Modules de Drinfeld et Cryptologie

A. A. Pantchichkine*

Institut Fourier, B.P.74, 38402 St.–Martin d'Hères, FRANCE
e-mail : panchish@mozart.ujf-grenoble.fr, FAX : 33 (0) 4 76 51 44 78

Résumé

Mon cours porte sur un travail en commun avec R. Gillard, F. Leprévost et X.-F. Roblot sur des nouveaux cryptosystèmes basés sur les modules de Drinfeld (voir [GLPR3]).

Les modules de Drinfeld sont des objets, provenants des analogies entre les entiers et les polynômes, et ils donnent des structures riches supplémentaires sur des ensembles finis, en particuliers, sur les corps finis. Les déscriptions analytique et algébrique de ces objets permettent de classifier leurs endomorphismes et torsion. Représentations galoisiennes donnent un analogue du théorème de Hasse.

Résumé (suite)

Soit $\mathcal{M}$ l'ensemble des messages (un ensemble fini). Une méthode de cryptage à clef publique consiste en la donnée d'une fonction bijective de $\mathcal{M}$ dans $\mathcal{M}$ publique, facilement évaluable, mais dont la réciproque est difficile à calculer sans connaître certains paramètres secrets. Toute personne peut crypter un message. Seul le détenteur des paramètres secrets peut déchiffrer le message. Dans le cas où $\mathcal{M}$ est un corps fini, une telle fonction est nécessairement un polynôme. De telles fonctions sont difficiles à construire en général. Nous établissons un procédé, basé sur les modules de Drinfeld, pour en obtenir.

On parlera aussi d'attaques diverses (décrites dans les travaux Th.Scanlon, S. R. Blackburn S. D. Galbraith et dans le mémoire de DEA de Vincent Despiegel)).

Cours N°1. Mardi le 7 octobre 2003

(disponible sur : http ://www-fourier.ujf-grenoble.fr/~panchish).

Introduction

Les objets pricipaux de mon cours sont les modules de Drinfeld introduits en 1973 à Moscou comme "modules elliptiques" à la base d'analogies entre les anneaux

$$\mathbb{Z} \text{ et } A = \mathbb{F}_q[T],$$

où $\mathbb{F}_q$ est un corps fini (Mémoire de Licence de V.G.Drinfeld sous la direction de Yu.I.Manin).

*Un cours de DEA à l'ENS Lyon (1e semestre 2003/2004)

Les groupes abéliens sont exactement les $\mathbb{Z}$-*modules*, et les modules de Drinfeld φ sont certains *A-modules*, analogues aux courbes elliptiques $E : y^2 = x^3 + ax + b \subset \mathbb{P}^2(\mathbb{C})$ (vues comme $\mathbb{Z}$-modules, $a, b \in \mathbb{Z}, 4a^3 + 27b^2 \neq 0$, avec l'élément neutre donné par le point à l'infini).

Ces objets et leures versions multidimensionnelles (les "chtoukas" de Drinfeld) ont étés utilisées par L.Lafforgue dans sa démonstration des conjectures de Langlands (Médaille Fields en 2002).

Avant donner les définitions : les courbes elliptiques ont trouvées beaucoup d'applications pour les sciences mais aussi dans la vie pratique (protection des cartes bancaires (cartes à puce) avec cryptosystèmes de type ECDLP utilisant la structure de groupe $E(\mathbb{F}_q)$ d'une courbe elliptique sur un corps fini.

C'est pourquoi on essaye de construire des nouveaux cryptosystèmes basées sur cette analogie [GLPR3], [Pa93].

Vers la fin du cours on parlera aussi d'attaques diverses (décrites dans les travaux Th.Scanlon, S. R. Blackburn S. D. Galbraith et dans le mémoire de DEA de Vincent Despiegel).

Définitions.

On considère l'anneau $A = \mathbb{F}_q[T]$ comme $\mathbb{F}_q$-espace vectoriel, et on considère sur A l'application de Frobenius τ et les applications linèaires :

$$\tau : A \to A,\ z \mapsto z^q,$$
$$a : A \to A, z \mapsto az \quad (a, z \in A)$$

On notera $A\{\tau\}$ l'anneau engendré par τ et a avec la composée comme multiplication de telle façon que $\tau a = a^q \tau$ (c'est un sous anneau non-commutatif dans l'anneau de toutes les applications $\mathbb{F}_q$-linéaires de A.

Définition préliminaire : Un morphisme d'anneaux $\varphi : A \to A\{\tau\}$ est dit un *module de Drinfeld de rang* $r \geq 1$ si

$$\varphi(T) = T + a_1\tau + \cdots + a_r\tau^r : z \mapsto Tz + a_1 z^q + \cdots + a_r z^{q^r} \text{ avec } a_r \neq 0.$$

Exemple. Module de Carlitz : $\varphi(T) = T + \tau$. On a $r = 1$,

$$\varphi(T^2) = (T + \tau)(T + \tau) = T^2 + (T + T^q)\tau + \tau^2.$$

Sécurité des cryptosystèmes et problèmes mathématiques

La sécurité des cryptosystèmes à clef publique est basée sur des problèmes mathématiques difficiles à résoudre en pratique. Citons par exemple les cryptosystèmes RSA, dont la sécurité est fondée sur le problème de la factorisation des entiers, celui de El Gamal ou le protocole d'échange de clefs de Diffie-Hellman basés sur le problème du logarithme discret dans le groupe multiplicatif d'un corps fini, ou dans le groupe des points rationnels d'une courbe elliptique définie sur un corps fini. Ces protocoles ont été longuement étudiés et sont standardisés (par exemple, voir [IEEE] et les références incluses).

Néanmoins, il est utile de disposer d'autres cryptosystèmes, dont la sécurité est basée sur d'autres problèmes, et qui, le cas échéant, peuvent être inclus dans de nouveaux standards.

On utilise des "bons" analogues connus des courbes elliptiques en caractèristique p : ce sont les modules de Drinfeld (voir [De-Hu], [Dr1], [Ge], et [Po] ainsi que [Pa93] pour ces objets).

Travaux de Th.Scanlon, de S. R. Blackburn et S. D. Galbraith.

Dans [Sca], Th.Scanlon montre que des cryptosystèmes provenants d'analogues naturels dans le cadre des modules de Drinfeld évoqués plus haut sont particulièrement faibles.

Nous esquissons ici une approche différente, qui contourne les faiblesses soulevées par Scanlon, en construisant une fonction sens unique à trappe (FSUT). Les détails apparaitront dans un article en commun avec R. Gillard, F. Leprévost et X.-F. Roblot [GLPR], et une demande de brevet (FR 02/12429), a été déposée sur ce nouveau cryptosystème.

On parlera aussi d'attaques diverses récentes (décrites dans les travaux S. R. Blackburn S. D. Galbraith et dans le mémoire de DEA de Vincent Despiegel).

Analogies entre $\mathbb{Z}$ et $A = \mathbb{F}_q[T]$

Soit

- $A = \mathbb{F}_q[T]$ l'anneau des polynômes d'une variable sur le corps de $q = p^n$ éléments,
- $K = \mathbb{F}_q(T)$,
- $K_\infty = \mathbb{F}_q((T^{-1}))$ (la complétion de K par rapport à la valeur absolue non-archimédienne donnée par la formule $\left|\frac{f}{g}\right|_\infty = q^{\deg f - \deg g}$), de telle façon que $|T^{-1}|_\infty = q^{-1} < 1$, et A est un sous-anneau discret de F_∞.
- On utilise la notation Ω pour la complétion d'une clôture algébrique du corps K_∞ :

$$\Omega = \widehat{\overline{K}}_\infty$$

$\mathbb{Z}$ (un anneau euclidien) $\mathbb{Z}$-modules (=groupes abéliens)	$A = \mathbb{F}_q[T]$ (un anneau euclidien) A-modules
$\mathbb{Q} = Quot(\mathbb{Z})$ (le corps des fractions de $\mathbb{Z}$)	$K = \mathbb{F}_q(T)$ (le corps des fractions de A)
Places finies de $\mathbb{Q}$: les nombres premiers p	Places finies de K : idéaux premiers $(f) \subset A$ $f(T) \in A$ (polynômes unitaires irréductibles)
une seule place infinie de $\mathbb{Q}$: la norme archimédienne usuelle $\lvert x\rvert = \lvert x\rvert_\infty$	une seule place infinie de K : la norme en $\infty \in \mathbb{P}^1_q$, $\lvert f/g\rvert_\infty = q^{\deg(f)-\deg(g)}$
la complétion de $\mathbb{Q}$ à l'infinie : $\mathbb{Q}_\infty = \mathbb{R}$ un corps localement compact connexe ($\lvert 10\rvert > 1$, la base de l'écriture décimale)	la complétion de K à l'infinie : $K_\infty = \mathbb{F}_q((T^{-1}))$ un corps localement compact totalement disconnect, $\lvert T\rvert_\infty = q > 1$
$\mathbb{C} = \overline{\mathbb{R}}$ (*topologiquement fermé, algébriquement clos*)	$\Omega = \widehat{\overline{K}}_\infty$ (la complétion d'une clôture algébrique $\overline{K}_\infty$ du corps K_∞
Une courbe elliptique sur $\mathbb{C}$ le groupe quotient abélien $E(\mathbb{C}) = \mathbb{C}/\Lambda_\mathbb{Z}$	Module de Drinfeld sur Ω le A-module quotient Ω/Λ_A

Complexité des problèmes mathématiques

Rappelons que la sécurité des cryptosystèmes à clef publique est basée à l'heure actuelle sur des problèmes mathématiques considérés comme difficiles à résoudre en pratique. Les protocoles utilisés de

nos jours se basent sur les trois problèmes mathématiques suivants :

- Factorisation de nombres entiers (IF)
- Calcul du logarithme discret dans le groupe multiplicatif d'un corps fini (DLP)
- Calcul du logarithme discret dans le groupe des points rationnels d'une courbe elliptique définie sur un corps fini (ECDLP)

C'est par exemple le cas des algorithmes de cryptage RSA, d'échange de clefs de Diffie-Hellman, etc. Ces protocoles ont été longuement étudiés et sont standardisés (eg. IEEE-P1363, ANSI X9.62, etc).

Il y a une recherche active sur ces différents problèmes. Les deux premiers problèmes mathématiques peuvent être résolus en temps sous-exponentiel. Pour le dernier, plus récent, il n'existe pas à l'heure actuelle de méthode générale de résolution en temps *sous-exponentiel*. Les meilleures méthodes existantes de résolution du troisième problème (encore une fois pour des choix des paramètres optimaux) opèrent en temps *exponentiel*.

Table des matières

Programme du cours

1. Analogies entre les nombres et les fonctions. Théorème d'Ostrowski.
2. Modules de Drinfeld : descriptions algébrique et analytique.
3. Points de torsion et endomorphismes des modules de Drinfeld.
4. Corps finis, automorphisme de Frobenius, elements primitifs, logarithme discret. Nombre de polynômes irréductibles de degree donne
5. Difficulté de la factorisation et de la vérification de primalite d'un nombre donné.
6. Représentations galoisiennes et l'hypothèse de Riemann pour les modules de Drinfeld.
7. Cryptosystèmes à clef publique des modules de Drinfeld.
8. Caractéristique d'Euler-Poincaré d'un module et calcul de la clef.
9. Attaques diverses

Remerciements

Une version préliminaire de ces résultats a été développé ensemble avec Roland Gillard, Frank Leprevost et Xavier Roblot pendant des exposés informels de l'auteur en novembre 2001 à l'Institut Fourier, et celui de Xavier Roblot au CIRM lors du Colloque "Théorie des nombres et applications", 14 - 18 janvier 2002, et nous sommes très reconnaissant aux organisateurs : C. Mauduit (Prof., Univ. Méditerranée), J. Rivat (Prof., Univ. Nancy 1). Des versions encore plus anciennes des cryptosystèmes basés sur les modules elliptiques de Drinfeld ont été proposées dans des exposés de l'auteur dans les universités de Bielefeld, de Caen, de Ohio-State, et de MPIM (Bonn) en été 1989.

Je remercie chaleureusement toutes ces institutions pour leur soutien.

Je suis reconnaissant au professeur Florian Hess pour l'information concernant un article récent de T.Scanlon, [Sca].

1 Analogies entre les nombres et les polynômes

L'anneau des nombres entiers $\mathbb{Z}$ est un objet algébrique fondamental, aussi bien que l'anneau $A = \mathbb{F}_q[X]$ (des polynômes à coefficients dans un corps fini $\mathbb{F}_q$). Ces deux anneaux sont commutatifs, associatifs unitaires sans diviseurs de zéro. De plus, tous les deux anneaux sont euclidiens. Il est commode d'exprimer la notion de divisibilité dans un anneau R ci–dessus à l'aide de la notion d'idéal : rappellons qu'un idéal I de R est une partie de R qui est un sous–groupe du groupe additif de R (c'est à direun sous groupe par rapport à l'addition), et qui est stable par rapport à la multiplication par tout élément de R. Tout élément $a \in R$ définit l'idéal $I = (a) = \{ax \mid x \in R\}$, et l'affirmation "$a$ divise b" est équivalent à "$b \in (a)$". Un idéal de type (a) est appelé idéal principal, et il est bien connu que les anneaux $R = \mathbb{Z}$, $A = \mathbb{F}_q[X]$ sont principaux, c'est à dire, tous ces ideaux sont principaux.

1.1 Normes de $\mathbb{Q}$ et de $\mathbb{F}_q(T)$.

On notera par $\|\cdot\|$ la valeur absolue habituelle (de $\mathbb{R}$).

Définition 1.1.1 *Soit k un corps.*
Une fonction $|\cdot|: k \to \mathbb{R}^{\geq 0}$ est appelée une norme *si*

1. $\forall x \neq 0 : \quad |x| > 0$
2. $|xy| = |x| \cdot |y|$
3. $|x + y| \leq |x| + |y|$.

On dit que $|\cdot|$ est non-archimédienne *si la condition plus forte*

$$|x + y| \leq \max\{|x|, |y|\}$$

soit satisfaite (dans ce cas on a

$$|x + y| \leq \max\{|x|, |y|\} \leq |x| + |y|)$$

Remarque 1.1.2 *Soit k un corps.*
Pour toute norme de k on a l'inégalité $|\alpha \pm \beta| \geq |||\alpha| - |\beta|||$ car

$$|\alpha| \leq |\alpha \pm \beta| + |\beta|, \ |\beta| \leq |\alpha \pm \beta| + |\alpha|$$

Définition 1.1.3 *Soit k un corps.*
(a) Deux normes $|\cdot|_{(1)}$ et $|\cdot|_{(2)}$ sont dites équivalentes *si et seulement si*

$$\exists s \in \mathbb{R}^{>0} : \quad \forall x \in k, |x|_{(1)} = |x|_{(2)}^s.$$

On le notera $|\cdot|_{(1)} \sim |\cdot|_{(2)}$.

(b) Une classe d'équivalence des normes de k est appelée une place de k.

Exemple. Soit $k = \mathbb{Q}$.

1. La valeur absolue $|x| = |x|_\infty$ est la *norme habituelle.*
2. Pour tout nombre premier p, la formule $|p^m \frac{a}{b}|_p = p^{-m}$, où $p \nmid a, b$, définie une norme, dite la *p-valeur absolue.*

Preuve : voir exercice 1.1. En particulier, $|p|_p = 1/p$, et $|p^k|_p = 1/p^k \to 0$ lorsque $k \to \infty$.

Exemple. Soit $k = \mathbb{F}_q(T)$

1. $|g|_\infty = q^{\deg g}$ définit une norme, appelée *la valeur absolue à ∞.*

2. Pour tout polynôme irréductible unitaire $f \in \mathbb{F}_q[T]$, une norme est définie par $|f^m \frac{g}{h}|_f = q^{-m \cdot \deg f}$, où $f \nmid g, h$.

PREUVE : voir exercice 1.2. En particulier, $|f^k|_f = 1/q^{k \cdot \deg f} \to 0$ lorsque $k \to \infty$.

THÉORÈME 1.1.4 (THÉORÈME D'OSTROWSKI)

1. *Toute norme non-triviale de $\mathbb{Q}$ est équivalente soit à $|\cdot|$, soit à $|\cdot|_p$ pour un nombre premier p.*
2. *Toute norme non-triviale de $\mathbb{F}_q(T)$ est équivalente soit à $|\cdot|_\infty$, soit à $|\cdot|_f$ pour un polynôme irréductible unitaire f.*

PREUVE

1. Soit $|\cdot|$ une norme de $\mathbb{Q}$. On va traiter deux cas.
   Premier cas : $\forall n \in \mathbb{N}, |n| \leq 1$. Il existe un nombre premier p tel que $|p| < 1$. (Sinon, la norme est triviale car
   $$\forall p \text{ premier}, |p| = 1 \Rightarrow \forall x \in \mathbb{Q}, |x| = 1$$
   à cause de à la décomposition primaire unique dans $\mathbb{Z}$.)
   Un tel nombre premier p est *unique* : Sinon,on supposons qu'il existe un autre nombre premier q avec $q \neq p$, $|q| < 1$. Alors en choisissant k, $l \in \mathbb{N}$ tels que
   $$|p^k| < \frac{1}{2} \text{ et } |q^l| < \frac{1}{2},$$
   et u, $v \in \mathbb{Z}$ tels que $1 = up^k + vq^l$, on obtient
   $$1 = |1| \leq |u||p^k| + |v||q^l| < \frac{1}{2} + \frac{1}{2} = 1,$$
   contradiction.

   On voit que l'ensemble
   $$\mathfrak{a} = \{a \in \mathbb{Z} \mid |a| < 1\}$$
   est un idéal dans $\mathbb{Z}$ avec $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$, ce que implique $\mathfrak{a} = p\mathbb{Z}$, car $p\mathbb{Z}$ est un idéal maximal dans $\mathbb{Z}$. En posant $x = p^m \cdot \frac{a}{b} \in \mathbb{Q}$ avec $p \nmid a, b$ et $\rho = |p|$, on voit que $|\frac{a}{b}| = 1$ et que
   $$\begin{aligned} |x| &= |p^m| \cdot |\frac{a}{b}| = |p^m| = |p|^m = \rho^m = p^{m \cdot \frac{\log \rho}{\log p}} \\ &= p^{-m \cdot (-\frac{\log \rho}{\log p})} = (p^{-m})^s = |x|_p^s \end{aligned}$$
   avec $s \in \mathbb{R}^{>0}$, d'où $|\cdot| \sim |\cdot|_p$.
   Deuxième cas : $\exists n \in \mathbb{N} :\ |n| > 1$. Soit alors $a > 1$ le nombre naturel minimal avec la condition $|a| > 1$. On écrit $|a| = |1 + \cdots + 1| \leq a \cdot |1| = a$, et on voit donc que $|a| = a^\alpha$ avec $0 < \alpha \leq 1$. Soit maintenant $N \in \mathbb{N}$ un nombre naturel, donc on peut décomposer N en base a d'une façon unique comme
   $$N = x_0 + x_1 a + \ldots + x_{k-1} a^{k-1}$$
   (avec $0 \leq x_i \leq a - 1$ $(\forall i \in \{1, \ldots, k-1\})$ et $x_{k-1} \geq 1$). Ceci implique $a^{k-1} \leq N < a^k$. En

appliquant la norme $|\cdot|$, on obtient

$$\begin{aligned} |N| &\leq |x_0| + |x_1||a| + \ldots + |x_{k-1}||a^{k-1}| \\ &\leq (a-1)(1 + a^\alpha + \ldots + a^{(k-1)\alpha}) \\ &= (a-1)\frac{a^{k\alpha}-1}{a^\alpha - 1} \\ &< (a-1)\frac{a^{k\alpha}}{a^\alpha - 1} \\ &= (a-1)\frac{a^\alpha}{a^\alpha - 1}a^{(k-1)\alpha} \\ &\leq CN^\alpha, \end{aligned}$$

ce que implique $|N| < CN^\alpha$, où C ne dépend pas de N.

En remplacant N par N^m, on obtient $|N|^m < CN^{m\alpha}$, et donc $|N| < \sqrt[m]{C}N^\alpha$. En laissant m tendre vers $+\infty$, on obtient donc $|N| \leq N^\alpha$. Posons mainenant $N = a^k + b$, avec $0 < b \leq a^k - a^{k-1}$. On obtient donc

$$|N| \geq |a^k| - |b| = a^{k\alpha} - |b|.$$

En même temps, on a déjà démontré que $|b| \leq b^\alpha$, donc

$$|b| \leq (a^k - a^{k-1})^\alpha,$$

d'où

$$|N| \geq a^{k\alpha} - (a^k - a^{k-1})^\alpha = (1 - (1 - \frac{1}{a})^\alpha)a^{k\alpha} > C'N^\alpha.$$

En remplaçant N par N^m, on obtient $|N|^m > C'N^{\alpha m}$, d'où $|N| > \sqrt[m]{C'}N^\alpha$, et, en laissant m tendre vers $+\infty$, $|N| \geq N^\alpha$. On a donc $|N| = N^\alpha$, d'où $|x| = |x|_\infty^\alpha$ pour tout $x \in \mathbb{Q}$.

2. Soit $|\cdot|$ une norme du $\mathbb{F}_q(T)$. On va traiter de nouveaux deux cas.
Premier cas : $|g| \leq 1$ pour tout $g \in \mathbb{F}_q[T]$. Il existe un polynôme irréductible unitaire f tel que $|f| < 1$. (Si $|f| = 1$ pour tout f irréductible unitaire, alors $|g| = 1$ pour tout $g \in \mathbb{F}_q(T)^\times$ grâce à la décomposition primaire unique dans $\mathbb{F}_q[T]$.) Un tel polynôme unitaire irréductible f est unique : sinon, on suppose qu'il existe un autre, h avec $f \neq h$, $|h| < 1$. Alors on choisit k, $l \in \mathbb{N}$ tels que

$$|f^k| < \frac{1}{2} \text{ et } |h^l| < \frac{1}{2},$$

et il existe u, $v \in \mathbb{F}_q[T]$ tels que $1 = uf^k + vh^l$, donc on obtient une contradiction parce que

$$1 = |1| \leq |u||f^k| + |v||h^l| < \frac{1}{2} + \frac{1}{2} = 1.$$

En posant $g = f^m \cdot \frac{a}{b} \in \mathbb{F}_q(T)$ avec $f \nmid a, b$ et $\rho = |f|$, on voit que $|\frac{a}{b}| = 1$ et que

$$\begin{aligned} |g| &= |f^m| \cdot |\frac{a}{b}| = |f^m| = |f|^m = \rho^m = q^{m \cdot \frac{\log \rho}{\log q}} = q^{-m \cdot (-\frac{\log \rho}{\log q})} \\ &= q^{-m \cdot \deg f (-\frac{\log \rho}{\log q \cdot \deg f})} = q^{-m \cdot \deg f \cdot s} = |g|_f^s \end{aligned}$$

avec $s \in \mathbb{R}^{>0}$, d'où $|\cdot| \sim |\cdot|_f$.
Deuxième cas : $\exists g \in \mathbb{F}_q[T] :\ |g| > 1$. Soit alors $g \in \mathbb{F}_q[T]$ un polynôme de degré k tel que $|g| > 1$, donc g s'écrit d'une façon unique :

$$g = a_0 + a_1 T + a_2 T^2 + \ldots + a_k T^k$$

avec $a_i \in \mathbb{F}_q$ pour $i \in \{1, \ldots, k\}$, $a_k \in \mathbb{F}_q^\times$. On a $|a_i| = 0$ ou 1, grâce au fait que $\forall x \in \mathbb{F}_q^\times$, $x^{q-1} = 1$, donc on obtient

$$\begin{aligned} |g| &= |a_0 + a_1 T + a_2 T^2 + \ldots + a_k T|^k \\ &\leq 1 + |T| + |T^2| + \cdots + |T|^k \end{aligned}$$

On remarque tout d'abord que $|T| > 1$. Sinon, on avait $|T| \leq 1$ et pour k fixé et tout m strictement positif

$$\begin{aligned} |g^m| &= |b_0 + a_1 T + b_2 T^2 + \ldots + b_{km} T|^{km} \\ &\leq 1 + |T| + |T^2| + \cdots + |T|^{km} \leq km \\ &\Rightarrow |g| \leq \sqrt[m]{km} \to 1, \end{aligned}$$

d'où $|g| \leq 1$, ce que donne une contradiction.
Maintenant, on peut supposer $|T| > 1$, et on remplace g par g^m ci-dessus :

$$\begin{aligned} |g^m| &\leq 1 + |T| + |T^2| + \cdots + |T|^{km} \\ &\leq \frac{|T|^{km+1} - 1}{|T| - 1} \leq C|T|^{km} \ (C = \frac{|T|}{|T| - 1}), \end{aligned}$$

donc

$$|g| \leq \sqrt[m]{C}|T|^k.$$

En faisant tendre m vers $+\infty$, on arrive à $|g| \leq |T|^k$. De plus, on a (grâce à l'inégalité $|\alpha \pm \beta| \geq |||\alpha| - |\beta|||$)

$$\begin{aligned} |g| &= |a_0 + a_1 T + a_2 T^2 + \ldots + a_k T^k| \\ &\geq |||a_0 + a_1 T + a_2 T^2 + \ldots + a_{k-1} T^{k-1}| - |a_k T^k||| \\ &\geq -(1 + |T| + \cdots + |T|^{k-1}) + |T|^k = |T|^k - \frac{|T|^k - 1}{|T| - 1} \\ &\geq |T|^k \frac{|T|}{|T| - 1} = C|T|^k. \end{aligned}$$

En remplaçant encore g par g^m, on obtient

$$|g^m| \geq C|T|^{km}$$

et donc

$$|g| \geq \sqrt[m]{C|T|^{km}}.$$

En faisant tendre m vers $+\infty$, on arrive à $|g| \geq |T|^k$, d'où $|g| = |T|^k$. On a donc

$$|g| = |T|^k = q^{k \frac{\log |T|}{\log q}} = q^{(k-1) \frac{\log |T| \frac{k}{k-1}}{\log q}} = q^{s \cdot \deg g}$$

avec $s \in \mathbb{R}^{>0}$, d'où $|\cdot| \sim |\cdot|_\infty$. Il reste à remarquer que $|g| = |T|^{\deg g}$ reste valable pour tout $g \in \mathbb{F}_q[T]$ (en exercice).

Solution : En effet, s'il existe un h avec $|h| \leq 1$ et avec $\deg h = l > 0$, alors pour tout m strictement positif on l'avait aussi $|h^m| \leq 1$ par la multiplicativité de la norme. Mais on a $h^m = c_0 + c_1 T +$

$c_2T^2 + \ldots + c_{ml}T^{ml}$ donc

$$\begin{aligned} |h^m| &= |c_0 + c_1T + c_2T^2 + \ldots + c_{ml}T^{ml}| \\ &\geq \| |c_0 + c_1T + c_2T^2 + \ldots + c_{ml-1}T^{ml-1}| - |a_{ml}T^{ml}| \| \\ &\geq -(1 + |T| + \cdots + |T|^{ml-1}) + |T|^{ml} = |T|^k - \frac{|T|^k - 1}{|T| - 1} \\ &\geq |T|^{ml}\frac{|T|}{|T| - 1} = C|T|^{ml} \to \infty, \end{aligned}$$

et on obtient une contradiction avec l'hypothèse $|h^m| \leq 1$

1.2 Formules de produit

Proposition 1.2.1 (Les formules de produit)

1. *Pour tout $x \in \mathbb{Q}^\times$, on a l'égalité*
$$\prod_v |x|_v = 1,$$
où v parcourt les nombres premiers p et le symbole ∞.
2. *Pour tout $g \in \mathbb{F}_q(T)^\times$, on a l'égalité*
$$\prod_v |g|_v = 1,$$
où v parcourt les polynômes unitaires irréductibles f de $\mathbb{F}_q[T]$ et le symbole ∞.

Preuve

1. On sait que chaque nombre entier x possède une décomposition unique
$$x = \pm \prod_{p \neq \infty} p^{\nu_p}.$$
En voyant que le signe de x est exactement $\frac{x}{|x|_\infty}$ et que pour chaque p premier, $p^{\nu_p} = \frac{1}{|x|_p}$, on obtient
$$x = \frac{x}{|x|_\infty} \prod_{p \neq \infty} \frac{1}{|x|_p} = x \prod_p \frac{1}{|x|_p},$$
d'où $\prod_p |x|_p = 1$. L'égalité reste valable dans le groupe $\mathbb{Q}^\times$ par la multiplicativité de la norme.
2. Soit $g \in \mathbb{F}_q(T)^\times$. On pose $g = \frac{G}{H}$ avec $G, H \in \mathbb{F}_q[T] \setminus \{0\}$. On a
$$|g|_\infty \prod_{f \neq \infty} |g|_f = q^{\deg G - \deg H} \prod_{f \neq \infty} q^{-m \cdot \deg f},$$
d'où
$$\begin{aligned} &|g|_\infty \prod_{f \neq \infty} |g|_f = 1 \iff \deg G - \deg H - \sum_{f \neq \infty} m \cdot \deg f = 0 \\ &\iff \sum_{f \neq \infty} m \cdot \deg f = \deg G - \deg H. \end{aligned}$$
Cette dernière égalité est obtenue grâce au fait que g se décompose d'une façon unique comme $g = \pm \prod_{f \neq \infty} f^{\nu_f}$, d'où $\deg g = \deg G - \deg H = \sum_{f \neq \infty} \nu_f \cdot \deg f$.

Exercices

1.1. *Soit $k = \mathbb{Q}$. Montrer que pour tout nombre premier p la formule $|p^m \frac{a}{b}|_p = p^{-m}$, où $p \nmid a, b$, définit une norme non-archimédienne, dite la p-*valeur absolue.

Solution : Pour *(i)*, il n'y a rien à montrer. Pour *(ii)*, on voit que $\forall$ *p premier*, $\forall x \in \mathbb{Q}$: $|x|_p = p^{-m} > 0$. De plus, pour $x, y \in \mathbb{Q}$, on a $|xy|_p = |p^{m+n} \frac{aa'}{bb'}|_p = p^{-(m+n)}$, car $p \nmid a, a', b, b'$ implique $p \nmid aa', bb'$. Enfin, avec $x = p^m \frac{a}{b}$ et $y = p^n \frac{a'}{b'}$, on obtient

$$|x+y|_p = |p^m(\frac{a}{b} + \frac{a'p^n}{b'p^m})|_p = |p^m \frac{ab'p^m + a'bp^n}{bb'p^m}|_p.$$

Si $m \leq n$, ceci implique que

$$|x+y|_p = \left|p^m \frac{ab' + a'bp^{n-m}}{bb'}\right|_p = p^{-m}.$$

Sinon,

$$|x+y|_p = \left|p^m \frac{ab' + a'b}{bb'p^{m-n}}\right|_p = \left|p^{m-(m-n)} \frac{ab' + a'b}{bb'}\right|_p = p^{-n}.$$

On obtient donc

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p.$$

1.2. *Soit $k = \mathbb{F}_q(T)$*

1. *$|g|_\infty = q^{\deg g}$ définit une norme non-archimédienne de k, appelée* la valeur absolue à ∞.
2. *Pour tout polynôme irréductible unitaire $f \in \mathbb{F}_q[T]$, une norme non-archimédienne est définie par la formule $|f^m \frac{g}{h}|_f = q^{-m \cdot \deg f}$, où $f \nmid g, h$.*

Solution :

1. On a $q^{\deg g} > 0$ pour tout g. De plus, $q^{\deg gh} = q^{\deg g} q^{\deg h}$ car $\deg gh = \deg g + \deg h$. Enfin, on a $\deg(g+h) \leq \max\{\deg g, \deg h\}$ et alors
$$q^{\deg(g+h)} \leq q^{\max\{\deg g,\ \deg h\}} = \max\{q^{\deg g},\ q^{\deg h}\} \leq q^{\deg g} + q^{\deg h}.$$
2. La démonstration est exactement la même comme dans l'exercice 1.1*(ii)*.

1.3. (Déterminant de Moore) *Soit k un corps contenant $\mathbb{F}_q$, $\beta_1, \cdots, \beta_n \in k$. Montrer que*

$$\begin{vmatrix} \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \beta_2 & \beta_2^q & \cdots & \beta_2^{q^{n-1}} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_n & \beta_n^q & \cdots & \beta_n^{q^{n-1}} \end{vmatrix} = \beta_1 \prod_{j=1}^{n-1} \prod_{c_1, \cdots, c_n \in \mathbb{F}_q} (\beta_{j+1} - \sum_{i=1}^{j} c_i \beta_i)$$

1.4. (Produit de polynômes irréductibles) *Tout élément $t \in \mathbb{F}_{q^n}$ est racine d'un polynôme irréductible unitaire $f = f_t$ de $\mathbb{F}_q[T]$ de degré d divisant n, En déduire*

$$T^{q^n} - T = \prod_{d|n} \prod_{\substack{f \text{ irréductible} \\ \deg f = d}} f(T),$$

On utilisera la notation $[n] := T^{q^n} - T$

1.5. (Produit des polynômes unitaires) *En déduire que*

$$P_n := \prod_{\substack{f \text{unitaire} \\ \deg f = n}} f(T) = \prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}},$$

On utilisera la notation $[n] := T^{q^n} - T$

1.6. (Factoriel de Carlitz) *Soit*

$$D_t = \prod_{\substack{f\ unitaire \\ \deg f \leq t}} f(T)$$

Montrer que

$$D_t = \prod_{n=1}^{t} P_n = \prod_{n=1}^{t}\prod_{m=1}^{n} [m]^{q^{n-m}} = \prod_{n=1}^{t}\prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}},$$

On utilisera la notation $[n] := T^{q^n} - T$

2 Description algébrique et analytique des modules de Drinfeld

Modules elliptiques de Drinfeld : théorie algébrique

Pour donner une définition algébrique des modules de Drinfeld on utilise l'anneau $\Omega\{\tau\}$ non–commutatif des polynômes d'une variable τ à coefficients dans Ω si-dessus, avec la règle de commutativité suivante : $\tau a = a^q \tau$ pour tout $a \in \Omega$.

On a l'isomorphisme d'anneaux

$$\Omega\{\tau\} \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_q}\mathbb{G}_{a,\Omega} = \Omega[z]_{\mathbb{F}_q-\mathrm{additifs}}.$$

(l'anneau des polynômes $\mathbb{F}_q$-additifs)

2.1 Polynômes $\mathbb{F}_q$-additifs

On note par τ l'endomorphisme de Frobenius ci-dessus $\tau : k \to k$, $z \mapsto z^q$, vu comme un endomorphisme $\mathbb{F}_q$-linéaire de $\mathbb{F}_q$-espace vectoriel k. Pour tout $a \in k$ on l'identifie avec l'endomorpfisme ($\mathbb{F}_q$-linéaire) $a : z \mapsto az$.

Alors on obtient un *isomorphisme d'anneaux*

$$k\{\tau\} \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_q}\mathbb{G}_{a,k} = k[z]_{\mathbb{F}_q-\mathrm{additifs}}$$

(c'est à dire,

$$f(z) \in k[z]_{\mathbb{F}_q-\mathrm{additifs}} \Longleftrightarrow \text{la fonction } z \mapsto f(z) \text{ est } \mathbb{F}_q-\text{additive},$$

où $f : k \to k$ *est la fonction determinée par le polynôme* f*.)*

Cet isomorphisme d'anneau est définit en associant au produit des polynômes de $k\{\tau\}$ *la composée* d'endomorphismes correspondents, en vue du théorème sur des *polynômes additifs* en caractéristique positive, voir [La], Ch.VIII, §12.

On rapelle ce résultat sous la forme suivante :

Définition 2.1.1 *Soit* k *un corps contenant* $\mathbb{F}_q$*, alors un polynôme*

$$f(X_1, \cdots, X_m) \in k[X_1, \cdots, X_m]$$

est dit $\mathbb{F}_q$*-additif s'il définie une application* $\mathbb{F}_q$*-linéaire* $k^m \to k$*.*

Pour un corps k contenant $\mathbb{F}_q$, et $a \in k$, on considère $\tau = \tau(z)$ et $a(z) = az$ comme des polynômes $\mathbb{F}_q$-additifs à coefficients dans k.

THÉORÈME 2.1.2 *L'application $\lambda : \tau \mapsto \tau(z)$, $\lambda : a \mapsto a(z)$ définie un isomorphisme d'anneaux*

$$k\{\tau\} \xrightarrow{\sim} \mathrm{End}_{\mathbb{F}_q}\mathbb{G}_{a,k} = k[z]_{\mathbb{F}_q-\mathrm{additifs}}$$

(c'est à dire, pour tout $f = a_0 + a_1\tau + \ldots + a_m\tau^m \in k\{\tau\}$ on pose

$$\lambda(f) = a_0 z + a_1 z^q + \ldots + a_m z^{q^m} \in k[z]_{\mathbb{F}_q-\mathrm{additifs}} \subset k_q[z]).$$

On rapellera ici la démonstration utilisant

DÉFINITION 2.1.3 *Soit k un corps contenant $\mathbb{F}_q$, alors un polynôme*

$$f(X_1, \cdots, X_m) \in k[X_1, \cdots, X_m]$$

est dit k-réduit si le degré de f en tout variable est $< \mathrm{Card}\,(k)$ dans le cas où k est un corps fini, où bien si k est infini (par exemple, si $k = \overline{k}$ est algébriquement clôs).

LEMME 2.1.4
(a) Soit k un corps contenant $\mathbb{F}_q$, alors pour tout polynôme

$$f(X_1, \cdots, X_m) = \sum_\nu a_\nu X_1^{\nu_1} \cdots X_m^{\nu_m} \in k[X_1, \cdots, X_m]$$

il existe un polynôme réduit $f^* \in k[X_1, \cdots, X_m]$ qui définie la même application que la fonction

$$f : k^m \to k,\ (x_1, \cdots, x_m) \mapsto f(x_1, \cdots, x_m)$$

($\nu = (\nu_1, \cdots, \nu_m) \in \mathbb{N}^m$) parcourt un nombre fini de multiindices.
(b) un tel polynôme f^* est unique.

PREUVE du lemme 2.1.4 (a) Si

$$f(X_1, \cdots, X_m) = \sum_\nu a_\nu X_1^{\nu_1} \cdots X_m^{\nu_m} \in k[X_1, \cdots, X_m] \text{ et } X_i^{\nu_i} = X_i^{|k|+\mu}, \mu \geq 0 \text{ pour un } i,$$

il suffit de remplacer $X_i^{\nu_i}$ par $X_i^{1+\mu}$, et répéter si nécessaire (en descendant le degré des monômes). Comme résultat, on obtient la même application $f : k^m \to k$ parce que $x_i^{|k|} = x_i$ pour tout $x_i \in k$.

(b) Si f et réduit, et l'application définie par f est identiquement nulle, alors $f \equiv 0$ (on raisonne par récurrence : dans le cas $m = 1$ le degré de f est $< |k|$ donc il ne peut pas avoir $|k|$ racines suf s'il est nul ; si $m \geq 2$, on écrit

$$f(X_1, \cdots, X_m) = \sum_\nu a_\nu X_1^{\nu_1} \cdots X_m^{\nu_m} = \sum_j f_j(X_1, \cdots, X_{m-1}) X_m^j \in k[X_1, \cdots, , X_{m-1}][X_m]$$

Si l'existait un $(b_1, \cdots, b_{m-1}) \in k^{m-1}$ avec $f_j(b_1, \cdots, b_{m-1}) \neq 0$ pour un j, alors $f_j(b_1, \cdots, b_{m-1}, X)$ soit un polynôme non-nul (contradiction). Alors $f_j(b_1, \cdots, b_{m-1}) = 0$ pour tout j et pour tout $(b_1, \cdots, b_{m-1}) \in k^{m-1}$, donc tous les $f_j(X_1, \cdots, X_{m-1})$ définissent les applications nulles, donc ils sont nuls par l'hypothèse de récurrence. On obtient que le polynôme f est nul.

LEMME 2.1.5 *Soit k un corps contenant $\mathbb{F}_q$, alors pour tout polynôme réduit $\mathbb{F}_q$-additif a la forme*

$$f(X_1, \cdots, X_m) = \sum_\nu A_{(\nu)} X_1^{q^{\nu_1}} \cdots X_m^{q^{\nu_m}} \in k[X_1, \cdots, X_m]$$

($\nu = (\nu_1, \cdots, \nu_m) \in \mathbb{N}^m$) parcourt un nombre fini de multiindices.

PREUVE du lemme 2.1.5. On remarque que

$$f(X_1, \cdots, X_m) = f_1(X_1) + \cdots + f_m(X_m)$$

où

$$f_j(X_j) = f(0, \cdots, X_j, \cdots, 0)$$

car la différence entre les deux parties est un polynôme réduit, qui définit une application nulle.

Si $m = 1$, $f(X) \in k[X]$ un polynôme $\mathbb{F}_q$-additif réduit, on considère un monôme $a_r X^r$ et on suppose $a_r \neq 0$; on pose

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

et on voit que ces monômes de degré r sont

$$a_r(X + Y)^r - a_r X^r - a_r Y^r.$$

Ceci implique que $g(X, Y)$ est identiquement nul car il est réduit et définie une application nulle. On écrit $r = p^t s$, avec $(s, p) = 1$, donc

$$0 = (X + Y)^r - X^r - Y^r = (X^{p^t} + Y^{p^t})^s - X^{p^t s} - Y^{p^t}$$

contient un terme non-nul $sX^{p^t(s-1)}Y^{p^t}$ comme $(s, p) = 1$. On obtient $s = 1$ donc

$$f(X) = a_0 X + a_1 X^p + \cdots + a_d X^{p^d},$$

ce que montre le lemme dans le cas $p = q$.

Dans le cas général $q = p^n$, et on écrit $p^\nu = q^{\nu_0} p^{\nu_1}$, avec $\nu_1 \leq n - 1$ par la division euclidienne de ν par n. Si $f(X)$ contient un monôme non nul $a_{p^\nu} X^{p^\nu}$, on considère $h(X) = f(\alpha X) - \alpha f(X)$ pour un générateur du group cyclique $\mathbb{F}_q^\times$. On voit que les termes de degré p^ν de $h(X)$ sont $a_{p^\nu}(\alpha^{p^\nu} - \alpha)X^{p^\nu}$. De plus, $h(X)$ est réduit et définie une application nulle sur k donc $h(X)$ est nul par lemme 2.1.4 (b). On remarque que

$$\alpha^{p^\nu} = \alpha^{p^{\nu_1} q^{\nu_0}} = \alpha^{p^{\nu_1}} \in \mathbb{F}_q \backslash \{\alpha\},$$

si $\nu_1 \geq 1$. Ceci implique

$$a_{p^\nu}(\alpha^{p^\nu} - \alpha)X^{p^\nu} \Rightarrow a_{p^\nu} = 0,$$

Cette contradiction prouve lemma 2.1.5.

Il reste à remarquer que la bijectivité de λ dans théorème 2.1.2 découle directement des lemmes 2.1.5 et 2.1.4.

Cours N°2. Mardi le 14 octobre 2003

Rappels du premier cours : Places de $\mathbb{Q}$ et de $K = \mathbb{F}_q(T)$. Polynômes $\mathbb{F}_q$-additifs et l'anneau $\Omega\{\tau\}$

Places de $\mathbb{Q}$ et de $K = \mathbb{F}_q(T)$.

Une place d'un corps k est une classe d'équivalence des normes (métrisations) $|\cdot| : k \to \mathbb{R}^{\geq 0}$:

- Soit $k = \mathbb{Q}$. Il y a les places suivantes :
  1. la valeur absolue habituelle $|x| = |x|_\infty$; la complétion $\mathbb{Q}_\infty = \mathbb{R}$.
  2. Pour tout nombre premier p, la formule $|p^m \frac{a}{b}|_p = p^{-m}$, où $p \nmid a, b$, définie une norme (métrisation), dite la *p-valeur absolue*. Cette norme est non-archimédienne : La complétion $\mathbb{Q}_p$ de $\mathbb{Q}$ par rapport à $|x|_p$ est dit le corps des nombres p-adiques,
  $$\mathbb{Q}_p = \Big\{ x = \sum_{i \in \mathbb{Z}, i \geq i_0} a_i p^i \;\Big|\; a_i = 0, 1, \cdots, p-1 \Big\},$$
  son sous-anneau des nombres p-adiques entiers est la boule de rayon 1 :
  $$\mathbb{Z}_p = \Big\{ x = \sum_{i \in \mathbb{Z}, i \geq 0} a_i p^i \;\Big|\; a_i = 0, 1, \cdots, p-1 \Big\} = \big\{ x \in \mathbb{Q}_p \;\big|\; |x|_p \leq 1 \big\}$$
- Dans le cas du corps $k = \mathbb{F}_q(T)$ on considère :
  1. une norme $|\frac{g}{h}|_\infty = q^{\deg g - \deg h}$, *la valeur absolue à ∞* ; on note la complétion $\mathbb{F}_q(T)_\infty$ de $\mathbb{F}_q(T)$ par rapport à $|x|_\infty$:
  $$\mathbb{F}_q(T)_\infty = \mathbb{F}_q((T^{-1})) = \Big\{ x = \sum_{i \in \mathbb{Z}, i \leq i_0} a_i T^i \;\Big|\; a_i \in \mathbb{F}_q \Big\}, \; \Big| \sum_{i \in \mathbb{Z}, i \leq i_0} a_i T^i \Big|_\infty = q^{i_0}, \text{ if } a_{i_0} \in \mathbb{F}_q^\times$$
  $$\mathcal{O} = \Big\{ x = \sum_{i \in \mathbb{Z}, i \leq 0} a_i T^i \;\Big|\; a_i \in \mathbb{F}_q \Big\} = \big\{ x \in \mathbb{F}_q((T^{-1})) \;\big|\; |x|_\infty \leq 1 \big\}.$$
  Remarquer que l'intersection $\mathcal{O} \cap A = \mathbb{F}_q$ est formée par les constantes uniquement.
  2. Pour tout polynôme irréductible unitaire $f \in \mathbb{F}_q[T]$, une norme définie par $|f^m \frac{g}{h}|_f = q^{-m \cdot \deg f}$, où $f \nmid g, h$.

  Exercice. Trouver la complétion $\mathbb{F}_q(T)_f$ de $\mathbb{F}_q(T)$ par rapport à $|x|_f$.

Théorème 1.1.4 (d'Ostrowski)

1. *Toute norme (ou "métrisation") non-triviale de $\mathbb{Q}$ est équivalente soit à $|\cdot|$, soit à $|\cdot|_p$ pour un nombre premier p.*
2. *Toute norme non-triviale de $K = \mathbb{F}_q(T)$ est équivalente soit à $|\cdot|_\infty$, soit à $|\cdot|_f$ pour un polynôme irréductible unitaire f.*

On considère le corps complet algébriquement clôs

$$\Omega = \widehat{\overline{K}}_\infty$$

obtenu à partir de la complétion d'une clôture algébrique du corps $K_\infty = \mathbb{F}_q((T^{-1}))$, la complétion de $K = \mathbb{F}_q(T)$ par rapport à la norme non-archimédienne $|\cdot|_\infty$.

Ce corps est un *analogue des nombres complexes* $\mathbb{C}$ en caractéristique positive.

Polynômes $\mathbb{F}_q$-additifs et l'anneau $k\{\tau\}$

Soit k un corps infini contenant $\mathbb{F}_q$. On considère l'anneau $k\{\tau\}$ non–commutatif des polynômes d'une variable τ à coefficients dans k si-dessus, avec la formule de commutation suivante : $\tau a = a^q \tau$ pour tout $a \in k$. On remarque que $k\{\tau\}$ est un $\mathbb{F}_q$-algébre car les constantes $\alpha \in k$ commutent avec τ et tous les $a \in k$

Puis, un polynôme $f(z) \in k[z]$ est dit $\mathbb{F}_q$ – additifs, s'il définit une application $\mathbb{F}_q$-linéaire de k dans k. On a noté par $k[z]_{\mathbb{F}_q-\text{additifs}}$ l'anneau des polynômes $\mathbb{F}_q$ – additifs avec la multiplication donnée par la composée. Par exemple, le morphisme de Frobenius $\tau(z) = z^q$, et le morphisme $a(z) = az$ sont $\mathbb{F}_q$ – additifs, $\tau, a : k \to k$.

THÉORÈME 2.1.2 (SUR LES POLYNÔMES $\mathbb{F}_q$-ADDITIFS) *L'application $\lambda : \tau \mapsto \tau(z)$, $\lambda : a \mapsto a(z)$ définie un isomorphisme d'anneaux (et de $\mathbb{F}_q$-algèbres,*

$$k\{\tau\} \xrightarrow{\sim} k[z]_{\mathbb{F}_q-\text{additifs}}$$

(c'est à dire, pour tout $f = a_0 + a_1\tau + \ldots + a_m\tau^m \in k\{\tau\}$ on pose

$$\lambda(f) = a_0 z + a_1 z^q + \ldots + a_m z^{q^m} \in k[z]_{\mathbb{F}_q-\text{additifs}} \subset k[z]).$$

2.2 Définition algébrique des modules de Drinfeld sur Ω

On considère le corps complet algébriquement clôs

$$\Omega = \widehat{\overline{K}}_\infty$$

obtenu à partir de la complétion d'une clôture algébrique du corps $K_\infty = \mathbb{F}_q((T^{-1}))$, la complétion de $K = \mathbb{F}_q(T)$ par rapport à la norme non-archimédienne $|\cdot|_\infty$.

DÉFINITION 2.2.1 *Un* module de Drinfeld *φ de rang r (à coefficients dans Ω) est un morphisme d'anneaux sur $\mathbb{F}_q$, $\varphi : A \to \Omega\{\tau\}$ (ceci dit, $a \mapsto \varphi(a)$, et $\forall \alpha \in \mathbb{F}_q$, $\varphi(\alpha) = \alpha$) tel que* $\deg_\tau \varphi(T) = r$ *et*

$$\varphi(T) = T + g_1\tau + \ldots + g_r\tau^r, \ g_1, \cdots, g_r \in \Omega.$$

On notera par $\varphi_a(z) = \lambda(\varphi(a))(z)$ le polynôme $\mathbb{F}_q$-additif correspondent à $\varphi(a)$ par l'isomorphisme λ du Théorème 2.1.2. Le degré de

$$\varphi_T(z) = Tz + g_1 z^q + \ldots + g_r z^{q^r},$$

en z est égale donc à q^r. On montrera aussi que pour tout $a \in A$, le degré de $\varphi_a(z)$ en z est égale à $q^{r\cdot \deg a}$, et que $D\varphi_a(z) = az$ (ici $D\varphi(x)$ désigne la partie linéaire de $\varphi(x)$).

DÉFINITION 2.2.2 *Soient $\varphi : A \to \Omega\{\tau\}$ et $\psi : A \to \Omega\{\tau\}$ deux modules de Drinfeld à coefficients dans Ω. Un élément $u \in \Omega\{\tau\}$ est dit un* morphisme *de φ dans ψ si*
Mor *pour tout $a \in A$ on a $\varphi(a)u = u\psi(a)$;*
Isog *une* isogénie *est un morphisme non-nul.*

EXEMPLE 2.2.3 *Soient $\varphi : A \to \Omega\{\tau\}$un module de Drinfeld à coefficients dans Ω. Alors pour tout $b \in A$, l'élément $u = \varphi(b) \in \Omega\{\tau\}$ est un morphisme de φ dans φ car pour tout $a \in A$ on a $\varphi(a)\varphi(b) = \varphi(b)\varphi(a) = \varphi(ab)$;*

2.3 Fonctions analytiques sur Ω et le théorème de préparation de Weierstrass

On donnera ici des détails sur les fonctions analytiques sur un corps algébriquement clos et complet Ω pour une norme (métrisation) non-archimédienne $|\cdot|$ (voir [Kob80], p. 13). On utilse un élément T de Ω avec $|T| = q > 1$, et pour tout $x \in \Omega^\times$, on notera $v(x) = -\log_q |x|$ de telle façon que $v(T^{-1}) = 1$.

Convergence des séries non-archimédiennes

On notera par

$$\mathcal{D}_a(r) = \mathcal{D}_a(r;\Omega) = \{x \in \Omega \mid |x-a| \leq r\}, \tag{2.1}$$
$$\mathcal{D}_a(r^-) = \mathcal{D}_a(r^-;\Omega) = \{x \in \Omega \mid |x-a| < r\}, \tag{2.2}$$

les disques ("fermé" et "ouvert") de rayon r, centrés en $a \in \Omega$, $r \geq 0$). On pose

$$\mathcal{O} = \mathcal{O}_\Omega = \{x \in \Omega \mid |x| \leq 1\} = \mathcal{D}_0(1) \text{ (c'est un anneau complet)}, \tag{2.3}$$
$$\mathfrak{m} = \mathfrak{m}_\Omega = \{x \in \Omega \mid |x| < 1\} = \mathcal{D}_0(1^-) \tag{2.4}$$
(c'est son idéal maximal).

Dans l'analyse classique, un critère connu de la convergence d'une série $\sum_{n=0}^{\infty} a_n$ dit que les sommes partielles

$$\sum_{N \leq n \leq M} a_n$$

sont petites pour tous N , M grands avec $M > N$.

Dans le cas d'un corps Ω complet pour une norme (métrisation) non-archimédienne $|\cdot|$, on a, grâce à la propriété non-archimédienne, que ceci arrive si et seulement si $|a_n| \to 0$ (i.e. $v(a_n) \to \infty$) lorsque $n \to \infty$.

Alors la convergence d'une série $\sum_{n\geq 0} a_n z^n$ ne dépend que de $|z|$ mais pas d'une valeur précise de z, donc il n'y a pas de "convergence conditionnelle" dans ce cas.

De même façon, la convergence d'un produit $\prod_{n\geq 0} (1 + \alpha_n)$ dans Ω est équivalent à $|\alpha_n| \to 0$.

Ceci implique que pour toute séries $\sum_{n\geq 0} a_n z^n$ on peut définir son rayon de convergence r de telle façon que l'une des deux conditions soient satisfaites :

$$\sum_{n=0}^{\infty} a_n z^n \quad \text{converge} \iff z \in \mathcal{D}_0(r^-), \tag{2.5}$$
$$\sum_{n=0}^{\infty} a_n z^n \quad \text{converge} \iff z \in \mathcal{D}_0(r). \tag{2.6}$$

Un exemple de la première possibilité est $\sum_{n\geq 0} z^n$, quand (2.5) est satisfaite avec $r = 1$, et un exemple de la deuxième possibilité est $\sum_{n\geq 0} T^{-n} z^{q^n - 1}$, où (2.6) est satisfaite aussi avec $r = 1$.

PROPOSITION 2.3.1 *Le rayon de convergence r d'une série*

$$\sum_{n\geq 0} a_n z^n \in \Omega[[z]]$$

est donné par la formule habituelle

$$r = \frac{1}{l} \text{ où } l = \limsup_{n\to\infty} \sqrt[n]{|a_n|}.$$

EXERCICE 2.3.2 *Pour tout $k \in \mathbb{N}$ trouver le rayon de convergence de la série*

$$\sum_{n\geq 0} T^{kn} z^{q^n-1}$$

Solution : On a

$$|a_{q^n-1}| = |T^{kn}| = q^{kn} \Rightarrow \limsup_{n\to\infty} \sqrt[n]{|a_n|} = \limsup_{n\to\infty} \sqrt[q^n-1]{|q^{kn}|} = 1,$$

car $\sqrt[m]{(m+1)^k} = \exp(k\frac{\log(m+1)}{m}) \to 1$ lorsque $m = q^n - 1 \to \infty$.

REMARQUE 2.3.3

(a) Toute série

$$f(z) = \sum_{n\geq 0} a_n z^n \in \Omega[[z]]$$

à coefficients $a_n \to 0$ dans Ω, converge sur $\mathcal{D}_0(1)$. On pose

$$\|f\| = \sup_n |a_n|$$

Dans ce cas il existe un élément $\beta \in \Omega^\times$ tel que

$$\beta^{-1} f(z) = \sum_{n\geq 0} \tilde{a}_n z^n \in \mathcal{O}[[z]],$$

et q'il existe $\tilde{a}_m \notin \mathfrak{m}$, par exemple, $\tilde{a}_0, \cdots, \tilde{a}_{m-1} \in \mathfrak{m}$ mais $\tilde{a}_m \notin \mathfrak{m}$. On a alors $\|f\| = |\beta|$.

En effet, on pose, par exemple, $\beta = a_m$ avec le plus petit m tel que $|a_m| = \sup_n |a_n| = \max_n |a_n|$) (le maximum est atteint lorsque $|a_n| \to 0$.

(b) Une série formelle $f(z) = \sum_{n=0}^\infty a_n z^n \in \mathcal{O}[[z]]$ est inversible dans l'anneau $\mathcal{O}[[z]]$ si et seulement si $a_0 \in \mathcal{O}^\times$.

Dans ce cas les séries $f(z)$ et $f(z)^{-1}$ convergent dans $\mathcal{D}_0(1^-)$.

Théorème de préparation de Weierstrass non-archimédien

THÉORÈME 2.3.4 *Pour toute série $f(z) = \sum_{n=0}^\infty a_n z^n \in \mathcal{O}[[z]]$ telle que $a_0, \cdots, a_{m-1} \in \mathfrak{m}$ mais $a_m \notin \mathfrak{m}$, il existe une factorisation de f en produit d'un polynôme $h(z) = z^m + c_{m-1}z^{m-1} + \cdots + c_1 z + c_0$ et une série inversible $g(z) = \sum_{n=0}^\infty b_n z^n \in \mathcal{O}[[z]]$ avec $b_0 \in \mathcal{O}^\times$:*

$$\sum_{n=0}^\infty a_n z^n = (z^m + c_{m-1}z^{m-1} + \cdots + c_1 z + c_0) \sum_{n=0}^\infty b_n z^n$$

De plus, $c_0, \cdots, c_{m-1} \in \mathfrak{m}$, et toutes les racines du polynôme $z^m + c_{m-1}z^{m-1} + \cdots + c_1 z + c_0$ se trouvent dans $\mathcal{D}_0(1^-)$.

REMARQUE. Soit $f(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathcal{O}[[z]]$ une série convergante dans une boule $\mathcal{D}_0(R)$.

Après la multiplication de la variable z par une constante convenable $\beta \in \Omega^\times$, on obtient par théorème 2.3.4 dans toute boule $\mathcal{D}_0(R)$ une factorisation

$$f(z) = h(z)g(z),$$

où $g(z)$ est inversible sur $\mathcal{D}_0(R)$, et $h(z)$ est un polynôme avec toutes les racines dans $\mathcal{D}_0(R)$.

Une démonstration simple du théorème 2.3.4 est basée sur une version de la divsion euclidienne pour les séries formelles :

LEMME 2.3.5 (DIVSION EUCLIDIENNE POUR LES SÉRIES FORMELLES) *Pour toute série f ci-dessus telle que $a_0, \cdots, a_{m-1} \in \mathfrak{m}$ mais $a_m \notin \mathfrak{m}$, et pour toute $F(z) = \sum_{n=0}^{\infty} A_n z^n \in \mathcal{O}[[z]]$ il existe un seul couple q, r, avec la propriété suivante*

$$F = qf + r,\ q(z) \in \mathcal{O}[[z]], r(z) \in \mathcal{O}[z],\ \deg r(z) \leq m-1. \tag{2.7}$$

Lemme 2.3.5 $\Rightarrow$ Théorème 2.3.4 :

Il suffit de prendre $F(z) = z^m$, on obtient

$$z^m = q(z)f(z) + r(z) \Rightarrow q(z)f(z) = z^m - r(z) \tag{2.8}$$

donc on obtient une série formelle $q(z) = \sum_{n=0}^{\infty} d_n z^n \in \mathcal{O}[[z]]$ qui est inversible dans l'anneau $\mathcal{O}[[z]]$ car $d_0 \in \mathcal{O}^\times$: lorsqu'on compare les coefficients de z^m à gauche et à droite de l'égalité (2.8), on a

$$d_0 a_m + d_1 a_{m-1} + \cdots + d_{m-1} a_1 + d_m a_0 = 1.$$

Puis, on pose $g(z) = q(z)^{-1} = \sum_{n=0}^{\infty} b_n z^n \in \mathcal{O}[[z]]$ avec $b_0 \in \mathcal{O}^\times$, par l'inversibilité de q.

La comparaison des deux parties de (2.7) $\mod \mathfrak{m}$ montre que $c_0, \cdots, c_{m-1} \in \mathfrak{m}$.

Puis, toute racine z_0 du polynôme

$$h(z) = z^m + c_{m-1} z^{m-1} + \cdots + c_1 z + c_0$$

se trouve dans $\mathcal{D}_0(1^-)$.

Sinon, on suppose d'abord que $|z_0| > 1$, alors $|z_0^{-1}| < 1$, et

$$\begin{aligned} h(z_0) = z_0^m + c_{m-1} z_0^{m-1} + \cdots + c_1 z_0 + c_0 = 0 \Rightarrow z_0 = -c_{m-1} z_0^{-1} - \cdots - c_1 z_0 - c_0 \\ \Rightarrow |z_0| < \max_{i \geq 1} |c_{m-i} z_0^{m-i}| < 1, \end{aligned}$$

une contradiction avec l'hypothèse $|z_0| > 1$.

Ensuite,

$$h(z_0) = z_0^m + c_{m-1} z_0^{m-1} + \cdots + c_1 z_0 + c_0 = 0 \Rightarrow |z_0| \leq 1 \Rightarrow |z_0| < 1,$$

car $\max_{i \geq 1} |c_{m-i}| < 1$ et

$$|z_0|^m = | - c_{m-1} z_0^{m-1} - \cdots - c_1 z_0 - c_0| \leq \max_{i \geq 1} |c_{m-i} z_0^{m-i}| < 1$$

Preuve du lemme 2.3.5 (sur la divsion euclidienne pour les séries formelles) :

On utilise les opérations de projection U et V sur le debut et sur la fin d'une série :

$$U(\sum_{n=0}^{\infty} b_n z^n) = \sum_{n=0}^{m-1} b_n z^n,\ V(\sum_{n=0}^{\infty} b_n z^n) = \sum_{n=m}^{\infty} b_n z^{n-m}$$

L'existence de q et de r est équivalente à l'existence d'une telle q que $V(F) = V(qf)$. On remarque que la série $V(f)$ est inversible dans l'anneau $\mathcal{O}[[z]]$ car son terme constante est $a_m \in \mathcal{O}^\times$. Mais $f = U(f)+z^m V(f)$, donc la question est équivalente à la solution d'une équation suivante : on pose $G = qV(f)$, alors trouver une série G telle que

$$V(F) = V\big(q(U(f) + z^m V(f))\big) = V\left(G\frac{U(f)}{V(f)}\right) + G = \left(Id + V \circ \frac{U(f)}{V(f)}\right) G.$$

On montrera que l'opérateur $Id + V \circ \frac{U(f)}{V(f)}$ est inversible dans $\mathcal{O}[[z]]$, et que

$$G = \left(Id + V \circ \frac{U(f)}{V(f)}\right)^{-1} (V(F)) \in \mathcal{O}[[z]],$$

Il suffit de remarquer

$$\frac{U(f)}{V(f)} \in \mathfrak{m}[[z]],$$

donc

$$V \circ \frac{U(f)}{V(f)} : \mathcal{O}[[z]] \to \mathfrak{m}[[z]].$$

Ceci implique :

$$\left(Id + V \circ \frac{U(f)}{V(f)}\right)^{-1} = Id - V \circ \frac{U(f)}{V(f)} + \left(V \circ \frac{U(f)}{V(f)}\right)^2 + \cdots,$$

La série d'opérateurs à droite converge car l'anneaux $\mathcal{O}[[z]]$ est topologiquement fermé (avec la convergence coefficient-par-coefficient).

2.4 Propriétés des fonctions entières sur Ω

DÉFINITION 2.4.1 *Une fonction $f : \Omega \to \Omega$ est dit* entière*, si elle est représentée par la somme d'une série convergeante partout dans Ω,*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \in \Omega[[z]].$$

Pour tous $c \in \Omega$, on peut redévelopper cette série suivant $(z - c)$.

Le diviseur *$div(f) = \sum_{x \in X} m_x(x)$ de f est une somme formelle qui porte sur l'ensemble X des zéros x de f, comptés avec leurs multiplicités $m_x \in \mathbb{Z}$ (c'est un élément du produit infini des groupes abéliens $\{\mathbb{Z}(x)\}_{x \in \Omega}$.*

Deux fonctions entières $f_1, f_2 : \Omega \to \Omega$ ont le même diviseur si et seulement si la fonction

$$z \mapsto \frac{f_1(z)}{f_2(z)}$$

se prolonge en une fonction continue à valeurs non-nulles.

PROPOSITION 2.4.2 *Toute fonction entière non-constante*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \in \Omega[[z]].$$

possède un zéro dans Ω.

PREUVE. Par l'hypothèse, il existe un coefficient $a_m \neq 0$ avec $m > 0$, et on montre tout d'abord, que, après la multiplication de f et de la variable z par des constantes convenables $\alpha, \beta \in \Omega^\times$, on obtient une autre fonction entière

$$f^*(z) = \beta^{-1} f(\alpha z) = \sum_{n=0}^{\infty} a_n^* z^n \in \mathcal{O}[[z]],$$

telle que la condition du théorème 2.3.4 de préparation de Weierstrass soient satisfaites avec un $m > 1$: il existe $a_m^* \notin \mathfrak{m}$, mais $a_0^*, \cdots, a_{m-1}^* \in \mathfrak{m}$.

Ensuite, on utilise directement la factorisation du théorème 2.3.4 de préparation de Weierstrass pour f^*, et on voit que f^* et f possèdent un zéro (comme une racine du polynôme $h(z)$).

Par exemple, on peut choisir $\alpha, \beta \in \Omega^\times$ de telle façon que

$$|\alpha| > \frac{\max_{i \leq m-1} |a_i| + 1}{|a_m|}$$

et

$$|\beta| = \max_{j \in \mathbb{N}} |a_j| \cdot |\alpha|^j$$

On rapelle que $|a_j| \cdot |\alpha|^j \to 0$ car f est entière, donc le maximum est atteint. Alors

$$a_j^* = \beta^{-1} \alpha^j a_j,$$

donc pour tout j, $|a_j^*| \leq 1$, et il existe un $m_0 \geq m$, tel que $|a_{m_0}^*| = 1$, et

$$|a_0^*| < 1, \cdots, |a_{m_0-1}^*| < 1.$$

THÉORÈME 2.4.3 *Toute fonction entière non-constante*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \in \Omega[[z]].$$

est déterminée par son diviseur à une constante multiplicative près.

PREUVE. Deux fonctions entières $f_1, f_2 : \Omega \to \Omega$ ont le même diviseur si et seulement si la fonction

$$z \mapsto \frac{f_1(z)}{f_2(z)}$$

se prolonge en une fonction continue à valeurs non-nulles partout dans Ω (par le revéveloppement en tout point $c \in \Omega$.

Pour montrer que $\dfrac{f_1(z)}{f_2(z)}$ est une constante il suffit donc de montrer (en vue de proposition 2.4.2), que cette fonction peut être présenté par une série entière $f_3(z)$. Après la multiplication de la variable z par une constante convenable $\beta \in \Omega^\times$, on obtient par théorème 2.3.4 dans toute boule $\mathcal{D}_0(R)$ des factorisations

$$f_1(z) = h_1(z) g_1(z), \ f_2(z) = h_2(z) g_(z)$$

où $g_1(z), g_(z)$ sont inversibles sur $\mathcal{D}_0(R)$, et $h_1(z), h_2(z)$ sont deux polynômes avec toutes les racines dans $\mathcal{D}_0(R)$.

Mais, par l'hypothèse, $h_1(z)$ et $h_2(z)$ sont proportionnels. Ceci dit, dans toute boule il existe une série entière, représentant la fonction

$$\frac{g_1(z)}{g_2(z)}.$$

Par l'unicité d'une telle série, elle représentant la fonction partout dans Ω, CQFD.

Fonction entière, attachée à un A-réseau

DÉFINITION 2.4.4 *Soit X un sous-A-module dans le corps complet algébriquement clôs*

$$\Omega = \widehat{\overline{K}}_\infty$$

obtenu à partir de la complétion d'une clôture algébrique du corps $K_\infty = \mathbb{F}_q((T^{-1}))$, la complétion de $K = \mathbb{F}_q(T)$ par rapport à la norme non-archimédienne $|\cdot|_\infty$.

On dit que X est un A-réseau si pour toute boule $\mathcal{D}_a(R)$ l'intersection $\mathcal{D}_a(R) \cap X$ est finie.

Soit X un A-réseaux. On définie une fonction

$$e_X(z) = z \prod_{X \ni l \neq 0} \left(1 - \frac{z}{l}\right) \tag{2.9}$$

PROPOSITION 2.4.5 *Soit X un A-réseaux.*

(a) La fonction $e_X(z)$ donnée par (2.10), est une fonction entière dans Ω avec les zéros simples en $l \in X$.

(b) La fonction $e_X(z)$ est X-périodique et $\mathbb{F}_q$-additive :

$$\begin{aligned} &e_X(z_1 + z_2) = e_X(z_1) + e_X(z_2) \text{ pour tout } z_1, z_2 \in \Omega \\ &e_X(\alpha z) = \alpha e_X(z) \text{ pour tout } \alpha \in \mathbb{F}_q^* \\ &e_X(z) = \sum_{m=0}^{\infty} A_m z^{q^m}. \end{aligned}$$

PREUVE. On a $e_X(z) = z \prod_{X \ni l \neq 0} \left(1 - \frac{z}{l}\right) = \lim_{n \to \infty} \prod_{\substack{X \ni l \neq 0 \\ |l| < n}} \left(1 - \frac{z}{l}\right)$ à cause de la convergence $\frac{z}{l} \to 0$ lorsque $|l| \to \infty$ pour tout $z \in \Omega$, d'où l'assertion (a).

Puis, on représente X comme l'union croissante

$$X = \bigcup_{n \in \mathbb{N}} H_n$$

des $\mathbb{F}_q$-sous-espaces $H_n \subset X$ de dimension finie. En fait, l'intersection de X avec toute boule donne un tel sous-espace. Graçe à la convergence, on représente alors $e_X(z)$ comme une limite des polynômes :

$$e_X(z) = \lim_{n \to \infty} z \prod_{H_n \ni l \neq 0} \left(1 - \frac{z}{l}\right).$$

Tout polynôme $z \prod_{H_n \ni l \neq 0} \left(1 - \frac{z}{l}\right)$ est déterminé par ces racines et donc il est $\mathbb{F}_q$-additifs.

Passant à la limite, on obtient l'assertion (b).

Cours N°3. Mardi le 21 octobre 2003

Description analytique et algébrique des modules de Drinfeld

Rappels : polynômes $\mathbb{F}_q$-additifs et l'anneau $k\{\tau\}$

Soit k un corps contenant $\mathbb{F}_q$. On considère l'anneau $k\{\tau\}$ non–commutatif des polynômes d'une variable τ à coefficients dans k, avec la formule de commutation suivante : $\tau a = a^q \tau$ pour tout $a \in k$.

Puis, un polynôme $f(z) \in k[z]$ est dit $\mathbb{F}_q$-additifs, s'il définit une application $\mathbb{F}_q$-linéaire de k dans k. On a noté par $k[z]_{\mathbb{F}_q-\text{additifs}}$ l'anneau des polynômes $\mathbb{F}_q$-additifs avec la multiplication donnée par la composée. Par exemple, le morphisme de Frobenius $\tau(z) = z^q$, et le morphisme $a(z) = az$ sont $\mathbb{F}_q$-additifs, $\tau, a : k \to k$.

THÉORÈME 2.1.2 (SUR LES POLYNÔMES $\mathbb{F}_q$-ADDITIFS) *L'application $\lambda : \tau \mapsto \tau(z)$, $\lambda : a \mapsto a(z)$ définie un isomorphisme d'anneaux*

$$k\{\tau\} \xrightarrow{\sim} k[z]_{\mathbb{F}_q-\text{additifs}},$$
$$\lambda(a_0 + a_1\tau + \ldots + a_m\tau^m) = a_0 z + a_1 z^q + \ldots + a_m z^{q^m} \in k[z]_{\mathbb{F}_q-\text{additifs}} \subset k[z]).$$

Une application très utile de ce résultat (Proposition 1.3 de [De-Hu], p.32) décrit les polynômes $\mathbb{F}_q$-additifs de racines simples ; on la donne ici sous la forme suivante :

PROPOSITION 2.4.6 *Soit $H \subset \Omega$ un sous-espace vectoriel fini sur $\mathbb{F}_q$. On considère le polynôme*

$$P_H(z) = \prod_{h \in H} (z - h).$$

Alors le polynôme $P_H(z)$ est $\mathbb{F}_q$-additif de racines simples, et

$$P_H(z) = z + a_1 z^q + \ldots + a_m z^{q^m},$$

avec $\deg(P_H) = \text{Card}\,(H) = q^m = q^{\dim H}$.

PREUVE. On considère le polynôme

$$Q_w(z) = P_H(z + w) - P_H(w) = \prod_{h \in H} (z + w - h) - \prod_{h \in H} (w - h) \in k(w)[z].$$

Ce polynôme s'annule sur H puisque H est un *groupe abélien*, de plus, $\deg(Q_w) = \deg(P_H) = \text{Card}\,(H)$. Ceci dit, Q_w et P_H sont deux polynômes unitaires avec les mêmes zéros dans $H \subset k \subset k(w)$, donc ils coïncident, d'où l'additivité :

$$P_H(z) = Q_w(z) = P_H(z + w) - P_H(w).$$

De même façon, la comparaison des racines montre la $\mathbb{F}_q$-additivité :

$$\forall \alpha \in \mathbb{F}_q, P_H(\alpha z) = \alpha^{q^{\dim H}} P_H(z), \text{ où } \alpha^{q^{\dim H}} = \alpha.$$

Rappel sur le corps $\widehat{\overline{K}}_\infty$:

On considère le corps complet

$$\Omega = \widehat{\overline{K}}_\infty$$

obtenu à partir de la complétion d'une clôture algébrique du corps $K_\infty = \mathbb{F}_q((T^{-1}))$, la complétion de $K = \mathbb{F}_q(T)$ par rapport à la norme non-archimédienne $|\cdot|_\infty$.

On a vu que ce corps est un *analogue des nombres complexes* $\mathbb{C}$ en caractéristique positive.

THÉORÈME 2.4.7 *Le corps $\Omega = \widehat{\overline{K}}_\infty$ est algébriquement clôs.*

PREUVE. Pour un polynôme

$$g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in k[X]$$

on pose $\|g\| = \max_i |b_i|$. On commence par

LEMME 2.4.8 *Soit k un corps avec une norme $|\cdot|$,*

$$g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in k[X]$$

un polynôme avec $|b_i| \leq R = \|g\|$. Alors il existe une constante $C = C(R)$ telle que pour toutes les racines β de $g(X)$ on a $|\beta| < C$. En fait,

$$C = \begin{cases} \max\{1, R\}, & \textit{si la norme est non-archimédienne} \\ \max\{1, nR\}, & \textit{sinon.} \end{cases}$$

Lemme 2.4.8 $\Rightarrow$ théorème 2.4.7

Soit

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \Omega[X]$$

On montrera qu'il existe une racine $r \in \Omega$ de Ω.

Pour tout a_i on considère une suite $\{a_{ij}\} \subset \overline{K}_\infty$ telle que $a_{ij} \to a_i$, et on pose

$$g_j(X) = X^n + a_{n-1,j}X^{n-1} + \cdots + a_{1,j}X + a_{0,j} \in \overline{K}_\infty[X]$$

et soient $r_{i,j} \in \overline{K}_\infty$ toutes les racines de $g_j(X)$. On va construire une suite de Cauchy $\left\{r_{i_j,j}\right\}$, alors on posera $r = \lim\limits_{j\to\infty} r_{i_j,j} \in \Omega$:

$$f(r) = \lim_{j\to\infty} f(r_{i_j,j}) = \lim_{j\to\infty} g_j(r_{i_j,j}) = 0.$$

Supposons, qu'on a déjà construit j premiers termes d'une telle suite, alors on construira $r_{i_{j+1},j+1}$ par récurrence.

On remarque que $g_{j+1}(z) = \prod_{i=1}^n (z - r_{i,j+1})$, donc

$$\prod_{i=1}^{n} |r_{i_j,j} - r_{i,j+1}| = |g_{j+1}(r_{i_j,j})| = |g_{j+1}(r_{i_j,j}) - g_j(r_{i_j,j})| \leq \delta_j A,$$

où $A = \sup_{l\in\mathbb{N}}(1, |r_{i,l}|^n)$ est une constante, dont l'existence est garantie par le lemme 2.4.8, et

$$\delta_j = |g_{j+1} - g_j| = \max_i |a_{i,j+1} - a_{i,j}| \to 0.$$

Alors il existe un i tel que

$$|r_{i_j,j} - r_{i,j+1}| \leq \sqrt[n]{\delta_j A},$$

et on pose $r_{i_{j+1},j+1} = r_{i,j+1}$.

Preuve du lemme 2.4.8

Soit k un corps avec une norme $|\cdot|$,

$$g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0 \in k[X]$$

un polynôme avec $|b_i| \leq R = \|g\|$.

Supposons que $\beta \in k$ est une racine, telle que $|\beta| > 1$. Il suffit d'écrire

$$0 = \beta^n + \beta^{n-1}b_{n-1} + \cdots + \beta b_1 + b_0 \Rightarrow \beta = -b_{n-1} - \cdots - \beta^{-(n-2)}b_1 - \beta^{-(n-1)}b_0,$$

donc

$$|\beta| \leq \begin{cases} \max\{1, R\}, & \text{si la norme est non-archimédienne} \\ \max\{1, nR\}, & \text{sinon.} \end{cases}$$ □

Rappel : fonction entière, attachée à un A-réseau

Définition 2.4.4 *Soit X un sous-A-module dans le corps complet algébriquement clôs*

$$\Omega = \widehat{\overline{K}}_\infty$$

obtenu à partir de la complétion d'une clôture algébrique du corps $K_\infty = \mathbb{F}_q((T^{-1}))$, la complétion de $K = \mathbb{F}_q(T)$ par rapport à la norme non-archimédienne $|\cdot|_\infty$.

On dit que X est un A-réseau si pour toute boule $\mathcal{D}_a(R)$ l'intersection $\mathcal{D}_a(R) \cap X$ est finie.

Soit X un A-réseaux. On définie une fonction

$$e_X(z) = z \prod_{X \ni l \neq 0} \left(1 - \frac{z}{l}\right), \tag{2.10}$$

Proposition 2.4.5 *Soit X un A-réseaux.*

(a) La fonction $e_X(z)$ donnée par (2.10), est une fonction entière dans Ω avec les zéros simples en $l \in X$.

(b) La fonction $e_X(z)$ est X-périodique et $\mathbb{F}_q$-additive :

$$e_X(z_1 + z_2) = e_X(z_1) + e_X(z_2) \text{ pour tout } z_1, z_2 \in \Omega$$
$$e_X(\alpha z) = \alpha e_X(z) \text{ pour tout } \alpha \in \mathbb{F}_q^*,$$
$$e_X(z) = \sum_{m=0}^{\infty} A_m z^{q^m}.$$

Preuve. On a $e_X(z) = z \prod_{X \ni l \neq 0} \left(1 - \frac{z}{l}\right) = \lim_{n\to\infty} \prod_{\substack{X \ni l \neq 0 \\ |l| < n}} \left(1 - \frac{z}{l}\right)$ à cause de la convergence $\frac{z}{l} \to 0$ lorsque $|l| \to \infty$ pour tout $z \in \Omega$, d'où l'assertion (a).

Puis, on représente X comme l'union croissante

$$X = \bigcup_{n\in\mathbb{N}} H_n$$

des $\mathbb{F}_q$-sous-espaces $H_n \subset X$ de dimension finie. En fait, l'intersection de X avec toute boule donne un tel sous-espace fini. Graçe à la convergence, on représente alors $e_X(z)$ comme une limite des polynômes :

$$e_X(z) = \lim_{n\to\infty} z \prod_{H_n \ni l \neq 0} \left(1 - \frac{z}{l}\right).$$

Tout polynôme $z \prod_{H_n \ni l \neq 0} \left(1 - \frac{z}{l}\right)$ est déterminé par ces racines et donc il est $\mathbb{F}_q$-additifs.

Passant à la limite, on obtient l'assertion (b).

Rappel : définition algébrique des modules de Drinfeld sur Ω

DÉFINITION 2.2.1 *Un* module de Drinfeld φ *de rang* r *(à coefficients dans* Ω*) est un morphisme d'anneaux sur* $\mathbb{F}_q$, $\varphi : A \to \Omega\{\tau\}$ *(ceci dit,* $a \mapsto \varphi(a)$*, et* $\forall \alpha \in \mathbb{F}_q$, $\varphi(\alpha) = \alpha$*) tel que* $\deg_\tau \varphi(T) = r$ *et*

$$\varphi(T) = T + g_1\tau + \ldots + g_r\tau^r, \ g_1, \cdots, g_r \in \Omega.$$

On notera par $\varphi_a(z) = \lambda(\varphi(a))(z)$ le polynôme $\mathbb{F}_q$-additif correspondent à $\varphi(a)$ par l'isomorphisme λ du Théorème 2.1.2. Le degré de

$$\varphi_T(z) = Tz + g_1 z^q + \ldots + g_r z^{q^r},$$

en z est égale donc à q^r.

LEMME 2.4.9 *Pour tout* $a \in A\backslash\{0\}$*, le degré de* $\varphi_a(z)$ *en* z *est égale à* $q^{r\cdot \deg a}$*, ensuite* $D\varphi_a(z) = az$ *(où* $D\varphi(x)$ *désigne la partie linéaire de* $\varphi(x)$*).*

De plus, un tel morphisme φ *est toujours* injectif

PREUVE. On considère la fonction

$$|a|_\varphi := \deg_z(\varphi_a(z)) = q^{\deg_\tau(\varphi(a))}$$

et on vérifie que cette fonction se prolonge par la multiplicativité à une norme du corps K telle que $|T|_\varphi > 1$. Par le théorème d'Ostrowski (théorème 1.1.4), $|a|_\varphi = |a|_\infty^r$, puisque $|T|_\varphi = q^r = |T|_\infty^r$.

L'assertion sur $D\varphi_a(z)$ est vraie pour $a = T$ et pour toutes les constantes $\alpha \in \mathbb{F}_q$, donc elle reste valable pour tous les monômes, et ensuite, pour tous les $a \in A$, grâce à l'homomorphie de φ.

L'assertion sur l'injectivité de φ est impiquée par le fait :

$$\forall a \in A\backslash\{0\}, \ |a|_\varphi = q^{\deg_\tau(\varphi_a(z))} = |a|_\infty^r \neq 0. \qquad \square$$

REMARQUE. Pour tout $f = a_0 + a_1\tau + \ldots + a_m\tau^m \in \Omega\{\tau\}$, on pose $\partial_0(f) = a_0$ (comme dans, [De-Hu], Ch.1). Alors l'assertion (b) signifie :

$$\forall a \in A, \ \partial_0(\varphi(a)) = a.$$

2.5 Définitions analytique des modules de Drinfeld

Soit φ un module de Drinfeld de rang r (à coefficients dans Ω) (un morphisme d'anneaux $\varphi : A \to \Omega\{\tau\}$ $(a \mapsto \varphi(a))$ tel que $\deg_\tau \varphi(T) = r$.

Un réseaux $\Lambda = \Lambda_A \subset \Omega$ de rang r est un sous-A-module dicret de Ω, qui est libre de rang r :

$$\Lambda_A = A \cdot \omega_1 + \cdots + A \cdot \omega_r \subset \Omega.$$

On montrera que tels φ correspondent aux A-réseaux de rang r, $\Lambda_A \subset \Omega$ via l'isomorphisme

$$e_{\Lambda_A} : \Omega/\Lambda \to \Omega$$

donné par la fonction entière

$$e_{\Lambda_A}(z) = z \prod_{\Lambda_A \ni l \neq 0} \left(1 - \frac{z}{l}\right) = \sum_{m=0}^{\infty} A_m z^{q^m}, \tag{2.11}$$

de telle façon que le *théorème d'addition* suivant soit satisfait :

$$\forall a \in A, e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z)) \text{ pour un polynôme } \varphi_a(z) = a_0 z + a_1 z^q + \ldots + a_m z^{q^m}.$$

THÉORÈME 2.5.1 (D'ADDITION) *Pour un A-réseau $\Lambda = \Lambda_A \subset \Omega$ de rang r, on pose*

$$\varphi_a(z) = az \prod_{0 \neq l \in a^{-1}\Lambda/\Lambda} \left(1 - \frac{z}{e_\Lambda(l)}\right),$$

Alors,

$$e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z)) = az \prod_{\Lambda \ni l \neq 0} \left(1 - \frac{az}{l}\right) = \sum_{m=0}^{\infty} A_m (az)^{q^m}, \tag{2.12}$$

PREUVE est impliquée par la propriété des fonctions entières sur Ω. On voit que

$$\forall a \in A \backslash \{0\}, e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z)) = 0, \iff z \in a^{-1}\Lambda_A.$$

La fonction (2.11)

$$e_{\Lambda_A}(z) = z \prod_{\Lambda_A \ni l \neq 0} \left(1 - \frac{z}{l}\right)$$

est un analogue de la fonction σ de Weierstrass, attachée à un tore complexe $\mathbb{C}/\Lambda$, $\Lambda = \langle \omega_1, \omega_2 \rangle$:

$$\sigma_\Lambda(z) = z \prod_{\Lambda \ni l \neq 0}{}' \left(1 - \frac{z}{l}\right) \exp\left(\frac{z}{l} + \frac{z^2}{2l^2}\right),$$

ou de la fonction complexe

$$\frac{\sin(\pi z)}{\pi} = z \prod_{\mathbb{Z} \ni n \neq 0}{}' \left(1 - \frac{z}{n}\right).$$

Ensuite, on montrera que

$$\forall a \in A, e_{\Lambda_A}(az) = \varphi_a(e_\Lambda(z)), \Rightarrow \forall a, b \in A, \varphi_{ab}(z) = \varphi_a(\varphi_b(z)).$$

Forme explicite des polynômes φ_a (description)

Pour un A-réseau donné $\Lambda \subset \Omega$ de rang r on a définit des polynômes :

$$\varphi_a(z) = az \prod_{0 \neq l \in a^{-1}\Lambda/\Lambda} \left(1 - \frac{z}{e_\Lambda(l)}\right),$$

qui donc satisfont la propriété d'homomorphie : $\varphi_{ab}(z) = \varphi_a(\varphi_b(z))$ par la comparaison de ses racines et les coefficients de z :

$$\forall a \in A \backslash \{0\}, e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z)) = 0, \iff z \in a^{-1}\Lambda_A.$$

C'est un analogue des *polynômes de Chebyshev* : On considère les polynômes $T_n(x)$ et $U_n(x)$ de degré n tels que

$$T_n(\cos(z)) = \cos(nz), \text{ et } U_n(\cos(z)) = \frac{\sin((n+1)z)}{\sin(z)}.$$

Réciproquement, pour un morphisme φ donné, on souhaite construire un A-réseau $\Lambda_A \subset \Omega$ de rang r à l'aide d'une série $e(z) = \sum_{m=0}^{\infty} A_m z^{q^m}$, de telle façon que $e(z) = e_{\Lambda_A}(z)$. On définit cette série à partir de la relation de récurrence suivante : pour tout $a \in A$,

$$\varphi_a(\sum_{m=0}^{\infty} A_m z^{q^m}) = e(az) = \sum_{m=0}^{\infty} A_m \cdot (az)^{q^m}$$

d'où on obtient un A-réseau comme le noyau de $e(z)$:

$$\Rightarrow \Lambda_A := \mathrm{Ker}\,(e(z)).$$

(bien sûr, il suffit de satisfaire cette relation pour $a = T \in \mathbb{F}_q[T] = A$, puisque φ est un morphisme d'anneaux sur $\mathbb{F}_q$).

Exemple 2.5.2 (Exponentielle de Carlitz) *: Pour le module de Carlitz $\varphi(T) = T + \tau$, on obtient*

$$e(z) = \sum_{m=0}^{\infty} A_m z^{q^m} = \sum_{m=0}^{\infty} \frac{z^{q^m}}{P_m}$$

où $P_n := \prod_{\substack{f \text{ unitaire} \\ \deg f = n}} f(T) = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}}$. *On peut montrer que $e(z)$ satisfait la relation de récurrence : pour tout $a \in A$*

$$\varphi_a(\sum_{m=0}^{\infty} A_m z^{q^m}) = e(az) = \sum_{m=0}^{\infty} A_m \cdot (az)^{q^m}$$

2.6 Lien entre les définitions analytiques et algébriques des modules de Drinfeld

Nous venons d'établir le résultat suivant :

Théorème 2.6.1 (Drinfeld) *Il existe une bijection entre les deux ensembles de classes d'isomorphisme*

$$\left\{ \begin{array}{c} A\text{-réseaux de rang } r \\ \Lambda_A = A \cdot \omega_1 + \cdots + A \cdot \omega_r \subset \Omega \end{array} \right\} \Big/ \begin{array}{c} \sim \\ (isom) \end{array}$$

$$\longleftrightarrow \left\{ \begin{array}{c} \text{morphismes d'anneaux sur } \mathbb{F}_q,\ \varphi : A \to \Omega\{\tau\} \\ a \mapsto \varphi(a) \text{ tels que } \deg_\tau \varphi(a) = r \cdot \deg a \text{ et} \\ \varphi(a) = a + a_1\tau + \cdots + a_m\tau^m, m = r \cdot \deg a \end{array} \right\} \Big/ \begin{array}{c} \sim \\ (isom) \end{array}$$

Notations. On notera par $\varphi_a(z) = \lambda(\varphi(a))(z) = \tilde{\varphi}(a)(z)$ le polynôme $\mathbb{F}_q$-additif correspondent à $\varphi(a)$ par l'isomorphisme λ du Théorème 2.1.2. Le degré de $\varphi_a(z)$ en z est égale donc à $q^{r \cdot \deg a}$.

Par ce qui précède, on associe à un réseau $\Lambda_A = A \cdot \omega_1 + \cdots + A \cdot \omega_r \subset \Omega$ de rang r une fonction Ω-analytique entière e_{Λ_A} donnée par l'égalité (2.10). Puis on a utilisé la propriété connue des fonctions Ω-analytiques entières (sur un corps algébriquement clos et complet pour une norme non-archimédienne) : telles fonctions sont déterminées à une constante multiplicative près par son *diviseur* (l'ensemble des zéros comptés avec multiplicités), voir théorème 2.4.3, ainsi que [Kob80] et [CP]. Par la définition (2.10), le diviseur de e_{Λ_A} coïncide avec Λ_A, et tous les zéros sont *simples* car

$$e_{\Lambda_A}(z) = z \prod_{\Lambda \ni l \neq 0} \left(1 - \frac{z}{l}\right) = \sum_{m=0}^{\infty} A_m z^{q^m},$$

et la dérivée de $e_{\Lambda_A}(z)$ est $\equiv 1$.

Rapellons que par proposition 2.4.5 la fonction $e_{\Lambda_A}(z)$ est Λ_A-périodique et additive :

$$e_{\Lambda_A}(z_1+z_2) = e_{\Lambda_A}(z_1) + e_{\Lambda_A}(z_2) \text{ pour tout } z_1, z_2 \in \Omega$$
$$e_{\Lambda_A}(\alpha z) = \alpha e_{\Lambda_A}(z) \text{ pour tout } \alpha \in \mathbb{F}_q^*.$$

En effet, pour tout z_2 fixé, les fonctions

$$z \mapsto e_{\Lambda_A}(z+z_2) - e_{\Lambda_A}(z_2), z \mapsto e_{\Lambda_A}(z),$$
$$z \mapsto e_{\Lambda_A}(\alpha z), z \mapsto \alpha e_{\Lambda_A}(z) \text{ pour tout } \alpha \in \mathbb{F}_q^*.$$

ont les mêmes diviseurs et les mêmes coefficients de z.

2.7 Torsion des modules de Drinfeld sur Ω

Un corollaire important de la description analytique des modules de Drinfeld donne la forme précise de la a-torsion pour tout $a \in A\backslash\{0\}$, c'est à dire, du A-module fini

$$_a\varphi = \{z \in \Omega \mid \varphi_a(z) = 0\}$$

formé par toutes les racines du polynôme $\varphi_a(z)$ $\mathbb{F}_q$-additif de degré $q^{r\cdot \deg a}$.

Ici φ est un module de Drinfeld de rang r (à coefficients dans Ω) (un morphisme d'anneaux $\varphi : A \to \Omega\{\tau\}$ $(a \mapsto \varphi(a))$ tel que $\deg_\tau \varphi(T) = r$.

En effet, pour un réseaux $\Lambda_A \subset \Omega$ de rang r on a

$$\Lambda_A = A\cdot\omega_1 \oplus \cdots \oplus A\cdot\omega_r \subset \Omega,$$

donc

$$e(az) = \varphi(e(z)) \Rightarrow {}_a\varphi \cong \Lambda_A/a\Lambda_A \cong (A/aA)^r,\ z \mapsto ae^{-1}(z) \bmod a\Lambda_A.$$

Cette description est analogue de la description classique de l'ensemble des points de n-division d'un cercle

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{\exp\frac{2i\pi a}{n} \;\middle|\; a = 0, 1, \cdots n-1\right\}$$

ou d'un tore complexe $\mathbb{C}/\Lambda$, $\Lambda = \langle\omega_1, \omega_2\rangle$, (c'est à dire, d'une courbe elliptique) :

$$E_n = \left\{\frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \;\middle|\; a, b \bmod n\right\}.$$

2.8 Analogies entre $\mathbb{Z}$ et $A = \mathbb{F}_q[T]$

$\mathbb{Z}$ (un anneau euclidien) $\mathbb{Z}$-modules (=groupes abéliens)	$A = \mathbb{F}_q[T]$ (un anneau euclidien) A-modules
$\mathbb{Q} = Quot(\mathbb{Z})$ (le corps des fractions de $\mathbb{Z}$)	$K = \mathbb{F}_q(T)$ (le corps des fractions de A)
Places finies de $\mathbb{Q}$: les nombres premiers p	Places finies de K : idéaux premiers $(f) \subset A$ $f(T) \in A$ (polynômes unitaires irréductibles)
une seule place infinie de $\mathbb{Q}$: la norme archimédienne usuelle $\lvert x\rvert = \lvert x\rvert_\infty$	une seule place infinie de K : la norme en $\infty \in \mathbb{P}^1_q$, $\lvert f/g\rvert_\infty = q^{\deg(f)-\deg(g)}$
la complétion de $\mathbb{Q}$ à l'infinie : $\mathbb{Q}_\infty = \mathbb{R}$ un corps localement compact connexe ($\lvert 10\rvert > 1$, la base de l'écriture décimale)	la complétion de K à l'infinie : $K_\infty = \mathbb{F}_q((T^{-1}))$, un corps localement compact totalement disconnect, $\lvert T\rvert_\infty = q > 1$
$\mathbb{Z} \subset \mathbb{R}$ un sous-anneau discret cocompact $\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} S^1$ (le cercle unité)	$A \subset K_\infty$ un sous-anneau discret cocompact $K_\infty/A \xrightarrow{\sim} T^{-1}\mathbb{F}_q[\![T^{-1}]\!]$
$\mathbb{C} = \overline{\mathbb{R}}$ (*topologiquement fermé, algébriquement clos*)	$\Omega = \widehat{\overline{K}_\infty}$ (la complétion d'une clôture algébrique $\overline{K}_\infty$ du corps K_∞)

2.9 Equation de Weierstrass et le théorème d'addition complexe

(voir aussi Annexe A). L'équation de Weierstrass est utilisée dans la théorie de l'uniformisation complexe des courbes elliptiques. Considérons un *tore complexe* de type $\mathbb{C}/\Lambda$, où $\Lambda = \langle \omega_1, \omega_2 \rangle$ est un réseau de $\mathbb{C}$. On muni $\mathbb{C}/\Lambda$ d'une structure d'une courbe projective complexe de la manière suivante.

Considèrons la fonctions $\wp$ de Weierstrass

$$\wp(u) = \wp(u, \Lambda) = \frac{1}{u^2} + \sum_{l \in \Lambda}{}' \left(\frac{1}{(u+l)^2} - \frac{1}{l^2} \right)$$

(le prime signifie que $l \neq 0$) ; c'est une fonction méromorphe double périodique *paire* sur $\mathbb{C}$ avec les pôles doulble dans les points $u = l$. Pour sa dérivé on a

$$\wp'(u) = \wp'(u, \Lambda) = -2 \sum_{l \in \Lambda} \frac{1}{(u-l)^3};$$

c'est une fonction méromorphe double périodique *impaire*

On pose pour $k \geq 2$

$$G_{2k}(\Lambda) = \sum_{l \in \Lambda}{}' \frac{1}{l^{2k}}.$$

Il est facile à voir que les développements de Laurent de $\wp(u)$ et de $\wp'(u)$ sont

$$\begin{aligned}
\wp(u) &= u^{-2} + \sum_{n=2}^{\infty} (2n-1) G_{2n}(\Lambda) u^{2n-2} = u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6) \\
\wp'(u) &= -2u^{-3} + \sum_{n=2}^{\infty} (2n-1)(2n-2) G_{2n}(\Lambda) u^{2n-3} \\
&= -2u^{-3} + 6G_4 u + 20 G_6 u^3 + \mathcal{O}(u^5)
\end{aligned}$$

D'où on obtient la *relation de Weierstrass* suivante

$$\wp'(u)^2 = 4\wp(u)^3 - g_2 \wp(u) - g_3,$$

où

$$g_2 = 60 \sum_{l \in \Lambda}{}' \frac{1}{l^4}, \qquad g_3 = 140 \sum_{l \in \Lambda}{}' \frac{1}{l^6}.$$

Analogies entre $\mathbb{Z}$ et $A = \mathbb{F}_q[T]$ (suite)

Un $\mathbb{Z}$-réseau : un sous-$\mathbb{Z}$-module discret $\Lambda_{\mathbb{Z}} \subset \mathbb{C}$, le rang de $\Lambda_{\mathbb{Z}}$=1, 2 où $(\varphi_n(P) = P + \cdots + P \quad (n\ fois))$	Un A-réseau : un sous-A-module discret $\Lambda_A \subset \Omega$ (A-rang de Λ_A est $r \in \mathbb{N}$) $\Lambda_A = A \cdot \omega_1 + \cdots + A \cdot \omega_r \subset \Omega$ $(\varphi_a(z) = a_0 z + a_1 z^q + \ldots + a_m z^{q^m})$
Une courbe elliptique sur $\mathbb{C}$ le groupe quotient abélien $E(\mathbb{C}) = \mathbb{C}/\Lambda_{\mathbb{Z}}$	Module de Drinfeld sur Ω le A-module quotient Ω/Λ_A
Description algébrique : une *courbe projective* $y^2 = 4x^3 - g_2 x - g_3 \subset \mathbb{P}^2$	Description algébrique : *un morphisme d'anneaux* $\varphi : A \to \mathrm{End}\Omega/\Lambda_A \subset \Omega\{\tau\}$, $a \mapsto \varphi(a) = a_0 + a_1\tau + \cdots + a_m\tau^m$
Les coefficients de Weierstrass : $y^2 = 4x^3 - g_2 x - g_3$ $g_2 = 60G_4$, $g_3 = 140G_6$	Les coefficients de $\varphi(T) = T + g_1\tau + \ldots + g_r\tau^r$, $r = \mathrm{rk}_A(\Lambda_A)$ $g_1, \cdots, g_r \in \Omega$
Points de torsion de $E(\mathbb{C}) = \mathbb{C}/\Lambda_{\mathbb{Z}}$ pour $n \in \mathbb{Z}$: $\mathrm{Ker}\,\varphi_n = E_n \cong (\mathbb{Z}/n\mathbb{Z})^2$	Points de torsion de φ pour $a \in A$: $\mathrm{Ker}\,\varphi_a = \{z \in \Omega \mid \varphi_a(z) = 0\}$,

Les points de n-division d'un tore complexe $\mathbb{C}/\Lambda$, $\Lambda = \langle \omega_1, \omega_2 \rangle$, (d'une courbe elliptique) :

$$E_n = \left\{ \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \;\middle|\; a, b \bmod n \right\}.$$

Exercices

2.1. *On considère les polynômes de Chebyshev $T_n(x)$ et $U_n(x)$ de degré n (tels que*

$$T_n(\cos(z)) = \cos(nz), \ \textit{et}\ U_n(\cos(z)) = \frac{\sin((n+1)z)}{\sin(z)}).$$

Montrer que $T_n(T_m(x)) = T_{nm}(x)$, et que

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), \quad T_0(x) = 1, T_1(x) = x, \frac{d}{dx}T_n(x) = nU_{n-1}(x)$$

2.2. (Module de Carlitz) *On considère un morphisme d'anneaux $\varphi : A \to A\{\tau\}$ déterminé par l'égalité $\varphi(T) = T + \tau$. (Module de Carlitz (de rang $r = 1$)). Calculer*

$$\varphi(T^3), \varphi(T^2 + T + 1), \varphi(T^4), \varphi(T^5)$$

2.3. (Exponentielle de Carlitz) *On considère le module de Carlitz donné par le morphisme d'anneaux $\varphi : A \to A\{\tau\}$ avec $\varphi(T) = T + \tau$. Soit*

$$P_n := \prod_{\substack{f\ unitaire \\ \deg f = n}} f(T) = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}},$$

(voir exercice 1.5. sur le produit des polynômes unitaires).

Montrer que la fonction

$$e(z) = \sum_{m=0}^{\infty} A_m z^{q^m} = \sum_{m=0}^{\infty} \frac{z^{q^m}}{P_m}$$

satisfait la relation de récurrence : pour tout $a \in A$

$$\varphi_a(\sum_{m=0}^{\infty} A_m z^{q^m}) = e(az) = \sum_{m=0}^{\infty} A_m \cdot (az)^{q^m}$$

(bien sûr, il suffit de satisfaire cette relation pour $a = T \in \mathbb{F}_q[T] = A$).

2.4. *On définit la fonction de Möbius $\mu(n)$ par l'égalité formelle*

$$\sum_{n=1}^{\infty} \mu(n) n^{-s} = \prod_{p} (1 - p^{-s}) = \zeta^{-1}(s)$$

Montrer que

$$\mu(n) = \begin{cases} 0, & \text{si } n \text{ est divisible par } p^2 (p \text{ premier} \\ (-1)^k, & \text{si } n = p_1 \cdot \ldots \cdot p_k, \ p_i \text{ distincts.} \end{cases}$$

2.5. *Soient a_n, b_n deux suites de nombres liées par*

$$b_n = \sum_{d|n} a_d$$

Montrer que

$$a_n = \sum_{d|n} \mu(n/d) b_d$$

Solution : Cette formule est facilement impliquée par l'identité formelle

$$\sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} b_n n^{-s} \zeta(s), \quad \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

2.6. (Nombre de polynômes irréductibles de degré donné.) *Tout élément $t \in \mathbb{F}_{q^n}$ est une racine d'un polynôme irréductible unitaire $f = f_t$ de $\mathbb{F}_q[T]$ de degré d divisant n, En déduire*

$$T^{q^n} - T = \prod_{d|n} \prod_{\substack{f \text{irrductible} \\ \deg f = d}} f(T),$$

Soit ν_d le nombre de polynômes irréductibles de degré d sur $\mathbb{F}_q$. Montrer que

$$q^n = \sum_{d|n} d\nu_d,$$

et pour récupérer ν_d de cette formule on utilise la formule d'inversion de Möbius.

Solution : Une application directe de cette formule montre que

$$n\nu_n = \sum_{d|n} \mu(n/d) q^d.$$

2.7. (Existence de polynômes irréductibles de degré donné.) *En déduire que pour tout n il existe un polynôme irréductible de degré n de $\mathbb{F}_q[T]$*

Solution : On voit facilement (par l'absurde) que l'expression à droit est non nul car elle est la somme des puissances différentes d'un nombre premier. D'autre part, $\nu_n \geq 0$; ceci implique $\nu_n > 0$.

Cours N°4. Mardi le 4 novembre 2003

3 Modules de Drinfeld sur un anneau

Rappels : torsion et endomorphismes des A-modules Ω/Λ

Un $\mathbb{Z}$-réseau : un sous-$\mathbb{Z}$-module discret $\Lambda_{\mathbb{Z}} \subset \mathbb{C}$, le rang de $\Lambda_{\mathbb{Z}}$=1, 2	Un A-réseau : un sous-A-module discret $\Lambda_A \subset \Omega$ (le A-rang de Λ_A est $r \in \mathbb{N}$) $\Lambda_A = A\cdot\omega_1 + \cdots + A\cdot\omega_r \subset \Omega$
Un tore complexe (le cas $r=2$, $\Lambda_{\mathbb{Z}} = \langle\omega_1,\omega_2\rangle$) : le groupe quotient abélien $\mathbb{C}/\Lambda_{\mathbb{Z}}$	Module de Drinfeld sur Ω : le A-module quotient Ω/Λ_A
Une courbe projective $E : y^2 = 4x^3 - g_2x - g_3 \subset \mathbb{P}^2_{\mathbb{C}}$	Un morphisme d'anneaux $a \mapsto \varphi(a) = a_0 + a_1\tau + \cdots + a_m\tau^m$
Les coefficients de Weierstrass : $g_2 = 60\sum_{0\neq l\in\Lambda} l^{-4}$ $\quad g_3 = 140\sum_{0\neq l\in\Lambda} l^{-6}$	Les coefficients du polynôme $\varphi(T) = T + g_1\tau + \ldots + g_r\tau^r$, $r = \mathrm{rk}_A(\Lambda_A)$
Isomorphisme $\mathbb{C}$-analytique $\mathbb{C}/\Lambda_{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{C})$ $z \longmapsto P = (\wp(z),\wp'(z))$, $nP = (\wp(nz),\wp'(nz))$	Isomorphisme Ω-analytique $\Omega/\Lambda_A \xrightarrow{\sim} \Omega$ $z \longmapsto e_\Lambda(z)$, $a * e_\Lambda(z) = e_\Lambda(az) = \varphi_a(e_\Lambda(z))$
Points de torsion de $E(\mathbb{C}) = \mathbb{C}/\Lambda_{\mathbb{Z}}$ pour $n \in \mathbb{Z}\backslash\{0\}$: $n^{-1}\Lambda_{\mathbb{Z}}/\Lambda_{\mathbb{Z}} \cong (\mathbb{Z}/n\mathbb{Z})^2 =$ $\left\{\frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \;\middle|\; a,b \bmod n\right\} \xrightarrow{\sim} \mathrm{Ker}\,(P \mapsto nP)$	Points de torsion de φ pour $a \in A$: $a^{-1}\Lambda_A/\Lambda_A \xrightarrow{\sim} \mathrm{Ker}\,(\varphi_a)$, $\mathrm{Ker}\,(\varphi_a) = \{z \in \Omega \mid \varphi_a(z) = 0\}$,

Les points de n-division d'un tore complexe $\mathbb{C}/\Lambda$, $\Lambda = \langle\omega_1,\omega_2\rangle$:

$$\left\{\frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \;\middle|\; a,b \bmod n\right\} \xrightarrow{\sim} E_n = \mathrm{Ker}\,(P \mapsto nP), z \longmapsto P = (\wp(z),\wp'(z))$$

sont analogues donc aux éléments du A-module fini

$$a^{-1}\Lambda_A/\Lambda_A \xrightarrow{\sim} \mathrm{Ker}\,(\varphi_a) = \{z \in \Omega \mid \varphi_a(z) = 0\},$$

où $\Lambda = \Lambda_A \subset \Omega$ est un A-réseau de rang r (un sous-A-module dicret de Ω, qui est libre de rang r) :

$$\Lambda_A = A\cdot\omega_1 + \cdots + A\cdot\omega_r \subset \Omega.$$

Un tore complexe est isomorphe à une courbe elliptique E sur $\mathbb{C}$

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}),\ E : y^2 = 4x^3 - g_2x - g_3, z \longmapsto (\wp(z),\wp'(z)),$$

où $\wp$ est la fonction de Weierstrass, $\wp(z) = \wp(z,\Lambda) = \dfrac{1}{z^2} + \sum_{l\in\Lambda}{}' \left(\dfrac{1}{(z+l)^2} - \dfrac{1}{l^2}\right)$ (c'est une fonction méromorphe double périodique, le prime signifie que $l \neq 0$) et les coefficients g_2, g_3 sont

$$g_2 = 60\sum_{l\in\Lambda}{}' \frac{1}{l^4}, \qquad g_3 = 140\sum_{l\in\Lambda}{}' \frac{1}{l^6}).$$

On a construit l'isomorphisme des groupes abéliens

$$e_{\Lambda_A} : \Omega/\Lambda \xrightarrow{\sim} \Omega, z \longmapsto x = e_{\Lambda_A}(z)$$

donné par la fonction entière (2.11) :

$$e_{\Lambda_A}(z) = z \prod_{\Lambda_A \ni l \neq 0} \left(1 - \frac{z}{l}\right) = \sum_{m=0}^{\infty} A_m z^{q^m},$$

de telle façon que le *théorème d'addition* suivant soit satisfait :

$$\forall a \in A\backslash\{0\}, e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z))$$

pour le polynôme $\mathbb{F}_q$-additif sur Ω de degré $q^{r \deg a}$:

$$\varphi_a(z) = az \prod_{0 \neq l \in a^{-1}\Lambda/\Lambda} \left(1 - \frac{z}{e_\Lambda(l)}\right) \in \Omega[z]$$

Soit $a \in A\backslash\{0\}$. Dans le corps Ω il n'y a pas de A-torsion pour la *structure habituelle* de A-module, puisque : $az = 0 \Rightarrow z = 0$.

Cependant, l'isomorphisme $e_{\Lambda_A} : \Omega/\Lambda \xrightarrow{\sim} \Omega, z \longmapsto x = e_{\Lambda_A}(z)$ muni Ω d'une *nouvelle structure* de A-module, donnée par la formule

$$a * e_{\Lambda_A}(z) := e_{\Lambda_A}(az) = \varphi_a(e_{\Lambda_A}(z)),$$

pour laquelle la torsion est non-triviale.

(Cette torsion est un analogue des racines d'unité dans $\mathbb{C}$, $\exp(2ik\pi/n) \in \mathbb{C}^\times$, les points de torsion pour la structure de groupe multiplicatif $\mathbb{C}^\times$).

La description ci-dessus montre que

$$\mathrm{Ker}\,(\varphi_a) = \{x \in \Omega \mid a * x = \varphi_a(x) = 0\} = e_{\Lambda_A}(a^{-1}\Lambda_A/\Lambda_A) \cong (A/(a))^r.$$

Exemple. Pour le module de Carlitz $\varphi(T) = T + \tau$, on obtient que pour tout $a \in A\backslash\{0\}$

$$\varphi_a(x) = \sum_{m=0}^{\deg a} a_m x^{q^m},$$

et que le module de torsion est monogène : $\mathrm{Ker}\,(\varphi_a) \cong A/(a)$, puisque le A-réseau correspondant $\Lambda = \Lambda_\varphi$ est de rang 1 (on pose $\forall b \in A, \forall x \in \mathrm{Ker}\,(\varphi_a), b * x = \varphi_b(x)$).

Application : On va déduire que tout endomorphisme $u \in \Omega\{\tau\}$ de module de Carlitz φ est de la forme $u = \varphi_c$ pour un $c \in A$. En effet, soit $u = a_0 + a_1\tau + \cdots + a_m\tau^m$ et on pose $\tilde{u}(x) = a_0x + a_1x^q + \cdots + a_mx^{q^m}, x \in \Omega$. L'égalité $u\varphi(a) = \varphi(a)u$ signifie que u est un morphisme de A-modules pour la nouvelle structure de A-module : $\forall a \in A, \forall x \in \Omega, a * x = \varphi_a(x) \Rightarrow u(a * x) = a * (u(x))$. Ceci implique que $\mathrm{Ker}\,(u)$ est un sous-A-module fini de $\mathrm{Ker}\,(\varphi_b)$ pour un b convenable (ceci dit, $\mathrm{Ker}\,(u)$ est annulé par $x \mapsto b * x = \varphi_b(x)$). Mais on a vu que $\mathrm{Ker}\,(\varphi_b) \cong A/(b)$, puisque le A-réseau correspondant $\Lambda = \Lambda_\varphi$ est de rang 1 donc $\mathrm{Ker}\,(u) = \mathrm{Ker}\,(\varphi_c)$ pour un $c \in A\backslash\{0\}$ convenable. On remarque aussi que les termes constantes des deux polynômes

$$u = a_0 + a_1\tau + \cdots + a_m\tau^m, \varphi_c = c + c_1\tau + \cdots + c_n\tau^n$$

ne s'annulent pas. En effet, d'une part $c \neq 0$. Si $a_0 = 0$, on suppose que

$$u = a_{m_0}\tau^{m_0} + \cdots + a_m\tau^m \text{ avec } a_{m_0} \neq 0, m_0 > 0,$$

et la comparaison des coefficients de τ^{m_0} dans l'égalité $u\varphi_T = \varphi_T u$ montre que $a_{m_0}T = a_{m_0}T^{q^{m_0}}$, qui est impossible. Ceci implique que les polynômes

$$\tilde{u}(x) = a_0x + a_1x^q + \cdots + a_mx^{q^m}, \tilde{\varphi}_c = cx + c_1x^q + \cdots + c_nx^{q^n}$$

sont proportionnels, car toutes ces racines dans Ω sont simples et coïncident, ceci dit, $\tilde{u} = (a_0/c)\tilde{\varphi}_c$. La constante $\beta = a_0/c$ est dans $\mathbb{F}_q^\times$. En effet, comme u est φ_c commutent avec φ_T, ils laissent stable

$\mathrm{Ker}\,(\varphi_T) \cong \mathbb{F}_q$, donc la multiplication par cette constante aussi laisse stable $\mathrm{Ker}\,(\varphi_T) \cong \mathbb{F}_q$, donc $u = \beta\varphi_c = \varphi_{\beta c}$, CQFD.

EXERCICE. Trouver tous les endomorphismes du module ψ de rang r donné par la formule $\psi : A \to \Omega\{\tau\}$, avec $\psi(T) = T + \tau^r$.

Maintenant on va expliquer comment définir les A-modules à coefficients dans une A-algèbre B. Cette construction muni aussi B d'une nouvelle structure de A-module.

3.1 Module de Drinfeld comme un foncteur

Soit B une A-algèbre, c'est à dire, un anneau muni de morphisme de structure $\gamma : A \to B$.

DÉFINITION 3.1.1 *On appelle le noyau de $\gamma : A \to B$ la A-*caractéristique *de l'algèbre B.*

On considère l'anneau $B\{\tau\}$ non–commutatif des polynômes d'une variable τ à coefficients dans B, avec la formule de commutation suivante : $\tau b = b^q \tau$ pour tout $b \in B$.

DÉFINITION 3.1.2 *Un morphisme d'anneau $\varphi : A \to B\{\tau\}$ est dit un module de Drinfeld sur une A-algébre B, si pour tout $a \in A$, le degré* $\deg_\tau \varphi(a) = r \cdot \deg a$, *et* $\varphi(a) = \gamma(a) + b_1\tau + \cdots b_m\tau^m$.

PROPOSITION 3.1.3 *Soit B une A-algèbre, et soit $\varphi : A \to B\{\tau\}$ un morphisme d'anneau (un module de Drinfeld sur une A-algébre B). Alors φ définie un* foncteur *:*

$$\mathcal{F}_\varphi : \{B\text{-}algèbres\ \} \to \{A\text{-}modules\ \}.$$

PREUVE. Soit C une B-algèbre, et on écrit

$$\varphi(a) = b_0 + b_1\tau + \cdots + b_m\tau^m \in B\{\tau\}, \varphi_a = bx + b_1x^q + \cdots + b_mx^{q^m} \in B[x].$$

On vérifie (par les définitions), que l'égalité

$$\forall a \in A, \forall x \in C, a * x = \varphi_a(x),$$

définie une structure de A-module sur chaque B-algèbre C.

Ensuite, tout morphisme de B-algèbres devient un morphisme de A-modules.

3.2 La caractéristique d'Euler - Poincaré d'un module de Drinfeld fini

(voir [Ge], [Tak]). On considère $\varphi : A \to A\{\tau\} \subset \Omega\{\tau\}$ (un module de Drinfeld de rang $r \geq 1$). En particulier, si $B = A/(f)$, on remarque que, pour tout $f \in A$, il y a une autre structure de A–module sur l'anneau $B = A/(f)$, désignée par $(A/(f))_\varphi$ et définie par la formule

$$a * x = \varphi_a(x), \quad x \in A/(f),\ a \in A,$$

DÉFINITION 3.2.1 *Soit*

$$(A/(f))_\varphi \cong A/(f_1^{k_1}) \oplus \cdots \oplus A/(f_t^{k_t})$$

une décomposition où tous les f_i sont unitaires irréductibles. Alors on appelle le produit $f_\varphi = \prod_{i=1}^{t} f_i^{k_i}$ la caractéristique d'Euler-Poincaré *de $(A/(f))_\varphi$.*

REMARQUE. On montrera que si $r = 1$, alors $(A/(f))_\varphi \cong (A/(f_\varphi)$, mais cette égalité n'est pas valable en cas général (même pour $r = 2$, voir exemple 3.6.6).

3.3 Analogue du groupe $E(\mathbb{Z}/p\mathbb{Z})$ et analogue du théorème de Hasse

Places finies de $\mathbb{Q}$: les nombres premiers p	Places finies de K : idéaux premiers $(f) \subset A$ $f(T) \in A$ *(les polynômes unitaires irréductibles)*
une *courbe elliptique* sur $\mathbb{Q}$ $y^2 = 4x^3 - g_2x - g_3 \subset \mathbb{P}^2_{\mathbb{C}}$ (on suppose $g_2, g_3 \in \mathbb{Z}$)	un *homomorphisme* $\varphi : A \to A\{\tau\}$, $a \mapsto \varphi_a = a_0 + a_1\tau + \cdots + a_m\tau^m$ $(\varphi_a(z) = a_0z + a_1z^q + \cdots + a_mz^{q^m})$,
la *réduction* $E \bmod p$: si $p \nmid \Delta_E$ $y^2 = 4x^3 - \overline{g_2}x - \overline{g_3} \subset \mathbb{P}^2_{\overline{\mathbb{F}}_p}$ $(g_2, g_3 \in \mathbb{Z},\ p \nmid g_2^3 - 27g_3^2)$	un *homomorphisme* $\bar\varphi : A \to k\{\tau\}$, $k = A/f$ $a \mapsto \bar\varphi_a = \bar a_0 + \bar a_1\tau + \cdots + \bar a_m\tau^m$ $(\bar\varphi_a(z) = \bar a_0z + \bar a_1z^q + \cdots + \bar a_mz^{q^m}$
$\Phi_p = Frob_p$, $N_{E,p} = \mathrm{Card}\,(E(\mathbb{F}_p))$ $E(\mathbb{F}_p) = \{x \in E(\overline{\mathbb{F}}_p) \mid (\Phi_p - id_E)(x) = 0\}$,	$\Phi_f = \tau^{\deg(f)}$, $f_\varphi =$ un *annulateur* de $(A/f)_\varphi$ $(A/f)_\varphi = \{x \in \overline{k} \mid \Phi_f(x) = x\}$,

3.4 Un analogue du théorème de Hasse, [Po]

THÉORÈME 3.4.1 *Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld à coefficients dans $A = \mathbb{F}_q[T]$, et soit $f \in A$ un polynôme irréductible unitaire. On suppose que la réduction $\varphi \bmod f$, $\varphi \bmod f : A \to (A/(f))\{\tau\}$ soit un module de Drinfeld de rang r (à coefficients dans le corps fini $k = A/(f)$). Alors*

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

Preuve du théorème 3.4.1 : préparation

On utilise l'anneau d'endomorphismes du module de Drinfeld $\bar\varphi = \varphi \bmod f$ sur le corps fini $k = A/(f)$. Cet anneau d'endomorphismes $\mathrm{End}(\bar\varphi)$ est une extension de

$$A = \{\varphi_a \mid a \in A\} \subset k\{\tau\},$$

mais aussi il contient l'élément de Frobenius Φ_f associé à f. La différence $f - f_\varphi$ est un analogue de $\mathrm{Card}\,E(\mathbb{F}_p) - p$ pour les courbes elliptiques E sur $\mathbb{F}_p$.

Comme pour les courbes elliptiques E sur $\mathbb{F}_p$, on exprime la différence $f - f_\varphi$ en terme des racines caractéristiques du *polynôme caractéristique* $P_{\Phi_f}(X) \in A[X]$ de l'élément Φ_f.

Cours N°5. Mardi le 18 novembre 2003

Isogénies et la caractéristique d'Euler-Poincaré

Rappels : la caractéristique d'Euler - Poincaré d'un module de Drinfeld fini

(voir section 3.2, ainsi que [Ge], [Tak]). On considère $\varphi : A \to A\{\tau\} \subset \Omega\{\tau\}$ (un module de Drinfeld de rang $r \geq 1$). En particulier, si $B = A/(f)$, on remarque que, pour tout $f \in A$, il y a une autre structure de A–module sur l'anneau $B = A/(f)$, désignée par $(A/(f))_\varphi$ et définie par la formule

$$a * x = \varphi_a(x), \quad x \in A/(f),\ a \in A,$$

Définition 3.2.1 *Soit*

$$(A/(f))_\varphi \cong A/(f_1^{k_1}) \oplus \cdots \oplus A/(f_t^{k_t})$$

une décomposition où tous les f_i sont unitaires irréductibles. Alors on appelle le produit $f_\varphi = \prod_{i=1}^{t} f_i^{k_i}$ la caractéristique d'Euler-Poincaré *de $(A/(f))_\varphi$.*

Remarque. E.-U.Gekeler utilise la notation : pour l'idéal maximal $\mathfrak{p} = (f) \in A$, $\chi(\varphi, \mathfrak{p}) = f_\varphi$ (voir [Ge]).

Remarque. Pour calculer f_φ on peut choisir une base dans tous les sous-espaces : pour $i = 1, \cdots, t$,

$$A/(f_i^{k_i}) = \left\langle 1, T, \cdots, T^{l_i - 1} \right\rangle \bmod (f_i)$$

On pose $f_i^{k_i} = \sum_{j=0}^{l_i} a_{i,j} T^j$, alors ces sous-espaces sont stables par l'action $x \mapsto T * x = \varphi_T(x)$, et dans la base choisie cette action est donnée par la matrice

$$A_i = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_{i,0} \\ 1 & 0 & \dots & 0 & -a_{i,1} \\ 0 & 1 & \dots & 0 & -a_{i,2} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & -a_{i,l_i-1} \end{pmatrix},$$

dont le polynôme caractéristique est égale à $f_i^{k_i}$. Il vient que f_φ est égale au polynôme caractéristique de φ_T dans une base de $A/(f)$:

$$\varphi_(u) \leftrightarrow (A_1, \cdots, A_t) \in \mathrm{End}(A/(f)).$$

Rappels : analogue du groupe $E(\mathbb{Z}/p\mathbb{Z})$ et analogue du théorème de Hasse (voir section 3.3)

Places finies de $\mathbb{Q}$: les nombres premiers p	Places finies de K : idéaux premiers $(f) \subset A$ $f(T) \in A$ *(les polynômes unitaires irréductibles)*
une *courbe elliptique* sur $\mathbb{Q}$ $y^2 = 4x^3 - g_2x - g_3 \subset \mathbb{P}^2_{\mathbb{C}}$ (on suppose $g_2, g_3 \in \mathbb{Z}$)	un *homomorphisme* $\varphi : A \to A\{\tau\}$, $a \mapsto \varphi_a = a_0 + a_1\tau + \cdots + a_m\tau^m$ $(\varphi_a(z) = a_0z + a_1z^q + \cdots + a_mz^{q^m})$,
la *réduction* $E \bmod p$: si $p \nmid \Delta_E$ $y^2 = 4x^3 - \overline{g_2}x - \overline{g_3} \subset \mathbb{P}^2_{\overline{\mathbb{F}}_p}$ $(g_2, g_3 \in \mathbb{Z},\ p \nmid g_2^3 - 27g_3^2)$	un *homomorphisme* $\bar\varphi : A \to k\{\tau\}$, $k = A/f$ $a \mapsto \bar\varphi_a = \bar a_0 + \bar a_1\tau + \cdots + \bar a_m\tau^m$ $(\bar\varphi_a(z) = \bar a_0z + \bar a_1z^q + \cdots + \bar a_mz^{q^m}$
$\Phi_p = Frob_p$, $N_{E,p} = \mathrm{Card}\,(E(\mathbb{F}_p))$ $E(\mathbb{F}_p) = \{x \in E(\overline{\mathbb{F}}_p) \mid (\Phi_p - id_E)(x) = 0\}$,	$\Phi_f = \tau^{\deg(f)}$, $f_\varphi =$ un *annulateur* de $(A/f)_\varphi$ $(A/f)_\varphi = \{x \in \overline{k} \mid \Phi_f(x) = x\}$,

Rappels : un analogue du théorème de Hasse, [Po] (voir section 3.4)

THÉORÈME 3.4.1 *Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld à coefficients dans $A = \mathbb{F}_q[T]$, et soit $f \in A$ un polynôme irréductible unitaire. On suppose que la réduction $\varphi \bmod f$, $\varphi \bmod f : A \to (A/(f))\{\tau\}$ soit un module de Drinfeld de rang r (à coefficients dans le corps fini $k = A/(f)$). Alors*

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

Preuve du théorème 3.4.1 : préparation
On utilise l'anneau d'endomorphismes du module de Drinfeld $\bar\varphi = \varphi \bmod f$ sur le corps fini $k = A/(f)$. Cet anneau d'endomorphismes $\mathrm{End}(\bar\varphi) \subset k\{\tau\}$ est une extension de l'anneau

$$A \cong \bar\varphi(A) = \{\bar\varphi_a \mid a \in A\} \subset k\{\tau\},$$

mais aussi $\mathrm{End}(\bar\varphi)$ contient l'élément de Frobenius $\Phi_f = \tau^{\deg f} \in Centre k\{\tau\}$ associé à f. La différence $f - f_\varphi$ est un analogue de $\mathrm{Card}\,E(\mathbb{F}_p) - p$ pour les courbes elliptiques E sur $\mathbb{F}_p$.

Comme pour les courbes elliptiques E sur $\mathbb{F}_p$, on exprime la différence $f - f_\varphi$ en terme des racines du polynôme caractéristique $P_{\Phi_f}(X) \in A[X]$ de l'élément Φ_f sur $A \cong \bar\varphi(A)$. Ce polynôme sera défini à l'aide d'une $r \times r$-matrice, représentant Φ_f (à préciser).

REMARQUE. Ne pas confondre $P_{\Phi_f}(X)$ avec le polynôme caractéristique de φ_T sur $A/(f)$.

3.5 Structure d'isogénies d'un A-module sur un corps k

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

DÉFINITION 3.5.1 *On appelle le noyau de $\gamma : A \to k$ la A-caractéristique du corps k, noté $\mathrm{Car}_A(k)$. On écrit $\mathrm{Car}_A(k) = \infty$, si $\mathrm{Ker}\,\gamma = 0$ (pour ne pas confondre avec l'idéal maximal $(T) = (T-0) \subset A$.*

On considère l'anneau $k\{\tau\}$ non–commutatif des polynômes d'une variable τ à coefficients dans k, avec la formule de commutation suivante : $\tau b = b^q\tau$ pour tout $b \in k$. Pour un $u = b_0 + b_1\tau + \cdot + b_m\tau^m \in k\{\tau\}$, on note $\partial_0(u) = b_0 \in k$.

On rappelle la définition générale (définition 3.1.2) dans le cas où $B = k$ est un corps sur A :

DÉFINITION 3.5.2 *Un morphisme d'anneau $\varphi : A \to k\{\tau\}$ est dit un module de Drinfeld sur k, si pour tout $a \in A$, le degré* $\deg_\tau \varphi(a) = r \cdot \deg a$, *et* $\varphi(a) = \gamma(a) + b_1\tau + \cdots + b_m\tau^m$. *Donc* $\partial_0(\varphi(a)) = \gamma(a)$

On notera toujours par $\varphi_a(z) = \lambda(\varphi(a))(z) = \widetilde{\varphi}(a)(z)$ le polynôme $\mathbb{F}_q$-additif sur k, qui corresponde à $\varphi(a)$ par l'isomorphisme λ du Théorème 2.1.2. Le degré de $\varphi_T(z) = \gamma(T)z + g_1z^q + \ldots + g_rz^{q^r}$, en z est égale donc à q^r, et $D\varphi_a(z) = az$ (la partie linéaire de $\varphi_a(z)$).

DÉFINITION 3.5.3 *Soient $\varphi : A \to k\{\tau\}$ et $\varphi' : A \to k\{\tau\}$ deux modules de Drinfeld à coefficients dans k. Un élément $u \in k\{\tau\}$ est dit un* morphisme *de φ dans φ' si*
Mor *pour tout $a \in A$ on a $\varphi'(a)u = u\varphi(a)$;*
End *un* endomorphisme *est un morphisme de φ dans φ ;*
Isog *une* isogénie *est un morphisme non-nul ;*
Hauteur *La* hauteur $\mathrm{ht}(u)$ *d'une isogénie u est un nombre naturel N tel que $u = \tau^N u_s$, où $u_s \in k\{\tau\}$ est un élément tel que $\partial_0(u_s) \neq 0$.*

EXEMPLE 3.5.4 *Soient $\varphi : A \to A/(f)\{\tau\}$ un module de Drinfeld à coefficients dans un corps fini $k = A/(f)$. Alors $\Phi_f = \tau^{\deg f}$ est une isogénie de hauteur $\mathrm{ht}(\Phi_f) = \deg f$ (une telle isogénie est dite purement inséparable).*

EXEMPLE 3.5.5 *Soient $\varphi : A \to k\{\tau\}$ un module de Drinfeld à coefficients dans k. Alors pour tout $b \in A\backslash\{0\}$, l'élément $u = \varphi(b) \in k\{\tau\}$ est une isogénie de φ dans φ (un endomorphisme de φ) car pour tout $a \in A$ on a*

$$\varphi(a)\varphi(b) = \varphi(b)\varphi(a) = \varphi(ab); \mathrm{ht}(\varphi(b)) > 0 \Longleftrightarrow b \in \mathrm{Car}_A(k).$$

On va décrire l'ensemble de toutes les isogénies $u \in k\{\tau\}$ entre deux modules de Drinfeld $\varphi : A \to k\{\tau\}$ et $\varphi' : A \to k\{\tau\}$ à coefficients dans k.

L'hypothèse-clé : on considère les deux cas suivants : soit $\mathrm{Car}_A(k) = \infty$, soit k est un corps fini contenant $A/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$, où $\mathfrak{p} = (g) = \mathrm{Car}_A(k)$ un idéal maximal de A (la A-caractéristique de k), $\mathbb{F}_\mathfrak{p} \cong \mathbb{F}_{q^{\deg f}}$.

THÉORÈME 3.5.6 *Soit $\mathrm{Car}_A(k) = \infty$, soit k est un corps fini contenant $A/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$, et soit $u \in k\{\tau\}$. Soit N un nombre naturel tel que $u = \tau^N u_s$, où $u_s \in k\{\tau\}$ est un élément avec $\partial_0(u_s) \neq 0$.*

Alors u est une isogénie entre deux modules de Drinfeld $\varphi : A \to k\{\tau\}$ et $\varphi' : A \to k\{\tau\}$ à coefficients dans k si et seulement si
(i) $\mathrm{Ker}\,(u_s)$ *est un sous-A-module fini $\subset \overline{k} = \overline{k}_\varphi$*
(ii) $N = 0$ si $\mathrm{Car}_A(k) = \infty$, ou $d_\mathfrak{p} | N$ dans le cas $\mathrm{Car}_A(k) = \mathfrak{p}$, $d_\mathfrak{p} = \dim_{\mathbb{F}_q} \mathbb{F}_\mathfrak{p}$.

REMARQUE. Ce résultat donne un analogue de la déscription connue des sous-groupes distingués comme les noyaux de morphismes.

PREUVE. $\Rightarrow$ On utilise $\varphi'_a u = u\varphi_a$, $u = \tau^N u_s$, alors la comparaison des termes constantes montre que $\forall a \in A, \gamma(a) = \gamma(a)^{q^N}$. Ceci implique :
(i) $N = 0$ si $\mathrm{Car}_A(k) = \infty$ (puisque l'image $= \gamma(A)$ est infinie) ;
(ii) Si $\gamma(A) \cong A/\mathfrak{p} = \mathbb{F}_\mathfrak{p} \subset \mathbb{F}_{q^N} \cong k$ (c'est un sous-corps $\gamma(A) \subset k\{\tau\}$ fixé par τ^N), d'où $d_\mathfrak{p} | N$.

$\Leftarrow$ On considère le corps des fractions $k(\tau) = \mathrm{Frac}(k\{\tau\})$. C'est un corps gauche, construite par Drinfeld comme un sous-corps gauche de $k((\tau^{-1}))$.
On remarque que :
(i) si $u = \varphi_b$, alors $\varphi_b\varphi_a\varphi_b^{-1} = \varphi_a$ puisque $\varphi_a\varphi_b = \varphi_b\varphi_a$;

(ii) si $u = \tau^N$, on a

$$\tau^N \varphi(a) \tau^{-N} = \varphi(a)^{q^N} = \gamma(a)^{q^N} + b_1^{q^N}\tau + \cdots + b_m^{q^N}\tau^m = \gamma(a) + b_1'\tau + \cdots + b_m'\tau^m$$

définie un autre module de Drinfeld sur k, noté φ', puisque $\gamma(a) = \gamma(a)^{q^N}$ pour tout $\gamma(a)$ dans k.

(iii) Cas général :

Lemme 3.5.7 *Pour tout polynôme* unitaire séparable $u \in k\{\tau\}$, $\partial_0(u) \neq 0$, *tel que* $\mathrm{Ker}\,(u)(\overline{k}) = H \subset \overline{k} = \overline{k}_\varphi$ *est un* sous-A module, *on montrera :*

il existe un autre module de Drinfeld, noté φ', *sur* k, *tel que* $\varphi'_a u = u\varphi_a$.

Signification géométrique de φ' : le résultat de la factorisation de φ modulo $\mathrm{Ker}\,(u)$. Notation : $\varphi' = u\varphi u^{-1}$.

Preuve du lemme 3.5.7 :

Premier cas : On suppose tout d'abord que $a \notin \mathfrak{p} = \mathrm{Car}_A(k)$, alors tous les deux φ_a et u sont séparables,

$$\mathrm{Ker}\,(u\varphi_a)(\overline{k}) = \left\{z \in \overline{k} \mid u(\varphi_a(z)) = 0\right\} = \varphi_a^{-1}(H) = H' \supset H$$

puisque H est un sous-A-module, donc

$$\varphi_a(H) \subset H \Rightarrow H \subset \varphi_a^{-1}(\varphi_a(H)) \subset \varphi_a^{-1}(H) = H'.$$

Ensuite,

$$\mathrm{Card}\,(H') = \mathrm{Card}\,(H)\deg_z \varphi_a = \mathrm{Card}\,(H)\mathrm{Card}\,((A/a)^r)$$

par la définition 3.5.2 du rang.

On pose $u(H') = H'' \cong H'/H$, donc

$$\mathrm{Card}\,(H'') = \deg_z \varphi_a \Rightarrow u\varphi_a = \varphi'_a u,$$

où on a noté

$$\varphi'_a(z) = \gamma(a) z \prod_{h'' \in H'' \setminus \{0\}} \left(1 - \frac{z}{h''}\right) \in \overline{k}_{\mathbb{F}_q - additifs}[z].$$

En effet, les polynômes $u\varphi_a$ et $\varphi'_a u$ ont le même ensemble H' des racines, et le même coefficient $\gamma(a)b_0$ de z, où $b_0 = \partial_0(u) \neq 0$.

D'un autre coté,

$$\varphi'(a) \in \overline{k}\{\tau\} \cap k(\tau) = k\{\tau\}$$

Ceci implique que $\varphi' : A \to k\{\tau\}$ est un *morphisme d'anneaux*.

Deuxième cas : Si $a \in \mathfrak{p}$, on écrit $a = 1 + (a-1)$. Alors $\varphi_a(z) = z + \varphi_{a-1}(z)$, $a - 1 \notin \mathfrak{p}$. Par le premier cas,

$$\varphi'_a(z) = z + \varphi'_{a-1}(z) \in k\{\tau\}$$

et $\varphi' : A \to k\{\tau\}$ est un morphisme d'anneaux, donc on a construit φ' tel que u est une igogénie de φ à φ', CQFD.

Corollaire 3.5.8 *Soit* u *est une isogénie entre deux modules de Drinfeld* $\varphi : A \to k\{\tau\}$ *et* $\varphi' : A \to k\{\tau\}$ *à coefficients dans un corps* k. *Alors* φ *et* φ' *ont le même rang.*

Preuve. Il suffit de comparer les degrés des polynômes dans l'égalité $u\varphi_T = \varphi'_T u$.□

Application à la démonstration du théorème 3.4.1 :

Tout d'abord, on remarque en utilisant le degré que le morphisme

$$\bar{\varphi} : A \to k\{\tau\}, k = A/f \text{ est injectif,}$$

donc il détermine un plongement

$$\bar{\varphi} : \mathrm{Frac}(A) = K \hookrightarrow k(\tau) \subset k((\tau^{-1}))$$

du corps commutatif K dans le corps *gauche* $k(\tau)$ construit par Drinfeld [Dr1] comme un sous-corps dans le corps gauche $k((\tau^{-1}))$ des séries de Laurent *non-commutatives*.

Élément de Frobenius d'un module de Drinfeld

Ensuite, on voit l'élément de Frobenius

$$\Phi_f = \tau^{\deg(f)} \in \mathrm{End}(\varphi \bmod f) \supset A,$$

comme un élément *central* de l'anneau non-commutatif $k((\tau^{-1}))$, et on considère
le polynôme charactéristique de Φ_f sur $K \hookrightarrow k(\tau) \subset k((\tau^{-1}))$:

$$P_{\Phi_f}(X) \in A[X], \deg P_{\Phi_f} = r, \text{ avec la propriété } P_{\Phi_f}(\Phi_f) = 0.$$

Propriétés du polynôme caractéristique (sans démonstration)

E.-U. Gekeler a vérifié que ([Ge], Théorème 5.1)

$$P_{\Phi_f}(X) = M_{\Phi_f}(X)^{r_2}$$

est une puissance du polynôme minimal $M_{\Phi_f}(X)$ de Φ_f sur K, avec $r = r_1 \cdot r_2$, où
$r_1 = [K(\Phi_f) : K]$.

Ici $M_{\Phi_f}(X) \in K[X]$ est le polynôme minimale de l'élément $\Phi_f = \tau^{\deg(f)}$ qui engendre une extension $K(\Phi_f)$ finie commutative du corps $K = \mathrm{Frac}(\varphi(A))$ dans $k((\tau^{-1}))$, de degré
$r_1 = [K(\Phi_f) : K]$.

De plus, il montre que $(P_{\Phi_f}(0)) = (f)$, $(P_{\Phi_f}(1)) = (f_\varphi)$ (en utilsant le théorème de Cayley-Hamilton).

Si le temps le permet, on rappelera ces propriétés plus tard.

Valeurs absolues des racines du polynôme caractéristique

Enfin, on montre qu'il n'y a qu'une *seule place* $\widetilde{\infty}$ de $K(\Phi_f)$ au-dessus de ∞, à cause des inclusions

$$K_\infty \hookrightarrow k((\tau^{-1})), K(\Phi_f) \otimes_A K_\infty \hookrightarrow k((\tau^{-1})), \quad T \mapsto \bar{\varphi}_T, T^{-1} \mapsto (\bar{\varphi}_T)^{-1}$$

(on utilise le fait général qu'il existe une *unique prolongement* d'une norme sur K_∞ dans une extension finie $K(\Phi_f) \otimes_A K_\infty$). Ceci implique que toutes les racines w_i du polynôme minimal de Φ sur K ont la même valeur absolue $|w_i|_{\widetilde{\infty}}$ en $\widetilde{\infty}$, donc

$$P_{\Phi_f}(X) = \prod_{j=1}^{r}(X - w_{i_j}), \quad P_{\Phi_f}(1) = \prod_{j=1}^{r}(1 - w_{i_j}), \quad P_{\Phi_f}(0) = (-1)^r \prod_{j=1}^{r} w_{i_j} \Rightarrow$$
$$P_{\Phi_f}(1) - P_{\Phi_f}(0) = 1 - (w_{i_1} + \cdots w_{i_r}) + \cdots + (-1)^{r-1}\sigma_{r-1}(w_{i_1}, \cdots, w_{i_r})$$
$$= \sum_{s=0}^{r-1}(-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}).$$

où $\sigma_s(w_{i_1}, \cdots, w_{i_r})$ est le polynôme élémentaire symétrique de degré $s \leq r-1$.
CONCLUSION :

$$P_{\Phi_f}(1) - P_{\Phi_f}(0) = \sum_{s=0}^{r-1} (-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r})$$
$$|w_i|_\infty = |f|_\infty^{1/r} \quad \Rightarrow f - f_\varphi = P_{\Phi_f}(0) - P_{\Phi_f}(1) \Rightarrow |f - f_\varphi|_\infty \leq |f|_\infty^{(r-1)/r}.$$

COROLLAIRE 3.5.9 *Si $r = 1$ alors $f_\varphi = f + c$, $c \in \mathbb{F}_q^\times$ (une constante non-nulle).*

En effet, dans ce cas $r - 1 = 0$, $|f - f_\varphi|_\infty \leq 1$ donc $f_\varphi = f + c$ puisque

$$f - f_\varphi \in A, \quad \deg(f - f_\varphi) = 0.$$

3.6 Torsion des modules de Drinfeld (description algébrique)

DÉFINITION 3.6.1 *(a) Soit $\varphi : A \to k\{\tau\}$ un module de Drinfeld à coefficients dans un corps k. Alors pour tout idéal $I \subset A$ on pose on pose*

$$_a\varphi := \mathrm{Ker}\,(\varphi_a) \subset \varphi;$$

c'est un sous-foncteur de

$$\mathcal{F}_\varphi : \{k\text{-algèbres }\} \to \{A\text{-modules }\};$$

(b) Pour tout idéal $I \subset A$ on pose

$$_I\varphi := \bigcap_{a \in I} \mathrm{Ker}\,(\varphi_a) = {}_a\varphi, (si\ I = (a));$$

REMARQUE. ${}_I\varphi$ est un A/I-module (il est souvent libre).

THÉORÈME 3.6.2 *Soit $\varphi : A \to k\{\tau\}$ un module de Drinfeld à coefficients dans un corps k, et soit $I \subset A$ un idéal non nul. Alors*

$$_I\varphi(\overline{k}) \cong (A/I)^r$$

si $\mathrm{Car}_A(k) = \infty$, ou si $\mathfrak{p} = \mathrm{Car}_A(k)$ est maximal tel que $(I, \mathfrak{p}) = A$. C'est un A/I-module libre de rang r.

PREUVE. Utilise la décomposition en produit des puissances d'idéaux maximaux

$$I = \mathfrak{q}_1^{\alpha_1} \cdot \ldots \cdot \mathfrak{q}_s^{\alpha_1}$$

avec $\mathfrak{q}_i \neq \mathfrak{p}$. Il vient

$$_I\varphi(\overline{k}) = {}_{\mathfrak{q}_1^{\alpha_1}}\varphi(\overline{k}) \oplus \cdots \oplus {}_{\mathfrak{q}_s^{\alpha_s}}\varphi(\overline{k}),$$

donc on peut supposer $I = \mathfrak{q}^m$. Dans ce cas

$$A/\mathfrak{q}^m \cong A_{(\mathfrak{q})}/\mathfrak{q}^m A_{(\mathfrak{q})},$$

où $V = A_{(\mathfrak{q})} \subset K$ la localisation de A en $\mathfrak{q}$; c'est un anneau de valuation discrète d'idéal maximal $\mathfrak{q}A = (\varpi)$.

NOTATIONS. Soit M un $V = A_{(\mathfrak{q})}$-module fini et soit $\ell(M)$ la *longueur* de M, c'est à dire, $\ell(M) = \log_{|V/(\varpi|}\,|M|$. L'action de $a \in V$ sur $x \in M$ est notée par $a_M x$.

LEMME 3.6.3 ("CRITÈRE DE LIBERTÉ") *Soit M un $V/(\varpi^{2m})$-module fini et soit $\ell(M)$ la longueur de M. Alors*

a) $2\ell(\operatorname{Ker}\varpi_M^m) \geq \ell(M)$,

b) L'égalité est atteinte pour $M \neq 0$ si et seulement si

$$M \text{ est un } V/(\varpi^{2m})\text{-module libre et}$$
$$\operatorname{Ker}\varpi_M^m \text{ est un } V/(\varpi^m)\text{-module libre.}$$

PREUVE voir [De-Hu], Lemma 3.2, p.35 : on décompose M en somme directe de modules de type $V/(\varpi^i)$ avec $0 < i \leq 2m$. Pour toute composante $N \cong V/\varpi^i$ on a

$$\operatorname{Ker}\varpi_N^m = \begin{cases} V/\varpi^i \text{ de longueur } i, & \text{si } i \leq m \\ \varpi^{i-m}V/\varpi^i \text{ de longueur } m, & \text{si } i \geq m \end{cases}$$

ceci implique $2\ell(\operatorname{Ker}\varpi_N^m) = 2\min(i,m) \geq i = \ell(N) \Rightarrow$ assertion (a) par la sommation des longueurs.

b) L'égalité est atteinte pour $N \cong V/\varpi^i \neq 0$ si et seulement si

$$N \text{ est un } V/(\varpi^{2m})\text{-module libre et}$$
$$\operatorname{Ker}\varpi_N^m \text{ est un } V/(\varpi^m)\text{-module libre.}$$

On suppose que N est un $V/(\varpi^{2m})$-module libre, alors

$$\operatorname{Ker}\varpi_N^m \text{ est un } V/(\varpi^m)\text{-module libre} \Longleftrightarrow i = 2m \Longleftrightarrow 2\ell(\operatorname{Ker}\varpi_N^m) = \ell(N)$$

(on remarque que $2\min(i,m) = i, 0 < i \leq 2m \Longleftrightarrow 2m = i$). Ceci prouve le lemme 3.6.3.

PREUVE du théorème 3.6.2.

On pose $I = (a)$, avec $a \notin \mathfrak{p}$, et on remarque que

$$\partial_0(\varphi_a) \neq 0 \Rightarrow \varphi_a \text{ est séparable } \Rightarrow \deg_z \varphi_a = \operatorname{Card}({}_a\varphi(\overline{k}) \Rightarrow$$

$$\boxed{\operatorname{Card}({}_{a^2}\varphi(\overline{k})) = \deg_z \varphi_{a^2} = (\deg_z \varphi_a)^2 = \operatorname{Card}({}_a\varphi(\overline{k}))^2}$$

Ensuite, on applique le lemme 3.6.3 avec $a = \varpi^m \in V$ sur

$$M = {}_{a^2}\varphi(\overline{k}) = {}_{\varpi^{2m}}\varphi(\overline{k}).$$

On a

$$M = {}_{\varpi^{2m}}\varphi(\overline{k}).$$

donc

$$\operatorname{Ker}\varpi_M^m = {}_{\varpi^m}\varphi(\overline{k}) \subset M,$$
$$\operatorname{Card} M = \operatorname{Card}({}_{\varpi^{2m}}\varphi(\overline{k})) = \operatorname{Card}({}_{\varpi^m}\varphi(\overline{k}))^2 = \operatorname{Card}(\operatorname{Ker}\varpi_M^m)^2 \Rightarrow$$
$$\ell(M) = 2\ell(\operatorname{Ker}\varpi_M^m) \Rightarrow \operatorname{Ker}\varpi_M^m \cong (V/\varpi^m)^r \text{ (un } V/(\varpi^m)\text{-module libre)}$$

Ceci prouve le théorème 3.6.2.

REMARQUE. Il vient de la démonstration que

$$\operatorname{Card}(M) = \operatorname{Card}(V/(\varpi))^{\ell(M)} = \operatorname{Card}(V/(\varpi^{2m}))^{\ell(M)/2m},$$
$$\operatorname{Card}(\operatorname{Ker}\varpi_M^m) = \operatorname{Card}(V/(\varpi))^{\ell(\operatorname{Ker}\varpi_M^m)} = \operatorname{Card}(V/(\varpi^m))^{\ell(\operatorname{Ker}\varpi_M^m)/m},$$

donc le rank du $V/(\varpi^m)$-module libre $\operatorname{Ker}\varpi^m$ est égal au

$$\frac{1}{m}\log_{|V/(\varpi)|}(\operatorname{Card}(\operatorname{Ker}\varpi^m)) = \frac{1}{m}\log_{|V/(\varpi)|}(\text{ le nombre des racines du polynôme } \varphi_{\varpi^m}).$$

Le cas de caractéristique finie $\mathfrak{p} \subset A$

Il restre à traiter le cas où $\varphi : A \to k\{\tau\}$, $\mathrm{Car}_A(k) = \mathfrak{p} \subset A$ est un idéal maximal, et $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$.

On considère l'anneau local $V = A_\mathfrak{p}$, on note $\mathfrak{p} = (\varpi)$, et on utilise de nouveau le lemme 3.6.3. Soit h la hauteur de l'endomorphisme φ_ϖ, alors

$$\varphi_\varpi = u_s\tau^h = \tau^h u_s^\circ, \quad \partial_0(u_s) \neq 0 \neq \partial_0(u_s^\circ) \Rightarrow \deg(\varphi_\varpi) = q^h \mathrm{Card}\,({}_\varpi\varphi)(\overline{k}).$$

Il vient que pour tout $n \in \mathbb{N}$,

$$\deg(\varphi_{\varpi^n}) = (\deg(\varphi_\varpi)^n = (q^h \mathrm{Card}\,{}_\varpi\varphi(\overline{k}))^n = q^{nh}\mathrm{Card}\,({}_{\varpi^n}\varphi)(\overline{k}).$$

Donc le lemme 3.6.3 implique que ${}_{\varpi^n}\varphi$ est un $V/(\varpi^n)$-module libre de rang $r - h < r$:

$$\boxed{\mathrm{Card}\,({}_{\varpi^{2n}}\varphi)(\overline{k}) = q^{-2nh}\deg(\varphi_{\varpi^{2n}}) = (q^{-nh}\deg(\varphi_{\varpi^n}))^2 = (\mathrm{Card}\,({}_{\varpi^n}\varphi)(\overline{k}))^2}$$

Définition 3.6.4 *Soit $\varphi : A \to k\{\tau\}$ un module de Drinfeld à coefficients dans un corps k, tel que $\mathrm{Car}_A(k) = \mathfrak{p} \subset A$ est un idéal maximal, et soit $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. La hauteur h de l'endomorphisme φ_ϖ, est dit la* hauteur *de φ. Dans ce cas*

$${}_{\varpi^n}\varphi(\overline{k}) \cong (A/(\varpi^n))^{r-h}.$$

Points de torsion d'une courbe elliptique E sur $\mathbb{Q}$ dans $\mathbb{P}^2(\overline{\mathbb{Q}})$	Points de torsion d'un module φ sur A dans $K^{sep} \subset \Omega$
pour $n \in \mathbb{Z}$, $E_n \cong (\mathbb{Z}/n\mathbb{Z})^2 \subset \mathbb{P}^2(\overline{\mathbb{Q}})$: (un $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module)	pour $a \in A$, $\mathrm{Ker}\,\varphi_a \cong (A/aA)^r \subset K^{sep}$ (un $\mathrm{Gal}(K^{sep}/K)$-module)
Points de torsion de $E(\overline{\mathbb{F}}_p)$: pour un nombre premier $l \in \mathbb{Z}$, $\mathrm{Ker}\,\varphi_l = E_l(\overline{\mathbb{F}}_p) \cong (\mathbb{Z}/l\mathbb{Z})^2$ ou $\mathbb{Z}/l\mathbb{Z}$ (un $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-module)	Points de torsion de $\bar{\varphi}$ dans $\overline{\mathbb{F}}_q$ pour un idéal maximal $\mathfrak{q} \in A$ ${}_\mathfrak{q}\varphi(\overline{k}) \cong (A/\mathfrak{q})^{r'}$, $r' \leq r$. (un $\mathrm{Gal}(\bar{k}/k)$-module)

Corollaire 3.6.5 *Soit $f \in A$ un polynôme irréductible, $k = A/f$. $r = 1$ alors le A-module $(A/f)_\varphi \cong A/(f_\varphi)$ est monogène.*

Preuve vient du fait que si $(a) = \mathrm{Ann}((A/f)_\varphi)$, alors ${}_a\varphi(k) \subset {}_a\varphi(\overline{k})$, et le A-module ${}_a\varphi(\overline{k})$ est monogène.

Exemple 3.6.6 *Un module de Drinfeld fini de rang 2, non-cyclique mod f , avec un calcul des racines du polynôme caractéristique.*

On utilise un exemple donné dans la thèse de I.Potemine [Po], p.74 : $B = A/g$, $q = p = 3$, $\varphi_T = T - T\tau^2 \in A\{\tau\}$, $\tau a = a^3\tau$, $\tau^2 a = a^9\tau^2$, $g = T^2 + 1$ unitaire irréductible sur $\mathbb{F}_3$, $\alpha := T \bmod 3$.

On pose $M := (A/g)_\varphi$, $\forall x \in M, T * x = \alpha x - \alpha x^9$. Mais $x^9 - x \equiv 0$ partout dans M donc $M \cong (A/T)^2$ donc c'est un A-module non-cyclique. Ensuite, $g_\varphi = T^2$.

Calcul des racines du polynôme caractéristique du morphisme de Frobenius *$\Phi = \tau^2$ de $\varphi \bmod g$:*

$$\Phi = \tau^2 \in \mathit{Centre}(\mathbb{F}_9\{\tau\}) \Rightarrow \Phi \in \mathrm{End}(\psi) \supset \psi(A) \cong A, \Phi \neq 0, \ \mathit{où}\ \psi := \varphi \bmod g.$$

Le polynôme caractéristique de Φ sur $\psi(A)$ est donc

$$\boxed{P_\Phi(X) = X^2 + X + g \in A[X]}$$

En effet, on vérifie que $P_\Phi(\Phi) = \Phi^2 + \Phi + g = 0$ dans $\mathbb{F}_9$, où on identifie $g \in A$ avec son image $\psi_g \in \mathbb{F}_9\{\tau\}$. Puisque

$$\psi_g = \psi_{T^2+1} = \psi_{T^2} + 1 = \psi_T\psi_T + 1 = (\alpha - \alpha\tau^2)(\alpha - \alpha\tau^2) + 1 =$$
$$(\alpha^{10} + 1)\tau^4 + (-\alpha^2 - \alpha^{10})\tau^2 + \alpha^2 + 1 \equiv 0$$

On retrouve donc la caractéristique d'Euler-Poincaré $P_\Phi(1) = 1 + 1 + g = T^2$
Racines *du polynôme* $P_\Phi(X)$ *:*

$$\omega_{1,2} = 1 \pm \sqrt{1 - T^2} \in \mathbb{F}_9((T^{-1}))\backslash\mathbb{F}_3((T^{-1}))$$

Elles sont "complexe-conjugées" dans $\mathbb{F}_9((T^{-1}))$ *: on utilise* $\alpha^2 = -1$*, et*

$$1 \pm (1 - T^2)^{1/2} = 1 \pm \alpha T((1 - T^{-2})^{1/2} \in \mathbb{F}_9((T^{-1})),$$

et on voit que

$$|\omega_1|_\infty = |\omega_2|_\infty = 3(= q) \text{ (" } \deg \omega_1 = \deg \omega_2 = 1\text{")},$$

où $g - g_\varphi$=1.

Remarque. *Les corps*

$$\mathbb{F}_9((\tau^{-1})) \supset \mathbb{F}_9((\tau^{-2})) \supset \mathbb{F}_3((\tau^{-2}))$$

sont analogues de $\mathbb{H} \supset \mathbb{C} \supset \mathbb{R}$*.*

Cours N°6. Mardi le 25 novembre 2003

4 Structure d'algèbres d'endomorphismes et calcul du polynôme caractéristique

4.1 Places au-dessus de 0 et de ∞

On considère un module de Drinfeld $\psi : A \to k\{\tau\}$, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k)$ du corps finie $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$.
On pose $k(\tau) = \mathrm{Frac}(k\{\tau\}) \subset k((\tau^{-1}))$ (c'est un corps gauche).

De même façon, on peut voir $k(\tau)$ comme un sous-corps gauche de $k((\tau))$:

$$(a_h\tau^h + \cdots + a_n\tau^n)^{-1} = ((1 + (a_{h+1}\tau a_h^{-1} + \cdots))a_h\tau^h)^{-1}$$
$$= \tau^{-h}a_h^{-1}((1 + (a_{h+1}a_h^{-q}\tau + \cdots))^{-1} = \tau^{-h}a_h^{-1}(1 - (a_{h+1}a_h^{-q}\tau + \cdots) + (a_{h+1}a_h^{-q}\tau\cdots)^2 - \cdots)$$
$$= \sum_{i=-h}^{\infty} b_i\tau^i \in k((\tau)).$$

On utilisera les extensions finies

$$k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p} \supset \mathbb{F}_q, \quad [k : \mathbb{F}_\mathfrak{p}] = m, \ [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d \Rightarrow |k| = q^n, n = m \cdot d,$$

et on pose $\Phi = \tau^n$, alors Φ commute avec $k\{\tau\}$, donc Φ ce trouve dans le centre de l'algèbre gauche $k(\tau)$, et $\Phi \in \mathrm{End}(\psi)$.

Nous avons deux fonctions de degré : $\deg_z : k[z]_{\mathbb{F}_q-\mathrm{additifs}}$ et $\deg_\tau : k\{\tau\} \to \mathbb{Z}$:

$$\deg_z(a_0z + a_1z^q + \cdots + a_nz^{q^n}) = q^n, \deg_\tau(a_0 + a_1\tau + \cdots + a_n\tau^n) = n$$

où $a_n \neq 0$. On a les relations suivantes : pour $\phi, \psi \in k[z]_{\mathbb{F}_q-\mathrm{additifs}}$ et $a, b \in k\{\tau\}$,

$$\deg_z(\phi\psi) = \deg_z(\phi)\deg_z(\psi), \quad \deg_z(\phi + \psi) \leq \max(\deg_z(\phi), \deg_z(\psi)),$$

$$\deg_\tau(ab) = \deg_\tau(a) + \deg_\tau(b), \quad \deg_\tau(a + b) \leq \max(\deg_\tau(a), \deg_\tau(b)).$$

Nous avons les fonctions de hauteur : $\mathrm{ht} : k[z]_{\mathbb{F}_q-\mathrm{additifs}} \to \mathbb{Z}$ and $\mathrm{ht} : k\{\tau\} \to \mathbb{Z}$ défines par les relations

$$\mathrm{ht}(a_hz^{q^h} + \cdots + a_nz^{q^n}) = h, \quad \mathrm{ht}(a_h\tau^h + \cdots + a_n\tau^n) = h,$$

où $a_h \neq 0$. On a $\mathrm{ht}(\phi) = \mathrm{ht}(\lambda(\phi))$, pour l'isomorphisme λ du théorème 2.1.2 sur les polynômes $\mathbb{F}_q$-additifs, et les relations suivantes pour $\phi, \psi \in k[z]_{\mathbb{F}_q-\mathrm{additifs}}$ et $a, b \in k\{\tau\}$:

$$\mathrm{ht}(\phi\psi) = \mathrm{ht}(\phi) + \mathrm{ht}(\psi), \quad \text{et} \quad \mathrm{ht}(ab) = \mathrm{ht}(a) + \mathrm{ht}(b), \mathrm{ht}(\phi + \psi) \geq \min(\mathrm{ht}(\phi), \mathrm{ht}(\psi)).$$

On utilise les notations suivantes $\partial_0 : k[z]_{\mathbb{F}_q-\mathrm{additifs}} \to k$ et $\partial : k\{\tau\} \to k$ défines par

$$\partial_0(\sum_{0\leq i} a_iz^{q^i}) = a_0, \quad \partial(\sum_{0\leq i} a_i\tau^i) = a_0$$

où ∂_0 est la dérivé à l'origine ∂ le terme constant.

PROPOSITION 4.1.1 *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 $\Phi = \infty$ et $\Phi = 0$ de $\mathbb{F}_q(\Phi)$ (c'est à dire, on considère $\Phi = \tau^n$ comme une variable indépendante, et on considère les places de $\mathbb{F}_q(\Phi)$, données par les normes

$$|u|_\infty = q^{\deg_\Phi u} = q^{(\deg_\tau u)/n} \sim q^{\deg_\tau u}, \quad |u|_\Phi = q^{-(\mathrm{ht} u)/n} \sim q^{-\mathrm{ht}(u)},$$

alors tout prolongement de $|u|_\infty$ sur E est une place au dessus de la place $\Phi = \infty$, et tout prolongement de $|u|_\Phi$ sur E est une place au dessus de la place $\Phi = 0$).

PREUVE. On considère les corps gauches

$$k((\tau^{-1})), k((\tau)) \supset k(\tau).$$

Le corps $k((\tau^{-1}))$ est munie de la fonction

$$\deg_\tau : k((\tau^{-1})) \to \mathbb{Z},$$

et $k((\tau))$ est munie de la fonction

$$\mathrm{ht} : k((\tau)) \to \mathbb{Z},$$

Ces fonctions définissent les normes :

$$|u|_\infty = q^{\deg_\tau u},$$

sur tout sous-corps commutatif contenu dans $k((\tau^{-1}))$, et

$$|u|_0 = q^{-\mathrm{ht}(u)}$$

sur tout sous-corps commutatif contenu dans $k((\tau))$.

En particulier, 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 $\Phi = \infty$ et $\Phi = 0$ de $\mathbb{F}_q(\Phi)$.

4.2 Endomorphismes

(voir [De-Hu], §4). Soit $\delta(u) = \deg_z u(z)$ le degré du polynôme additif $u \in \mathrm{End}_k(\psi)$. La fonction $\delta : \mathrm{End}_k(\psi) \to \mathbb{Z}$ donc se prolonge sur

$$\begin{array}{ccccc} \mathrm{End}_k(\psi) & \longrightarrow & \mathrm{End}_k(\psi) \otimes_A K & \longrightarrow & \mathrm{End}_k(\psi) \otimes_A K_\infty \quad \subset k((\tau^{-1})) \\ \downarrow \delta & & \downarrow \delta & & \downarrow \delta \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q} \end{array}$$

REMARQUE. On étudie la A-algèbre $\mathrm{End}_k(\psi)$ à l'aide de δ en utilisant les propriétés suivantes de δ : $\mathrm{End}_k(E) \otimes_A K_\infty \to \mathbb{Q}$:

(1) $\delta(u) \geq 0$ et $\delta(u) = 0$ si et seulement si $u = 0$.

(2) $\delta(au) = \|a\|\delta(u)$ pour $a \in F$, où $\|a\| = \delta(\psi_a)$ est une norme sur K, équivalente à $|\cdot|_\infty$, puisque $\|T\| = \delta(\psi_T) = r > 1$ (on utilise le théorème 1.1.4 (d'Ostrowski).

(3) $\delta(vu) = \delta(v)\delta(u)$.

De plus, $\mathrm{End}_k(\psi) \hookrightarrow \mathrm{End}_k(\psi) \otimes_A K_\infty$ est un sous A-module discret dans cet espace vectoriel métrique sur K_∞, voir [De-Hu], (4.9)(2).

On va montrer tout d'abord que $\mathrm{End}_k(\psi)$ est un A-module de génération finie. On utilisera les deux lemmes suivants :

LEMME 4.2.1 *Soit $A^n \subset X \subset K_\infty^n$ un A-module discret. Alors X est de génération finie.*

PREUVE. Pour tout i on observe que $\mathfrak{m}_\infty^i + A \subset K_\infty$ est d'indice fini, e.g. $t^{-i}k[\![1/t]\!] + k[t] \subset k((t^{-1}))$ est d'indice $\mathrm{Card}\,(k)^i$. Il existe un i avec $X \cap (\mathfrak{m}_\infty^i)^n = 0$ puisque X est discret, donc il existe une inclusion de X dans $(K_\infty/\mathfrak{m}_\infty^i)^n$ et il existe une inclusion de X/A^n dans le A-module fini $(K_\infty/\mathfrak{m}_\infty^i + A)^n$. Puisque A^n est de génération finie, il vient que X est un A-module de génération finie.

PROPOSITION 4.2.2 *Pour tout espace vectoriel V sur K de $\mathrm{End}_k(\psi) \otimes_A K$, il vient que $V \cap \mathrm{End}_k(\psi)$ est un A-module libre de rang finie.*

PREUVE. Pour $V_\infty = K_\infty \otimes_K V$, il vient que $X = V \cap \mathrm{End}_k(\psi) = V_\infty \cap \mathrm{End}_k(\psi)$ et on peut supposer que X engendre V et donc V_∞, ou son sous-espace. Soit $x_1, \ldots, x_n$ une base de V_∞ avec $x_i \in X$. Alors avec cette base $A^n \subset X \subset K_\infty^n = V_\infty$ et on se ramène au lemme 4.2.2 puisque $\mathrm{End}_k(\psi)$ est est un sous-A-module discret de $\mathrm{End}_k(\psi) \otimes_A K_\infty$. Pour montrer que $X = V \cap \mathrm{End}_k(\psi)$ est libre, il reste à remarquer qu'il n'a pas de A-torsion et il est de génération finie (sur l'anneau principal A).

COROLLAIRE 4.2.3 *Le A-module $\mathrm{End}_k(\psi)$ est libre.*

PREUVE. Soit $W = \oplus_i W_i$ où $W = \mathrm{End}_k(\psi) \otimes_A K$ et $\dim_K W_i$ est finie. Alors $X_i = \mathrm{End}_k(\psi) \cap W_i$ est libre par Proposition 4.2.2 et les restrictions des projections $W \to W_i$ sur $f_i : \mathrm{End}_k(\psi) \to X_i$ définissent un morphisme $f : \mathrm{End}_k(\psi) \to \oplus_i X_i$ sur un module libre avec $\mathrm{Ker}\,(f) = 0$. Donc $\mathrm{End}_k(\psi)$ est libre.

Pour éstimer le rang on utilise le lemme suivant.

LEMME 4.2.4 *Soit $a \in A$ premier à la A-caractéristique de k. Alors l'application*

$$\mathrm{End}_k(\psi) \otimes (A/a) \to \mathrm{End}_k(\psi_a)$$

est injective.

PREUVE. Si $w \in \mathrm{End}(\psi)$ et $w(\mathrm{Ker}\,(\psi_a)) = 0$ alors il vient que $w = v\psi_a$, et $w|\psi_a = 0$ implique $w \in \mathrm{End}(\psi)a$.

Maintenant on résume tous ces propriétés de base dans le théorème suivant :

THÉORÈME 4.2.5 *Soit ψ un module de Drinfeld sur un corps algébriquement clos $\overline{k}$ de rang r. Alors*
(1) $\mathrm{End}(\psi)$ *est un A-module libre de rang $\leq r^2$, et*
(2) $\mathrm{End}(\psi) \otimes_A K_\infty$ *est un corps, et il existe une inclusion de* $\mathrm{End}(\psi)$ *comme un sous-A-module discret dans cet espace vectoriel normé sur K_∞.*

PREUVE. (1) Le fait que $\mathrm{End}(\psi)$ est projectif est contenu dans Corollaire 4.2.3 et l'injectivité de $\mathrm{End}_k(\psi) \otimes (A/a) \to \mathrm{End}_k(\psi_a)$ borne le rang par r^2 puisque ψ_a est un A/a-module de rang r pour a premier à la A-caractéristique de k.

(2) On a les inclusions

$$\mathrm{End}(\psi) \otimes_A K \subset \mathrm{End}_k(\psi) \otimes_A K_\infty \subset k((\tau^{-1}))$$

qui montrent que c'est un corps.

De plus, le sous-espace où $\delta = 0$ sur $\mathrm{End}(\psi) \otimes_A K_\infty$ est nul.

REMARQUE 4.2.6

(1) Dans la notation du théorème 4.2.5 l'anneau $\mathrm{End}_k(\psi)$ est commutatif pour k de A-caractéristique ∞, de plus, son rang est $\leq r$,

(2) Puisque l'extension K_∞/K est séparable, $\mathrm{End}(\psi) \otimes_A K_\infty$ est aussi un corps.

4.3 Module de Tate $T(\psi)_{\mathfrak{q}}$ en place finie $\mathfrak{q}$ attaché a un module de Drinfeld $\psi : A \to k\{\tau\}$

(voir [Ge], p.190). On considère un module de Drinfeld $\psi : A \to k\{\tau\}$, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k)$ d'un corps fini $k = A/\mathfrak{p}$

DÉFINITION 4.3.1 *Soit $\mathfrak{q} \subset A$ un idéal maximal de A, différant de la caractèristique $\mathfrak{p} = \mathrm{Car}_A(k)$.*

(a) On pose

$$\mathfrak{q}^\infty \psi := \varinjlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong (\varinjlim_n A/\mathfrak{q}^n)^r \cong (\varinjlim_n \mathfrak{q}^{-n}/A)^r = (K_{\mathfrak{q}}/A_{\mathfrak{q}})^r$$

C'est un A-module, mais aussi un $A_{\mathfrak{q}}$-module, où $A_{\mathfrak{q}} = \varprojlim_n A/\mathfrak{q}^n$ est la complétion de A en $\mathfrak{q}$, et $K_{\mathfrak{q}} = \mathrm{Frac}(A_{\mathfrak{q}})$ son corps des fractions (il est isomorphe à la complétion du corps K en place attachée au $\mathfrak{q}$).

(b) On définie le module de Tate *$T(\psi)_{\mathfrak{q}}$ attaché a un module de Drinfeld $\psi : A \to A/\mathfrak{p}\{\tau\}$ en place finie $\mathfrak{q}$ comme le $A_{\mathfrak{q}}$-module*

$$T(\psi)_{\mathfrak{q}} = \mathrm{Hom}_{A_{\mathfrak{q}}}(K_{\mathfrak{q}}/A_{\mathfrak{q}}, {}_{\mathfrak{q}^\infty}\psi) \cong \varprojlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong (\varprojlim_n A/\mathfrak{q}^n)^r = (A_{\mathfrak{q}})^r.$$

REMARQUE 4.3.2 *Le A-module $K_{\mathfrak{q}}/A_{\mathfrak{q}}$ est un analogue du groupe abélien divisible $\mathbb{Q}_p/\mathbb{Z}_p \cong \mu_{p^\infty} = \sqrt[p^\infty]{1}$ de toutes les racines de l'unité de degré p^n.*

Sur le module de Tate $T(\psi)_{\mathfrak{q}}$, il existe les structures fondementales suivantes

- Représentation galoisienne

$$\rho_{\mathfrak{q}} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}}) \cong \mathrm{GL}_r(A_{\mathfrak{q}})$$

- Représentation d'algèbre d'endomorphismes

$$\iota_{\mathfrak{q}} : \mathrm{End}(\psi) \otimes A_{\mathfrak{q}} \to \mathrm{End}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}}) \cong \mathrm{M}_r(A_{\mathfrak{q}}), \ (\mathfrak{q} \neq \mathfrak{p}).$$

En effet, le noyau de tout endomorphisme $u \in k\{\tau\}$ de ψ est finie, donc il est déterminé par son action sur les points de torsion. Ceci implique que le morphisme

$$\iota_{\mathfrak{q}} : \mathrm{End}(\psi) \to \mathrm{End}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}})$$

est injective.

4.4 Groupe de Brauer d'un corps et les invariants locales d'algèbres simples centrales (sans démonstrations)

Tout d'abord, on rappelle quelques faits de base sur le groupe de Brauer d'un corps $\mathcal{K}$ (voir [Ma-Pa], p. 157–161).

Une algèbre de dimension finie $\mathcal{A}$ sur $\mathcal{K}$ est dite une algèbre centrale simple sur $\mathcal{K}$, s'il existe $n \geq 1$ tel que $\mathcal{A} \otimes \overline{\mathcal{K}} \cong \mathrm{M}_n(\overline{\mathcal{K}})$, où M_n note la $n \times n$–algèbre matricielle et $\overline{\mathcal{K}}$ est une clôture algébrique de $\mathcal{K}$. Le produit tensoriel induit une structure d'un semigroupe commutatif sur l'ensemble d'algèbres centrales sur $\mathcal{K}$ (modulo un isomorhisme). Le relation d'équivalence suivante transforme cet ensemble dans un groupe : on dit que l'algèbre $\mathcal{A}$ est équivalente à une algèbre $\mathcal{B}$, s'il existe $m, n \geq 1$ tels que $\mathcal{A} \otimes \mathrm{M}_m(\mathcal{K})$ est isomorphe à $\mathcal{B} \otimes \mathrm{M}_n(\mathcal{K})$. Toutes les algèbres matricielles sont équivalentes l'une de l'autre, et elles forment une classe neutre d'algèbres. La classe de l'algèbre $\mathcal{A}^\circ$, inverse à $\mathcal{A}$ (i.e. formée par les mêmes élements et muni de même addition, mais avec la multiplication dans l'ordre opposé), est l'inverse of $\mathcal{A}$ pour la structure de groupe induite par le produit tensoriel. Pour le voir, on considère l'application

canonique $\mathcal{A} \otimes \mathcal{A}^\circ \to \mathrm{End}_{\mathcal{K}}(\mathcal{A})$ (les endomorphismes de l'espace vectoriel $\mathcal{A}$), qui attache à un élément $x \otimes y \in \mathcal{A} \otimes \mathcal{A}^\circ$ la multiplication par x à gauche, suivie par la multiplication par y à droite.

Le noyau de cette application ce réduit à (0), car $\mathcal{A} \otimes \mathcal{A}^\circ$ est simple, et la dimension de $\mathcal{A} \otimes \mathcal{A}^\circ$ coïncide avec la dimension de$\mathrm{End}_{\mathcal{K}}(\mathcal{A})$, i.e. avec $(\dim \mathcal{A})^2$. Donc cette application est un isomorphisme, et $\mathcal{A} \otimes \mathcal{A}^\circ$ est isomorphe à $\mathrm{End}_{\mathcal{K}}(\mathcal{A}) \cong \mathrm{M}_{\dim \mathcal{A}}(\mathcal{K})$.

Le groupe des classes d'algèbres simples centrales sur $\mathcal{K}$ est dit le groupe de Brauer de $\mathcal{K}$ et il est noté par Br $\mathcal{K}$.

Cours N°7. Mardi le 2 décembre 2003

Algèbres d'endomorphismes et leurs applications

Rappels :

On considère un module de Drinfeld $\psi : A \to k\{\tau\}$ sur un corps k fini. Pour éstimer le rang du A-module libre $\mathrm{End}_k(\psi)$ on utilise le lemme suivant.

LEMME 4.2.4 *Soit $a \in A$ premier à la A-caractéristique de k. Alors l'application*

$$\mathrm{End}_k(\psi) \otimes (A/a) \to \mathrm{End}_k(\psi_a)$$

de restriction d'un $w \in \mathrm{End}(\psi) \otimes (A/a) \cong \mathrm{End}(\psi)/a\mathrm{End}(\psi)$ sur le sous-A-module fini $\psi_a \subset \overline{k}_\psi$ est injective.

PREUVE. Si $w \in \mathrm{End}(\psi)$ et $w(\mathrm{Ker}\,(\psi_a)) = 0$ alors il vient que $w = v\psi_a$,
c'est à dire, que $w|\mathrm{Ker}\,\psi_a$ implique $w \in a\mathrm{End}(\psi) = \mathrm{End}(\psi)\psi_a$.

En effet, soit $H = \mathrm{Ker}\,\psi_a$, alors on a

$$\psi_a(x) = \gamma(a)x \prod_{h \in H\setminus\{0\}} \left(1 - \frac{x}{h}\right)$$

puisque le polynôme $\psi_a(x)$ est séparable. De plus $w = \tau^h w_s$, où $\mathrm{Ker}\,w = \mathrm{Ker}\,w_s$ est un sous-A-module fini de $\overline{k}_\psi$, et le polynôme $w_s(x)$ est séparable de terme linéaire bx, $b \in k^*$ (mais il se peut que $w_s(x)$ n'est pas un endomorphisme).

On pose $H' = \mathrm{Ker}\,w = \mathrm{Ker}\,w_s \supset H = \mathrm{Ker}\,\psi_a$, alors $H'' = \psi_a(H') \cong H'/H$. On pose donc

$$v_s = b\gamma(a)^{-1}x \prod_{h \in H''\setminus\{0\}} \left(1 - \frac{x}{h}\right) \in \overline{k}[x]_{\mathbb{F}_q-\text{additifs}}$$

$$v = \tau^h v_s \Rightarrow w_s = v_s(\psi_a) \Rightarrow w = \tau^h w_s = \tau^h v_s(\psi_a) = v(\psi_a)$$

Mais $v = w\psi(a)^{-1} \in k(\tau) \subset k((\tau))$ commute avec tous les $\psi(c)$, $c \in A$, donc

$$v \in k((\tau)) \cap \overline{k}\{\tau\} = k\{\tau\}$$

est un endomorphisme cherché.

4.3. Rappels : Module de Tate $T(\psi)_\mathfrak{q}$ en place finie $\mathfrak{q}$ attaché a un module de Drinfeld $\psi : A \to k\{\tau\}$

(voir [Ge], p.190). On considère un module de Drinfeld $\psi : A \to k\{\tau\}$, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k)$ d'un corps fini $k = A/\mathfrak{p}$.

NOTATIONS.

$$A_\mathfrak{q} = \varprojlim_n A/\mathfrak{q}^n$$
$$= \left\{(x_1, x_2, \cdots, x_n \cdots) \in A/\mathfrak{q} \times A/\mathfrak{q}^2 \times \cdots \times A/\mathfrak{q}^n \times \cdots \middle| \forall n \geq m, x_n \bmod \mathfrak{q}^m = x_m\right\}$$

est la complétion de A en $\mathfrak{q}$, et $K_\mathfrak{q} = \mathrm{Frac}(A_\mathfrak{q})$ est son corps des fractions (il est isomorphe à la complétion du corps K en place attachée au $\mathfrak{q}$).

On note par

$$A_{(\mathfrak{q})} = \left\{\frac{u}{v} \in K \middle| v \notin \mathfrak{q}\right\}$$

le localisé de A en $\mathfrak{q}$, c'est un anneau locale d'idéal maximal $\mathfrak{q}A_{(\mathfrak{q})} = (\varpi)A_{(\mathfrak{q})}$, alors $K = \mathrm{Frac}(A_{(\mathfrak{q})})$. On considère le A-module discret (il est aussi un $A_{\mathfrak{q}}$-module) :

$$K/A_{(\mathfrak{q})} = \bigcup_{n=1}^{\infty} \varpi^{-n} A_{(\mathfrak{q})}/A_{(\mathfrak{q})} \cong K_{\mathfrak{q}}/A_{\mathfrak{q}}.$$

DÉFINITION 4.3.1 (rappel et rectificatif) *Soit $\mathfrak{q} \subset A$ un idéal maximal de A, différant de la caractèristique $\mathfrak{p} = \mathrm{Car}_A(k)$.*

(a) On pose

$$_{\mathfrak{q}^\infty}\psi := \varinjlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong (\varinjlim_n A/\mathfrak{q}^n)^r \cong (\varinjlim_n \mathfrak{q}^{-n}/A)^r = (K_{\mathfrak{q}}/A_{\mathfrak{q}})^r$$

C'est un A-module, mais aussi un $A_{\mathfrak{q}}$-module.

(b) On définie le module de Tate $T(\psi)_{\mathfrak{q}}$ attaché a un module de Drinfeld $\psi : A \to A/\mathfrak{p}\{\tau\}$ en place finie $\mathfrak{q}$ comme le $A_{\mathfrak{q}}$-module

$$T(\psi)_{\mathfrak{q}} = \mathrm{Hom}_{A_{\mathfrak{q}}}(K_{\mathfrak{q}}/A_{\mathfrak{q}}, {}_{\mathfrak{q}^\infty}\psi) \cong \varprojlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong (\varprojlim_n A/\mathfrak{q}^n)^r = A_{\mathfrak{q}}^r.$$

REMARQUE 4.4.1

$$T(\psi)_{\mathfrak{q}} = \mathrm{Hom}_{A_{\mathfrak{q}}}(K_{\mathfrak{q}}/A_{\mathfrak{q}}, {}_{\mathfrak{q}^\infty}\psi) = \varprojlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) =$$
$$= \left\{(x_1, x_2, \cdots, x_n \cdots) \in {}_{\mathfrak{q}}\psi \times {}_{\mathfrak{q}^2}\psi \times \cdots {}_{\mathfrak{q}^n}\psi \times \cdots \times \Big| \forall n \geq m, \psi_{\varpi^{n-m}}(x_n) = x_m\right\}$$

Pour tout n, ${}_{\mathfrak{q}^n}\psi$ est un $A/\mathfrak{q}^n$-module libre de rang r, et $\forall n \geq m, \psi_{\varpi^{n-m}}$ est un morphisme surjectif de $A_{\mathfrak{q}}$-modules de noyau

$$\psi_{\varpi^{n-m}} \subset \psi_{\varpi^n}.$$

REMARQUE 4.4.2 *Le A-module $K_{\mathfrak{q}}/A_{\mathfrak{q}}$ est un analogue du groupe abélien divisible $\mathbb{Q}_p/\mathbb{Z}_p \cong \mu_{p^\infty} = \sqrt[p^\infty]{1}$ de toutes les racines de l'unité de degré p^n.*

Sur le module de Tate $T(\psi)_{\mathfrak{q}}$, il existe les structures fondementales suivantes

- Représentation galoisienne

$$\rho_{\mathfrak{q}} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}}) \cong \mathrm{GL}_r(A_{\mathfrak{q}})$$

(l'action du groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ sur les racines des polynômes ψ_a avec $a \in \mathfrak{q}^n$).

- Représentation d'algèbre d'endomorphismes

$$\iota_{\mathfrak{q}} : \mathrm{End}(\psi) \to \mathrm{End}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}}) \cong \mathrm{M}_r(A_{\mathfrak{q}}), \ (\mathfrak{q} \neq \mathfrak{p}).$$

En effet, le noyau de tout endomorphisme $u \in k\{\tau\}$ de ψ est finie, donc il est déterminé par son action sur les points de torsion (par l'interpolation de Lagrange). Ceci implique que le morphisme

$$\iota_{\mathfrak{q}} : \mathrm{End}(\psi) \to \mathrm{End}_{A_{\mathfrak{q}}}(T(\psi)_{\mathfrak{q}})$$

est injectif.

4.4. Rappels : groupe de Brauer d'un corps et les invariants locales d'algèbres simples centrales (survol, sans démonstrations)

Tout d'abord, on rappelle quelques faits de base sur le groupe de Brauer d'un corps $\mathcal{K}$ (voir [Bour], §10, [Wei74], Ch.IX, [Ma-Pa], p. 157–161).

Une algèbre de dimension finie $\mathcal{A}$ sur $\mathcal{K}$ est dite une algèbre centrale simple sur $\mathcal{K}$, s'il existe $n \geq 1$ tel que $\mathcal{A} \otimes \overline{\mathcal{K}} \cong \mathrm{M}_n(\overline{\mathcal{K}})$, où M_n note la $n \times n$–algèbre matricielle et $\overline{\mathcal{K}}$ est une clôture algébrique de $\mathcal{K}$. Le produit tensoriel induit une structure d'un semigroupe commutatif sur l'ensemble d'algèbres centrales sur $\mathcal{K}$ (modulo un isomorhisme). Le relation d'équivalence suivante transforme cet ensemble dans un groupe : on dit que l'algèbre $\mathcal{A}$ est équivalente à une algèbre $\mathcal{B}$, s'il existe $m, n \geq 1$ tels que $\mathcal{A} \otimes \mathrm{M}_m(\mathcal{K})$ est isomorphe à $\mathcal{B} \otimes \mathrm{M}_n(\mathcal{K})$. Toutes les algèbres matricielles sont équivalentes l'une de l'autre, et elles forment une classe neutre d'algèbres. La classe de l'algèbre $\mathcal{A}^\circ$, inverse à $\mathcal{A}$ (i.e. formée par les mêmes élements et muni de même addition, mais avec la multiplication dans l'ordre opposé), est l'inverse of $\mathcal{A}$ pour la structure de groupe induite par le produit tensoriel. Pour le voir, on considère l'application canonique $\mathcal{A} \otimes \mathcal{A}^\circ \to \mathrm{End}_{\mathcal{K}}(\mathcal{A})$ (les endomorphismes de l'espace vectoriel $\mathcal{A}$), qui attache à un élément $x \otimes y \in \mathcal{A} \otimes \mathcal{A}^\circ$ la multiplication par x à gauche, suivie par la multiplication par y à droite.

Le noyau de cette application ce réduit à (0), car $\mathcal{A} \otimes \mathcal{A}^\circ$ est simple, et la dimension de $\mathcal{A} \otimes \mathcal{A}^\circ$ coïncide avec la dimension deEnd$_{\mathcal{K}}(\mathcal{A})$, i.e. avec $(\dim \mathcal{A})^2$. Donc cette application est un isomorphisme, et $\mathcal{A} \otimes \mathcal{A}^\circ$ est isomorphe à $\mathrm{End}_{\mathcal{K}}(\mathcal{A}) \cong \mathrm{M}_{\dim \mathcal{A}}(\mathcal{K})$.

Le groupe des classes d'algèbres simples centrales sur $\mathcal{K}$ est dit le groupe de Brauer de $\mathcal{K}$ et il est noté par Br $\mathcal{K}$.

Soit $\mathcal{L}/\mathcal{K}$ une extension de $\mathcal{K}$. On l'appelle le corps neutralisant d'une $\mathcal{K}$-algèbre $\mathcal{A}$ si et seulement si $\mathcal{A} \otimes_{\mathcal{K}} \mathcal{L} \cong \mathrm{M}_n(\mathcal{L})$. Les algèbres équivalentes ont les mêmes corps neutralisants.

Soit $\mathrm{Br}(\mathcal{K}, \mathcal{L})$ la partie du groupe de Brauer, formée par les classes de $\mathcal{K}$-algèbres, admettant $\mathcal{L}$ comme un corps neutralisant. C'est un sous-groupe de $\mathrm{Br}(\mathcal{K})$.

Exemple. On pose $\mathcal{A} = k(\tau)$, $\Phi = \tau^n$, $\mathcal{K} = \mathbb{F}_q(\Phi)$, $\mathcal{L} = k(\Phi)$, alors

$$k(\tau) \otimes_{\mathbb{F}_q(\Phi)} k(\Phi) \cong \mathrm{M}_n(k(\Phi)) \cong \mathrm{End}_{\mathcal{L}}(\mathcal{A}).$$

(les endomorphismes de l'espace vectoriel $\mathcal{A}$ sur $\mathcal{L}$). En effet, on considère l'application canonique $\mathcal{A} \otimes_{\mathcal{K}} \mathcal{L} \to \mathrm{End}_{\mathcal{L}}(\mathcal{A})$ (les endomorphismes de l'espace vectoriel $\mathcal{A}$ sur $\mathcal{L}$), qui attache à un élément $x \otimes y \in \mathcal{A} \otimes \mathcal{L}$ la multiplication par x à gauche, suivie par la multiplication par y à droite.

Le noyau de cette application ce réduit à (0), car $\mathcal{A} \otimes_{\mathcal{K}} \mathcal{L}$ est simple, et la dimension de $\mathcal{A} \otimes_{\mathcal{K}} \mathcal{L}$ sur $\mathcal{L}$ coïncide avec la dimension de $\mathrm{End}_{\mathcal{L}}(\mathcal{A})$, i.e. avec $(\dim_{\mathcal{L}} \mathcal{A})^2 = n^2$.

On pose $N = n^2$ et on choisit une base $\{a_1, \ldots, a_N\}$ de $\mathcal{A}$ sur $\mathcal{K}$. Si on considère un isomorphisme

$$F : \mathcal{A} \otimes_{\mathcal{K}} \overline{\mathcal{K}} \xrightarrow{\sim} \mathrm{M}_n(\overline{\mathcal{K}}), \tag{4.1}$$

alors tous les élements $a = \sum_{i=1}^N x_i a_i \in \mathcal{A}$ ($x_i \in \mathcal{K}$) deviennent matrices $F(a) \in \mathrm{M}_n(\overline{\mathcal{K}})$. Alors on vérifie que les applications

$$\mathrm{tred}(a) = \mathrm{Tr}(F(a)), \quad \mathrm{nred}(a) = \det(F(a))$$

sont des fonctions polynômiales de $x_1, \ldots, x_N$ à coefficient dans le corps $\mathcal{K}$. Ces application sont appelées respectivement la trace réduite et la norme réduite d'un élément $a \in \mathcal{A}$:

$$\begin{aligned} &\mathrm{tred}(a) = l_{\mathcal{A}}(x_1, x_2, \ldots, x_N) \text{ une forme linéaire,} \\ &\mathrm{nred}(a) = \Phi_{\mathcal{A}}(x_1, x_2, \ldots, x_N) \text{ un polynôme homogène de degré } n. \end{aligned}$$

Puisque $F(ab) = F(a)F(b)$ par l'isomorphisme (4.1), on a $\mathrm{nred}(ab) = \mathrm{nred}(a)\mathrm{nred}(b)$.

Maintenant, on va décrire l'invariant local

$$\mathrm{inv}_{\mathcal{K}} : \mathrm{Br}\ \mathcal{K} \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{4.2}$$

dans le cas où $\mathcal{K}$ est une extension finie de $\mathbb{Q}_p$ ou $\mathcal{K} \cong \mathbb{F}_q((T))$. Soit $\mathcal{A}$ un corps gauche de centre $\mathcal{K}$, $[\mathcal{A} : \mathcal{K}] = n^2$. La valuation $v = v_{\mathcal{K}}$ de $\mathcal{K}$ possède une unique extension à une valuation $v_{\mathcal{A}}$ de $\mathcal{A}$, qui coïncide avec $v_{\mathcal{K}}$ sur le centre $\mathcal{K}$ de $\mathcal{A}$. Par exemple, on peut d'abord prolonger v sur les corps locaux $\mathcal{K}(\alpha)$ pour $\alpha \in \mathcal{A}$ et ensuite utiliser la compatibilité de ces valeurs absolues prolongées (vu la propriété d'unicité d'un tel prolongement dans les extensions finies d'un corps local). En considérant la réduction de l'algèbre $\mathcal{A}$ modulo la valuation $v_{\mathcal{A}}$ on vérifie que $\mathcal{A}$ contient un sous-corps commutatif maximal $\mathcal{L}$ non-ramifié sur le centre $\mathcal{K}$ (c'est à dire, $v_{\mathcal{A}}(\varpi_{\mathcal{L}}) = 1$ pour l'élément uniformisant $\varpi_{\mathcal{L}}$ de $\mathcal{L}$. On obtient un élément $\delta \in \mathrm{Br}\ \mathcal{K}$ qui corresponde à $\mathcal{A}$ et admet $\mathcal{L}$ comme un corps neutralisant.

Exemple. Soit $[k : \mathbb{F}_q] = n$, $\Phi = \tau^n$,

$$k((\tau)) \supset k((\Phi)) \supset \mathbb{F}_q((\Phi)), \quad [k((\tau)) : k((\Phi))] = n, \ [k((\Phi)) : \mathbb{F}_q((\Phi))] = n.$$

Dans ce cas $\mathcal{K} = \mathbb{F}_q((\Phi))$, $\mathcal{L} = k((\Phi))$, $\varpi_{\mathcal{L}} = \varpi_{\mathcal{K}} = \Phi$.

Il se peut qu'une extension maximale non-ramifiée $\mathcal{L}$ de $\mathcal{K}$ ne soit pas unique dans $\mathcal{A}$, mais toutes telles extensions sont conjugées par le théorème de Skolem–Noether.

Théorème 4.4.3 (Skolem–Noether) *Soient $\mathcal{A}$ une algèbre simple sur un corps $\mathcal{K}$, ayant pour centre $\mathcal{K}$, $\mathcal{B}$ une algèbre simple de rang fini sur $\mathcal{K}$. Si f et g sont deux $\mathcal{K}$-isomorphismes de $\mathcal{B}$ sur des sous-algèbres de $\mathcal{A}$, il existe un automorphisme intérieure θ de $\mathcal{A}$ tel que $g = \theta \circ f$.*

(voir [Bour], p.110).

Ce théorème général implique que tout isomorphisme de $\mathcal{L}$ dans $\mathcal{A}$ sur $\mathcal{K}$ est induit par un automorphisme intérieur de $\mathcal{A}$. Par conséquance, il existe un élément $\gamma \in \mathcal{A}$ tel que $\gamma \mathcal{L} \gamma^{-1} = \mathcal{L}$ et l'automorphisme interieur $x \mapsto \gamma x \gamma^{-1}$, considéré sur le sous-corps $\mathcal{L}$, coïncide avec l'automorphisme de Frobenius $\mathrm{Fr}_{\mathcal{L}/\mathcal{K}}$.

De plus, l'élément γ est déterminé à un facteur de $\mathcal{L}^\times$ près. Soit $v_{\mathcal{A}} : \mathcal{A}^\times \to \frac{1}{n}\mathbb{Z}$ une extension de $v_{\mathcal{K}}$ sur $\mathcal{A}$. Alors on peut définir $\mathrm{inv}_{\mathcal{K}}\delta$ comme l'image de $v_{\mathcal{A}}(\gamma)$ dans le groupe $(\frac{1}{n}\mathbb{Z})/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. Cette définition peut être reformulée, en utilisant le fait que l'application $x \mapsto \gamma^n x \gamma^{-n}$ est égale à $\mathrm{Fr}^n_{\mathcal{L}/\mathcal{K}}$ et donc elle est identité (car $n = [\mathcal{L} : \mathcal{K}]$). Ceci implique que l'élément γ^n commute tous les éléments de $\mathcal{L}$ et $\gamma^n = c \in \mathcal{L}^\times$. Ceci nous donne

$$v_{\mathcal{A}}(\gamma) = \frac{1}{n} v_{\mathcal{A}}(\gamma^n) = \frac{1}{n} v_{\mathcal{A}}(c) = \frac{1}{n} v_{\mathcal{L}}(c). \tag{4.3}$$

Il vient qu'on a

$$\mathrm{inv}_{\mathcal{K}}\delta = i/n \quad (\text{ où } c = \varpi^i_{\mathcal{L}} u),$$

et $u \in \mathcal{O}^\times_{\mathcal{L}}$, $\varpi_{\mathcal{L}}$ est un élément uniformisant de $\mathcal{L}$, i.e. $v_{\mathcal{L}}(\varpi_{\mathcal{L}}) = 1$, $v_{\mathcal{L}}(u) = 0$.

Exemple 4.4.4 *On pose $\mathcal{A} = k((\tau))$, $\mathcal{K} = \mathbb{F}_q((\Phi))$, $\mathcal{L} = k((\Phi))$, alors $\mathrm{Fr}_{L/K}(x) = x^q = \tau x \tau^{-1}$, donc $\gamma = \tau$, $\gamma^n = \tau^n = \Phi$, donc*

$$\mathrm{inv}_{\mathbb{F}_q((\Phi))} k((\tau)) = \frac{1}{n}, \ \textit{et}$$
$$\mathrm{inv}_{\mathbb{F}_q((\Phi^{-1}))} k((\tau^{-1})) = -\frac{1}{n}.$$

Exemple 4.4.5 *On pose $\mathcal{A} = \mathbb{F}_{q^3}((\tau^2))$, $\Phi = \tau^3$, $\mathcal{K} = \mathbb{F}_q((\Phi^2))$, $\mathcal{L} = \mathbb{F}_{q^3}((\Phi^2))$, alors $\mathrm{Fr}_{L/K}(x) = x^q = \tau^4 x \tau^{-4}$, donc $\gamma = \tau^4 = \Phi^2$, $\gamma^3 = \tau^{12} = \Phi^4$, donc*

$$\mathrm{inv}_{\mathbb{F}_q((\Phi^2))} \mathbb{F}_{q^3}((\tau^2)) = \frac{v_{\Phi^2}(\Phi^4)}{3} = \frac{2}{3}.$$

On a donc un corps gauche $\mathcal{A} = \mathbb{F}_{q^3}((\tau^2))$ de centre $\mathcal{K}$, et de dimension 9 sur le centre.

4.5 Classification d'algèbres d'endomorphismes d'un module de Drinfeld

On considère un module de Drinfeld $\psi : A \to k\{\tau\}$, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k)$ du corps finie $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$.

On pose $k(\tau) = \mathrm{Frac}(k\{\tau\}) \subset k((\tau^{-1}))$ (c'est un corps gauche). On utilise les extensions finies

$$k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p} \supset \mathbb{F}_q, \quad [k : \mathbb{F}_\mathfrak{p}] = m, \ [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d \Rightarrow |k| = q^n, n = m \cdot d,$$

et on pose $\Phi = \tau^n$, alors Φ commute avec $k\{\tau\}$, donc Φ ce trouve dans le centre du corps gauche $k(\tau)$, et $\Phi \in \mathrm{End}(\psi)$. Ceci implique que $k(\tau)$ est l'algèbre de division centrale sur $\mathbb{F}_q(\Phi)$ de degré n^2 :

$$k(\tau) \supset k(\Phi) \supset \mathbb{F}_q(\Phi), \quad [k(\tau) : k(\Phi)] = n, \ [k(\Phi) : \mathbb{F}_q(\Phi)] = n.$$

Selon un résultat profond de la théorie du corps de classes, une telle algèbre sur $\mathbb{F}_q(\Phi)$ est déterminée par ces invariantes locales en places du corps $\mathbb{F}_q(\Phi) \cong \mathbb{F}_q(T)$.

Notations. On pose $K = \mathrm{Frac}(\psi(A)) \subset k(\tau)$, et $L = K(\Phi)$ (c'est une extension commutative finie de K.

Lorsqu'on tensorise l'algèbre $k(\tau)$ avec les complétions de $K(\Phi)$ en $\Phi = 0$ et $\Phi^{-1} = 0$, on obtient les invariantes de $k(\tau)$. On a $\mathrm{Fr}_{L/K}(x) = x^q = \tau x \tau^{-1}$, donc $\gamma = \tau$, $\gamma^n = \tau^n = \Phi$, donc

$$\mathrm{inv}_{\mathbb{F}_q((\Phi))}\big(k(\tau) \otimes \mathbb{F}_q((\Phi))\big) = \mathrm{inv}_{\mathbb{F}_q((\Phi))}\big(k((\tau))\big) = \frac{1}{n} \text{ en } \Phi = 0, \text{ et}$$
$$\mathrm{inv}_{\mathbb{F}_q((\Phi^{-1}))}\big(k(\tau) \otimes \mathbb{F}_q((\Phi^{-1}))\big) = \mathrm{inv}_{\mathbb{F}_q((\Phi^{-1}))}\big(k((\tau^{-1}))\big) = -\frac{1}{n} \text{ en } \Phi^{-1} = 0.$$

En toute autre place $\mathfrak{Q}$ de L l'invariant $\mathrm{inv}_{L_\mathfrak{Q}}$ s'annule puisque on a vu que Φ appartient à un seul idéal maximal $\mathfrak{P}$ de $A[\Phi]$ au-dessus de $\mathfrak{p} \subset A$.

Théorème 4.5.1 (Gekeler) *Soit $L = K(\Phi) \subset \mathrm{End}(\psi) \otimes_A K$, 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 $r = r_1 r_2$, et $\mathcal{A} = \mathrm{End}(\psi) \otimes_A K$ est une algèbre de division centrale sur L de rang r_2^2, avec seulement deux invariantes locales non-nuls :

$$\mathrm{inv}_{L_\mathfrak{P}}(\mathrm{End}(\psi) \otimes_L L_\mathfrak{P}) = -\frac{1}{r_2} \text{ en } \mathfrak{P}, \text{ et}$$
$$\mathrm{inv}_{L_{\widetilde{\infty}}}(\mathrm{End}(\psi) \otimes_L L_{\widetilde{\infty}}) = \frac{1}{r_2} \text{ en } \widetilde{\infty}.$$

4.6 Propriétés d'isogénies d'un module de Drinfeld $\varphi : A \to A\{\tau\}$ et calcul du polynôme caractéristique

Normes d'isogénies

On considère l'application

$$N : \mathrm{End}(\psi) \otimes_A K \to K,$$

obtenue comme la composé de la norme réduite

$$\mathrm{nred} : \mathrm{End}(\psi) \otimes_A K \to L,$$

et la norme de l'extension des 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 $H \subset \mathrm{End}(\psi) \otimes_A K$, voir [Ge], p.192, [Wei74], Proposition 11, Ch.IX.

LEMME 4.6.1 *Pour $u \in \mathrm{End}(\psi)$ on a*

$$\deg_\tau N(u) = r \cdot \deg_\tau u.$$

En particulier, $\deg_\tau N(\Phi) = r \cdot \deg_\tau(\tau^n) = rn$.

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

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

puisque $r = r_1 r_2$.

Pour tout idéal maximal $\mathfrak{q} \neq \mathfrak{p}$ de A, et pour tout sous-corps comutatif maximal $H \subset \mathrm{End}(\psi) \otimes_A K$, on considère l'anneau commutatif $\iota_\mathfrak{q}(H) \otimes K_\mathfrak{q}$, qui est une sous-algèbre maximale commutative de $\mathrm{End}_{K_\mathfrak{q}}(T_\mathfrak{q}(\psi) \otimes K_\mathfrak{q})$. On utilise ensuite le fait ci-dessus que l'application de norme coïncide sur H avec le déterminant, voir [Wei74], Proposition 11, Ch.IX.

Ceci implique que

$$N = \det \circ \iota_\mathfrak{q}. \tag{4.4}$$

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

$$P_\Phi(X) = \det(X \cdot \mathrm{Id}_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi)). \tag{4.5}$$

LEMME 4.6.2 *Pour $u \in \mathrm{End}(\psi)$ on a*

$$P_\Phi(X) = M_\Phi(X)^{r_2}, \ \textit{où } r_2 = r/[L:K].$$

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

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

puisque $L = K(\Phi)$.

COROLLAIRE 4.6.3 *Les coefficients du polynôme caractéristique $P_\Phi(X) = M_\Phi(X)^{r_2}$ dans la représentation $\iota_\mathfrak{q}$ se trouvent dans A, et ils ne dépendent pas de $\mathfrak{q}$.*

Propriétés du polynôme caractéristique

Soit $\psi : A \to k\{\tau\}$ un module de Drinfeld, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k)$ d'un corps fini $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. On utilise les extensions finies

$$k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p} \supset \mathbb{F}_q, \ \ [k:\mathbb{F}_\mathfrak{p}] = m, \ [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d \Rightarrow |k| = q^n, n = m \cdot d,$$

et on pose $\Phi = \tau^n$.

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

Nous avons vu que

$$P_{\Phi_f}(X) = M_{\Phi_f}(X)^{r_2}$$

est une puissance du polynôme minimal $M_{\Phi_f}(X)$ de Φ_f sur K, avec $r = r_1 \cdot r_2$, où $r_1 = [K(\Phi_f) : K]$, (voir [Ge], Théorème 5.1).

Ici $M_{\Phi_f}(X) \in K[X]$ est le polynôme minimale de l'élément $\Phi_f = \tau^{\deg(f)}$ qui engendre une extension $K(\Phi_f)$ finie commutative du corps $K = \mathrm{Frac}(\psi(A))$ dans $k((\tau^{-1}))$, de degré $r_1 = [K(\Phi_f) : K]$.

THÉORÈME 4.6.4 (E.-U. GEKELER) *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 caractèristique d'Euler-Poincaré $\chi(k,\psi)$ du A-module fini k_ψ.

(ii) $(P_\Phi(0)) = \mathfrak{p}^m$.

(iii) Pour tous les zéros σ_i de $(P_\Phi(X)$ on a $|\sigma_i|_\infty = q^{n/r}$.

PREUVE. (ii) Nous avons vu que $(P_\Phi(0)) = (N(\Phi))$ appartient à un seul idéal maximal $\mathfrak{p} = (f)$ dans $A = \psi(A) \subset k\{\tau\}$, 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 4.1.1 (rappelons que cette place est donnée par la hauteur, qui est positive seulement au-dessus de $\mathfrak{p}$.

L'exposant m vient de la formule du produit dans K, et du fait que $\deg\Phi = n/r$ 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 ∞, $r_1 = [L : K]$, voir Proposition 4.1.1.

De plus, $\deg\tau(\mathfrak{p}^m)) = \deg(\psi_{f^m}) = rdm = rn$. 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 $|w_i|_{\widetilde{\infty}}$ en $\widetilde{\infty}$, donc $|\sigma_i|_\infty = q^{n/r}$.

(i) Enfin, on calcule la $\mathfrak{q}$-composante de l'idéal principal $(P_\Phi(1))$.

On considère le A-module fini

$$M = \mathrm{Ker}\,(\Phi - 1) = k_\psi,$$

et on pose

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

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

$$(P_\Phi(1))_\mathfrak{q} = (\det\circ\iota_\mathfrak{q}(\Phi - 1)) = (T_\mathfrak{q}(\psi)/\mathrm{Im}\,(\iota_\mathfrak{q}(\Phi - 1)) = \chi(\mathrm{Ker}\,(\Phi - 1)_\mathfrak{q}, \psi) = \chi({}_{\mathfrak{q}^\infty}\psi(k), \psi).$$

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 de produit, leur valuations $\mathfrak{p}$-adiques coïncident, d'où (i).

Rappels : un analogue du théorème de Hasse, [Po] (voir section 3.4)

THÉORÈME 3.4.1 *Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld à coefficients dans $A = \mathbb{F}_q[T]$, et soit $f \in A$ un polynôme irréductible unitaire. On suppose que la réduction $\varphi \bmod f$, $\varphi \bmod f : A \to (A/(f))\{\tau\}$ soit un module de Drinfeld de rang r (à coefficients dans le corps fini $k = A/(f)$). Alors*

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

Application à la démonstration du théorème 3.4.1 :

On voit l'élément de Frobenius

$$\Phi_f = \tau^{\deg(f)} \in \mathrm{End}(\varphi \bmod f) \supset A,$$

comme un élément *central* de l'anneau non-commutatif $k((\tau^{-1}))$, et on considère le polynôme caractéristique de Φ_f sur $K \hookrightarrow k(\tau) \subset k((\tau^{-1}))$:

$$P_{\Phi_f}(X) \in A[X], \deg P_{\Phi_f} = r, \text{ avec la propriété } P_{\Phi_f}(\Phi_f) = 0.$$

Utilisation des propriétés du polynôme caractéristique

Selon théorème 4.6.7 (avec $m = 1$, $n = d = \deg f$, $f = \mathfrak{p}$, [Ge], Théorème 5.1) on a :

$$P_{\Phi_f}(X) = M_{\Phi_f}(X)^{r_2}$$

est une puissance du polynôme minimal $M_{\Phi_f}(X)$ de Φ_f sur K, où $r = r_1 \cdot r_2$, $r_1 = [K(\Phi_f) : K]$.

Ici $M_{\Phi_f}(X) \in K[X]$ est le polynôme minimale de l'élément $\Phi_f = \tau^{\deg(f)}$ qui engendre une extension $K(\Phi_f)$ finie commutative du corps $K = \mathrm{Frac}(\varphi(A))$ dans $k((\tau^{-1}))$, de degré
$r_1 = [K(\Phi_f) : K]$. De plus, $(P_{\Phi_f}(0)) = (f)$, $(P_{\Phi_f}(1)) = (f_\varphi)$.

Valeurs absolues des racines du polynôme caractéristique

Enfin, on montre qu'il n'y a qu'une *seule place* $\widetilde{\infty}$ de $K(\Phi_f)$ au-dessus de ∞, à cause des inclusions

$$K_\infty \hookrightarrow k((\tau^{-1})), K(\Phi_f) \otimes_K K_\infty \hookrightarrow k((\tau^{-1})), \quad T \mapsto \bar{\varphi}_T, T^{-1} \mapsto (\bar{\varphi}_T)^{-1}$$

(on utilise le fait général qu'il existe une *unique prolongement* d'une norme sur K_∞ dans une extension finie $K(\Phi_f) \otimes_K K_\infty$). Ceci implique que toutes les racines w_i du polynôme minimal de Φ sur K ont la même valeur absolue $|w_i|_{\widetilde{\infty}}$ en $\widetilde{\infty}$, donc

$$\begin{aligned}
&P_{\Phi_f}(X) = \prod_{j=1}^{r}(X - w_{i_j}), \quad P_{\Phi_f}(1) = \prod_{j=1}^{r}(1 - w_{i_j}), \quad P_{\Phi_f}(0) = (-1)^r \prod_{j=1}^{r} w_{i_j} \Rightarrow \\
&P_{\Phi_f}(1) - P_{\Phi_f}(0) = 1 - (w_{i_1} + \cdots w_{i_r}) + \cdots + (-1)^{r-1}\sigma_{r-1}(w_{i_1}, \cdots, w_{i_r}) \\
&= \sum_{s=0}^{r-1}(-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}).
\end{aligned}$$

où $\sigma_s(w_{i_1}, \cdots, w_{i_r})$ est le polynôme élémentaire symétrique de degré $s \leq r - 1$.
Conclusion :

$$\begin{aligned}
&P_{\Phi_f}(1) - P_{\Phi_f}(0) = \sum_{s=0}^{r-1}(-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}) \\
&|w_i|_{\widetilde{\infty}} = |f|_\infty^{1/r} \quad \Rightarrow f - f_\varphi = P_{\Phi_f}(0) - P_{\Phi_f}(1) \Rightarrow |f - f_\varphi|_\infty \leq |f|_\infty^{(r-1)/r}.
\end{aligned}$$

Corollaire 4.6.5 *Si $r = 1$ alors $f_\varphi = f + c$, $c \in \mathbb{F}_q^\times$ (une constante non-nulle).*

En effet, dans ce cas $r - 1 = 0$, $|f - f_\varphi|_\infty \leq 1$ donc $f_\varphi = f + c$ puisque

$$f - f_\varphi \in A, \quad \deg(f - f_\varphi) = 0.$$

Dans les calculs pratiques du polynôme $P_{\Phi_f}(X)$ (voir [Po], p.74), on utilise la borne

Corollaire 4.6.6 *Pour les coefficients $c_i \in A$ du polynôme caractéristique $P_{\Phi_f}(X) = \sum_{i=0}^{r} c_i X^{n-i}$ on a l'inégalité suivante :*

$$\deg(c_i) \leq \left[\frac{i \deg f}{r}\right] \quad (i = 0, \cdots, r). \tag{4.6}$$

Exemple de calcul du polynôme caractéristique, voir [Po], p.74

Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau + \tau^2,$$

On pose $q = 3$, $f = T^2 + 1$, $k = A/(f)$, $\psi : A \to k\{\tau\}$ la réduction $\varphi \bmod g$.

(a) Calculer le polynôme caractéristique de l'élément $\Phi_\varphi = \tau^2$ sur le sous-corps $\mathrm{Frac}(\psi(A))$ dans $k\{\tau\}$.

(b) Pour tout idéal maximal $\mathfrak{q} \subset A$ montrer que

$$\varinjlim_{\mathfrak{q}^n} {}_{\mathfrak{q}^n}\varphi(\overline{k}) \cong \begin{cases} (K/A_{(\mathfrak{q})})^2, & \text{si } \mathfrak{q} \neq (f) \\ K/A_{(\mathfrak{q})}, & \text{si } \mathfrak{q} = (f). \end{cases}$$

(c) Décomposer le module A-divisible $\overline{k}_\varphi$ en somme directe de A-modules isomorphes à

$$K/A_{(\mathfrak{q})} = \varinjlim_{n} \mathfrak{q}^{-n} A_{(\mathfrak{q})}/A_{(\mathfrak{q})}.$$

Solution : On pose $k = \mathbb{F}_3[\alpha]$, où $\alpha^2 + 1 = 0$. On a

$$\varphi_{T^2+1} = 1 + T^2 + (T^3 + T)\tau + (T + T^9 + 1)\tau^2 + 2\tau^3 + \tau^4,$$

d'où $\psi_{T^2+1} = (1 - \alpha)\tau^2 + 2\tau^3 + \tau^4$.

On cherche $P_\Phi(X) = X^2 + c_1 X + c_{2,0}(T^2 + 1)$, $c_1 = c_{1,1}T + c_{0,1}$, avec $c_{2,0}, c_{1,1}, c_{0,1}$ dans $\mathbb{F}_3$. Pour vérifier la condition :$P_\Phi(\Phi) = 0$ on développe :

$$\begin{aligned} &\Phi^2 + (c_{1,1}\psi_T + c_{0,1})\Phi + c_{2,0}\psi_{T^2+1} = \\ &\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3 + \tau^4 \\ &2\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3, \end{aligned}$$

et on obtient un système d'équations linéaires

$$\begin{aligned} &2 + c_{1,1} = 0 \Longleftrightarrow c_{1,1} = 1 \\ &c_{1,1}\alpha + c_{0,1} + c_{2,0} + 2c_{2,0}\alpha = 0 \\ &c_{1,1} + 2c_{2,0} = 0 \Rightarrow c_{2,0} = 1, \\ &c_{0,1} + c_{2,0} = 0 \Rightarrow c_{0,1} = -1 \end{aligned}$$

Réponse :

$$P_\Phi(X) = X^2 + (c_{1,1}T + c_{0,1})X + c_{2,0}(T^2 + 1) = X^2 + (T - 1)X + (T^2 + 1)$$

En particulier,

$$\begin{aligned} &P_\Phi(1) = T^2 + T + 1 = (T + 2)^2 \bmod 3, \\ &P_\Phi(1) - P_\Phi(0) = T. \end{aligned}$$

Cours N°8. Mardi le 9 décembre 2003

Devoir surveillé du 9 décembre 2003

I) Soit $A = \mathbb{F}_3[T]$, $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau^2,$$

et on définit une série

$$e_\varphi(z) = \sum_{m=0}^{\infty} A_m z^{q^m}, \text{ avec } A_0 = 1$$

à partir de la relation de récurrence suivante :

$$\varphi_T(\sum_{m=0}^{\infty} A_m z^{q^m}) = e(Tz)$$

On pose $A_0 = 1$. Trouver les coefficients A_m de $e_\varphi(z)$.

II) Soit

$$\mathcal{O}_\infty = \Big\{ x = \sum_{i \in \mathbb{Z}, i \leq 0} a_i T^i \;\Big|\; a_i \in \mathbb{F}_q \Big\}.$$

On considère l'anneaux $\mathcal{O}_\infty[[z]]$ des séries formelles $f(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathcal{O}_\infty[[z]]$.

(a) Trouver tous les idéaux premiers de $\mathcal{O}_\infty[[z]]$, contenants

$$f = T^{-1}z + z^q + T^{-3}z^{q^2}.$$

(b) Trouver tous les idéaux maximaux de $\mathcal{O}_\infty[[z]]$.

III) Soit $A = \mathbb{F}_3[T]$, $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau + \tau^2,$$

On pose $f = T^2 + T - 1$, $k = A/(f)$, $\psi : A \to k\{\tau\}$ la réduction φ mod f.

(a) Calculer la caractéristique d'Euler-Poincaré du module k_ψ.

(b) Trouver le cardinal de l'ensemble $\operatorname{Ker} \psi_{T^3+T^2-T}(\overline{k})$.

Exemples de calculs

- Calcul de la caractéristique d'Euler-Poincaré

```
>  P := T^2+T-1;
```

$$P := T^2 + T - 1$$

```
>  PhiTerm := proc(p::posint, P::polynom(integer, T),
>  i::posint, j::posint)
>  RETURN(coeff(Rem(T^(p*(j-1))+T^(j), P, T) mod p,
>  T, i-1))
>  #coefficient de T^(i-1) du polynôme (T+tau)(T^(j-1))
>  end :
>  PhiMatrix1 := matrix(2, 2, (i,j) -> PhiTerm(3, P, i,j)) ;
>  # la matrice de T+tau sur F_3[T]/(P) dans la base T^(i-1)
```

$$PhiMatrix1 := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

```
> charpoly(%,T);
```

$$(T-1)^2$$

```
> map(item -> Expand(item) mod 3,%) ;
```

$$(T+2)^2$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%

```
> P := T^2+T-1;
```

$$P := T^2 + T - 1$$

```
> PhiTerm := proc(p::posint, P::polynom(integer, T),
> i::posint, j::posint)
> RETURN(coeff(Rem(T^(p^2*(j-1))+T^(p*(j-1))+T^(j), P, T) mod p,
> T, i-1))
> #coefficient de T^(i-1) du polynôme (T+tau+tau^2)(T^(j-1))
> end :
> PhiMatrix1 := matrix(2, 2, (i,j) -> PhiTerm(3, P, i,j)) ;
> # la matrice de T+tau +tau^2 sur F_3[T]/(P) dans la base T^(i-1)
```

$$PhiMatrix1 := \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}$$

```
> charpoly(%,T);
```

$$(T-2)^2$$

```
> map(item -> Expand(item) mod 3,%) ;
```

$$(1+T)^2$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%

- Calcul dans l'algébre de Ore

```
> restart;with(Ore_algebra):p:=3;
> n:=10;A:=skew_algebra(comm={seq(a[i],
> i=1..n),seq(a[i,1],
> i=1..n),seq(a[i,2],
> i=1..n),
> seq(a[i,3],
> i=1..n)},
> user=[tau,T,
> proc(f,n) subs(T=T^(p^n),f) end proc,
> proc(f,n) `if`(n=0,f,0) end proc],characteristic=3):
> print('tau*T'=skew_product(tau,T,A));
```

$$p := 3$$

$$n := 10$$

$$\tau\, T = T^3\, \tau$$

```
> pr:=skew_product(T+tau+tau^2,T+tau+tau^2,A);
```

$$pr := T^2 + (T + T^3)\,\tau + (T + 1 + T^9)\,\tau^2 + 2\,\tau^3 + \tau^4$$

```
> add(coeff(pr,tau,i)*z^(3^i),i=0..4);
```

$$T^2\,z + (T + T^3)\,z^3 + (T + 1 + T^9)\,z^9 + 2\,z^{27} + z^{81}$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%

```
> P := T^2+T-1;PhiTerm := proc(p::posint, P::polynom(integer, T),
> i::posint, j::posint)
> RETURN(coeff(Rem(add(coeff(skew_product(T+tau+tau^2,T^(j-1),A),tau,k),
> k=0..2), P, T) mod p,
> T, i-1))
> #coefficient de T^(i-1) du polynôme (T+tau+tau^2)(T^(j-1))
> end :
> PhiMatrix1 := matrix(2, 2, (i,j) -> PhiTerm(3, P, i,j)) ;
> # on retrouve la matrice de T+tau +tau^2 sur F_3[T]/(P) dans la base T^(i-1)
```

$$P := T^2 + T - 1$$

$$PhiMatrix1 := \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}$$

```
> with(linalg) : charpoly(PhiMatrix1,T);
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

$$(T - 2)^2$$

```
> map(item -> Expand(item) mod 3,%) ;
```

$$(T + 1)^2$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%

- Module de Drinfeld aléatoire

```
> restart ;
> with(linalg) :
```

```
Warning, the protected names norm and trace have been redefined and
unprotected
```

```
> rnd := rand(0..6) :
> rndP := proc(n)
> RETURN(sort(T^n + add(rnd()*T^i, i=0..(n-1))))
> end :
> _seed := 1730 :
> P,P1, P2 := rndP(2),rndP(3), rndP(3) ;
```

$$P,\, P1,\, P2 := T^2 + 2\,T + 4,\, T^3 + 4\,T^2 + 2\,T + 1,\, T^3 + T^2 + 2\,T + 4$$

```
> with(Ore_algebra):p:=3;
> n:=10;A:=skew_algebra(comm={seq(a[i],
> i=1..n),seq(a[i,1],
> i=1..n),seq(a[i,2],
> i=1..n),
> seq(a[i,3],
> i=1..n)},
> user=[tau,T,
> proc(f,n) subs(T=T^(p^n),f) end proc,
> proc(f,n) `if`(n=0,f,0) end proc],characteristic=3):
> print('tau*T'=skew_product(tau,T,A));
```

$$p := 3$$
$$n := 10$$
$$\tau\, T = T^3\, \tau$$

```
> rnd := rand(0..6) :
> rndP := proc(n)
> RETURN(sort(T^n + add(rnd()*T^i, i=0..(n-1))))
> end :
> _seed := 1730 :
> g = [seq(g[i]=rndP(2),i=1..4)] mod 3;
```

$$g = [g_1 = T^2 + 2\,T + 1,\; g_2 = T^2 + 2\,T + 1,\; g_3 = T^2 + T + 1,\; g_4 = T^2 + T + 2]$$

```
> g[1]:= T^2+2*T+1; g[2]:= T^2+2*T+1; g[3]:= T^2+T+1;
> g[4]:= T^2+T+2:phi(T):=T+skew_product(g[1],tau^(1),A)+
> skew_product(g[2],tau^(2),A)+skew_product(g[3],tau^(3),A)+skew_product
> (g[4],tau^(4),A):print('phi(T)'=phi(T));print('phi[T]'=add(coeff(phi(T
> ),tau,i)*z^(3^i),i=0..4));
```

$$g_1 := T^2 + 2\,T + 1$$
$$g_2 := T^2 + 2\,T + 1$$
$$g_3 := T^2 + T + 1$$
$$\phi(T) = T + (T^2 + 2\,T + 1)\,\tau + (T^2 + 2\,T + 1)\,\tau^2 + (T^2 + T + 1)\,\tau^3 + (T^2 + T + 2)\,\tau^4$$
$$\phi_T = T\,z + (T^2 + 2\,T + 1)\,z^3 + (T^2 + 2\,T + 1)\,z^9 + (T^2 + T + 1)\,z^{27} + (T^2 + T + 2)\,z^{81}$$

```
> P := T^2+T-1;PhiTerm := proc(p::posint, P::polynom(integer, T),
> #g : :vector(g[k] : :polynom(integer,T)),
> i::posint, j::posint)
> RETURN(coeff(Rem(add(coeff(skew_product(phi(T),T^(j-1),A),tau,k),k=0..
> 6), P, T) mod p,
> T, i-1))
> #coefficient de T^(i-1) du polynôme phi_T(T^(j-1))
> end :
```

$$P := T^2 + T - 1$$

```
> PhiMatrix1 := matrix(2, 2, (i,j) -> PhiTerm(3,P,i,j));
> # la matrice de phi_T sur F_3[T]/(P) dans la base T^(i-1)
```

$$PhiMatrix1 := \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}$$

```
> charpoly(PhiMatrix1,T);
```

$$T\,(T - 2)$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%

- Calcul du polynôme caractéristique :

```
> with(Ore_algebra):p:=3;
> n:=10;A:=skew_algebra(user=[tau,T,
> proc(f,n) subs(T=T^(p^n),f) end proc,
> proc(f,n) `if`(n=0,f,0) end proc],characteristic=3):
> print('tau*T'=skew_product(tau,T,A));
```

$$p := 3$$
$$n := 10$$
$$\tau\, T = T^3\, \tau$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%

phi_(T^2+1)

```
> pr1:=skew_product(T+tau+tau^2,T+tau+tau^2,A)+1;
```

$$pr1 := T^2 + (T + T^9 + 1)\,\tau^2 + 2\,\tau^3 + \tau^4 + (T + T^3)\,\tau + 1$$

psi_(T^2+1)

```
> alias(alpha = RootOf(T^2+1) mod 3) ;
```

$$\alpha$$

```
> pr1:=eval(pr1,T=alpha)mod 3;
```

$$pr1 := \alpha^2 + (\alpha + \alpha^9 + 1)\,\tau^2 + 2\,\tau^3 + \tau^4 + (\alpha + \alpha^3)\,\tau + 1$$

```
> pr1:=add((simplify(coeff(%,tau,i) mod 3)*tau^i,i=0..4)) mod 3;
> # pr1 est le polynôme psi(T^2+1)(z) ; il est de hauteur 2
```

$$pr1 := (2\,\alpha + 1)\,\tau^2 + 2\,\tau^3 + \tau^4$$

```
> add(coeff(%,tau,i)*z^(3^i),i=0..4): simplify(%) mod 3;
> # le polynôme psi_(T^2+1)(z), il est de hauteur 2
```

$$2\,z^9\,\alpha + z^9 + 2\,z^{27} + z^{81}$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%

Exemple de calcul avec les coefficients indéterminés (pour calculer le polynôme caractéristique) P_Phi(X). On substitue X=Phi =tau^2 pour obtenir P_Phi(X)=0 :

```
> tau^4+
> (c[1,1]*(alpha+tau+tau^2)+c[0,1])*tau^2+
> c[2,0]*(pr1);
```

$$\tau^4 + (c_{1,1}\,(\alpha + \tau + \tau^2) + c_{0,1})\,\tau^2 + c_{2,0}\,((2\,\alpha + 1)\,\tau^2 + 2\,\tau^3 + \tau^4)$$

On va ranger les coefficients dans l'algebre non-commutative

```
> pr2:=add(coeff(%,tau,i)*tau^i,i=0..4);
```

$$pr2 := (c_{1,1}\,\alpha + c_{0,1} + c_{2,0}\,(2\,\alpha + 1))\,\tau^2 + (c_{1,1} + 2\,c_{2,0})\,\tau^3 + (1 + c_{1,1} + c_{2,0})\,\tau^4$$

```
> coeff(coeff(pr2,tau,2),alpha,1);coeff(coeff(pr2,tau,2),alpha,0);coeff
> (pr2,tau,3); coeff(pr2,tau,4);
```

$$c_{1,1} + 2\,c_{2,0}$$
$$c_{0,1} + c_{2,0}$$
$$c_{1,1} + 2\,c_{2,0}$$
$$1 + c_{1,1} + c_{2,0}$$
$$1 + c_{1,1} + c_{2,0}$$

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%

```
> with(linalg) :x := vector(3, [c[1,0],c[1,1],c[2,0]]);
```

$$x := [c_{1,0},\, c_{1,1},\, c_{2,0}]$$

```
> A := matrix(3, 3, [0,1,2,1,0,1,0,1,1]) ;
```

- Idem pour un vecteur second membre.

$$A := \begin{bmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

```
>  b := vector(3, [0,0,-1]) ;
```

$$b := [0,\, 0,\, -1]$$

- Linsolve(...) mod 3 permet de résoudre dans GF(3^2).

```
>  x := Linsolve(A,b) mod 3 ;
```

$$x := [2,\, 1,\, 1]$$

On retrouve donc le même résultat que dans [Po], p.74 :
P_Phi(X)=X^2+(c_{1,1}T+c_{0,1})X+c_{2,0}(T^2+1)= X^2+(T-1)X+(T^2+1)
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %

Cours N°9. Mardi le 16 décembre 2003

Corrigé de devoir surveillé du 9 décembre 2003

I) Soit $A = \mathbb{F}_3[T]$, $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau^2,$$

et on définit une série

$$e_\varphi(z) = \sum_{m=0}^{\infty} A_m z^{q^m}, \text{ avec } A_0 = 1$$

à partir de la relation de récurrence suivante :

$$\varphi_T(\sum_{m=0}^{\infty} A_m z^{q^m}) = e(Tz).$$

On pose $A_0 = 1$. Trouver les coefficients A_m de $e_\varphi(z)$.

Solution (Agnés DAVID)

$$\begin{aligned}
&\varphi_T(\sum_{m=0}^{\infty} A_m z^{q^m}) = \sum_{m=0}^{\infty} A_m (Tz)^{q^m} \\
&\iff T \times \sum_{m=0}^{\infty} A_m z^{q^m}) + \left(\sum_{m=0}^{\infty} A_m z^{q^m}\right)^{q^2} = \sum_{m=0}^{\infty} A_m T^{q^m} z^{q^m} \\
&\iff \sum_{m=0}^{\infty} A_m T z^{q^m} + \sum_{m=0}^{\infty} A_m^{q^2} z^{q^{m+2}} = \sum_{m=0}^{\infty} A_m T^{q^m} z^{q^m} \\
&\iff \sum_{m=0}^{\infty} A_m T z^{q^m} + \sum_{m'=2}^{\infty} A_m^{q^2} z^{q^{m'}} = \sum_{m=0}^{\infty} A_m T^{q^m} z^{q^m} \\
&\iff \sum_{m=0}^{\infty} A_m T^{q^m} z^{q^m} = A_0 T z + A_1 T z^q + \sum_{m=2}^{\infty} (A_m T + A_{m-2}^{q^2}) z^{q^m} \\
&\iff \begin{cases} A_0 T = A_0 T \\ A_1 T = A_1 T^q \\ \forall m \geq 2, A_m T^{q^m} = (A_m T + A_{m-2}^{q^2}) \end{cases}
\end{aligned}$$

On a $A_0 = 1$, $A_1 T = A_1 T^q, (q = 3)$, donc $A_1 = 0$,

$$\forall m \geq 2, A_m = \frac{1}{(T^{q^m} - T)} A_{m-2}^{q^2}$$

En particulier,

$$\forall m \geq 2, m \text{ impair, une récurrence montre que } A_m = 0$$

Si $\forall m \geq 2, m$ pair :

$$\begin{aligned}
A_2 &= \frac{1}{(T^{q^2} - T)} A_0^{q^2} = \frac{1}{(T^{q^2} - T)} \\
A_4 &= \frac{1}{(T^{q^4} - T)} A_2^{q^2} = \frac{1}{(T^{q^4} - T)} \frac{1}{(T^{q^4} - T^{q^2})}
\end{aligned}$$

On montre par récurrence que

$$A_{2m} = \prod_{i=0}^{m-1} \frac{1}{(T^{q^{2m}} - T^{q^{2i}})}.$$

D'où le résultat : $\boxed{\begin{array}{l} A_0 = 1, \forall m \geq 1, A_{2m} = \displaystyle\prod_{i=0}^{m-1} \frac{1}{(T^{q^{2m}} - T^{q^{2i}})} \\ \forall m \geq 0, A_{2m+1} = 0 \end{array}}$

(Une autre solution utilise simplement le changement de variables τ par τ^2, et donc q par q^2, dans l'exemple 2.5.2(voir aussi exercice 2.3.) : pour le module de Carlitz $\varphi(T) = T + \tau$, on a

$$e(z) = \sum_{m=0}^{\infty} A_m z^{q^m} = \sum_{m=0}^{\infty} \frac{z^{q^m}}{P_m}$$

où $P_n := \prod_{\substack{f \text{unitaire} \\ \deg f = n}} f(T) = \prod_{m=1}^{n} (T^{q^m} - T)^{q^{n-m}})$.

II) Soit

$$\mathcal{O}_\infty = \Big\{ x = \sum_{i \in \mathbb{Z}, i \leq 0} a_i T^i \;\Big|\; a_i \in \mathbb{F}_q \Big\}.$$

On considère l'anneaux $\mathcal{O}_\infty[[z]]$ des séries formelles $f(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathcal{O}_\infty[[z]]$.

(a) Trouver tous les idéaux premiers de $\mathcal{O}_\infty[[z]]$, contenants

$$f = T^{-1} z + z^q + T^{-3} z^{q^2}.$$

(b) Trouver tous les idéaux maximaux de $\mathcal{O}_\infty[[z]]$.

Solution : On pose $\mathcal{O} = \mathcal{O}_\infty$, $\pi = T^{-1}$, $R = \mathcal{O}_\infty[[z]]$. On note par $P(z) = z^n + a_{n-1} z^{n-1} + \cdots + a_0 \in \mathcal{O}[z]$ un polynôme tel que $\pi | a_i$ pour tous les $i = 0, \cdots, n-1$, dit distingué. Selon le théorème de préparation de Weierstrass, pour tout $g \in R$ il existe P et $U \in R^*$ tels que $g = \pi^\mu \cdot P \cdot U$, et donc R est un anneau factoriel avec les éléments premiers π, P (distingué irréductibles).

Montrons que tous les idéaux premiers de R sont (0), (P), (π) et $\mathfrak{m} = (\pi, z)$. Soit $I \subset R$ un idéal premier non nul, et $f = \pi^s H$ un polynôme de degré minimal dans I. Ceci implique, que soit $\pi^s \in I \Rightarrow \pi \in I$, soit $H \in I$.

Si $\pi \in I$ et $I \neq (\pi)$, alors il existe un $P \in I$ (distingué irréductible). Il vient que

$$P^i \equiv P^j \bmod I \Rightarrow z^{ni} \equiv z^{nj} \bmod I \text{ avec } i > j \Rightarrow z^{nj}(z^{n(i-j)} - 1) \in I,$$

d'où $z \in I$ puisque $z^{n(i-j)} - 1 \in R^*$. Donc, $I = (\pi, z)$, Dans le cas où $\pi \notin I$ il existe un $P \in I$ (distingué irréductible). Si $I \neq (P)$, alors il existe un autre $Q \in I$ (distingué irréductible), donc P, Q sont premiers entre eux dans $\mathcal{K}[z]$, où $\mathcal{K} = \mathrm{Frac}(\mathcal{O})$. Par l'identité de Bezout,

$$Pu + Qv = 1 \text{ dans } u, v \in \mathcal{K}[z] \Rightarrow P\tilde{u} + Q\tilde{v} = \pi^s \in I \text{ dans } u, v \in \mathcal{O}[z],$$

d'où $\pi \in I$ $(I \neq R)$, contradiction, d'où $I = (P)$.

Pour trouver tous les idéaux premiers I contenant

$$f = T^{-1} z + z^q + T^{-3} z^{q^2} = z(T^{-1} + z^{q-1} + T^{-3} z^{q^2-1}),$$

il reste à considérer les polynômes z et $T^{-1}+z^{q-1}+T^{-3}z^{q^2-1}$ et remarquer qu'il existe un seul polynôme P distingué irréductible de degré $q-1$ tel que

$$T^{-1}+z^{q-1}+T^{-3}z^{q^2-1}=P\cdot U, U\in R^*$$

(comparer les deux parties $\mathrm{mod}\,\pi^2$, et utiliser le critère d'Eisenstein dans $\mathcal{O}[z]$).

Réponse : (a) $I=(z)$, $(T^{-1}+z^{q-1}+T^{-3}z^{q^2-1})$, et $\mathfrak{m}=(T^{-1},z)$, (b) $\mathfrak{m}=(T^{-1},z)$.

Attention : Le polynôme $T^{-1}+z^{q-1}+T^{-3}z^{q^2-1}$ n'est pas un polynôme de plus petit degré dans son idéal premier principal $(T^{-1}+z^{q-1}+T^{-3}z^{q^2-1})$, puisque il n'est pas distingué.

III) Soit $A=\mathbb{F}_3[T]$, $\varphi: A\to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T)=T+\tau+\tau^2,$$

On pose $f=T^2+T-1$, $k=A/(f)$, $\psi: A\to k\{\tau\}$ la réduction φ mod f.

(a) Calculer la caractéristique d'Euler-Poincaré du module k_ψ.

(b) Trouver le cardinal de l'ensemble $\mathrm{Ker}\,\psi_{T^3+T^2-T}(\overline{k})$.

Solution (Michel SCOTTO) (a) Une base de $k=(1,T)$ mod f (sur $\mathbb{F}_q$).

$$\psi_T(z)=Tz+z^q+z^{q^2}\ \mathrm{mod}\ f\Rightarrow$$
$$\psi_T(1)=T+2=T-1\ \mathrm{mod}\ f, \psi_T(T)=T^2+T^q+T^{q^2}\ \mathrm{mod}\ f,$$
$$T^2=1-T\ \mathrm{mod}\ f,$$
$$T^q=T^3=T(1-T)\ \mathrm{mod}\ f=T-T^2=T-(1-T)=2T-1=-(T+1)\ \mathrm{mod}\ f,$$
$$T^{q^2}=(T^3)^3=-(T+1)^3=-(T+1)(T-1)=-(T^2-1)=-(T^2-1)=T\ \mathrm{mod}\ f,$$
$$\psi_T(T)=T^2+T^q+T^{q^2}=1-T-(T+1)+T=-T\ \mathrm{mod}\ f$$

Dans la base $(1,T)$ mod f, la matrice de ψ_T est $\begin{pmatrix}-1 & 0\\ 1 & -1\end{pmatrix}$, d'où $\chi_{\psi_T}(X)=(X+1)^2$. Conclusion : $\boxed{f_\psi=(T+1)^2}$

(b) On a $T^3+T^2-T=T\cdot f\in\mathbb{F}_3[T]$, donc $\psi_{T^3+T^2-T}$ n'est pas séparable, et on va calculer sa hauteur :

$$\psi_{T^2+T-1}=\psi_{T^2}+\psi_T-\psi_1=(T+\tau+\tau^2)^2+T+\tau+\tau^2-1,$$

le coefficient de τ^2 :

$$\tau^2T+T\tau^2+2\tau^2=(T^9+T+2)\tau^2,$$

et $T^9=T$ mod f vu a). On a donc

$$\mathrm{ht}(\psi_{T^3+T^2-T})=2\Rightarrow\psi_{T^3+T^2-T}=\tau^2u_s,$$

où $u_s\in\overline{k}\{\tau\}$ est séparable, et

$$\mathrm{Ker}\,\psi_{T^3+T^2-T}(\overline{k})=\mathrm{Ker}\,u_s(\overline{k})\ \mathrm{car}\ \forall z\in\overline{k}, \psi_{T^3+T^2-T}(z)=u_s(z)^{q^2}$$

Mais

$$\deg_\tau u_s=\deg_\tau(\psi_{T^3+T^2-T})-2=6-2=4$$

car ψ est un module de Drinfeld de rang 2, donc

$$\deg_z u_s=3^4=81=\mathrm{Card}\,\mathrm{Ker}\,u_s(\overline{k})$$

car u_s est séparable. Conclusion : $\boxed{\mathrm{Card}\,\mathrm{Ker}\,\psi_{T^3+T^2-T}(\overline{k})=81}$.

Applications de l'élément de Frobenuis

Rappels sur la caractéristique d'Euler-Poincaré

Soit $A = \mathbb{F}_q[T]$, et M un A-module fini. On définie la caractéristique d'Euler-Poincaré $\chi_A(M)$ comme un idéal $\chi_A(M) \subset A$ de telle façon que $\chi_A(A/\mathfrak{q}) = \mathfrak{q}$ pour tout idéal maximal, et $\chi_A(M) = \chi_A(M_1)\chi_A(M_2)$ pour toute suite exacte

$$0 \to M_1 \to M \to M_2 \to 0 \Rightarrow \chi_A(M) = \chi_A(M_1)\chi_A(M_2)$$

En particuler, $\chi_A(A/\mathfrak{q}^n) = \mathfrak{q}^n$, $\chi_A(A/(a) = (a)$ pour tout $a \in A\backslash\{0\}$. Remarquer que $\operatorname{Card} M = \operatorname{Card} A/\chi_A(M)$, quoique les modules M et $A/\chi_A(M)$ ne sont pas isomorphes en général.

Pour tout endomorphisme $u : M \to M$ de modules finis, on a

$$0 \to \operatorname{Ker} u \to M \to M \to \operatorname{Coker} u = M/\operatorname{Im} u \to 0,$$

ceci implique $\chi_A(\operatorname{Ker} u) = \chi_A(M/\operatorname{Im} u)$, puisque $\chi_A(\operatorname{Ker} u)\chi_A(\operatorname{Im} u) = \chi_A(M)$, et $\chi_A(\operatorname{Im} u)\chi_A(M/\operatorname{Im} u) = \chi_A(M)$.

Soit $\psi : A \to k\{\tau\}$ un module de Drinfeld, où $\mathfrak{p} \subset A$ est un idéal maximal de A, la A-caractéristique $\mathfrak{p} = \operatorname{Car}_A(k) = (f)$ (générateur unitaire irréductible) d'un corps fini $k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. On utilise les extensions finies

$$k \supset \mathbb{F}_\mathfrak{p} = A/\mathfrak{p} \supset \mathbb{F}_q, \quad [k : \mathbb{F}_\mathfrak{p}] = m, \ [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d = \deg f \Rightarrow |k| = q^n, n = m \cdot d,$$

et on pose $\Phi = \tau^n$. On utilise la notation $M = k_\psi$ pour le A-module donné par l'action de ψ sur k, et on note f_φ (ou f_ψ) le générateur unitaire de l'idéal $\chi_A(k_\psi)$, si $\psi = \varphi \bmod \mathfrak{p}$, et $\mathfrak{p} = (f)$.

Calcul de la caractéristique d'Euler-Poincaré

On utilise une décomposition

$$k_\psi \cong A/(f_1^{k_1}) \oplus \cdots \oplus A/(f_t^{k_t})$$

où tous les f_i sont unitaires irréductibles. Alors $\chi_A(k_\psi) = (\prod_{i=1}^{t} f_i^{k_i})$ est la caractéristique d'Euler-Poincaré de $k_\psi = (A/(f))_\psi$, et on la calcule comme le polynôme caractéristique sur $\mathbb{F}_q$ de l'endomorphisme ψ_T sur $k = A/(f)$, puisque chaque sous-A-module cyclique $A/(f_i^{k_i})$ est stable par $x \mapsto T * x$ (de polynôme caractéristique $f_i^{k_i}$).

Rappels : un analogue du théorème de Hasse, [Po] (voir section 3.4)

THÉORÈME 3.4.1 *Soit $\psi : A \to k\{\tau\}$ un module de Drinfeld de rang r (à coefficients dans le corps fini $k = A/(f)$). Alors*

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

Application à la démonstration du théorème 3.4.1 :

On utilise l'élément de Frobenius

$$\Phi = \Phi_f = \tau^n \in \operatorname{End}(\psi) \supset \psi(A),$$

comme un élément central du corps gauche $k(\tau) \subset k((\tau^{-1}))$. Alors

$$k = \mathrm{Ker}\,(\Phi - \mathrm{Id})(\overline{k}),\ \text{donc}\ k_\psi = \bigoplus_{\mathfrak{q}} \mathrm{Ker}\,(\Phi - \mathrm{Id})(_{\mathfrak{q}^\infty}\psi(\overline{k})).$$

Pour déterminer toute composante avec $\mathfrak{q} \neq \mathfrak{p}$, on utilise la représentation d'anneau d'endomorphismes sur le module de Tate $\mathfrak{q}$-adique :

$$\iota_\mathfrak{q} : \mathrm{End}(\psi) \to \mathrm{End}_{A_\mathfrak{q}}(T(\psi)_\mathfrak{q}) \cong \mathrm{M}_r(A_\mathfrak{q}),\ (\mathfrak{q} \neq \mathfrak{p}), \boxed{T(\psi)_\mathfrak{q} = \varprojlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong A_\mathfrak{q}^r}.$$

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

$$P_\Phi(X) = \det(X \cdot \mathrm{Id}_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi)) \in A_\mathfrak{q}[X] \Rightarrow \deg P_\Phi = r, M_\Phi(X) \in A[X].$$

Pour décrire ses propriétés, on utilise le corps

$$\begin{aligned}
&\mathcal{K} = \mathrm{Frac}(\psi(A)) = \mathbb{F}_q(\psi_T) \subset k(\tau),\\
&\mathcal{L} = \mathcal{K}(\Phi)(\Phi \text{ commute avec tous les } \psi_a, a \in A\\
&\mathcal{A} = \mathrm{End}(\psi) \otimes_A \mathcal{K} \subset k(\tau) \text{ c'est un sous-corps gauche de } k(\tau),\\
&\text{on a vu que } Centre(k(\tau)) = \mathbb{F}_q(\Phi), Centre(\mathcal{A}) = \mathcal{L}, [k(\tau) : \mathbb{F}_q(\Phi)] = n^2.
\end{aligned}$$

On pose $[\mathcal{L} : \mathcal{K}] = r_1$. Nous avons vu aussi que $r = r_1 r_2$, où

$$\begin{aligned}
&[\mathcal{A} : \mathcal{L}] = r_2^2\\
&\text{et } P_\Phi(X) = M_\Phi(X)^{r_2} \in A[X] \Rightarrow P_\Phi(\Phi) = 0
\end{aligned}$$

(voir [Ge], Théorème 5.1).

THÉORÈME 4.6.7 (E.-U. GEKELER) *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 caractèristique d'Euler-Poincaré $\chi(k_\psi)$ du A-module fini k_ψ.

(ii) $(P_\Phi(0)) = \mathfrak{p}^m$.

(iii) Pour tous les zéros σ_i de $(P_\Phi(X))$ on a $|\sigma_i|_\infty = q^{n/r}$.

PREUVE. Selon la proposition 4.1.1, pour tout corps commutatif emboité E

$$\mathbb{F}_q(\Phi) \subset E \subset k(\tau).$$

il existe une seule place de E au dessus des places $\Phi = \infty$ et $\Phi = 0$ de $\mathbb{F}_q(\Phi)$. Ces places sont données par les normes topologiques :

$$|u|_\infty = q^{\deg_\tau u},\ \ |u|_0 = q^{-(\mathrm{ht}_\tau u)} \Rightarrow |\Phi|_\infty = q^n,\ |\Phi|_0 = q^{-n}, |\psi_T|_\infty = q^r,\ |\psi_f|_0 = q^{-\mathrm{ht}\psi_f}.$$

On considère l'application de la norme algébrique d'isogénie, définie comme la norme algébrique habituelle dans toute extension maximale commutative de $\mathcal{K}$ dans $\mathcal{A}$:

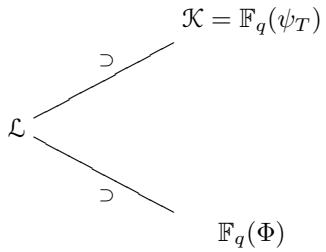
$$N : \mathrm{End}(\psi) \otimes_A \mathcal{K} \to \mathcal{K}.$$

Pour $u \in \mathrm{End}(\psi)$ on a (lemme 4.6.1) :

$$\begin{aligned}
&\deg_\tau N(u) = r \cdot \deg_\tau u \Rightarrow \deg_\tau N(\Phi) = r \cdot \deg_\tau(\tau^n) = rn,\\
&\text{et } N(u) = \det \circ \iota_\mathfrak{q}(u) \Rightarrow P_\Phi(t) = \det(t \cdot \mathrm{Id}_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi)) = N_\mathcal{K}^\mathcal{L}(t-u)^{r_2},\ \text{si } t \in \mathcal{L}.
\end{aligned}$$

(ii) Nous avons vu que $(P_\Phi(0)) = (N(\Phi))$ appartienne à un seul idéal maximal $\mathfrak{p} = (f)$ dans $A = \psi(A) \subset k\{\tau\}$, puisqu'il existe une seule place $\mathfrak{P}$ de $\mathcal{L} = \mathcal{K}(\Phi)$ divisant Φ, et elle se trouve au-dessus de $\mathfrak{p}$, voir Proposition 4.1.1 (rappelons que cette place est donnée par la hauteur, qui est positive seulement au-dessus de $\mathfrak{p} = (f)$.

$\mathcal{L} \ni \Phi$ divise $N(\Phi) \in \mathcal{K}$ dans $\mathcal{L} \cap k\{\tau\}$



L'exposant m dans $(P_\Phi(0)) = \mathfrak{p}^m$ vient de la formule du produit dans $\mathcal{K}$, et du fait que $\deg N(\Phi) = n$ (en tant que $N(\Phi) \in A$), donc $(N(\Phi)) = \mathfrak{p}^m$. En effet, $\deg_\tau(\psi(N(\Phi))) = rn$, puisqu'il existe une seule place $\widetilde{\infty}$ de $\mathcal{L} = \mathcal{K}(\Phi)$ au-dessus de ∞, voir Proposition 4.1.1.

De plus, $\mathfrak{p} = (f)$, et $\deg_\tau(\psi_{f^m}) = rdm = rn$. Ceci implique (ii).

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

(i) Enfin, on calcule la $\mathfrak{q}$-composante de l'idéal principal $(P_\Phi(1))$.

On considère le A-module fini

$$M = \mathrm{Ker}\,(\Phi - 1)(\overline{k}) = k_\psi,$$

et on pose

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

On utilise la notation $(P_\Phi(1))_\mathfrak{q} = (P_\Phi(1))A_\mathfrak{q}$. Alors

$$M_\mathfrak{q} \cong T_\mathfrak{q}(\psi)/\mathrm{Im}\,(\iota_\mathfrak{q}(\Phi - 1)) \cong \mathrm{Ker}\,(\Phi - 1)({}_{\mathfrak{q}^\infty}\psi(\overline{k})),$$

donc

$$(P_\Phi(1))_\mathfrak{q} = (\det \circ \iota_\mathfrak{q}(\Phi - 1)).$$

Lemme 4.6.8 *Soit $u \in \mathrm{End}(A_\mathfrak{q}^r)$ tel que $M = A_\mathfrak{q}^r/u(A_\mathfrak{q}^r)$ est fini. Alors*

$$(\det u)A_\mathfrak{q} = (\chi(M))A_\mathfrak{q} = (\chi(M))_\mathfrak{q}$$

Preuve. Dans des bases convenables de $A_\mathfrak{q}^r$ et de $u(A_\mathfrak{q}^r)$, l'endomorphisme u est représentée par une matrice diagonale

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix},$$

donc

$$M \cong A_\mathfrak{q}/(d_1) \oplus \cdots \oplus A_\mathfrak{q}/(d_r) \Rightarrow \chi_A(M)_\mathfrak{q} = \chi_A(A_\mathfrak{q}/(d_1))_\mathfrak{q} \cdot \ldots \cdot \chi_A(A_\mathfrak{q}/(d_r))_\mathfrak{q} = (d_1 \cdot \ldots \cdot d_r)_\mathfrak{q}.$$

Remarque. Sous l'hypothèse du lemme on a, pour un i assez grand,

$$M = A_{\mathfrak{q}}^r/u(A_{\mathfrak{q}}^r) \cong (A/\mathfrak{q}^i)^r/u((A/\mathfrak{q}^i))$$

(on peut prendre tout i tel que $(d_1 \cdot \ldots \cdot d_r) \supset \mathfrak{q}^i$).

On applique ce résultat à $u = \Phi - \mathrm{Id}$, et on obtient

$$(P_\Phi(1))_{\mathfrak{q}} = (\det \circ \iota_{\mathfrak{q}}(\Phi - 1)) = \chi((T_{\mathfrak{q}}(\psi)/\mathrm{Im}\,(\iota_{\mathfrak{q}}(\Phi - 1)) = \chi(\mathrm{Ker}\,(\Phi - 1)({}_{\mathfrak{q}^i}\psi(\overline{k}))) = \chi({}_{\mathfrak{q}^i}\psi(k)) = \chi(M_{\mathfrak{q}}).$$

Ceci montre que (i) est vérifiée pour tous les $\mathfrak{q} \neq \mathfrak{p}$.

De plus, $\deg_\tau N(\Phi - 1) = \deg_\tau N(\Phi) = rn$, 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 de produit, leur valuations $\mathfrak{p}$-adiques coïncident, d'où (i) : l'idéal principal $(P_\Phi(1))$ de A coïncide avec la caractèristique d'Euler-Poincaré $\chi(k_\psi)$ du A-module fini k_ψ. En effet,

$$\psi(A) \ni P_\Phi(1) = N(\Phi - 1) \Rightarrow \mathrm{Card}\,(\mathrm{Ker}\,(\Phi - 1)(\overline{k})) = q^n = \mathrm{Card}\,(A/\chi(k_\psi)).$$

Application à la démonstration du théorème 3.4.1 : valeurs absolues des racines du polynôme caractéristique

Enfin, on utilise de nouveau le fait qu'il n'y a qu'une *seule place* $\widetilde{\infty}$ de $\mathcal{L} = \mathcal{K}(\Phi)$ au-dessus de ∞. Ceci implique que toutes les racines w_i du polynôme minimal de Φ sur $\mathcal{K}$ ont la même valeur absolue $|w_i|_{\widetilde{\infty}}$ en $\widetilde{\infty}$, donc

$$\begin{aligned}
&P_\Phi(X) = \prod_{j=1}^r (X - w_{i_j}), \quad P_\Phi(1) = \prod_{j=1}^r (1 - w_{i_j}), \quad P_\Phi(0) = (-1)^r \prod_{j=1}^r w_{i_j} \Rightarrow \\
&P_\Phi(1) - P_\Phi(0) = 1 - (w_{i_1} + \cdots w_{i_r}) + \cdots + (-1)^{r-1}\sigma_{r-1}(w_{i_1}, \cdots, w_{i_r}) \\
&= \sum_{s=0}^{r-1} (-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}).
\end{aligned}$$

où $\sigma_s(w_{i_1}, \cdots, w_{i_r})$ est le polynôme élémentaire symétrique de degré $s \leq r - 1$.

Conclusion :

$$\begin{aligned}
&P_\Phi(1) - P_\Phi(0) = \sum_{s=0}^{r-1} (-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}) \\
&|w_i|_{\widetilde{\infty}} = |f|_\infty^{1/r} \quad \Rightarrow (f^m - f_\psi) = (P_\Phi(0) - P_\Phi(1)) \Rightarrow |f^m - f_\psi|_\infty \leq |f|_\infty^{m(r-1)/r}.
\end{aligned}$$

Corollaire 4.6.9 *Si $r = 1$ et $m = 1$, alors $f_\psi = f + c$, $c \in \mathbb{F}_q^\times$ (une constante non-nulle).*

En effet, dans ce cas $r - 1 = 0$, $|f - f_\psi|_\infty \leq 1$ donc $f_\psi = f + c$ puisque

$$f - f_\psi \in A, \quad \deg(f - f_\varphi) = 0.$$

Dans les calculs pratiques du polynôme $P_{\Phi_f}(X)$ (voir [Po], p.74), on utilise la borne

Corollaire 4.6.10 *Si $m = 1$, alors les coefficients $c_i \in A$ du polynôme caractéristique $P_\Phi(X) = \sum_{i=0}^r c_i X^{n-i}$ vérifient l'inégalité suivante :*

$$\deg(c_i) \leq \left[\frac{i \deg f}{r}\right] \quad (i = 0, \cdots, r). \tag{4.7}$$

Exemple de calcul du polynôme caractéristique, voir [Po], p.74

Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau + \tau^2,$$

On pose $q = 3$, $f = T^2 + 1$, $k = A/(f)$, $\psi : A \to k\{\tau\}$ la réduction φ mod g.

Calculer le polynôme caractéristique de l'élément $\Phi_\varphi = \tau^2$ sur le sous-corps $\mathrm{Frac}(\psi(A))$ dans $k\{\tau\}$.

Solution : On pose $k = \mathbb{F}_3[\alpha]$, où $\alpha^2 + 1 = 0$. On a

$$\varphi_{T^2+1} = 1 + T^2 + (T^3 + T)\tau + (T + T^9 + 1)\tau^2 + 2\tau^3 + \tau^4,$$

d'où $\psi_{T^2+1} = (1 - \alpha)\tau^2 + 2\tau^3 + \tau^4$.

On cherche $P_\Phi(X) = X^2 + c_1 X + c_{2,0}(T^2 + 1)$, $c_1 = c_{1,1}T + c_{0,1}$, avec $c_{2,0}, c_{1,1}, c_{0,1}$ dans $\mathbb{F}_3$. Pour vérifier la condition :$P_\Phi(\Phi) = 0$ on développe :

$$\begin{aligned}
&\Phi^2 + (c_{1,1}\psi_T + c_{0,1})\Phi + c_{2,0}\psi_{T^2+1} = \\
&\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3 + \tau^4 \\
&2\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3,
\end{aligned}$$

et on obtient un système d'équations linéaires

$$\begin{aligned}
&2 + c_{1,1} = 0 \Longleftrightarrow c_{1,1} = 1 \\
&c_{1,1}\alpha + c_{0,1} + c_{2,0} + 2c_{2,0}\alpha = 0 \\
&c_{1,1} + 2c_{2,0} = 0 \Rightarrow c_{2,0} = 1, \\
&c_{0,1} + c_{2,0} = 0 \Rightarrow c_{0,1} = -1
\end{aligned}$$

Réponse :

$$P_\Phi(X) = X^2 + (c_{1,1}T + c_{0,1})X + c_{2,0}(T^2 + 1) = X^2 + (T - 1)X + (T^2 + 1)$$

En particulier,

$$\begin{aligned}
&P_\Phi(1) = T^2 + T + 1 = (T + 2)^2 \bmod 3, \\
&P_\Phi(1) - P_\Phi(0) = T.
\end{aligned}$$

Cours N°10. Mardi le 6 janvier 2004

Utilisation des A-modules finis en cryptologie

Rappels : un analogue du théorème de Hasse, [Po] (voir section 3.4)

Soit $A = \mathbb{F}_q[T]$, et $\psi : A \to k\{\tau\}$ un module de Drinfeld sur un corps fini k de la A-caractéristique $\mathfrak{p} = \mathrm{Car}_A(k) = (f)$ (générateur unitaire irréductible). On utilise les notations

$$[k : \mathbb{F}_\mathfrak{p}] = m,\ [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q] = d = \deg f \Rightarrow |k| = q^n, n = m \cdot d,$$

et on pose $\Phi = \tau^n$. On utilise aussi la notation $M = k_\psi$ pour le A-module fini donné par l'action de ψ sur k, et on note f_φ (ou f_ψ) le générateur unitaire de l'idéal $\chi_A(k_\psi)$, sa caractéristique d'Euler-Poincaré.

- On va expliquer comment on utilise le A-module fini $M = k_\psi$ dans les problèmes d'échange d'information protégés.

- Rapellons que la caractéristique d'Euler-Poincaré $\chi_A(M)$ d'un A-module fini est un idéal $\chi_A(M) \subset A$ tel que $\chi_A(A/\mathfrak{q}) = \mathfrak{q}$ pour tout idéal maximal, et
  $\chi_A(M) = \chi_A(M_1)\chi_A(M_2)$ pour toute suite exacte

  $$0 \to M_1 \to M \to M_2 \to 0 \Rightarrow \chi_A(M) = \chi_A(M_1)\chi_A(M_2)$$

  En particulier, $\chi_A(A/\mathfrak{q}^n) = \mathfrak{q}^n$, $\chi_A(A/(a)) = (a)$ pour tout $a \in A\backslash\{0\}$. Remarquer que $\mathrm{Card}\, M = \mathrm{Card}\, A/\chi_A(M)$, quoique les modules M et $A/\chi_A(M)$ ne sont pas isomorphes en général.
  Pour tout endomorphisme $u : M \to M$ de modules finis, on a

  $$0 \to \mathrm{Ker}\, u \to M \to M \to \mathrm{Coker}\, u = M/\mathrm{Im}\, u \to 0,$$

  ceci implique $\chi_A(\mathrm{Ker}\, u) = \chi_A(M/\mathrm{Im}\, u)$, puisque $\chi_A(\mathrm{Ker}\, u)\chi_A(\mathrm{Im}\, u) = \chi_A(M)$, et
  $\chi_A(\mathrm{Im}\, u)\chi_A(M/\mathrm{Im}\, u) = \chi_A(M)$.

THÉORÈME 3.4.1(une version précisée) *Soit $\psi : A \to k\{\tau\}$ un module de Drinfeld de rang r à coefficients dans le corps fini k, $[k : A/(f)] = m$. Alors*

$$\deg(f^m - f_\psi) \leq \frac{(r-1)}{r} m \deg f.$$

Rappels et fin de la démonstration du théorème 3.4.1 :

On utilise l'élément de Frobenius $\Phi = \Phi_f = \tau^n \in \mathrm{End}(\psi) \supset \psi(A), \mathrm{End}(\psi) \subset k\{\tau\}$ Alors

$$k = \mathrm{Ker}\,(\Phi - \mathrm{Id})(\overline{k}),\ \text{donc}\ k_\psi = \bigoplus_{\mathfrak{q}} \mathrm{Ker}\,(\Phi - \mathrm{Id})({}_{\mathfrak{q}^\infty}\psi(\overline{k})).$$

Pour déterminer toute composante avec $\mathfrak{q} \neq \mathfrak{p}$, on utilise la représentation d'anneau d'endomorphismes sur le module de Tate $\mathfrak{q}$-adique :

$$\iota_\mathfrak{q} : \mathrm{End}(\psi) \to \mathrm{End}_{A_\mathfrak{q}}(T(\psi)_\mathfrak{q}) \cong \mathrm{M}_r(A_\mathfrak{q}),\ (\mathfrak{q} \neq \mathfrak{p}), \boxed{T(\psi)_\mathfrak{q} = \varprojlim_n {}_{\mathfrak{q}^n}\psi(\overline{k}) \cong A_\mathfrak{q}^r}.$$

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

$$P_\Phi(X) = \det(X \cdot \mathrm{Id}_{T_\mathfrak{q}} - \iota_\mathfrak{q}(\Phi)) = M_\Phi^{r_2}(X) \in A[X], \deg M_\Phi = r_1, r_1 \cdot r_2 = r.$$

THÉORÈME (E.-U. GEKELER) 4.6.7 *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 caractèristique d'Euler-Poincaré $\chi(k_\psi)$ du A-module fini k_ψ.

(ii) $(P_\Phi(0)) = \mathfrak{p}^m$.

(iii) Pour tous les zéros ρ_i de $(P_\Phi(X))$ on a $|\rho_i|_\infty = q^{n/r}$.

Application à la démonstration du théorème 3.4.1 : valeurs absolues des racines du polynôme caractéristique

Enfin, on utilise de nouveau le fait qu'il n'y a qu'une *seule place* $\widetilde{\infty}$ de $\mathfrak{L} = \mathcal{K}(\Phi)$ au-dessus de ∞. Ceci implique que toutes les racines w_i du polynôme minimal de Φ sur $\mathcal{K}$ ont la même valeur absolue $|w_i|_{\widetilde{\infty}}$ en $\widetilde{\infty}$, donc

$$P_\Phi(X) = \prod_{j=1}^{r}(X - w_{i_j}), \quad P_\Phi(1) = \prod_{j=1}^{r}(1 - w_{i_j}), \quad P_\Phi(0) = (-1)^r \prod_{j=1}^{r} w_{i_j} \Rightarrow$$
$$P_\Phi(1) - P_\Phi(0) = 1 - (w_{i_1} + \cdots w_{i_r}) + \cdots + (-1)^{r-1}\sigma_{r-1}(w_{i_1}, \cdots, w_{i_r})$$
$$= \sum_{s=0}^{r-1}(-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r}).$$

où $\sigma_s(w_{i_1}, \cdots, w_{i_r})$ est le polynôme élémentaire symétrique de degré $s \leq r-1$.

CONCLUSION :

$$P_\Phi(1) - P_\Phi(0) = \sum_{s=0}^{r-1}(-1)^s \sigma_s(w_{i_1}, \cdots, w_{i_r})$$
$$|w_i|_{\widetilde{\infty}} = |f|_\infty^{m/r} \quad \Rightarrow (f^m - f_\psi) = (P_\Phi(0) - P_\Phi(1)) \Rightarrow |f^m - f_\psi|_\infty \leq |f|_\infty^{m(r-1)/r}.$$

COROLLAIRE 4.6.11 *Si $r = 1$ et $m = 1$, alors $f_\psi = f + c$, $c \in \mathbb{F}_q^\times$ (une constante non-nulle).*

En effet, dans ce cas $r - 1 = 0$, $|f - f_\psi|_\infty \leq 1$ donc $f_\psi = f + c$ puisque

$$f - f_\psi \in A, \quad \deg(f - f_\varphi) = 0.$$

Dans les calculs pratiques du polynôme $P_{\Phi_f}(X)$ (voir [Po], p.74), on utilise la borne

COROLLAIRE 4.6.12 *Si $m = 1$, alors les coefficients $c_i \in A$ du polynôme caractéristique $P_\Phi(X) = \sum_{i=0}^{r} c_i X^{n-i}$ vérifient l'inégalité suivante :*

$$\deg(c_i) \leq \left[\frac{i \deg f}{r}\right] \quad (i = 0, \cdots, r). \tag{4.1}$$

Exemple de calcul du polynôme caractéristique, voir [Po], p.74

Soit $\varphi : A \to A\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = T + \tau + \tau^2,$$

On pose $q = 3$, $f = T^2 + 1$, $k = A/(f)$, $\psi : A \to k\{\tau\}$ la réduction φ mod g.

Calculer le polynôme caractéristique de l'élément $\Phi_\varphi = \tau^2$ sur le sous-corps $\mathrm{Frac}(\psi(A))$ dans $k\{\tau\}$.

Solution : On pose $k = \mathbb{F}_3[\alpha]$, où $\alpha^2 + 1 = 0$. On a

$$\varphi_{T^2+1} = 1 + T^2 + (T^3 + T)\tau + (T + T^9 + 1)\tau^2 + 2\tau^3 + \tau^4,$$

d'où $\psi_{T^2+1} = (1 - \alpha)\tau^2 + 2\tau^3 + \tau^4$.

On cherche $P_\Phi(X) = X^2 + c_1 X + c_{2,0}(T^2 + 1)$, $c_1 = c_{1,1}T + c_{0,1}$, avec $c_{2,0}, c_{1,1}, c_{0,1}$ dans $\mathbb{F}_3$. Pour vérifier la condition :$P_\Phi(\Phi) = 0$ on développe :

$$\begin{aligned}
&\Phi^2 + (c_{1,1}\psi_T + c_{0,1})\Phi + c_{2,0}\psi_{T^2+1} = \\
&\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3 + \tau^4 \\
&2\tau^4 + (c_{1,1}(\alpha + \tau + \tau^2) + c_{0,1})\tau^2 + c_{2,0}(1 - \alpha)\tau^2 + 2\tau^3,
\end{aligned}$$

et on obtient un système d'équations linéaires

$$\begin{aligned}
&2 + c_{1,1} = 0 \Longleftrightarrow c_{1,1} = 1 \\
&c_{1,1}\alpha + c_{0,1} + c_{2,0} + 2c_{2,0}\alpha = 0 \\
&c_{1,1} + 2c_{2,0} = 0 \Rightarrow c_{2,0} = 1, \\
&c_{0,1} + c_{2,0} = 0 \Rightarrow c_{0,1} = -1
\end{aligned}$$

Réponse :

$$P_\Phi(X) = X^2 + (c_{1,1}T + c_{0,1})X + c_{2,0}(T^2 + 1) = X^2 + (T - 1)X + (T^2 + 1)$$

En particulier,

$$\begin{aligned}
&P_\Phi(1) = T^2 + T + 1 = (T + 2)^2 \bmod 3, \\
&P_\Phi(1) - P_\Phi(0) = T.
\end{aligned}$$

5 Application à la cryptographie

La cryptographie théorique est une science qui étudie les systèmes d'échange d'information protégé.

On considère un système d'utilisateurs $U_1, U_2, U_3 \ldots$. De temps en temps chaque couple d'utilisateurs aurait pu besoin d'échanger de messages que doivent rester secret pour les autres utilisateurs ou pour toute autre person non autorisée.

Dans les systèmes classiques de cryptographie, ils doivent échanger d'abord les clés et après les garder secret. La cryptographie à clef publique évite la dernière restriction : les communications secretes deux-à-deux devienent possible en utilisant seulement une information ouverte pour tout le monde. Un tel système peut être réalisé de façon suivante : Pour l'ensemble $\{U_i\}$ d'utilisateurs et un ensemble fini $\mathcal{M}$ des "messages" , et on associe à tout U_j deux applications

$$\mathcal{E}_j : \mathcal{M} \to \mathcal{M}, \text{ et } \mathcal{D}_j : \mathcal{M} \to \mathcal{M},$$

de telle façon que $\mathcal{D}_j$ est secret, $\mathcal{E}_j$ est publique (ouverte), et

$$\mathcal{E}_j \circ \mathcal{D}_j = id = \mathcal{D}_j \circ \mathcal{E}_j : \mathcal{M} \to \mathcal{M}.$$

(donc le savoir de $\mathcal{E}_j$ ne donne pas $\mathcal{D}_j = \mathcal{E}_j^{-1}$.

Cryptographie asymétrique.

Les méthodes anciennes utilisées pour cryptage et pour décryptage ont été symétriques : les applications

$$\mathcal{E}_{ij} : \mathcal{M} \to \mathcal{M}, \text{ et } \mathcal{D}_{ij} : \mathcal{M} \to \mathcal{M},$$

ont été connu pour U_i et U_j, mais secrets pour tout autre utilisateur U_k, avec $k \neq i, j$.

Par exemple, on a utilisé souvent le cryptage *par permutation* $\mathcal{E}_{ij}$, ou cryptage par *addition avec un grand nombre aléatoire* dans $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$.

En 1976, des nouveaux systèmes de cryptographie *asymétriques* ont été découverts par Diffie, Hellman, Rivest, Shamir, Adleman à la base de la difficulté du *problème d'inversion*.

5.1 Fonctions sens unique à trappe.

Soient $\mathcal{E}$ et $\mathcal{F}$ deux ensembles finis, par exemple $\mathcal{E} = \mathcal{F} = \mathcal{M}$. Une fonction ψ bijective de $\mathcal{E}$ dans $\mathcal{F}$ est dite une *fonction sens unique* (FSU) si étant donné $y \in \mathcal{F}$ tel qu'il existe $x \in \mathcal{E}$ avec $\psi(x) = y$, la seule donnée de ψ et de y ne permet pas de calculer x ; c'est le *problème d'inversion*, c'est-à-dire calculer la fonction inverse ψ^{-1} de ψ. La fonction ψ est dite *fonction sens unique à trappe* (FSUT) si c'est une FSU telle que il existe une information supplémentaire, la *clé secrète* $\mathcal{K}$, qui permet de résoudre le problème d'inversion.

Utilisations des fonctions sens unique à trappe.

Soit ψ une FSUT de $\mathcal{E}$ dans $\mathcal{F}$ avec la clé secrète $\mathcal{K}$. Les messages possibles sont les éléments de $\mathcal{E}$ et les messages cryptés sont les éléments de $\mathcal{F}$. Afin de recevoir des messages cryptés, *Alice* (un utilisateur) rend publique la fonction ψ (fonction de cryptage), elle garde secret néanmoins la clé $\mathcal{K}$. Pour transmettre un message $x \in \mathcal{E}$ à *Alice*, *Bob* calcule $y = \psi(x)$ et envoie y. Afin de décoder le message y, il faut pouvoir calculer $x = \psi^{-1}(y)$, or seule *Alice*, qui possède $\mathcal{K}$, arrive à calculer ψ^{-1} (fonction de décryptage). Ainsi, tout le monde peut coder un message, mais seule *Alice* peut le décoder.

5.2 Principaux protocoles.

Les principaux protocoles existants utilisant des FSU ou des FSUT sont le protocole RSA, et les protocoles de type ElGamal basés sur le problème du logarithme discret : dans le groupe des éléments inversibles d'un corps fini ou dans le groupe des points d'une courbe elliptique sur un corps fini.

Le protocole RSA (comme Rivest, Shamir, Adleman), voir [RSA]

Soient p et q deux nombres premiers de grande taille, on pose $n = p \cdot q$. L'ensemble $\mathcal{E}$ et l'ensemble $\mathcal{F}$ sont le même ensemble : l'ensemble $\mathcal{M} = \{0, \ldots, n-1\}$ des nombres entiers entre 0 et $n-1$. Soit e un nombre entier premier avec $(p-1)(q-1)$. La fonction ψ est la fonction

$$\psi(x) = x^e \mod n,$$

la clef secrète $\mathcal{K}$ est un entier d tel que

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)},$$

alors on a

$$\psi^{-1}(x) = x^d \pmod{n}.$$

Cette assertion est vraie pour tous les $x \mod pq$.

Si $\text{pgcd}(x, pq) = 1$, on utilise le théorème d'Euler-Fermat :

$$x^{ed} \equiv x \bmod pq.$$

Si, par exemple $p|x$, mais $q \nmid x$, on a donc

$$ed = 1 + (p-1)(q-1)t \Rightarrow x^{ed} = (x)^{1+(p-1)(q-1)t} = x(x^{(p-1)t})^{q-1} \equiv x \bmod pq$$
$$\Rightarrow x^{ed} = \begin{cases} x((x)^{(p-1)})^{q-1} \equiv x \cdot 1 \bmod q, \\ \equiv 0 \equiv x \bmod p \end{cases} \quad \Rightarrow x^{ed} \equiv x \bmod pq.$$

La sécurité du protocole RSA

réside sur le fait que pour calculer l'entier d, il faut connaître les nombres p et q, et donc être à même de factoriser l'entier n.

Pour réaliser ce schéma on utilise la difficulté technique de factorisation de grands nombres entiers en produit de nombres premiers.

Système RSA pour plusieurs utilisateurs

a). Chaque utilisateur U_i choisit deux grand nombres premiers p_i, q_i, et deux classes $e_i, d_i \bmod n_i$ où $n_i = p_i q_i$ telles que $e_i d_i \equiv 1 \bmod \varphi(n_i)$ où $\varphi(n_i) = (p_i - 1)(q_i - 1)$ désignes la fonction de Euler.

b). Les nombres (e_i, n_i) sont publiques pour tous les utilisateurs (ils sont publiés dans une sorte de "pages blanches").

On suppose qu'il n'est pas possible de calculer d_i à partir de (e_i, n_i), donc d_i peut être consideré comme une clef secrète de décryptage connue seulement à U_i. En effet, on montrera qu'un algorithme efficace pour calculer d_i trouve aussi la *factorisation* de n_i (ceci dit, un tel algorithme est *équivalente* à la résolution d'un problème supposé difficile). Supposons qu'on connait d_i. Alors on connait que $\varphi(n_i)$ *divise* $e_i d_i - 1$. Si l'on avait connu $\varphi(n_i)$ on aurait pu trouver facilement p_i, q_i car

$$\varphi(n_i) = (p_i - 1)(q_i - 1) = p_i q_i - (p_i + q_i) + 1 \Rightarrow$$
$$p_i + q_i = n_i + 1 - \varphi(n_i) \text{ et } p_i - q_i = \sqrt{(p_i + q_i)^2 - 4n_i}.$$

On peut montrer même que si l'on connait seulement un multiple de $\varphi(n_i)$ on puisse trouver p_i, q_i.

c). Supposons qu'un utilisateur U_i souhaite à transmettre à U_j un message secret repésenté comme un suite de bits. Tout d'abord, il décompose cette suite en blocs de longueur $[\log_2 n_j]$, alors il considère tout bloc comme une classe des résidue $m \bmod n_j$ et finalement il crypte le message par la classe $m^{e_j} \bmod n_j$. Ceci dit, (n_j, e_j) sers comme une clef de cryptage de j-e utilisateur.

d). Ayant reçu le message crypté, U_j le décrypte bloc-par-bloc $b \bmod n_j$ par calcule de $b^{d_j} \bmod n_j$ (rapellons qu'il connait seulement sa clef de décryptage d_j). Ceci est impliqué immédiatement par le théorème d'Euler-Fermat.

Exemple de cryptage avec RSA

On suppose qu'on travaille avec un alphabet de N symboles, alors on utilise une base d'écriture $= N$. Soient $k < l$ deux entiers strictement positifs tel que $N^k < n_j < N^l$, par exemple $k = [\log_N n_j]$. Alors les blocs de k lettres correspondent aux nombres
$0 \leq m < n_j$. Tout message est présenté comme une suite de tel blocs, et on crypte par blocs $M = m \bmod n_j$. Soit $f(M) = \mathcal{E}_j(M)$, $f : \mathbb{Z}/n_j\mathbb{Z} \to \mathbb{Z}/n_j\mathbb{Z}$. L'image $f(M)$ peut être présentée comme un bloc de l lettres car $n_j < N^l$ mais pas tous les blocs de l lettres paraissent de telle façon.

Exemple. Soit $N = 26$ (l'alphabet de 26 lettres), $p_j = 281$, $q_j = 167$, $n_j = 46927$, $e_j = 39423$, $d_j = 26767$, $k = 3$, $l = 4$,

$$N^3 = 17576 < 46927 < N^4 = 456976.$$

Le mot "YES" correspond à $24 \cdot N^2 + 4 \cdot N + 18 = 16346 = m \bmod n_j$.

$$16346^{39423} \bmod 46927 = 21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2 = \text{ "BFIC" } = \bmod n_j$$

Pour décrypter le message, l'utilisateur U_j applique

$$b \mapsto b^{d_j} \bmod n_j,\ 21166^{26767} \bmod 46927 = 16346.$$

Le protocole ElGamal

s'applique dès que l'on a un groupe cyclique fini G. Dans la pratique, le groupe G est soit le groupe multiplicatif d'un corps fini $\mathbb{F}_p^\times$, soit le groupe $E(\mathbb{F}_p)$ des points d'une courbe elliptique E sur un corps fini $\mathbb{F}_p$. On fixe g un générateur de G et on note M l'ordre de G. L'ensemble $\mathcal{E}$ est égal à G et l'ensemble $\mathcal{F}$ est le produit $G \times G$, c'est-à-dire à l'ensemble formé des couples de deux élément de G. *Alice* choisit, au hasard, un élément a dans $\{0, \ldots, M-1\}$ et calcule g^a. Puis elle rend publique G, g et g^a. La clé secrète $\mathbb{K}$ est l'entier a. Pour crypter un message $x \in G$, *Bob* choisit un entier k au hasard dans $\{0, \ldots, M-1\}$ et calcule $y_1 = g^k$, puis $y_1 = x \cdot (g^a)^k$ (ce qui est possible puisque g^a est publique). Le message crypté est le couple (y_1, y_2). En d'autres termes, la fonction de cryptage FSUT ψ est donnée par

$$\psi(x) = \left(g^k, x \cdot (g^a)^k\right)$$

avec k un entier choisi au hasard dans $\{0, \ldots, M-1\}$ et différent à chaque fois. Pour décrypter un tel message (y_1, y_2), *Alice* calcule y_1^{-a} et obtient

$$y_1^{-a} \cdot y_2 = g^{-ak} \cdot x \cdot g^{ak} = g^{ak-ak} \cdot x = x.$$

Ainsi la fonction de décryptage

$$\psi^{-1}(y_1, y_2) = y_1^{-a} \cdot y_2$$

n'est calculable que si on connaît la clé secrète $\mathbb{K}$.

La sécurité de ce protocole repose sur la difficulté de résoudre le problème du logarithme discret. Plus précisément, le problème de retrouver l'entier a étant donnés g et g^a. C'est un problème difficile dans la plupart des cas si l'ordre du G groupe est divisible par un grand nombre premier.

5.3 Signatures éléctroniques

Bien évidemmement, on peut varier les détails de ce schéma *ad infinitum*. Par exemple, on peut construire une procédure d'authentification ("electronic signature") qui utilise une forme *signé* d'un message secret de U_i à U_j permettant U_j de convaincre une troisième personne (un "juge") que l'auteur du message est bien U_i donc ce message n'été pas falcifié par U_j lui-même. Ceci peut être crucial pour certaines transactions interbancaires.

On considère l'application $\mathcal{E}_i$ de cryptage pour les messages adressés à U_i et soit $\mathcal{D}_i$ l'application de décryptage de U_i. Alors on a vu que $\mathcal{E}_i$ est publique tandis que $\mathcal{D}_i$ est privé (la propriété de U_i). Pour tout message M on a $\mathcal{D}_i(\mathcal{E}_i(M)) = M$ et $\mathcal{E}_i(\mathcal{D}_i(M)) = M$. L'utilisateur U_i en envoiant à U_j son message M utilise comme sa signature $S = \mathcal{D}_i(M)$ et il transmet à U_j sa version cryptée $\mathcal{E}_j(S)$. A son tour, U_j d'abord calcule $S = \mathcal{D}_j(\mathcal{E}_j(S))$ et ensuite $M = \mathcal{E}_i(S)$ en utilisant la clef publique $\mathcal{E}_i$. Le récépteur peut convaincre un juge que M vient de U_i parce que seulement avec l'application $\mathcal{E}_i$ on peut transformer S en un message sensé M.

De plus, le récépteur de $S = \mathcal{D}_i(M)$ ne peut pas le falcifier car il ne connait pas $\mathcal{D}_i$.

Maintenant on discutra plutôt des aspects arithmétiques que les aspects informatiques de la théorie des cryptosystèms à clef publique. On montrera que les résultats classiques de l'arithméique peuvent être appliqués dans ce domaine.

Problème 1. Comment produire des grands nombres premiers ?

On a besoin d'une méthode vraiment efficace pour organiser une production en masse des grands nombres premiers "suffisemment aléatoirs" pour permettre à un utulisateur à calculer (à l'aide d'un ordinateur) son couple customisé (p_i, q_i) et d'être sûr qu'aucun autre utilisateur ne prendra cette paire.

Problème 2. Comment factoriser grands nombres entiers ?

Ce problème est clé pour la troisième partie qui souhaite casser le cryptosystème mais aussi, bien-sûr, pour les développeurs essayant assurer la fiaibilité d'un tel système.

6 Construction d'une fonction sens unique à trappe.

Nous pouvons à présent expliquer comment construire une FSUT de B dans lui-même en utilisant les modules de Drinfeld. Cette construction sera plus rapidement détaillée dans la section suivante.

6.1 Présentation théorique du protocole.

Soit p un nombre premier. On note $A = \mathbb{F}_p[T]$ l'anneau des polynômes à une variable et à coefficients dans le corps $\mathbb{F}_p$. Puis, on pose $A\{\tau\}$ l'anneau des polynômes à coefficients dans A et en la variable τ avec les règles d'addition usuelle et pour la multiplication, la règle de commutation suivante :

$$\tau^k \times a = a^{p^k} \times \tau^k$$

pour $a \in A$ et $k \geq 1$.

Exemple. Prenons $p = 3$, et multiplions deux éléments de $A\{\tau\}$:

$$\begin{aligned}\big((T+1)\tau^2 + (T^2+2)\tau\big) \times (2T\tau + 1)& \\ &= (T+1)\tau^2 \times 2T\tau + (T+1)\tau^2 + (T^2+2)\tau \times 2T\tau + (T^2+2)\tau \\ &= (T+1)(2T)^9\tau^3 + (T+1)\tau^2 + (T^2+2)(2T)^3\tau^2 + (T^2+2)\tau \\ &= (2T^{10} + 2T^9)\tau^3 + (T+1)\tau^2 + (2T^5 + T^3)\tau^2 + (T^2+2)\tau. \\ (T+\tau)^2 = (T+\tau) \times (T+\tau) &= T^2 + T \times \tau + \tau \times T + \tau^2 \\ &= T^2 + T \times \tau + T^3 \times \tau + \tau^2 = T^2 + (T+T^3) \times \tau + \tau^2\end{aligned}$$

Par la suite, les exemples reprendront toujours les notations définies dans les exemples précédents. Nous définissons un module de Drinfeld comme une morphisme φ de $\mathbb{F}_p$-algèbre de A dans $A\{\tau\}$ telle $\varphi(T)$ est un polynôme (en τ) non constant et de terme constant T. Soit $a = \sum_{i=0}^m a_i T^i$ un élément de A, on a donc

$$\varphi(a) = \varphi\left(\sum_{i=0}^m a_i T^i\right) = \sum_{i=0}^m a_i \varphi(T^i) = \sum_{i=0}^m \varphi(a_i T^i) = \sum_{i=0}^m a_i \varphi(T)^i.$$

Ainsi, le module de Drinfeld φ est complètement défini une fois que $\varphi(T)$ a été choisi.

Exemple. L'exemple le plus simple de module de Drinfeld est le module de Carlitz défini par $\varphi(T) = \tau + T$. On a :

$$\varphi(T^2+T+1) = (\tau+T)^2 + (\tau+T) + 1 = \tau^2 + (T^3+T+1)\tau + (T^2+T+1).$$

Chaque élément de $A\{\tau\}$ défini une application de A dans lui-même en identifiant chaque élément $a \in A$ avec l'application $z \mapsto az$ et τ avec l'application de Frobenius $z \mapsto z^p$, la multiplication dans $A\{\tau\}$ correspond alors à la composition des fonctions. Ainsi, on obtient :

$$\sum_{i=0}^m a_i \tau^i : z \mapsto \sum_{i=0}^m a_i z^{p^i}.$$

Pour $a \in A$, on note φ_a l'application de A dans lui-même définie par $\varphi(a) \in A\{\tau\}$. L'application φ_1 est l'identité sur A.

EXEMPLE. La fonction définie par l'exemple précédent est :

$$\varphi_{T^2+T+1}(z) = \left(\tau^2 + (T^3+T+1)\tau + (T^2+T+1)\right) z = z^9 + (T^3+T+1)z^3 + (T^2+T+1)z.$$

6.2 Nouvelles structures de modules sur les A-algèbres.

Soit $d > 1$ un entier et soit $f(T) \in A$ un polynôme irréductible de degré d. On pose B le quotient de A par $f(T)$. Ainsi B est isomorphe au corps fini à p^d éléments. Pour $a \in A$, on pose $\overline{a}$ la classe de a dans B. L'anneau fini B a donc une structure naturelle de A-module donnée par :

$$a \times \beta = \overline{ab}$$

pour $a \in A$ et $\beta \in B$ tel que $\beta = \overline{b}$ avec $b \in A$.

Soit $a \in A$, on note $\overline{\varphi_a}$ l'application de B dans B défini par :

$$\overline{\varphi_a} \colon \beta \mapsto \overline{\varphi_a(b)}.$$

(avec les mêmes notations que ci-dessus). Alors, le module de Drinfeld φ permet de munir B d'une autre structure de A-module donnée par :

$$a \times_\varphi \beta = \overline{\varphi_a}(\beta)$$

La même construction marche pour munir toute A-algèbre B d'une (nouvelle) φ-structure d'un A-module notée par B_φ.

EXEMPLE. Posons $d = 2$ et $f(T) = T^2 + 1$. On a alors

$$\overline{\varphi_{T^2+T+1}}(z) = z^9 + z^3 + \overline{T}z.$$

On note B_φ l'ensemble B muni de la structure de A-module défini ci-dessus. Puisque on suppose que le rang de φ est égal 1, et B_φ est un A-module de cardinal p^d, il existe un polynôme unitaire $f_\varphi \in A$ de degré d tel que

$$B_\varphi \simeq A/(f_\varphi)$$

comme A-module, voir Corollaire 3.6.5. En général, f_φ n'est pas irréductible.

EXEMPLE. On calcule (voir la section suivante pour la méthode de calcul) :

$$f_\varphi(T) = T^2.$$

Une remarque fondamentale est que deux éléments a_1 et a_2 de A donnent la même application $\overline{\varphi_{a_1}} = \overline{\varphi_{a_2}}$ si et seulement si

$$a_1 \equiv a_2 \pmod{f_\varphi}.$$

Ainsi, l'application $\overline{\varphi_a}$ est bijective si et seulement a est premier avec f_φ et, dans ce cas, l'application inverse est $\overline{\varphi_{a'}}$ où $a' \in A$ est tel que $aa' \equiv 1 \pmod{f_\varphi}$.

EXEMPLE. Le polynôme $T+1$ est premier avec $f_\varphi(T) = T^2$ donc l'application

$$\overline{\varphi_{T+1}} \colon z \mapsto z^3 + (\overline{T+1})z$$

est inversible. On a $(T+1)(1-T) \equiv 1 \pmod{f_\varphi}$ et donc la fonction

$$\overline{\varphi_{1-T}} : z \mapsto -z^3 + (\overline{1-T})z$$

est la fonction inverse de $\overline{\varphi_{T+1}}$.

6.3 Présentation pratique du protocole

Nous pouvons à présent expliquer comment construire une FSUT de B dans lui-même en utilisant les modules de Drinfeld. Cette construction sera plus rapidement détaillée dans la section suivante.

Nous reprenons les notations de la section 5.1 On prend $\mathcal{E} = \mathcal{F} = B$. La *clé secrète* $\mathbb{K}$ est composé de deux éléments c_1 et c_2 de A, tous les deux premiers avec f_φ, et d'une bijection σ de B dans lui-même (voir la section suivante pour des exemples de choix de σ). La fonction ψ est alors défini par :

$$\psi(z) = \left(\overline{\varphi_{c_1}} \circ \sigma \circ \overline{\varphi_{c_2}}\right)(z)$$

donné comme une fonction polynômiale de $B[z]$. Cette fonction est bijective et sa réciproque est la fonction

$$\psi^{-1}(z) = \left(\overline{\varphi_{c_2'}} \circ \sigma^{-1} \circ \overline{\varphi_{c_1'}}\right)(z)$$

avec c_1' et c_2' deux éléments de A tels que $c_1\, c_1' \equiv 1 \pmod{f_\varphi}$, $c_2\, c_2' \equiv 1 \pmod{f_\varphi}$. Cette fonction inverse ne peut être déterminée facilement que si la clé secrète (c_1, c_2, σ) est connue.

Supposons choisis les différents paramètres p, φ, d et f – les choix de ceux-ci seront discutés dans la section suivante –, nous montrons comment trouver c_1, c_2 et σ, puis calculer les fonctions ψ et ψ^{-1} et s'en servir pour le codage et le décodage.

Exemple. Nous utiliserons les paramètres suivants pour illustrer cette construction : $p = 3$, $\varphi_T = \tau + T$ (module de Carlitz), $d = 3$, $f(T) = T^3 + 2T^2 + 1$.

6.4 Calculs dans les modules de Drinfeld finis.

Pour calculer dans B, nous représentons chaque classe par l'unique polynôme de degré $< d$ contenu dans la classe. Ce polynôme est le reste de la division euclidienne d'un polynôme quelconque de la classe par $f(T)$.

Exemple. Effectuons une multiplication dans B :

$$\overline{(T^2 + 2T + 1)} \times \overline{(2T^2 + T + 1)} = \overline{2T^4 + 2T^3 + 2T^2 + 1} = \overline{T}$$

puisque, dans A, on a :

$$2T^4 + 2T^3 + 2T^2 + 1 = (T^3 + 2T^2 + 1) \times (2T + 1) + T.$$

Soit $a \in A$ et $\beta \in B$, on veut à présent pouvoir calculer $\overline{\varphi_a}(\beta)$. On écrit :

$$a = \sum_{i=0}^{m} a_i T^i,$$
$$\beta = \sum_{j=0}^{d-1} \overline{b_j T^j}.$$

alors :

$$\overline{\varphi_a}(\beta) = \sum_{i=0}^{m} \overline{a_i \varphi_{T^i}}(\beta) = \sum_{i=0}^{m} \overline{a_i} \sum_{j=0}^{d-1} \overline{b_j}\, \overline{\varphi_{T^i}}(\overline{T^j}) = \sum_{i=0}^{m} \sum_{j=0}^{d-1} \overline{a_i b_j}\, \overline{\varphi_{T^i}}(\overline{T^j}).$$

Donc il suffit de savoir calculer $\overline{\varphi_{T^i}}(\overline{T^j})$ pour en déduire par cette formule $\overline{\varphi_a}(\beta)$. De surcroît, puisque $\overline{\varphi_a} = \overline{\varphi_{a'}}$ si $a \equiv a' \pmod{f_\varphi}$, si on prend pour a' le reste de la division euclidienne de a par f_φ, on voit qu'il est suffisant de connaître considérer uniquement les exposants i tels que $0 \leq i \leq d-1$. On écrit

$$\varphi(T) = \sum_{k=0}^{d} g_k \tau^k$$

avec $g_k \in A$ et, par définition, $g_0 = T$. Alors, on a, pour tout $j \geq 0$:

$$\overline{\varphi_1}(\overline{T^j}) = \overline{T^j},$$
$$\overline{\varphi_T}(\overline{T^j}) = \sum_{k=0}^{d} \overline{g_k \times T^{jp^k}},$$

puis la formule de récurrence, pour $i \geq 1$:

$$\overline{\varphi_{T^{i+1}}}(\overline{T^j}) = \overline{\varphi_T}\Big(\overline{\varphi_{T^i}}(\overline{T^j})\Big)$$

pour calculer les autres valeurs.

EXEMPLE. Soient $a = 2T^2 + 1 \in A$ et $\beta = \overline{T^2 + T + 1} \in B$, on va calculer $\overline{\varphi_a}(\beta)$. On commence par calculer les $\overline{\varphi_T}(\overline{T^j})$ pour $j = 0, 1, 2, 3$:

$$\overline{\varphi_T}(\overline{1}) = \overline{T + 1}$$
$$\overline{\varphi_T}(\overline{T}) = \overline{T^3 + T^2} = \overline{2T^2 + 2}$$
$$\overline{\varphi_T}(\overline{T^2}) = \overline{T^6 + T^3} = \overline{2T + 2}.$$

On en déduit les valeurs de $\overline{\varphi_{T^i}}(\overline{T^j})$ pour $i = 2$:

$$\overline{\varphi_{T^2}}(\overline{1}) = \overline{\varphi_T}\big(\overline{\varphi_T}(\overline{1})\big) = \overline{\varphi_T}\big(\overline{T + 1}\big) = \overline{\varphi_T}(\overline{T}) + \overline{\varphi_T}(\overline{1}) = \overline{2T^2 + T},$$
$$\overline{\varphi_{T^2}}(\overline{T}) = \overline{\varphi_T}\big(\overline{\varphi_T}(\overline{T})\big) = \overline{\varphi_T}\Big(\overline{2T^2 + 2}\Big) = \overline{0},$$
$$\overline{\varphi_{T^2}}(\overline{T^2}) = \overline{\varphi_T}\Big(\overline{\varphi_T}(\overline{T^2})\Big) = \overline{\varphi_T}\big(\overline{2T + 2}\big) = \overline{T^2 + 2T}.$$

Ainsi, finalement, on trouve :

$$\begin{aligned}\overline{\varphi_a}(\beta) &= 2\overline{\varphi_{T^2}}(\beta) + \overline{\varphi_1}(\beta) \\ &= \overline{2}\,\overline{\varphi_{T^2}}(\overline{T^2}) + \overline{2}\,\overline{\varphi_{T^2}}(\overline{T}) + \overline{2}\,\overline{\varphi_{T^2}}(\overline{1}) + \overline{\varphi_1}(\overline{T^2}) + \overline{\varphi_1}(\overline{T}) + \overline{\varphi_1}(\overline{1}) \\ &= \overline{T^2 + T + 1}.\end{aligned}$$

6.5 Calcul de la caractéristique d'Euler-Poincaré.

Maintenant que nous savons calculer dans B_φ, il faut calculer le polynôme f_φ. En tant que $\mathbb{F}_p$-espace vectoriel B est de dimension d admettant la famille $\{\overline{1}, \overline{T}, \ldots, \overline{T}^{d-1}\}$ pour base. L'application $\overline{\varphi_T}$ est en fait un endomorphisme de cette espace vectoriel donc on calcule facilement la matrice, puis le polynôme caractéristique $C(T)$. Alors f_φ est égal à $C(T)$. En effet, si on écrit

$$C(T) = T^d + \lambda_{d-1}T^{d-1} + \cdots + \lambda_1 T + \lambda_0,$$

on a donc la relation

$$\overline{\varphi_T}^d + \lambda_{d-1}\overline{\varphi_T}^{d-1} + \cdots + \lambda_1\overline{\varphi_T} + \lambda_0 = \mathbb{O}$$

où $\mathbb{O}\colon z \mapsto \overline{0}$ est l'application nulle. Mais, par les propriétés de φ, cette relation se réécrit sous la forme

$$\overline{\varphi_{T^d + \lambda_{d-1}T^{d-1} + \cdots + \lambda_1 T + \lambda_0}} = \mathbb{O}$$

d'où $\overline{\varphi_{C(T)}} = \mathbb{O}$, ce qui démontre le résultat puisque $C(T)$ est unitaire et degré d.

EXEMPLE. On a déjà calculé les $\overline{\varphi_T}(\overline{T^j})$ pour $0 \leq j \leq 2$, on en déduit la matrice de l'endomorphisme $\overline{\varphi_T}$:

$$\begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & 2 \\ 0 & 2 & 0 \end{pmatrix} \text{ puisque } \begin{array}{l} \overline{\varphi_T}(\overline{1}) = \overline{T+1} \\ \overline{\varphi_T}(\overline{T}) = \overline{T^3+T^2} = \overline{2T^2+2} \\ \overline{\varphi_T}(\overline{T^2}) = \overline{T^6+T^3} = \overline{2T+2}, \end{array} \text{ , et } f(T) = T^3 + 2T^2 + 1.$$

Donc le polynôme caractéristique est

$$C(T) = -\det \begin{pmatrix} 1-T & 2 & 2 \\ 1 & -T & 2 \\ 0 & 2 & -T \end{pmatrix} = T^3 + 2T^2.$$

Ainsi, $f_\varphi(T) = T^3 + 2T^2 = T^2(T+2)$.

6.6 Calcul de la clef.

Il faut à présent choisir la clé secrète, c'est-à-dire les deux éléments c_1 et c_2 de A, de degré $< d$ et premiers avec la caractéristique d'Euler-Poincaré f_φ, et la bijection σ. Pour c_1 et c_2, la meilleure méthode est de choisir au hasard un couple de deux polynômes distincts jusqu'à ce qu'ils soient tous deux premiers avec f_φ. On calcule aussi les deux polynômes c_1' et c_2' de degré $< d$ et tels que :

$$c_1\, c_1' \equiv 1 \pmod{f_\varphi} \quad \text{et} \quad c_2\, c_2' \equiv 1 \pmod{f_\varphi},$$

ces deux polynômes serviront pour le décryptage. Pour la bijection σ, il faut une fonction simple et rapide à calculer, donné sous la forme d'un polynôme. Soit $e < p^d - 1$ un entier non divisible par p et premier avec $p^d - 1$, on prend :

$$\sigma \colon z \mapsto z^e + \delta$$

où δ est un élément pris au hasard dans B. Si on note f un entier tel que

$$ef \equiv 1 \pmod{p^d - 1}$$

alors, on a :

$$\sigma^{-1} \colon z \mapsto (z - \delta)^f.$$

EXEMPLE. On considère toujours $p = 3$, $\varphi_T = \tau + T$ (module de Carlitz), $d = 3$, $f(T) = T^3 + 2T^2 + 1$. On prend donc au hasard

$$c_1 = T^2 + T + 2 \quad \text{et} \quad c_2 = 2T^2 + T + 1,$$

qui sont bien des polynômes premiers avec $f_\varphi = T^3 + 2T^2$, et on calcule

$$c_1' = 2T + 2 \quad \text{et} \quad c_2' = T^2 + 2T + 1.$$

```
> gcdex( T^2 + T + 2,T^3 + 2*T^2, T, 'U', 'V') : #A*U+B*V=gcd
> Expand(U) mod 3;
```

$$2 + 2\,T$$

```
> gcdex( 2*T^2 + T + 1,T^3 + 2*T^2, T, 'U', 'V') : #A*U+B*V=gcd
> Expand(U) mod 3;
```

$$1 + 2\,T + T^2$$

Pour la fonction σ, on prend $e = 7$ et

$$\delta = \overline{T^2 + T + 1}.$$

Ainsi, on a $1/7 \bmod 26 = 15$, donc

$$\sigma\colon z \mapsto z^7 + \overline{T^2+T+1},$$
$$\sigma^{-1}\colon z \mapsto \left(z - \overline{(T^2+T+1)}\right)^{15}.$$

A présent, on calcule la FSUT

$$\psi(z) = \left(\overline{\varphi_{c_1}} \circ \sigma \circ \overline{\varphi_{c_2}}\right)(z)$$

sous la forme d'un polynôme. Pour cela, on écrit à nouveau :

$$a = \sum_{i=0}^{d-1} a_i T^i$$

avec $a_i \in A$, et donc

$$\overline{\varphi_a}(z) = \sum_{i=0}^{d-1} \overline{a_i}\, \overline{\varphi_{T^i}}(z).$$

Les $\overline{\varphi_{T^i}}(z)$ sont reliés par la relation de récurrence déjà mentionnés ci-dessus :

$$\overline{\varphi_1}(z) = z,$$
$$\overline{\varphi_{T^i}}(z) = \overline{\varphi_T}(\overline{\varphi_{T^{i-1}}}(z)) \quad \text{si } i > 0.$$

Pour utiliser cette formule, on écrit

$$\varphi_T = \sum_{k=0}^{d} g_k \tau^k$$

avec $g_i \in A$, et, par convention, $g_0 = T$. Alors, pour tout polynôme

$$P(z) = \sum_{i=0}^{m} \pi_i z^i \in B[z],$$

on a

$$\boxed{\overline{\varphi_T}(P(z)) = \sum_{k=0}^{d} \sum_{i=0}^{m} \overline{g_k} \pi_i^{p^k} z^{ip^k}.}$$

Donc on calcule $\overline{\varphi_{c_2}}(z)$ par cette formule, on en déduit $\sigma(\overline{\varphi_{c_2}})(z)$ en remplaçant z par $\overline{\varphi_{c_2}}(z)$ dans la définition de σ, et finalement on trouve $\psi(z)$ en remplaçant, dans l'expression de $\overline{\varphi_{c_1}}(z)$, z par l'expression trouvée pour $\sigma(\overline{\varphi_{c_2}})(z)$. On obtient une expression pour $\psi(z)$ donné comme un polynôme en z et à coefficients dans B. Il est à noter que dans ce calcul, on doit remplacer les termes de la forme

$$\gamma z^m \quad \text{avec } m \geq p^d$$

par

$$\gamma z^r$$

où r est le reste de la division euclidienne de m par $p^d - 1$, puisque :

$$\beta^m = \beta^r$$

pour tout $\beta \in B$. On s'assure ainsi que tous les termes de $\psi(z)$ reste de degré borné par p^d.

EXEMPLE. On considère toujours $p = 3$, $\varphi_T = \tau + T$ (module de Carlitz), $d = 3$, $f(T) = T^3 + 2T^2 + 1$. On calcule (pour $c_1 = T^2 + T + 2$, $c_2 = 2T^2 + T + 1$) :

$$\begin{aligned}
\overline{\varphi_1}(z) &= z,\\
\overline{\varphi_T}(z) &= z^3 + \overline{T}z,\\
\overline{\varphi_{T^2}}(z) &= \overline{\varphi_T}\big(z^3 + \overline{T}z\big) = z^9 + \overline{T^2 + T + 2}\, z^3 + \overline{T^2}z.
\end{aligned}$$

On en déduit :

$$\begin{aligned}
\overline{\varphi_{c_1}}(z) &= \overline{\varphi_{T^2}}(z) + \overline{\varphi_T}(z) + 2\overline{\varphi_1}(z) = z^9 + \overline{T^2 + T}\, z^3 + \overline{T^2 + T + 2}\, z,\\
\overline{\varphi_{c_2}}(z) &= 2\overline{\varphi_{T^2}}(z) + \overline{\varphi_T}(z) + \overline{\varphi_1}(z) = \overline{2}\, z^9 + \overline{2T^2 + 2T + 2}\, z^3 + \overline{2T^2 + T + 1}\, z.
\end{aligned}$$

Ensuite, on a :

$$\begin{aligned}
\sigma(\overline{\varphi_{c_2}}(z)) &= \Big(\overline{2}\, z^9 + \overline{2T^2 + 2T + 2}\, z^3 + \overline{2T^2 + T + 1}\, z\Big)^7 + \overline{T^2 + T + 1}\\
&= \overline{T}\, z^{21} + \overline{T^2}\, z^{19} + \overline{T^2 + 2T}\, z^{15} + Tz^{11} + \overline{T^2 + 1}\, z^9\\
&\qquad + \overline{T + 2}\, z^7 + \overline{T^2 + 2T}\, z^5 + \overline{2T^2 + T + 1}\, z^3 + \overline{2T^2}\, z + \overline{T^2 + T + 1}
\end{aligned}$$

et en substituant dans l'expression de $\overline{\varphi_{c_1}}(z)$, on obtient finalement l'expression de $\psi(z)$ recherchée :

$$\begin{aligned}
\psi(z) = \overline{T^2 + T + 2}\, z^{21} &+ \overline{T + 2}\, z^{19} + \overline{T + 2}\, z^{15} + \overline{2T^2 + 2T}\, z^{11}\\
&+ \overline{2T^2}\, z^9 + \overline{T^2 + T}\, z^7 + \overline{2T^2}\, z^5 + \overline{T + 2}\, z^3 + \overline{T^2 + T}\, z^1 + \overline{T^2 + 2T}.
\end{aligned}$$

Le cardinal de B est p^d, donc la FSUT ψ permet de coder des messages donnés sous la forme d'un nombre M vérifiant $0 \leq M < p^d$. En effet, étant donné un tel nombre M, on le transforme en un élément de B en utilisant l'écriture de M en base p : il existe des entiers uniques $m_0, \ldots, m_{d-1}$ vérifiant $0 \leq m_i < p$ et tels que

$$M = m_0 + m_1\, p + m_2\, p^2 + \cdots + m_{d-1}\, p^{d-1},$$

ce qui permet d'associer de manière unique à l'entier M, l'élément

$$\mu = \overline{m_0 + m_1 T + \cdots + m_{d-1} T^{d-1}}$$

de B. On calcule alors

$$\chi = \psi(\mu) = \overline{k_0 + k_1 T + \cdots + k_{d-1} T^{d-1}}$$

et le message codé C est alors donné, comme nombre entre 0 et p^d, par le procédé inverse :

$$C = k_0 + k_1\, p + \cdots + k_{d-1}\, p^{d-1}.$$

6.7 Décryptage d'un message.

Pour décrypter le message, on utilise la procédure inverse, à partir de C, on construit l'élément χ de B correspondant, on applique ψ^{-1} pour en déduire μ et finalement M. Il est à noter cependant, que plutôt de calculer $\psi^{-1}(z)$ sous forme d'un polynôme pour effectuer le calcul de $\psi^{-1}(\mu)$, il est plus efficace de faire ce calcul en utilisant l'expression :

$$\psi^{-1}(\mu) = \overline{\varphi_{c_2'}}\big(\sigma^{-1}\big(\overline{\varphi_{c_1'}}(\mu)\big)\big)\,,$$

c'est-à-dire d'appliquer successivement $\overline{\varphi_{c'_1}}$, σ^{-1} et $\overline{\varphi_{c'_2}}$.

EXEMPLE. Les paramètres choisis pour cet exemple permettent de coder un nombre compris M avec $0 \leq M \leq 3^3 - 1 = 26$. Prenons $M = 17$, on a donc :

$$M = 2 + 2 \times 3 + 1 \times 3^2,$$

d'où $\mu = \overline{T^2 + 2T + 2}$. On calcule

$$\chi = \psi(\overline{T^2 + 2T + 2}) = \overline{2T^2 + T + 1},$$

d'où le message crypté $C = 1 + 1 \times 3 + 2 \times 3^2 = 22$.

Pour décrypter le message $C = 22$, on calcule $\chi = \overline{2T^2 + T + 1}$, puis on applique successivement les différentes fonctions composant ψ^{-1} :

$$\begin{aligned}
\overline{\varphi_{c'_1}}(\mu) &= \overline{2T^2 + 1}, \\
\left(\sigma^{-1} \circ \overline{\varphi_{c'_1}}\right)(\mu) &= \sigma^{-1}(\overline{2T^2 + 1}) = \overline{2T + 1}, \\
\left(\overline{\varphi_{c'_2}} \circ \sigma^{-1} \circ \overline{\varphi_{c'_1}}\right)(\mu) &= \overline{\varphi_{c'_2}}(\overline{2T + 1}) = \overline{T^2 + 2T + 2}.
\end{aligned}$$

Ainsi, on retrouve le message :

$$M = 2 + 2 \times 3 + 1 \times 3^2 = 17.$$

Exercices de préparation à l'exemen, version préliminaire

Cours de DEA à l'ENS Lyon (1e semestre 2003/2004)

"Modules de Drinfeld et Cryptologie"
Prof. A. A. Pantchichkine

I) Soient $A = \mathbb{F}_3[T]$, $f = T^2 + T - 1$, et on considère l'anneau quotient $B = A/(f)$, $\overline{T} = T \bmod f$, et soit $\varphi : A \to B\{\tau\}$ un module de Drinfeld tel que

$$\varphi(T) = \overline{T} + \tau + \tau^2.$$

(a) Calculer la caractéristique d'Euler-Poincaré f_φ du module B_φ.
(b) Trouver tous les $c \in A$, pour lesquels l'application $\varphi_c : B \to B$ soit inversible.
(c) Pour $c_1 = T + 2$ et $c_2 = 2T \in A$, trouver les applications inverses $\varphi_{c_1}^{-1}$ et $\varphi_{c_2}^{-1}$.

II) Calcul de la clef. Soient $A = \mathbb{F}_p[T]$, f un polynôme unitaire irréductible de degré d, $B = A/(f)$, $\overline{T} = T \bmod f$, et soit $\varphi : A \to B\{\tau\}$ un module de Drinfeld avec la caractéristique d'Euler-Poincaré f_φ. Soient c_1 et c_2, un couple de deux polynômes distincts premiers avec f_φ.

(a) Montrer qu'il existe deux polynômes c_1' et c_2' de degré $< d$ et tels que :

$$c_1\, c_1' \equiv 1 \pmod{f_\varphi} \quad \text{et} \quad c_2\, c_2' \equiv 1 \pmod{f_\varphi},$$

et que $\varphi_{c_1}^{-1} = \varphi_{c_1'}$,$\varphi_{c_2}^{-1} = \varphi_{c_2'}$.

(b) Soit $e < p^d - 1$ un entier non divisible par p et premier avec $p^d - 1$, on prend :

$$\sigma\colon z \mapsto z^e + \delta$$

où δ est un élément dans B. Si on note f un entier tel que

$$ef \equiv 1 \pmod{p^d - 1}$$

alors montrer que :

$$\sigma^{-1}\colon z \mapsto (z - \delta)^f.$$

(c) On considère toujours $p = 3$, $\varphi_T = \tau + T$ (module de Carlitz), $d = 3$, $f(T) = T^3 + 2T^2 + 1$. On considère des polynômes

$$c_1 = T^2 + T + 2 \quad \text{et} \quad c_2 = 2T^2 + T + 1.$$

Montrer que c_1 et c_2 sont deux polynômes premiers avec la caractéristique d'Euler-Poincaré $f_\varphi(T) = T^3 + 2T^2 = T^2(T + 2)$ du module B_φ, et que

Montrer que

$$c_1' = 2T + 2 \quad \text{et} \quad c_2' = T^2 + 2T + 1.$$

(d) Pour la fonction σ, on prend $e = 7$ et

$$\delta = \overline{T^2 + T + 1}.$$

Montrer que :

$$\sigma\colon z \mapsto z^7 + \overline{T^2 + T + 1}, \text{ et } \sigma^{-1}\colon z \mapsto \left(z - \overline{(T^2 + T + 1)}\right)^{15}.$$

(e) Calcul de la fonction $\psi(z) = (\overline{\varphi_{c_1}} \circ \sigma \circ \overline{\varphi_{c_2}})(z)$ sous la forme d'un polynôme. Montrer que $\psi(z)$ est une fonction polynômiale bijective sur B. Trouver le degré minimal d'un polynôme représentant $\psi(z)$.

(f)*(difficile) Vérifier que

$$\psi(z) = \overline{T^2+T+2}\, z^{21} + \overline{T+2}\, z^{19} + \overline{T+2}\, z^{15} + \overline{2T^2+2T}\, z^{11} + \overline{2T^2}\, z^9 + \overline{T^2+T}\, z^7 + \overline{2T^2}\, z^5 + \overline{T+2}\, z^3 + \overline{T^2+T}\, z^1 + \overline{T^2+2T}.$$

III) Cryptage d'un message. Le cardinal de B est p^d, donc la fonction ψ permet de coder des messages donnés sous la forme d'un nombre M vérifiant $0 \leq M < p^d$. En effet, étant donné un tel nombre M, on le transforme en un élément de B en utilisant l'écriture de M en base p : il existe des entiers uniques $m_0, \ldots, m_{d-1}$ vérifiant $0 \leq m_i < p$ et tels que

$$M = m_0 + m_1\, p + m_2\, p^2 + \cdots + m_{d-1}\, p^{d-1},$$

ce qui permet d'associer de manière unique à l'entier M, l'élément

$$\mu = \overline{m_0 + m_1 T + \cdots + m_{d-1} T^{d-1}}$$

de B. On calcule alors

$$\chi = \psi(\mu) = \overline{k_0 + k_1 T + \cdots + k_{d-1} T^{d-1}}$$

et le message codé C est alors donné, comme nombre entre 0 et p^d, par le procédé inverse :

$$C = k_0 + k_1\, p + \cdots + k_{d-1}\, p^{d-1}.$$

Les paramètres choisis pour cet exemple permettent de coder un nombre compris M avec $0 \leq M \leq 3^3 - 1 = 26$. Prenons $M = 17$, on a donc :

$$M = 2 + 2 \times 3 + 1 \times 3^2,$$

d'où $\mu = \overline{T^2 + 2T + 2}$.

Montrer que :

$$\chi = \psi(\overline{T^2+2T+2}) = \overline{2T^2+T+1},$$

d'où le message crypté $C = 1 + 1 \times 3 + 2 \times 3^2 = 22$.

IV) Décryptage d'un message. Pour décrypter le message, on utilise la procédure inverse, à partir de C, on construit l'élément χ de B correspondant, on applique ψ^{-1} pour en déduire μ et finalement M. Il est à noter cependant, que plutôt de calculer $\psi^{-1}(z)$ sous forme d'un polynôme pour effectuer le calcul de $\psi^{-1}(\mu)$, il est plus efficace de faire ce calcul en utilisant l'expression :

$$\psi^{-1}(\mu) = \overline{\varphi_{c_2'}}\big(\sigma^{-1}\big(\overline{\varphi_{c_1'}}(\mu)\big)\big)\,,$$

c'est-à-dire d'appliquer successivement $\overline{\varphi_{c_1'}}$, σ^{-1} et $\overline{\varphi_{c_2'}}$.

Pour décrypter le message $C = 22$, calculer $\chi = \overline{2T^2+T+1}$, et appliquer successivement les différentes fonctions composant ψ^{-1} :

$$\overline{\varphi_{c_1'}}(\mu) = \overline{2T^2+1},\ \big(\sigma^{-1} \circ \overline{\varphi_{c_1'}}\big)(\mu) = \sigma^{-1}(\overline{2T^2+1}) = \overline{2T+1},$$
$$\big(\overline{\varphi_{c_2'}} \circ \sigma^{-1} \circ \overline{\varphi_{c_1'}}\big)(\mu) = \overline{\varphi_{c_2'}}(\overline{2T+1}) = \overline{T^2+2T+2}.$$

Montrer qu'on retrouve le message :

$$M = 2 + 2 \times 3 + 1 \times 3^2 = 17.$$

Cours N°11. Mardi le 13 janvier 2003

7 Sécurité du protocole et choix des paramètres

Dans cette section, nous décrivons des attaques sur le protocole. Les meilleurs choix de paramètres, au vu de ces attaques et des considérations de taille et de rapidité de calcul, seront discutés dans le dernier paragraphe. Nous utilisons les notations des sections précédentes.

7.1 Attaques sur les protocoles.

Complexité d'un attaque

La sécurité d'un protocole dépend d'un paramètre s (parfois, de plusieurs). Plus ce paramètre est grand, plus le protocole est considéré comme sûr, mais aussi, *a contrario*, plus le protocole nécessite en général de temps de calcul ou de stockage mémoire. Pour le protocole RSA, ce paramètre s est la taille (en bits) de l'entier N, pour les protocoles ElGamal, ce paramètre est le plus petit nombre premier divisant l'ordre du groupe G. Pour un algorithme d'attaque sur un protocole, notons $T(s)$ la fonction qui rend le nombre maximal de calculs nécessaires pour "casser" le protocole en fonction de s. On mesure l'efficacité de l'attaque – en d'autre termes, sa *complexité* – en estimant comment cette fonction $T(s)$ varie quand le paramètre s augmente. On distingue essentiellement trois types de complexité :

- complexité *polynômiale* : quand le paramètre s double, la nouvelle valeur $T(2s)$ reste **inférieure** à $C \times T(s)$ où $C \geq 1$ est une constante indépendante de s. C'est le cas le plus favorable. Par exemple, si $T(s) = s^5 + s^4 \log(s)$, alors $T(2s) < 64\, T(s)$ pour tout $s \geq 1$, et donc la complexité est polynômiale.
- complexité *exponentielle* : quand le paramètre s double, la nouvelle valeur $T(2s)$ devient **supérieure** à $T(s)^\alpha$ où $\alpha > 1$ est une constante indépendante de s. C'est le cas le plus défavorable. Par exemple, si $T(s) = 3^s - s^{10}$, alors on a $T(2s) > T(s)^{1,8}$ si $s \geq 32$.
- complexité *sous-exponentielle* : c'est le cas intermédiaire. Il n'existe pas de constante C et α telles que les conditions énoncées ci-dessus soient vérifiées. Par exemple, si $T(s) = \exp\{\sqrt{\log(s)}\}$, alors la complexité croît plus vite que n'importe quelle complexité polynômiale, mais moins vite cependant qu'une complexité exponentielle.

Tout protocole admettant une attaque de complexité polynômiale ne présente aucune garantie de sécurité et ne doit pas être utilisé. L'existence d'une attaque sous-exponentielle ne met pas en cause la sécurité du protocole mais oblige à augmenter le paramètre s, ce qui rend le protocole moins efficace.

Les protocoles mentionnés décrits dans la section précédente ont été longuement étudiés et sont standardisés (ex. IEEE-P1363, ANSI X9.62, etc). Il y a une recherche active sur ces différents problèmes. Il existe des attaques sous-exponentielles sur le protocole RSA et le protocole ElGamal sur le groupe $\mathbb{F}_p^\times$. Pour le protocole ElGamal sur le groupe $E(\mathbb{F}_p)$, plus récent, il n'existe pas à l'heure actuelle d'attaque sous-exponentielle.

7.2 Attaque par calcul du cycle.

Définissons une suite d'éléments de B de la manière suivante :

$$\begin{aligned} \chi_0 &= \chi, \\ \chi_{i+1} &= \psi(\chi_i) \quad \text{pour } i \geq 0. \end{aligned}$$

Puisque l'ensemble B est fini, il existe deux indices i_0 et i_1 tels que $i_0 \neq i_1$ et $\chi_{i_0} = \chi_{i_1}$. En fait, puisque ψ est une bijection, on peut montrer que la plus petite valeur possible pour i_0 est $i_0 = 0$. Mais, on a alors

$$\chi = \chi_{i_1} = \psi(\chi_{i_1 - 1})$$

et donc $\chi_{i_1-1} = \psi^{-1}(\chi) = \mu$. Ainsi, on retrouve le message décodé. Des arguments standards montrent que i_1 est de la taille de la racine carrée du cardinal de B. Il faut donc que ce cardinal soit assez grand, on prend

$$\#B = p^d > 10^{40},$$

ainsi il faut calculer environ 10^{20} termes, soit un calcul d'environ 10^8 années, de la suite (χ_i) pour casser le message codé. Il est à noter que cette restriction englobe celle déduite de l'attaque précédente.

7.3 Attaque par factorisation.

Puisque $\chi = \psi(\mu)$, l'élément μ est une racine du polynôme $\psi(z) - \chi$. De plus, en tant qu'élément de B, μ est aussi racine de $z^{p^d} - z$. Ainsi $z - \mu$ est un facteur du PGCD de $\psi(z) - \chi$ et $z^{p^d} - z$. En fait, $\psi(z) - \chi$ n'a que des racines simples, puisque $\psi(z)$ définit une bijection, et donc on montre facilement que :

$$\mathrm{PGCD}\Big(\psi(z) - \chi, z^{p^d} - z\Big) = z - \mu.$$

Ainsi, le calcul de ce PGCD permet de décoder le message. La première étape dans ce calcul est d'obtenir le reste $R(z)$ de la division euclidienne de $z^{p^d} - z$ par $\psi(z) - \chi$, c'est un calcul rapide de l'ordre de $d \log p$ opérations. Puis, il faut calculer le PGCD entre deux polynômes arbitraires $R(z)$ et $\psi(z) - \chi$, le nombre d'opérations de ce calcul est de la taille de l^2 où l est le maximum entre $\deg(\psi(z) - \chi)$ et $\deg(R(z))$. On impose que les deux polynômes c_1 et c_2 n'ont aucun coefficient nul. Dans ce cas, il y a une très grande probabilité que le degré de $\psi(z) - \chi$ soit $\geq p^{d-1}$. On choisit p et d tels que :

$$p^{d-1} > 10^{10},$$

ainsi le nombre d'opérations pour casser le code par cette méthode est comparable à celui de la méthode précédente, environ 10^{20} opérations, soit à peu près 10^8 années.

7.4 Attaque par énumération.

Un dernière attaque possible est de considérer l'ensemble de toutes les clés (c_1, c_2, δ) possibles. Pour chaque triplé, on calcule $\tilde{\psi}(\chi)$ où $\tilde{\psi}$ est la fonction correspondante, et on regarde si $\tilde{\psi}(\chi) = \psi(\chi)$. Si c'est le cas, alors on connaît la clé secrète, on peut donc en déduire $\mu = \psi^{-1}(\chi)$ et décoder le message. Le nombre de choix possible pour δ est p^d, pour c_1 et c_2, le nombre de choix possibles est aussi de l'ordre de p^d si p est grand devant d (le nombre de polynômes non inversibles modulo f_φ et avec au moins un coefficient nul est alors négligeable). Le nombre de clés à tester est donc de l'ordre de p^{3d}. Afin de contrer cette attaque, on choisit p et d tels que

$$p^{3d} \geq 10^{20}.$$

Alors, il faut, environ 10^{15} années pour casser le protocole par cette attaque.

7.5 Choix des paramètres.

Les considérations données ci-dessus montrent que l'on doit prendre p très grand par rapport à d. Cependant, afin d'optimiser l'efficacité des calculs, on veut que $p < 2^{32}$ afin que les entiers modulo p entrent dans un `long` sur un ordinateur 32 bits. La taille du polynôme $\psi(z)$ augmente avec l'exposant e, donc e doit être petit. D'un autre côté, e doit être premier avec $p^d - 1$, donc e est impair. Des choix raisonnables sont $e = 5$ ou $e = 7$.

Finalement, afin de pouvoir utiliser ce protocole pour crypter des clés AES, il faut que $p^d > 2^{160} \simeq 1,46 \cdot 10^{48}$.

Il faut évidemment rajouter les restrictions données par les attaques décrites ci-dessus.

Nous faisons un résumé des restrictions sur les paramètres :

– p est un grand nombre premier plus petit que 2^{32},

– d est un entier tel que $p^d \geq 2^{160}$,

– f est un polynôme de $\mathbb{F}_p[T]$ irréductible de degré d,

– e est petit et premier avec $p^d - 1$,

– φ est le module de Carlitz,

– c_1 et c_2 sont deux polynômes de $\mathbb{F}_p[T]$ de degré $d-1$, premiers avec f_φ, et sans coefficients nuls,

– δ est un élément de B.

Notons que les inégalités exigées pour contrer les attaques énoncées ci-dessus sont satisfaites avec ces choix.

Pour conclure, nous donnons un exemple explicite de choix de paramètres :

– $p = 1073741477$ ($p \simeq 2^{30}$),
– $d = 6$ ($p^d \simeq 2^{180}$),
– $f = T^5 + 13775595T^4 + 788683423T^3 + 305120033T^2 + 585880735T + 686097596$,
– $e = 5$,
– $\varphi(T) = \tau + T$,
– $c_1 = 437605822T^5 + 392755332T^4 + 925212769T^3 + 890100049T^2 + 541320556T + 287847229$,

  $c_2 = 246570738T^5 + 496274932T^4 + 883670503T^3 + 909401730T^2 + 64842034T + 732002645$,

– $\delta = \overline{842509909T^5 + 193124111T^4 + 551953889T^3 + 843139803T^2 + }$

  $\overline{188647249T + 872485075.}$

Avec ces choix, $\psi(z)$ est un polynôme avec 235 termes et le stockage des données de cryptage nécessite environ 26000 caractères (28k). Sur un Pentium 700MHz, tournant sous Linux, une implémentation de ce protocole en `C++` avec la librairie NTL (voir [Shou]) donne un temps de codage de l'ordre de un centième de seconde. Le temps de décodage est négligeable.

8 Attaques sur les cryptosystèmes et bases de Groebner

(Vincent Despiegel, mémoire de DEA)

8.1 Problèmes de l'inversion et du logarithme discret sur les modules de Drinfeld

La cryptographie est l'étude des méthodes d'envoi de message de manière déguisée afin que seuls les destinataires autorisés puissent déchiffrer et lire ce dernier. Le principe de la cryptographie à clé publique consiste à rendre publique la fonction de cryptage afin que toute personne puisse l'utiliser. Cependant, la réciproque est gardée secrète et seul le destinataire peut déchiffrer le message codé. L'objectif, pour rendre possible de tels protocoles est donc de trouver des fonctions f telles que la connaissance de celles ci ne donnent aucune information (ou suffisament peu) sur leurs inverses f^{-1}.

De nombreux problèmes mathématiques permettent de construire de telles fonctions à partir de paramètres secrets permettant ainsi à la personne connaissant ces paramètres de calculer l'inverse.

Ainsi, le protocole RSA utilise la difficulté à factoriser un nombre composé. En effet, on rend publique $n := p*q$ où p et q sont premiers et de grandes tailles et e n'ayant aucun facteur commun avec $(p-1)(q-1)$. On a alors $f(x) := x^e$ la fonction de cryptage. Pour décrypter le message, il suffit de calculer d tel que $d \equiv e^{-1}[\phi(n)]$ (vu que $f^{-1} := x^d$). Cela nécéssite la connaîssance des paramètres secrets. En effet, $\phi(n) := (p-1)(q-1)$ ne peut être calculé aisément à partir de pq sans la connaissance de p et q.

De même, à l'aide du protocole ElGamal, il est possible d'utiliser la structure de groupe de $E_{\mathbb{F}_p}$, une courbe elliptique sur $\mathbb{F}_p$ pour créer une autre fonction de cryptage à clé publique. Celui ci repose sur la difficulté à calculer le logarithme discret d'un élément d'un groupe multiplicatif. Etant donné que les courbes elliptiques peuvent être muni d'une structure de groupe et qu'elle nous fournissent un grand nombre de groupe finis en les regardant sur des corps finis, il est logique de chercher à les utiliser dans le cadre du protocole El Gamal.

L'objectif de ce rapport est d'étudier un système de cryptage sur les modules de Drinfeld. Ceux ci présentent de nombreuses similarités avec les courbes elliptiques et il est donc logique de chercher à imiter les protocoles de cryptage déjà existant sur cette famille de courbes. Cependant, il s'avère que le problème du logarithme discret, insoluble sur les courbes elliptiques en temps raisonnable peut être résolu en temps polynomial sur les modules de Drinfeld. T. Scanlon l'a prouvé dans son article : public key cryptosystems based on Drinfeld modules are insecure. Il est donc nécéssaire d'envisager une autre approche.

Une fonction à trappe à sens unique sur les modules de Drinfeld a été construite par F. Leprevost, A. Panchishkin, X. Roblot et R. Gillard. Ce protocole de cryptage présente de nombreuses similitudes avec le système HFE, reposant sur la difficulté de résoudre en temps raisonnable un système de polynômes (Le schéma HFE ("Hidden Field Equations") par J.Patarin est un protocole de cryptographie se basant sur la difficulté à résoudre un système d'équation algébrique, voir Section 9). Les attaques les plus prometteuses récemment dans ce domaine sont dues à J. C. Faugère. En effet, ses améliorations dans l'algorithme de calcul des bases de Groebner on accélerer considérablement la résolution de tels systèmes. Nous allons donc étudier spécifiquement les bases de Groebner et voir de quelle manière il est possible d'utiliser celles ci dans le cadre d'attaques sur le protocole de cryptage sur les modules de Drinfeld.

Dans cette partie, il s'agit de montrer que l'on ne peut se contenter d'imiter des protocoles de cryptographie déjà existant aux modules de Drinfeld. En effet, les deux problèmes principaux servant de base à de nombreux algorithme de cryptage (ie : problème d'inversion et problème du logarithme discret) peuvent être résolu en temps polynomial sur les modules de Drinfeld.

Avant tout, definissons les objets sur lesquels nous travaillerons :

Définition 8.1.1 *Un module de Drinfeld sur $\mathbb{F}_p[t]$ est un homomorphisme d'anneau $\phi : \mathbb{F}_p[t] \to \mathcal{K}\{F\}$ tel que $deg(\phi(t)) > 0$*

On peut associer à F le Frobenius de $\mathcal{K}$ dans $\mathcal{K}$ qui à x associe x^p où p est la caractéristique de $\mathcal{K}$ et à tout élément a de $\mathcal{K}$ l'application $x \to ax$. On peut donc associer à tout élément de $\mathcal{K}\{F\}$ un unique homomorphisme de $\mathcal{K}$ dans $\mathcal{K}$. Ainsi :

Définition 8.1.2 *Nous noterons l'homomorphisme de $\mathcal{K}$ dans $\mathcal{K}$ associé à $\phi(a)$ pour $a \in \mathbb{F}_p[t]$ par*

$$\iota \circ \phi(a)$$

Il est important de noter que nous ne choisissons pas la définition la plus générale des modules de Drinfeld. Cependant, il s'agit de ceux que nous utiliserons par la suite dans le cadre de notre système de cryptage. Les différentes propositions qui suivent peuvent très bien être prouvées dans un cadre général. Pour cela, on peut se référer à l'article de T. Scanlon.

Enonçons maintenant à quoi correspondent les problèmes d'inversion et de logarithme discret sur les modules de Drinfeld.

Définition 8.1.3 *Par problème de logarithme discret sur les modules de Drinfeld, on entend : soit un corps fini $\mathcal{K}$ de caracteristique p, un module de Drinfeld ϕ et des éléments $x, y \in \mathcal{K}$, trouver $a \in \mathbb{F}_p[t]$ tel que $\phi(a)(x) = y$.*

Définition 8.1.4 *Par problème d'inversion pour les modules de Drinfeld, on entend : soit un corps fini $\mathcal{K}$ de caracteristique p, un module de Drinfeld ϕ et $a \in \mathbb{F}_p[t]$ tel que $\phi(a) : \mathcal{K} \to \mathcal{K}$ soit une bijection, trouver $b \in \mathbb{F}_p[t]$ tel que $\phi(b) : \mathcal{K} \to \mathcal{K}$ soit l'inverse de $\phi(a)$*

Si l'on prouve que ces problèmes peuvent être résolu en temps polynomial, on prouvera que les équivalents sur les modules de Drinfeld des protocoles standards existant sur les corps de nombres et sur les groupes de points sur les groupes elliptiques ne sont pas sûrs. Voici à quoi ressembleraient les analogues de ces protocoles :

Définition 8.1.5 *Protocole de Diffie Hellman appliqué aux modules de Drinfeld. Soit p premier et q une puissance de p. Soit $\mathcal{K} := \mathbb{F}_q$. Soit ϕ un module de Drinfeld et soit un élément $\xi \in \mathcal{K}$. Ces éléments font parties du domaine publique. A et B choisissent chacun a (resp b) dans $\mathbb{F}_p[t]$. A transmet $\phi(a)(\xi)$ à B et B transmet $\phi(b)(\xi)$ à A. Alors, leur clé privée commune est $\phi(b)(\phi(a)(\xi)) = \phi(b * a)(\xi) = \phi(a * b)(\xi) = \phi(a)(\phi(b)(\xi))$.*

Définition 8.1.6 *Protocole El Gamal appliqué aux modules de Drinfeld. Soit p premier et soit q une puissance de p. $\mathcal{K} := \mathbb{F}_q$, ϕ un module de Drinfeld, ξ un élément de $\mathcal{K}$, publique. A choisit a dans $\mathbb{F}_p[t]$. Il rend publique $\phi(a)(\xi)$. Si B souhaite lui transmettre un message crypté de P, il choisit au hasard un élément $k \in \mathbb{F}_p[t]$ et lui envoie la paire $(\phi(k)(\xi), P + \phi(k)(\phi(a)(\xi))$. De cette manière, A, connaissant a peut retrouver P de la manière suivante :*

$$P + \phi(k)(\phi(a)(\xi)) - \phi(a)(\phi(k)(\xi)) := P + \phi(ka)(\xi) - \phi(ak)(\xi) = P$$

Nous allons maintenant présenter les attaques possibles faces à ces différents problèmes. Pour attaquer ces cryptosystèmes, observons dans un premier temps que l'anneau des fonctions induit par un module de Drinfeld est égal à un anneau de fonctions linéaires, correctement interprété. Tout consiste à regarder le corps $\mathcal{K}$ comme un espace vectoriel sur un corps fini plus petit et ensuite à effectuer quelques opérations matricielles. Pour cela, nous devons fixer une base pour $\mathcal{K}$ et exprimer les éléments de $\mathcal{K}$ en fonction de cette base. Même si dans la pratique, $\mathcal{K}$ est déjà exprimé de cette manière là, prouvons que si cela n'est pas le cas, il est très rapide de s'y ramener en temps polynomial.

Proposition 8.1.7 *Il existe un algorithme en temps polynomial qui à partir d'un corps fini $\mathcal{K}$ de caractéristique p produit une base de $\mathcal{K}$ sur $\mathbb{F}_p$ et un algorithme en temps polynomial permettant d'exprimer n'importe quel élément de $\mathcal{K}$ en fonction de cette base.*

Preuve.
Soit $d := [\mathcal{K} : \mathbb{F}_p] = log_p(|\mathcal{K}|)$. Pour cela on choisit $B := (e_1, ..., e_d) \in \mathcal{K}^d$ au hasard. B est alors un base avec probabilité $\prod_{i=0}^{d-1}(1-p^{-i})$ En répétant cette opération $-log_p\epsilon$ fois, on trouve au moins une base avec probabilité $1-\epsilon$, le problème étant de repérer si un d-uplet est ou non une base en temps convenable.

Pour cela, nous définissons des éléments $b_i \in \mathcal{K}$ et des opérateurs additifs $\phi_i : \mathcal{K} \to \mathcal{K}$ de la manière suivante : $b_1 := e_1$ et $\phi_1 := id_{\mathcal{K}}$. On construit alors ϕ_{i+1} et b_{i+1} en fonction de ϕ_i et b_i comme suit.

$$\phi_{i+1} := b_i^p(F-1)b_i^{-1}\phi_i$$

$$b_{i+1} := \phi_{i+1}(e_{i+1})$$

Ici F correspond bien entendu au Froebenius. Prouvons par récurrence que B est une base si et seulement si tous les b_i sont différents de zéro. Pour cela, nous allons voir par récurrence que $ker(\phi_i) =< e_1, ...e_{i-1} >$. Ceci est vérifié pour ϕ_1. On a d'abord $ker(F-1) = \mathcal{K}$. On a donc par récurrence $dim(ker(\phi_i)) \leq i-1$. De plus, en utilisant l'hypothèse de récurrence, on a $< e_1, ..., e_{i-1} > \subset ker(\phi_{i+1})$. Enfin il reste donc à prouver que $e_i \in ker(\phi_{i+1})$. Or $\phi_{i+1}(e_i) = b_i^p(F-1)b_i^{-1}\phi_i(e_i) = b_i^p(F-1)b_i^{-1}b_i = 0$ On a donc bien $ker(\phi_i) =< e_1, ...e_{i-1} >$ et donc B est une base si et seulement si tous les b_i sont non nuls.

Ensuite, il est facile à l'aide des ϕ_i d'exprimer les coordonnées de n'importe quel élément x dans la base $(e_i)_{i=1}^d$. Pour cela, on les construit de manière descendante : $x_i = b_i^{-1}\phi_i(x - \sum_{j>i} x_j e_j)$. On prouve aisément que on a alors $x = \sum_{i=1}^d x_i e_i$. En comptant le nombre d'additions et multiplications nécéssaires pour effectuer cette opération, on obtient un nombre en $O(log(p)d^3)$. (En effet, pour calculer l'inverse d'un élément, on peut utiliser l'égalité $b^{-1} = b^{p^d-1}$.)

Après avoir prouvé que trouver une base et exprimer tout élément de $\mathcal{K}$ dans celle ci ne pose pas de problème, nous allons utiliser celle ci pour prouver la proposition suivante.

Proposition 8.1.8 *Il existe un algorithme en temps polynomial pour résoudre le problème d'inversion pour les modules de Drinfeld.*
Plus précisément, il existe des nombres réels C et α et un algorithme qui à partir de p premier, un corps fini $\mathcal{K}$ de caracteristique p, un module de Drinfeld $\phi : \mathbb{F}_p[t] \to \mathcal{K}\{F\}$ et $a \in \mathbb{F}_p[t]$ tel que $\phi(a)$ est une bijection de $\mathcal{K}$ trouve $b \in \mathbb{F}_p[t]$ tel que $\phi(b)$ est son inverse le tout en moins de $C(log_p|\mathcal{K}|)^\alpha$ opérations dans $\mathbb{F}_p$.

Preuve.
$\mathbb{F}_p[t]$ peut être engendré par t et son corps des constantes $\mathbb{F}_p$. Notons comme précédement, $\mathbb{A} := \iota \circ \phi(\mathbb{F}_p[t]) \subseteq Hom(\mathcal{K}, +)$. Les éléments de $\mathbb{A}$ sont des homomorphismes additifs mais ont peu de chance d'être $\mathcal{K}$ linéaires. Ces homomorphismes sont néanmoins $\mathbb{F}_p$ linéaires. Nous allons donc utiliser ce fait pour se ramener à du calcul matriciel.

D'après la proposition précédente, il est possible de trouver une base Γ de $\mathcal{K}$ sur $\mathbb{F}_p$. Cela nous permet ainsi d'identifier $Hom(\mathcal{K})$ avec l'anneau des matrices $M_m(\mathbb{F}_p)$ où m est la dimension de $\mathcal{K}$ sur $\mathbb{F}_p$. Grace à cela, on identifie $\mathbb{A}$ avec un sous anneau de l'anneau des matrices $m \times m$ sur $\mathbb{F}_p$. Soit $a \in \mathbb{F}_p[t]$ tel que $\iota \circ \phi(a)$ soit inversible, on peut trouver l'inverse de $\iota \circ \phi(a)$ en inversant simplement la matrice correspondante. On obtient alors $\beta \in \mathbb{A}$ cet inverse. Sans prendre en compte d'autres informations sur a, cette inversion ne requiert au pire que $O(m^\omega)$ operations dans $\mathbb{F}_p$ où ω est la constante telle que le problème de multiplication de deux matrices quelconques $m \times m$ sur un corps $\mathbb{L}$ soit résolu en $O(m^\omega)$ operations d'anneau dans ! $\mathbb{L}$. Comme $\mathbb{A}$ est une sous algèbre commutative de $M_m(\mathbb{F}_p)$ on a nécéssairement $dim_{\mathbb{F}_p}(\mathbb{A}) \leq m$. Dans un premier temps, on calcule l'ensemble des matrices S suivant

$$S := \{\iota \circ \phi(t^i) : 0 \leq i < m\}$$

En supposant que nous connaissons déjà $\iota \circ \phi(t)$ sous forme matricielle dans la base Γ, tout ceci requiert m multiplications matricielles et peut être accompli en $O(m^{1+\omega})$ operations dans $\mathbb{F}_p$. On peut extraire de

S une base B de $\mathbb{A}$ en $O(m^{\omega+1})$ opérations dans $\mathbb{F}_p$ en utilisant l'algorithme de la proposition précédente. De cette manière, nous avons trouvé un entier l tel que $\{\phi(t^i) : 0 \leq i \leq l\}$ soit une base de $\mathbb{A}$ sur $\mathbb{F}_p$.

Comme nous l'avons vu précédement, nous avons une base Γ de $\mathcal{K}$. A partir de celle ci, nous obtenons une base canonique Γ' de $Hom(\mathcal{K}, +)$. Comme β appartient à $\mathbb{A}$, il peut s'exprimer en fonction des $\phi(t^i)$ avec $0 \leq i \leq l$. Pour cela, il suffit d'exhiber la matrice $C \in M_{(|B|+1)\times m^2}$ telle que

$$C\Gamma' = (\beta, (\phi(t^i))_{0\leq i\leq l}$$

Pour trouver β comme combinaison linéaire de tels éléments, il suffit de trouver le noyau de C ce qui se fait en $O(m^4)$. Ainsi, nous obtenons l'expression suivante avec $\alpha_i \in \mathbb{F}_p$:

$$\beta = \sum_{0\leq i\leq l} \alpha_i \phi(t^i)$$

En conséquence, on peut trouver des constantes C et α telles que trouver $b \in \mathbb{F}_p[t]$ tel que $\phi(b)$ soit l'inverse de $\phi(a)$ nécessite moins de $C * (log_p(|\mathcal{K}|))^\alpha$ opérations dans $\mathbb{F}_p$.

Les techniques utilisées pour prouver la proposition précédente peuvent être étendues au problème du logarithme discret dans les modules de Drinfeld. La proposition suivante en découle donc :

Proposition 8.1.9 *Il existe un algorithme en temps polynomial pour résoudre le problème du logarithme discret pour les modules de Drinfeld.*
Plus précisément, il existe des constantes C' et α' et un algorithme qui à partir de p premier, d'un corps fini $\mathcal{K}$ de caracteristique p un module de Drinfeld $\phi : \mathbb{F}_p[t] \to \mathcal{K}\{F\}$ et des éléments ξ et y de $\mathcal{K}$ calcule $a \in \mathbb{F}_p[t]$ tel que $\phi(a)(\xi) = y$, en utilisant moins de $C'(log_p|\mathcal{K}|)^{\alpha'}$ opérations dans $\mathbb{F}_p$

Preuve.
Comme il est précisé plus haut, nous allons utiliser le même type de méthode que celles utilisées pour prouver la proposition précédente.

Premièrement, soit les définitions suivantes. $M := \phi(\mathbb{F}_p[t]).\xi$ le $\mathbb{F}_p[t]$ -module engendré par ξ. Soit $\mathbb{A} := \iota \circ \phi(\mathbb{F}_p[t]) \subseteq Hom(\mathcal{K}, +)$ Soit $m := dim_{\mathbb{F}_p}(\mathcal{K})$. $\mathbb{F}_p[t]$ est engendré par t et par son corps des constantes $\mathbb{F}_p$.

Comme précédement, on définit l'ensemble $\{\phi(t^i) : 0 \leq i < m\}$ et on le réduit à une base B de M. Comme précédemment, ceci peut être accompli en $O(m^{1+\omega})$ opérations dans $\mathbb{F}_p$.

Soit $y \in M$, c'est à dire qu'il existe $a \in A$ tel que $y = \phi(a)(\xi)$. Il ne nous reste donc qu'à exprimer cet élément dans la base précédemment exhibée comme on l'a fait pour prouver la proposition précédente. On obtient alors en utilisant les notations de la preuve précédente :

$$y = \sum_{0\leq i\leq l} a_i \phi(t^i)(\xi)$$

Cela nous permet d'obtenir $a = \sum_{0\leq i\leq l} a_i t^i$ Comme précédemment, cet élément peut être calculé en un temps en $O(log_p(|\mathcal{K}|)^4)$. On peut donc trouver des constantes permettant de satisfaire la conclusion de la proposition, c'est à dire C' et α' tel que a puisse être trouvé en moins de $C'(log_p|\mathcal{K}|)^{\alpha'}$ opérations dans $\mathbb{F}_p$.

Ainsi, nous venons de prouver qu'aucun cryptosystème à clé publique basé sur l'irrésolubilité du problème du logarithme discret pour les modules de Drinfeld (comme Diffie Hellman ou ElGamal adapté aux modules de Drinfeld) n'est sûr.

8.2 Protocole de cryptage sur les modules de Drinfeld

Nous allons présenter dans un premier temps les objets avec lesquels nous allons travailler. Voici une définition précise des modules de Drinfeld sur lesquels nous allons implémenter notre protocole :

Définition 8.2.1 *Un module de Drinfeld est un morphisme ϕ de $\mathbb{F}_p[t]$ dans $\mathbb{F}_p[t]\{F\}$ de $\mathbb{F}_p$ algèbre tel que $\phi(t)$ soit un polynôme en F non constant et de terme constant égal à t.*

Un module de Drinfeld étant un morphisme, il en découle nécéssairement que seule la valeur de $\phi(t)$ le determine totalement. En effet, si $a := \sum a_i t^i$ on obtient :

$$\phi(a) = \sum a_i (\phi(t))^i$$

De même que dans la partie précédente, on peut associer à F le Frobenius (ie : $z \to z^p$) et à $a \in \mathbb{F}_p[t]$ l'application $z \to z^p$. On a donc la même définition que précédemment.

Définition 8.2.2 *A tout élément de $a = \sum_i a_i F^i \in \mathbb{F}_p[t]\{F\}$ on peut associer un unique homomorphisme de $\mathbb{F}_p[t]$ dans $\mathbb{F}_p[t]$ par l'application ι présenté dans la partie précédente :*

$$\sum a_i F^i \xrightarrow{\iota} (z \to \sum a_i z^{p^i})$$

Nous noterons alors $\iota \circ \phi(a)$ par ϕ_a pour simplifier les notations.

Le système de cryptographie sur les modules de Drinfeld que nous allons étudier code des éléments de $\mathbb{F}_{p^d}$ Nous allons donc étudier les corps à $\mathbb{F}_{p^d}$ éléments.
Si on choisit un polynôme irréductible de $\mathbb{F}_p[t]$, de degrès d on a bien entendu

$$B := \mathbb{F}_p[t]/(f(t)) \cong \mathbb{F}_{p^d}$$

Ce corps peut être aisément muni d'une structure canonique de $\mathbb{F}_p[t]$ module par passage au quotient. Cependant une autre structure de $\mathbb{F}_p[t]$ module peut elle aussi être apposée à l'aide des morphismes additifs ϕ_a. En effet, ces derniers sont compatibles avec le passage au quotient vu que $\phi_a(s(t)f(t)) \equiv 0[f(t)]$ pour tout a et s. Appelons $\overline{\phi_a}$ ces morphismes passés au quotient. On peut ainsi munir B d'une autre structure de $\mathbb{F}_p[t]$ de la manière suivante :

$$a \times_\phi \beta = \overline{\phi_a}(\beta)$$

Ainsi, si on note B_ϕ, B vu comme $\mathbb{F}_p[t]$ module muni de cette structure, il existe un unique polynôme unitaire de degrès d tel que :

$$B_\phi \cong \mathbb{F}_p[t]/(f_\phi)$$

Ce polinôme présente de nombreuses propriétés qui justifient son intérêt dans l'étude des $\overline{\phi_a}$. Ainsi, on dispose de la proposition suivante :

Proposition 8.2.3 *$\overline{\phi_a} = \overline{\phi_b}$ si et seulement si $a \equiv b[f_\phi]$.*
$\overline{\phi_a}$ est bijective de B dans B si et seulement si a est premier à f_ϕ. Alors son inverse est ϕ_b avec $ab \equiv 1[f_\phi]$.

L'idée principale pour construire la fonction à trappe ψ est de jouer avec ces deux structures sur B et de cette manière là, en les melant d'empêcher de retrouver à partir de ψ les différents éléments constituant la bijection. Ainsi, l'idée de F. Leprevost, A. Panchishkin, R. Gillard et X. Roblot est de construire une clé publique de la forme suivante :

$$\psi(z) := \overline{\phi_{c_1}} \circ \sigma \circ \overline{\phi_{c_2}}(z)$$

où σ est une fonction bijective facile à inverser de la forme $\sigma(z) := z^e + \delta$ (avec e premier avec p et avec $p^d - 1$ et δ un élément de B), et où c_1 et c_2 sont premiers avec f_ϕ de sorte que nos deux fonctions ϕ_{c_1} et ϕ_{c_2} soient inversibles.

Comme nous l'avons vu précédemment, ces deux fonctions seront facile à inverser : il suffira de trouver c_i' tels que $c_i c_i' \equiv 1[f_\phi]$ pour $i = 1$ et $i = 2$. On obtiendra alors :

$$\psi^{-1}(z) := \overline{\phi_{c_2'}} \circ \sigma^{-1} \circ \overline{\phi_{c_1'}}(z)$$

On a bien entendu $\sigma^{-1}(z) := (z - \delta)^f$ avec $ef \equiv 1[p^d - 1]$.

En résumé, on rend publique le polynôme ψ et on garde privés nos quatres paramètres (c_1, c_2, δ, e) qui nous permettent aisément de calculer ψ^{-1}. Il est à noter qu'en fait, le paramètre e n'est pas véritablement secret. D'une part, il peut facilement être retrouvé grace au nombre de termes intervenant dans le polynôme ψ (ie de l'ordre de $\binom{d+e-1}{d-1}$) et surtout, d'autre part, pour travailler avec des polynômes de taille raisonnable, on doit nécéssairement se restreindre à e très petit de l'ordre de 5 ou 7. Ceci présente un faiblesse de taille. En effet, la fonction intermédiare se trouve quasiment dévoilée. De plus nous allons maintenant voir que le paramètre δ peut facilement être supprimé.

8.3 Suppression du paramètre δ

Comme nous l'avons vu, nous calculons successivement ϕ_{c_2}, $\sigma_\delta \circ \phi_{c_2}$ pour finalement obtenir par composition par ϕ_{c_1} la fonction de cryptage publique ψ. Cela signifie que l'on a :

$$\psi = \phi_{c_1}((\phi_{c_2})^e + \delta)$$

Or, on a nécéssairement $\phi_a(0) = 0$ pour tout a. En effet, notre polyôme ϕ_a est la combinaison linéaire de polynôme sans terme constant. En conséquence, si l'on calcule $\psi(0)$ On obtient :

$$\psi(0) = \phi_{c_1}((\phi_{c_2})^e + \delta)(0) = \phi_{c_1}((\phi_{c_2}(0))^e + \delta) = \phi_{c_1}(\delta)$$

De plus, nos applications ϕ_a sont linéaires. En effet, les multiplications par des constantes et le Frobenius sont des applications linéaires. De plus, ϕ_a s'écrit comme somme de compositions de telles fonctions et est donc elle aussi linéaire, quel que soit a. En conséquence, si l'on retire $\psi(0)$ à ψ, on obtient :

$$\psi(z) - \psi(0) = \phi_{c_1}((\phi_{c_2}(z))^e + \delta) - \phi_{c_1}(\delta) = \phi_{c_1}((\phi_{c_2}(z))^e)$$

Ainsi, nous avons fait disparaître le paramètre δ de notre fonction. Il suffit donc de trouver l'inverse de cette nouvelle fonction et d'effectuer une translation par $-\phi_{c_1}(\delta)$ pour obtenir l'inverse de ψ.

Ainsi, le paramètre ne rentre aucunement en ligne de compte dans la sécurité du protocole et on peut donc prendre $\delta = 0$ sans changer en rien la sécurité du protocole. Cependant, pour éviter cela, il est sans doute possible d'introduire le paramètre δ en amont. On a alors un polynôme/clé publique de la forme $\phi_{c_2} \circ z^7 \circ \phi_{c_1}(z + \delta)$. Dans ce cas, il ne pourra être supprimé aussi aisément et récupererai un paramètre supplémentaire.

8.4 Les bases de Groebner

HFE correspond à un algorithme de cryptage utilisant des polynômes de plusieurs variable sur des corps finis (dans sa version classique, il s'agit de $\mathbb{F}_2$ et $\mathbb{F}_{2^n}$) (Le schéma HFE ("Hidden Field Equations") par J.Patarin est un protocole de cryptographie se basant sur la difficulté à résoudre un système d'équation algébrique, voir Section 9). Pour casser ce protocole de cryptage, de nombreuses methodes furent utilisées. En particulier, dans leur article, Aviad Kipnis et Adi Shamir proposaient d'utiliser une méthode de relinéarisation. Cependant, l'un des types d'attaque les plus prometteurs consiste à calculer la base de Groebner de certains idéaux. En effet, assez recemment, de nombreuses accélérations/optimisations des algorithmes traditionnels tel que l'algorithme de Buchberger (en particulier de nouveaux algorithmes par Jean Charles Faugères tels que les algorithmes F_4 et F_5) rendent possible le calcul de certaines bases de Groebner, calcul qui parraissait informatiquement innaccessible auparavant.

Ceci présente de nombreux intérêts pour le problème considéré. En effet, le protocole de cryptage HFE présente de nombreuses similitudes avec le protocole de cryptage exposé plus haut (Le schéma HFE ("Hidden Field Equations") par J.Patarin est un protocole de cryptographie se basant sur la difficulté à résoudre un système d'équation algébrique, voir Section 9). Cela signifie que le calcul de base de Groebner constitue une possibilité d'attaquer ce protocole de cryptage. Nous allons dans un premier temps énoncer un certain nombre de définitions sur les bases de Groebner ainsi que les propriétés essentielles pour le problème considéré. Ensuite nous verrons de quelle manière cela peut être utilisé dans le cas du protocole HFE. Finalement, nous verrons une manière de l'appliquer au protocole de cryptage sur les modules de Drinfeld, tout en soulignant les différences entre HFE et MED, source de problèmes dûs en particulier à la grande taille de p.

8.5 Bases de Groebner : definition et propriétés

Supposons dans un premier temps que nous disposons d'un systèmes de polynômes en n variables $f_1, \cdots, f_m$. Nous souhaitons étudier leurs racines communes c'est à dire plus précisément les éléments $(x_1, \cdots, x_n)$ tels que

$$f_1(x_1, \cdots, x_n) = f_2(x_1, \cdots, x_n) = \cdots = f_m(x_1, \cdots, x_n) = 0$$

Appelons I l'idéal engendré par ces $f_1, \cdots, f_m$ (i.e. : $I := \langle f_1, \cdots, f_m \rangle$) et appelons $V_{\mathcal{K}}$ l'ensemble des solutions dans $\mathcal{K}$ de ce système de polynômes. Nous avons donc la variété algébrique suivante

$$V_{\mathcal{K}} := \{(z_1, \cdots, z_n) \in \mathcal{K} | f_i(z_1, \cdots, z_n) = 0 : i = 1..m\}$$

Nous devons aussi choisir un ordre entre les différents monomes en $x_1, \cdots, x_n$ determinant une base de Groebner spécifique. En effet, celle ci est assugétie au choix d'un ordre. Celui ci peut être l'ordre lexicographique (i.e. : $x_1^{\alpha_1} \cdots x_m^{\alpha_m} < x_1^{\beta_1} \cdots x_m^{\beta_m}$ pour l'ordre lexicographique ssi on peut trouver k tel que $\alpha_i = \beta_i$ pour tout $i < k$ et $\alpha_k < \beta_k$.) Il existe bien entendu d'autres ordres comme l'ordre DRL (ie : degree reverse lexicographical order) ou encore des ordres selon le degrès total ou le degrès total pondéré. Maintenant, definissons termes dominants et monômes dominants d'un polynôme pour cet ordre :

Définition 8.5.1 *Fixons un ordre sur les monomes de $\mathcal{K}[x_1, \cdots, x_m]$.*
$LM(f)$ correspond au monome de plus haut degrès pour cet ordre intervenant dans f avec un coefficient non nul.
$LT(f)$ correspond au terme de plus haut degrès pour cet ordre intervenant dans f avec un coefficient non nul.

Par exemple, pour le polynome $f := 2 * x^2 + xy + y^3$ on obtient pour l'ordre lexicographique $LM(f) = x^2$ et $LT(f) = 2x^2$

Nous disposons maintenant de toutes les definitions pour définir une base de Groebner :

Définition 8.5.2 *Soit G un ensemble fini d'éléments de I. G est un base de Groebner si et seulement si pour tout élément f de I, il existe un élément g de G tel que $LT(g)$ divise $LT(f)$.*

Cette définition peut aussi être reformulée de la manière suivante :

Définition 8.5.3 *Fixons un ordre, un sous ensemble $G := \{g_1, \cdots, g_m\}$ d'un idéal I est dit une base de Groebner si et seulement si*

$$LT(I) = \langle LT(g_1), \cdots, LT(g_m) \rangle$$

par exemple, soit $I := \langle x^2 + 1, xy \rangle$. Choisissons l'ordre lexicographique. On a alors $G := (x^2 + 1, xy)$ qui n'est pas une base de Groebner. En effet, y est un élément de I et G ne vérifie pas la condition nécéssaire la définition pour ce terme. Par contre, $G' = (x^2 + 1, y)$ en est une.

Supposons maintenant que nous souhaitions calculer l'ensemble $V_{\mathcal{K}}$ pour une corps $\mathcal{K}$ particulier. Pour résoudre ce système d'équations, il est possible d'utiliser les bases de Groebner.

Proposition 8.5.4 *La base de Groebner de l'idéal suivant dans* $\mathbb{F}_{p^d}[x_1, \cdots, x_n]$

$$\left\langle f_1, \cdots, f_m, x_1^{p^d} - x_1, \cdots, x_n^{p^d} - x_n \right\rangle$$

permet de déduire toutes les éléments de $V_{\mathbb{F}_{p^d}}$. *En particulier, on dispose des cas particuliers suivants :*

- $V_{\mathbb{F}_{p^d}} = \emptyset$ *si et seulement si* $G = \{1\}$
- $V_{\mathbb{F}_{p^d}}$ *possède un unique élément* $(a_1, \cdots, a_n)$ *si et seulement si* $G = \{(x_1 - a_1), \cdots, (x_n - a_n))\}$

Cela permet de faire jaillir tout l'intéret que présente le calcul de base de Groebner. En effet, comme nous le verrons plus tard, il existe de nombreux algorithmes permettant d'automatiser ce calcul. Cela signifie donc que si l'on en réduit la complexité et si l'on sait qu'un système de polynômes dans un corps $\mathcal{K}$ ne dispose que d'une unique racine, un simple lecture de la base de Groebner réduite calculée permet de connaître ce dit élément.

Définition 8.5.5 *Fixons un ordre sur les monomes. Soit* $F := \{f_1, \cdots, f_s\}$ *un ensemble fini de polynômes dans* $\mathcal{K}[x_1, \cdots, x_n]$. *Un polynôme* g *est réduit modulo* F *si aucun* $LM(f_i)$ *ne divise* $LM(g)$.

Par exemple, si $F := \{x^2 + y, xy, y^3\}$, nous avons $x^3 + xy$ qui n'est pas sous forme réduite. Par contre x l'est.
Remarquons que nous pouvons réduire un élément modulo F de manière à l'avoir sous forme réduite. Il est à noter que sans autres précisions sur l'ensemble F, un même élément peut avoir plusieurs formes réduites.
par exemple $x^2y + y^2 \equiv (x^2 + y)y \equiv 0$ qui est une forme réduite. De même $x^2y + y^2 \equiv (xy)y + y^2 \equiv y^2$ se trouve aussi sous forme réduite. Cependant, ces deux polynômes ne sont bien évidemment nullement égaux. Nous verrons par contre que dans le cas de base de Groebner il n'existe qu'une unique forme réduite.

Proposition 8.5.6 *Soit* $G := \{g_1, \cdots, g_s\}$ *une base de Groebner d'un idéal* I *de* $\mathcal{K}[x_1, \cdots, x_n]$ *et soit* f *un polynôme de* $\mathcal{K}[x_1, \cdots, x_n]$. *Alors, il existe un unique élément* $r \in \mathcal{K}[x_1, \cdots, x_n]$ *tel que*

- r *est completement réduit modulo* G
- *il existe un unique* g *dans* $\langle g_1, \cdots, g_s \rangle$ *tel que* $f = g + r$

Il est a remarquer qu'en appliquant un algorithme de division euclidienne classique, on n'exprime pas forcément g avec les même coéfficents en g_i. Cependant, quel que soit l'ordre des divisions par les g_i, le reste r reste identique. Par exemple, dans le cas d'une base de Groebner $G := \langle y - x^2, z - x^3 \rangle$ avec l'ordre lexicographique $z > y > x$, si l'on considère l'élément yz on a les deux possibilités suivantes.
Si on divise d'abord par $y - x^2$, on obtient $yz = z(y - x^2) + zx^2 = z(y - x^2) + x^2(z - x^3) + x^5$. On obtient $r = x^5$
Si par contre, on divise d'abord par $z - x^3$, on obtient alors $yz = y * (z - x^3) + yx^3 = y * (z - x^3) + x^3 * (y - x^2) + x^5)$. On obtient aussi un r identique. par contre, les coefficient en $y - x^2$ et $z - x^3$ ne sont nullement les même.

De cette manière là on obtient directement un corollaire

Corollaire 8.5.7 G *est une base de Groebner de* I *idéal de* $\mathcal{K}[x_1, \cdots, x_n]$. *Alors* f *appartient à* I *si et seulement si sa forme réduite modulo* G *est nulle.*

Cela permet de prouver aisément et de manière algorithmique l'appartenance d'un élément à I.

Enfin nous allons enfin définir le $S-$ polynôme de deux éléments f et g

Définition 8.5.8 *Soit un ordre entre les monomes fixé. Soit f et g deux éléments de $\mathcal{K}[x_1, \cdots, x_n]$ et soit $h := \text{ppcm}(LM(f), LM(g))$. $S(f, g)$ le $S-$ polynôme de f et g est le polynôme suivant*

$$S(f, g) := \frac{h}{LT(f)} * f - \frac{h}{LT(g)} * g$$

Il est bien entendu essentiel de remarquer que les termes

$$\frac{h}{LT(f)} \text{ et } \frac{h}{LT(g)}$$

sont en fait des monômes de par la définition de h.

8.6 L'algorithme de Buchberger

L'algorithme de Buchberger constitue l'algorithme classique de calcul de bases de Groebner. Historiquement, il s'agit du premier. De plus, toutes les améliorations (algorithmes F_4 et F_5 dus à J.-C. Faugère) se basent sur celui ci. Il s'agit simplement de mieux choisir les éléments choisis au hasard tout au long de l'agorithme de Buchberger pour réduire le calcul d'une base de Groebner à un problème d'algèbre linéaire. Nous allons donc présenter en détail cet algorithme.

Celui ci est avant tout basé sur la proposition suivante qui justifie les opérations accomplies tout au long de l'algorithme.

Proposition 8.6.1 *Soit $G := \{g_1, \cdots, g_s\}$ un sous ensemble de I idéal de $\mathcal{K}[x_1, \cdots, x_n]$ et soit un certain ordre sur les monomes de $\mathcal{K}[x_1, \cdots, x_n]$. Alors G est une base de Groebner si et seulement si pour tout couple g_i, g_j, $S(g_i, g_j)$ se réduit modulo G à 0.*

Comme nous le verrons ci dessous, il s'agit des seules opérations qui sont effectuées.

L'algorithme de Buchberger admet donc en entrée un ensemble $F := \{f_1, \cdots, f_m\}$ tel que $\langle f_1, \cdots, f_m \rangle = I$ l'idéal dont on veut calculer un base de Groebner. En sortie, on devra obtenir un ensemble $G := \{g_1, \cdots, g_t\}$ tel que G forme une base de Groebner. L'algorithme se déroule de la manière suivante.

- Nous initialisons G avec les éléments de F (ie : $F \to G$)
  Nous initialisons un ensemble de couple M (ie : $M := \{(f_i, f_j) : f_i, f_j \in G, i < j\}$)
- Tant que M est non vide, nous effectuons les opérations suivantes (ie : While $M \neq \emptyset$ do)
  Nous choisissons un couple $\{p, q\}$ de M que nous supprimons de l'ensemble M (ie : $M - \{p, q\} \to M$)
  Nous calculons $S(p, q)$ (ie : $S(p, q) \to S$)
  Nous calculons h le reste de $S(p, q)$ modulo G. (ie : $S(p, q)$ mod $G \to h$)
  A ce moment là, on a deux possibilités, soit $h = 0$. Dans ce cas, on ne fait rien et on passe au couple suivant dans M. Sinon, on ajoute h à G et et ajoute tous les couples (g, h) à M pour tout $g \in G$. Ensuite on choisit à nouveau un élément de M et on réitère l'opération. (ie : if $h \neq 0$ do $G \cup \{h\} \to G$, $M \cup \{(h, g), g \in G\} \to M$, end, end)

Il est important de remarquer qu'à première vu, l'algorithme peut boucler. En effet, à chaque boucle, on peut ajouter l nouveaux couples à M où l est la taille de G au rang précédent. Cependant, soit H_i l'ensemble des termes dominants de G une fois que le i ème h (noté h_i) est ajouté dans l'algorithme. D'après le procédé de construction, son coefficient dominant ne peut en aucun cas être divisible par le terme dominant d'un élément de F ou celui d'un h_j pour $j < i$ vu que nous avons effectué une division modulo G_{i-1}. Ainsi,les $\langle H_j \rangle$ forment une suite croissante d'idéaux. Nous allons utiliser le théorème de la base de Hilbert pour prouver que cette suite est nécessairement stationaire à un certain rang n.

Théorème 8.6.2 *Tout idéal de $\mathcal{K}[x_1, \cdots, x_n]$ est engendré par un nombre fini d'éléments.*

Une conséquence directe de ce théorème est que toute suite croissante d'idéaux de $\mathcal{K}[x_1, \cdots, x_n]$ est forcément stationnaire à partir d'un certain rang. En effet, soit I_j cette suite. On a $I = \bigcup_j I_j$ est un idéal. Il est donc engendré par un nombre fini d'éléments, qui les I_j étant emboités sont forcément contenus dans un certain I_n. Ainsi la suite est stationaire à partir du rang n. En conséquence, notre suite d'idéaux $\langle H_j \rangle$ est forcément stationaire à partir d'un certain rang n, rang auquel l'algorithme doit nécessairement aboutir

Voici un exemple d'utilisation de l'algorithme de Buchberger. Supposons que nous ayons à calculer la base de Groebner de $F := \{f_1 = x^2 + y^2, f_2 = x^3 - x, f_3 = y^3 - y\}$ avec l'ordre lexicographique. Dans un premier temps, on initialise $G := F$ et $M := \{(f_1, f_2), (f_1, f_3), (f_2, f_3)\}$. On applique la boucle à (f_1, f_2). On calcule $S(f_1, f_2) = x * (x^2 + y^2) - (x^3 - x) = xy^2 + x = f_4$ Cet élément étant sous forme réduite, on ajoute à M les trois couples (f_i, f_4) pour $i < 4$. On réitère l'opération avec (f_1, f_3), on ajoute ainsi l'élément $x^2y + y$ à G et quatre nouveaux couples à M. Enfin, avec le couple (f_2, f_3) on obtient $h = 0$ et donc on peut passer directement au couple suivant. Avec le couple $(x^2y + y, x^3 - x)$, on obtient $S(x^2y + y, x^3 - x) = 2xy$ qui est sous forme réduite. Finalement, avec les couples $(x^2y + y, 2xy)$ et $(xy^2 + x, 2xy)$ on obtient finalement x et y. Pour finir, par l'algorithme de Buchberger, on obtient un base de Groebner sous forme réduite $G := \langle x, y \rangle$ dès qu'on a retiré les éléments superflus.

On se rend rapidement compte que cet algorithme peut être amélioré. En effet, tout depend de l'ordre dans lequel on choisit les éléments de M. En effet, l'algorithme peut connaître de nombreuses réductions à zeros qui ralentissent inutilement le processus et peuvent être évité comme il est vu dans les algorithmes de JC Faugère F_4 et F_5. Plus précisément, l'algorithme F_4, permet d'accéléer de manière significative l'algorithme de Buchberger en réduisant plusieurs polynômes en même temps par un liste de polynômes et en utilisant pour ce faire des méthodes d'algèbre linéaire. A l'opposé, l'algorithme F_5 permet d'enlever un grand nombres de couples inutiles dans M. Comme une bonne partie du temps de calcul est passé justement dans l'algorithme de Buchberger classique à calculer des réductions de polynômes inutiles dans la base de Groebner finale, on comprend tout l'interêt de ces types d'algorithmes. La combinaison de ces deux algorithmes permet d'accélérer significativement le calcul d'une base de Groebner et rend envisageable la résolution d'un grand nombre de systèmes de polynômes auparavant inatteignable.

Dans un premier temps, nous allons détailler quelques stratégies permettant d'accélerer l'algorithme de Buchberger. En premier lieu, il existe deux critères connus sous le nom de critères de Buchberger qui accélèrent significativement les calculs :

Proposition 8.6.3 (Critère de Buchberger(1)) *:*
Si le $\text{ppcm}(LM(p), LM(q)) = LM(p) * LM(q)$*, alors* $S(p, q)$ *se réduit à zero par division par* p *et* q

En effet, on alors l'égalité suivante :

$$S(p,q) = \frac{LM(p)LM(q)}{LT(p)} * p - \frac{LM(p)LM(q)}{LT(q)} * q$$

$$S(p,q) = \frac{pq}{LT(p)LT(q)} - \frac{pq}{LT(p)LT(q)} + p * \frac{q - LT(q)}{LC(p)LC(q)} - q * \frac{p - LT(p)}{LC(p)LC(q)}$$

où l'on nomme LC le coefficient dominant de notre polynôme. On peut donc sans hésiter supprimer les couples où les coefficients dominants sont premiers entre eux puisque les termes qu'ils pourraient faire intervenir ne sont nullement essentiels.
En conclusion, on ne choisit des couples (p, q) dans l'algorithme de Buchberger que si $\text{ppcm}(LM(p), LM(q)) <> LM(p)LM(q)$. Nous avons un deuxième critère qui permet d'éviter des calculs inutiles.

Proposition 8.6.4 (Critère de Buchberger (2)) *:*
Supposons que nous considérons la paire (p, q) *et supposons qu'il existe un élément* $r \in G$ *tel que* $\text{ppcm}(LM(p), LM(q))$ *soit divisible par* $LM(r)$ *et* $S(p, r)$ *et* $S(q, r)$ *on déjà été considérés dans l'algorithme. Alors* $S(p, q)$ *re réduit à* 0 *par division par des éléments de* G*.*

Il suffit de réécrire $S(p,r)$, $S(q,r)$ et $S(p,q)$ et on obtient directement la réduction à zéro de ce dernier.

Une autre stratégie consiste à choisir les paires qui sont les plus prometteuses dans l'algorithme pour accélerer le calcul. Si nous choisissons (p,q) tel que ppcm$(LM(p), LM(q))$ est aussi petit que possible (suivant l'ordre entre les monômes que nous nous sommes imposés au départ), cela conduit à manipuler des polynômes plus simple. De plus, la chance d'utiliser le critère 2 augmente. Ainsi, on améliore de manière significative l'algorithme de calcul de bases de Groebner.

9 HFE et attaques utilisant les bases de Groebner

(Vincent Despiegel, mémoire de DEA)

Le schéma HFE ("Hidden Field Equations") par J.Patarin est un protocole de cryptographie se basant sur la difficulté à résoudre un système d'équation algébrique. En effet, ce dernier problème étant NP complet, il parrait assez logique de chercher à construire un protocole de cryptographie à clé publique reposant sur ce problème. Nous allons présenter le système HFE classique. On construit un polynôme f sur $\mathbb{F}_{2^n}$ de la manière suivante :

$$f(x) := \sum \beta_{i,j} x^{2^{\theta_{i,j}}+2^{\phi_{i,j}}} + \sum \alpha_k x^{2^{\epsilon_k}} + \mu$$

Appelons d son degrès. Vu que $\mathbb{F}_{2^n}$ est isomorphe à $\mathbb{F}_2[z]/(g(z))$ où g est un polynôme irreductible de degrès n, on dispose d'un isomorphisme direct entre $\mathbb{F}_{2^n}$ et $(\mathbb{F}_2)^n$. De plus, de par le choix de f effectué plus haut et vu que le carré dans $\mathbb{F}_{2^n}$ est une application linéaire, on peut aisément représenter la fonction f comme un polynôme en n variables dans $\mathbb{F}_2$:

$$f(x_1, \cdots, x_n) = (q_1(x_1, \cdots, x_n), \cdots, q_n(x_1, \cdots, x_n))$$

On a ainsi nécéssairement, q_i de degrès total égal à 2, par construction de f. En effet, les $\beta_{i,j} x^{2^{\theta_{i,j}}+2^{\phi_{i,j}}}$ peuvent être vu comme produit de 2 polynômes de degrès 1 en les x_k. Les autres termes sont des polynômes de degrès 1 ou 0 en les x_k.

Nous choisissons deux matrices S et T inversibles de taille $n \times n$ à coefficients dans $\mathbb{F}_2$. On rend publique le $n-$ uplet de polynôme suivant :

$$S(f(TX)) := (p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n))$$

Comme combinaisons linéaires de polyômes de degrè total égal à 2, les p_i sont nécéssairement de degrès 2.

Le protocole de cryptage à clé publique HFE consiste à rendre publique $S(f(TX))$ et à garder secrets les paramètres S, T et f. Pour coder un message dans $(x_1, \cdots, x_n) \in (\mathbb{F}_2)^n$, il suffit de de calculer

$$y := ((p_1(x_1, \cdots, x_n), \cdots, p_n(x_1, \cdots, x_n))$$

et de transmettre le message ainsi codé. Pour décrypter il suffit de calculer $T^{-1}y$, de résoudre l'équation $f(z) = T^{-1}y$ pour finalement calculer $S^{-1}z$. Ainsi, on peut déchiffrer le message crypté et obtenir x, l'élément de départ. Cependant, pour cela, il faut résoudre l'équation $f(z) = \alpha$. il s'agit donc de résoudre un polynôme de degrès d à coefficient dans $\mathbb{F}_{2^n}$. Ceci peut être fait en $O(M(d) * log(d))$ opérations dans $\mathbb{F}_{2^n}$. $M(d)$ correspond au coût d'une multiplication de polynômes de degrès d

Le calcul de bases de Groebner des différents polynômes $p_1 - y_1, \cdots p_n - y_n$ à n variables dans $\mathbb{F}_2$ auxquels on associe les n polynômes $x_i^2 - x_i$, nous permettant, comme nous l'avons vu précédement dans le paragraphe sur les base de Groebner, de calculer la solution de notre système de polynôme, c'est à dire le n uplet $(x_1, \cdots, x_n)$. De plus, la présence des n derniers ponynômes nous assure que les polynômes intervenants dans le calcul de la base de Groebner ont un degrès majoré par n. Ainsi, l'accélération des

algorithmes de calcul des bases de Groebner rend possible de casser le protocole HFE pour certaines valeurs de d (le degrès de notre polynôme dans $\mathbb{F}_{2^n}$) et n. Par exemple, J. Patarin avait proposé un prix symbolique de 500 dollars à quiconque decrypterai son "HFE first challenge" avec paramètre $d = 96$, $n = 80$. A l'aide de l'algorithme F_5 de calcul des bases de Groebner, J.-C. Faugère a réussi en un peu plus de deux jours à le décrypter.

9.1 Attaques du protocole par les bases de Groebner

Comme nous l'avons vu dans la partie précédente, la raison principale pour laquelle il est réalisable d'attaquer HFE à l'aide des bases de Groebner réside dans le fait que nous travaillons sur $\mathbb{F}_2$. Pour cette raison, les polynômes qui seront créés lors du calcul de la base seront de degrès majoré par n où n est le nombre de variables intervenant dans nos polynômes. En effet, pour chaque variable x_i nous avons le polynôme $x_i^2 - x_i$ qui permet de réduire le degrès partiel en x_i à 1 ou 0. Cela nous assure donc de travailler avec des polynômes de taille raisonnable et explique pourquoi cette méthode se révèle efficace.

En contrepartie, dans le cas du protocole sur les modules de Drinfeld proposé par A. Pantchichkine, F. Leprevost, R. Gillard et X. Roblot, nous travaillons sur un corps $\mathbb{F}_p$ (ou $\mathbb{F}_{p^d}$) avec p grand (de l'ordre de 2^{30}). Cela signifie que les polynômes qui seront manipulé seront de taille très importante et en grand nombre ce qui fait que la methode sera beaucoup trop coûteuse en temps de calcul pour pouvoir être appliquée.

Il me semble donc que contrairement à ce qui est annoncé dans l'article de S. R. Blackburn et S. D. Galbraith, et contrairement à ce que suggerait JC. Faugère, les bases de Groebner ne peuvent servir efficacement à casser le protocole. En effet, il faudrait une nette amélioration dans les algorithmes de calcul pour résoudre ce problème par cette méthode.

9.2 Attaques du protocole par un procédé de linéarisation

Cependant, une autre methode bien plus prometteuse est à envisager. S. R. Blackburn et S. D. Galbraith en font part dans leur article Cryptanalysis of a cryptosystem based on Drinfeld modules. Le principe consiste à renommer les monomes de degrès total superieur ou égal à 2 par de nouveaux noms de variables et à applique la methode de Gauss pour réduire le nombre de variables vu qu'alors, nous disposons d'un système linéaire d'équations.

Pour cela, commençons d'abord par supprimer le paramètre δ qui comme nous l'avons ne joue aucun rôle dans la sécurité du protocole.. Nous devons donc trouver $x_0, \cdots, x_{d-1}$ et $y_0, \cdots, y_{d-1}$ tels que :

$$\begin{aligned}
&\phi_{c_1'} := x_0 id + \cdots + x_{d-1} F^{d-1} \\
&\phi_{c_2} := y_0 id + \cdots + y_{d-1} F^{d-1} \\
&\phi_{c_1'}(\psi(z)) = (\phi_{c_2}(z))^e
\end{aligned}$$

Pour cela, nous disposons de la fonction de cryptage ψ qui nous permet de créer de nombreux couples $(z, \psi(z))$. Nous developpons formellement $(\phi_{c_2}(z))^e$. Cela fait intervenir un nombre restreint de monomes de degrès e en les y_i. (en effet, e doit être maintenu petit pour que la fonction de codage, ψ reste de taille raisonnable. En pratique il est pris égal à 5 ou 7.) En utilisant le procédé de linéarisation sur ces monomes (c'est à dire en renommant les éléments de la forme $\prod_j y_j^{e_j}$ par des u_k), on se ramène à un système linéaire à moins de $d^e + d$ variables. A l'aide de notre fonction ψ on génère un grand nombre de couples

$$(z, w = \psi(z))$$

avec un grand nombre de z choisis au hasard dans $\mathbb{F}_{p^d}$. Ainsi on se ramène à un grand nombre d'équation linéaire en les x_i et les u_k de la forme :

$$\phi_{c_1'}(w) = (\phi_{c_2}(z))^e$$

On cherche dans un premier temps par un procédé de Gauss à supprimer les u_k. Si cette methode aboutie, (ie : nos nombreuses équations en ces coefficients sont suffisament indépendantes), alors on se retrouve à un système en y_{d-1}^e et en les x_i. On ajoute alors à ce système l'équation $y_{d-1} = 1$ et on résoud le système. On trouve alors les valeurs $x_0, \cdots, x_{d-1}$ en utilisant le fait que les x_i sont les coefficients d'un ϕ_a et doivent donc prendre des valeurs particulières. A partir de ces paramètres, on peut calculer aisément :

$$(\phi_{c_2}(z))^e$$

Pour retrouver les paramètres de c_2, ϕ_{c_2} étant linéaire, il suffit de calculer $(\phi_{c_2}(t^i))^e$ pour tout i variant entre 0 et $d-1$. En élevant ces résultats à la puissance f (tel que $ef \equiv 1[p^d - 1]$), on obtient $\phi_{c_2}(t^i)$ et on en déduit aisément les paramètres y_i.

Il est à noter qu'il est nullement prouvé qu'en choisissant au hasard un nombre r d'éléments (où r est le nombre de variables u_k et x_k) de $\mathbb{F}_{p^d}$, il soit possible par la methode de Gauss de trouver les paramètres x_i. Cependant, il est à noter que pour les tests sur des petites valeurs des paramètres (p et d) sous Maple, nous avons toujours réussi à nous ramener par cette methode à un système en les x_i, facile à résoudre.

9.3 Exemple et application du procédé de linéarisation

Nous allons présenter dans un exemple comment utiliser la méthode de linéarisation pour retrouver les paramètres de cryptage. Nous utiliserons les paramètre suivants : $p = 7$, $d = 3$ et le module de Carlitz (ie : $\phi(t) := F + t$). Nous utiliserons le polynôme irreductible sur $\mathbb{F}_7$, $f(t) := t^3 + t + 1$. Appelons $\mathcal{A}$ la matrice représentant ϕ_t dans la base canonique :

$$\mathcal{A} := \begin{pmatrix} 1 & 6 & 0 \\ 1 & 0 & 2 \\ 0 & 3 & 6 \end{pmatrix}$$

Il suffit alors de calculer le polynôme caractéristique de $\mathcal{A}$ pour en déduire $f_\phi(t)$

$$f_\phi(t) := t^3 + t$$

Choisissons alors des polynômes de degrès 2, c_1 et c_2 comme paramètres secrets et $e = 5$.

$$\begin{array}{ll} c_1 = t^2 + 3t + 1 & c_1' = t^2 + 2t + 1 \\ c_2 = t^2 + 5t + 2 & c_2' = t^2 + 6t + 4 \end{array}$$

On obtient ainsi la fonction de cryptage (ie : la clé publique) suivante :

$$\begin{array}{ccccccccc} \psi(z) & := & (5t^2+6t+1)z^5 & + & (4t^2+3t+4)z^{11} & + & (3t^2+4t)z^{17} & + \\ (3t^2+3t)z^{23} & + & (3t^2+4t+3)z^{29} & + & (t+2)z^{35} & + & (2t^2+2t)z^{53} & + \\ (6t^2+2t+1)z^{59} & + & (3t^2+3t)z^{65} & + & (4t^2+2)z^{71} & + & (3t^2+4t+1)z^{77} & + \\ (t+2)z^{101} & + & (5t+1)z^{107} & + & (5t^2+2t+1)z^{113} & + & (4t^2+4t+6)z^{119} & + \\ (6t^2+3t+3)z^{149} & + & (t^2+5t+4)z^{155} & + & (5t^2+2t+3)z^{161} & + & (2t^2)z^{197} & + \\ (3t^2+6t+1)z^{203} & + & (3t+6)z^{245} & & & & & \end{array}$$

On retrouve bien le nombre de terme de ψ en fonction de e et d comme nous l'avons vu plus haut (i.e. : $\binom{d+e-1}{d-1} = \binom{7}{2} = 21$). Ainsi, à partir de cette fonction de cryptage,on peut coder un entier entre 0 et $7^3 - 1 = 342$. Pour cela, on exprime $\mathcal{M} \in 0..342$ dans la base 7. Prenons par exemple $\mathcal{M} := 235$. On a

$$\mathcal{M} := 4 * 7^2 + 5 * 7 + 4 * 1$$

On l'associe de manière unique à un élément de $\mathbb{F}_{7^3}$ de la manière suivante :

$$\mu := 4 * t^2 + 5 * t + 4$$

En appliquant ψ, on obtient le message crypté suivant $\chi := \psi(\mu) = 2t^2 + 4t + 1$ et donc le message codé $\mathcal{M}' := 127$.

L'objectif maintenant est d'étudier comment pratiquement il est possible en utilisant le procédé de linéarisation de retrouver les paramètres secrets.

Pour cela, dans un premier temps, on écrit les polynômes secrets avec les $2d$ inconnues suivantes (ie : les x_i et les y_i) dans $\mathbb{F}_{7^3}$:

$$\begin{array}{rcl} \phi_{c_1'}(z) & = & x_0 + x_1 z^7 + x_2 z^{49} \\ \phi_{c_2}(z) & = & y_0 + y_1 z^7 + y_2 z^{49} \end{array}$$

Ensuite, on développe $(\phi_{c_2}(z))^5$ de manière formelle et on obtient un polynôme en z et en les monômes de degrès 5 en les y_i. Renommons ces monômes en u_k de la manière suivante : $y_0^5 = u_1$, $y_0^4 y_1 = u_2$, $y_0^4 y_2 = u_3$, $y_0^3 y_1^2 = u_4, \cdots, y_2 = u_{21}$. On a donc un grand nombre d'équations en les x_i et les u_k de la manière suivante

$$\phi_{c_1'}(\psi(z)) = (\phi_{c_2}(z))^5$$

On prend au hasard 24 éléments de $\mathcal{K} = \mathbb{F}_{7^3}$ et on obtient ainsi 24 équations en les u_k et les x_i. On applique la methode de Gauss à la matrice ainsi constituée en commençant par supprimer les u_k. A la fin du processus, on obtient une matrice de la forme suivante :

$$\mathcal{N} := \begin{pmatrix} 1 & & * & \overset{u_{21}}{\widehat{*}} & * \\ 0 & \ddots & & * & * \\ \vdots & & \ddots & \vdots & * \\ \vdots & 0 & & 1 & * \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}$$

Il suffit de lire la 21 ème ligne de la matrice pour obtenir une équation liant y_2^5 et les x_i. On peut sans perte de généralité considérer que $y_2 = 1$ (A une multiplication par un élément de $\mathcal{K}_7$ c'est le cas). On obtient alors un équation linéaire en les x_i :

$$6t^2 + 6t + 1 = (5t^2 + 2) * x_0 + (3t^2 + 3t + 3) * x_1 + (5t^2 + 5t + 1)x_2$$

Maintenant, il ne faut pas oublier que $\phi_{c_1'}$ n'a pas des coefficients quelconques en z, z^7 et z^{49}. En effet, $\phi_{c_1'} := c\phi_{t^2} + b\phi_t + a\phi_1$ avec a, b et c dans $\mathcal{K} = \mathbb{F}_7$. Vu que $\phi_t(z) = z^7 + tz$ et $\phi_{t^2}(z) = z^{49} + (2t^2 + t + 6)z^7 + t^2 z$, il en découle alors le système suivant :

$$\left\{ \begin{array}{rcl} 6 & = & 5a + 3b + 2c \\ 6 & = & 6c \\ 1 & = & 2a + 5b + 3c \end{array} \right.$$

On en déduit bien $c_1' := t^2 + 2t + 1$. Ensuite, pour obtenir c_2, connaissant e et c_1' il suffit de calculer $\phi_{c_2}(1)$, $\phi_{c_2}(t)$, $\phi_{c_2}(t^2)$ et on en déduit aisément $c_2 = t^2 + 5t + 2$.

A Annexe : Equation de Weierstrass et le théorème d'addition complexe

L'équation de Weierstrass est utilisée dans la théorie de l'uniformisation complexe des courbes elliptiques. Considérons un *tore complexe* de type $\mathbb{C}/\Lambda$, où $\Lambda = \langle \omega_1, \omega_2 \rangle$ est un réseau de $\mathbb{C}$. On muni $\mathbb{C}/\Lambda$ d'une structure d'une courbe projective complexe de la manière suivante.

Considèrons la fonctions $\wp$ de Weierstrass

$$\wp(u) = \wp(u, \Lambda) = \frac{1}{u^2} + \sum_{l \in \Lambda}{}' \left(\frac{1}{(u+l)^2} - \frac{1}{l^2} \right)$$

(le prime signifie que $l \neq 0$) ; c'est une fonction méromorphe double périodique *paire* sur $\mathbb{C}$ avec les pôles doulble dans les points $u = l$. Pour sa dérivé on a

$$\wp'(u) = \wp'(u, \Lambda) = -2 \sum_{l \in \Lambda} \frac{1}{(u-l)^3};$$

c'est une fonction méromorphe double périodique *impaire*

On pose pour $k \geq 2$

$$G_{2k}(\Lambda) = \sum_{l \in \Lambda}{}' \frac{1}{l^{2k}}.$$

Il est facile à voir que les développements de Laurent de $\wp(u)$ et de $\wp'(u)$ sont

$$\begin{aligned}
\wp(u) &= u^{-2} + \sum_{n=2}^{\infty} (2n-1) G_{2n}(\Lambda) u^{2n-2} = u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6) \\
\wp'(u) &= -2u^{-3} + \sum_{n=2}^{\infty} (2n-1)(2n-2) G_{2n}(\Lambda) u^{2n-3} \\
&= -2u^{-3} + 6G_4 u + 20 G_6 u^3 + \mathcal{O}(u^5)
\end{aligned}$$

D'où on obtient la *relation de Weierstrass* suivante

$$\wp'(u)^2 = 4\wp(u)^3 - g_2 \wp(u) - g_3,$$

où

$$g_2 = 60 \sum_{l \in \Lambda}{}' \frac{1}{l^4}, \qquad g_3 = 140 \sum_{l \in \Lambda}{}' \frac{1}{l^6}.$$

En effet, la fonction $\wp'(u)^2 - 4\wp^3 + 60 G_4 \wp + 140 G_6$ est identiquement nulle car son développement de Laurent en 0 ne contient que des puissances positives de u :

$$\begin{aligned}
\wp(u) &= u^{-2} + 3G_4 u^2 + 5G_6 u^4 + \mathcal{O}(u^6), \\
\wp^3(u) &= u^{-6} + 9G_4 u^{-2} + 15 G_6 + \mathcal{O}(u^2) \\
\wp'(u) &= -2u^{-3} + 6G_4 u + 20 G_6 u^3 + \mathcal{O}(u^5), \\
\wp'^2(u) &= 4u^{-6} - 24 G_4 u^{-2} - 80 G_6 + \mathcal{O}(u^2)
\end{aligned}$$

et cette fonction est une fonction double périodique sur $\mathbb{C}$ qui s'annule à l'origine, c'est à dire, elle est la constante 0 par le *théorème de Liouville*.

Maintenant on note par $E_\Lambda \subset \mathbb{P}^2_{\mathbb{C}}$ la courbe définie par l'equation de Weierstrass avec g_2 et g_3 ci-dessus, et on définit une application

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E_\Lambda(\mathbb{C})$$

par $u \mapsto (\wp(u) : \wp'(u) : 1)$, si u n'est pas dans Λ, et 0 s'applique sur $(0 : 1 : 0)$.

L'application définie un isomorphisme complexe analytique . Pour décrire explicitement l'application inverse on peut aussi utiliser la différentielle

$$dx/y = dx/\sqrt{4x^2 - g_2 x - g_3}$$

sur $E = E_\Lambda(\mathbb{C})$ et l'intégrer autour un contour qui joint un point initial fixe (disons, o) avec un point varié. L'intégral depends du choix de contour mais l'image dans $\mathbb{C}/\Lambda$ est invariant. Le réseau

$$\Lambda = \left\{ \int_\gamma \omega \;\middle|\; \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\}$$

est définit par le choix de la différentielle ; si l'on remplace ω par $u\omega$, $u \in \mathbb{C}$, le réseau Λ ce remplace par le réseau $\Lambda' = u\Lambda$.

L'isomorphisme $\mathbb{C}/\Lambda \xrightarrow{\sim} E_\Lambda(\mathbb{C})$ est compatible avec les structures naturelles de groupe. En termes de fonctions elliptiques, ce fait s'exprime comme le *théorème d'addition* des fonction elliptiques :

THÉORÈME A.0.1 *Soit u_1, $u_2 \notin \Lambda$, et $u_1 \pm u_2 \notin \Lambda$, alors*

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right)^2.$$

En termes des coordonnées (x, y) on a

$$x_3 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$

où

$$P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = P_1 + P_2 = (x_3, y_3).$$

Démonstration du théorème d'addition A.0.1 et basée sur la

PROPOSITION A.0.2 *(a) Pour une fonction $0 \neq f$ méromorphe double périodique avec $\operatorname{div}(f) = \sum_{u \in \mathbb{C}/\Lambda} n_u(u)$ on a $\sum_{u \in \mathbb{C}/\Lambda} n_u = 0$;*

(b) Ensuite, on a $\sum_{u \in \mathbb{C}/\Lambda} n_u u \equiv 0 (\mathrm{mod} \Lambda)$.

Preuve. La première assertion exprime une propriété générale des fonctions méromorphes sur les surfaces de Riemann compactes $\deg \operatorname{div}(f) = 0$ (mais montrer la directement en utilisant l'annulation de l'intégrale

$$\int_{\partial \Pi} \frac{f'(u)}{f(u)} du = 2\pi i \sum_u n_u,$$

où Π désigne le parallelogramme fondamental de Λ, et $\partial\Pi$ sa borne).

La deuxième assertion est impliqué par un calcule facile de l'intégrale

$$\int_{\partial \Pi} u \frac{f'(u)}{f(u)} du = 2\pi i \sum_u n_u u,$$

où Π désigne le parallelogramme fondamental de Λ, et $\partial\Pi$ sa borne. D'autre part, l'intégrale peut être calculer à l'aide de calcule les intégrales lelong les côtés opposites. Par exemple, un des deux couples de ces intégrales est égale à

$$\begin{aligned}&\int_{\alpha}^{\alpha+\omega_1} u\frac{f'(u)}{f(u)}du - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} u\frac{f'(u)}{f(u)}du\\ &= -w_2\int_{\alpha}^{\alpha+\omega_1}\frac{f'(u)}{f(u)} = -w_2\int_{\alpha}^{\alpha+\omega_1} d(\ln f(u))du = 2\pi ik\omega_2 \in \Lambda,\end{aligned}$$

où $k \in \mathbb{Z}$ (car l'accroissement du logarithme lelong un chemin fermé qui joigne $f(\alpha)$ et $f(\alpha+\omega_1) = f(\alpha)$, est égale à $2\pi ik$).

Maintenant, pour $u_1, u_2 \in \mathbb{C}/\Lambda$, $u_1 \not\equiv u_2 \bmod \Lambda$ on choisit des nombres complexes a et b tels que

$$\wp'(u_1) = a\wp(u_1) + b, \quad \wp'(u_2) = a\wp(u_2) + b,$$

i.e. $y = ax + b$ la droite passant par les points (x_i, y_i), où $x_i = \wp(u_i)$, $y_i = \wp'(u_i)$, $(i = 1, 2)$. La fonction $\wp'(u) - (a\wp(u) + b)$ a exactement trois zéros, comptées avec multiplicités, $u = u_1, u_2, u_3$ puisque $\wp'(u) - (a\wp(u) + b)$ n'a qu-un seul pôle (qui est triple) en $u = 0$.

On a alors par Proposition A.0.2 (b) : $u_1 + u_2 + u_3 \equiv 0(\mathrm{mod}\Lambda)$. On a soit $u_1 = u_3$, $2u_1 + u_2 \equiv 0(\bmod \Lambda)$, soit $u_3 \equiv -(u_1 + u_2)(\bmod \Lambda)$. Ceci implique que le polynôme $4x^3 - g_2x - g_3 - (ax + b)^2$ a trois racines $x_i = \wp(u_i)$, $(i = 1, 2, 3)$, i.e.

$$4x^3 - g_2x - g_3 - (ax + b)^2 = 4(x - \wp(u_1))(x - \wp(u_2))(x - \wp(u_3)).$$

Puisque $a(\wp(u_1) - \wp(u_2)) = \wp'(u_1) - \wp'(u_2)$, on a

$$\wp(u_1) + \wp(u_2) + \wp(u_3) = \frac{a^2}{4}$$

(coefficient de x^2), d'où

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)}\right)^2.$$

Si $u_1 = u_2 = u$, on a

$$\wp(2u) = -2\wp(u) + \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2.$$

par un passage à la limite $u \to u_1$ dans la formule précédente :

$$\wp(u_1 + u) = -\wp(u_1) - \wp(u) + \frac{1}{4}\left(\frac{\wp'(u_1) - \wp'(u)}{\wp(u_1) - \wp(u)}\right)^2.$$

B Annexe : L'algèbre gauche de Ore et l'anneau $A\{\tau\} = \mathbb{F}_p[T]\{\tau\}$

Pour travailler dans l'anneau $A\{\tau\} = \mathbb{F}_p[T]\{\tau\}$, on peut utiliser "l'algèbre gauche de Ore" (en Maple). Ici on note par a_i, et $a_{i,j}(i = 1, 2, \cdots, n; j = 1, 2, 3)$ éléments du corps simple $\mathbb{F}_p$, qui commutent avec T et τ.

"Let us define the Mahlerian operator of order p (voir "Help" de Maple, la section "Commutation rules in Ore algebra"). The commutation rule reads :" tau(f(x)) = f(x^p).

```
> restart;with(Ore_algebra):p:=3;
> n:=10;A:=skew_algebra(comm={seq(a[i],
> i=1..n),seq(a[i,1],
> i=1..n),seq(a[i,2],
> i=1..n),
> seq(a[i,3],
> i=1..n)},
> user=[tau,T,
> proc(f,n) subs(T=T^(p^n),f) end proc,
> proc(f,n) `if`(n=0,f,0) end proc],characteristic=3):
> skew_product(tau,T,A);
```

$$p := 3$$

$$n := 10$$

$$T^3\,\tau$$

```
> skew_product(T+tau+a[2]*tau^2,T,A);
```

$$T^2 + T^3\,\tau + a_2\,T^9\,\tau^2$$

```
> skew_product(T+tau+a[2]*tau^2,T+tau+a[2]*tau^2,A);
```

$$T^2 + 2\,a_2\,\tau^3 + {a_2}^2\,\tau^4 + (T + T^3)\,\tau + (T\,a_2 + 1 + a_2\,T^9)\,\tau^2$$

```
> f[1]:=add(a[i,1]*T^i,i=1..n);
> f[2]:=add(a[i,2]*T^i,i=1..n);
> f[3]:=add(a[i,3]*T^i,i=1..n);skew_product(tau^2,f[2],A);
```

$$f_1 := a_{1,1}\,T + a_{2,1}\,T^2 + a_{3,1}\,T^3 + a_{4,1}\,T^4 + a_{5,1}\,T^5 + a_{6,1}\,T^6 + a_{7,1}\,T^7 + a_{8,1}\,T^8 + a_{9,1}\,T^9 + a_{10,1}\,T^{10}$$

$$f_2 := a_{1,2}\,T + a_{2,2}\,T^2 + a_{3,2}\,T^3 + a_{4,2}\,T^4 + a_{5,2}\,T^5 + a_{6,2}\,T^6 + a_{7,2}\,T^7 + a_{8,2}\,T^8 + a_{9,2}\,T^9 + a_{10,2}\,T^{10}$$

$$f_3 := a_{1,3}\,T + a_{2,3}\,T^2 + a_{3,3}\,T^3 + a_{4,3}\,T^4 + a_{5,3}\,T^5 + a_{6,3}\,T^6 + a_{7,3}\,T^7 + a_{8,3}\,T^8 + a_{9,3}\,T^9 + a_{10,3}\,T^{10}$$

$$(a_{1,2}\,T^9 + a_{2,2}\,T^{18} + a_{3,2}\,T^{27} + a_{4,2}\,T^{36} + a_{5,2}\,T^{45} + a_{6,2}\,T^{54} + a_{7,2}\,T^{63} + a_{8,2}\,T^{72} + a_{9,2}\,T^{81} + a_{10,2}\,T^{90})\tau^2$$

```
> skew_product(T+tau+tau^2,f[1],A);
```

$$a_{1,1}\,T^2 + a_{2,1}\,T^3 + a_{3,1}\,T^4 + a_{4,1}\,T^5 + a_{5,1}\,T^6 + a_{6,1}\,T^7 + a_{7,1}\,T^8 + a_{8,1}\,T^9 + a_{9,1}\,T^{10} + a_{10,1}\,T^{11} + (a_{1,1}\,T^3 + a_{2,1}\,T^6 + a_{3,1}\,T^9 + a_{4,1}\,T^{12} + a_{5,1}\,T^{15} + a_{6,1}\,T^{18} + a_{7,1}\,T^{21} + a_{8,1}\,T^{24} + a_{9,1}\,T^{27} + a_{10,1}\,T^{30})\tau + (a_{1,1}\,T^9 + a_{2,1}\,T^{18} + a_{3,1}\,T^{27} + a_{4,1}\,T^{36} + a_{5,1}\,T^{45} + a_{6,1}\,T^{54} + a_{7,1}\,T^{63} + a_{8,1}\,T^{72} + a_{9,1}\,T^{81} + a_{10,1}\,T^{90})\tau^2$$

```
> skew_product(f[1],T+tau+tau^2,A);
```

$$a_{1,1}T^2 + a_{2,1}T^3 + a_{3,1}T^4 + a_{4,1}T^5 + a_{5,1}T^6 + a_{6,1}T^7 + a_{7,1}T^8 + a_{8,1}T^9 + a_{9,1}T^{10} + a_{10,1}T^{11} + (a_{1,1}T + a_{2,1}T^2 + a_{3,1}T^3 + a_{4,1}T^4 + a_{5,1}T^5 + a_{6,1}T^6 + a_{7,1}T^7 + a_{8,1}T^8 + a_{9,1}T^9 + a_{10,1}T^{10})\tau + (a_{1,1}T + a_{2,1}T^2 + a_{3,1}T^3 + a_{4,1}T^4 + a_{5,1}T^5 + a_{6,1}T^6 + a_{7,1}T^7 + a_{8,1}T^8 + a_{9,1}T^9 + a_{10,1}T^{10})\tau^2$$

```
> skew_product(skew_product(f[1],T+tau+tau^2,A),T+tau+tau^2,A);
```

$$a_{10,1}T^{12} + a_{2,1}T^4 + a_{3,1}T^5 + a_{1,1}T^3 + a_{5,1}T^7 + a_{6,1}T^8 + a_{7,1}T^9 + a_{4,1}T^6 + a_{9,1}T^{11} + a_{8,1}T^{10} + (2\,a_{1,1}T + 2\,a_{2,1}T^2 + 2\,a_{4,1}T^4 + 2\,a_{8,1}T^8 + 2\,a_{5,1}T^5 + 2\,a_{6,1}T^6 + 2\,a_{3,1}T^3 + 2\,a_{9,1}T^9 + 2\,a_{10,1}T^{10} + 2\,a_{7,1}T^7)\tau^3 + (a_{1,1}T + a_{2,1}T^2 + a_{3,1}T^3 + a_{4,1}T^4 + a_{5,1}T^5 + a_{6,1}T^6 + a_{7,1}T^7 + a_{8,1}T^8 + a_{9,1}T^9 + a_{10,1}T^{10})\tau^4 + (a_{10,1}T^{13} + a_{9,1}T^{12} + (a_{10,1} + a_{8,1})T^{11} + (a_{7,1} + a_{9,1})T^{10} + (a_{8,1} + a_{6,1})T^9 + (a_{7,1} + a_{5,1})T^8 + (a_{6,1} + a_{4,1})T^7 + (a_{3,1} + a_{5,1})T^6 + (a_{2,1} + a_{4,1})T^5 + (a_{1,1} + a_{3,1})T^4 + a_{2,1}T^3 + a_{1,1}T^2)\tau + (a_{10,1}T^{19} + a_{9,1}T^{18} + a_{8,1}T^{17} + a_{7,1}T^{16} + a_{6,1}T^{15} + a_{5,1}T^{14} + a_{4,1}T^{13} + a_{3,1}T^{12} + (a_{2,1} + a_{10,1})T^{11} + (a_{9,1} + a_{10,1} + a_{1,1})T^{10} + (a_{9,1} + a_{8,1})T^9 + (a_{7,1} + a_{8,1})T^8 + (a_{7,1} + a_{6,1})T^7 + (a_{5,1} + a_{6,1})T^6 + (a_{5,1} + a_{4,1})T^5 + (a_{3,1} + a_{4,1})T^4 + (a_{2,1} + a_{3,1})T^3 + (a_{1,1} + a_{2,1})T^2 + a_{1,1}T)\tau^2$$

```
> sort(%,tau);
```

$$(a_{1,1}T + a_{2,1}T^2 + a_{3,1}T^3 + a_{4,1}T^4 + a_{5,1}T^5 + a_{6,1}T^6 + a_{7,1}T^7 + a_{8,1}T^8 + a_{9,1}T^9 + a_{10,1}T^{10})\tau^4 + (2\,a_{6,1}T^6 + 2\,a_{5,1}T^5 + 2\,a_{7,1}T^7 + 2\,a_{8,1}T^8 + 2\,a_{2,1}T^2 + 2\,a_{1,1}T + 2\,a_{4,1}T^4 + 2\,a_{3,1}T^3 + 2\,a_{10,1}T^{10} + 2\,a_{9,1}T^9)\tau^3 + (a_{10,1}T^{19} + a_{9,1}T^{18} + a_{8,1}T^{17} + a_{7,1}T^{16} + a_{6,1}T^{15} + a_{5,1}T^{14} + a_{4,1}T^{13} + a_{3,1}T^{12} + (a_{2,1} + a_{10,1})T^{11} + (a_{9,1} + a_{10,1} + a_{1,1})T^{10} + (a_{9,1} + a_{8,1})T^9 + (a_{7,1} + a_{8,1})T^8 + (a_{7,1} + a_{6,1})T^7 + (a_{5,1} + a_{6,1})T^6 + (a_{4,1} + a_{5,1})T^5 + (a_{4,1} + a_{3,1})T^4 + (a_{3,1} + a_{2,1})T^3 + (a_{1,1} + a_{2,1})T^2 + a_{1,1}T)\tau^2 + (a_{10,1}T^{13} + a_{9,1}T^{12} + (a_{8,1} + a_{10,1})T^{11} + (a_{9,1} + a_{7,1})T^{10} + (a_{8,1} + a_{6,1})T^9 + (a_{7,1} + a_{5,1})T^8 + (a_{6,1} + a_{4,1})T^7 + (a_{3,1} + a_{5,1})T^6 + (a_{4,1} + a_{2,1})T^5 + (a_{1,1} + a_{3,1})T^4 + a_{2,1}T^3 + a_{1,1}T^2)\tau + a_{10,1}T^{12} + a_{5,1}T^7 + a_{2,1}T^4 + a_{3,1}T^5 + a_{4,1}T^6 + a_{1,1}T^3 + a_{6,1}T^8 + a_{7,1}T^9 + a_{8,1}T^{10} + a_{9,1}T^{11}$$

```
> sort(%,[T,tau]);
```

$$a_{10,1}T^{12} + a_{9,1}T^{11} + a_{8,1}T^{10} + a_{7,1}T^9 + a_{6,1}T^8 + a_{5,1}T^7 + a_{4,1}T^6 + a_{3,1}T^5 + a_{2,1}T^4 + (a_{10,1}T^{10} + a_{9,1}T^9 + a_{8,1}T^8 + a_{7,1}T^7 + a_{6,1}T^6 + a_{5,1}T^5 + a_{4,1}T^4 + a_{3,1}T^3 + a_{2,1}T^2 + a_{1,1}T)\tau^4 + a_{1,1}T^3 + (2\,a_{10,1}T^{10} + 2\,a_{9,1}T^9 + 2\,a_{8,1}T^8 + 2\,a_{7,1}T^7 + 2\,a_{6,1}T^6 + 2\,a_{5,1}T^5 + 2\,a_{4,1}T^4 + 2\,a_{3,1}T^3 + 2\,a_{2,1}T^2 + 2\,a_{1,1}T)\tau^3 + (a_{10,1}T^{19} + a_{9,1}T^{18} + a_{8,1}T^{17} + a_{7,1}T^{16} + a_{6,1}T^{15} + a_{5,1}T^{14} + a_{4,1}T^{13} + a_{3,1}T^{12} + (a_{2,1} + a_{10,1})T^{11} + (a_{9,1} + a_{10,1} + a_{1,1})T^{10} + (a_{9,1} + a_{8,1})T^9 + (a_{7,1} + a_{8,1})T^8 + (a_{7,1} + a_{6,1})T^7 + (a_{5,1} + a_{6,1})T^6 + (a_{5,1} + a_{4,1})T^5 + (a_{3,1} + a_{4,1})T^4 + (a_{2,1} + a_{3,1})T^3 + (a_{1,1} + a_{2,1})T^2 + a_{1,1}T)\tau^2 + (a_{10,1}T^{13} + a_{9,1}T^{12} + (a_{10,1} + a_{8,1})T^{11} + (a_{7,1} + a_{9,1})T^{10} + (a_{8,1} + a_{6,1})T^9 + (a_{7,1} + a_{5,1})T^8 + (a_{6,1} + a_{4,1})T^7 + (a_{3,1} + a_{5,1})T^6 + (a_{2,1} + a_{4,1})T^5 + (a_{1,1} + a_{3,1})T^4 + a_{2,1}T^3 + a_{1,1}T^2)\tau$$

```
> skew_product(f[2],tau,A);
```

$$(a_{1,2}\,T + a_{2,2}\,T^2 + a_{3,2}\,T^3 + a_{4,2}\,T^4 + a_{5,2}\,T^5 + a_{6,2}\,T^6 + a_{7,2}\,T^7 + a_{8,2}\,T^8 + a_{9,2}\,T^9 + a_{10,2}\,T^{10})\tau$$

```
> skew_product(f[3],tau^2,A);
```

$$(a_{1,3}\,T + a_{2,3}\,T^2 + a_{3,3}\,T^3 + a_{4,3}\,T^4 + a_{5,3}\,T^5 + a_{6,3}\,T^6 + a_{7,3}\,T^7 + a_{8,3}\,T^8 + a_{9,3}\,T^9 + a_{10,3}\,T^{10})\tau^2$$

```
> skew_product(f[1]+skew_product(f[2],tau,A)+skew_product(f[3],tau^2,A)
> ,T+tau+tau^2,A);
```

$$\begin{aligned}
&a_{1,1}\,T^2 + a_{2,1}\,T^3 + a_{3,1}\,T^4 + a_{4,1}\,T^5 + a_{5,1}\,T^6 + a_{6,1}\,T^7 + a_{7,1}\,T^8 + a_{8,1}\,T^9 + a_{9,1}\,T^{10} \\
&+ a_{10,1}\,T^{11} + ((a_{10,3} + a_{10,2})\,T^{10} + (a_{9,3} + a_{9,2})\,T^9 + (a_{8,2} + a_{8,3})\,T^8 \\
&+ (a_{7,3} + a_{7,2})\,T^7 + (a_{6,3} + a_{6,2})\,T^6 + (a_{5,2} + a_{5,3})\,T^5 + (a_{4,3} + a_{4,2})\,T^4 \\
&+ (a_{3,3} + a_{3,2})\,T^3 + (a_{2,2} + a_{2,3})\,T^2 + (a_{1,3} + a_{1,2})\,T)\tau^3 + (a_{1,3}\,T + a_{2,3}\,T^2 + a_{3,3}\,T^3 \\
&+ a_{4,3}\,T^4 + a_{5,3}\,T^5 + a_{6,3}\,T^6 + a_{7,3}\,T^7 + a_{8,3}\,T^8 + a_{9,3}\,T^9 + a_{10,3}\,T^{10})\tau^4 + (a_{10,2}\,T^{13} \\
&+ a_{9,2}\,T^{12} + a_{8,2}\,T^{11} + (a_{7,2} + a_{10,1})\,T^{10} + (a_{9,1} + a_{6,2})\,T^9 + (a_{8,1} + a_{5,2})\,T^8 \\
&+ (a_{7,1} + a_{4,2})\,T^7 + (a_{3,2} + a_{6,1})\,T^6 + (a_{2,2} + a_{5,1})\,T^5 + (a_{1,2} + a_{4,1})\,T^4 + a_{3,1}\,T^3 \\
&+ a_{2,1}\,T^2 + a_{1,1}\,T)\tau + (a_{10,3}\,T^{19} + a_{9,3}\,T^{18} + a_{8,3}\,T^{17} + a_{7,3}\,T^{16} + a_{6,3}\,T^{15} + a_{5,3}\,T^{14} \\
&+ a_{4,3}\,T^{13} + a_{3,3}\,T^{12} + a_{2,3}\,T^{11} + (a_{10,1} + a_{10,2} + a_{1,3})\,T^{10} + (a_{9,1} + a_{9,2})\,T^9 \\
&+ (a_{8,1} + a_{8,2})\,T^8 + (a_{7,1} + a_{7,2})\,T^7 + (a_{6,1} + a_{6,2})\,T^6 + (a_{5,2} + a_{5,1})\,T^5 \\
&+ (a_{4,1} + a_{4,2})\,T^4 + (a_{3,1} + a_{3,2})\,T^3 + (a_{2,2} + a_{2,1})\,T^2 + (a_{1,1} + a_{1,2})\,T)\tau^2
\end{aligned}$$

C Annexe : Systèmes linéaires dans GF(p^d) (F. SERGERAERT)

```
> restart :
```

- Exemple dans GF(3^4).

- On prend un polynôme irréductible de degré 4 dans F_3, affecté à **irr34**.

```
> irr34 := op(1, select(has, Factor(x^81-x) mod 3, 4)) ;
```

$$irr34 := x^4 + 2\,x^3 + 2\,x^2 + x + 2$$

- Le polynôme irréductible obtenu par ce procédé n'est pas forcément le même d'une session à l'autre.

- On aliasse α à une racine de ce polynôme dans une extension de F_3, de sorte que GF(3^4) = F_3[α].

```
> alias(alpha = RootOf(irr34) mod 3) ;
```

$$\alpha$$

- La procédure **rnd3** génére un entier modulo 3 pseudo-aléatoire.

```
> rnd3 := rand(0..2) :
> seq(rnd3(), i = 1..5) ;
```

$$0,\ 2,\ 0,\ 2,\ 1$$

- La procédure **rnd34** génère un élément pseudo-aléatoire de GF(3^4).

```
> rnd34 := () -> add(rnd3()*alpha^i, i=0..3) :
> seq(rnd34(), i = 1..5) ;
```

$$2 + 2\,\alpha + 2\,\alpha^2 + \alpha^3,\ 1 + \alpha,\ 2 + 2\,\alpha + \alpha^2,\ 2\,\alpha^2,\ \alpha^2$$

- La matrice A est une matrice 3x3 pseudo-aléatoire à coefficients dans GF(3^4).

```
> A := matrix(3, 3, rnd34) ;
```

$$A := \begin{bmatrix} 1 + 2\,\alpha^2 + 2\,\alpha^3 & 2 + 2\,\alpha + 2\,\alpha^3 & 2 + 2\,\alpha^2 + 2\,\alpha^3 \\ 2\,\alpha^2 & 2 + \alpha + \alpha^2 & 1 + \alpha^3 \\ 2 + 2\,\alpha + \alpha^3 & 1 + \alpha^2 & \alpha + 2\,\alpha^2 \end{bmatrix}$$

- Idem pour un vecteur second membre.

```
> b := vector(3, rnd34) ;
```

$$b := \left[\alpha^3,\ \alpha^3,\ 2 + 2\,\alpha^2\right]$$

- Linsolve(...) mod 3 permet de résoudre dans GF(3^4).

```
> x := Linsolve(A,b) mod 3 ;
```

$$x := \left[\alpha^3 + 2\,\alpha^2 + 2,\ \alpha + \alpha^2,\ 2\right]$$

- Vérification. Calcul de $A\,x - b$.

```
> zerov := evalm(A &* x - b) ;
```

$$zerov := \Big[(1+2\,\alpha^2+2\,\alpha^3)\,(\alpha^3+2\,\alpha^2+2)+(2+2\,\alpha+2\,\alpha^3)\,(\alpha+\alpha^2)+4+4\,\alpha^2+3\,\alpha^3,$$
$$2\,\alpha^2\,(\alpha^3+2\,\alpha^2+2)+(2+\alpha+\alpha^2)\,(\alpha+\alpha^2)+\alpha^3+2,$$
$$(2+2\,\alpha+\alpha^3)\,(\alpha^3+2\,\alpha^2+2)+(1+\alpha^2)\,(\alpha+\alpha^2)+2\,\alpha+2\,\alpha^2-2\Big]$$

- Les termes du vecteur obtenu ne sont pas « réduits » à leur forme canonique dans $\mathrm{GF}(3^4) = F_3[\alpha]$. Pour obtenir la réduction.

```
> map(item -> Expand(item) mod 3, zerov) ;
```

$$[0,\ 0,\ 0]$$

Références

[Bl-Ga] S. R. Blackburn et S. D. Galbraith, *Cryptanalysis of a cryptosystem based on Drinfeld modules*, (manuscript, 2003)

[Bour] Bourbaki N. *Algèbre, Chap.8 . "Modules et anneaux semi-simples"*, Masson, Paris 1981.

[Cas] J. W. S. Cassels *Lectures on elliptic curves*, London mathematical society Student text 24

[CKPS] N. Courtois, A. Klimov, J. Patarin et A. Shamir, *Efficient algorithms for solving overdefined systems of multivariate polynomial equations*, LNCS 1807 pp. 392-407, 2000

[CP] M. Courtieu et A.A. Panchishkin, *Non-Archimedean L-Functions and Arithmetical Siegel Modular Forms*, LNM 1471 (2nd ed.) 01.09.2003, ISBN 3-540-40729-4.

[De-Hu] Deligne P. et Husemöller D., *Survey of Drinfel'd modules*, Current Trends in Arithmetical Algebraic Geometry, Contemporary Mathematics, 67 (1987), 25 - 91

[Di-He] Diffie, W. et Hellman, M.E., *New directions in cryptography*, IEEE Trans. Inform. Theory, 22 (1976), 644-654

[Dr1] V.G.Drinfeld *Elliptic modules*, Math.USSR-Sbornik,23,1976, 561-592

[Dr2] V.G.Drinfeld, *Elliptic modules, II*, Math.USSR-Sbornik, 31, 1977, 159-170

[ElG1] ElGamal, T., *On computing logarithms over finite fields*, Advances in cryptology – CRYPTO '85 (Santa Barbara, Calif., 1985), 396–402, Lecture Notes in Comput. Sci., 218, Springer, Berlin, 1986

[ElG2] ElGamal, T., *A public key cryptosystem and a signature scheme based on discrete logarithms*, Advances in cryptology (Santa Barbara, Calif., 1984), 10–18, Lecture Notes in Comput. Sci., 196, Springer, Berlin, 1985

[Faug99] J. C. Faugère, *A new efficient algorithm for computing Groebner bases (F_4)*, Journal of pure and applied algebra 139 (1999) 61-88

[Faug] J. C. Faugère, *A new efficient algorithm for computing Groebner bases without reduction to zero (F_5)*, V1.2

[Faug03] J. C. Faugère, *Algebraic cryptanalysis of HFE using Groebner bases*, Rapport de recherche numero 4738, février 2003

[Ge] Gekeler E.-U., *On finite Drinfeld modules*, J. of Algebra, 141 (1991), 187-203

[GLPR3] R. Gillard, F. Leprevost, A. Panchishkin et X. Roblot, *Utilisation des modules de Drinfeld en cryptologie*, C R Acad. Sci. Paris, Théorie des nombres, Ser. I, 336, pp. 879-882 (2003)

[GLPR] R. Gillard, F. Leprévost, A. Panchishkin et X.-F. Roblot, *A new public-key cryptosystem based on Drinfeld modules* (En préparation), 2004

[Go1] Goss, D., *The algebraist's upper half-plane*, Bull Aler. Math. Soc. 2, no.2 (May 1980) 391-415

[Go2] Goss, D., *L-series of t-motives and Drinfeld modules*, The Arithmetic of function fields, D.Goss et al. (Eds), Proc. of the workshop at Ohio State University, 1991, Walter de Gruyter 1992, 313-402

[Hay] Hayes, D.R., *A brief introduction to Drinfeld modules*, The Arithmetic of function fields, D.Goss et al. (Eds), Proc. of the worshop at Ohio State University, 1991, Walter de Gruyter 1992

[Ki-Sh] A. Kipnis et A Shamir, , *Cryptanalysis of the HFE public key cryptosystem by relinearisation*, LNCS 1666, pp. 19-30, 1999

[Kob80] Koblitz, N., $p-$adic analysis : a short course on recent work. London Math. Soc. Lecture Note Ser., London : Cambridge Univ. Press (1980).

[Kob84] Koblitz, N., Introduction to elliptic curves and modular forms. New York : Springer Verlag, 1984.

[Kob87] Koblitz, N., *A course of number theory and cryptography*, Graduate texts in mathematics 114, New York : Springer Verlag, 1987.

[La] Lang, S. , Algebra. Reading, Mass. : Addison–Wesley (1965). Zbl.211, 385.

[Le1] Lenstra, H.W., Jr., *Factoring integers with elliptic curves*, Ann. Math., 126, no. 3 (1987), 649-673

[Li-Ni] Rudolf Lidl et Harald Niederreiter, *Introduction to finite fields and their applications.* Addison–Wesley : Reading, 1983

[Ma-Pa] Manin Yu.I. et Panchishkin A.A., *Number Theory I : Introduction to Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49, Springer-Verlag, 1995, 303 p.

[Me] Menezes, A., *Elliptic curve public key cryptosystems*, Kluwer, 1993, 128 p.

[Pa93] Panchishkin A.A., *Algorithmes rapides pour factorisation des nombres et des polynômes, tests de primalité, courbes elliptiques et modules de Drinfeld*, Séminaire de Théorie des nombres (Caen), Fascicule de l'Année 1993-94. p.1-10.

[Pey] Emmanuel Peyre, *Corps finis et courbes elliptiques.* DESS Cryptologie, sécurité et codage d'information, Modules A1A et A1B, Grenoble, 2002, pp. 1-128

[Po] Potemine I.Yu., *Arithmétique des corps globaux des fonctions et géométrie des schémas modulaires de Drinfeld*, Thèse de Doctorat, Institut Fourier `http ://www-fourier.ujf-grenoble.fr/THESE/ps/tpotemine97.ps.gz`, (Grenoble), 1997

[RSA] R. L. Rivest, A. Shamir et L. M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, CACM,21,1978, 120–126

[Sca] T. Scanlon, *Public key cryptosystems based on Drinfeld modules are insecure*, Journal of Cryptology, 14, 2001, 225-230

[Silv] J. H. Silverman *The arithmetic of elliptic curves*, Graduate texts in mathematics 106, Springer-Verlag

[IEEE] IEEE Standards, *Group P1363 : Standard Specification for Public-Key Cryptography*, page internet : `http ://grouper.ieee.org/groups/1363` , 1999

[Shou] V. Shoup, *NTL : A Library for doing Number Theory*, page internet : `http ://shoup.net/ntl/`, 2002,

[Stein] William Stein, *An Explicit Approach to Number Theory* (à paraître, voir page internet : `http ://modular.fas.harvard.edu/edu/Fall2001/124/lectures`).

[Tak] Takahashi T., *Good reduction of elliptic modules*, J. Math. Soc. Japan, 34 (1982), 475-487

[Wei74] Weil A., Basic Number Theory. 3rd ed. Berlin–Heidelberg–New York : Springer–Verlag, 1974.

Institut Fourier,
B.P.74, 38402 St.–Martin d'Hères,
FRANCE