Explicit Class Field Theory For Rational Function Fields

by

Tahina Rakotoniaina

Thesis presented in partial fulfilment of the requirements for the degree of Master of Science at Stellenbosch University Department of Mathematical Sciences

Supervisor: Prof Florian Breuer
Stellenbosch University

December 2008

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the owner of the copyright thereof (unless to the extent explicitly stated otherwise) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 25 November 2008

Abstract

Class field theory describes the abelian extensions of a given field K in terms of various class groups of K, and can be viewed as one of the great successes of 20th century number theory. However, the main results in class field theory are pure existence results, and do not give explicit constructions of these abelian extensions. Such explicit constructions are possible for a variety of special cases, such as for the field $\mathbb{Q}$ of rational numbers, or for quadratic imaginary fields. When K is a global function field, however, there is a completely explicit description of the abelian extensions of K, utilising the theory of sign-normalised Drinfeld modules of rank one. In this thesis we give detailed survey of explicit class field theory for rational function fields over finite fields, and of the fundamental results needed to master this topic.

Opsomming

Klasliggaamteorie beskryf die abelse uitbreidings van 'n gegewe liggaam K in terme van die klasgroepe van K, en kan as een van groot prestasies van die getalleteorie van die 20ste eeu beskou word. Nogtans is die hoofresultate van klasliggaamteorie suiwer bestaanstellings, en gee geen eksplisiete konstruksies van hierdie abelse uitbreidings nie. Sulke ekplisiete konstruksies is wel bekend in 'n paar spesiale gevalle, soos vir die liggaam $\mathbb{Q}$ van rasionale getalle, of vir imaginêre kwadratiese liggame. Wanneer K 'n globale funksieliggaam is, bestaan daar wel 'n explisiete beskrywing van die abelse uitbreidings van K wat gebruik maak van die teorie van teken-genormaliseerde Drinfeld-modules van rang een. Hierdie proefskrif gee 'n oorsig van die ekplisiete klasliggaamteorie vir rasionale funksieliggame oor eindige liggame, sowel as van die fundamentele resultate wat nodig is om hierdie tema onder die knie te kry.

Acknowledgements

A large number of people have influenced the writing of my thesis either directly or indirectly. My first thanks go to my supervisor Prof. Florian Breuer for his helpful guidance and constant assistance. I extend my warm thanks to the other lecturers, Prof. Barry Green and Dr. Keet, for their friendliness and collaboration. I also want to express my gratitude to AIMS and the University of Stellenbosch which awarded the scholarship which enabled me to complete my master degree in Number Theory. My final word of thanks belongs to Dimby.

MISAOTRA TOMPOKO

Contents

Introduction

There are basically two branches of Number Theory. The first one deals with the quotient field $\mathbb{Q}$ of the ring of integers $\mathbb{Z}$. The second one deals with the quotient field $k := \mathbb{F}(T)$ of the ring of polynomials $\mathbb{F}[T]$ over finite field $\mathbb{F}$. Both rings, $\mathbb{Z}$ and $\mathbb{F}[T]$, are principal ideal domains, have the property that the residue class ring of any non-zero ideal is finite, have finitely many units and have infinitely many primes. Moreover, $\mathbb{F}[T]$ has almost all the analogues of the famous theorems in $\mathbb{Z}$. These are, for example, the analogues of Fermat's little theorem, Wilson's theorem, the prime number theorem and Dirichlet's theorem. The analogue of the Riemann Hypothesis is true for function fields. For a treatment of these analogues and a good background on function fields see [Sti] or [Ros1].

In this thesis, which has four chapters, we explore other similarities between Function Fields $\mathbb{F}(T)$ and Rational numbers $\mathbb{Q}$. The similarities are centered in the finite extensions of each field. For example, in the field $\mathbb{Q}$, if $\zeta_m \in \mathbb{C}$ is a primitive m-th root of unity, then $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is an abelian extension. A similar thing happens in the rational function field k. If $C_m(x) \in k[x]$ is a polynomial derived from the Carlitz module for some nonzero $m \in \mathbb{F}[T]$, then $k(\lambda_m)$ turns out to be an abelian extension of k as well. Here λ_m is a generator of the $\mathbb{F}[T]$-module formed by the roots of $C_m(x)$. Moreover, the primes, both finite and infinite, behave in exactly the same way in each of these abelian extensions. Also there are two analogue extension fields where each prime at infinity of k and $\mathbb{Q}$ splits in the same way. Unexpectedly, for the case of function fields, some of the abelian extensions of k are not contained in $k(\lambda_m)$ for some $m \in \mathbb{F}[T]$. However, the Kronecker-Weber theorem states that every abelian extension of the rational numbers $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ for some positive integer m.

The first chapter starts with some basic Algebraic Number Theory in order to make the thesis more self-contained. Most of these basic theories are needed along the three chapters. Thereafter, in the second section, the theory of cyclotomic fields is introduced in which one sees how primes in $\mathbb{Z}$ behave in $\mathbb{Q}(\zeta_m)$. Some background is assumed to be known, but for a good treatment of cyclotomic fields one could read [Lan2], [Was], or [Hun]. The Kronecker-Weber theorem is found in the last section. This famous theorem can be proven by a straightforward algebraic construction. For instance see [Gre]. We will derive it from class field theory.

Chapter 2 has two important roles. Not only does it illustrate the similarities between k an $\mathbb{Q}$ but it also provides a background for the third chapter. The theory of cyclotomic function fields is done via the Carlitz module. The Carlitz module is just a particular case of Drinfeld modules. The last ones give an explicit class field theory in global function fields. An introduction to Drinfeld modules is developed in the first section. The two following sections after that deal with the behaviour of finite primes in $k(\lambda_m)$ using only the Carlitz module. The last section shows how the prime at infinity splits. To engage with that, one section that gives a notion about Newton Polygons has to be inserted.

Since the analogy of the Kronecker-Weber is quite different and more complicated, I dedicate the third chapter for developping this. In the first section and second section, a field $\mathcal{A}$ and homomorphism ψ is constructed respectively. $\mathcal{A}$ and ψ are proved to be the maximal abelian extension of k and the reciprocity law homomorphism respectively. In the section 4 of this chapter I give a short discussion of Class Field Theory and state the main theorems on abelian extensions.

Numerous elementary proofs have been found for the Kronecker-Weber theorem for the number fields. The last chapter, at the first place, gives a brief summary of some of those proof, thereafter it analyzes the proofs and show which of the steps in the proof can be followed for the rational function fields and which cannot. It seems that the local-global principle might be promissing since we have local fields in both cases.

Chapter 1

Cyclotomic Number Fields

A cyclotomic field K of rational numbers is formed by adjoining a primitive m^{th} root of unity ζ_m (for more see [Lan2]). The cyclotomic fields play a crucial role in the development of modern algebra and number theory. As a direct application, Gauss made early inroads in the theory of cyclotomic fields, in connection with the geometrical problem of construction a regular n-gon with a compass and straightedge. He stated that a regular p-gon can be constructed if and only if p is a Fermat prime (see [How]). Cyclotomic fields theory has also a relation with Fermat's last theorem. A natural approach to proving the theorem is to factor the binomial $X^m + Y^m$ where m is an odd prime, appearing in one side of Fermat's equation as follows:

$$X^m + Y^m = (X + Y)(X + \zeta_m Y)...(X + \zeta_m^{m-1} Y)$$

Here X and Y are ordinary integers, whereas the factors are algebraic integers in the cyclotomic field K.

We start by giving some background in Algebraic Number Theory.

1.1 Ramification in number fields

We are going to restrict ourselves within an extension of number fields for this section, however the theory is still true for any finite and separable extension fields.

Let L/K be an extension of number fields and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be their respective rings of integers. The ring of integers of a number field is a Dedekind domain. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$. One of the most important results in Algebraic Number Theory is the following. The ideal $\mathfrak{p}\mathcal{O}_L$ can be written uniquely as a finite product of powers of prime ideals of $\mathcal{O}_L$. Lets assume that the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ into primes of $\mathcal{O}_L$ is as follows:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \tag{1.1}$$

Then we say that the primes $\mathfrak{P}_i$ lie above $\mathfrak{p}$ (or $\mathfrak{P}_i$ divide $\mathfrak{p}$) with ramification index $e(\mathfrak{P}_i/\mathfrak{p}) := e_i$. Since the ring of integers is a Dedekind domain, the quotient ring $l_i = \mathcal{O}_L/\mathfrak{P}_i$ is a finite field extension of the finite field $k = \mathcal{O}_K/\mathfrak{p}$ for each i. The latter field is called the residue field and the extension degree $f(\mathfrak{P}_i/\mathfrak{p}) := [l_i : k]$ is called the residue degree. If there is no confusion, we will denote e_i and f_i the ramification index and the residue degree, respectively, to simplify our notation. With these notations the following equality holds:

$$\sum_{i=1}^{r} e(\mathfrak{P}_i/\mathfrak{p}) f(\mathfrak{P}_i/\mathfrak{p}) = [L : K] \tag{1.2}$$

Definition 1.1.1. Let L, K and $\mathfrak{P}_i$, $\mathfrak{p}$ be as above.

1. We say that $\mathfrak{P}_i$ is ramified over $\mathfrak{p}$ if $e_i > 1$ for some i. And we say that $\mathfrak{p}$ is unramified in F/K if $e_i = 1$ for all i. There are only finitely many primes which ramify in L/K.

2. We say that $\mathfrak{p}$ is totally ramified in L/K if there is a unique prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$ and $f = 1$. In this case $e = [L : K]$.

3. We say that $\mathfrak{p}$ splits completely in F/K if $e_i = f_i = 1$ for all i. Here we have $r = [L : K]$

4. Finally, let p be the characteristic of the residue field $\mathcal{O}_K/\mathfrak{p}$. We say that $\mathfrak{P}_i$ is tamely ramified if $e_i > 1$ and $(e_i, p) = 1$. And we say that $\mathfrak{P}_i$ is wildly ramified if $p \mid e_i$.

The set $\mathcal{D}(\mathfrak{P}_i/\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$ is called the decomposition group, and it is isomorphic to $\mathrm{Gal}(l/k)$ when $\mathfrak{P}_i/\mathfrak{p}$ is unramified. The element, noted by $(\mathfrak{p}, K_m/\mathbb{Q})$, in $D(\mathfrak{P}_i/\mathfrak{p})$ which corresponds to the p-th Frobenius map in $\mathrm{Gal}(l/k)$ is called the Artin automorphism. Here p is the characteristic of k.

1.2 Cyclotomic Extensions

This section, which is one of the main purposes of this chapter, tries to recap some important results in cyclotomic theory. It mostly follows [Ros1]. We will see in the following chapter their analogues for the function fields case. We mostly turn our attention to the way how primes in $\mathbb{Z}$ split.

We start with the following theorem:

Theorem 1.2.1. *Let $\zeta_m \in \mathbb{C}$ be a primitive m-th root of unity where $m > 2$ is an integer. Then $K_m := \mathbb{Q}(\zeta_m)$ is a Galois extension of $\mathbb{Q}$*

$$\mathrm{Gal}(K_m/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*. \tag{1.3}$$

Consequently $K_m/\mathbb{Q}$ is an abelian extension.

This theorem is well known, so we leave the proof. Any subfield of K_m for some integer m is called cyclotomic. Our next task is to find the ring of integer of K_m. Throughout the rest of this section we let m not be twice an odd integer. This restriction allows us to apply all the previous results (we took $m > 2$). It does not affect our treatment since if m_0 is an odd number, then, $K_{m_0} = K_{2m_0}$. To see this, let ζ be a root of $x^{m_0} - 1$. Then, ζ is also a root of $x^{2m_0} - 1$. Thus, $K_{m_0} \subseteq K_{2m_0}$. And we get the equality by noticing that $\phi(2m_0) = \phi(m_0)$. We starts with one nice proposition.

Proposition 1.2.2. *Let L and K be two number fields. Assume that their discriminants are relatively prime and they are linearly disjoint. Then $\mathcal{O}_{LK} = \mathcal{O}_L\mathcal{O}_K$.*

Let $m = p_1^{r_1}p_2^{r_2}...p_t^{r_t}$ and ζ a primitive p^r-th root of unity, then the proposition above suggests to check two properties. Firstly, the K_m is equal to the compositum of the fields $K_{P_i^{r_i}}$, noted by $K_m = \vee K_{p_i^{r_i}}$, and secondly that for a basis

$W = \left\{1, \zeta, ..., (\zeta)^{\phi(p^r)-1}\right\}$ of $K_{p^r}/\mathbb{Q}$ the discriminant is a power of p. The discriminant of $d(W)$ is in fact $\pm p^s$ where $s = p^{r-1}(rp - r - 1)$ (see [Neu] page 59). The first property follows from the following proposition.

Proposition 1.2.3. *Let p be a prime number and r be a positive integer. Then the prime ideal (p) is totally ramified in $K_{p^r}/\mathbb{Q}$. The prime lying above (p) in $\mathcal{O}_m$ is just $(1-\zeta)$. If $q \neq p$ a prime number, then (q) is unramified.*

Proof. We begin to prove the second part of the theorem. Let $g(x) \in \mathbb{Q}[x]$ be the minimum polynomial of ζ and let $f(x) = x^{p^r} - 1$. It is clear that

$$g'(\zeta)h(\zeta) = f'(\zeta) = p^r \zeta^{p^r-1} \text{ for some } h(x) \in \mathbb{Q}[x]. \tag{1.4}$$

Since K_{p^r} is generated by ζ the different $D(\mathcal{O}_{p^r}/\mathbb{Z})$ must divide $(g'(\zeta))$. And if (q) is a ramified prime ideal with ramification index e, then $(q)^{e-1}$ divides $D(\mathcal{O}_{p^r}/\mathbb{Z})$ (see proposition 8, page 62 in [Lan1]). In another words, using the equation 1.4, we have

$$(p)^r \subseteq (g'(\zeta)) \subseteq D(\mathcal{O}_{p^r}/\mathbb{Z}) \subseteq (q)^{e-1}. \tag{1.5}$$

Hence q must be equal to p. That proves the last part of the proposition.

For the first part we should know that the minimum polynomial of ζ in $\mathbb{Q}[x]$ is

$$\begin{aligned} \mathcal{F}(x) &= \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \\ &= \frac{(x^{p^{r-1}})^p - 1}{x^{p^{r-1}} - 1} \\ &= 1 + x^{p^{r-1}} + ... + (x^{p^{r-1}})^{p-1} \end{aligned}$$

Since the roots of $\mathcal{F}(x)$ are all the primitive m-th roots of unity, one has

$$\mathcal{F}(x) = \prod_{\substack{a=1 \\ (a,p)=1}}^{\phi(p^r)} (x - \zeta^a)$$

Substituting x by 1 and noticing that $\frac{1-\zeta^a}{1-\zeta}$ is unit for all a prime to p yield

$$p = \prod (1 - \zeta^a) = (1 - \zeta)^{\phi(p^r)} \times unit.$$

Passing to the ideal in $\mathcal{O}_m$, we find $(p) = (1-\zeta)^{\phi(p^r)}$. Since $[K_{p^r} : \mathbb{Q}] = \phi(p^r)$, it follows that $(1-\zeta)$ has to be a prime ideal of $\mathcal{O}_m$. That completes the proof.

□

This proposition implies that all the fields $K_{p_i{}^{r_i}}$ are pairwise linearly disjoint. And since $\phi(m) = \phi(p_1^{r_1})\phi(p_2^{r_2})...\phi(p_t^{r_t})$ then $K_m = \vee K_{p_i^{r_i}}$. The proposition 1.2.2 reduces our task from any integer m down to a prime power p^r.

Proposition 1.2.4. *$\mathbb{Z}[\zeta]$ is the ring of integers $\mathcal{O}_{p^r}$ in K_{p^r}.*

Proof. Since the inclusion $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_{p^r}$ is obvious, we only need to prove the other one. Let W be an element of $\mathcal{O}_{p^r}$. from the fact that $\mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$ and $[K_{p^r} : \mathbb{Q}] = \phi(p^r)$, we can write

$$w = \sum_{i=0}^{\phi(p^r)-1} a_i(1-\zeta)^i \text{ where } a_i \in \mathbb{Q}.$$

From that we just need to prove that all the a_i are in $\mathbb{Z}$. Since $d(W)$ is a power of p, using Cramer's rule we find that the a_i's have denominators a power of p. Then $a_i = \frac{b_i}{p^n}$ with $b_i \in \mathbb{Z}$. We assume that not all of the b_i are divisible by p. We have

$$p^n w = \sum b_i(1-\zeta)^i \text{ where } b_i \in \mathbb{Z}. \tag{1.6}$$

All we need is to prove that $n = 0$. This is done by comparing the valuation of both sides in the previous equation. From proposition 1.2.3 we can extend v_p to K_{p^r} by writing $\phi(p^r)v_p(x) = v_{(1-\zeta)}(x)$ for any $x \in K_{p^r}$. We first have

$$v_p(p^n w) \geq n \tag{1.7}$$

On the other hand, if i_0 is the smallest integer such that $v_p(b_{i_0}) = 0$, then

$$v_p(\sum b_i(1-\zeta)^i) \geq min\left\{v_p(b_i(1-\zeta)^i)) \mid 1 \leq i \leq \phi(p^r)\right\}.$$

It can be shown that the numbers $v_p(b_i(1-\zeta)^i)$, $1 \leq i \leq \phi(p^r)$ are distinct (see for

example page 2 in [Was]). Therefore

$$\begin{aligned} v_p(p^n w) &= min\left\{v_p(b_i(1-\zeta)^i)) \mid 1 \leq i \leq \phi(p^r)\right\} \\ &\leq v_p(b_{i_0}(1-\zeta)^{i_0}) \\ &= 1/\phi(p^r).v_{(1-\zeta)}(b_{i_0}(1-\zeta)^{i_0}) \\ &= \frac{1}{\phi(p^r)}.i_0 \end{aligned}$$

□

Let $m = p_1^{r_1}p_2^{r_2}...p_t^{r_t}$ be a positive integer, then from the proposition above $\mathcal{O}_{p_i^{r_i}} \subseteq \mathbb{Z}[\zeta_{p_i^{r_i}}] \subseteq \mathbb{Z}[\zeta_m]$ for every $1 \leq i \leq t$. And by the proposition 1.2.2 $\mathcal{O}_m \subseteq \mathbb{Z}[\zeta_m]$. Hence we have

Proposition 1.2.5. *$\mathbb{Z}[\zeta_m]$ is the ring of integers $\mathcal{O}_m$ in K_m.*

From proposition 1.2.3 now follows

Theorem 1.2.6. *Let $m = p_1^{r_1}p_2^{r_2}...p_t^{r_t}$ be a positive integer. Then the only primes that ramify in K_m are the (p_i), $1 \leq i \leq t$.*

Let $w \in \mathcal{O}_m$. From the discussion in the first section we get

$$(p\mathbb{Z}, K_m/\mathbb{Q})w = w^p \pmod{\mathfrak{P}} \text{ for any } w \in \mathcal{O}_m. \tag{1.8}$$

Where $(p\mathbb{Z}, K_m/\mathbb{Q})$ is the Artin automorphism. By proposition 1.2.5, we can write

$$w = \sum_{i=0}^{\phi(m)-1} a_i\zeta_m^i \text{ where } a_i \in \mathbb{Z} \tag{1.9}$$

It is easy to check that

$$\begin{aligned} \sigma_p(w) &= \sigma_p(\sum a_i\zeta_m^i) \\ &= \sum a_i\zeta_m^{pi} \\ &\equiv (\sum a_i\zeta_m^i)^p \pmod{\mathfrak{P}}. \end{aligned}$$

We have proved the following proposition.

Proposition 1.2.7. *Let σ_p be the automorphism in* $\mathrm{Gal}(K_m/\mathbb{Q})$ *which sends ζ_m to ζ_m^p. Then σ_p is the Artin automorphism $(p\mathbb{Z}, K_m/\mathbb{Q})$.*

We end this section with the following theorem.

Theorem 1.2.8. *Let p be a prime number not dividing m and let f be the smallest positive integer such that $p^f \equiv 1 \pmod{m}$. Then $p\mathbb{Z}$ splits into $\phi(m)/f$ primes of degree f in K_m. In particular if $f = 1$ then $p\mathbb{Z}$ splits completely.*

Proof. The order of σ_p is the residue degree $[\mathcal{O}_m/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}] = f$. It is clear that $\sigma_p^f = 1$ if and only if $p^f \cong 1 \pmod{m}$. Since $K_m/\mathbb{Q}$ is a Galois extension, we have $e.f.g = \phi(m)$ where e is the ramification index and g is the number of primes lying above (p). By theorem 1.2.6, $e = 1$ and that completes the proof. □

The last thing about cyclotomic fields which we need to discuss in this section is the behaviour of the prime at infinity. In $\mathbb{Q}$ there is only one archimedean prime given by the usual absolute value. We consider the field $K_m^+ := \mathbb{Q}(\zeta_m + \bar{\zeta_m})$, where $\bar{\zeta_m}$ denotes the complex conjugate of ζ_m. The field K_m^+ is real and so is every embedding of it into the complex numbers. The element $\zeta_m \in K_m$ satisfies the equation $x^2 - (\zeta_m + \bar{\zeta_m})x + 1 = 0$. Then, $[K_m : K_m^+] = 2$. Since $[K_m : \mathbb{Q}] = \phi(m)$, thus the prime at infinity in $\mathbb{Q}$ splits into $\phi(m)/2$ real primes in K_m^+. Each of these ramifies to a complex prime in K_m. We note that every embedding from K_m into $\mathbb{C}$ is complex since the only roots of unity in the real numbers $\mathbb{R}$ are ± 1.

1.3 Kronecker-Weber Theorem

In Algebraic Number Theory, the Kronecker-Weber theorem classifies the abelian extensions of $\mathbb{Q}$. Kronecker provided most of the proof in 1853, with Weber in 1889 and Hilbert in 1896 filling the gaps. It is an easy consequence of Class Field Theory. In this section we first state some theorems, without proof, from Class Field Theory and then derive the Kronecker-Weber theorem from that.

Let k be a number field (finite extension of $\mathbb{Q}$). Let $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$, where $\mathfrak{M}_0$ is an integral ideal of k (it is a finite product of powers of prime ideals in $\mathcal{O}_k$) and $\mathfrak{M}_\infty$ is a formal squarefree product of real archimedean places of k. We call $\mathfrak{M}$ a divisor of k.

Definition 1.3.1. Let $\alpha \in k^*$ and $\mathfrak{M} = \mathfrak{M}_0\mathfrak{M}_\infty$ such that $\mathfrak{M}_0 = \prod \mathfrak{p}_i{}^{e_i}$, then we write $\alpha \equiv 1 \pmod^* \mathfrak{M}$ if we have the following conditions:

i) $v_{\mathfrak{p}_i}(\alpha - 1) \geq e_i$ for all $\mathfrak{p}_i$ in the factorization of $\mathfrak{M}_0$.

ii) $\alpha > 0$ at the real embeddings corresponding to the archimedean places in $\mathfrak{M}_\infty$.

We denote by $P_{\mathfrak{M}}$ the group of principal fractional ideals of k which have a generator $\alpha \equiv 1 \pmod^* \mathfrak{M}$ and by $I_{\mathfrak{M}}$ the group of fractional ideals which are relatively prime to $\mathfrak{M}$. The group $P_{\mathfrak{M}}$ is a subgroup of $I_{\mathfrak{M}}$ and the quotient $I_{\mathfrak{M}}/P_{\mathfrak{M}}$ is a finite group. The quotient $I_{\mathfrak{M}}/P_{\mathfrak{M}}$ is called the generalized ideal class group mod $\mathfrak{M}$.

Example 1.3.2. :

i) If we set $k = \mathbb{Q}$ and $\mathfrak{M} = n$ a positive integer, then $I_{\mathfrak{M}}/P_{\mathfrak{M}} \cong (\mathbb{Z}/n\mathbb{Z})^*/\{\pm 1\}$.

ii) If we set $k = \mathbb{Q}$ and $\mathfrak{M} = n\infty$ where ∞ is given by the usual absolute value, then $I_{\mathfrak{M}}/P_{\mathfrak{M}} \cong (\mathbb{Z}/n\mathbb{Z})^*$.

iii) I_1/P_1 is the ideal class group

We need the following theorems from Class Field Theory (see [Gra]) to prove the Kronecker-Weber Theorem.

Theorem 1.3.3. *Let K/k be a finite abelian extension. Then there exists a divisor $\mathfrak{f}$ of k that satisfies the following:*

i) a prime $\mathfrak{p}$ (archimedean or non-archimedean) ramifies in K/k if and only if $\mathfrak{p}$ divides $\mathfrak{f}$

ii) if $\mathfrak{M}$ is a divisor of k such that $\mathfrak{f}$ divides $\mathfrak{M}$, then there is a subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$ such that $I_{\mathfrak{M}}/H \cong \mathrm{Gal}(K/k)$.

The minimal such divisor $\mathfrak{f}$ is called the conductor of K/k.

Theorem 1.3.4 (Artin Existence Theorem)**.** *Let $\mathfrak{M}$ be a divisor of k and let H be a subgroup with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$. Then there exists a unique abelian extension of K/k, unramified at any prime not dividing $\mathfrak{M}$ such that $I_{\mathfrak{M}}/H \cong \mathrm{Gal}(K/k)$.*

Theorem 1.3.5. *Let K_1/k and K_2/k be finite abelian extensions of conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$ respectively. Let $\mathfrak{M}$ be a multiple of $\mathfrak{f}_1$ and $\mathfrak{f}_2$, and let $H_1,\ H_2 \subseteq I_{\mathfrak{M}}$ be the corresponding subgroups described in the theorem 1.3.3. Then $H_1 \subseteq H_2$ if and only if $K_1 \supseteq K_2$.*

For example let $\mathfrak{M} = 1$ and $H = P_1$. We denote by $\mathcal{H}(k)$ the unramified abelian extension we get by theorem 1.3.4. The Galois group $\mathrm{Gal}(\mathcal{H}(k)/k)$ is isomorphic to the ideal class group of k, I_1/P_1. Let K'/k be a finite unramified abelian extension. By theorem 1.3.3 we have $\mathfrak{f}' = 1$. Choosing $\mathfrak{M} = 1$ and using theorem 1.3.5 yield that $\mathcal{H}(k)$ is the maximal unramified abelian extension. It is called the Hilbert Class field of k.

Now we set $k = \mathbb{Q}$ and we let n be a positive number. It can be proved just by considering from $I_n = I_{n\infty}$ into $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ that $I_{n\infty}/P_{n\infty} \cong \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let K be a number field with $K/\mathbb{Q}$ abelian extension. By theorem 1.3.3, choosing an appropriate divisor $\mathfrak{M}$ we get the subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$ and $I_{\mathfrak{M}}/H \cong \mathrm{Gal}(K/\mathbb{Q})$. We can assume that $\mathfrak{M} = n\infty$. Then $P_{n\infty} \subseteq H$ and by theorem 1.3.5 we have $K \subseteq \mathbb{Q}(\zeta_n)$. In summary, the following holds,

Theorem 1.3.6 (Kronecker-Weber Theorem)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field, i.e. a field obtained by adjoining a root of unity to $\mathbb{Q}$.*

Chapter 2

Cyclotomic Function Fields

Having developed the cyclotomic theory in number fields we now proceed to discuss the cyclotomic function fields. This analogy was first discovered by L. Carlitz in the 1930's (see [Car]). In the late 1970's, D. Hayes developed the idea to make it more understandable (see [Hay]). The idea is to change the operation-law of an A-algebra for some ring A by the well known "Carlitz module". This fascinating trick was generalized by V. Drinfeld to provide an explicit class field theory for any global function field. Since we are going to restrict ourselves to the case of rational function fields we will follow [Ros1] and work within finite fields.

2.1 Drinfeld modules

Drinfeld modules of rank r can be thought as an homomorphism derived from elliptic curves of lattices of rank r. For the analytic point of view of this theory see [Gos]. Before we develop the main task it is worthwhile it to give an introduction to Drinfeld modules.

Definition 2.1.1. Let $\mathbb{F}$ be a finite field of order $q = p^s$ for some prime p. We define the twisted polynomial ring noted $\mathbb{F} < \tau >$ to be the set of all polynomials in τ over $\mathbb{F}$ where the multiplicative operation is defined in this way, for any m_i and n_j in $\mathbb{F}$ we have $m_i\tau^i.n_j\tau^j = m_i n_j^{q^i}\tau^{i+j}$ for some integers i and j.

We set $\tau(x) = x^q$ for some x in some F-algebra, then is this way any element in $\mathbb{F} < \tau >$ gives rise to an endomorphism in any $\mathbb{F}$-algebra. From finite field theory $\alpha^{q^i} = \alpha$ for any integer i and any $\alpha \in \mathbb{F}$. Hence $\tau^i \alpha = \alpha^{q^i} \tau^i = \alpha \tau^i$. In another word if $f = \sum a_i \tau^i \in \mathbb{F} < \tau >$, then $f(\alpha x) = \alpha f(x)$ for any $\alpha \in \mathbb{F}$ and our endomorphism respects the $\mathbb{F}$-algebra structure. From now on we let $A := \mathbb{F}[T]$ the ring of polynomials over $\mathbb{F}$ and $k := \mathbb{F}(T)$ its quotient field.

To give a motivation and to understand more this definition we can introduce the notion of an additive polynomial. A polynomial $f(X) \in F[X]$ is said additive if we have $f(X+Y) = f(X) + f(Y)$. If we note $\mathcal{A}(F)$ the set of all additive polynomials, then $(\mathcal{A}(F), +, \circ)$ is a ring where the $\circ$ is the composition. For an additive polynomial $f(X)$ there are elements $a_i \in F$ such that $f(X) = a_0 X + a_1 X^p + ... + a_r X^{p^r}$. From that, it is not hard to see that $(F < \tau >, +, .) \cong (\mathcal{A}(F), +, \circ)$.

Definition 2.1.2. Let $\rho : A \to k < \tau >$; $m \mapsto \rho_m$ be a homomorphism of $\mathbb{F}$-algebras. Then we say that ρ is a Drinfeld module if the constant term of ρ_m is m and for at least one $m \in A$, $\rho_m \notin A$.

As we see in the definition a Drinfeld module is not a module. However it provides a new structure of a given module. So if B be an A-algebra, which is often just a ring which contains A, then given a Drinfeld module ρ, we define a new multiplication by $m.x = \rho_m(x)$ $\forall$ $m \in A$ and $\forall$ $x \in B$. In this way B has been made into an A-algebra in new way. We will call B with this new A-module structure, B_ρ.

The notion of Drinfeld modules is much more general but as we told before we are working with some restriction. The second condition in the definition is just to ensure that the new A-module structure is not like the previous one.

Since A is freely generated by the element T as an algebra, any given Drinfeld Module ρ is completely determined by the twisted polynomial ρ_T. From the definition the constant term of ρ_T is T. If $\rho_T = T + c_1\tau + c_2\tau^2 + ... + c_r\tau^r$ where $c_i \in k$, $1 \leq i \leq r$ and $c_r \neq 0$, we say that the Drinfeld module ρ has rank r. So given for any $m \in A$ we can write ρ_m explicitly just by knowing ρ_T. In fact if $m = \sum_i \alpha_i T^i$ then

$$\rho_m = \sum_i \alpha_i \rho_{T^i} = \sum_i \alpha_i (\rho_T)^i. \tag{2.1}$$

It implies that the degree of the polynomial $\rho_m(x)$ is $q^{r\deg(m)}$.

The k-algebra which will receive the most attention is the algebraic closure of k, $\bar{k}$. Given a Drinfeld module ρ we define the set $\Lambda_\rho[m] := \left\{\lambda \in \bar{k} \mid \rho_m(\lambda) = 0\right\}$ for some $0 \neq m \in A$. $\Lambda_\rho[m]$ is called the m-torsion module and it is a submodule of $\bar{k}$ as an A-module. In fact, for any $n \in A$ and $\lambda \in \Lambda_\rho[m]$, $\rho_m(n.\lambda) = \rho_m(\rho_n(\lambda))$ and since A is a commutative ring, the RHS in the equality is $\rho_n(\rho_m(\lambda)) = 0$.

We shall see now the similarities between cyclotomic number fields and cyclotomic function fields. For that we start by looking at the extension field $k(\Lambda_\rho[m])$ of k and its Galois group.

By some trivial calculation, one can see that the derivative of $\rho_m(x)$ with respect to x is not equal to zero. Hence the extension field $k(\Lambda_\rho[m])/k$ is separable. And since $\Lambda_\rho[m]$ is the set of the roots of this polynomial then it is a Galois extension. For any $n \in mA$ and $\lambda \in \Lambda_\rho[m]$ we have $n.\lambda = \rho_n(\lambda) = 0$. Hence $\Lambda_\rho[m]$ is an A/mA-module and any $\sigma \in \mathrm{Gal}(k(\Lambda_\rho[m])/k)$ induces an automorphism in $\Lambda_\rho[m]$. We get an embedding

$$\mathrm{Gal}(k(\Lambda_\rho[m])/k) \hookrightarrow Aut_{A/mA}(\Lambda_\rho[m]) \tag{2.2}$$

since the identity map on $\Lambda_\rho[m]$ must be the identity automorphism.

We now investigate the set $\Lambda_\rho[m]$ in order to interpret the group $Aut_{A/mA}(\Lambda_\rho[m])$. Let $m = \alpha P_1^{e_1} P_2^{e_2} ... P_t^{e_t}$ be a prime decomposition for m, where $\alpha \in \mathbb{F}$ and the P_i's are monic irreducible polynomials. For any $1 \leq i \leq t$ the set $\Lambda_\rho[P_i]$ is a vector space over A/P_iA, and as told before $\Lambda_\rho[P_i]$ has $q^{r\deg(P_i)}$ elements where r is the rank of ρ. Since the number of elements of A/P_iA is $q^{\deg(P_i)}$, then

$$\Lambda_\rho[P_i] \cong \underbrace{A/P_iA \oplus A/P_iA \oplus ... \oplus A/P_iA}_{r \text{ times}}. \tag{2.3}$$

Since we are working over a principle ideal domain, one finds

$$\Lambda_\rho[P_i^{e_i}] \cong \underbrace{A/P_i^{e_i}A \oplus A/P_i^{e_i}A \oplus ... \oplus A/P_i^{e_i}A}_{r \text{ times}}. \tag{2.4}$$

On the other hand we have $\rho_m = \alpha\rho_{P_1^{e_1}}\rho_{P_2^{e_2}}...\rho_{P_t^{e_t}}$. Then

$$\Lambda_\rho[m] \cong \Lambda_\rho[P_1^{e_1}] \oplus \Lambda_\rho[P_2^{e_2}] \oplus ... \oplus \Lambda_\rho[P_t^{e_t}], \tag{2.5}$$

also from the Chinese Remainder Theorem we have,

$$A/mA \cong A/P_1^{e_1}A \oplus A/P_2^{e_2}A \oplus ... \oplus A/P_t^{e_t}. \tag{2.6}$$

Finally

$$\Lambda_\rho[m] \cong \underbrace{A/mA \oplus A/mA \oplus ... \oplus A/mA}_{r \text{ times}}. \tag{2.7}$$

This last equation shows how the rank of a Drinfeld module plays an important role and from this equation we have

$$\begin{aligned} Aut_{A/mA}(\Lambda_\rho[m]) &= Aut_{A/mA}(A/mA \oplus A/mA \oplus ... \oplus A/mA) \\ &= GL_r(A/mA) \end{aligned}$$

Where $GL_r(A/mA)$ is the group of invertible $r \times r$ matrices with entries in A/mA. It implies that for a Drinfeld of rank one the $\mathrm{Gal}(k(\Lambda_\rho[m])/k)$ is embedding into $(A/mA)^*$. We have proved the following theorem.

Theorem 2.1.3. *Let ρ be a drinfeld of rank one and let $m \in A$. Then the extension $k(\Lambda_\rho[m])/k$ is an abelian extension.*

2.2 Ramification in function fields

In the previous section we dealt with Drinfeld modules of rank r and we saw that we can construct explicitly an abelian extension of the field k from any Drinfeld module of rank 1. The Carlitz module is a Drinfeld module C of rank 1 given by $C_T = T + \tau$. We call a cyclotomic function field any subextension of $K_m := k(\Lambda_C[m])$ for some $m \in A$.

In this section we will show the following theorem

Theorem 2.2.1. *Let m be in A. Then K_m/k is a Galois extension and*

$$\mathrm{Gal}(K_m/k) \cong (A/mA)^* \tag{2.8}$$

Consequently K_m/k is abelian.

We know already that $\mathrm{Gal(K_m/k)} \hookrightarrow (A/aA)^*$, all we need to do is to show that $[K_m : k] = \phi(m)$ (the number of elements of $(A/mA)^*$) where ϕ is the Euler function for the function field. At the same time we show how prime ideals ramify in k_m. Let $m = \alpha P_1^{e_1} P_2^{e_2} ... P_t^{e_t}$ the prime decomposition. We show first that $K_m = \vee K_{P_i^{e_i}}$. To complete this task we need the following lemma.

Lemma 2.2.2. *Let m be a polynomial in A and let λ_m be a generator of Λ_m as an A-module. Then $C_a(\lambda_m)$ is a generator if and only if $(a, m) = 1$. So Λ_m has $\phi(m)$ generators.*

Proof. We know that $\Lambda_m \cong A/mA$ as an A-module so it has a generator. If λ_m is such a generator, then for any $\lambda \in \Lambda$ there exists $\gamma \in A$ such that $\lambda = \gamma.\lambda_m = C_\gamma(\lambda_m)$. If $(a, m) = 1$ then there exists $b, f \in A$ such that $C_b C_a + C_f C_m = 1$ so $\lambda = C_b C_a(\lambda) = C_b C_a C_\gamma(\lambda_m)$. Therefore $\lambda = b\gamma.C_a(\lambda_m)$. Reciprocally, if $C_a(\lambda_m)$ is a generator then there exists $b \in A$ such that $\lambda_m = b.C_a(\lambda_m)$. Thus $1 = C_{ab}$ and $1 \equiv ba \pmod m$ □

Alternative proof. Since $\Lambda_m \equiv A/aA$ as an A-module, there exists β such that $\beta \to 1$ where the " $\to$ " represents the isomorphism from Λ_m to A/aA. And if λ_m is a generator of Λ_m, then there exists b such that $\lambda_m \to b = b.1$ and $(b, m) = 1$. Thus $\lambda_m = b.\beta = C_b(\beta)$, then $C_a(\lambda_m) \to ab$ and ab is a generator of A/aA if and only if $(a, m) = 1$. □

Having this lemma, we set $m_i = \frac{m}{P_i^{e_i}}$, one can see that $C_{m_i}(\lambda_m)$ is a generator of $\Lambda_{P_i^{e_i}}$. For an easy notation we set $\lambda_{P_i^{e_i}} = C_{m_i}(\lambda_m)$. Since $\lambda_{P_i^{e_i}} \in \Lambda_m$ we have $K_{P_i^{e_i}} = k(\lambda_{P_i^{e_i}}) \subseteq k(\lambda_m)$, and thus, the compositum of the fields $K_{P_i^{e_i}}$ is contained in K_m. Clearly we have $(m_1, m_2, ..., m_t) = 1$. Then, there exists a set of polynomials $a_1, a_2, ..., a_t$ in A such that $\sum_{i=1}^t a_i m_i = 1$. It implies that $\sum_{i=1}^t C_{a_i} C_{m_i} = 1$. We apply λ_m to both sides, then we get $\sum_{i=1}^t C_{a_i}(\lambda_{P_i^{e_i}}) = \lambda_m$. Therefore K_m is contained in the compositum of the fields $K_{P_i^{e_i}}$.

The following proposition will imply theorem 2.2.1.

Proposition 2.2.3. *Let $P \in A$ be a monic irreducible polynomial and $e \in \mathbb{Z}$ a positive integer. Then, the prime ideal PA is totally ramified in K_{P^e} with ramification index $\phi(P^e)$ and the prime ideal above PA is $\lambda_{P^e}\mathcal{O}_{P^e}$ where λ_{P^e} is a generator of Λ_{P^e}. If $QA \neq PA$ is a prime ideal then, QA is unramified in K_{P^e}.*

To be able to prove this proposition we need the following two lemmas.

Lemma 2.2.4. *Let $\mathcal{O}_m$ be the integral closure of A in K_m and λ_m a generator of Λ_m. Suppose $(a, m) = 1$. Then, $C_a(\lambda_m)/\lambda_m$ is a unit in $\mathcal{O}_m$.*

Proof. We have $C_a(\lambda_m)/\lambda_m \in \mathcal{O}_m$. Since $(a, m) = 1$ there exists $b, f \in A$ such that $C_aC_b + C_fC_m = 1$. Thus $C_b(C_a(\lambda_m)) = \lambda_m$ and $\frac{\lambda_m}{C_a(\lambda_m)} = \frac{C_b(C_a(\lambda_m))}{C_a(\lambda_m)}$, but following the same logic we see that $\frac{C_b(C_a(\lambda_m))}{C_a(\lambda_m)} \in \mathcal{O}_m$. □

Lemma 2.2.5. . *Let P be a monic irreducible polynomial in A and e a positive integer. Then λ is a generator of Λ_{P^e} if and only if $C_{P^e}(\lambda) = 0$ and $C_{P^{e-1}}(\lambda) \neq 0$.*

Proof. We know that $\Lambda_{P^e} \cong A/P^eA$ as A-module. We denote by " $*$ " and "." the actions of A on Λ_{P^e} and A/P^eA respectively. Let λ be a generator of Λ_{P^e} and m its image in A/P^eA. Then the following are equivalent:

i) m is a generator of A/P^eA.

ii) $(m, P) = 1$

iii) $P^{e-1} \,.\, m \neq 0$

iv) $P^{e-1} \ * \ \lambda_m \neq 0$

v) $C_{P^{e-1}}(\lambda) \neq 0$

□

By this lemma the generators of Λ_{P^e} are precisely the roots of the polynomial

$$\begin{aligned}\mathcal{F}(x) &= \frac{C_{P^e}(x)}{C_{P^{e-1}}(x)} \\ &= \frac{C_P(C_{P^{e-1}}(x))}{C_{P^{e-1}}(x)} \\ &= P + [P,1]C_{P^{e-1}}(x)^{q-1} + ... + [P,d]C_{P^{e-1}}(x)^{q^d-1}., \end{aligned} \tag{2.9}$$

Where the $[P,i]$'s are polynomials in A and d is the degree of P.

It is important to notice that the degree of $\mathcal{F}(x)$ is $\phi(P^e)$ as it should be.

Proof of the proposition. Following the same process as in the proof of the proposition 1.2.3, we see that PA is the only possible prime ideal in A ramified in K_{P^e}.

We have $\mathcal{F}(x) = \prod(x - \zeta)$ where ζ runs through the generators of Λ_{P^e} and by lemma 2.2.2 we have

$$\mathcal{F}(x) = \prod_{\substack{(a,P)=1 \\ a \in A/P^eA}} (x - C_a(\lambda_{P^e}))$$

Substituting x by 0 in the equation 2.9 we get,

$$P = \pm \prod_{\substack{(a,P)=1 \\ a \in A/P^eA}} C_a(\lambda_{P^e})$$

Using the lemma 2.2.4, we see that $P = \lambda_{P^e}^{\phi(P^e)} \times unit$. It follows that $PA.\mathcal{O}_{P^e} = P.\mathcal{O}_{P^e} = (\lambda_{P^e})^{\phi(P^e)}$. Let $\mathfrak{P}$ be a prime which lies above PA. Then the ramification index $e(\mathfrak{P}/PA)$ is divisible by $\phi(P^e)$, but looking at the degree of $\mathcal{F}(x)$ we have $[K_{P^e} : k] \leq \phi(P^e)$. Therefore $e(\mathfrak{P}/PA) = \phi(P^e)$ and $\mathfrak{P} = (\lambda_{P^e}) = \lambda_{P^e}\mathcal{O}_{P^e}$. □

The proposition says that $[K_{P_i^{e_i}} : k] = \phi(P_i^{e_i})$ and all the fields $K_{P_i^{e_i}}$ are pairwise linearly disjoint. Therefore

$$\begin{aligned}[K_m : k] &= [K_{P_1^{e_1}} : k][K_{P_2^{e_2}} : k]...[K_{P_t^{e_t}} : k] \\ &= \phi(P_1^{e_1})\phi(P_2^{e_2})...\phi(P_t^{e_t}) \\ &= \phi(m). \end{aligned} \tag{2.10}$$

That completes the proof of the theorem. Since K_m is the compositum of the fields $K_{P_i^{e_i}}$, all the P_iA are ramified in K_m. If $QA \neq P_iA$ for every i then, by the proposition above QA is unramified in $K_{P_i^{e_i}}$ for every $1 \leq i \leq t$. Thus QA is unramified in K_m. In summary we have

Theorem 2.2.6. *Let $m \in A$ be a polynomial of positive degree and let $m = \alpha P_1^{e_1} P_2^{e_2} ... P_t^{e_t}$ be its prime decomposition. Then, K_m is the compositum of the fields $K_{P_i^{e_i}}$. The only prime ideals in A ramified in K_m are the P_iA's with $1 \leq i \leq t$.*

2.3 Finite primes

The last theorem in the previous section is one of the results which shows how function fields are similar to number fields. As promised in the introduction we still need to investigate other results. We will show in this section how finite primes in A split in $\mathcal{O}_m$, the integral closure of A in K_m. At the same time we will explore the analogue of the result about the Artin automorphism. We first need to find $\mathcal{O}_m$.

Let $m = \alpha P_1^{e_1} P_2^{e_2} ... P_t^{e_t}$ be the prime decomposition of m. We already have the hypothesis of the proposition 1.2.2, hence $\mathcal{O}_m = \vee \mathcal{O}_{P_i^{e_i}}$ for all $1 \leq i \leq t$. And for a monic irreducible polynomial P in A we have

Proposition 2.3.1. *Let λ_{P^e} be a generator of Λ_{P^e}. Then, $\mathcal{O}_{P^e} = A[\lambda_{P^e}]$.*

Proof. Let $w \in \mathcal{O}_{P^e}$. Since $[K_{P^e} : k] = \phi(P^e)$, we can write w in this form,

$$w = \sum_{i=0}^{\phi(P^e)-1} a_i \lambda_{P^e}^i \quad \text{where all the } a_i \in k \tag{2.11}$$

We will just prove that all the a_i's can be chosen in A. The discriminant of $A[\lambda_{P^e}]$ is a power of P, then each a_i is of the form $\frac{b_i}{P^n}$ where $b_i \in A$ and n a positive integer. We can choose n in such a way that at least one of the b_i is not divisible by P. Otherwise $w = Pw'$ and we do the proof with w'. Having that we get

$$P^n w = \sum_{i=0}^{\phi(P^e)-1} b_i \lambda_{P^e}^i. \tag{2.12}$$

If we can prove that $n = 0$ then we are done. To see this we will consider the discreet valuation of K_m/k at P, noted by v_P, of both sides of the equation 2.12. Before that we should notice that $\phi(P^e).v_P = v_{(\lambda_{P^e})}$ where $v_{(\lambda_{P^e})}$ is the discreet valuation of K_m/k at (λ_{P^e}). This is a direct consequence of the proposition 2.2.3. Now let i_0 be the smallest integer in $1, 2, ..., \phi(P^e) - 1$ such that $v_P(b_{i_0}) = 0$. i_0 exists since at least one of the b_i's is not divisible by P. We have

$$v_P(P^n w) = v_p(\sum_{i=0}^{\phi(P^e)-1} b_i \lambda_{P^e}^i) \tag{2.13}$$

One can show that the numbers $v_P(b_i\lambda_{P^e}^i)$, $1 \leq i \leq \phi(P^e) - 1$ are distinct. Then

$$\begin{aligned} v_P(P^n w) &= min\left\{v_P(b_i\lambda_{P^e}^i),\ 1 \leq i \leq \phi(P^e) - 1\right\} \\ &\leq v_p(b_{i_0}\lambda_{P^e}^{i_0}) \\ &= v_p(\lambda_{P^e}^{i_0}) \end{aligned}$$

It is clear that $v_P(P^n w) \geq n$, and,

$$v_p(\lambda_{P^e}^{i_0}) = \frac{1}{\phi(P^e)}.v_{(\lambda_{P^e})}(\lambda_{P^e}^{i_0}) = \frac{i_0}{\phi(P^e)} \tag{2.14}$$

So n must be zero since these two valuations must be equal. We have proven $\mathcal{O}_{P^e} \subseteq A[\lambda_{P^e}]$. The other inclusion is straightforward. □

By this proposition $\mathcal{O}_{P_i^{e_i}} = A[\lambda_{P_i^{e_i}}]$ for any $1 \leq i \leq t$. Hence

$$\begin{aligned} \mathcal{O}_m &\subseteq \vee\mathcal{O}_{P_i^{e_i}} \\ &\subseteq \vee A[\lambda_{P_i^{e_i}}] \\ &\subseteq A[\lambda_m]. \end{aligned}$$

Since the other inclusion is obvious we have proved

Proposition 2.3.2. *Let $\mathcal{O}_m$ be the integral closure of A in K_m and λ_m be a generator of Λ_m. Then $\mathcal{O}_m = A[\lambda_m]$.*

Remark 2.3.3. Before we state the analogues of the results about the Artin automorphism, we need to look closely at the isomorphism from $\mathrm{Gal}(K_m/k)$ to $(A/mA)^*$

in the theorem 2.2.1. Let λ_m be a generator of Λ_m. Then, for any $\sigma \in \mathrm{Gal}(K_m/k)$, $\sigma(\lambda_m)$ is also a generator of Λ_m. Then, from our discussion in the second section there exists an $a \in A/mA$ with $(a, m) = 1$ such that $\sigma(\lambda_m) = C_a(\lambda_m)$. Since $K_m = k(\lambda_m)$, the automorphism σ is completely determined by this last equation. Hence the map that sends σ to a is the isomorphism from $\mathrm{Gal}(K_m/k)$ to $(A/mA)^*$, and we write $\sigma = \sigma_a$. Now let P be a monic irreducible polynomial in A with $(P, m) = 1$ and $\deg(P) \leq \deg(m)$. We let $\sigma_P \in \mathrm{Gal}(K_m/k)$ be the preimage of $P \in (A/mA)^*$.

Remark 2.3.4. Let P be a monic irreducible polynomial in A, with $(P, m) = 1$ and $\deg(P) \leq \deg(m)$, and let $\mathfrak{P}$ a prime ideal of $\mathcal{O}_m$ which lies above PA. We set $i = \mathcal{O}_m/\mathfrak{P}$, $j = A/PA$ and $|P| = q^{\deg(P)}$. We should notice that the number of elements in j is $|P|$. Let $D(\mathfrak{P}/PA) = \{\sigma \in \mathrm{Gal}(K_m/k) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ the decomposition group, then $D(\mathfrak{P}/PA) \cong \mathrm{Gal}(i/j)$. The Artin automorphism in $D(\mathfrak{P}/PA)$, denoted $(PA, K_m/k)$, corresponds to the $|P|$-th power Frobenius map in $\mathrm{Gal}(i/j)$. In other words we have,

$$(PA, K_m/k)(\omega) \equiv \omega^{|P|} \pmod{\mathfrak{P}} \quad \text{for any } \omega \in \mathcal{O}_m. \tag{2.15}$$

Now we are in a position to state and prove the following theorem.

Theorem 2.3.5. *With the all the notations above we have $\sigma_P = (PA, K_m/k)$.*

Proof. The polynomial $C_P(x)/x$ is an Eisenstein polynomial at P. In fact $C_P(x)/x$ is $\mathcal{F}(x)$ for $e = 1$. It implies that $C_P(x)$ is also an Eisenstein polynomial at P. Since C_P has degree $q^{\deg(P)}$ and P is monic we have $C_P(x) \equiv x^{|P|} \pmod{P}$. Since $P \in \mathfrak{P}$, we get

$$C_P(x) \equiv x^{|P|} \pmod{\mathfrak{P}} \tag{2.16}$$

Now let $\omega \in \mathcal{O}_m$. By proposition 2.3.2, we can write $\omega = \sum_i a_i \lambda_m^i$ where $a_i \in A$. Then we get,

$$\begin{aligned} \sigma_P(\omega) &= \sigma_P(\sum_i a_i \lambda_m^i) \\ &= \sum_i a_i \sigma_P(\lambda_m^i) \\ &= \sum_i \sigma_P(\lambda_m)^i \end{aligned}$$

However from the equation 2.16, $\sigma_P(\lambda_m) = C_P(\lambda_m) \equiv \lambda_m^{|P|} \pmod{\mathfrak{P}}$. Hence,

$$\sigma_P(\omega) \equiv \sum_i a_i \lambda_m^{|P|i} \tag{2.17}$$

Using Fermat's Little Theorem for polynomials and the fact that $|P|$ is a power of the characteristic of k, one sees easily that

$$\sigma_P(\omega) \equiv (\sum_i a_i \lambda_m^i)^{|P|} \equiv \omega^{|P|} \pmod{\mathfrak{P}}. \tag{2.18}$$

This last equation completes the proof. □

Theorem 2.3.6. *Let $P \in A$ be a monic irreducible polynomial not dividing m, and let f be the smallest positive integer such that $P^f \equiv 1 \pmod{m}$. Then, $P\mathcal{O}_m$ is the product of $\phi(m)/f$ prime ideals each of degree f. Consequently PA splits completely if and only if $P \equiv 1 \pmod{m}$*

Proof. It follows exactly the process in the proof of the theorem 1.2.8 □

We should notice now that we only need to see how the prime at infinity splits to complete our task for this chapter. To be able to do it we need some preliminaries.

2.4 Newton polygon

To see how the prime at infinity splits, we have to consider the property of the roots of C_m for some polynomial m in A. One way to deal with it is by investigating an elementary technique of non-archimedean analysis, the Newton polygon. In [Rob] one can read more about Newton polygons.

Much more of the proofs in Cyclotomic theory are done in complete fields. More precisely, for instance the case of function fields, having a prime P of k, it is helpful to take the completion k_P of k with respect to the valuation v_P. For further study on that one can read [Sti].

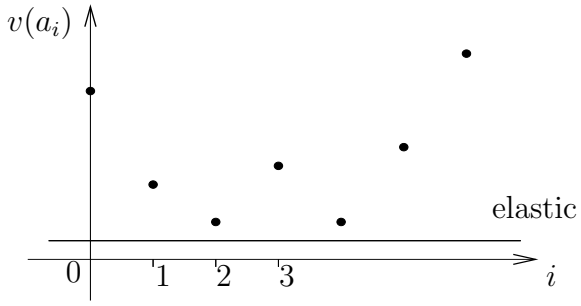
We let v be a discrete valuation (at finite or infinite prime), and denote by k_v the

completion of k at v. Let K be a finite extension of k_v. Then v extends to K uniquely (see for example [Rob]). From now on forward we will also denote v this extension.

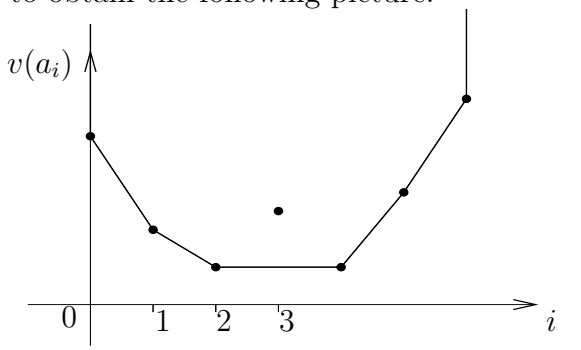
Let $f(x) = \sum_{i=0}^{d} a_i x^i \in k_v[x]$. We assume that a_0 and a_d are nonzero elements. We consider the set of points:

$$S_f = \big\{(i, v(a_i)) \in \mathbb{R}^2 \mid 0 \leq i \leq d,\ a_i \neq 0\big\}$$

suppose we can draw a horizontal straight line under all the points



Thinking of the straight line as an elastic band, we can wrap all the points and pull the ends up to infinity to obtain the following picture.



With this process we will have a polygon path connecting $(0, v(a_0))$ with (d, v_d). This polygonal path is called the Newton polygon of f. Formally, we have constructed the lower convex hull of the set S_f.

Theorem 2.4.1. *With the same notation as above we let $\bar{k_v}$ denote the algebraic closure of k_v and $f(x) = \sum_{i=0}^{d} a_i x^i \in k_v[x]$ a polynomial with $a_0 a_d \neq 0$. Let l be a line segment of the Newton polygon of f joining the points $(i, v(a_i))$ and $(j, v(a_j))$ with $i \leq j$. Then $f(x)$ has exactly $j - i$ roots $\ddot{\lambda} \in \bar{k_v}$ such that $v(\ddot{\lambda}) = -s$ with s the slope of l.*

2.5 Infinite prime

Finally, Having developed some prerequisites in the two previous sections, we are now in good position to deal with our last task in this chapter. We will turn our intention mostly to the completion of k at ∞, k_∞. We are still using the notation that we used before. The polynomial $C_m(x) = \sum_{i=0}^{d}[m,i]x^{q^i}$ where $[m,i] \in A$ and $\deg([m,i]) = (d-1)q^i$. To be able to apply the theorem 2.4.1 we consider $f(x) = C_m(x)/x = \sum_{i=0}^{d}[m,i]x^{q^i-1}$. Then we have $v_\infty([m,i]) = -(d-i)q^i$ and

$$S_f = \left\{((q^i-1), -(d-i)q^i) \mid 0 \leq i \leq d\right\}.$$

A line segment connecting two successive points in S_f give slope:

$$\frac{-(d-i)q^i - (-(d-i+1)q^{i-1})}{q^i - q^{i-1}} = -(d-1) + \frac{1}{q-1}$$

With a little reflection one could check that the Newton polygon for f is just the union of the all line segments connecting two successive points in S_f. Since $C_m(x) = x.f(x)$ by theorem 1.3.4 there exist exactly $q^i - q^{i-1}$ roots $\ddot{\lambda} \in \bar{k}_\infty$ of $C_m(x)$ such that,

$$v_\infty(\ddot{\lambda}) = d - i - \frac{1}{q-1}$$

In particularly, there are $q-1$ roots $\ddot{\lambda}$ of $C_m(x)$ in $\bar{k}_\infty$ such that $v_\infty(\ddot{\lambda}) = d-1-\frac{1}{q-1}$. And more, for each such root, we have $\ddot{\lambda}^{q-1}$ in k_∞.

Let us now proceed gradually to the last task of this chapter. Since $\bar{k}_\infty$ is an A-algebra, we can use the Carlitz action to make it into an A-algebra different for the trivial one as we did for $\bar{k}$. It means, if $m \in A$ and $u \in \bar{k}_\infty$, we define $m.u = C_m(u)$. We set the torsion module:

$$\ddot{\Lambda_m} = \left\{\ddot{\lambda} \in \bar{k}_\infty \mid C_m(\ddot{\lambda}) = 0\right\}$$

Proposition 2.5.1. *Let h be a monomorphism over k from K_m to $\bar{k}_\infty$. Let $\ddot{\lambda}_m \in \ddot{\Lambda_m}$ such that $v_\infty(\ddot{\lambda}_m) = (d-1) - \frac{1}{q-1}$ and let $\lambda_m \in k_m$ such that $h(\lambda_m) = \ddot{\lambda}_m$. Then, we have $k(\Lambda_m) = k(\lambda_m)$ and $k_\infty(\ddot{\Lambda_m}) = k_\infty(\ddot{\lambda_m})$.*

Proof. Suppose that λ is root of $C_m(x) \in \bar{k}$. Since $C_m(\lambda) = 0$ implies $C_m(h(\lambda)) = 0$, we see that h maps Λ_m to $\ddot{\Lambda}_m$. The map is in fact an A-module isomorphism. The element $\ddot{\lambda}_m$ exists by the discussion above. To complete the proof we just need to prove that $\ddot{\lambda}_m$ is a generator of $\ddot{\Lambda_m}$. Suppose $0 \neq a \in A$ of degree less that d. Then,

$$v_\infty(C_a(\ddot{\lambda}_m)) \;=\; v_\infty(\sum_{i=0}^{\deg(a)} [a,i]\ddot{\lambda}_m^{q^i})$$

By proposition 2.2.2 one has,

$$\begin{aligned} v_\infty(C_a(\ddot{\lambda}_m)) &= min\left\{v_\infty([a,i]\ddot{\lambda}_m^{q^i}) \mid 0 \leq i \leq \deg(a)\right\} \\ &= v_\infty(a\ddot{\lambda}_m) \\ &= d - \deg(a) - 1 - \frac{1}{q-1} \end{aligned}$$

If $\ddot{\lambda}_m$ were not an A-module generator of $\ddot{\Lambda_m}$ there would be a proper divisor a of m such that $C_a(\ddot{\lambda}) = 0$. But this is impossible since $v_\infty(0) = \infty \neq d - \deg(a) - 1 - \frac{1}{q-1}$.

□

Finally, the next two theorems will complete our task. For that we need to appeal to our notation, $\sigma_a \in \mathrm{Gal}(K_m/k)$ for some $a \in A$, as we defined in the section 2.3.

Theorem 2.5.2. *Let $\Omega = \{\sigma_\alpha \in \mathrm{Gal}(K_m/k) \mid \alpha \in \mathbb{F}^*\}$ and set K_m^+ the fixed field of Ω. Then ∞ splits completely in K_m^+.*

Proof. Let λ_m be the element defined in the proposition 2.5.1. Let $\sigma_\alpha \in \Omega$. Then, $\sigma_\alpha(\lambda_m^{q-1}) = (\alpha\lambda_m)^{q-1} = \lambda_m^{q-1}$ for any $\alpha \in \mathbb{F}^*$. Hence $k(\lambda_m^{q-1}) \subseteq K_m^+$. It follows that

$$[K_m : K_m^+] \leq [K_m : k(\lambda_m^{q-1})].$$

Since $K_m = k(\lambda_m)$, we have $[K_m : k(\lambda_m^{q-1})] \leq q-1$. However, by Galois theory, $[K_m : K_m^+] = q-1$. So K_m^+ must be equal to $k(\lambda_m^{q-1})$. Now we let h be the embedding that we defined in the proposition 2.5.1. We see that $h(K_m^+) = h(k(\lambda_m^{q-1})) \subseteq k_\infty(\ddot{\lambda}_m^{q-1})$ and we have $h(K_m^+) \subseteq k_\infty$. Since $e(k_\infty/k) = f(k_\infty/k) = 1$, the prime at infinity splits completely in K_m^+. □

Theorem 2.5.3. *Let* $\Omega = \{\sigma_\alpha \in \mathrm{Gal}(K_m/k) \mid \alpha \in \mathbb{F}^*\}$ *and set* K_m^+ *the fixed field of* Ω*. Then every prime above* ∞ *is totally and tamely ramified in* K_m/K_m^+*.*

Proof. Let h be the embedding of proposition 2.5.1. Then we set

$$\mathcal{V}_\infty = \{w \in K_m \mid v_\infty(h(w)) \geq 0\}.$$

It is a discrete valuation ring inside K_m, its maximal ideal is

$$\mathfrak{P}_\infty = \{w \in K_m \mid v_\infty(h(w)) > 0\}.$$

We set $\mathcal{O}_\infty = \{w \in k \mid v_\infty(w) \geq 0\}$. Since h fixes all elements in k, we have $\mathcal{O}_\infty \subseteq \mathcal{V}_\infty$. Hence the prime $\mathfrak{P}_\infty$ lies above ∞ and the embedding h corresponds to a prime of K_m lying above ∞. Let $\mathcal{P}_\infty$ be the prime of K_m^+ lying below $\mathfrak{P}_\infty$. By the proof of the theorem above, the completion of K_m^+ at $\mathcal{P}_\infty$ is k_∞. Since $h(K_m) = k(\ddot{\lambda}_m)$, it is clear that the completion of K_m at $\mathfrak{P}_\infty$ is $k_\infty(\ddot{\lambda}_m)$. We should notice from that that that $\mathcal{P}_\infty$ is totally ramified if and only if $[k_\infty(\ddot{\lambda}_m) : k_\infty] = q - 1$. Let us then prove that the degree of the extension of $k_\infty(\ddot{\lambda}_m)/k_\infty$ is $q - 1$. By proposition 2.5.1, $v_\infty(\ddot{\lambda}_m) = (d-1) + \frac{1}{q-1}$. Since v_∞ is a discrete valuation ring,

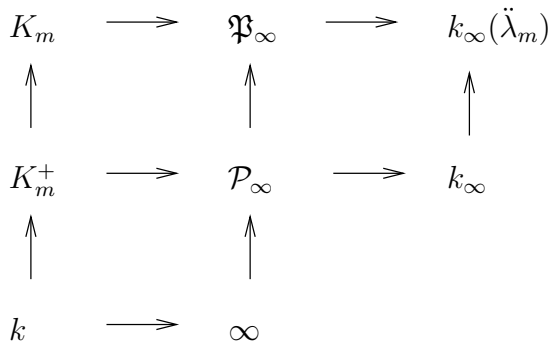
$$e(\mathfrak{P}_\infty/\mathcal{P}_\infty) = [k_\infty(\ddot{\lambda}_m) : k_\infty] \geq q - 1.$$

On the other hand $\ddot{\lambda}_m$ is a root of $x^{q-1} - \ddot{\lambda}_m^{q-1} \in k_\infty$. Then

$$[k_\infty(\ddot{\lambda}_m) : k_\infty] \leq q - 1.$$

These two last equations show that $[k_\infty(\ddot{\lambda}_m) : k_\infty] = q - 1$. $\mathcal{P}_\infty$ is of course tamely ramified since $q - 1$ is not divisible p. This completes the proof since in a Galois extension all the primes behave the same. □

.


K_m
$\mathfrak{P}_\infty$
$k_\infty(\ddot{\lambda}_m)$
K_m^+
$\mathcal{P}_\infty$
k_∞
k
∞

Chapter 3

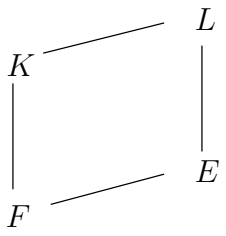
Kronecker-Weber theorem for Function Fields

In the previous chapter, we have described explicitly the cyclotomic function field K_m, One would now expect that, as for the cyclotomic number fields, all finite abelian extensions of $k := \mathbb{F}(T)$ will be contained in K_m for some $m \in A$. To begin this chapter, we show that this is impossible. For that we first need to introduce some definitions. Throughout this chapter we keep the notations that we used before.

In general, for an extension field K/F, K is a function field in one variable over F if K contains one transcendental element x over F such that $K/F(x)$ is a finite extension. An obvious example of that is the rational function field $F(T)$ over F. The field F is called the full constant field of K if F is algebraically closed in K. In this case we say K/F is a constant field. The field K is called a global function field if F is finite.

Let K/F be a constant field and L be a finite extension of K. Let E be the algebraic closure of F in L. Then L/E is a constant field. If $L = EK$ then we say L is a constant field extension of K. If $E = F$ then we say that L is a geometric extension of K. We nota that EK is a constant field extension of K and L is a geometric extension of K. One should notice that, by definition, a geometric extension field cannot contain a constant field extension.

.



The following proposition is one way to see that not all finite abelian extensions of $k := \mathbb{F}(T)$ will be inside of K_m for some $m \in A$.

Proposition 3.0.4. *Let n be a positive integer and m a polynomial in A.*

i) Let $\mathbb{F}_n$ be a finite extension of $\mathbb{F}$ of degree n. Then $\mathbb{F}_n k$ is an abelian constant field extension of k.

ii) K_m is a geometric extension of k.

Proof. By proposition 1.2.1 in [Sti], the full constant field of k is $\mathbb{F}$. Since $\mathbb{F}_n$ is algebraic over $\mathbb{F}$, the field $\mathbb{F}_n k$ is a constant extension of k. It is clear that $\mathbb{F}_n k = \mathbb{F}_n(T)$, and we have

$$\mathrm{Gal}(\mathbb{F}_n k/k) \cong \mathrm{Gal}(\mathbb{F}_n(T)/\mathbb{F}(T)) \cong \mathrm{Gal}(\mathbb{F}_n/\mathbb{F}) \tag{3.1}$$

By Galois theory $\mathrm{Gal}(\mathbb{F}_n/\mathbb{F})$ is a cyclic group. Thus $\mathbb{F}_n k/k$ is an abelian extension.

To see the second part of the proposition we need the last two theorems in the previous chapter. Let $\mathcal{O}_\infty$ be the valuation ring of k at ∞. Then, the quotient $\mathcal{O}_\infty/\infty$ is just $\mathbb{F}$. Let P_∞ be a prime in K_m^+ lying above ∞. By theorem 2.5.2, $f(P_\infty/\infty) = 1$, then the residue class field at P_∞ is $\mathbb{F}$. Let $\mathfrak{P}_\infty$ be a prime lying above P_∞. By theorem 2.5.3, $f(\mathfrak{P}_\infty/P_\infty) = 1$, then the residue field at $\mathfrak{P}_\infty$ is also $\mathbb{F}$. By the residue class map we can embed the full constant field of K_m into the residue filed at $\mathfrak{P}_\infty$. That completes the proof. □

Moreover, in K_m, a piece containing the extension where ∞ is wildly ramified is lacking. This chapter has three sections. In the first section, we construct the field $\mathcal{A}$ which is shown to be the maximal abelian extension of k in section 4. Section 2 will focus on the homomorphism from the group of k-ideles J into the Galois group

of $\mathcal{A}/k$. This homomorphism is in fact the reciprocity law homomorphism from Class Field Theory.

3.1 Compositum field $\mathcal{A}$

As told before, K_m is not big enough to cover all abelian extensions. In this section we construct three pairwise linearly disjoint extensions (K^+, $\tilde{K}$, L^-) and take a careful look to their Galois groups. The compositum of these fields will be the maximal abelian extension. We first fix our notation to begin this section. We will follow closely the paper [Hay]. However, instead of just copying we will explain all the details, provide the missing proofs and try to make the context self contained.

Notation 3.1.1. Let X and Y by two topological groups. If there is a map, both homomorphism and homeomorphism, from X into Y then we write $X \approx Y$. We denote by $\varprojlim$ the projective limit.

To describe the Galois group of these extensions we need the following theorem which is just a particular case of the example 1, page 271 in [Neu].

Theorem 3.1.2. *Let F be a field and $(K_i)_{i\in I}$ a family of finite Galois extensions of F. Let $K = \bigcup_i K_i$, then*

$$\mathrm{Gal}(K/F) \approx \varprojlim_{i\in I} \mathrm{Gal}(K_i/K). \tag{3.2}$$

These are the three extensions of k:

1. Let K^+ be the union of all the fields K_m for all polynomials m in A. Then, the Galois group $\mathrm{Gal}(K^+/k)$ is the projective limit of $\mathrm{Gal}(K_m/k)$. And by theorem 2.2.6, we have

$$G^+ := \mathrm{Gal}(K^+/k) \approx \varprojlim_{m\in A} (A/mA)^*. \tag{3.3}$$

   The group G^+ acts on K^+ via its quotient groups $(A/mA)^*$. We recall that $\sigma(\lambda_m) = C_a(\lambda_m) = a * \lambda_m$ for some $a \in (A/mA)^*$.

2. Let $\bar{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$ and $\tilde{K} = \bar{\mathbb{F}}k$ be the compositum of the fields $\bar{\mathbb{F}}$ and k. The field $\tilde{K}$ is in fact the maximal constant field extension of k. Let $\mathbb{F}_n$ be the field $\mathbb{F}$ adjoining the roots of the polynomial $x^{q^n} - x$. $\mathbb{F}_n/\mathbb{F}$ is a Galois extension of degree n and

$$\mathrm{Gal}(\mathbb{F}_n/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z} \tag{3.4}$$

The Galois group of $\mathbb{F}_n/\mathbb{F}$ is generated by the Frobenius automorphism $x \to x^q$. It is clear that $\tilde{K}$ is the union of the all fields $\mathbb{F}_n k$ for all positive integers n. Since $\mathrm{Gal}(\mathbb{F}_n k/k) \cong \mathrm{Gal}(\mathbb{F}_n/\mathbb{F})$, we have

$$\tilde{G} := \mathrm{Gal}(\tilde{K}/k) \approx \varprojlim_{n \in \mathbb{N}^*} \mathbb{Z}/n\mathbb{Z} \tag{3.5}$$

$\tilde{G}$ is, then generated as a topological group by the unique automorphism `Frob` of $\tilde{K}/k$ whose restriction to $\bar{\mathbb{F}}$ is the Frobenius automorphism $x \to x^q$.

3. The third field is obtained by reworking the theory which is developed in chapter 2 but using $\frac{1}{T}$ instead of T. For that we have $C_{1/T} = \frac{1}{T} + \tau$. We adjoin the elements of $\Lambda_{1/T^{n+1}}$ to k to form the field $K_n^- := k(\Lambda_{1/T^{n+1}})$. Considering the isomorphism $T \to 1/T$, one has almost the same results between the extensions of $\mathbb{F}(T)$ and $\mathbb{F}(\frac{1}{T})$. For instance,

$$[K_n^- : k] = \phi(T^{n+1}) = q^{n+1} - q^n. \tag{3.6}$$

Let $A^- := \mathbb{F}(\frac{1}{T})$ and λ^- be the generator of $\Lambda_{1/T^{n+1}}$ as A^--module. One can see easily that, by translating remark 2.3.3, any polynomial $m^- \in A^-$ modulo $1/T^{n+1}$ with non zero constant term acts on K_n^- by way of the automorphism which takes λ^- to $C_{m^-}(\lambda^-)$. Let $\Omega := \{C_\alpha \in \mathrm{Gal}(K_n^-/k) \mid \alpha \in \mathbb{F}^*\}$ and we set L_n^- the fixed field of Ω. By Galois theory, $[K_n^- : L_n^-] = q-1$. It is now clear that the extension L_n^-/k is Galois of degree q^n. By proposition 2.2.3, the prime ideal TA is totally ramified in K_{T^n}, hence so is ∞ in K_n^-. Since $[L_n^- : k] = q^n$ the prime at infinity is totally and wildly ramified in L_n^-. It is obvious that, by our construction, $\mathrm{Gal}(L_n^-/k)$ can be identified with the group G_n of polynomials in $\frac{1}{T}$ mod $1/T^{n+1}$ which have constant term 1. We set L^- the union of all fields

L_n^-. Then

$$G^- := \mathrm{Gal}(L_n^-/k) \approx \varprojlim_{n\in\mathbb{N}^*} G_n \tag{3.7}$$

For any positive integer n, $L_n^- \subseteq L_{n+1}^-$. Then taking the natural ordering on $\mathbb{N}^*$, we have $x_{n+1} \equiv x_n \mathrm{mod}\ n$ for any $(x_n) \in \varprojlim G_n$. Thus G^- is identified with the multiplicative group in the ring of formal power series $\mathbb{F}[[\frac{1}{T}]]$ consisting of those power series with constant term 1. G^- acts on L^- via its quotient groups G_n.

We take $\mathcal{A}$ to be the compositum of K^+, $\tilde{K}$ and L^-. We should notice that our constructions are explicit. In another words each one of the finite subextension of $\mathcal{A}$ is generated by the roots of a polynomial which we can write down. The following proposition tells us about the nature of $G_{\mathcal{A}} := \mathrm{Gal}(\mathcal{A}/k)$.

Proposition 3.1.3. *The extension K^+/k and $\tilde{K}/k$ are linearly disjoint, and their compositum $K^+.\tilde{K}/k$ is linearly disjoint from L^-/k. Consequently,*

$$G_{\mathcal{A}} \cong G^+ \times \tilde{G} \times G^- \tag{3.8}$$

Proof. Let r be a positive integer and $m \in A$. By theorem III.6.3 in [Sti], $\mathbb{F}_r k/k$ is an unramified extension. In particular ∞ is unramified in this field. However we see from theorem 2.5.3 that ∞ is tamely ramified in K_m. Thus $K_m \bigcap \mathbb{F}_r k = k$. Since r and m have been chosen arbitrary, the extensions K^+/k and $\tilde{K}/k$ are linearly disjoint. Let s be a positive integer. We have seen that the prime ideal ∞ is ramified in L_s^-. Since any finite subextension of $K^+.\tilde{K}/k$ is contained in the composite of a finite constant field extension of k and some K_m, ∞ is tamely ramified in $K^+.\tilde{K}/k$. But ∞ is totally ramified in L_n^-. Therefore $K^+.\tilde{K} \bigcap L_n^- = k$. □

3.2 Homomorphism ψ

In the previous section we have constructed the field $\mathcal{A}$. We now proceed to construct a homomorphism ψ from the group of k-ideles J into the Galois group $G_{\mathcal{A}}$. This homomorphism is proved in the last section to be the reciprocity law homomorphism.

Our first task is to write J as a direct product of four of its subgroups. From now on forward, by abuse of language, we denote by P a prime in k. The prime P could be finite or infinite. The difference between k and $\mathbb{Q}$ is the fact that all primes in k are non-archimedean.

Setting $|x_1 - x_2|_P = q^{-v_P(x_1-x_2)}$, k becomes a metric space. We denote by k_P the completion of k at P with respect to this distance. k_P is a topological group. For instance, choosing the prime TA, two polynomials will be close to one another in the resulting topology if their "initial coefficients coincide". For $u \in k_P$ and $\rho \in \mathbb{R}_+^*$ the set $\mathtt{B}(u,\rho) = \{x \in k_P \mid |u-x|_P < \rho\}$ is a basic system of neighbourhoods of u. We define the induced topology on k_P^*.

We denote by $\mathcal{M}_P$ (respectively $\mathcal{U}_P$)the maximal ideal (the group of units) of $\mathcal{O}_P$. If We denote by π_P be the uniformizing parameter at P, One has the following.

$$\begin{aligned}
k_P &= \left\{ x = \sum_{i=-n}^{\infty} a_i {\pi_P}^i \mid a_i \in \mathcal{O}_P/\mathcal{M}_P \right\} \\
&= \{x = u\pi_P^z \mid u \in \mathcal{U}_P \text{ and } z \in \mathbb{Z}\} \\
\mathcal{O}_P &= \{x \in k_P \mid v_P(x) \geq 0\} \\
&= \{x \in k_P \mid |x|_P \leq 1\} \\
&= \mathbb{F}[[\pi_P]], \text{ the ring of formal power series} \\
\mathcal{U}_P &= \{x \in k_P \mid v_P(x) = 0\} \\
&= \{x \in k_P \mid |x|_P = 1\} \\
&= \{x \in \mathbb{F}[[\pi_P]] \mid x \text{ has non} - \text{zero constant term}\} \\
\mathcal{M}_P &= \{x \in k_P \mid v_P(x) > 0\} \\
&= \{x \in k_P \mid |x|_P < 1\}
\end{aligned}$$

Proposition 3.2.1. *$\mathcal{U}_P$ is an open compact subset of k_P.*

Proof. Let $x = \sum_{i=0}^{\infty} a_i {\pi_P}^i \in \mathcal{U}_P$. It is clear that $\emptyset \neq \mathtt{B}(x,1) \subseteq \mathcal{U}_P$. Hence $\mathcal{U}_P$ is open. To complete the proof we just need to show that $\mathcal{U}_P$ is closed since $\mathcal{O}_P$ is compact. Let ${\mathcal{M}_P}^c = \{x \in k_P \mid |x|_P \geq 1\}$, then ${\mathcal{M}_P}^c$ is closed. In the other hand $\mathcal{U}_P = \mathcal{O}_P \bigcap {\mathcal{M}_P}^c$. Since $\mathcal{O}_P$ is closed then $\mathcal{U}_P$ is closed. □

We should notice that $\mathcal{U}_P$ is an open compact subset of k_P^* as well.

Writing $x = u\pi_P^z$ we have the following canonical map

$$\begin{aligned} \mathcal{U}_P &\rightarrow (\mathcal{O}_P/\mathcal{M}_P)^* \\ u &\rightarrow \bar{u} \text{ (constant term of u)} \end{aligned}$$

Then, we define a multiplicative homomorphism sgn_p by

$$\begin{aligned} sgn_p : k_P^* &\rightarrow (\mathcal{O}_P/\mathcal{M}_P)^* \\ u\pi_P^z &\rightarrow \bar{u} \end{aligned}$$

We set $V_P := ker(sgn_p)$ the kernel of sgn_p. Without effort, one has

$$V_P = \left\{ x = \sum_{i=-n}^{\infty} a_i {\pi_P}^i \in k_P^* \mid a_{-n} = 1 \right\} \tag{3.9}$$

With the same idea in the proof of the previous proposition it can be shown that V_P is an open subset of k_P^*. We let $k_P^1 = V_P \bigcap \mathcal{U}_P$. One can see easily that

$$k_P^1 = \{x \in \mathbb{F}[[\pi_P]] \mid \text{constant term of } x \text{ is } 1\} \tag{3.10}$$

and it is obviously an open subset of V_P.

Setting the induced topology from k_P on V_P and k_P^1, we have the following

Proposition 3.2.2. $V_P \approx k_P^1 \times \mathbb{Z}$

Before proving this proposition, we first consider the following lemma which is more general.

Lemma 3.2.3. *Let X be a topological space and V be a subgroup of X equipped with the induced topology. Let O be an open subgroup of V and D a discrete group. Suppose that there is a group isomorphism*

$$\begin{aligned} f \ : \ V &\rightarrow O \times D \\ x &\rightarrow (u, z) \end{aligned}$$

where there exist $z_0 \in D$ such that $u = f^{-1}(u, z_0)$ for any $u \in O$. Then, setting the induced topology on O, we have

$$V \approx O \times D.$$

Proof. Let $U \times Z$ be an open subset of $O \times D$. The following holds

$$f^{-1}(U \times Z) \;=\; \bigcup_{z \in Z} (\bigcup_{u \in U} f^{-1}(u, z))$$

Also $\bigcup_{u\in U} f^{-1}(u, z_0) = U \approx U \times \{z_0\} \approx U \times \{z\} \approx \bigcup_{u\in U} f^{-1}(u, z)$. Since O is open in V, then U is an open in V. Thus, for a fixed z, the set $\bigcup_{u\in U} f^{-1}(u, z)$ is an open subset of V. Therefore $\bigcup_{z\in Z}(\bigcup_{u\in U} f^{-1}(u, z))$ is an open in V, and f is continuous. Since D is discrete space, f^{-1} is continuous and that completes the proof. □

proof of the proposition 3.2.2. The map is given by

$$\begin{aligned} V_p &\to k_P^1 \times \mathbb{Z} \\ u\pi_P^z &\to (u, z). \end{aligned}$$

□

J is defined to be the set of $(j_P) \in \prod_P k_P^*$ such that j_P (the P-th coordinate of (j_P)) is in $\mathcal{U}_P$ for almost all primes P in k. The idele group comes equipped with a canonical topology. If we denote by (1_P) the element of J such that $1_P = 1$ for all P, then a basic system of neighbourhoods of $(1_P) \in J$ is given by the set

$$\prod_{P\in S} W_P \times \prod_{P\notin S} \mathcal{U}_P \tag{3.11}$$

where S runs through the finite sets of places of k, and $W_P \subseteq k_P^*$ is a basic system of neighbourhoods of $1 \in k_P^*$. For more about product topology one could see[G-A-C].

We are now going to describe four subgroups of J and later we write J as a direct product of these subgroups.

The group U_T. The groups $\mathcal{U}_P$'s are compact, hence so is $\prod_{P\neq\infty} \mathcal{U}_P$. If we let

$U_T = \{(j_P) \in J \mid j_\infty = 1, \text{ and } j_P \in \mathcal{U}_P \text{ for all } P \neq \infty\}$, then it is clear that $U_T \approx \prod_{P\neq\infty} \mathcal{U}_P$.

The group k^*. We can embed k^* into J by taking $x \in k_P^*$ to (x_P) where $x_P = x$ for all P. That is because for any $x \in k_P^*$, $v_P(x) = 0$ for all but finitely many P. The elements in k^* are often called principal ideles.

Proposition 3.2.4. *k^* is a discrete subgroup of J.*

Proof. We show that $(1_P) \in J$ has a neighbourhood which contains no other principal idele. Choose $S = \{\infty\}$, then

$$\mathtt{B} = \{(\alpha_P) \in J \mid |\alpha_P|_{P\neq\infty} = 1,\ |\alpha_\infty - 1|_\infty < 1\}$$

is a neighbourhood of (1_P). Suppose B contained a principal idele $x \in k^*$ different from (1_P), then by translating the proposition 1.3, page 185 in [Neu] from $\mathbb{Q}$ to $\mathbb{F}[T]$ we have

$$\begin{aligned} 1 &= \prod_P |x-1|_P \\ &= \prod_{P\neq\infty} |x-1|_P |x-1|_\infty. \end{aligned}$$

Since x is in B then

$$1 < \prod_{P\neq\infty} |x-1|_P \leq \prod_{P\neq\infty} \max\{|x|_P,\ 1\} \leq 1$$

And that is a contradiction. □

The groups k_∞^1 and $\mathbb{Z}$. We know already that $V_\infty \approx k_\infty^1 \times \mathbb{Z}$.

Proposition 3.2.5. *With the notations above, we have*

$$J \approx k^* \times U_T \times k_\infty^1 \times \mathbb{Z} \tag{3.12}$$

Proof. For an $(j_P) \in J$, let

$$d(j_P) = sgn_\infty(j_\infty).\prod_{P\neq\infty} \pi_P^{v_P(j_P)} \ \in k^*.$$

Then we Write

$$\begin{aligned}(j_P) &= d(j_P)\ .\ (j_P^*) \\ &= d(j_P)\ .\ (j_{P\neq\infty}^*)\ .\ j_\infty^*\end{aligned}$$

Obviously $j_P^* = j_P.d(j_P)^{-1}$. Let Q be a finite prime, then for any finite prime $P \neq Q$ we have $\pi_P \in \mathcal{U}_Q$ and $\frac{1}{\pi_P} \in \mathcal{U}_Q$. Thus $(j_{P\neq\infty}^*)$ is in U_T. For the sake of simplicity we write $(j_{P\neq\infty}^*) = j_T$. Also, since π is monic then $sgn_\infty(\pi) = 1$ and $sgn_\infty(\frac{1}{\pi}) = 1$. Writing $j_\infty = u_o(\frac{1}{T})^{z_o}.$, we have $sgn_\infty(\frac{u_o}{sgn_\infty(j_\infty)}) = 1$. Since $j_\infty^* = j_\infty.d(j_P)^{-1}$ and sgn_∞ is a multiplicative homomorphism, then $j_\infty^* \in V_\infty \approx k_\infty^1 \times \mathbb{Z}$. If $j_\infty^* = u(\frac{1}{T})^z$, then we write $j_\infty^* = \underline{j_\infty}.j_z$ where $\underline{j_\infty} = u$ and $j_z = v_\infty(j_\infty^*)$. In summary we write

$$(j_P) = d(j_P)\ .\ j_T\ .\ \underline{j_\infty}\ .\ j_z. \tag{3.13}$$

This representation is unique and gives the isomorphism. We have shown that k^* is a discrete subgroup in J and V_∞ is open in k_∞^*. Since $\mathcal{U}_P$ is an open in k_∞^*, then $U_T \times V_\infty$ is an open in J. Then the proposition follows from lemma 3.2.3.

□

We are now in a good position to construct the homomorphism ψ. We complete this task by showing the following theorem.

Theorem 3.2.6. *There is a continuous homomorphism ψ from the group of k-ideles J into the Galois group* $\mathrm{Gal}(\mathcal{A}/k)$ *with kernel k^*.*

To make clear the proof of this theorem, we should give some lemmas

Lemma 3.2.7. *There is a continuous monomorphism ψ_z from $\mathbb{Z}$ into the Galois group $\tilde{G}$.*

Proof. We define ψ_z by the map which sends 1 to `Frob`. This homomorphism is certainly continuous since $\mathbb{Z}$ has the discrete topology. □

Lemma 3.2.8. *There is a continuous isomorphism ψ_∞ from k_∞^1 into the Galois group G^-.*

Proof. It is obvious □

Lemma 3.2.9. *There is a continuous isomorphism ψ_T from U_T into the Galois group G^+.*

Proof. We first begin by constructing a homomorphism $\psi_T^m : U_T \to \mathrm{Gal}(K_m/k)$ for some monic polynomial $m \in A$. To do so, we need to see how an $u \in U_T$ acts on K_m. Let $m = P_1^{e_1} P_2^{e_2} ... P_t^{e_t}$ be the prime decomposition of $m \in A$. By the Chinese remainder theorem $(A/mA)^* \cong \oplus_i (A/P_i^{e_i} A)$. It means that for any set of polynomials $\{m_1, m_2, ..., m_t\} \subseteq A$ such that $(m_i, P_i) = 1$, there exists $a \in A$ such that $a \equiv m_i \pmod{P_i^{e_i}}$ for every $1 \leq i \leq t$. So for a given $u \in U_T$, there exists $a \in A$ such that $a \equiv u_p \pmod{P_i^{e_i}}$ for every $1 \leq i \leq t$. a is uniquely determined modulo m. Again by remark 2.3.3, u corresponds to a unique $\sigma_a \in \mathrm{Gal}(K_m/k)$. Then we get the homomorphism ψ_T^m defined by $\psi_T^m(u) = \sigma_a$. Considering $\mathrm{Gal}(K_m/k)$ as a finite discrete topological group yields that ψ_T^m is continuous.

Now we take the limit and using theorem 2.2.6 we get the continuous map

$$\psi_T : U_T \to \varprojlim_{m \in A} (A/mA)^*.$$

The ordering on A is given by divisibility and for n dividing m the continuous homomorphism from $(A/mA)^*$ into $(A/nA)^*$ is just the restriction. The map ψ_T is injective since for $(u_P) \neq (v_P)$ then there exists Q prime in k such that $u_Q \neq v_Q$, taking m multiple of Q yields $\psi_T^m(u_Q) \neq \psi_T^m(v_Q)$. Therefore $\psi_T(u_P) \neq \psi_T(v_P)$. The last task in this proof is to show that ψ_T is surjective. To do so, we prove that $\psi_T(U_T)$ is dense and closed. By proposition 3.2.1, U_T is compact and since ψ_T is continuous, then $\psi_T(U_T)$ is compact. But $\varprojlim_{m \in A} (A/mA)^*$ is Hausdorff, then $\psi_T(U_T)$ is closed. For density we show that taking $(x_m) \in \varprojlim (A/mA)^*$, $V \bigcap \psi_T(U_T) \neq \emptyset$ for any neighbourhood V of (x_m). The set

$$U_S = \prod_{m \notin S} (A/mA)^* \times \prod_{m \in S} 1$$

where S is a finite set of A is a basic system of neighbourhoods of $(1_m) \in \prod_m (A/mA)^*$. Hence the set $(x_m)(U_S \bigcap \varprojlim (A/mA)^*)$ is a neighbourhood of (x_m) in $\varprojlim (A/mA)^*$. We set $B = \bigcap_{m \in S} mA$, then there exists $l \in A$ such that $B = lA$. Choose $(u_P) \in U_T$ such that $\psi_T^l(u_P) = x_l$ (always possible), Then $\psi_T \in x_m(U_S \bigcap \varprojlim (A/mA)^*)$ since l divides m for any $m \in S$.

□

Proof of the theorem 3.2.6. By proposition 3.2.5, we have $J \approx k^* \times U_T \times k_\infty^1 \times \mathbb{Z}$. And by exercise 2, page 264 in [Neu], we have $\mathrm{Gal}(\mathcal{A}/k) \approx G^+ \times G^- \times \tilde{G}$. Now, we define the map

$$\begin{aligned} k^* \times U_T \times k_\infty^1 \times \mathbb{Z} &\rightarrow G^+ \times G^- \times \tilde{G} \\ d(j_P) \cdot j_T \cdot \underline{j_\infty} \cdot j_z &\rightarrow \psi_T(1/j_T) \cdot \psi_\infty(1/\underline{j_\infty}) \cdot \psi_z(j^z) \end{aligned}$$

Which is a continuous homomorphism with kernel k^*. □

3.3 Class Field Theory

In the tow previous sections we have constructed the field $\mathcal{A}$ and the homomorphism ψ. To prove that $\mathcal{A}$ is actually the maximal abelian extension of k we need Class Field Theory. In this section we give a short discussion about Class Field Theory and state the main theorem of abelian extension.

Let L/K be a finite Galois extension and let $\mathfrak{P}$ be a prime in L. For any σ in $\mathrm{Gal}(L/K)$, $\sigma\mathfrak{P}$ is another prime in L. If $\mathfrak{P}$ is a non-archimedean with valuation ring $\mathcal{O}_\mathfrak{P}$ then $\sigma\mathcal{O}_\mathfrak{P} = \mathcal{O}_{\sigma\mathfrak{P}}$. Moreover, σ induces by continuity an isomorphism $\sigma_\mathfrak{P} : L_\mathfrak{P} \rightarrow L_{\sigma\mathfrak{P}}$ where $L_\mathfrak{P}$ and $L_{\sigma\mathfrak{P}}$ are the completions of L with respect to the prime $\mathfrak{P}$ and $\sigma\mathfrak{P}$ respectively. Let $\tau \in \mathrm{Gal}(L/K)$, then clearly, $\sigma_{\tau\mathfrak{P}} \circ \tau_\mathfrak{P} = (\sigma\tau)_\mathfrak{P}$. Let P be a prime of K lying below $\mathfrak{P}$ then $\sigma_\mathfrak{P}$ is a K_P-isomorphism. The decomposition group $\mathcal{D}_\mathfrak{P}$ of $\mathfrak{P}$ is the set

$$\mathcal{D}_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma\mathfrak{P} = \mathfrak{P}\}$$

We note that $\mathcal{D}_{\tau\mathfrak{P}} = \tau\mathcal{D}_\mathfrak{P}\tau^{-1}$. If $\mathfrak{P}$ and $\mathfrak{P}'$ are two primes above P then there

exists a automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma\mathfrak{P} = \mathfrak{P}'$. Thus, $\mathcal{D}_{\mathfrak{P}}$ is determined up to a conjugacy by the prime P. If $\sigma \in \mathcal{D}_{\mathfrak{P}}$ then $\sigma_{\mathfrak{P}}$ is a K_P-automorphism and we have an injection form $\mathcal{D}_{\mathfrak{P}}$ into $\mathrm{Gal}(L_{\mathfrak{P}}/K_P)$ which is in fact an isomorphism. As we see this is a generalisation of the discussion in the first chapter.

Now let $\mathfrak{P}$ be a non-archimedean unramified prime of L which lies above P. One has the following:

$$\mathcal{D}_{\mathfrak{P}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_P) \cong \mathrm{Gal}(R(\mathfrak{P})/R(P))$$

where $R(\mathfrak{P})$ and $R(P)$ denote the residue class fields of K and L with respect to $\mathfrak{P}$ and P respectively. The Galois group $\mathrm{Gal}(R(\mathfrak{P})/R(P))$ is cyclic with canonical generator

$$F : x \mapsto x^{N_P}$$

where N_P is the absolute norm. The preimage of F in $\mathcal{D}_{\mathfrak{P}}$ is called the Frobenius automorphism associated with the prime $\mathfrak{P}$ and denoted by $Frob_{\mathfrak{P}}$. The automorphism $Frob_{\mathfrak{P}}$ is characterized by the property

$$Frob_{\mathfrak{P}}(a) \equiv a^{N_P} \pmod{\mathcal{M}_{\mathfrak{P}}}$$

for all $a \in \mathcal{O}_{\mathfrak{P}}$ where $\mathcal{M}_{\mathfrak{P}}$ is the maximal ideal of $\mathcal{O}_{\mathfrak{P}}$. Since $Frob_{\sigma\mathfrak{P}} = \tau^{-1} Frob_{\mathfrak{P}} \tau$ the Frobenius automorphism is determined by P up to a conjugacy. We define by $(P, L/K)$ the set of the $Frob_{\mathfrak{P}}$'s for all $\mathfrak{P}$ above P. Let S be a finite set of primes of K containing the archimedean primes and the primes ramified in L/K. We denote by $\mathfrak{M}_K$ the set of primes of K. We have the following map

$$\begin{array}{rcl} (\quad, L/K) : \mathfrak{M}_K - S & \to & \text{conjugacy class of } \mathrm{Gal}(L/K) \\ P & \mapsto & (P, L/K) \end{array}$$

The map $(\quad, L/K)$ is called the Artin symbol.

For the rest of this section we assume that L/K is a finite abelian extension. Thus $(\quad, L/K)$ is a map from $\mathfrak{M}_K - S$ into $\mathrm{Gal}(L/K)$. Let I^S be the free abelian group on the elements of $\mathfrak{M}_K - S$. We can extend $(\quad, L/K)$ to a homomorphism (denoted

by (,L/K) as well) from I^S into $\mathrm{Gal}(L/K)$ by putting

$$(\prod_{P\notin S} P^{n_P}, L/K) = \prod_{P\notin S} (P, L/K)^{n_P}$$

Where n_P are integers and almost equal to zero.

Furthermore, we can define the Artin symbol for any abelian extension. Indeed for an abelian extension L/K we have,

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(L_i/K)$$

where $L_i \subseteq L$ runs over all finite abelian subextensions of K.

Let $a \in K^*$, then we write $(a)^S = \prod_{P\notin S} P^{v_P(a)}$. We note that $(a)^S$ is in I^S.

The reciprocity law says: If L/K is an abelian extension and S is a set as above, then for each neighbourhood N of the identity element 1 in $\mathrm{Gal}(L/K)$ there exists $\varepsilon > 0$ such that $((a)^S, L/K) \in N$ whenever $a \in K^*$ and $|a-1|_P < \varepsilon$ for all $P \in S$.

We can now state the main theorem of abelian extension (see [Cas]).

Theorem 3.3.1 (The Main Theorem on Abelian Extension)**.** *Every abelian extension L/K satisfies the reciprocity law.*

Let J_K be the idele group of K. We denote by J_K^S the set of elements of J_K which have 1 at the P-th component for all $P \in S$. For $x = (x_P) \in J_K$ we write $(x)^S = \prod_{P\notin S} P^{v_P(x_P)} \in I^S$. The main theorem on abelian extension is equivalent to the following,

Theorem 3.3.2 (The Main Theorem on Abelian Extension)**.** *Let L/K be an abelian extension, then there exist a unique homomorphism $\psi^\star$ of $J_K \to \mathrm{Gal}(L/K)$ such that*

1. *$\psi^\star$ is continuous*
2. *$\psi^\star(K^*) = 1$*
3. *$\psi^\star(x) = ((x)^S, L/K)$ for all $x \in J_K^S$*

$\psi^\star$ is called the reciprocity law homomorphism.

3.4 Maximal abelian extension and reciprocity law homomorphism

Having constructed the field extension $\mathcal{A}/k$ in the first section and the homomorphism ψ in the second section, our goal in this last section which is also the goal of the chapter is to prove the following theorem:

Theorem 3.4.1. *The extension $\mathcal{A}/k$ is the maximal abelian extension of k and the homomorphism ψ is the reciprocity law homomorphism.*

The Kronecker-Weber theorem for rational function field follows easily from that.

Theorem 3.4.2 (Kronecker-Weber theorem for rational function field)**.** *Every finite abelian extension of k is contained in the compositum of the fields K_m, $\mathbb{F}_n k$ and L_r^- for some $m \in A$, n positive integer and r positive integer.*

To begin with we let $\mathcal{A}^*$ be the maximal abelian extension of k. And let ψ^* be the reciprocity law homomorphism from J into $\mathrm{Gal}(\mathcal{A}^*/k)$. Let R/k a finite extension field. The restriction of ψ^* from $\mathrm{Gal}(\mathcal{A}^*/k)$ to $\mathrm{Gal}(R/k)$ induces a homomorphism $\psi^r : J \to \mathrm{Gal}(R/k)$. For an idele $j \in J$, let

$$\delta(j) := \prod_P P^{v_P(j_P)} \qquad \text{for all P primes in } k \tag{3.14}$$

To tackle the proof of this theorem we need to appeal the main theorem on abelian extension from class field theory. In our case here we have,

Theorem 3.4.3. *Let S be any finite set primes of k which contains at least all those primes which ramify in R/k, and J^S denote the group of ideles (j_P) such that $j_Q = 1$ for all $Q \in S$. Then ψ^r is the unique homomorphism from J into* $\mathrm{Gal}(R/k)$ *such that*

1. *ψ^r is continuous*
2. *$\psi^r(k) = 1$*
3. *$\psi^r(j)$ is the same as the Artin automorphism $(\delta(j), R/k)$ for all $j \in J^S$.*

Before going further we need one more definition. An idele $j \in J^S$ is called Q-blip if $j_Q = \pi_Q$ and $j_P \in \mathcal{U}_P$ for all $P \neq Q$. It is not hard to see that every idele in J^S can be written as the finite product of P-blips and inverses of P-blips for various P not in S.

Proposition 3.4.4. *The homomorphisms ψ and ψ^r agree on the finite subextensions K_m/k, $\mathbb{F}_n k/k$ and L_n^-/k.*

Proof. We need to check that ψ satisfies the conditions 1, 2 and 3 for each subextension. The condition 1 and 2 are already done, so all we need to do is to check the condition 3. It is enough to check this condition for any j P-blip.

Firstly, we assume that $R/k = K_m/k$. We first assume that $m = P_o^e$ for some positive integer e. We take $S = \{P_o, \infty\}$ since by theorem 2.2.6 and theorem 2.5.3, the only primes that ramify in K_m/k are P_o and ∞. Let $Q \neq P_o, \infty$ be a prime and $(j_P) \in J^S$ a Q-blip. By definition $d(j) = \pi_Q$ and $j_{P_o} = 1$. Then the P_o-th coordinate of (j_P^*) is $1/Q$. As we see in the proof of lemma 3.2.9, (j_P) acts on K_m via σ_Q. Then $\psi(j_P) = \psi_T(1/j_T)$ on K_m is the automorphism which maps λ to $C_Q(\lambda)$ for every $\lambda \in \Lambda_m$ which is the Artin map $(\delta(j_P) = Q, K_m/k)$ by theorem 2.3.5. Now let $m = \alpha P_1^{e_1}.P_2^{e_2}...P_t^{e_t}$. We take $S = \{\infty, P_1, ..., P_t\}$ and $(j_P) \in J^S$ where Q is not in S. We still have $\delta(j_P) = Q$. Since K_m is the compositum of the fields $K_{P_i^{e_i}}$ and $\mathcal{O}_m$ is the compositum of the rings $\mathcal{O}_{P_i^{e_i}}$ for $1 \leq i \leq t$, then $(\delta(j_P), K_m/k)$ is completely determined by each $(\delta(j_P), K_{P_i^{e_i}}/k)$. Also, by construction in the proof of the lemma 3.2.9 ψ_T^m is completely determined by each $\psi_T^{P_i^{e_i}}$.

Secondly let $R/k = \mathbb{F}_n k/k$ a be constant field. Again from theorem III.6.3. in [Sti], there is no ramified prime in $\mathbb{F}_n k$. For convenience we take $S = \{\infty\}$. Let $Q \neq \infty$ be a prime and $(j_P) \in J^S$ a Q-blip. We have $j_\infty = 1$, $d(j_P) = \pi_Q$, then $j_\infty^* = j_\infty \,.\, {\pi_Q}^{-1}$. Thus $j_z = v_\infty(j_\infty^*) = v_\infty({\pi_Q}^{-1}) = \deg Q$. Therefore $\psi(j) = \psi_z(j_z) = \texttt{Frob}^{\deg Q}$ on $\mathbb{F}_n k$. The Artin automorphism $(Q, \mathbb{F}_n k)$ is easily seen to be the $\texttt{Frob}^{\deg Q}$ on $\mathbb{F}_n k$. And we are done since $\delta(j_P) = Q$.

Finally, let $R/k = L_n^-/k$. Since T and ∞ are ramified in $K_{T^{n+1}}$, then ∞ and T are ramified in $K_{T^{-n-1}} = K_n^-$. They are also ramified in L_n^-, and all other primes are unramified. We then take $S = \{T, \infty\}$. Let $(j_P) \in J^S$ be a P-blip, where P is not in S and of degree d. We have $j_\infty = 1$ and $d(j_P) = P$. Then $j_\infty^* = P^{-1} = P^{-1}T^d(\frac{1}{T})^d$.

Therefore $\underline{j_\infty} = P^{-1}T^d$. Let a_o denote the constant term of P. We write $PT^{-d} = a_o\bar{P}$ where $\bar{P}$ is a monic polynomial in $\frac{1}{T}$. Therefore, we have on K_n^-

$$\psi(j_P) = \psi_\infty(P\ T^{-d}) = \psi_\infty(a_o\ \bar{P}).$$

As we explained in the beginning of this chapter, $\psi_\infty(a_o\bar{P})$ is just the automorphism that takes λ^- to $C_{a_o\bar{P}}(\lambda^-)$ and the restriction on L_n^- is the automorphism $\lambda^- \mapsto C_{\bar{P}}(\lambda^-)$. However $v_P(\bar{P}) = v_P(PT^{-d}) = v_P(P) = 1$. Then $\bar{P}$ is the uniformizing parameter at P for the theory with $\frac{1}{T}$ for the generator of k. Hence $(\delta(j_P) = P, L_n^-/k) = (\bar{P}, L_n^-/k))$ and by theorem 2.3.5 we are done. □

proof of the theorem 3.4.1. Let $\psi^* : J \to \mathrm{Gal}(\mathcal{A}^*/k)$ be the reciprocity law homomorphism. Since $\mathcal{A}/k$ is abelian, $\mathcal{A} \subseteq \mathcal{A}^*$ and one has the restriction homomorphism $res : \mathrm{Gal}(\mathcal{A}^*/k) \to \mathrm{Gal}(\mathcal{A}/k)$.

$$\begin{array}{ccc} \mathrm{J} & \xrightarrow{\psi^*} & \mathrm{Gal}(\mathcal{A}^*/k) \\ \mathrm{id}\downarrow & & \downarrow res \\ \mathrm{J} & \xrightarrow{\psi} & \mathrm{Gal}(\mathcal{A}/k) \end{array}$$

By Galois theory, if $res \circ \psi^* = \psi$ then $\mathcal{A}^* = \mathcal{A}$ and $\psi^* = \psi$. In order to show that $res \circ \psi^* = \psi$, it suffices to prove for every idele $(j_P) \in J$ that $\psi^*(j_P) = \psi(j_P)$ restricts to the same automorphism on each finite subextension of $\mathcal{A}/k$. However every finite subextension of $\mathcal{A}/k$ is contained in a composite of subextensions of K_m, $\mathbb{F}k$ and L_n^-. And the theorem follows from proposition 3.4.4. □

Chapter 4

Elementary Proof

Since rational function fields and the field of rational numbers are very similar, in this last chapter we want to see if we can follow the tricks used in the elementary proofs of the Kronecker-Weber theorem for number fields to prove of an analogue for rational function fields. We mean by elementary a proof without class field theory. Throughout the chapter we will keep our previous notations.

4.1 Number Fields

To begin with let us first outline the elementary proof of the Kronecker-Weber theorem done by M. J. Greenberg [Gre]. This outstanding proof, which does not involve the local-global principle, used only higher ramification and some basics in Algebraic Number Theory.

Let K be a finite abelian extension of $\mathbb{Q}$ and $G := \mathrm{Gal}(K/\mathbb{Q})$ its Galois group. Then by the structure theorem for abelian groups we have

$$G = \prod_{i=1}^{g} G_i \quad \text{where } G_i \text{ is cyclic of prime power order.} \tag{4.1}$$

If we denote by K_i the fixed field of $\prod_{i \neq j} G_j$ we get $K = \vee K_i$ and $\mathrm{Gal}(K_i/\mathbb{Q}) = G_i$. It simplifies the task to the following proposition.

Proposition 4.1.1. *Every cyclic extension of prime power order δ^r is cyclotomic.*

From now we only restrict ourselves to the case where $\delta \neq 2$. By using the properties of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ for some prime p and higher ramification groups one can reduce the case further to

Proposition 4.1.2. *Every cyclic extension of prime power δ^r degree, such that every prime $p \neq \delta$ is unramified, is cyclotomic.*

Finally by Minkowski's theorem, which states that $\mathbb{Q}$ has no proper unramified extension, we can prove the Kronecker-Weber theorem just by proving the following lemma.

Lemma 4.1.3. *Every cyclic extension of prime power δ^r, such that δ is the only ramified prime, is cyclotomic.*

Proof. Let ζ be a δ^{r+1}-st root of unity. Since $\mathbb{Q}(\zeta)/\mathbb{Q}$ is cyclic of order $\delta^r(\delta-1)$ there exists an unique subfield K' of $\mathbb{Q}(\zeta)$ of order δ^r. We have KK' an abelian extension of order δ^l where $l \geq r$. Since δ is the only ramified prime in KK' one can prove that KK' is a cyclic extension of $\mathbb{Q}$. And by Galois theory $\mathrm{Gal}(KK'/\mathbb{Q})$ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K'/\mathbb{Q})$, then $l = r$. □

If we are trying to follow this idea to prove the Kronecker-Weber theorem for rational function fields then there are a few obvious obstacles. After breaking down the abelian extension into cyclic extensions we encounter our first problem in proposition 4.1.2 since a finite prime for a rational function field is a monic irreducible polynomial. Also we do not have an analogue of Minkowski's theorem, and worst of all is the fact that $k(\lambda_{P^r})/k$ is not cyclic.

Instead, one may try a local-global approach, similar to the proof in [Was] . Moreover, both the p-adic numbers $\mathbb{Q}_p$ for some prime p and the field of Laurent series $\mathbb{F}((T))$ are local fields. The global Kronecker-Weber theorem says

Theorem 4.1.4. *Every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity.*

Then we reduce this theorem to the local Kronecker-Weber theorem which says

Theorem 4.1.5. *Every finite abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_m)$ where ζ_m is a primitive m-th root of unity and p is a prime.*

This process is called the local-global principle. To prove that theorem 4.1.5 implies theorem 4.1.4 one can check [Was] or [Neu]. The proof uses facts about inertia groups and also the Minkowski's theorem. Having done this reduction, Washington proved the theorem 4.1.5 without using class field theory which we would like to follow.

4.2 Rational Function Fields

In this section we will state a local-global principle for rational function fields, thereafter we will give a short analysis on how far we can imitate the elementary proof of the local theorem of number fields. We start with some propositions which will be useful.

Proposition 4.2.1. *Let $m \in A$, let P be a monic irreducible polynomial and k_P the completion of k at P. Suppose P^r is the highest power of P dividing m. Then the inertia group of $k_P(\lambda_m)/k_P$ is isomorphic to $(A/P^rA)^*$.*

Proof. Let I_P be the inertia group of $k(\lambda_m)/k$ at P, then I_P is the inertia group of $k_P(\lambda_m)/k_P$. But P is totally ramified in $k(\lambda_{P^r})/k$ and

$$\mathrm{Gal}(k(\lambda_m)/k) \cong (A/P^rA)^* \times (A/nA)^* \quad \text{where } (n, P) = 1. \tag{4.2}$$

Therefore $I_P \cong (A/P^rA)^*$, since the fixed field of $(A/nA)^*$ is $k(\lambda_{P^r})$. □

The next proposition is obvious

Proposition 4.2.2. *A subextension of a geometric extension is geometric.*

The following theorem will play the role of the Minkowski's theorem for rational function fields.

Theorem 4.2.3. *Let L be a finite separable extension of $k = \mathbb{F}(T)$. If L/k is unramified at all finite primes and at most tamely ramified at ∞, then $L = \mathbb{F}_n(T)$ for some constant field extension $\mathbb{F}_n/\mathbb{F}$.*

Before proving this theorem, we first fix our notations. Let L/K be a finite extension of function fields with constant fields E/F. Let $\mathfrak{p}$ be a prime in K and $\mathfrak{P}$ be a prime in L above $\mathfrak{p}$ with valuation rings $\mathcal{O}_{\mathfrak{P}}$ and $\mathcal{O}_{\mathfrak{p}}$ respectively. We set $\deg_L\mathfrak{P} = [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : E]$ and $\deg_K\mathfrak{p} = [\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} : F]$. We should notice that

$$[E : F]\ \deg_L\mathfrak{P} = f(\mathfrak{P}/\mathfrak{p})\ \deg_K\mathfrak{p}. \tag{4.3}$$

The theorem 4.2.3 is a consequence of the following.

Theorem 4.2.4. *(Riemann-Hurwitz [Sti]). Let L/K be a finite, separable, geometric extension of function fields. Assume that all ramified primes are tamely ramified, then*

$$(2g_L - 2) = [L : K](2g_K - 2) + \sum_{\mathfrak{p}\in S_K}\sum_{\mathfrak{P}/\mathfrak{p}}(e(\mathfrak{P}/\mathfrak{p}) - 1)\deg_L\mathfrak{P}. \tag{4.4}$$

where S_K is the set of primes of K. Here g_L and g_K are the genus of L and K respectively.

Proof of theorem 4.2.3. We can assume that L/k is geometric. In fact if L/k is not geometric then there exist an integer n such that $L/\mathbb{F}_n(T)$ is geometric. We will show, then, that $L = k$. Let S_∞ be the set of primes in L lying above ∞. Since the rational function field k is of genus 0 then by equation 4.4

$$(2g_L - 2) = -2[L : k] + \sum_{\mathfrak{P}\in S_\infty}(e(\mathfrak{P}/\infty) - 1)\deg_L\mathfrak{P}. \tag{4.5}$$

The extension L/k is geometric and $\deg_k\infty = 1$. From equation 4.3 we have

$$\deg_L\mathfrak{P} = f(\mathfrak{P}/\infty). \tag{4.6}$$

Hence

$$(2g_L - 2) = -2[L : k] + \sum_{\mathfrak{P}\in S_\infty}(e(\mathfrak{P}/\infty)f(\mathfrak{P}/\infty) - \sum_{\mathfrak{P}\in S_\infty} f(\mathfrak{P}/\infty). \tag{4.7}$$

As L/k is separable, we get

$$(2g_L - 2) = -[L : k] - \sum_{\mathfrak{P}\in S_\infty} f(\mathfrak{P}/\infty). \tag{4.8}$$

The genus g_L is a positive integer. Then we get a contradiction in this last equation if $L \neq k$. $\square$

We are now in a good position to state the local-global principle for rational function fields. We will prove that the local claim implies the global one.

Local Claim 4.2.5. Every abelian extension of k_P lies inside $\mathbb{F}_n.k_P(\lambda_m)$ for some $m \in \mathbb{F}[T]$ and $\mathbb{F}_n/\mathbb{F}$.

Global Claim 4.2.6. Every abelian extension of k which is at most tamely ramified at ∞ lies inside $\mathbb{F}_n.k(\lambda_m)$ for some $m \in \mathbb{F}[T]$.

Theorem 4.2.7. *(Local-Global Principle). Local claim 4.2.5 implies Global claim 4.2.6.*

Proof. Let L be an abelian extension which is at most tamely ramified at ∞. Set S be the set of finite ramified primes of L/k. Let P be a prime for which the local claim holds, and denote L_P the completion of L at a prime of L above P. Then L_P is an abelian extension of k_P and by local claim $L_P \subseteq k_P(\lambda_{m_P}).\mathbb{F}_n$ for some $m_P \in A$. We set

$$m = \prod_{P \in S} P^{r_P} \quad \text{where } P^{r_P} \text{ is the precise power of } P \text{ dividing } m_P. \tag{4.9}$$

We let $M = L(\lambda_m)$. Then M/k is abelian. We have

$$k_P(\lambda_m) \subseteq M_P = L_P(\lambda_m) \subseteq k_P(\lambda_m, \lambda_{m_p}).\mathbb{F}_n = k_P(\lambda_{m_p}).\mathbb{F}_n. \tag{4.10}$$

By lemma 4.2.1 the inertia I_P group of M_P/k_P is isomorphic to $(A/mA)^*$, so

$$|I_P| = \varphi(P^{e_P}). \tag{4.11}$$

We let I be the subgroup of $Gal(M/k)$ generated by all I_P where $P \in S$ and we denote by $F = Fix(I)$ its fixed field. By construction, the ramified finite primes of M/k are precisely the primes in S. This implies that F/k is unramified for all prime $P \in S$, since $Fix(I) \subseteq Fix(I_P)$ for any prime $P \in S$. Also, F is at most tamely ramified at ∞. By theorem 4.2.3, which is considered as the analogue of Minkowski's theorem, F is a constant field extension of k, i.e. $F = \mathbb{F}_n.k = \mathbb{F}_n(T)$ where $[\mathbb{F}_n : \mathbb{F}] = n$. Now since F/k is a constant field extension and $k(\lambda_m)/k$ is geometric we see that $F \bigcap k(\lambda_m) = k$. It follows that the compositum $F.k(\lambda_m) = \mathbb{F}_n.k(\lambda_m)$ is a constant

field extension of degree n at $k(\lambda_m)$, and $[F.k(\lambda_m) : F] = [k(\lambda_m) : k] = \varphi(m)$. On the other hand, $I = Gal(M/k)$. so

$$[M : F] = |I| \leq \prod_{P \in S} |I_P| = \varphi(m) = [k(\lambda_m) : k]. \tag{4.12}$$

and since $F.k(\lambda_m) \subseteq M$, we get $M = F.k(\lambda_m) = \mathbb{F}_n.k(\lambda_m)$. We have thus shown that $L \subseteq \mathbb{F}_n.k(\lambda_m)$. This proves the global claim.

□

For the p-adic numbers $\mathbb{Q}_p$ there are many elementary proofs of the local Kronecker-Weber theorem, for instance in Washington [Was], Michael Rosen [Ros2], S. Vostokov [Vos] and J. Rosenberg [Ro]. For the rest of this section we do a brief analysis on the local claim for rational function fields. We consider only the completion of k at the monic irreducible prime T, which is the field of Laurent series $\mathbb{F}((T))$.

In [Ros2], we know that every abelian extension of a local field is contained in the composite of an unramified extension and a totally ramified abelian extension. Also for local fields any unramified extension is obtained by adjoining a primitive n-th root of unity where n is relatively prime to the characteristic of the residue field. Therefore the unramified extensions of the p-adic numbers are of the form $\mathbb{Q}_p(\zeta_n)$ where $(p, n) = 1$. However for the rational function field it is of the form $\mathbb{F}_n((T))$ where $\mathbb{F}_n$ is obtained from $\mathbb{F}$ by adjoining the roots of the polynomial $X^{q^n} - X$ and it cannot be of the form $\mathbb{F}((T))(\lambda_m)$.

In [Was], for instance, in order to prove that any totally ramified abelian extension of $\mathbb{Q}_p$ is contained in $\mathbb{Q}_p(\zeta_n)$ for some n, he first used the structure of abelian groups to reduce the task to a cyclic extension of prime power δ^r. Then there are three cases: $\delta = p$, $\delta \neq p$ and $\delta = 2$.

Let us have a look at the first case. The prime p is totally ramified in $\mathbb{Q}(\zeta_{p^{r+1}})/\mathbb{Q}$, then taking the completion at p the extension $\mathbb{Q}_p(\zeta_{p^{r+1}})/\mathbb{Q}_p$ is totally ramified and cyclic of order $p^r(p-1)$. Hence it has a unique totally cyclic unramified subextension K_r. It can be proved that for any $m \geq 1$ there is an unramified cyclic extension of $\mathbb{Q}_p$ of degree m. So let K_u be the unramified extension of $\mathbb{Q}_p$ of order p^r. And from what we have just said above $K_u = \mathbb{Q}_p(\zeta_n)$ for some n. Then

$$\mathrm{Gal}(K_r K_u/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/p^r\mathbb{Z} \tag{4.13}$$

which looks like a manageable group. It can be proved by Kummer theory that any totally ramified cyclic extension of $\mathbb{Q}_p$ of degree p^r is inside $\mathbb{Q}_p(\zeta_{p^{r+1}}, \zeta_n)$ which is again $\mathbb{Q}_p$ adjoining some roots of unity.

For rational function fields, we assume $q = p^f$. The unramified extension of $\mathbb{F}((T))$ of degree p^r we have is $\mathbb{F}_{p^r}((T))$ and it is a cyclic extension. However to find a totally ramified extension we have to look at $\mathbb{F}((T))(\lambda_{T^e})$. For this we have

$$\mathrm{Gal}(\mathbb{F}((T))(\lambda_{T^e})/\mathbb{F}((T))) \cong \mathrm{Gal}(\mathbb{F}(T)(\lambda_{T^e})/\mathbb{F}(T)) \cong (A/T^eA)^* \tag{4.14}$$

Hence the degree extension of $F((T))(\lambda_{T^e})/\mathbb{F}((T))$ is $p^{f(e-1)}(p^f - 1)$. Then to get a subfield of degree p^r we need at least $f(e-1) \geq r$. But since this is not always cyclic then we may have many subfields of degree p^r and we cannot see easily its Galois group.

So far we may say that any finite abelian extension of $\mathbb{F}((T))$ is contained in the composite $\mathbb{F}_n((T)).\mathbb{F}((T))(\lambda_m)$. We may be concerned about the third extension L_n^-. But from the construction of L_n^- and the Theorem 2.5.2, one can see easily that T splits totally in L_n^-, therefore the completion of L_n^- at any prime above T is $F((T))$ itself.

4.3 Conclusion

In summary, our attempts to find an elementary proof for the Kronecker-Weber Theorem for rational function fields fail because of the important non-analogies between number fields and function fields:

1 $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n}/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic when $p > 2$. But $\mathrm{Gal}(k(\lambda_{P^n})/k) \cong (A/P^nA)^*$ is not cyclic in general. In fact, the number of generators of $(A/P^nA)^*$ tends to infinity as $n \to \infty$.

2 Extension degrees are positive integer, and thus elements of $\mathbb{Z}$ not of A.

For a proof of the local claim for rational function fields one could probably use Lubin-Tate theory and formal groups but that goes beyond the scope of this thesis.

Bibliography

[Car] L. Carlitz, *A Class of Polynomials*, Transactions of American Mathematical Society, Vol. 43, pp. 167-182, 1974.

[Cas] J. W. S. Cassels and A. Frolich (editors), *Algebraic Number Theory*, Academic Press, New York, 1967.

[Cox] David A. Cox, *Primes of the form* $X^2 + nY^2$, Wiley Interscience, Amherst, Massachusetts, 1989.

[Vos] I. Fesenko, S. Vostokov, *Local Fields And Their Extensions*, American Mathematical Society, Providence, Rhode Island, second edition, Translation of Mathematical Monographs, vol 121.

[G-A-C] G. Christol, A. Cot and C. Michel, *Topologie*, Ellipses, edition marketing S.A., 1997.

[Gos] D. Goss, *Basic of Function Field Arithmetic*, Springer-Verlag, Berlin, New York, 1998.

[Gra] G. Gras, *Class Field Theory*, Springer-Verlag, Berlin, New York, 2002.

[Gre] M. Greenberg, *An Elementary proof of the Kronecker-Weber Theorem*, The American Mathematical Monthly, Vol. 81, No. 6, pp. 601-607, 1974.

[Hay] D. Hayes, *Explicit Class Field Theory for Rational Function Fields*, Transactions of American Mathematical Society, Vol. 189, 1974.

[Hun] Thomas W. Hungerford, *Algebra*, Springer-Verlag, Berlin, New York, 1980.

[How] John M. Howie, *Fields and Galois Theory*, Springer-Verlag, Berlin, New York, 2005.

[H-W] G. Hardy and E. Wright, *An Introduction to the Theory of Number*, Clarendon Press. Oxford. New York, 1978.

[Lan1] S. Lang, *Algebraic Number Theory*, Springer-Verlag, Berlin, New York, 1994.

[Lan2] S. Lang, *Cyclotomic Fields I and II*, Springer-Verlag, Berlin, New York, 1990.

[Neu] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, New York, 1999.

[Rob] Alain M. Robert *A Course in P-adic Analysis*, Springer-Verlag, Berlin, New York, 2000.

[Ros1] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, Berlin, New York, 2002.

[Ros2] M. Rosen, *An Elementary Proof Of The Local Kronecker-Weber Theorem*, Transactions of American Mathematical Society, Vol. 265, pp. 599-605, 1981.

[Ro] J. Rosenberg, *Algebraic K-theory And Its Applications*, Springer-Verlag, Berlin, New York, 1996.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, New York, 1993.

[Was] Lawrence C. Washington, *Introduction To Cyclotomic Fields*, Springer-Verlag, Bering, New York, 2003.