rho(f) = -\infty$.*

Proposition 3.1.15 *[14] Soit f une fonction entière sur K n'ayant pas de zéros. Alors f est constante.*

Preuve :

Si f ne s'annule pas sur K, alors $a_0 = f(0) \neq 0$ et $f(x)$ est de valuation égale à $\nu(a_0)$ jusqu'au premier rayon critique d'après la proposition 3.1.12. Mais d'après le théorème précédent, si f a un rayon critique $r > \rho(f)$ alors f a un zéro dans la sphère. Par suite, f n'a pas de rayon critique. Il s'ensuit que $\nu(f(x)) = \nu(a_0)$ pour tout $x \in K$.

Mais alors, pour tout entier $n > 0$ fixé et tout élément x de K, on a $\nu(a_n) + n\nu(x) > \nu(a_0)$. En faisant tendre $\nu(x)$ vers $-\infty$ (ce qui est possible car $\rho(f) = -\infty$) on en déduit que a_n est nul. Ce qui montre que f est constante.

Corollaire 3.1.16 *[33, 14] Toute fonction entière non constante sur K est surjective.*

Preuve :

Soit $a \in K$. On applique le théorème précédent à la fonction $f - a$ qui reste entière sur K.

Théorème 3.1.17 *[14] Soit f une fonction entière sur K et soit $(\lambda_n)_{n\in\mathbb{N}}$ ses racines non nulles dans K. Alors*

- *(1) $lim_{n\longrightarrow\infty}\nu(\lambda_n) = -\infty$*
- *(2) $f(x) = cx^n \prod_{k\geq 0}(1 - \frac{x}{\lambda_k})$ où c est une constante non nulle de K et n est l'ordre de f en 0.*

Réciproquement, si (λ_n) vérifie la condition (1) précédente et $c \in K \setminus \{0\}$, alors le produit infini précédent est convergent pour tout $x \in K$ et définit une fonction entière.

Corollaire 3.1.18 *Deux fonctions entières ayant les mêmes zéros (avec même multiplicité) sont proportionnelles.*

3.1.3 Caractérisation des polynômes additifs et linéaires

Soit k un corps de caractéristique p et $\bar{k}$ une clôture algébrique fixée de k.

Définition 3.1.19 *[14] Soit $P \in k[X]$. P est dit :*

- *additif sur k si $\forall x, y \in k, P(x + y) = P(x) + P(y)$*
- *absolument additif si P est additif sur $\bar{k}$*

Remarque 3.1.20

- *L'ensemble des polynômes additifs est un k espace vectoriel stable par composition*
- *Soit $\tau = x^p$. Alors τ est absolument additif*

Définition 3.1.21 *[14] On désigne par $k\{\tau\}$ le sous-espace de $k[x]$ engendré par les $(\tau^n, n \in \mathbb{N}^\star)$.*

D'après la remarque précédente, $k\{\tau\}$ est un anneau pour la composition non commutatif si $k \neq \mathbb{F}_p$ puisqu'il vérifie :

$$\forall \alpha \in k, \tau\alpha = \alpha^p\tau$$

On a vu que tout élément de $k\{\tau\}$ est additif et même absolument additif.

La réciproque, à savoir qu'un polynôme additif est un élément de $k\{\tau\}$ n'est pas toujours vraie comme le montre l'exemple suivant :

$k = \mathbb{F}_3$ et $P(x) = x + (x^3 - x)^2 = x^6 + x^4 + x^2 + x$. P est additif puisque si $a \in k, P(a) = a$ alors que $P \notin k\{\tau\}$.

En revanche, si k est infini, on a le résultat suivant :

Proposition 3.1.22 [12] *Soit k un corps infini de caractérisique p. Alors un polynôme $P \in k[X]$ est additif si et seulement si $P \in k\{\tau\}$.*

Preuve :

Il reste uniquement le sens direct. Supposons donc P additif et montrons que $P \in k\{\tau\}$.

Tout d'abord, si $a \in k$, alors le polynôme $P(x+a) - P(x) - P(a)$ a une infinité de racines (puisque k est infini), donc est nul. En calculant sa dérivée en 0, on obtient :

$$P'(a) = P'(0)$$

Ce qui montre que P' est constant. Notons $P' = c$. Il s'ensuit que P s'écrit sous la forme :

$$P(x) = cx + \sum_{i=1}^{s} a_i x^{n_i}$$

où $n_i \equiv 0\ [p]$.

On écrit alors $P(x) = P_0(x) + P_1(x)$ où $P_0 \in k\{\tau\}$. P_1 est la somme des monômes $a_i x^{n_i}$ avec n_i divisible par un nombre premier distinct de p qui apparaîssent dans l'écriture de P. Il s'agit donc de montrer que $P_1 = 0$. On remarque alors pour commencer que P_1 est également additif. De plus, $\tau \in \mathrm{Aut}(\bar{k})$. Soit p^e la plus grande puissance de p qui divise tous les n_i et $P_2(x) = P_1(x)^{\frac{1}{p^e}}$. Maintenant, il est clair que τ^{-1} est encore additif, ce qui montre que P_2 est lui aussi additif. D'après ce qui précède, on a donc $P_2' = 0$. Mais par construction, ceci n'est possible que si P_2 est identiquement nul, ce qui achève la preuve.

On peut aussi caractériser les polynômes additifs en fonction de leur racines :

Théorème 3.1.23 *[14] On suppose k algébriquement clos. Soit $P \in k[x]$ un polynôme séparable et soit $W = \{w_1, \ldots, w_n\} \subset k$ ses racines.*

Alors P est additif si et seulement si W est un sous-groupe de $(k, +)$

Preuve :

Il est clair que si P est additif, alors W est un sous-groupe. Il s'agit donc de démontrer la réciproque. On suppose donc que W est un sous-groupe et montrons que $P(x) = \prod_{i=1}^{n}(x - w_i)$ est additif.

Pour commencer, on constate que si $w \in W$, $P(x+w) = P(x)$. Maintenant, soit $y \in k$ et $H(x) = P(x+y) - P(x) - P(y)$. Il est alors facile de voir que pour tout $w \in W, H(w) = 0$. Comme $\deg H < \deg P = n$, on en déduit que $H(x) = 0$.

Maintenant, si $F(y) = P(x+y) - P(x) - P(y) \in k[x][y] = k[x,y]$ alors d'après ce qui précède, tout élément de k est racine de F. Comme k est infini, on conclut que $F = 0$ et le résultat.

Corollaire 3.1.24 *[14] Sous les conditions du théorème précédent, P est $\mathbb{F}_q$-linéaire si et seulement si W est un $\mathbb{F}_q$-espace vectoriel.*

3.2 Définition algébrique et analytique des modules de Drinfeld

Dans les paragraphes qui suivent, on adopte les notations suivantes : p est un nombre premier, q une puissance de p. On considère $A = \mathbb{F}_q[T]$, $K = \mathbb{F}_q(T)$, $K_\infty = \mathbb{F}_q((T^{-1}))$ (la complétion de K à l'infini) et $\Omega = \hat{\bar{K}}_\infty$, la complétion d'une clôture algébrique fixée de K_∞.

3.2.1 Définition algébrique

Soit τ l'endomorphisme de Frobienus défini sur Ω par $\tau(x) = x^q$. On considère l'anneau non commutatif $\Omega\{\tau\}$ (la règle de commutation étant donnée par $\tau x = x^q \tau$).

Définition 3.2.1 *On appelle module de Drinfeld (voir [33] ; pour une définition plus générale, voir [5, 16]) de rang r sur Ω toute application φ de A dans $\Omega\{\tau\}$ vérifiant les conditions suivantes :*

- *(i) φ est un morphisme d'anneaux*
- *(ii) $deg_\tau \varphi(T) = r$*
- *(iii) $D\varphi(T)(z) = Tz$ où $D\varphi_a(z)$ désigne la partie linéaire*

Remarque 3.2.2 *La définition même de φ entraîne d'une part que pour tout élément a de A, $deg_\tau(\varphi_a) = r\ deg(a)$ et d'autre part que φ est $\mathbb{F}_q$-linéaire.*

Remarque 3.2.3 *Soit $f = \sum_{i=0}^{n} a_i \tau^i \in \Omega\{\tau\}$.*

- *Alors f agit $\mathbb{F}_q$-linéairement sur Ω de manière naturelle, i.e. $f(z) = \sum_{i=0}^{n} a_i \tau^i(z) = \sum_{i=0}^{n} a_i z^{q^i}$. Dans toute la suite, $f(z)$ désignera l'élément précédent.*
- *Le polynôme $\varphi_a(z)$ est séparable de degré $q^{r\,deg(a)}$ dès que a est non nul.*
- *φ est une application injective.*

En effet, on constate que $\mid a \mid_\varphi = \deg_z(\varphi_a(z))$ est une valeur absolue sur A équivalente à la place à l'infini. On peut d'ailleurs montrer que $\mid a \mid_\varphi = \mid a \mid_\infty^r$. Dans le cas plus général, consulter [5, 10, 37].

3.2.2 Définition analytique

Dans le cas des courbes elliptiques, le théorème d'uniformisation de Riemann établit une correspondance entre courbes elliptiques sur $\mathbb{C}$ et réseaux de $\mathbb{C}$. Le cas des modules de Drinfeld est tout à fait analogue :

Théorème 3.2.4 *(Drinfeld)* [14, 33] *Soit φ un module de Drinfeld de rang r. Alors :*

- *(1) Il existe une unique fonction entière sur Ω $e(z) = \sum_{n\geq 0} a_n z^{q^n}$ avec $a_0 = 1$ telle que $\forall a \in A, \forall z \in \Omega, e(az) = \varphi_a(e(z))$.*
- *(2) $\Lambda = Ker(e) = \{z \in \Omega, e(z) = 0\}$ est un A-module libre de rang r et discret.*

Réciproquement, à tout A-réseau de Ω on peut associer un module de Drinfeld :

Théorème 3.2.5 *(Drinfeld)* [14, 33] *Soit Λ un sous-A-module libre de rang r discret de Ω. Alors :*

- *(i) L'application e_Λ de Ω dans Ω définie par $e_\Lambda(z) = z\prod_{a\in\Lambda\setminus\{0\}}(1-\frac{z}{a})$ définit une fonction entière $\mathbb{F}_q$-linéaire sur Ω.*
- *(ii) $\forall a \in A, e_\Lambda(az) = ae(z)\prod_{0\neq\alpha\in a^{-1}\Lambda/\Lambda}\left(1-\frac{e_\Lambda(z)}{e_\Lambda(\alpha)}\right)$*
- *(iii) Pour tout $a \in A$, il existe un unique polynôme $\mathbb{F}_q$-linéaire φ_a tel que $\forall z \in \Omega, e_\Lambda(az) = \varphi_a(e_\Lambda(z))$*
- *(iv) L'application φ qui à un élément $a \in A$ associe le polynôme φ_a est un module de Drinfeld de rang r.*

La fonction e_Λ est l'analogue de la fonction $\wp$ de Weierstrass.

3.2.3 Torsion des modules de Drinfeld

La description analytique des modules de Drinfeld permet d'établir un corollaire très important quant à la structure des points de torsion. En effet, si $a \in A$ non constant est donné, on s'intéresse aux points de a-torsion ${}_a\varphi$, c'est-à-dire aux éléments z de Ω vérifiant $\varphi_a(z) = 0$. Cet ensemble n'est autre que les racines du polynôme $\mathbb{F}_q$-linéaire et séparable φ_a et est donc de cardinal $q^{r\deg a}$. En adoptant la description analytique, considérons le réseau Λ et la fonction e associée par le théorème 3.2.4. On a $e(az) = \varphi_a(e(z))$ et par suite, les points de a-torsion sont isomorphe au quotient de $a^{-1}\Lambda$ par Λ ; d'où le corollaire :

Corollaire 3.2.6 [14] *Si $a \in A \setminus \{0\}$, alors $E_a = ker\varphi_a$ est un $A/(a)$-module libre de rang r .*

3.3 Analogies avec les courbes elliptiques

Dans les paragraphes précédents, on a rappelé les résultats fondamentaux sur les modules de Drinfeld, notant au passage de fortes analogies avec les courbes elliptiques. En fait, les modules de Drinfeld jouent le rôle des courbes elliptiques dans le cadre des corps de fonctions algébriques. Dans cette section, on commence par mettre en évidence ces analogies, puis on étudie les propriétés des isogénies pour aboutir aux résultats profonds de Gekeler [10], et Potémine [37].

3.3.1 Structure des points de torsion

Dans le cas des courbes elliptiques, la description analytique en terme de réseau permet d'établir que si $n \in \mathbb{N}^\star$ est donné, alors le sous-groupe $E(\mathbb{C})[n]$ des points de n-torsion est isomorphe à $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire que $E(\mathbb{C})[n]$ est un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2. Le paragraghe 4.2.3 établit un résultat tout à fait analogue, puisque les points de a-torsion forment pour leur part un $A/(a)$-module libre de rang r.

3.3.2 Isogénies

Dans le cas des courbes elliptiques, l'anneau des endomorphismes d'une courbe elliptique contient beaucoup d'informations importantes. Le cas des modules de Drinfeld est tout à fait analogue. Dans ce paragraphe, on définit les isogénies et on établit les propriétés remarquables.

Soit k un corps sur A, c'est-à-dire un corps muni d'un morphisme de structure $\gamma : A \to k$.

Définition 3.3.1 *Le noyau de γ est appelé la A-caractéristique de k et notée $Car_A(k)$. On écrit $Car_A(k) = \infty$ lorsque γ est injectif.*

Dans ce paragraphe et les suivants, on aura besoin d'une définition un peu plus générale des modules de Drinfeld (voir [5, 10] par exemple) :

Définition 3.3.2 *Un morphisme d'anneaux $A \to k\{\tau\}$ est appelé module de Drinfeld de rang r si pour tout $a \in A$, $deg_\tau(\varphi_a) = r\ deg(a)$ et $D\varphi_a = \gamma(a)$.*

Définition 3.3.3 *Soit φ, ψ deux modules de Drinfeld à coefficients dans k.*
- *Un morphisme de φ dans ψ est un élément $u \in k\{\tau\}$ vérifiant pour tout $a \in A$, $u\varphi_a = \psi_a u$.*
- *Un endomorphisme de φ est un morphisme de φ dans φ.*
- *Une isogénie est un endomorphisme non nul.*
- *La hauteur d'une isogénie u, notée $ht(u)$, est l'unique entier tel que $u = \tau^{ht(u)} u_s$ avec u_s séparable (i.e. $Du_s \neq 0$).*

Exemple 3 *Un cas typique est lorsque l'on prend γ la réduction modulo f. Alors $\Phi_f = \tau^{deg\ f}$ est une isogénie de hauteur $ht(\Phi_f) = deg\ f$.*

On peut alors caractériser les isogénies dans les deux cas suivants :

Théorème 3.3.4 *Soit k un corps qui est soit de A-caractéristique ∞, soit une extension finie de $\mathbb{F}_\mathfrak{p}$ et $u \in k\{\tau\}$. Alors u est une isogénie entre deux modules de Drinfeld φ et φ' à coefficients dans k si et seulement si :*
- *(i) $Ker(u_s)$ est un sous-A-module fini de $\bar{k}$.*
- *(ii) $ht(u) = 0$ si $Car_A(k) = \infty$, et $d_\mathfrak{p} \mid ht(u)$ si $Car_A(k) = \mathfrak{p}$ où l'on a posé $d_\mathfrak{p} = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q]$.*

Preuve :

Si $\varphi' u = u\varphi$, alors la comparaison des parties linéaires montre que pour tout $a \in A$, $\gamma(a) = \gamma(a)^{q^{ht(u)}}$. Ceci implique que :
- *(i)* $ht(u) = 0$ si $\mathrm{Car}_A(k) = \infty$, car alors $\gamma(A)$ est infini.
- *(ii)* Sinon, $\gamma(A) = A/\mathfrak{p} \subset \mathbb{F}_{q^{ht(u)}}$ (c'est un sous corps fixé par $\tau^{ht(u)}$). On conclut en regardant les degrés.

Réciproquement, on considère le corps de fractions $k(\tau)$, vu comme sous corps non commutatif de $k((\tau^{-1}))$. On remarque alors que d'une part, si $u = \varphi_b$ alors $\varphi_b \varphi_a \varphi_b^{-1} = \varphi_a$ puisque l'image de φ est commutative et d'autre part que

si $u = \tau^{ht(u)}$, $\tau^{ht(u)}\varphi_a\tau^{-ht(u)} = \varphi_a^{q^{ht(u)}}$ définit un autre module de Drinfeld φ' sur k puisque $\gamma(a) = \gamma(a)^{q^{ht(u)}}$.

Pour traiter le cas général, on utilise le lemme suivant :

Lemme 3.3.5 *Pour tout polynôme unitaire séparable $u \in k\{\tau\}$ tel que $H = Ker(u)(\bar{k})$ est un sous-A-module, alors il existe un module de Drinfeld φ' sur k vérifiant $\varphi' u = u\varphi$.*

Preuve du lemme :
On distingue deux cas :
- Premier cas : $a \notin \mathfrak{p}$
  Alors φ_a et u sont tous deux séparables et $H' = Ker(u\varphi_a) = \varphi_a^{-1}(H) \supset H$ puisque H est un sous-A-module. De plus, $\mid H' \mid = \mid H \mid \times \deg_z(\varphi_a)$. En posant alors $u(H') = H'' \simeq H'/H$ et
  $$\varphi'_a(z) = \gamma(a)z \prod_{l \in H'' \setminus \{0\}} \left(1 - \frac{z}{l}\right)$$
  Ceci définit un élément $\varphi'_a \in \bar{k}\{\tau\} \cap k(\tau) = k\{\tau\}$ qui vérifie $u\varphi_a = \varphi'_a u$ (ces deux polynômes ont les mêmes racines et même terme constant). On remarque alors que ceci définit bien un morphisme d'anneaux.
- Deuxième cas : $a \in \mathfrak{p}$
  On écrit alors $a = 1 + (a-1)$ avec $(a-1) \notin \mathfrak{p}$ et on applique le premier cas.

Ce qui achève la preuve du lemme.

Corollaire 3.3.6 *Si φ et ψ sont isogènes, alors ils ont le même rang.*

Preuve :
Il suffit de comparer les degrés des polynômes dans l'égalité $u\varphi_T = \psi_T u$.

De même que pour les courbes elliptiques, on dispose de résultats sur la structure des endomorphismes d'un module de Drinfeld :

Théorème 3.3.7 *[10] Soit ψ un module de Drinfeld sur un corps algébriquement clos $\overline{k}$ de rang r. Alors*
- *(1) $End(\psi)$ est un A-module libre de rang $\leq r^2$.*
- *(2) $End(\psi) \otimes_A K_\infty$ est un corps, et il existe une inclusion de $End(\psi)$ comme un sous-A-module discret dans cet espace vectoriel normé sur K_∞.*

3.3.3 Théorème de Potemine : analogue de Hasse

Dans ce paragraphe, on rappelle le théorème de Potemine qui est l'analogue du théorème de Hasse pour les courbes elliptiques. Avant de l'énoncer, on rappelle le cadre et les résultats nécéssaires à la preuve.

On considère un module de Drinfeld $\varphi : A \to k\{\tau\}$, où $\mathfrak{p} = Car_A(k)$ est un idéal maximal de A, k étant une extension finie du corps fini $A/(\mathfrak{p})$. On pose alors $k(\tau) = \mathrm{Frac}(k\{\tau\}) \subset k((\tau^{-1}))$ (corps gauche).

On utilisera les extensions suivantes : $\mathbb{F}_q \subset \mathbb{F}_\mathfrak{p} = A/(\mathfrak{p}) \subset k$, $[k : \mathbb{F}_\mathfrak{p}] = m$, $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d$ (on a donc $\mid k \mid = q^n$ avec $n = md$). On pose alors $\Phi = \tau^n$, et on remarque que Φ commute avec $k\{\tau\}$ et que $\Phi \in End(\varphi)$.

Proposition 3.3.8 *[10] Soit E un corps commutatif intermédiaire $\mathbb{F}_q(\Phi) \subset E \subset k(\tau)$. Alors il existe une seule place de E au dessus des places $\Phi = 0$ et $\Phi = \infty$.*

Soit $\mathfrak{q}$ une place de A. On considère $A_{(\mathfrak{q})}$ le localisé de A en $\mathfrak{q}$, π une uniformisante, $A_\mathfrak{q}$ la complétion de A en $\mathfrak{q}$, $K_\mathfrak{q} = \mathrm{Frac}(A_\mathfrak{q})$ et enfin, le A-module discrèt (qui est également un $A_\mathfrak{q}$-module) :

$$K/A_{(\mathfrak{q})} = \cup_{n\geq 1} \pi^{-n} A_{(\mathfrak{q})}/A_{(\mathfrak{q})} \simeq K_\mathfrak{q}/A_\mathfrak{q}$$

Définition 3.3.9 *On considère une place $\mathfrak{q} \neq \mathfrak{p} = Car_A(k)$. En notant ${}_a\varphi(L)$ les points de a-torsion qui sont dans L, on définit :*

- *(a)*

$$\mathfrak{q}^\infty\varphi = \lim_{\to n} {}_{\mathfrak{q}^n}\varphi(\overline{k}) \cong (\lim_{\to n} A/\mathfrak{q}^n)^r \cong (\lim_{\to n} \mathfrak{q}^{-n}/A)^r = (K_\mathfrak{q}/A_\mathfrak{q})^r$$

  C'est un A-module mais aussi un $A_\mathfrak{q}$-module.
- *(b) On définit alors pour tout module de Drinfeld $\varphi : A \to \mathbb{F}_\mathfrak{p}\{\tau\}$, le module de Tate en place finie $\mathfrak{q}$, que l'on note $T(\varphi)_\mathfrak{q}$, comme le $A_\mathfrak{q}$-module*

$$T(\varphi)_\mathfrak{q} = Hom_{A_\mathfrak{q}}(K_\mathfrak{q}/A_{\mathfrak{q},\mathfrak{q}^\infty}\varphi) \cong \lim_{n\leftarrow} {}_{\mathfrak{q}^n}\varphi(\bar{k}) \cong A_\mathfrak{q}^r$$

Ceci permet de définir une représentation d'algèbre d'endomorphismes :

$$\iota_\mathfrak{q} : End(\varphi) \to End_{A_\mathfrak{q}}(T(\varphi)_\mathfrak{q}) \cong \mathcal{M}_r(A_\mathfrak{q})$$

D'autre part, comme le noyau d'une isogénie est un ensemble fini (ce sont les racines d'un polynôme), l'application $\iota_\mathfrak{q}$ est injective (car sinon, tous les points de $\mathfrak{q}^k$-torsion seraient des racines de u, pour tout entier k).

Mais ceci permet également de définir une représentation galoisienne puisque le groupe de Galois $Gal(\bar{L}/L)$ agit naturellement sur le module de Tate :

$$\rho_\mathfrak{q} : Gal(\bar{L}/L) \mapsto GL_r(A_\mathfrak{q})$$

Nous n'étudierons pas les propriétés de ces représentations.

On dispose alors d'une classification des algèbres d'endomorphismes d'un module de Drinfeld :

Théorème 3.3.10 *[10] Soit $\varphi : A \to k\{\tau\}$ un module de Drinfeld de rang r. φ étant injective, on peut considérer K, comme un sous-corps de $k\{\tau\}$. Soit $L = K(\Phi) \subset End(\varphi) \otimes_A K$. Alors :*

- *(a) Il existe une seule place $\widetilde{\infty}$ de L au-dessus de ∞, et une seule place $\mathfrak{P}$ de L au-dessus de $\mathfrak{p}$.*

– *(b) On pose $r_1 = [L : K]$. Alors $r = r_1 r_2$, $End(\varphi) \otimes_A K$ est une algèbre de division centrale sur L de rang r_2^2, avec seulement deux invariants locaux non nuls :*

$$\begin{aligned} Inv_{L_{\mathfrak{P}}}(End(\varphi) \otimes_L L_{\mathfrak{P}}) &= -\frac{1}{r_2} \text{ en } \mathfrak{P} \\ Inv_{L_{\widetilde{\infty}}}(End(\varphi) \otimes_L L_{\widetilde{\infty}}) &= \frac{1}{r_2} \text{ en } \widetilde{\infty} \end{aligned}$$

Maintenant on peut construire le polynôme caractéristique de Φ associé à chaque représentation $\mathfrak{q}$-adique. On peut constater que les résultats qui suivent, dus à Gekeler, sont tout à fait identiques au cas des courbes elliptiques où l'on peut montrer que le polynôme caractéristique du Frobienus $\mathfrak{p}$ agissant sur le module de Tate associé à un nombre premier $l \notin \mathfrak{p}$ est en fait indépendant de l et à coefficients dans $\mathbb{Z}$. Une étude plus précise permet également d'exprimer la différence entre le nombre de points $\mathbb{F}_q$-rationnels de la courbe elliptique et le nombre de points de la droite projective sur $\mathbb{F}_q$ en fonction de valeurs prises par ce polynôme.

On considère l'application

$$N : End(\varphi) \otimes_A K \to K$$

obtenue comme la composée de la norme réduite $nred : End(\varphi) \otimes_A K \to L$ et de la norme de l'extension de corps commutatifs $N_K^L : L \to K$. Alors N est K-homogène de degré r, et on peut vérifier qu'elle coïncide avec la norme algébrique $N_K^H : H \to K$ sur tout sous-corps commutatif maximal $H \subset End(\varphi) \otimes_A K$, voir [10].

Lemme 3.3.11 *[10] Pour $u \in End(\varphi)$ on a $deg_\tau N(u) = r.deg_\tau u$. En particulier, $deg_\tau N(\Phi) = r.deg_\tau(\tau^n) = rn$.*

Preuve :

Les deux parties définissent les valuations (données par des normes topologiques) sur l'algèbre $K \subset End(\varphi) \otimes_A K$. Les deux parties sont équivalentes à la (seule) valuation ∞-adique. Ceci implique qu'elles diffèrent par une constante, qui se calcule par l'évaluation en $u = \varphi_a$:

$$\deg_\tau N(\varphi_a) = \deg_\tau(N_K^L(\varphi_a^{r_2})) = \deg_\tau(\varphi_a^{r_2 r_1}) = r_1 r_2 \deg_\tau(\varphi_a) = r \deg_\tau(\varphi_a)$$

puisque $r = r_1 r_2$.

Pour tout idéal maximal $\mathfrak{q} \neq \mathfrak{p}$ de A, et pour tout sous-corps commutatif maximal $H \subset End(\varphi) \otimes_A K$, on considère l'anneau commutatif $\iota_\mathfrak{q}(H) \otimes K_\mathfrak{q}$, qui est une sous-algèbre maximale commutative de $End_{K_\mathfrak{q}}(T_\mathfrak{q}(\varphi) \otimes K_\mathfrak{q})$. On utilise ensuite le fait ci-dessus que l'application de norme coïncide sur H avec le déterminant, voir [44, Proposition 11]. Ceci implique que

$$N = \det \circ \iota_\mathfrak{q}$$

Soit $P_\Phi(X)$ le polynôme caractéristique de $\iota_\mathfrak{q}(\Phi)$, et soit $M_\Phi(X)$ le polynôme minimal de Φ sur K :

$$P_\Phi(X) = \det(X.Id_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi))$$

Lemme 3.3.12 *[10] On a $P_\Phi(X) = M_\Phi(X)^{r_2}$, où $r_2 = r/[L:K]$.*

Preuve :

Il suffit de montrer que $P_\Phi(t) = M_\Phi(t)^{r_2}$ pour tous les $t \in L = K(\Phi)$ (c'est un corps infini). Mais

$$P_\Phi(t) = \det(t \cdot Id_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi)) = N_K^L \circ nred(t - \Phi) = N_K^L((t-\Phi)^{r_2}) = M_\Phi(t)^{r_2}$$

puisque $L = K(\Phi)$.

Corollaire 3.3.13 *[10] Les coefficients du polynôme caractéristique $P_\Phi(X) = M_\Phi(X)^{r_2}$ dans la représentation $\iota_\mathfrak{q}$ sont dans A et ne dépendent pas de $\mathfrak{q}$.*

Théorème 3.3.14 *[10] Soit $P_\Phi(X)$ le polynôme caractéristique de $\iota_\mathfrak{q}(\Phi)$ et soit $M_\Phi(X)$ le polynôme minimal de Φ sur A. Alors :*

- *(i) L'idéal principal $(P_\Phi(1))$ de A coïncide avec la caractéristique d'Euler-Poincaré $\chi(k,\varphi)$ du A-module fini k_φ.*
- *(ii) $(P_\Phi(0)) = \mathfrak{p}^m$*
- *(iii) Pour tous les zéros σ_i de $P_\Phi(X)$ on a $\mid \sigma_i \mid_\infty = q^{\frac{n}{r}}$.*

Preuve :

(ii) Nous avons vu que $(P_\Phi(0)) = (N(\Phi))$ appartient à un seul idéal maximal $\mathfrak{p} = (f)$ dans $A = \varphi(A) \subset k\{\tau\}$, puisqu'il existe une seule place $\mathfrak{P}$ de $L = K(\Phi_f)$ divisant Φ, et elle se trouve au-dessus de $\mathfrak{p}$, voir proposition 3.3.8. L'exposant m vient de la formule du produit dans K, du fait que $\deg\Phi = \frac{n}{r}$ et donc $(N(\Phi)) = \mathfrak{p}^m$. En effet, $\deg_\tau(N(\Phi)) = rn$, puisqu'il existe une seule place $\widetilde{\infty}$ de $L = K(\Phi_f)$ au-dessus de ∞. De plus, $\deg_\tau(\mathfrak{p}^m) = \deg(\varphi_{f^m}) = rdm = rn$. Ceci implique (ii).

(iii) On remarque qu'il existe une seule place $\widetilde{\infty}$ de $K(\Phi_f)$ au-dessus de ∞. Ceci implique que toutes les racines w_i du polynôme minimal de Φ sur K ont la même valeur absolue $\mid w_i \mid_{\widetilde{\infty}}$ en $\widetilde{\infty}$, et donc $\mid \sigma_i \mid_\infty = q^{\frac{n}{r}}$.

(i) Enfin, on calcule la $\mathfrak{q}$-composante de l'idéal principal $(P_\Phi(1))$. On considère le A-module fini $M = \mathrm{Ker}(\Phi - 1) = k_\varphi$, et on pose

$$M_\mathfrak{q} = \mathrm{Ker}(\Phi - 1) \cap {}_{\mathfrak{q}^\infty}\varphi(\overline{k}) = {}_{\mathfrak{q}^\infty}\varphi(k)$$

On utilise la notation $(P_\Phi(1))_\mathfrak{q} = (P_\Phi(1))A_\mathfrak{q}$. Alors $M_\mathfrak{q} \cong T_\mathfrak{q}(\varphi)/\mathrm{Im}(\iota_\mathfrak{q}(\Phi - 1))$ et donc :

$$\begin{aligned}(P_\Phi(1))_\mathfrak{q} &= (\det \circ \iota_\mathfrak{q}(\Phi - 1)) \\ &= T_\mathfrak{q}(\varphi)/\mathrm{Im}(\iota_\mathfrak{q}(\Phi - 1)) \\ &= \chi(\mathrm{Ker}(\Phi - 1)_\mathfrak{q}, \varphi) \\ &= \chi({}_{\mathfrak{q}^\infty}\varphi(k), \varphi)\end{aligned}$$

De plus, $\deg_\tau(\Phi - 1) = \deg_\tau \Phi = rn$, donc $(P_\Phi(1))$ et $N(\Phi - 1)$ ont les mêmes valuations $\mathfrak{q}$-adiques, en places $\mathfrak{q} \neq \mathfrak{p}$ et $\mathfrak{q} = \infty$. Donc par la formule du produit, leurs valuations $\mathfrak{p}$-adiques coïncident, d'où (i).

On peut alors énoncer le théorème de Potemine, qui est l'analogue du théorème de Hasse pour les courbes elliptiques. Pour une forme plus générale de ce résultat, voir le texte original de Potemine [37].

Théorème 3.3.15 *[37] Soit $f \in A$, irréductible unitaire et soit $\varphi : A \to A\{\tau\}$. On suppose que la réduction $\bar{\varphi} : A \to A/(f)\{\tau\}$ est encore un module de Drinfeld (pour γ la réduction modulo f et $k = A/(f)$). Alors :*

$$deg(f - f_\varphi) \leq \frac{r-1}{r} deg(f)$$

où f_φ est la caractéristique d'Euler-Poincaré de k.

Preuve :

On applique le théorème 3.3.14 avec ici $\mathfrak{p} = (f)$, $n = d = \deg(f)$ et $m = 1$: $(P_{\Phi_f}(0)) = (f)$ et $(P_{\Phi_f}(1)) = (f_\varphi)$. Mais toujours d'après ce théorème, toutes les racines w_i de P_Φ ont la même valuation ∞. On en déduit donc que :

$$P_{\Phi_f}(1) - P_{\Phi_f}(0) = \sum_{i=0}^{r-1} \Sigma_i(w_1, \ldots, w_r)$$

où Σ_i désigne la $i$ème fonction symétrqiue élémentaire. Mais comme pour tout $1 \leq i \leq r$, $\mid w_i \mid_\infty = \mid f \mid_\infty^{\frac{1}{r}}$, on en déduit bien que :

$$\begin{aligned} \mid f - f_\varphi \mid_\infty &= \mid P_{\Phi_f}(0) - P_{\Phi_f}(1) \mid_\infty \\ &= \mid \sum_{i=0}^{r-1} \Sigma_i(w_1, \ldots, w_r) \mid_\infty \\ &\leq \text{Max} \mid \Sigma_i(w_1, \ldots, w_r) \mid_\infty \\ &\leq \mid f \mid_\infty^{\frac{r-1}{r}} \end{aligned}$$

Ce qui achève la preuve du théorème.

3.3.4 Tableau d'analogie

Pour résumer les résultats des derniers paragraphes et les mettre en parallèle avec leurs analogues dans le cas des courbes elliptiques, il est pratique de faire le tableau d'analogies qui suit :

$\mathbb{Z}$	$\longleftrightarrow$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$\longleftrightarrow$	$k = \mathrm{Frac}(A) = \mathbb{F}_q(T)$
places finies de $\mathbb{Q}$	$\longleftrightarrow$	places finies de K
les nombres premiers		les polynômes irréductibles
une seule place infinie	$\longleftrightarrow$	une seule place infinie
$\mid x \mid = \mid x \mid_\infty$		$\mid f/g \mid_\infty = q^{\deg f - \deg g}$
$\mathbb{R}$	$\longleftrightarrow$	$k_\infty = \mathbb{F}_q((T^{-1}))$
$\mathbb{C}$	$\longleftrightarrow$	$\Omega = \hat{\bar{k}}_\infty$
$\mathbb{Z}-$ module	$\longleftrightarrow$	$A-$ module
E (courbe elliptique)	$\longleftrightarrow$	φ (module de Drinfeld sur A)
K corps de nombres	$\longleftrightarrow$	L extension finie de k
E définie sur K	$\longleftrightarrow$	φ défini sur L
groupe abélien $\mathrm{Hom}(E, E')$	$\longleftrightarrow$	$A-$ module $\mathrm{Hom}(\varphi, \psi)$
anneau $\mathrm{End}_{\mathbb{Q}}(E)$	$\longleftrightarrow$	anneau $\mathrm{End}_k(\varphi)$
algèbre $\mathrm{End}_{\mathbb{Q}}(E) \otimes \mathbb{Q}$	$\longleftrightarrow$	algèbre $\mathrm{End}_k(\varphi) \otimes_A k$
Λ réseau de $\mathbb{C}$	$\longleftrightarrow$	$A-$ module libre et discret Λ
$E(\mathbb{C})[n]$	$\longleftrightarrow$	${}_a\varphi(\Omega)$
$\mathbb{Z}/n\mathbb{Z}-$ module		$A/(a)-$ module de rang r
module de Tate $T_l(E)$	$\longleftrightarrow$	module de Tate $T_{\mathfrak{q}}(\varphi)$
polynôme caractéristique du Frobienus	$\longleftrightarrow$	polynôme caractéristique
$P_{\mathfrak{p},l}$		$P_{\Phi,\mathfrak{q}}$
indépendant de l	$\longleftrightarrow$	indépendant de $\mathfrak{q}$
$P_{\mathfrak{p},l}(0) = \mathrm{Card}(k_{\mathfrak{p}})$	$\longleftrightarrow$	$(P_{\Phi,\mathfrak{q}}(0)) = (\mathfrak{p})^m$
$P_{\mathfrak{p},l}(1) = \mathrm{Card}(E(k_{\mathfrak{p}}))$	$\longleftrightarrow$	$(P_{\Phi,\mathfrak{q}}(1)) = \chi(k, \varphi)$
théorème de Hasse	$\longleftrightarrow$	théorème de Potemine

Chapitre 4

Etude de la torsion des modules de Drinfeld

Soit A une variété abélienne définie sur un corps de nombres K. Le théorème de Mordell-Weil [7] établit que $A(K)$ est un groupe abélien de type fini, c'est-à-dire que $A(K) \simeq A(K)_{tor} \times \mathbb{Z}^r$, où $A(K)_{tor}$ est le groupe fini des points de torsion K-rationnels et r un entier ≥ 0. De nombreuses questions restent encore ouvertes. Par exemple, si on fixe la dimension g, et le corps de nombres K, existe-t-il des variétés abéliennes A, définies sur K et de dimension g, de rang arbitraire ? Même pour $g = 1$ et $K = \mathbb{Q}$ ou $\mathbb{Q}(t)$, on ne dispose pas de réponse définitive. Les résultats dans cette direction ont été initiés par Néron [31], mais surtout Mestre [27, 28, 29], puis Fermigier [8], Nagao [30] (voir également [18, 23]).

En ce qui concerne la torsion, la conjecture de la borne uniforme affirme la chose suivante : soient d, g des entiers ≥ 1, alors il existe un entier $B(d, g) \geq 1$ tel que pour toute variété abélienne A de dimension g définie sur un corps de nombres K de degré d, $\mid A(K)_{tor} \mid \leq \ B(d, g)$.

Pour $g \geq 2$, cette conjecture est encore ouverte, et l'on ne dispose essentiellement que de résultats montrant que certains groupes sont des groupes de torsion de Jacobiennes de courbes de genre g [9, 20, 32].

En revanche, pour $g = 1$, qui correspond au cas des courbes elliptiques, cette conjecture est maintenant un théorème, dû à Merel ([26] ; voir également [6, 34] ainsi que [22] pour des résultats sur la p-torsion).

Pour d petit, on dispose de résultats précis sur le groupe des points rationnels de torsion d'une courbe elliptique E définie sur un corps de nombres de degré d, et qui ont été obtenus historiquement avant ceux de Merel. En particulier, pour $d = 1$ (pour $d = 2$, voir les résultats de Kamienny [17]), le théorème de Mazur [24] donne la liste des quinze groupes $E(\mathbb{Q})_{tor}$ possibles.

Ce chapitre, dont les résultats se trouvent dans [11], s'attache à certaines de ces questions. Dans un premier temps, nous précisons la structure induite par un module de Drinfeld. Dans un second temps, nous étudions la torsion d'un

module de Drinfeld et obtenons un analogue du théorème de Mazur et donc de la conjecture de la borne uniforme dans ce cas. Plus précisement, nous montrons que pour un $\mathbb{F}_q[T]$-module de Drinfeld rationnel, le module des points de torsion sur $\mathbb{F}_q[T]$ est isomorphe à l'un des modules suivants :

- (i) Si $q = 2$: $\{0\}$, $\mathbb{F}_q[T]/(T)$, $\mathbb{F}_q[T]/(T+1)$, $\mathbb{F}_q[T]/(T^2+T)$.
- (ii) Si $q > 2$, $\{0\}$, $\mathbb{F}_q[T]/(T-a)$, pour $a \in \mathbb{F}_q$.

Enfin, dans la dernière partie, nous obtenons d'une part un analogue du théorème de Merel et d'autre part nous retrouvons et précisons dans un cadre plus restreint un résultat de Poonen [35]. Plus précisement, nous montrons que si $n \geq 1$ est fixé, il existe une constante $C(q,n)$ ne dépendant que de q et n telle que, pour tout anneau B entier et de type fini sur $\mathbb{F}_q[T]$ vérifiant $[L : \mathbb{F}_q(T)] \leq n$, où L désigne le corps des fractions de B, et pour tout $\mathbb{F}_q[T]$-module de Drinfeld B-rationnel, le module des points de torsion B-rationnels est de cardinal $\leq C(q,n)$. Nous montrons qu'une valeur convenable pour $C(q,n)$ est $q^{\frac{nq}{q-1}}$.

4.1 Groupe de Mordell-Weil d'un module elliptique de Drinfeld

On se place ici dans le cas où $\varphi : A \to A\{\tau\}$ et on considère la nouvelle structure de A-module sur A induite par φ :

$$\begin{aligned} A \times A &\to A \\ (a,x) &\to a.x = \varphi_a(x) \end{aligned}$$

A^φ désignera dans ce qui suit l'ensemble A muni de cette structure de A-module : c'est l'analogue du groupe de Mordell-Weil pour les variétés abéliennes. A^φ_{tor} désignera le A-module de torsion.

Dans les généralités, on a vu que si l'on considère un module de Drinfeld à valeurs dans $\Omega\{\tau\}$, alors pour tout $a \in A$ non nul, les points de a-torsion forment un $A/(a)$-module libre de rang r. En particulier, on a une infinité de points de torsion. Dans le cas présent, c'est-à-dire le cas où φ est à valeurs dans $A\{\tau\}$ (φ est A-rationnel), on peut remarquer les deux choses suivantes :

Proposition 4.1.1 *Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld de rang r. Alors :*

- *(1) A^φ_{tor} est fini.*
- *(2) A^φ n'est pas de type fini sur A.*

Remarque : Nous proposons ici une démonstration élémentaire et constructive, différente de celle de [4, 36, 42], où ces résultats sont établis dans un cadre plus général.

Notons $\varphi_T = b_0 + b_1\tau + \cdots + b_r\tau^r$ où $b_0 = T$, $b_i \in A$ pour $i \geq 1$ et $b_r \neq 0$. Lorsque $a \in A$ est de degré suffisamment élevé, on a $\deg(\varphi_T(a)) = \deg(b_r) + q^r\deg(a)$. Ce qui montre que a n'est pas de torsion. Ceci établit le premier point : à savoir que A^φ_{tor} est fini.

Montrons à présent que A^φ n'est pas de type fini. Pour cela, on va exhiber une famille infinie d'éléments de A qui soit A-libre.

On note $b = \deg(b_r)$, $b \geq 0$ puisque φ est de rang r. Considérons alors la suite d'entiers i_n définie par $i_0 = b - 1 + \lambda q$ (où λ est un entier tel que T^{i_0} ne soit pas de torsion), et $i_{n+1} = i_n + q$.

Lemme 4.1.2 *La suite $(T^{i_n})_{n\in\mathbb{N}}$ est une famille A-libre de A^φ.*

On raisonne par l'absurde. Supposons que $\sum_{m=0}^{n} A_m.T^{i_m} = 0$ où $A_i \in A$ (non tous nuls). Par définition de A^φ, ceci équivaut à : $\sum_{m=0}^{n} \varphi_{A_m}(T^{i_m}) = 0$ Mais par construction, T^i_m n'est pas de torsion pour tout entier m. D'après ce qui précède, on a donc pour tout indice m apparaissant dans la somme pour lequel $A_m \neq 0$, en posant $a_m = \deg(A_m)$: $\deg(\varphi_{A_m}(T^{i_m})) = \frac{q^{a_m r}-1}{q^r-1} b + q^{a_m r} i_m$ Montrons alors que ces degrés sont deux à deux distincts. Ceci permettra de conclure puisque dans ce cas le degré de la somme sera non nul (puisque au moins A_m est non nul), ce qui contredit la nullité de cette même somme. On suppose donc que : $\frac{q^{a_m r}-1}{q^r-1} b + q^{a_m r} i_m = \frac{q^{a_l r}-1}{q^r-1} b + q^{a_l r} i_l$. En multipliant cette expression par $q^r - 1$ (qui est non nul), on obtient : $q^{a_m r} b - b + (q^r - 1) q^{a_m r} i_m = q^{a_l r} b - b + (q^r - 1) q^{a_l r} i_l$. Soit encore :

$$((q^r - 1) i_m + b)\, q^{a_m r} = ((q^r - 1) i_l + b)\, q^{a_l r}$$

On distingue alors deux cas :

- $a_m = a_l$: dans ce cas, on a $i_m = i_l$, ce qui n'est pas possible pour deux indices l et m distincts.
- $a_m \neq a_l$: quitte à échanger les indices, on peut supposer $a_m < a_l$. Dans ce cas, l'équation précédente peut s'écrire sous la forme :

  $$(q^r - 1) i_m + b = ((q^r - 1) i_l + b)\, q^{(a_l - a_m) r}$$

  Mais le membre de gauche de la dernière égalité est congru à zéro modulo q (puisque $a_l - a_m > 0$) alors que le membre de droite vérifie :

  $$(q^r - 1) i_m + b \equiv -i_m + b \bmod q \equiv 1 \bmod q$$

  Ce qui est impossible. Ceci montre bien que les degrés sont deux à deux distincts et achève la preuve du lemme.

4.2 Structure de $\mathbb{F}_q[T]^\varphi_{tor}$

Dans ce paragraphe, nous étudions le A-module A^φ_{tor} qui est fini d'après ce qui précède. En appliquant la méthode précédente (consistant à évaluer le degré de $\varphi_T(a)$ en fonction du degré de a), on peut montrer que pour $r = 1$, la torsion est majorée par q si $q \neq 2$ et par 4 si $q = 2$. En revanche, il est facile de vérifier que pour $r = 2$ la torsion est majorée par q. En étudiant de manière précise le comportement du degré de $\varphi_T(a)$ en fonction du degré de a, on peut montrer que la torsion est majorée par $q^{\mathrm{Max}(2,r)}$.

Mais la borne précédente n'étant pas optimale (pour $r = 2$ par exemple) on cherche à l'améliorer. Dans ce paragraphe, nous montrons d'abord que la borne uniforme est indépendante de r et nous donnons les structures possibles de A^φ_{tor}. Le théorème suivant est une sorte d'analogue (beaucoup plus élémentaire) du théorème de Mazur évoqué précédemment.

Théorème 4.2.1 *Pour tout module de Drinfeld A-rationnel de rang r, on a :*

- *(1) Si $q = 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q^2$.*
  De plus A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :
  $$\{0\} \ , \ A/(T) \ , \ A/(T+1) \ , \ A/(T(T+1))$$

- *(2) Si $q > 2$, alors $\mid A^{\varphi}_{tor} \mid \leq q$.*
  De plus A^{φ}_{tor} est isomorphe (en tant que A-module) à l'un des modules suivants :
  $$\{0\} \ , \ A/(T-\alpha) \text{ avec } \alpha \in \mathbb{F}_q$$

De plus, si l'on fixe $r \geq 1$ ($r \neq 2$ si $q = 2$) et B l'un des modules cycliques précédents, il existe un module de Drinfeld de rang r dont la torsion est isomorphe à B.

On commence par démontrer deux lemmes :

Lemme 4.2.2 *Soit f un polynôme non constant et P un point de f-torsion pour φ (de rang r quelconque). Alors :*

$$P \neq 0 \Rightarrow P^{q-1} \mid f^s$$

pour un entier $s \geq 1$.

En effet, soit $n = \deg(f)$ et $s \geq 1$. Il existe $c_1, \ldots, c_{nrs} \in A$ tels que :

$$\varphi_{f^s} = f^s + \sum_{i=0}^{nrs} c_i \tau^i$$

Maintenant, si P est un point de f-torsion non nul, alors il existe un s tel que :

$$0 = \varphi_{f^s}(P) = f^s P + \textstyle\sum_{i=0}^{nsr} c_i P^{q^i} = P(f^s + \sum_{i=0}^{nrs} c_i P^{q^i - 1})$$

P étant non nul et A intègre, on en déduit que :

$$f^s = -\textstyle\sum_{i=0}^{nsr} c_i P^{q^i - 1} = P^{q^{i_0}-1}(-\sum_{i=i_0}^{nsr} c_i P^{q^i - q^{i_0}})$$

où i_0 est le plus petit entier tel que $c_{i_0} \neq 0$ (un tel entier existe puisque c_{nrs} est non nul).

Il s'ensuit que P^{q-1} divise f^s (puisque $(q-1)$ divise $(q^{i_0} - 1)$) et le lemme est démontré.

Lemme 4.2.3 *Soit $f \in A$ unitaire irréductible et $A^{\varphi}[f]$ le A-module des points de f-torsion (i.e. annulés par une puissance de f). Alors*

$$dim_{\mathbb{F}_q}(A^{\varphi}[f]) \leq 1$$

Tout d'abord, notons que, φ_a étant $\mathbb{F}_q$-linéaire pour tout $a \in A$, les points de f-torsion forment bien un $\mathbb{F}_q$-espace vectoriel.

Supposons que $\dim_{\mathbb{F}_q}(A^{\varphi}[f]) \geq 2$. Soit alors (P_1, P_2) une famille $\mathbb{F}_q$-libre de $A^{\varphi}[f]$. Quitte à les multiplier par une constante non nulle, on peut les supposer

unitaires. Pour $i \in \{1,2\}$, P_i est un point de f-torsion donc d'après le lemme précédent, on en déduit que P_i^{q-1} divise f^{α_i} pour un entier $\alpha_i \geq 1$. P_i étant unitaire et f unitaire irréductible, il s'ensuit que $P_i = f^{a_i}$ où a_i est un entier vérifiant $(q-1)a_i \leq \alpha_i$. On distingue alors deux cas :

- Si $a_1 = a_2$ alors $P_1 = P_2$ ce qui contredit le fait que (P_1, P_2) est une famille $\mathbb{F}_q$-libre.
- Sinon, quitte à échanger les indices $a_1 < a_2$. Mais alors

$$P_1 + P_2 = f^{a_1}(1 + f^{a_2 - a_1})$$

  Or $P_1 + P_2$ est également un point de f-torsion donc divise une puissance de f d'après le lemme précédent, ce qui est contradictoire avec la dernière égalité.

Ceci achève la preuve du lemme. Terminons à présent la preuve du théorème : on désigne par S l'ensemble A_{tor}^{φ} muni de sa structure de $\mathbb{F}_q$-espace vectoriel. De plus, A_{tor}^{φ} étant fini, il est a fortiori de dimension finie sur $\mathbb{F}_q$: soit n cette dimension. Par ailleurs, soit $\Phi \in \mathrm{End}_{\mathbb{F}_q}(S)$ défini par $\Phi(P) = \varphi_T(P)$, M_Φ son polynôme minimal et $M_\Phi = f_1^{\alpha_1} \dots f_s^{\alpha_s}$ la décomposition de M_Φ en facteurs irréductibles. Alors :

$$S \simeq \bigoplus_{i=1}^{s} A^{\varphi}[f_i]$$

En effet, A_{tor}^{φ} est la somme directe des modules de f-torsion (la somme étant prise sur tous les polynômes irréductibles unitaires) mais si f est irréductible et distinct des f_i ,$1 \leq i \leq s$, alors il existe $u, v \in A$ tels que $uf + vM_\Phi = 1$. En appliquant cette égalité à Φ, on en déduit donc que $\varphi_u \varphi_f = \mathrm{Id}_S$. Par suite, $A^{\varphi}[f]$ est réduit à zéro. En regardant alors les dimensions, il vient :

$$n = \dim_{\mathbb{F}_q}(S) = \dim_{\mathbb{F}_q}(\bigoplus_{i=1}^{s} A^{\varphi}[f_i]) = \sum_{i=1}^{s} \dim_{\mathbb{F}_q}(A^{\varphi}[f_i]) \leq \sum_{i=1}^{s} 1 \leq s$$

Mais l'inégalité inverse découle du fait que le degré de M_Φ est inférieur ou égal à n (Cayley-Hamilton). Par suite, $s = n$, $\forall i \in \{1, \dots, n\}$, $\alpha_i = 1$, $\deg(f_i) = 1$ et $\dim_{\mathbb{F}_q}(A^{\varphi}[f_i]) = 1$.

Ceci entraîne donc que

$$A_{tor}^{\varphi} \simeq \bigoplus_{i=1}^{n} A/(T - a_i)$$

où l'on a posé $f_i = T - a_i$ pour tout entier $1 \leq i \leq n$. On distingue maintenant deux cas :

- Si $q > 2$

  Pour $1 \leq i \leq n$, soit P_i un générateur de $A^{\varphi}[f_i]$, alors d'après le lemme, $P_i^{q-1} \mid (T - a_i)$. Par suite, P_i est constant donc $A_{tor}^{\varphi} \subset \mathbb{F}_q$ et $n \leq 1$. De plus, si $n = 1$, alors $A_{tor}^{\varphi} \simeq A/(T - \alpha)$ pour $\alpha \in \mathbb{F}_q$. Ce qui démontre le point (2) du théorème.

– Si $q = 2$
Le même raisonnement montre que les générateurs de $A^{\varphi}[f_i]$ sont de degré inférieur ou égal à un. Par suite $n \leq 2$.
De plus, si $n = 1$, alors d'après la décomposition de S trouvée ci-dessus, les points de torsions sont isomorphes au quotient de A par un polynôme de degré 1, i.e. par T ou $T + 1$ (car $q = 2$).
Enfin, si $n = 2$, A^{φ}_{tor} est isomorphe $A/(T - a) \oplus A/(T - b)$. Mais ces facteurs sont premiers entre eux (ce sont les facteurs irréductibles de M_{Φ}). Par suite, $A^{\varphi}_{tor} \simeq A/((T+1)T)$ (puisque $q = 2$). Ce qui démontre le point (1) du théorème.

En ce qui concerne le point (3), il est facile de vérifier que :
– Si $q > 2$ alors pour tout $r \geq 1$
  – pour $\varphi_T = T + (\alpha - T)\tau^r$, $A^{\varphi}_{tor} \simeq A/(T - \alpha)$.
  – pour $\varphi_T = T + \tau^r$, $A^{\varphi}_{tor} = \{0\}$.

– Si $q = 2$ et $r \geq 3$:
  – pour $\varphi_T = T + (T^{2^r-2} + 1)\tau + \tau^r$ alors $A^{\varphi}_{tor} \simeq A/(T)$.
  – pour $\varphi_T = T + T\tau + \tau^r$ alors $A^{\varphi}_{tor} \simeq A/(T + 1)$.
  – pour $\varphi_T = T + g_r\tau + g_r\tau^2 + \tau^r$ où l'on a posé $g_r = \sum_{i=0}^{2^{r-1}-2} T^{2^i}$ alors $A^{\varphi}_{tor} \simeq A/(T(T + 1))$.
  – pour $\varphi_T = T + \tau^r$ alors $A^{\varphi}_{tor} = \{0\}$.
– Si $q = 2$ et $r = 1$:
  – pour $\varphi_T = T + \tau$ alors $A^{\varphi}_{tor} \simeq A/(T(T + 1))$.
  – pour $\varphi_T = T + T\tau$ alors $A^{\varphi}_{tor} \simeq A/(T)$.
  – pour $\varphi_T = T + (T + 1)\tau$ alors $A^{\varphi}_{tor} \simeq A/(T + 1)$.
– Si $q = 2$ et $r = 2$, il est facile de constater que dans ce cas particulier, la torsion est majorée par q et :
  – pour $\varphi_T = T + T\tau^2$ alors $A^{\varphi}_{tor} \simeq A/(T)$.
  – pour $\varphi_T = T + (T + 1)\tau^2$ alors $A^{\varphi}_{tor} \simeq A/(T + 1)$.
  – pour $\varphi_T = T + \tau^2$ alors $A^{\varphi}_{tor} \simeq \{0\}$.
Ce qui achève la démonstration du théorème.

4.3 Borne uniforme pour les extensions entières finies de $\mathbb{F}_q[T]$

Dans ce paragraphe, on démontre un analogue beaucoup plus élémentaire du théorème de Merel évoqué plus haut.

Théorème 4.3.1 *Soit $n \geq 1$ fixé. Alors pour tout anneau B entier et de type fini sur A vérifiant $[L : k] \leq n$ (où L désigne le corps de fractions de B) et pour tout module de Drinfeld B-rationnel φ,*

$$| B^{\varphi}_{tor} | \leq \ q^{\frac{nq}{q-1}}$$

Preuve :

Soit B comme dans l'énoncé du théorème et φ un module de Drinfeld B-rationnel de rang $r \geq 1$. On a alors par définition, $\varphi_T = b_0 + b_1\tau + \cdots + b_r\tau^r$ où $b_0 = T$, $b_i \in B$ pour $1 \leq i \leq r$ et $b_r \neq 0$. Considérons ω la valuation discrète de k associée au polynôme T et soit ν une valuation discrète de L au-dessus de ω. On note O_ω (resp. O_ν) l'anneau de valuation de ω (resp. ν) et π_ω (resp. π_ν) une uniformisante pour ω (resp. ν). On notera par la suite $e = e(\nu/\omega)$ l'indice de ramification de ν par rapport à ω, et $f = f(\nu/\omega)$ le degré résiduel.

On remarque alors pour commencer que d'une part, $A \subset O_\omega$, et d'autre part $B \subset O_\nu$ (puisque B est entier sur A). On a alors :

$$\nu(b) > \frac{e}{q-1} \quad \Rightarrow \quad \nu(\varphi_T(b)) = \nu(b) + e$$

Ceci montre que les points de torsion sont de valuation comprise entre 0 et $\frac{e}{q-1}$. Soit N la partie entière de $\frac{e}{q-1}$ et $B_i = B_{tor}^\varphi \cap \{x \in L, \nu(x) \geq i\}$ pour $0 \leq i \leq N$. On constate alors d'une part que $\dim_{\mathbb{F}_q}(B_N) \leq f$, et d'autre part que pour tout $0 \leq i \leq N-1$, $\dim_{\mathbb{F}_q}(B_i/B_{i+1}) \leq f$. Par suite,

$$\dim_{\mathbb{F}_q}(B_{tor}^\varphi) = \sum_{i=0}^{N-1} \dim_{\mathbb{F}_q}(B_i/B_{i+1}) + \dim_{\mathbb{F}_q}(B_N) \leq (N+1)f$$

On en déduit donc que $\mid B_{tor}^\varphi \mid \ \leq q^{(N+1)f} \leq q^{\frac{ef}{q-1}+f} \leq q^{\frac{qn}{q-1}}$, ce qui achève la preuve du théorème.

En revanche, contrairement au cas $B = A$, le module B_{tor}^φ n'est pas nécessairement cyclique. Il est d'ailleurs assez élémentaire de construire un anneau B vérifiant les hypothèses du théorème précédent et tel que la torsion contienne un module donné :

Proposition 4.3.2 *Soient $r \geq 2$ et $k \geq 1$ deux entiers fixés, f_i $(1 \leq i \leq k)$ des polynômes irréductibles distincts, $e_i \leq r$ $(1 \leq i \leq k)$ des entiers et φ un module de Drinfeld unitaire en τ (ou dont le coefficient dominant est premier avec chaque f_i). Alors il exsite B une extension finie entière de A telle que $B_{tor}^\varphi \supset \bigoplus A/(f_i)^{e_i}$.*

Preuve :

Il suffit de considérer $B_i =_{f_i} \varphi$. D'après les hypothèses, c'est une extension finie entière de A pour chaque $1 \leq i \leq k$, qui contient tous les points de f_i-torsions, c'est-à-dire $A/(f_i)^r$ et donc $A/(f)^{e_i}$ puisque $e_i \leq r$. $B = \prod_{i=1}^r B_i$ convient.

4.4 Conjecture de la borne uniforme : une preuve pour $r = 1$

Jusqu'ici nous nous sommes intéréssés aux modules de Drinfeld à coefficients entiers. Il est naturel de se demander si ces résultats s'étendent au cas des

extensions finies de $\mathbb{F}_q(T)$. On ne peut cependant pas s'attendre à trouver des bornes identiques. En effet, nous avons démontré que la torsion des modules de Drinfeld à coefficients entiers est bornée uniformément, indépendamment du rang. Ceci n'est plus vrai lorsque les coefficients ne sont plus entiers (ou si l'on ne se restreint plus aux points de torsions qui sont entiers. En effet, si W est un sous-espace vectoriel de dimension finie r de $k = \mathbb{F}_q(T)$, alors $P = \prod_{w \in W}(X - w)$ est un polynôme $\mathbb{F}_q$-linéaire, donc de la forme $P_0 x + ... + P_r x^{q^r}$. En considérant $\varphi_T = T + ... + \frac{P_r}{P_0}\tau^r$, on constate que la torsion contient W, donc est de cardinal au moins q^r.

Parmi les questions ouvertes, citons les conjectures suivantes [35] :

Conjecture 4.4.1 *Soit $r \geq 1$ et L une extension finie de $k = Frac(A)$ fixés. Alors il existe une constante $B(r, L)$ telle que pour tout module de Drinfeld L-rationnel de rang r, le cardinal de L^{φ}_{tor} soit majoré par $B(r, L)$.*

Conjecture 4.4.2 *Soit $r \geq 1$ et $d \geq 1$ fixés. Alors il existe une constante $B(r, d)$ telle que pour toute extension finie de k de degré inférieur ou égal à d et pour tout module de Drinfeld rationnel de rang r, le cardinal de L^{φ}_{tor} soit majoré par $B(r, d)$.*

Poonen [35] a démontré que la conjecture 4.4.2 est vraie pour $r = 1$ dans un cadre plus général : à savoir lorsque A désigne l'anneau des fonctions régulières d'une courbe affine obtenue en retirant un point fermé "∞" d'une courbe projective lisse X définie sur $\mathbb{F}_q$.

La méthode précédente permet de retrouver et de préciser ce résultat lorsque $A = \mathbb{F}_q[T]$:

Corollaire 4.4.3 *Soit $n \geq 1$ alors pour toute extension finie L de k de degré $\leq n$ et pour tout module de Drinfeld de rang 1 L-rationnel, le cardinal de L^{φ}_{tor} est majoré par $q^{\frac{nq}{q-1}}$.*

Soit L/k une extension de degré $\leq n$ et φ un A-module de Drinfeld L-rationnel de rang 1. Notons $\varphi_T = T + B\tau$ où $B \in L^{\star}$. Soit ω la valuation normalisée de k associée au polynôme T et ν un prolongement de ω à L. On note e (respectivement f) l'indice de ramification (resp. le degré résiduel) de ν par rapport à ω. De même que précédemment, on remarque que :

$$\begin{aligned} \nu(x) > \frac{e - \nu(B)}{q-1} \quad &\Rightarrow \quad \nu(\varphi_T(x)) = \nu(x) + e \\ \nu(x) < \frac{-\nu(B)}{q-1} \quad &\Rightarrow \quad \nu(\varphi_T(x)) < \nu(x) \end{aligned}$$

On en déduit donc que les points de torsion L-rationnels sont de valuation comprise entre $\frac{-\nu(B)}{q-1}$ et $\frac{e-\nu(B)}{q-1}$. Mais ν est à valeurs entières. Par suite, il y a au plus $\frac{e}{q-1} + 1$ valeurs de $\nu(x)$ pour lesquelles x peut être un point de torsion. Le même raisonnement que précédemment permet alors de conclure que $\dim_{\mathbb{F}_q}(L^{\varphi}_{tor}) \leq f(\frac{e}{q-1} + 1) \leq \frac{nq}{q-1}$, ce qui achève la preuve du corollaire.

Chapitre 5

Applications des polynômes irréductibles et bijectifs à la cryptologie

5.1 Structure induite par un module de Drinfeld

Soit φ un module de Drinfeld de rang r, à coefficients dans A. Soit $f \in A$ non nul fixé, alors φ induit une nouvelle structure de A-module sur le quotient $A/(f)$, notée $A/(f)_\varphi$:

$$\begin{array}{rcl} A \times A/(f)_\varphi & \to & A/(f)_\varphi \\ (a, \bar{x}) & \mapsto & \overline{\varphi_a(x)} \end{array}$$

On peut remarquer que cette action est bien définie car si $P \in (f)$, alors $\varphi_a(P) \in (f)$ pour tout a dans A.

On peut remarquer que ce A-module n'est pas toujours cyclique, sauf dans le cas particulier où $r = 1$. En effet,

Proposition 5.1.1 *Soit φ un module de Drinfeld de rang 1, alors $A/(f)_\varphi$ est cyclique.*

Preuve :

En effet, en considérant $\gamma : A \to A/(f)$ la réduction modulo f, on obtient un nouveau module de Drinfeld $\psi : A \to A/(f)\{\tau\}$. Maintenant, si g est irréductible, et si x vérifie $\varphi_g(x) \equiv 0 \bmod f$, alors, ceci fournit un point de g-torsion pour ψ. Mais on a vu que les points de g-torsion forment un $A/(g)$-module libre de rang $r' \leq r$, ce qui montre ici que dans le cas $r = 1$, ${}_g\psi$ est monogène. Par conséquent, $A/(f)_\varphi$ est cylique.

Dans le cas $r \geq 2$, l'exemple suivant montre que ce module n'est pas toujours cyclique : il s'agit d'un exemple de la thèse de Potemine [37]. Considérons $q =$

$p = 3$, $f = T^2 + 1$, et $\varphi_T = T - T\tau^2$, alors il est facile de vérifier que $A/(f)_\varphi \cong A/(T) \times A/(T)$. En effet, $\varphi_T(1) = 0$, $\varphi_T(T) = T^2 - T^{10} = T(T - T^9) \equiv 0 \bmod T^2 + 1$, d'où le résultat.

5.2 Calcul de la caractéristique d'Euler-Poincaré

5.2.1 Définition

Dans le chapitre 4, nous avons utilisé la caractéristique d'Euler-Poincaré d'un A-module fini. Nous rappelons ici la définition formelle :

Définition 5.2.1 *Soit $\mathcal{M}$ l'ensemble des A-modules finis. On définit alors une fonction χ, appelée caractéristique d'Euler-Poincaré, de $\mathcal{M}$ dans l'ensemble des idéaux de A par les deux règles suivantes :*

- *(i) Si $\mathfrak{p} \in Spec(A)$ et $M \cong A/\mathfrak{p}$, alors $\chi(M) = \mathfrak{p}$,*
- *(ii) Si $0 \to M_1 \to M \to M_2 \to 0$, alors $\chi(M) = \chi(M_1)\chi(M_2)$.*

On peut constater que ceci définit bien χ. En effet, d'une part, pour tout idéal premier $\mathfrak{p}$ de A, on a les suites exactes suivantes pour tout entier n :

$$0 \to A/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1} \to A/\mathfrak{p}^{n+1} \to A/\mathfrak{p}^n \to 0$$

Ceci permet d'établir par récurrence que $\chi(A/\mathfrak{p}^n) = \mathfrak{p}^n$. D'autre part, tout A-module fini se décompose en somme directe de module cyclique de la forme $A/\mathfrak{p}^n$. D'où le résultat en utilisant à nouveau (ii).

Mais dans le cadre de notre étude, l'anneau $A = \mathbb{F}_q[T]$ est principal. On peut donc identifier la caractéristique d'Euler-Poincaré d'un A-module M avec un générateur unitaire de $\chi(M)$. De manière plus précise, soit M un A-module fini. D'après la structure des modules sur un anneau principal, on en déduit qu'il existe des éléments $f_1, \ldots, f_s \in A$ et des entiers $e_1, \ldots, e_s$ tels que :

$$M \simeq \bigoplus_{i=1}^{s} A/(f_i^{e_i})$$

Dans ce cas, en posant $f_\varphi = \prod_{i=1}^{s} f_i^{e_i}$, on obtient que $(f_\varphi) = \chi(M)$. En supposant f_φ unitaire, on peut donc identifier f_φ et la caractéristique d'Euler-Poincaré de M.

5.2.2 Calcul pratique

Dans le paragraphe précédent, on a rappelé la définition formelle de la caractéristique d'Euler-Poincaré d'un A-module. On s'intéresse maintenant au calcul pratique. L'inconvéniant de la définition précédente est qu'elle nécéssite la connaissance de la décomposition du module en modules cycliques, ce qui d'un point de vue pratique est un inconvéniant majeur. D'autant plus que si le module est ¨grand¨, ces calculs deviennent vite très onéreux en temps et en mémoire, ce qui est génant si l'on souhaite utiliser les modules de Drinfeld en cryptographie.

Le principe est le suivant : soit $f \in A$, non nul. On a donc en conservant les notations du paragraphe précédent :

$$\begin{aligned} A/(f)_\varphi &\cong \bigoplus_{i=1}^{s} A/(f_i^{e_i}) \\ f_\varphi &= \prod_{i=1}^{s} f_i^{e_i} \end{aligned}$$

Mais par définition de l'isomorphisme, il s'ensuit que φ_T agit sur $\bigoplus_{i=1}^{s} A/(f_i^{e_i})$ tout simplement par multiplication par T. Il s'ensuit que f_φ ne représente rien d'autre que le polynôme caractéristique de φ_T (considéré comme élément de $End_{\mathbb{F}_q}(A/(f))$) puisque sur chaque module cyclique $A/(f_i^{e_i})$, la matrice de multiplication par T est la matrice compagnon du polynôme $f_i^{e_i}$. Ceci fournit une méthode élémentaire pour le calcul pratique de f_φ.

Exemple 4 *Considérons le polynôme $f = T^2 + T + 1$ irréductible sur $\mathbb{F}_2$, et soit $\varphi_T = T + T\tau$ et $\psi_T = T + T\tau^2$. On a alors :*

$$\begin{aligned} \varphi_T(1) &= T + T \\ &= 0 \\ \varphi_T(T) &= T^3 + T^2 \\ &\equiv T \ mod\ f \end{aligned}$$

$$\begin{aligned} \psi_T(1) &= 0 \\ \psi_T(T) &= T^2 + T^5 \\ &\equiv 0 \ mod\ f \end{aligned}$$

D'où l'on déduit que les matrices de φ_T et de ψ_T considérés comme des éléments de $End_{\mathbb{F}_q}(A/(f))$ sont respectivement : $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

On conclut alors en prenant les polynômes caractéristiques normalisés (ce qui est déjà le cas ici puisque la dimension est paire) que $f_\varphi = f - 1 = T^2 + T$ et $f_\psi = T^2$.

5.2.3 Cas du module de Carlitz

Définition 5.2.2 *On appelle module de Carlitz le module de Drinfeld sur A, défini par $\varphi_T = T + \tau$.*

Dans ce cas, on peut calculer explicitement la fonction e associé à ce module de Drinfeld :

Proposition 5.2.3 *Soit φ le module de Carlitz. Alors la fonction entière associée $e = \sum a_n z^{q^n}$ vérifie : $a_0 = 1$ et $\forall n \geq 1, a_n = \frac{a_{n-1}^q}{T^{q^n} - T}$. C'est-à-dire,*

$$\begin{aligned} a_n &= \left(\prod_{i=1}^{n} (T^{q^i} - T)^{q^{n-i}} \right)^{-1} \\ &= \left(\prod_{g \in S_n} g \right)^{-1} \end{aligned}$$

où S_n désigne l'ensemble des polynômes unitaires de degré n.

Remarque 5.2.4 *$D_n = \prod_{g \in S_n} g$ peut être interprété comme le factoriel $n!$.*

Preuve :
Seule la dernième égalité est à démontrer, les deux premières étant des conséquences immédiates des définitions.

Soit f un polynôme irréductible unitaire de degré $d \leq n$. D'après le lemme 1.1.2, $T^{q^i} - T$ est égal au produit de tous les polynômes irréductibles unitaires de degré j divisant i. En notant a (respectivement b) le quotient (resp. le reste) de la division de n par d, et en remarquant que $T^{q^i} - T$ est séparable, on en déduit que :

$$\begin{aligned} -\nu_f(a_n) &= \sum_{i=1}^{n} q^{n-i} \nu_f(T^{q^i} - T) \\ &= \sum_{i=1}^{a} q^{n-id} \\ &= q^b \frac{q^{ad} - 1}{q^d - 1} \end{aligned}$$

Déterminons à présent la multiplicité de f dans D_n. Pour cela, on va déterminer le nombre de polynômes unitaires de degré n qui sont divisibles exactement par f^i pour tout entier i compris entre 1 et a.

- Nombre de polynômes divisibles par f^a exactement
  Si g est unitaire de degré n et divisible par f^a exactement, alors g s'écrit $g = f^a h$ où h est unitaire de degré b. Comme $b < d$, tout tel polynôme h est premier avec f. On en déduit donc qu'il y a exactement q^b polynômes unitaires de degré n ayant une multiplicité en f égale à a.
- Soit $1 \leq i \leq a - 1$. Déterminons le nombre de polynôme ayant une multiplicité en f égale à $a - i$. Pour un tel g, on a alors $g = f^{a-i} h$ où h est unitaire de degré $id + b$, et premier à f. Or le nombre de polynôme unitaire de degré $id + b$ divisible par f est $q^{(i-1)d+b}$. On en déduit donc que le nombre de polynôme unitaire de degré n ayant une multiplicité en f égale à $a - i$ vaut $q^{id+b} - q^{(i-1)d+b}$.

On en déduit alors successivement :

$$\begin{aligned}
\nu_f(D_n) &= aq^b + \sum_{i=1}^{a-1}(a-i)(q^{id+b} - q^{(i-1)d+b}) \\
&= aq^b + a(q^{(a-1)d+b} - q^b) - \sum_{i=1}^{a-1} i(q^{id+b} - q^{(i-1)d+b}) \\
&= aq^{(a-1)d+b} - \sum_{i=1}^{a-1} iq^{id+b} + \sum_{i=1}^{a-1} iq^{(i-1)d+b} \\
&= aq^{(a-1)d+b} + q^b - (a-1)q^{(a-1)d+b} + \sum_{i=1}^{a-2} q^{id+b} \\
&= \frac{q^b}{q^d-1}\left((q^d-1)q^{(a-1)d} + (q^d-1) + q^d(q^{(a-2)d}-1)\right) \\
&= \frac{q^b(q^{ad}-1)}{q^d-1}
\end{aligned}$$

Ainsi, pour tout polynôme irréductible unitaire de degré $d \leq n$, a_n et D_n ont la même multiplicité en f. De plus, il est clair que si f est irréductible de degré strictement plus grand que n, f ne divise ni a_n, ni D_n. De plus, a_n et D_n étant unitaires, on en déduit l'égalité, ce qui achève la preuve de la proposition.

La fonction e associée au module de Carlitz est appelée exponentielle de Carlitz. Cette appellation provient de l'analogie avec la fonction exponentielle classique. En effet, les coefficients de e sont données par l'inverse du produit de tous les polynômes unitaires de degré n, c'est-à-dire par l'inverse du factoriel.

Pour terminer ce paragraphe, nous allons démontrer que la caractéristique d'Euler-Poincaré associée au module de Carlitz se calcule en fait très simplement :

Proposition 5.2.5 *[12] Soit f irréductible unitaire et φ le module de Carlitz. Alors :*

$$f_\varphi = f - 1$$

Preuve :

D'après le théorème 3.3.15, $f_\varphi = f - a$ où $a \in \mathbb{F}_q$. Mais φ_{f_φ} est identiquement nulle sur $A/(f)$ par définition, il s'ensuit donc que φ_f agit par aId sur $A/(f)$.

D'autre part, comme $\varphi_T = T + \tau$, on en déduit que sur $A/(f) = \mathbb{F}_q(\alpha)$, $\varphi_T = m_\alpha + \sigma$ et que $\varphi_f = f + \sum_{k=1}^{n-1} P_k\tau^k + \tau^n$ où les $P_k \in A$, soit encore $\varphi_f = \sum_{k=1}^{n-1} P_k(\alpha)\sigma^k + \sigma^n$. Par conséquent, $Id + \sum_{k=1}^{n-1} P_k(\alpha)\sigma^k = aId$. Mais d'après le lemme d'indépendance de Dedekind, on en déduit que $a = 1$, ce qui achève la preuve de la proposition.

Cette méthode se généralise très légèrement aux modules de Drinfeld de rang $r = 1$:

Proposition 5.2.6 *Soit $\varphi_T = T + g\tau$ un module de Drinfeld de rang 1 avec $g \in A \setminus \{0\}$ et f un polynôme irréductible unitaire de degré n. Désignons par $\alpha \in \mathbb{F}_{q^n}$ une racine de f. Alors :*

$$f_\varphi = f - N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g(\alpha))$$

Preuve :

Toujours d'après le théorème 3.3.15, $f_\varphi = f - a$ pour un certain $a \in \mathbb{F}_q$. D'où en appliquant la même méthode que dans la proposition précédente, on en déduit que a est égal au coefficient en τ^n de φ_f. Mais comme f est de degré n et unitaire, ce coefficient vaut $g^{\sum_{i=0}^{n-1} q^i}$, il s'ensuit que $a = g(\alpha)^{\sum_{i=0}^{n-1} q^i}$, ce qui n'est rien d'autre que la trace de $g(\alpha)$ sur $\mathbb{F}_q$.

Cette méthode de calcul de la caractéristique d'Euler-Poincaré n'est pas toujours efficace, dépendant de la "complexité" du polynôme g. En revanche, lorsque g est un monôme, cette proposition permet de calculer très facilement f_φ puisque si $g = \lambda T^k$ avec $\lambda \in \mathbb{F}_q^\star$ et $k \geq 0$, alors $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g(\alpha)) = \lambda^n N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)^k$.

Mais comme la norme de α est égale (à $(-1)^n$ près) au terme constant de f, il n'y a aucun calcul à faire : en notant par a le terme constant de f, il s'ensuit que $f_\varphi = f - (-1)^{nk}\lambda^n a^k$.

5.2.4 Application au corps finis

Théorème 5.2.7 *[12] Soit α un élément primitif de $\mathbb{F}_{q^n}/\mathbb{F}_q$ et σ le Frobienus. En désignant par m_α l'endomorphisme de multiplication par α, alors :*

$$det(m_\alpha + \sigma) = det(m_\alpha) + det(\sigma)$$

Preuve :

Soit φ le module de Carlitz, α un élément primitif de $\mathbb{F}_{q^n}/\mathbb{F}_q$ et f le polynôme minimal de α. D'après la proposition 5.2.5, on a donc $f_\varphi = f - 1$ puisque f est irréductible. En conservant les notations précédentes, et en évaluant les deux polynômes précédents en zéro, il vient :

$$\begin{aligned} f_\varphi(0) &= (-1)^n \det\,(\varphi_T) \\ &= (-1)^n \det\,(m_\alpha + \sigma) \\ f(0) - 1 &= (-1)^n N_{\mathbb{F}_{q^n}}(\alpha) - 1 \\ &= (-1)^n \left(\det\,(m_\alpha) + (-1)^{n+1}\right) \\ &= (-1)^n \left(\det\,(m_\alpha) + \det(\sigma)\right) \end{aligned}$$

D'où le résultat en simplifiant par $(-1)^n$.

Dans le cas particulier où $q = 2$, on peut montrer le résultat légèrement plus fort mais plus élémentaire :

Proposition 5.2.8 *Soit $\alpha \in \mathbb{F}_{2^n}$ (plus nécessairement primitif) et σ le Frobienus de $\mathbb{F}_{2^n}/\mathbb{F}_2$. Alors :*

$$det(m_\alpha + \sigma) = det(m_\alpha) + det(\sigma)$$

Preuve :

Si $\alpha = 0$, il n'y a rien à démontrer. On suppose donc $\alpha \neq 0$. Dans ce cas, m_α et σ sont inversibles et leur déterminant est non nul. Comme $q = 2$, chaque déterminant vaut 1. La proposition est donc équivalente à ce que $m_\alpha + \sigma$ n'est pas inversible, soit encore qu'il existe un élément non nul $x \in \mathbb{F}_{2^n}$, tel que $\alpha x + \sigma(x) = 0$. Ce qui est trivialement le cas : $x = \alpha$ convient.

5.2.5 Application à la factorisation des polynômes

A l'aide des modules de Drinfeld, on peut construire un analogue de l'algorithme de Lenstra [33, 37]. En effet, soit $f \in A$ un polynôme que l'on cherche à factoriser. Soit g un facteur irréductible inconnu de f. Supposons que la caractéristique d'Euler-Poincaré de g soit k-lisse pour un entier k donné, c'est-à-dire que g_φ divise D_k (le factoriel k). Alors φ_{D_k} agit par 0 sur le quotient $A/(g)$. Il s'ensuit que pour tout polynôme P, $\varphi_{D_k}(P) \wedge g = g$. Ainsi en calculant le pgcd de φ_{D_k} et f, on trouvé un facteur non trivial.

L'avantage, tout comme l'algorithme de Lenstra, est qu'on dispose ici d'un grand choix pour le module de Drinfeld. On utilise alors la méthode d'abandon rapide.

5.3 Application à la cryptologie

La cryptographie théorique est une science qui étudie les systèmes d'échange d'information protégé. Depuis des siècles, les hommes n'ont cessé de chercher des techniques pour mieux protéger leurs communications et échanger les clés secrètes. Mais ce n'est qu'en 1976, que W. Diffie et M. Hellman ont découvert un nouveau type de cryptographie : la cryptographie à clé secrète, dont l'exemple le plus connu (et encore massivement utilisé aujourd'hui), RSA, date de 1978.

La sécurité des cryptosystèmes à clé publique est en général fondée sur des problêmes mathématiques difficiles à résoudre dans la pratique, comme par exemple la factorisation des entiers (comme RSA ou le protocole d'échange de Diffie-Hellman) ou le problême du logarithme discret dans le groupe multiplicatif d'un corps fini, ou dans le groupe des points rationnels d'une courbe elliptique sur un corps fini.

Depuis quelques années maintenant, les modules de Drinfeld ont fait leur apparition en cryptographie. Les premières tentatives qui consistaient à prendre les analogues des problêmes déjà existants et de les transposer au cas des modules de Drinfeld, comme le problême du logarithme discret par exemple, ont été des echecs (voir [39]). En recanche, dans un travail récent, R. Gillard, F. Leprévost, A. Panchishkin et X-F. Roblot [13] ont proposé un nouveau modèle de cryptosystème à clé publique basé sur les modules de Drinfeld. Dans ce dernier paragraphe, on rappelle comment fonctionnent les différents protocoles existants ainsi que le problême mathématique sur lequel la sécurité de chacun de ceux-ci dépend, puis on décrit ce nouveau cryptosystème. Le cadre est le même

que précédemment à cette nuance près : dans le protocole pratique, on prendra $q = p$ est un nombre premier, et non plus une puissance d'un nombre premier.

5.3.1 Fonction sens unique à trappe

D'un point de vue théorique, on peut modéliser la cryptographie comme suit : on considère deux ensembles finis $\mathcal{E}$ et $\mathcal{F}$ (dans la pratique, il est souvent plus facile de prendre $\mathcal{E} = \mathcal{F} = \mathcal{M}$, où $\mathcal{M}$ désigne l'ensemble des messages). Le cryptage d'un message est obtenu en prenant l'image par $f : \mathcal{E} \mapsto \mathcal{F}$ du message $x \in \mathcal{E}$, où f est une fonction bijective. Le décryptage est fait en calculant l'image réciproque du message crypté. Dans ces conditions, il est bien évident que la sécurité des transmissions dépend fortement de la fonction f choisie. Afin de pouvoir "quantifier" cette sécurité, on est amené à définir les notions de fonction sens unique (FSU) et fonction sens unique à trappe (FSUT) comme suit :

Définition 5.3.1 *Soit f une fonction de $\mathcal{E}$ dans $\mathcal{F}$, bijective.*

- *(i) On dit que f est une fonction sens unique si la seule donnée de $y \in \mathcal{F}$ et de f ne permet pas de calculer $x = f^{-1}(y)$.*
- *(ii) On dit que f est une fonction sens unique à trappe si c'est une FSU telle qu'il existe une information supplémentaire, la clé secrète $\mathcal{K}$, qui permet de calculer facilement l'inverse par f de tout élément.*

Les exemples de FSU et de FSUT sont nombreux et plus ou moins facile à construire, nous en donnerons quelques uns dans les paragraphes suivants.

5.3.2 Principaux protocoles

Le protocole RSA (Rivest, Shamir, Adleman [1])

Soient p et q deux nombres premiers distincts (de préférence de grande taille pour améliorer le niveau de sécurité) et $n = pq$. On considère ici $\mathcal{E} = \mathcal{F} = \{0, \ldots, n-1\}$. Soit e un entier premier avec $\varphi(n) = (p-1)(q-1)$ (φ désigne ici l'indicatrice d'Euler). On définit alors une fonction f en posant $f(x) = x^e \bmod n$. Cette fonction est effectivement bijective par choix de e (il est premier avec l'ordre du groupe $\mathbb{Z}/n\mathbb{Z}^\star$).

Considérons à présent l'entier d vérifiant $ed \equiv 1 \bmod \varphi(n)$. il est alors clair que $f^{-1}(x) = x^d$. En effet, pour $x \wedge pq = 1$, $x^{ed} \equiv x \bmod n$ d'après le théorème d'Euler-Fermat et si par exemple p divise x, alors d'une part q ne divise pas x sinon $x \geq n$ ne pourrait appartenir à $\{0, \ldots, n-1\}$, et d'autre part, on a en posant $ed = 1 + t(p-1)(q-1)$:

$$\begin{aligned} x^{ed} &= x(x^{(p-1)t})^{q-1} \\ x^{ed} &\equiv x \bmod q \\ &\equiv 0 \bmod p \end{aligned}$$

d'où l'on déduit par le lemme chinois que $x^{ed} \equiv x \bmod pq$

Sous ces conditions, il est facile de constater que f est une FSUT, la clé secrète étant l'entier d. Connaissant n et e, trouver d est équivalent à connaître

les entiers p et q, c'est-à-dire la factorisation de l'entier n. La sécurité de ce protocole dépend donc de la difficulté à factoriser un nombre.

Le grand avantage de RSA par rapport aux cryptosystèmes préexistant est qu'il s'agit de cryptographie à clé publique. Chaque personne A choisit deux nombres premiers distincts p_A, q_A, un entier e_A premier avec $\varphi(n_A)$ et publie sa clé publique : (n_A, e_A). Toute personne peut alors envoyer un message crypté à A, en calculant x^{e_A}. En revanche, seul l'utilisateur A peut décrypter ce message en utilisant sa clé secrète (n_A, d_A).

Le protocole ElGamal

Le protocole d'ElGamal s'applique dans n'importe quel groupe cyclique fini. Dans la pratique, le groupe G est soit le groupe multiplicatif $\mathbb{F}_q^\star$, soit le groupe $E(\mathbb{F}_q)$ des points d'une courbe elliptique sur un corps fini. Certains ont proposé de prendre pour G la Jacobienne d'une courbe de genre plus élevé, mais en fait la sécurité du protocole suivant diminue lorsaue le genre est supérieur ou égal à 3. C'est pour cette raison que dans la pratique, on se limite aux deux exemples cités ci-dessus.

On fixe g un générateur de G et on note N le cardinal de G. On prend $\mathcal{E} = G$ et $\mathcal{F} = G \times G$. Alice choisit aléatoirement un entier $a \in \{0, \dots N-1\}$ et calcule g^a. Sa clé publique est alors (G, g, g^a), la clé secrète est $\mathcal{K} = a$. Pour crypter un message $x \in G$ qu'il souhaite envoyer à Alice, Bob choisit un entier k au hasard dans $\{0, \dots, N-1\}$ et calcule $y_1 = g^k$ puis $y_2 = x(g^a)^k$. Le message crypté est le couple (y_1, y_2). En d'autres termes, la fonction de cryptage FSUT est donnée par :

$$f(x) = (g^k, xg^{ak})$$

Pour décrypter le message, Alice calcule $f^{-1}(y, z) = y^{-a}z$, qui n'est calculabl que si l'on connait la clé secrète a.

La sécurité de ce protocole repose sur la difficulté de résoudre le problême du logarithme discret (DLP), c'est-à-dire de retrouver l'entier a connaissant g et g^a. C'est un problême difficile dans la plupart des cas. Pour l'anecdote, c'est d'ailleurs sur le DLP sur une courbe elliptique que repose la sécurité des cartes bancaires actuelles.

Le protocole d'échange de clés de Diffie-Hellman

Dans l'état actuel des connaissances et des technologies, la cryptographie à clé publique est relativement lente comparée aux cryptosystèmes à clés secrètes. Il est donc intéressant de voir comment on peut mélanger ces deux principes : c'est le cas du protocole d'échange de clés de Diffie-Hellman. On utilise la cryptographie à clé publique pour partager une clé secrète, puis on crypte les messages en utilisant la clé secrète que l'on partage. Voici le protocole plus en détail : on suppose publique un groupe cyclique fini G, ainsi qu'un générateur g. Alice choisit un entier a au hasard, compris entre 0 et $N-1$ (N désigne à nouveau le

cardinal de G), Bob choisit également un entier b au hasard. Alic rend publique g^a, et Bob fait de même avec g^b. Alors Alice et Bob partagent une clé secrète : g^{ab}. La sécurité de ce protocole d'échange de clés repose sur l'hypothèse de Diffie-Hellman :
Hypothèse de Diffie-Hellman : Connaissant g^a et g^b, on ne peut calculer g^{ab}.

Il est bien entendu que si l'on sait résoudre le DLP, alors on sait résoudre l'hypothèse de Diffie-Hellman. En revanche, la réciproque, à savoir que si l'on sait résoudre l'hypothèse de Diffie-Hellamn, on sait résoudre le DLP, reste une question ouverte à ce jour.

5.3.3 Signatures électroniques

Un des problêmes les plus important qui apparait en cryptologie est l'authenticité : comment peut-on s'assurer que le message provient bien de la bonne personne? En 1991, le gouvernement des Etats-Unis d'Amérique a proposé un standard pour la signature électronique des messages, le DSS (Digital Signature Standard). Il s'agit d'un protocole similaire à celui d'ElGamal que nous décrivons ici.

On conserve les notations précédentes. Bob souhaite signer son message afin qu'Alice puisse être sûre de l'authenticité du message. Pour cela, en utilisant sa clé secrète b, Bob calcule $z = (x + bg^k)k^{-1}$. Il signe le message x avec (g^k, z). Alice calcule alors $u = xz^{-1}$ et $v = g^k z^{-1}$ et n'a plus qu'à vérifier que $w = g^u g^{bv}$ est bien égal à g^k. Alice connait bien g^b puisqu'il s'agit de la clé publique de Bob.

5.3.4 Utilisation des modules de Drinfeld en cryptologie

Etant donné les fortes analogies existant entre courbes elliptiques et modules de Drinfeld, il est logique de se demander si l'on peut transposer aux modules de Drinfeld les cryptosystèmes déjà existant. De nombreuses tentatives ont donné lieu à des cryptosystèmes utilisant les modules de Drinfeld, mais dont la sécurité jusqu'ici était très insatisfaisante, en particulier pour le DLP dans les modules de Drinfeld (voir Scanlon [39]). Dans ce dernier paragraphe, on présente les travaux de Gillard, Leprévost, Pantchichkine et Roblot [13], qui ont trouvé un moyen d'utiliser efficacement les modules de Drinfeld en cryptologie.

Soit f un polynôme irréductible sur $\mathbb{F}_q$ de degré d et considérons le A-module $A/(f)_\varphi$, que l'on notera B par la suite. Il s'agit de prendre $\mathcal{E} = \mathcal{F} = B$ et de trouver de nouvelles FSUT sur B. On peut déjà constater les deux choses suivantes :

Proposition 5.3.2 *Soit M le polynôme minimal de $\varphi_T \in \mathcal{L}_{\mathbb{F}_q}(A/(f))$. Alors*
- *(i) $\varphi_a = \varphi_b$ en tant qu'applications de B dans lui-même si et seulement si $a \equiv b \bmod M$. En particulier, si $a \equiv b \bmod f_\varphi$, alors $\varphi_a = \varphi_b$*
- *(ii) φ_a est bijective si et seulement si a est premier avec f_φ. De plus, dans ce cas, l'inverse de φ_a est donné par φ_b, où $b \in A$ vérifie $ab \equiv 1 \bmod f_\varphi$.*

Preuve :

Pour (i), c'est clair puisque par définition du polynôme minimal, $\varphi_a = a(\varphi_T)$ est identiquement nulle si et seulement si M divise a. De plus, comme f_φ a les mêmes facteurs irréductibles que M, avec des multiplicités plus grandes, il s'ensuit bien que si f_φ divise a, alors M divise a.

Pour (ii), on constate évidement que $\varphi_a = a(\varphi_T)$ est inversible si et seulement si $a \wedge M = 1$. Mais comme dans (i), $a \wedge M = 1$ si et seulement si $a \wedge f_\varphi = 1$. Puis, dans ces conditions, en utilisant la relation de Bézout, il existe deux polynômes u et v tels que $ua + vf_\varphi = 1$, d'où le résultat en prenant l'image par φ.

Remarque 5.3.3 *Il est en revanche faux que si $\varphi_a = \varphi_b$ sur B alors $a \equiv b \bmod f_\varphi$, comme le montre l'exemple suivant : comme dans le paragraphe* 6.1*, on prend $q = 3$, $f = T^2 + 1$ et $\varphi_T = T - T\tau^2$. Alors $f_\varphi = T^2$ et $B \simeq A/(T) \oplus A/(T)$. Par suite φ_T est nulle sur B bien que $T \not\equiv 0 \bmod T^2$.*

Remarque 5.3.4 *Ceci fournit donc une infinité de polynômes bijectifs. Il suffit de prendre φ_a avec a premier avec f_φ.*

La dernière proposition permet de construire une nouvelle fonction sens unique à trappe, en se servant des modules de Drinfeld. En effet, on considère alors la clé secrète (c_1, σ, c_2), composée de deux éléments de A, c_1 et c_2 tous deux premiers avec f_φ et d'une bijection σ de B. On obtient ainsi une fonction sens unique à trappe : $\psi = \varphi_{c_1} \circ \sigma \circ \varphi_{c_2}$, dont la bijection réciproque est donnée par $\psi^{-1} = \varphi_{c_2'} \circ \sigma^{-1} \circ \varphi_{c_1'}$, où $c_i c_i' \equiv 1 \bmod f_\varphi$.

Pour la fonction σ, il faut tout de même choisir une fonction simple et rapide à calculer. Dans [13], les auteurs sugèrent de prendre $\sigma(z) = z^e + \delta$, où e est un entier premier avec $p(p^d - 1)$ et δ un élément de B choisi aléatoirement. La fonction inverse est alors donnée par $\sigma^{-1}(z) = (z-\delta)^f$, avec $ef \equiv 1 \bmod (p^d - 1)$.

Les procédés de cryptage et de décryptage sont obtenus comme suit :

- Cryptage :
  Soit M un message à crypter. On commence par le transformer en un élément de B : on écrit $M = \sum_{k=0}^{d-1} m_k p^k$ (écriture en base p), puis on lui associe de manière unique l'élément $\mu = \sum_{k=0}^{d-1} m_k T^k \bmod f_\varphi \in B$.
  Le message crypté est alors obtenu en calculant le polynôme $\chi = \psi(\mu) = \sum_{i=0}^{d-1} k_i T^i \bmod f_\varphi$, et en lui associant le nombre $C = \sum_{i=0}^{d-1} k_i p^i$.
- Décryptage :
  On fait la même chose que le cryptage, sauf qu'on applique ψ^{-1}.

Dans leur article [13], les auteurs proposent des choix des paramètres, notamment sur le choix du nombre premier p, de la fonction σ et du module de Drinfeld. En particulier, ils suggèrent l'utilisation du module de Carlitz. Mais nous avons démontré que dans ce cas, $f_\varphi = f - 1$ (proposition 5.2.5), ce qui permet donc de réduire les calculs préliminaires. De même, en prenant n'importe quel module de Drinfeld de rang $r = 1$, on peut également utilisé la proposition 5.2.6 pour calculer f_φ rapidement.

Bibliographie

[1] Adleman, L.M., Rivest, R.L., et Shamir, A. : *A method for obtaining Digital Signatures and Public-Key Cryptosystems* (CACM, 21 (1978), p. 120-126)

[2] Cassels, H.W. et Fröhlich, A. : *Algebraic Number Theory* (Academic Press 1967)

[3] Deligne, P. et Husemöller, D. : *Survey of Drinfeld modules* (Contemp. Math. 67 (1987), p. 25-91)

[4] Denis, L. : *Hauteurs canoniques et modules de Drinfeld* (Math. Ann. 294 (1992),p. 213-223)

[5] Drinfeld, D. : *Elliptic modules* (Math. USSR Sb., 23 (1974), p. 561-592)

[6] Edixhoven, B. : *Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur)* (Séminaire Bourbaki 782, Vol. 1993/94, Astérisque No. 227 (1995), Exp No. 782, 4, p. 209-227)

[7] Faltings, G. : *Finiteness theorems for abelian varieties over number fields* (Invent. Math. 73 (1983), no. 3, p. 349-366)

[8] Fermigier, S. : *Une courbe elliptique définie sur* $\mathbb{Q}$ *de rang* ≥ 22 (Acta Arithmetica, LXXXII (1997), 4, p. 359-363)

[9] Flynn, E.V. :*Large rational torsion on abelian varieties* (J. Number Theory 36, p. 257-265)

[10] Gekeler, E.U. : *On finite Drinfeld Modules* (Journal of Algebra 141 (1991), p. 187-203)

[11] Gewirtz, A. : *Torsion des modules de Drinfeld à coefficients entiers* (Prépublication n^o 602 de l'Institut Fourier (2003))

[12] Gewirtz, A. : *Torsion des modules de Drinfeld à coefficients entiers* (Soumis pour publication)

[13] Gillard, R., Leprévost, F., Panchishkin, A. et Roblot, X-F. : *Utilisation des modules de Drinfeld en cryptologie* (C.R.A.S. Paris, t. , série I, théorie des nombres.)

[14] Goss, D. : *Basic Structures of Function Field Arithmetic* (Springer 1998)

[15] Hasse, H. : *Number Theory* (Springer Classics in Mathematics) (2002) (Reprint of the 1980 edition)

[16] Hayes, D. : *A brief introduction to Drinfeld modules* (The Arithmetic of Function Fields, ed. D. Goss, D.R. Hayes, et M.I. Rosen, de Gruyter, Berlin 1992)

[17] Kamienny, S. : *Torsion points on elliptic curves over all quadratic fields* (Duke Math. J. 53 (1986), no. 3, p. 545-551)

[18] Kihara, S. : *On an elliptic curve over $\mathbb{Q}(t)$ of rank ≥ 14* (Proc. Japan Acad, Ser A, Math. Sci 77 (2001),p. 50-51)

[19] Koch,H. : *Algebraic Number Theory (second edition)* (Springer 1997)

[20] Leprévost, F. : *Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 2$* (Manuscripta Math. 92 (1997), no. 1, p. 47-63)

[21] Lidl, R. et Niederreiter, H. : *Introduction to finite fields and their applications* (Cambridge University Press 1986)

[22] Manin, J. : *The p-torsion of elliptic curves is uniformly bounded* (Math. USSR - Izvestija 3 (1969) p. 433-438)

[23] Martin, R. et Mc-Millen, W. : *An Elliptic Curve over $\mathbb{Q}$ with rank ≥ 24* (Number Theory Listserver, May 2000)

[24] Mazur, B. : *Modular curves and the Eisenstein ideal* (IHES Publi. Math. 47 (1977) p. 33-186)

[25] Menezes, A. J. : *Applications of finite fields* (Kluwer Academic Publishers 1993)

[26] Merel, L. : *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (Invent. Math. 124 (1996), no.1-3, p. 437-449)

[27] Mestre, J.F. : *Courbes elliptiques de rang ≥ 12 sur $\mathbb{Q}(t)$* (CRAS, t.313, Série I (1991), no. 4, p. 171-174)

[28] Mestre, J.F. :*Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(t)$* (CRAS, t.313, Série I (1991), no. 3, p. 139-142)

[29] Mestre, J.F. : *Un exemple de courbe elliptique sur $\mathbb{Q}$ de rang ≥ 15* (CRAS, t.314, Série I (1992),p. 453-455)

[30] Nagao, K.I. : *An example of Elliptic Curve over $\mathbb{Q}$ with rank ≥ 20* (Proc. Jap. Acad. , 69 (1993), Ser A, p. 291-293)

[31] Néron, A. : *Propriétés arithmétiques de certaines familles de courbes elliptiques* (Proc. Int. Cong. Math., Amsterdam (1954), vol III, p. 481-488)

[32] Ogawa, H. : *Curves of genus 2 with a rational torsion divisor of order 23* (Proc. Japan Acad. 70 (1994), Ser A, p. 295-298)

[33] Panchishkin, A. : *Algorithmes rapides pour la factorisation des nombres et des polynômes, tests de primalité, courbes elliptiques et modules de Drinfeld* (Séminaire de théorie des nombres de Caen 1993-94, p. 1-10)

[34] Parent, P. : *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres* (J. Reine Angew. Math. 506 (1999), p. 85-116)

[35] Poonen, B. : *Torsion in rank one Drinfeld modules and the uniform boundedness conjecture* (Math. Ann. 308 (1997) 4, p. 571-586)

[36] Poonen, B. : *Local height functions and the Mordell-Weil theorem for Drinfeld modules* (Compositio Math. 97 (1995), p. 349-368)

[37] Potemine, I. : *Arithmétique des corps globaux de fonctions et géométrie des schémas modulaires de Drinfeld* (Thèse à l'Institut Fourier 1997)

[38] Robert, A.M. : *A course in p-adic Analysis* (GTM 198 Springer)

[39] Scanlon, T. : *Public key cryptosystems based on Drinfeld modules are insecure* (Journal of Cryptology 14 (2001), p. 225-230)

[40] Swan, R.G. : *Factorization of polynomials over finite fields* (University of Chicago Press)

[41] Tsfasman, M.A. et Vlădut, S.G. : *Algebraic-Geometric Codes* (Mathematics and Its Applications, vol. 58, Kluwer Academic Publishers 1991)

[42] Wang, J. : *The Mordell-Weil theorems for Drinfeld modules over finitely generated function fields* (Manuscripta Math. 106 (2001),no. 3, p. 305-314)

[43] Washington, L.C. : *Introduction to Cyclotomic Fields (second edition)* (GTM 83 Springer)

[44] Weil, A. : *Basic Number Theory, 3rd Edition* (Springer-Verlag (1974))