Rapport de stage:
Extensions abéliennes de corps locaux et globaux

Olaf Kwiatkowski
Encadrant: Luis Garcia

18 août 2024

Table des matières

1 Introduction

1.1 Contexte

L'objectif de ce stage est de découvrir certaines façons de décrire de façon explicite la théorie des extensions abéliennes de certains corps. Savoir décrire ces extensions est l'objectif de la théorie des corps de classes que l'on introduit dans ce qui suit.

Nous commencerons par un exemple connu. Soit K un corps. Soit L/K une extension de K. On rappelle que l'on définit le groupe de Galois de l'extension $\mathrm{Gal}(L/K)$ comme étant le groupe des automorphismes de corps σ de L tels que $\sigma(x) = x$ pour $x \in K$. On rappelle qu'une extension finie L/K est galoisienne si $\#\,\mathrm{Gal}(L/K) = [L : K]$. Si l'extension L/K n'est pas finie, on dira qu'elle est **galoisienne** si c'est une union d'extensions finies galoisiennes. On rappelle qu'une extension L/K est **abélienne** si elle est galoisienne et que le groupe $\mathrm{Gal}(L/K)$ est abélien.
La théorie des corps de classes répond aux questions que l'on pourrait se poser à propos de ces extensions :
- Peut-on décrire toutes les extensions abéliennes d'un corps donné K ?
- Considérons K^{ab} l'union de toutes les extensions abéliennes de K. Que vaut le groupe de Galois $\mathrm{Gal}(K^{ab}/K)$, et quelles sont ses quotients finis ?

Pour illustrer cette théorie, commençons par un exemple célèbre. Soit $n \in \mathbb{N}^\times$ un entier naturel non nul. on note ζ_n une racine primitive n-ième de l'unité. Alors $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est une extension galoisienne, appélée une **extension cyclotomique**. Par ailleurs $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$, donc l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est abélienne. On dispose du résultat suivant :

Théoreme 1.1. *(Kronecker-Weber)*
Toute extension finie abélienne de $\mathbb{Q}$ est incluse dans une extension cyclotomique de $\mathbb{Q}$.

En particulier, nous avons donc $\mathbb{Q}^{ab} = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$. Ceci permet également le calcul de $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \prod_{p \text{ premier}} \mathbb{Z}_p^\times$, où les anneaux $\mathbb{Z}_p$ sont décrits plus tard dans ce rapport. Avec plus de travail, on peut même décrire explicitement l'isomorphisme ci-dessus.

Qu'en est-il du cadre général ? Tout d'abord la théorie des corps de classe se restreint dans un premier temps à l'étude de deux types de corps seulement : les corps locaux, et les corps globaux. Obtenir des résultats plus généraux est difficile. Dans ces cas la théorie des corps de classes répond entièrement aux questions posées ci-dessus dans ces deux cas. Cependant les démonstrations des théorèmes fondamentaux de cette théorie font appels à des arguments abstraits et des calculs cohomologiques. En particulier, ces preuves ne donnent pas de descriptions explicites des extensions abéliennes d'un corps comme dans la théorie de $\mathbb{Q}$. C'est à la question de la description explicite de ces extensions que s'intéresse ce rapport.

Nous savons aujourd'hui décrire les extensions abéliennes d'un corps dans quelques cas particuliers. Tout d'abord pour ce qui est des corps de nombre, nous savons décrire les extensions abéliennes de $\mathbb{Q}$ comme nous venons de le voir, mais aussi des extensions quadratiques imaginaires $\mathbb{Q}(\sqrt{-d})$, où d est un entier positif sans facteurs carrés. La théorie fait intervenir les courbes elliptiques ainsi que la multiplication complexe, mais nous ne décrirons pas cette théorie dans ce rapport. Le cas des corps de nombres généraux est encore un problème ouvert. Nous avons également une description satisfaisante dans le cas des corps locaux, ainsi que pour pour les corps

globaux de caractéristique $p > 0$. Ce sont ces théories que l'on propose de développer dans ce rapport.

1.2 Déroulé du stage

J'ai effectué mon stage à Londres, pour une durée de 3 mois, du 26 Avril 2024 au 24 Juillet 2024 à l'University College de Londres (UCL). J'y étais encadré par Luis Garcia.

J'ai commencé mon stage en suivant le livre *Corps locaux* de Jean Pierre Serre afin de me familiariser avec les notions de base de la théorie algébrique des nombres, à savoir les anneaux de Dedekind, la ramification des idéaux premiers ainsi que l'étude des propriétés de base des corps locaux. J'ai ensuite pu commencer à lire les papiers présentant les théories des extensions abéliennes explicites que je développe dans la suite, en commançant par la théorie de Lubin-Tate. Avant de poursuivre avec les extensions explicites de corps globaux j'ai tout de même eu besoin d'apprendre les théorèmes fondamentaux de la théorie des corps de classe. Cela m'a permis par la suite de discuter avec mon encadrant de multiples sujets proches qui apparaissent dans ces papiers, notamment des modules de Drinfeld, ainsi que de généralisations qui demandent une connaissance de la géométrie algébrique que je ne possède pas pour le moment.

Je remercie Luis Garcia pour ces discussions que nous avons eu, ainsi que le département de mathématiques de l'UCL pour m'avoir accueilli durant ces 3 mois.

2 Théorie de Lubin-Tate

Dans cette section nous présentons la théorie de Lubin-Tate, qui est une théorie permettant de construire de façon explicite les extensions abéliennes de corps locaux. Nous commençons donc par définir les corps locaux. On trouvera les preuves de toutes les propositions de cette section dans le livre de Serre [6]

2.1 Corps Locaux

Nous introduisons dans cette section les corps locaux ainsi que certaines de leurs propriétés qui nous seront utiles dans la suite.

Définition 2.1. Soit K un corps. Une **valuation discrète** sur K est un morphisme de groupe surjectif :

$$v : K^\times \twoheadrightarrow \mathbb{Z}$$

verifiant :

$$v(a+b) \geq \inf(v(a), v(b)).$$

Soit (K, v) un corps muni d'une valuation discrète. On note $A := \{x \in K : \ v(x) \geq 0\}$. par les propriétés de v, A est un anneau. Il s'agit en fait d'un anneau principal et local, c'est à dire qu'il dispose d'un unique idéal premier. Cet idéal est $\mathfrak{m} = \{x \in K \ v(x) > 0\}$. Il est engendré par un élément π quelconque de valuation 1. On appelle π une **uniformisante** de A. Un tel anneau est appelé un **anneau de valuation discrète**. On pose aussi $k = A/\mathfrak{m}$. Il s'agit d'un corps qu'on appelle le **corps résiduel** de A.

Une valuation sur K définit une valeur absolue non archimédienne sur K dont on rappelle la définition ci-dessous :

Définition 2.2. Soit K un corps. Une **valeur absolue non archimédienne** sur K est une application $|\cdot| : K \to \mathbb{R}_+$ telle que :
(i) $|x| = 0 \Rightarrow x = 0$ pour $x \in K$,
(ii) $|xy| = |x||y|$ pour $x, y \in K$,
(iii) $|x + y| \leq \sup(|x|, |y|)$ pour $x, y \in K$.

Une valuation non archimédienne sur K définit une valeur absolue non archimédienne sur K. Pour cela on fixe $a \in \mathbb{R}_+$ tel que $0 < a < 1$, puis on définit $|\cdot|$ par la formule :

$$|x| = \begin{cases} a^{v(x)} \text{ si } x \neq 0, \\ 0 \text{ si } x = 0. \end{cases}$$

En particulier ceci définit une topologie métrique sur K.

Exemple. 1. Soit p un nombre premier. Il existe une valuation discrète sur $\mathbb{Z}$, définie par $v_p(a) = \sup\{k \in \mathbb{N} : \ p^k | a\}$ pour $a \in \mathbb{Z}^\times$ et prolongée à $\mathbb{Q}$ par $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ pour $a, b \in \mathbb{Z}^\times$. L'anneau de valuation discrète correspondant est le localisé $\mathbb{Z}_{(p)} = \{\frac{a}{b} : \ a, b \in \mathbb{Z}, \ p \nmid b\}$. Dans ce cas la valeur absolue induite par v_p est notée $|\cdot|_p$, et on utlise la normalisation $|x|_p = p^{-v_p(x)}$.

Plus généralement, fixons K un corps de nombres, et notons $\mathcal{O}_K$ son anneau des entiers. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$. Les propriétés générales de ces anneaux assurent que la fonction définie par $v_\mathfrak{p}(a) = \sup\{k \in \mathbb{N} : \ a \in \mathfrak{p}^k\}$ est une valuation discrète sur $\mathcal{O}_K$.

2. Soit q une puissance d'un nombre premier p. On note $\mathbb{F}_q$ un corps fini à q élément. On considère le corps $K = \mathbb{F}_q(T)$. On peut définit une valuation discrète sur K de la même façon que pour $\mathbb{Z}$. On fixe un polynôme irréductible $P \in \mathbb{F}_q[T]$, et on définit la valuation discrète v_P par la même formule que ci-dessus. Il existe cependant une dernière valuation discrète sur K qui ne correspond à aucun idéal premier de $\mathbb{F}_q[T]$. Il s'agit de la valuation v_∞ définie par $v_\infty(F) = -\deg(F)$.

Comme pour les corps de nombres, on peut généraliser ces valuations pour les extensions finies de $\mathbb{F}_q(T)$.

Soit K un corps muni d'une valuation v. K est alors un espace métrique, et on peut se demander s'il est complet pour la distance induite par cette valuation. Ce n'est en général pas le cas. On peut donc considérer le complété K_v de K pour la valuation v. On peut vérifier que l'addition et la multiplication de K se prolonge de façon continue à K_v, ce qui fait de K_v un corps topologique. La valuation discrète v se prolonge également à K_v. On note $\mathcal{O}_K$ l'anneau de valuation discrète correspondant à K.

Proposition 2.3. *Le corps résiduel k_v de $\mathcal{O}_{K_v}$ est égal au corps résiduel k de $\mathcal{O}_K$ pour la valuation v.*

Démonstration. On a un morphisme de corps induit par l'inclusion $k \to k_v$. Il suffit de montrer qu'il est surjectif. Soit $a \in \mathcal{O}_{K_v}$ un représentant d'un élément de k_v. Par densité de K dans K_v, il existe un élément $a' \in K$ tel que $v(a' - a) \geq 1$. On en déduit que $a' \in \mathcal{O}_K$ et que a' et a représentent la même classe de k_v. D'où $k = k_v$. □

Exemple. 1. Lorsque p est un nombre premier, on peut vérifier que le corps $\mathbb{Q}$ n'est pas complet pour la valuation v_p. Le complété de $\mathbb{Q}$ pour la valuation v_p est noté $\mathbb{Q}_p$, et on l'appelle le **corps des nombres p-adiques**. Son anneau des entiers est noté $\mathbb{Z}_p$, et est appelé **l'anneau des entiers**

p-adiques. Le corps résiduel de $\mathbb{Z}_p$ est par la proposition 2.3 égal à $\mathbb{F}_p$.

Dans le cas plus général d'un corps de nombre K, les complétés de K pour des valuations discrètes sont des extensions finies de $\mathbb{Q}_p$.

2. Lorsque $K = \mathbb{F}_q(T)$, si P est un polynôme irréductible de degré d, on peut montrer que K_{v_P} est isomorphe à $\mathbb{F}_{q^d}((X))$ le corps des série entières formelles à coefficients dans $\mathbb{F}_{q^d}$, et où X a valuation 1. Le corps résiduel de K_{v_P} est $\mathbb{F}_{v_P}$.

Proposition 2.4. *Soit K un corps complet pour une valuation discrète v. Il y a équivalence entre :*
(i) K est localement compact,
(ii) $\mathcal{O}_K$ est compact,
(iii) le corps résiduel k de K est fini.

Définition 2.5. Un **corps local** est un corps K complet et localement compact pour une valuation discrète.

Exemple. Les corps mentionnés dans l'exemple précédent sont des corps locaux.

Nous aurons besoin pour la suite de quelques propriétés des corps locaux et de leurs extensions :

Proposition 2.6. *Soit K un corps local, et L/K une extension finie. Il existe une unique valuation sur L prolongeant celle de K, et L est un corps local pour cette valuation. De plus $\mathcal{O}_L$ est finiement engendré en tant que $\mathcal{O}_K$-module.*

Proposition 2.7. *Soit K un corps local. Soit q le cardinal de k. Soit l/k une extension finie de degré d du corps résiduel de K. Il existe à unique isomorphisme près une unique extension de degré d de K dont le corps résiduel est l. Une telle extension est appelé une extension $nonramifie$ de K. De plus une inclusion entre corps $l \subset m$ induit une inclusion correspondante $L \subset M$. Enfin l'extension L/K est galoisienne de groupe de Galois $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k)$. De plus cet isomorphisme est induit par l'action de $\mathrm{Gal}(L/K)$ sur $\mathcal{O}_L$, à l'aide de la projection $\mathcal{O}_L \to l$.*

En particulier on peut former l'union de ces corps K^{nr}, que l'on appelle **l'extension non ramifiée maximale** de K (la raison de cette dénomination provient de la théorie de la ramification). On conclut cette section en décrivant l'extension K^{nr} :

Proposition 2.8. *Soit K un corps local dont le corps résiduel a pour caractéristique $p > 0$. Soit n un entier premier à p. Soit ζ_n une racine primitive n-ième de l'unité. Alors l'extension $K(\zeta_n)/K$ est une extension non ramifiée de K dont l'extension résiduelle est $k(\zeta_n)/k$.*

On en déduit que K^{nr} est obtenu par l'union $K^{nr} = \bigcup_n K(\zeta_n)$, où l'union porte sur les entiers n premiers à p.

2.2 Extensions de Lubin-Tate

Les constructions de cette section proviennent de [5].
Soit K un corps local, dont la valuation est notée v_K. Nous notons $\bar{K}$ le corps résiduel de K, q son cardinal, $\mathcal{O}_K$ l'anneau des entiers de K, et $\mathfrak{m}_K$ son idéal maximal. Soit K^{ac} une clôture algébrique de K. On notera aussi $\mathfrak{M} = \{x \in K^{ac} : \ |x| < 1\}$. Si A est un anneau commutatif, on note $A[[X_1, \cdots, X_n]]$ l'anneau des séries entières formelles en n indéterminées à coefficients dans A.

La théorie de Lubin-Tate est inspirée de la théorie des extensions abéliennes des corps quadratiques imaginaires. Dans cette théorie nous avons un groupe abélien, en l'occurence une courbe elliptique, sur laquelle agit l'anneau des entiers du corps de base, lui procurrant une structure de module. On considère ensuite des points de torsion pour obtenir des extensions abéliennes.

Nous allons de façon similaire cette section définir une structure de $\mathcal{O}_K$-module sur $\mathfrak{M}$, et définir des extensions abéliennes de K à l'aide de ses points de torsions. Nous aurons d'abord besoin de définir les séries entières de Frobenius. Fixons pour cela une uniformisante π de K.

Définition 2.9. Une série entière de Frobenius (pour π) est une série entière $\phi(X) \in \mathcal{O}_K[[X]]$ telle que $\phi(X) = \pi X + \mathcal{O}(X^2)$, et $\phi(X) \equiv X^q \bmod \pi\mathcal{O}_K[[X]]$.

Exemple. 1. On peut considérer $\phi(X) = \pi X + X^q$.

Nous avons besoin d'un lemme technique avant de continuer :

Lemme 2.10. *Soit ϕ et ψ deux séries entières de Frobenius pour les uniformisantes π et π' respectivement. Soit $F_1(X_1, \cdots, X_n) = a_1X_1 + \cdots a_nX_n \in \mathcal{O}_K[X_1, \cdots, X_n]$ un polynôme linéaire en n indéterminées. Alors il existe une unique série entière formelle $F(X_1, \cdots, X_n) \in \mathcal{O}_K[[X_1, \cdots, X_n]]$ telle que :*
1. *$F(X_1, \cdots, X_n) = F_1(X_1, \cdots, X_n) +$ termes de degré au moins 2,*
2. *$\phi(F(X_1, \cdots, X_n)) = F(\psi(X_1), \cdots, \psi(X_n))$.*

Nous pouvons à présent définir la structure de groupe abélien sur $\mathfrak{M}$ sur laquelle nous définirons la structure de $\mathcal{O}_K$-module.

Proposition 2.11. *Soit $\phi(X)$ une série entière de Frobenius pour π. Il existe une unique série entière $F_\phi(X, Y) \in \mathcal{O}_K[[X, Y]]$ telle que :*
(i) $F_\phi(X, 0) = X$ et $F_\phi(0, Y) = Y$. En particulier $F_\phi(X, Y) = X+Y+$termes de degré au moins 2,
(ii) $F_\phi(X, Y) = F_\phi(Y, X)$ (commutativité),
(iii) $F_\phi(F_\phi(X, Y), Z) = F_\phi(X, F_\phi(Y, Z))$ (associativité),
(iv) $\phi(F_\phi(X, Y)) = F_\phi(\phi(X), \phi(Y))$.

Démonstration. L'existence et unicité d'une série entière vérifiant (iv) et la deuxième partie de (i) est assurée par le lemme 2.10. Pour vérifier (ii), il suffit de remarquer que $F'_\phi(X, Y) := F_\phi(Y, X)$ vérifie les points 1 et 2 du lemme, et donc par unicité $F'_\phi = F_\phi$. Le point (iii) se vérfie de la même façon. pour la première partie du point (i), on pose $H(X) = F_\phi(X, 0) = X + \sum_{n\geq 2} c_iX^i$. On utilise alors l'associativité :

$$H(X) = F_\phi(X, 0) = F_\phi(X, F_\phi(0, 0)) = F_\phi(F_\phi(X, 0), 0) = H(H(X)) = H(X) + \sum_{n\geq 2} c_iH(X)^i.$$

On en déduit successivement en regardant les termes de plus bas degré $c_i = 0$ pour $i \geq 2$. On utilise la commutativité pour obtenir aussi $F_\phi(0, Y) = Y$. □

Définition 2.12. On appelle F_ϕ la **loi de groupe formelle de Lubin-Tate** relative à ϕ.

Exemple. Lorsque $\phi(X) = \pi X + X^q$, on appelle F_ϕ la loi de groupe de Lubin-Tate spéciale pour π. On remarque que si $\mathrm{char}(K) > 0$, $F_\phi(X, Y) = X + Y$ convient. En charactéristique nulle, cette loi de groupe est plus difficile à calculer, mais on peut récursivement obtenir un nombre fini de termes à l'aide de la preuve du lemme 2.10.

Remarquons que si $x, y \in \mathfrak{M}$, alors la série entière $F_\phi(x, y)$ converge vers un élément de $\mathfrak{M}$. Ainsi F_ϕ définit une loi de monoïde commutatif sur $\mathfrak{M}$, que l'on note $+_{F_\phi}$. On peut également montrer qu'il s'agit d'une loi de groupe, c'est à dire que tout élément de $\mathfrak{M}$ possède un opposé. Il reste maintenant à définir une structure de $\mathcal{O}_\mathcal{K}$-module sur $\mathfrak{M}$.

Proposition 2.13. *Pour tout $a \in \mathcal{O}_K$, il existe une unique série formelle $[a]_\phi(X) \in \mathcal{O}_K[[X]]$ telle que :*
(i) $[a]_\phi(X) = aX + \mathcal{O}(X^2)$,
(ii) $\phi([a]_\phi(X)) = [a]_\phi(\phi(X))$.
De plus si $b \in \mathcal{O}_K$,
(iii) $F_\phi([a]_\phi(X), F_\phi$,
(iv) $[a + b]_\phi(X) = F_\phi([a]_\phi(X), [b]_\phi(X))$,
(v) $[ab]_\phi(X) = [a]_\phi([b]_\phi(X))$.

Remarque. On peut vérifier par les propriétés caractérisant $[a]_\phi$ que :
- $[1]_\phi(X) = X$
- $[\pi]_\phi(X) = \phi(X)$, et donc $[\pi^n]_\phi(X) = \phi^n(X)$ (où l'exposant du terme de droite dénote la composition).

De nouveau il suffit d'utiliser l'existence et l'unicité du lemme 2.10 pour prouver cette proposition. Par la proposition ci-dessus, on obtient un morphisme d'anneaux :

$$\begin{aligned} \mathcal{O}_K &\longrightarrow \mathrm{End}(\mathfrak{M}) \\ a &\longmapsto [a]_\phi, \end{aligned}$$

ce qui définit une structure de $\mathcal{O}_K$-module sur $\mathfrak{M}$ par $a \cdot z = [a]_\phi(z)$ pour $a \in \mathcal{O}_K$, $z \in \mathfrak{M}$.

Nous pouvons à présent définir les extensions de Lubin-Tate :

Définition 2.14. Soit ϕ une série entière de Frobenius pour π. On définit pour $n \geq 0$:

$$\mathcal{F}_n = \{z \in \mathfrak{M} : \ \phi^n(z) = \pi^n \cdot z = 0\}. \tag{1}$$

Il s'agit des modules de π-torsion du $\mathcal{O}_K$-module $\mathfrak{M}$. On définit alors les **extensions de Lubin-Tate** :

$$K_n = K(\mathcal{F}_n), \qquad\qquad K_\infty = \bigcup_{n \geq 1} K_n. \tag{2}$$

Remarque. Avec plus de travail, il est possible de montrer que les extensions K_n sont indépendantes du choix de la série entière de Frobenius ϕ. En utilisant la loi de groupe de Frobenius spéciale, on voit que les K_n sont des extensions galoisiennes de K. En effet K_n/K est normale au vu de la définition de K_n, et est séparable car la dérivée de ϕ^n est égale à π^n (constante) si $\mathrm{char}(K) > 0$.

On peut également montrer que pour ce choix de série entière de Frobenius toutes les racines de $\phi^n(X)$ sont dans $\mathfrak{M}$. En particulier $\#\mathcal{F}_n = q^n$.

Nous devons à présent montrer que ces extensions sont abéliennes. Pour cela on s'inspire de la théorie des extensions cyclotomiques. Pour rappel en étudiant les extensions cyclotomiques, on fixe un générateur ζ_n du Z-module des racines n-ièmes de l'unité, et on remarque que si σ est un automorphisme de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, $\sigma(\zeta_n)$ est encore une racine primitive n-ième de l'unité, donc il existe

un entier m unique modulo n et premier à n tel que $\sigma(\zeta_n) = \zeta_n^m$. Nous allons de façon similaire construire un morphisme injectif :

$$\chi_n : \mathrm{Gal}(K_n/K) \longrightarrow (\mathcal{O}_K/\mathfrak{m}_K^n)^\times.$$

Considérons $\sigma \in \mathrm{Gal}(K^{ac}/K)$. Soit $z_1, z_2 \in \mathfrak{M}$. On a les formules :

$$\sigma(z_1 +_{F_\phi} z_2) = \sigma(z_1) +_{F_\phi} \sigma(z_2),$$
$$\sigma(a \cdot z_1) = a \cdot \sigma(z_1) \text{ pour } a \in \mathcal{O}_K.$$

On en déduit que σ agit $\mathcal{O}_K$-linéairement sur $\mathcal{F}_n$. Nous avons à présent besoin du lemme suivant :

Lemme 2.15. *$\mathcal{F}_n$ est un $\mathcal{O}_K/\mathfrak{m}_K^n$-module libre de rang 1.*

Démonstration. Considérons $z \in \mathcal{F}_n \backslash \mathcal{F}_{n-1}$. Alors on obtient un morphisme injectif de $\mathcal{O}_K$-modules :

$$\begin{aligned} \mathcal{O}_K/\mathfrak{m}_k^n &\longrightarrow \mathcal{F}_n \\ a &\longmapsto a \cdot z, \end{aligned}$$

puis par égalité des cardinaux, il s'agit d'un isomorphisme. □

A présent puisque $\mathrm{Gal}(K_n/K)$ agit $\mathcal{O}_K/\mathfrak{m}_K^n$-linéairement sur $\mathcal{F}_n$, pour tout $\sigma \in \mathrm{Gal}(K_n/K)$ il existe un unique $\chi_n(\sigma) \in (\mathcal{O}_K/\mathfrak{m}_k^n)^\times$ tel que :

$$\sigma(z) = \chi_n(\sigma) \cdot z \text{ pour tout } z \in \mathcal{F}_n. \tag{3}$$

Ceci définit une application $\chi_n : \mathrm{Gal}(K_n/K) \to (\mathcal{O}_K/\mathfrak{m}_K^n)^\times$. On vérifie par 3 qu'il s'agit d'un homomorphisme de groupes. Il également injectif car $K_n = K(\mathcal{F}_n)$.

On en déduit que $\mathrm{Gal}(K_n/K)$ s'identifie à un sous groupe de $(\mathcal{O}_K/\mathfrak{m}_k^n)^\times$, qui est abélien. On en déduit que l'extension K_n/K est abélienne.

Remarque. On peut en fait montrer que χ_n est un isomorphisme.

Définition 2.16. On définit $K^{LT} := K_\infty \cdot K^{nr}$. Il s'agit d'une extension abélienne de K.

Théoreme 2.17. *On a $K^{LT} = K^{ab}$. Autrement dit toute extension abélienne de K est incluse dans K^{LT}.*

Remarque. On pourrait montrer que les extensions K_∞ et K^{nr} sont linéairement disjointes. Ceci nécessiterait cependant de développer la théorie de la ramification. On obtient alors $\mathrm{Gal}(K^{ab}/K) \simeq \mathrm{Gal}(K_\infty/K) \times \mathrm{Gal}(K^{nr}/K)$. En poursuivant les calculs, on pourrait montrer que $\mathrm{Gal}(K^{ab}/K) \simeq \hat{\mathcal{O}_K^\times} \times \hat{\mathbb{Z}}$, qui est un groupe obtenu à partir de $\mathcal{O}_K^\times \times \mathbb{Z}$ par un procédé appelé la complétion profinie.

2.3 Exemple des extensions abéliennes de $\mathbb{Q}_p$

On illustre dans cette section les concepts développés plus tôt au cas où $K = \mathbb{Q}_p$. Dans ce cas on rappelle que $\mathcal{O}_K$ est noté $\mathbb{Z}_p$. On choisit naturellement p comme uniformisante. On rappelle que le corps résiduel de $\mathbb{Q}_p$ est $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Nous devons commencer par choisir une série entière de Frobenius pour p. On pourrait choisir $\phi(X) = pX + X^p$, mais nous choisirons ici plutôt $\phi(X) = (1+X)^p - 1$. L'intérêts est qu'on peut calculer F_ϕ aisément dans ce cas :

Proposition 2.18. *La loi de Frobenius spéciale relative à ϕ est $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$.*

Démonstration. On voit que la propriété (i) de la proposition 2.11 est vérifiée. Il suffit de calculer :

$$\begin{aligned}\phi(F(X,Y)) &= ((1+X)(1+Y) - 1 + 1)^p - 1 \\ &= (1+X)^p(1+Y)^p - 1 \\ &= F(\phi(X), \phi(Y))\end{aligned}$$

□

A présent on s'intéresse au groupe abélien $(\mathfrak{M}, +_F)$. On dispose en fait d'un isomorphisme :

$$\begin{aligned}(\mathfrak{M}, +_F) &\xrightarrow{\simeq} ((1+\mathfrak{M}), \times) \\ z &\mapsto 1 + z,\end{aligned}$$

ainsi on appelle $+_F$ la loi de groupe **multiplicative**. On utilise cet isomorphisme dans la suite. La structure de $\mathbb{Z}_p$-module sur $(1+\mathfrak{M})$ prolonge par continuité la structure de $\mathbb{Z}$-module (i.e de groupe abélien). En particulier :

$$p^n \cdot \zeta = \zeta^{p^n}.$$

Les points de p-torsion sont donc les racines p^n-ième de l'unité. par l'isomorphisme ci-dessus, on a donc :

$$\mathcal{F}_n = \{\zeta - 1 : \ \zeta^{p^n} = 1\}, \qquad\qquad K_n = \mathbb{Q}_p(\zeta_{p^n}).$$

On rappelle que $\mathbb{Q}_p^{nr}$ est obtenu en prenant l'union des extensions $\mathbb{Q}_p(\zeta_n)$, où n est un entier premier avec p. On obtient donc :

$$\mathbb{Q}_p^{LT} = \bigcup_{n \geq 1} \mathbb{Q}_p(\zeta_n).$$

D'où l'on déduit la version locale du théorème de Kronecker-Weber :

Théoreme 2.19. *(Kronecker-Weber local)*
Toute extension finie abélienne de $\mathbb{Q}_p$ est incluse dans une extension cyclotomique de $\mathbb{Q}_p$.

3 Extensions abéliennes de corps de fonctions globaux

Nous développerons dans cette section les idées permettant de décrire les extensions abéliennes de corps de fonctions globaux, c'est à dire des extensions finies de $\mathbb{F}_q(T)$. Nous nous concentrerons cependant sur le cas de $\mathbb{F}_q(T)$, où la théorie est encore plus explicite.

On verra par ailleurs que la théorie est de nouveau similaire à la théorie des extensions abéliennes des corps quadratiques imaginaires, ou encore à le théorie de Lubin-Tate. On définira une structure de module sur un objet algébrique, en l'occurrence une clôture algébrique K^{ac} du corps de base K. En l'occurence nous verrons que l'on peut conserver la structure additive de K^{ac} comme groupe abélien pour définir sa structure de module. On obtiendra les extensions abéliennes voulues en considérant les points de torsion de ce module.

3.1 Modules de Drinfeld

Pour une introduction plus complète à la notion de module de Drinfeld on renvoie à [2].

Soit K un corps de fonctions global. On note k le corps des constantes de K, c'est à dire le corps des éléments x de K dont toutes les valuations $v(x)$ sont positives. Par exemple lorsque $K = \mathbb{F}_q(T)$, on a $k = \mathbb{F}_q$. Il s'agit d'un corps fini de cardinal q en général.

On dispose de l'endomorphisme de Frobenius $X \mapsto X^q$. Soit L une extension de K. On considère l'anneau non commutatif $L[\tau]$ des polynômes en τ, en imposant la règle de multiplication $\tau a = a^q \tau$ pour $a \in L$. $L[\tau]$ est isomorphe en tant qu'anneau aux polynômes en l'endomorphisme de Frobenius, réprésenté par τ, et où la multiplication de l'anneau est définie par la composition des endomorphismes.

Fixons dans la suite une valuation v_∞ de K. On note A l'anneau des éléments de $x \in K$ tels que $v(x) \geq 0$ pour toutes les valuations v de K autres que v_∞. On note par ailleurs d_∞ le degré de l'extension k_∞/k, où k_∞ est le corps résiduel du complété de K pour la valuation v_∞.

Définition 3.1. Un **module de Drinfeld** sur L est un homomorphisme d'anneaux $\phi : A \to L[\tau]$ dont l'image n'est pas contenue dans les constantes L.

Remarque. Un module de Drinfeld $\phi : A \to L[\tau]$ définit une structure de A-module sur K^{ac}, en identifiant $\phi_x \in L[\tau]$ à un polynôme en l'endomorphisme de Frobenius, et en définissant $x \cdot z = \phi_x(z)$ pour $x \in A$ et $z \in K^{ac}$.

Soit $\partial : L[\tau] \to L$ l'application qui envoie un polynôme sur son terme constant. Alors la composée $\partial \circ \phi$ est un morphisme $A \to L$. Son noyau est un idéal premier de A. On supposera dans la suite que ce noyau est nul. On dit dans ce cas que ϕ est de **caractéristique générique**.

Proposition 3.2. *il existe un entier $r \geq 1$ tel que pour tout $x \in A$,*

$$\deg_\tau(\phi_x) = -r d_\infty v_\infty(x). \tag{4}$$

*On appelle cet entier r le **rang** du module de Drinfeld ϕ.*

Remarque. Soit $\mathbb{C}_\infty$ le complété d'une clôture algébrique de K_∞. Il s'agit d'un corps à la fois complet pour une valeur absolue non archimédienne, et d'un corps algébriquement clos. On peut montrer de façon générale l'existence de modules de Drinfeld de tout rang sur $\mathbb{C}_\infty$ par des méthodes analytiques. Les modules qui nous intéressent en particulier dans l'étude des extensions abéliennes de K sont les modules de Drinfeld de rang 1.

On mentionne avant de poursuivre un fait utilisé dans la suite. Soit F un corps local de caractéristique $p > 0$. Alors F contient son corps résiduel. En fait on a même un isomorphisme $F \simeq \mathbb{F}_q((T))$, où $\mathbb{F}_q$ est le corps résiduel de F, et T est un élément de valuation 1.

Supposons dans la suite que L est un corps parfait (ce qui est le cas par exemple si $L = \mathbb{C}_\infty$). On peut prolonger ϕ en un morphisme d'anneaux $\phi : K \to L((\tau^{-1}))$, l'anneau à division des séries de Laurent formelles en τ^{-1}, avec la règle de multiplication $\tau^{-1} a = a^{\frac{1}{q}} \tau^{-1}$. Par (4), cette application est continue si l'on munit K de la topologie induite par v_∞, et $L((\tau^{-1}))$ de la topologie induite par $-\deg_\tau$. On en déduit que ϕ se prolonge en un morphisme d'anneaux $\phi : K_\infty \to L((\tau^{-1}))$.

On peut à présent restreindre le morphisme étendu ϕ à $\mathbb{K}_\infty$, le corps résiduel de K_∞. Puisque les éléments de $\mathbb{K}_\infty$ sont de valuation nulle, on a un morphisme d'anneaux $\phi_{|\mathbb{K}_\infty} : \mathbb{K}_\infty \to L[[\tau^{-1}]]$, l'anneau des séries entières en τ^{-1}. En composant avec le morphisme qui envoie une série entière sur son terme constant, on obtient un morphisme de corps $\mathbb{K}_\infty \to L$, auquel on pensera comme à une inclusion.

Définition 3.3. On définit l'application $\mu_\phi : K_\infty \to L$ en posant pour $x \in K_\infty$ $\mu_\phi(x)$ comme étant le coefficient devant le premier terme (vis à vis de τ^{-1}) non nul de ϕ_x. Le premier terme de ϕ_x est donc $\mu_\phi(x)\tau^{-rd_\infty v_\infty(x)}$.

Si $x, y \in K_\infty$, on peut calculer le premier terme de $\phi_{xy} = \phi_x\phi_y$, pour obtenir :

$$\mu_\phi(xy) = \mu_\phi(x)\mu_\phi(y)^{\frac{1}{q^{rd_\infty v_\infty(x)}}}. \tag{5}$$

Remarquons alors que si μ_ϕ prend ses valeurs dans $\mathbb{K}_\infty$, μ_ϕ devient un morphisme de groupes $K_\infty \to \mathbb{K}_{infty}$. De plus vis-à-vis de l'inclusion précédemment définie, μ_{phi} se restreint à l'identité sur $\mathbb{K}_\infty^\times$.

Définition 3.4. On dit qu'un morphisme de groupes $\varepsilon K_\infty^\times \to \mathbb{K}_\infty^\times$ est une **fonction signe** si ε se restreint à l'identité sur $\mathbb{K}_\infty$.
Un module de Drinfeld ϕ est dit **normalisé** si la fonction μ_ϕ est prend ses valeurs dans $\mathbb{K}_\infty$.
Soit ε une fonction signe. Un module de Drinfeld est dit **ε-normalisé** s'il est normalisé et si la fonction $\mu_\phi : K_\infty \to \mathbb{K}_\infty$ est égale ε à un automorphisme de $\mathbb{K}_\infty$ près.

Remarque. Une fonction signe est déterminée par la valeur qu'elle prend en une uniformisante T de K_∞.

Dans la suite, fixons une fonction signe ε. Nous définissons maintenant les modules de Drinfeld qui nous intéressent dans la suite.

Définition 3.5. Un **module de Hayes** pour ε est une module de Drinfeld $\phi : A \to \mathbb{C}_\infty[\tau]$ ε-normalisé de rang 1.

Remarque. Nous avons mentionné précédemment que les modules de Drinfeld de rang 1 sur $\mathbb{C}_\infty$ existent. Il est également possible de "ε-normaliser" un module de Drinfeld. Ainsi les modules de Hayes existent, quel que soit le corps K avec lequel on travaille.

3.2 Module de Carlitz

Nous nous concentrons à présent sur le cas de $K = \mathbb{F}_q(T)$. Ce cas est traité par D. Hayes dans [1]. Dans ce cas la valuation v_∞ est définie par $v_\infty(x) = -\deg(x)$ pour $x \in K$. Alors $A = \mathbb{F}_q[T]$. Dans ce cas $d_\infty = 1$, et $\mathbb{K}_\infty$ est le corps des constantes $\mathbb{F}_q$. On définit la fonction signe ε par $\varepsilon(T^{-1}) = 1$. Pour que le module de Drinfeld que l'on définiera $\phi : A \to \mathbb{C}_\infty[\tau]$ soit un module de Hayes pour ε, on rappelle qu'il doit être de rang 1 et ε-normalisé. Par la propriété universelle de $\mathbb{F}_q[T]$, définir ϕ revient à définir l'image de T. Le fait que ϕ doit être de rang 1 se traduit par :

$$\deg_\tau(\phi_T) = \deg_T(T) = 1$$

et le fait que ϕ est ε-normalisé se traduit par le fait que le coefficient dominant de ϕ_T est égal à 1. Bien sûr le coefficient constant de ϕ_T est T car le module de Drinfeld est de caractéristique générique. Au final cela ne laisse qu'une possibilité : le module de Carlitz.

Définition 3.6. Le **module de Carlitz** est le module de Drinfeld $\phi : \mathbb{F}_q[T] \to K[\tau]$ défini par $\phi_T = T + \tau$.

Comme mentionné précédemment, ceci définit une structure de A-module sur K^{ac}. Avant de définir les extensions abéliennes que l'on souhaite, on mentionne le lemme suivant, qui provient du fait que ϕ est un module de Hayes pour ε :

Lemme 3.7. *Soit $M \in \mathbb{F}_q[T]$ un polynôme de degré d. Alors il existe des polynômes $f_{M,i}(T)$ tels que :*

$$\phi_M = \sum_{i=0}^{d} f_{M,i}(T)\tau^i. \tag{6}$$

De plus on a $f_{M,0}(T) = M$ et $f_{M,d}(T)$ est le coefficient dominant de M.

Démonstration. Tout d'abord par linéarité, il suffit de considérer le cas $M = T^d$. Il suffit alors de développer $(T + \tau)^d$, en tenant compte du fait que $\tau a = a^q \tau$ pour $a \in A$. On voit alors en regroupant les termes uniquement en T que $f_{T^d,0}(T) = T^d$, et en regroupant les termes en τ que $f_{T^d,d} = 1$. □

De nouveau en identifiant ϕ_M en un polynôme en X par la formule :

$$\phi_M = \sum_{i=0}^{d} f_{M,i}(T)X^{q^i}.$$

On remarque que ϕ_M est un polynôme séparable, car sa dérivée est constante égale à M. En particulier ϕ_M possède q^d racines dans K^{ac}.

Définition 3.8. Soit Λ_M le A-module des points de M-torsion de K^{ac} pour sa structure de A-module. Plus concrètement :

$$\Lambda_M = \{z \in K^{ac} : \ \phi_M(z) = 0\}.$$

Il s'agit d'un A-module de cardinal q^d.

de nouveau nous aurons besoin de comprendre l'action du groupe de Galois $\mathrm{Gal}(K^{ac}/K)$ sur ce module afin de montrer que les extensions que l'on construira à partir des Λ_M sont abéliennes. Comme dans le cas de la théorie de Lubin-Tate il faut comprendre la structure de A-module de Λ_M.

Proposition 3.9. *Supposons que $M = P^n$, où $P \in A$ est un polynôme irréductible de degré $d > 0$. Alors Λ_M est un A-module monogène.*

Démonstration. On prouve ce résultat par récurrence sur n. Commençons par le cas $n = 1$. Dans ce cas la structure de A-module sur Λ_M se factorise en une structure de $A/(P)$-espace vectoriel. On en déduit que Λ_M est un $A/(P)$-espace vectoriel de dimension $k \geq 1$. Or $\#\Lambda_M = q^d$, et $\#A/(P) = q^d$, donc k doit être égal à 1. Supposons à présent le résultat vrai au rang $n - 1$ pour $n \geq 2$. La multiplication par P définit une suite exacte courte :

$$0 \to \Lambda(P) \to \Lambda(P^n) \xrightarrow{P\cdot} \Lambda(P^{n-1}) \to 0$$

Soit μ est un générateur de $\Lambda(P^{n-1})$ en tant que A-module, et soit λ tel que $P \cdot \lambda = \mu$. Montrons que λ est un générateur de $\Lambda(P^n)$. Soit $z \in \Lambda(P^n)$. Par hypothèse il existe $R \in A$ tel que $R \cdot \mu = P \cdot z$, d'où $P \cdot (R \cdot \lambda - z) = 0$. On en déduit que $R \cdot \lambda - z \in \Lambda(P)$, or μ génère $\Lambda(P^{n-1})$ qui contient $\Lambda(P)$ d'où l'existence de $S \in A$ tel que $S \cdot \mu = R \cdot \lambda - z$. On obtient donc $z = (R - PS) \cdot \lambda$ et λ génère $\Lambda(P^n)$ comme voulu. □

A présent en décomposant le module de torsion Λ_M en ses modules de P-torsion, on obtient que Λ_M est un A-module monogène pour M quelconque.

Corollaire 3.10. *Soit $M \in A$ un polynôme de degré d. Λ_M est un $A/(M)$-module libre de rang 1.*

Démonstration. En considérant un générateur λ de Λ_M comme A-module, on obtient un morphisme surjectif de A-modules :

$$\begin{aligned} A &\longrightarrow \Lambda_M \\ P &\longmapsto P \cdot \lambda \end{aligned}$$

qui se factorise par $A/(M)$. Par égalité des cardinaux, il s'agit d'un isomorphisme. □

3.3 L'extension abélienne maximale de $\mathbb{F}_q(T)$

On considère dans la suite les extensions $K(\Lambda_M)$. Ce sont des extensions galoisiennes de K.

Nous pouvons à présent décrire l'action du groupe de Galois $\mathrm{Gal}(K(\Lambda_M)/K)$ sur Λ_M. Tout d'abord comme Λ_M est le lieu des zéros d'un polynôme à coefficient dans K, Λ_M est stable par $\mathrm{Gal}(K(\Lambda_M)/K)$. De plus on remarque que $\sigma \in \mathrm{Gal}(K(\Lambda_M)/K)$ agit A-linéairement sur Λ_M, i.e $\sigma(P(z)) = P(\sigma(z))$ si $P \in A$ et $z \in \Lambda_M$. Comme σ est un automorphisme du $A/(M)$-module libre de rang 1, il existe un polynôme $\chi_M(\sigma)$ unique modulo M et premier à M tel que pour tout $z \in \Lambda_M$:

$$\sigma(z) = \chi_M(\sigma) \cdot z.$$

On en déduit comme dans le cas des extensions de Lubin-Tate :

Proposition 3.11. *χ_M est un morphisme de groupes injectif :*

$$\begin{aligned} \chi_M : \mathrm{Gal}(K(\Lambda_M)/K) &\longrightarrow (A/(M))^\times \\ \sigma &\longmapsto \chi_M(\sigma). \end{aligned}$$

En particulier $\mathrm{Gal}(K(\Lambda_M)/K)$ s'identifie à un sous groupe de $(A/(M))^\times$, et $K(\Lambda_M)/K$ est une extension abélienne.

Remarque. On peut montrer qu'il s'agit d'un isomorphisme.

On note dans la suite K_T l'union des corps $K(\Lambda_M)$ pour $M \in \mathbb{F}_q[T]$ non constant unitaire.

A présent nous souhaitons décrire l'extension abélienne maximale de K. Tout d'abord il existe un autre type d'extension facile à décrire. On rappelle que k est le corps des constantes de K. En l'occurence $k = \mathbb{F}_q$ est un corps fini à q éléments. Nous pouvons alors former des extensions finies abéliennes en considérant les extensions $\mathbb{F}_{q^n}(T)$ (on parle **d'extensions du corps de base**). Le groupe de Galois $\mathrm{Gal}(\mathbb{F}_{q^n}(T)/\mathbb{F}_q(T))$ est cyclique d'ordre n et est engendré par un automorphisme agissant sur $\mathbb{F}_{q^n}$ comme l'automorphisme de Frobenius $x \mapsto x^q$. Soit E/K l'extension obtenue en prenant l'union des extensions du corps de base. Il s'agit d'une extension abélienne par ce qui précède.

Pour des raisons liées à la théorie de la ramification, on sait en fait que le compositum des extensions E/K et K_T/K dans K^{ac} ne peut être égal à l'extension abélienne maximale de K. Il reste donc un dernier type d'extension à décrire.

Pour cela nous allons considérer la même théorie que ci-dessus mais en posant $A = \mathbb{F}_q[\frac{1}{T}]$. Dans le langage de la section 3.1, on change la valuation que l'on considère comme v_∞, qui devient maintenant celle induite par le polynôme irréductible T. On peut alors considérer le module de Drinfeld tel que $\phi(\frac{1}{T}) = \frac{1}{T}+\tau$. On considère les extensions $K(\Lambda_{T^{-\nu-1}})$ pour $\nu \geq 1$. Afin d'obtenir des extensions linéairement disjointe dans la suite, on ne considérera pas ces extensions directement, mais certaines de leurs sous-extensions. Plus précisément le groupe de Galois $\mathrm{Gal}(K(\Lambda_{T^{-\nu-1}})/K)$ est égal à $\left(\mathbb{F}_q[\frac{1}{T}]/(T^{-\nu-1})\right)^\times$. Il contient en particulier les polynômes constants $\mathbb{F}_q^\times$. Soit L_ν le sous-corps de $K(\Lambda_{T^{-\nu-1}})$ fixé par $\mathbb{F}_q^\times$. Il s'agit d'une extension abélienne de K, dont le groupe de Galois est isomorphe aux polynômes en $\frac{1}{T}$ mod $\frac{1}{T^{\nu+1}}$ dont le terme constant est égal à 1. On pose L_∞ l'union des corps L_ν, $\nu \geq 1$.

Définition 3.12. On pose $K^H = K_T \cdot E \cdot L_\infty$. Il s'agit d'une extension abélienne de K.

Remarque. Comme mentionné dans le paragraphe précédent, la construction des extensions L_ν permet de rendre $K_T \cdot E/K$ linéairement disjointe de L_∞/K. Les extensions K_T/K et E/K sont également linéairement disjointes.

Ceci permet le calcul du groupe de Galois $\mathrm{Gal}(K^H/K)$ comme produit direct $\mathrm{Gal}(K_T/K) \times \mathrm{Gal}(E/K) \times \mathrm{Gal}(L_\infty/K)$.

Théoreme 3.13. *K^H est l'extension abélienne maximale de K. Autrement dit toute extension abélienne de K est incluse dans K^H.*

Remarque. Ce théorème permet de calculer le groupe de Galois de $\mathrm{Gal}(K^{ab}/K)$. Cependant en pratique on utilise plutôt les théorèmes de la théorie des corps de classes afin de calculer ce groupe, et la preuve du théorème ci-dessus revient en fait à montrer que le groupe de Galois $\mathrm{Gal}(K^H/K)$ est égal à $\mathrm{Gal}(K^{ab}/K)$, en exhibant l'isomorphisme explicitement.

Remarque. Si l'on note également $K_{\frac{1}{T}}$ l'extension définie comme dans la théorie précédente mais en choisissant $\frac{1}{T}$ comme générateur de K, on peut considérer le compositum $K_T \cdot K_{\frac{1}{T}}$. On montre alors que ce compositum est lui aussi égal à K^{ab}. Ceci donne une description à priori plus simple de K^{ab}, mais moins pratique du point de vue de la théorie de Galois puisque ces extensions ne sont pas linéairement disjointes.

3.4 Généralisation

On mentionne avec moins de détails comment généraliser les constructions précédentes. On renvoie à [2] et [7] pour approfondir ces notions. On verra qu'il existe quelques différences. On fixe pour la suite ε une fonction signe.

Définition 3.14. On note X_ε l'ensemble des modules de Drinfeld ε-normalisés.

Nous avons vu que dans le cas $K = \mathbb{F}_q(T)$, l'ensemble X_ε est constitué d'un unique module de Drinfeld : le module de Carlitz. Ce n'est cependant pas le cas en général. Fixons toute de même pour la suite un module $\phi \in X_\varepsilon$. Nous aurons besoin du lemme suivant :

Lemme 3.15. *Si L est un corps de caractéristique $p > 0$, les idéaux à gauche de l'anneau $L[\tau]$ sont principaux.*

Démonstration. Il suffit de suivre la preuve usuelle pour les anneaux de polynômes sur un corps, c'est à dire par division euclidienne, mais en tenant compte de la multiplication modifiée. On utilise pour cela le fait que la division euclidienne par un polynôme unitaire en τ est bien définie. □

A présent soit $\mathfrak{a}$ un idéal non nul de A. On considère l'idéal à gauche $I_{\phi,\mathfrak{a}}$ de $\mathbb{C}_\infty[\tau]$ engendré par les éléments $\{\phi_a : a \in \mathfrak{a}\}$. Il s'agit d'un idéal principal, il existe donc un unique polynôme unitaire $\phi_\mathfrak{a} \in \mathbb{C}_\infty[\tau]$ tel que $I_{\phi,\mathfrak{a}} = \mathbb{C}_\infty[\tau]\phi_\mathfrak{a}$.

On aimerait à présent définir des extensions abéliennes à partir de ϕ. On rappelle que tout élément de $\mathbb{C}_\infty[\tau]$ s'identifie à un polynôme à coefficients dans $\mathbb{C}_\infty[X]$. Nous aimerions cependant que nos polynômes soient à coefficients dans K afin de définir des extensions de K. Ce n'est bien sûr pas le cas mais en général. On peut cependant montrer la proposition suivante :

Proposition 3.16. *Soit ϕ un module de Hayes pour ε. Soit $y \in A$ non constant. Alors les coefficients de ϕ_y sont algébriques sur K. De plus si H_A^+ dénote le corps engendré sur K par les coefficients de ϕ_y, ce corps est indépendant de y, et même de ϕ. Il dépend cependant de ε.*

Définition 3.17. On appelle H_A^+ le corps normalisateur du triplet (K, ∞, ε).

Comme voulu, on peut montrer que H_A^+ est une extension abélienne de K. Par la proposition 3.16, ϕ est en fait un module de Drinfeld $\phi : A \to H_A^+[\tau]$. Nous pouvons à présent définir certaines extensions abéliennes de K.

Définition 3.18. Soit $\mathfrak{a}$ un idéal non nul de A. On définit le A-module $\phi[\mathfrak{a}]$ des éléments z de K^{ac} tels que $\phi_x(z) = 0$ pour tout $x \in \mathfrak{a}$. De façon équivalente $\phi[\mathfrak{a}]$ est le lieu des zéros de $\phi_\mathfrak{a}$. Les éléments de $\phi[\mathfrak{a}]$ sont séparables car les polynômes ϕ_x pour $x \in \mathfrak{a}$ le sont.

Comme précédemment, on a :

Proposition 3.19. *$\phi[\mathfrak{a}]$ est un $A/\mathfrak{a}$-module libre de rang 1.*

Remarque. De façon plus générale, si l'on considère un module de Drinfeld de rang $r > 0$, le A-module $\phi[\mathfrak{a}]$ est un A-module libre de rang r. C'est pour cela que l'on considère des modules de Drinfeld de rang 1.

Proposition 3.20. *Les extensions $K(\phi[\mathfrak{a}])/K$ sont abéliennes.*

Nous n'avons pas donné l'action du groupe de Galois $\mathrm{Gal}(K^{ac}/K)$ sur ces extensions. Cela est dû au fait que les polynômes ϕ_x ne sont pas à valeur dans K, mais dans H_A^+. En particulier les A-modules $\phi[\mathfrak{a}]$ ne sont pas stable par l'action du groupe de Galois. Montrer que ces extensions sont abéliennes en général n'est donc pas aussi facile que dans les cas particulier. Il faudrait pour cela définir une action des idéaux de A sur les modules de Hayes à ε fixé (voir [2] et [7]).

Il est en revanche plus simple de comprendre l'action de $\mathrm{Gal}(K^{ac}/H_A^+)$ sur $K(\phi[\mathfrak{a}])$. En effet dans ce cas $\mathrm{Gal}(K^{ac}/H_A^+)$ agit A-linéairement sur $\phi[\mathfrak{a}]$, qui est un $A/\mathfrak{a}$-module libre de rang 1 et on a donc comme précédemment un morphisme injectif de groupes :

$$\begin{aligned} \chi_\mathfrak{a} : \mathrm{Gal}(K(\phi[\mathfrak{a}]))/K) &\longrightarrow (A/\mathfrak{a})^\times \\ \sigma &\longmapsto \chi_\mathfrak{a}(\sigma) \end{aligned}$$

On peut définir $K^\infty = \bigcup_\mathfrak{a} K(\phi[\mathfrak{a}])$, l'union portant sur les idéaux non nuls de A. Il s'agit d'une extension abélienne de K. On a alors le théorème suivant :

Théoreme 3.21. *Soit $v_{\infty'}$ une valuation de K distincte de v_∞. Alors le compositum $K^\infty \cdot K^{\infty'}$ est l'extension abélienne maximale de K.*

Remarque. Ceci est à rapprocher de la remarque après le théorème 3.13. Comme précisé à ce moment, ces deux extensions ne sont pas linéairement disjointe, ce qui n'est pas satisfaisant du point de vue de la théorie de Galois. De plus cela nécessite un deuxième choix non naturel : celui d'un idéal premier de A à utiliser pour la valuation $v_{\infty'}$. Décrire K^{ab} sans ce deuxième choix nécessiterait comme précédemment une nouvelle construction.

4 Conclusion

J'aimerais conclure en mentionnant quelques concepts que j'ai pu découvrir durant mon stage liés à ces concepts, ainsi que les choix faits pour ce rapport.

Tout d'abord j'ai décidé d'exposer ces deux théories sans prouver la plupart des théorèmes principaux. L'une des raisons bien sûr est que développer ces théories nécessiterait de montrer bien plus de lemmes techniques que ceux mentionnés ici. Mais une autre raison est due aux prérequis. Développer ces théories nécessiterait d'introduire un certain nombre de concepts liés soit à la théorie algébrique des nombres soit plus précisément à la théorie des corps de classes. J'ai préféré éviter de considérer ces concepts comme acquis afin de présenter au moins les constructions qui peuvent être appréciées par tous.

L'un des concepts qu'il aurait été nécessaire d'introduire pour prouver de nombreuses proposition de ce rapport est la ramification des idéaux premiers. Il s'agit d'un concept de base en théorie algébrique des nombres permettant notamment de comprendre plus précisément les structures des extensions de corps ainsi que des groupes de Galois. L'idée de base est de regarder comment se décomposent les idéaux premiers dans les extensions de corps. Prenons un exemple connu : $\mathbb{Q}$ et son extension $\mathbb{Q}(i)$. Les anneaux d'entiers correspondants sont $\mathbb{Z}$ et $\mathbb{Z}[i]$. On peut regarder comment se décomposent les nombres premiers de $\mathbb{Z}$ dans $\mathbb{Z}[i]$. Il est alors connu par exemple que $2 = -i(1+i)^2$, $5 = (3+4i)(3-4i)$, et que 3 reste premier dans $\mathbb{Z}[i]$. La théorie de la ramification examine ces comportements plus en détail. On renvoie à [3] et [6] pour une introduction.

Afin de compléter certaines des preuves il aurait également été nécessaire d'introduire les concepts fondamentaux de la théorie des corps de classes. Ici l'un des théorèmes fondamentaux est l'existence et l'unicité d'un morphisme de groupe ψ depuis un groupe appelé le groupe des idèles de K vers le groupe de Galois $\mathrm{Gal}(K^{ab}/K)$. Ce morphisme est appelé application de réciprocité d'Artin. L'intérêt de ce morphisme est qu'il est possible par son biais de travailler avec le groupe des idèles, que l'on peut calculer explicitement à partir uniquement du corps de base K, plutôt que le groupe de Galois, plus abstrait. La théorie des corps de classes est riche et contient de nombreux théorèmes, et leurs preuves nous auraient amenées bien trop loin pour ce rapport. Pour une introduction à la théorie des corps de classes, on pourra consulter [4].

Références

[1] David R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77-91.

[2] David R. Hayes, *A brief introduction to Drinfeld modules*, The arithmetic of function fields : Proceedings of the Workshop at the Ohio State University (1991), 1-33.

[3] James S. Milne, *Algebraic Number Theory (v3.08)*, 2020, https ://www.jmilne.org/math/CourseNotes/ANT.pdf.

[4] James S. Milne, *Class Field Theory (v4.03)*, 2020, https ://www.jmilne.org/math/CourseNotes/CFT.pdf.

[5] Peter Schneider, *Lubin-Tate Theory*, Course at Münster (2017) https ://ivv5hpp.uni-muenster.de/u/pschnei/publ/lectnotes/Lubin-Tate.pdf .

[6] Jean-Pierre Serre, *Local Fields*, Springer (1979).

[7] David Zywina, *Explicit class field theory for global function fields*, J. Number Theory 133 (2013), no.3, 1062–1078.