Local Class Field Theory via Lubin-Tate Theory

by

Adam Mohamed

Thesis presented in partial fulfilment of the requirements for the degree of

Master of Science

at

Stellenbosch University

Supervisor: Dr. Arnold Keet
Department of Mathematical Sciences
Faculty of Sciences

Date: 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 otherwise stated) and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: November 2008

Abstract

This is an exposition of the explicit approach to Local Class Field Theory due to J. Tate and J. Lubin. We mainly follow the treatment given in [15] and [25]. We start with an informal introduction to p-adic numbers. We then review the standard theory of valued fields and completion of those fields. The complete discrete valued fields with finite residue field known as *local fields* are our main focus. Number theoretical aspects for local fields are considered. The standard facts about Hensel's lemma, Galois and ramification theory for local fields are treated. This being done, we continue our discussion by introducing the key notion of relative Lubin-Tate formal groups and modules. The torsion part of a relative Lubin-Tate module is then used to generate a tower of totally ramified abelian extensions of a local field. Composing this tower with the maximal unramified extension gives the maximal abelian extension: this is the *local Kronecker-Weber theorem*. What remains then is to state and prove the theorems for explicit local class field theory and end our discussion.

Opsomming

Hierdie tesis is 'n uiteensetting van die eksplisiete beskrywing van klasliggaamteorie van J. Tate en J. Lubin. Ons volg die behandeling wat in [15] en [25] gegee is. Ons begin met 'n informele inleiding aan p-adiese getalle. Ons beskou dan die standaarde teorie van liggame met waardering en hul vervollediging. Die volledige diskrete liggame met waardering en 'n eindige resklasliggaam is bekend as lokaleliggame, en ons fokus op hulle. Ons beskou die getalleteorie van lokaleliggame. Die bekende feite oor Hensel se lemma, Galois teorie en vertakkingteorie is behandel. Daarna beskou ons die sleutel begrippe van relatiewe Lubin-Tate formele groepe en modules. Die torsie deel van 'n relatiewe Lubin-Tate module is gebruik om 'n toring van totale vertakte abelse uitbreidings van 'n lokaleliggaam voort te bring. As ons hierdie toring met die maksimum onvertakte uitbreiding saamstel dan kry ons die maksimale abelse uitbreiding: dit is die lokale Kronecker-Weber stelling. Wat dan oorbly is om die stellings van eksplisiete lokale klasliggaamteorie te stel en te bewys. Ons sluit dan af.

Acknowledgments

This is the place for me to express my deepest gratitude to my supervisor, Dr. Arnold Keet. His constant support, help, suggestions and teaching have made this thesis a reality.

I would like also to take this opportunity to thank Prof B. Green and Prof F. Breuer for all their help.

During my master's studies and the writing of this thesis I had the supports of an AIMS partial bursary for master's studies, Stellenbosch University Science Faculty bursary for graduate studies and I was awarded an NRF-Africa scholarship for graduate studies. I thank these institutions for their support.

Contents

1 Introduction **3**

2 p-adic Numbers, an Introduction **5**
2.1 Where does all this come from? 5

3 Valued and Complete Fields **11**
3.1 Absolute values and Valuations 11
3.1.1 Generalities 11
3.1.2 Absolute value or valuation on number fields and rational function field 18
3.2 Complete Fields 22

4 Algebraic extensions of complete valued fields **33**
4.1 Extending absolute values 33
4.2 Galois theory and the norm group of local fields. 39
4.2.1 Ramification in an extension of a local field. 39
4.2.2 Galois theoretical aspects for local fields. 44
4.2.3 The group of norms 52

5 Formal group law, Lubin-Tate extensions and Local Class Field Theory **55**
5.1 Introduction 55
5.2 Relative Lubin-Tate formal group law 56
5.2.1 Generalities 56
5.2.2 Relative Lubin-Tate formal group laws 57
5.3 Relative Lubin-Tate extensions 61
5.3.1 Isomorphism of Lubin-Tate extensions 63
5.4 Local class field theory 69
5.4.1 The local Kronecker-Weber theorem 69
5.4.2 The theorems of local class field theory 71

Chapter 1

Introduction

In his famous address at the Second International Conference of Mathematicians in Paris in 1900, Hilbert asked among other things whether the *Kronecker-Weber theorem*, that is every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(e(2\pi ir))$, $r \in \mathbb{Q}$, has an analogue for a number field F. This is Hilbert 12th Problem or *Explicit Class Field Theory*. Depending on how F can be embedded into $\mathbb{C}$, answers and approaches to this problem elegantly illustrate the interconnections between the algebraic, analytic and geometric sides of Number Theory.

Indeed in the situation where F is a quadratic imaginary field, the theory of Complex Multiplication gives an explicit way to generate all abelian extensions of F, for example the Hilbert class field of F. Here the j invariant of an elliptic curve $E/\mathbb{Q}$ with endomorphism ring an order of F, $\mathcal{O}$, plays the role of $e(x)$.

For a totally real field F, if Starks's conjectures are true, as has been proved in many special cases by computation, then Hilbert's problem would have a positive answer. Here the so-called Stark units play the role of the roots of unity in the classical case. See [19] and [5] for details.

If instead of number fields, i.e., finite extensions of $\mathbb{Q}$, we take finite extensions K of the p-adic numbers $\mathbb{Q}_p$, which are *local fields*, then we have an explicit class field theory due to J. Lubin and J. Tate. They called it *Formal Complex Multiplication in Local Fields*. Here we exploit the completeness of K and explicitly construct abelian extensions using a formal group. The maximal ideal of the algebraic closure of K becomes a module over the ring of integers of K, and we adjoin the torsion points to K to obtain a tower of totally ramified extensions of K. Composing this with the maximal unramified extension of K, we obtain the maximal abelian extension of K. Our aim in this thesis is to give a nearly self-contained exposition of this theory, following the treatment in [15] and its recent refinement in [25], in which the *local Kronecker-Weber theorem* is proved using the *Hasse-Arf theorem*.

More precisely we shall prove

Theorem 1.0.1. (Local Class Field Theory) *Let K be a local field. If K'/K is an algebraic extension of K, we write $N(K'/K) := \bigcap N_{L/K}(L^*)$ where L runs over the finite subextensions of K inside K' and let K^{ur} be the maximal unramified extension of K. Let φ_K be the Frobenius of $Gal(K^{ur}/K)$. Then:*

1. *There is a unique homomorphism called the Artin map:*

$$Art_K : K^* \to Gal(K^{ab}/K)$$

characterized by the following properties:
- *For a prime $\pi \in K$, then $Art_K(\pi)|_{K^{ur}} = \varphi_K$*
- *For an abelian extension K'/K, then $Art_K(N(K'/K))|_{K'} = id$.*

2. *For a finite abelian extension K'/K, the Artin map induces the exact sequence:*

$$1 \to N_{K'/K}(K'^*) \to K^* \to Gal(K'/K) \to 1.$$

To this end we have organized the thesis as follows.

In chapter 2 we give an informal introduction to the p-adic numbers $\mathbb{Q}_p$. We will make use of the celebrated *Hensel's lemma* to justify that we have strict a embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.

Thereafter, in chapter 3 we review the basic notions of absolute values or valuations on a field K and the completion of K. We emphasize *non-archimedean* absolute values and give a version of Hensel's lemma for K complete with respect to a non-archimedean absolute value.

In chapter 4 we consider algebraic extensions of a *complete discrete valued field*. In this setting, one important consequence of Hensel's lemma is the uniqueness of the extension of the absolute value on a complete discrete valued field K to its algebraic extensions. We next define *local fields* and classify them. We also discuss some number theoretical aspects on local fields: Galois theory, ramification theory, lower and upper numbering of higher ramification groups and we finish with a brief discussion on the norm group of an extension of a complete discrete valued field.

Lastly, in chapter 5 we introduce the notion of Lubin-Tate formal group law in order to define Lubin-Tate modules. Then torsion points on a Lubin-Tate module give rise to *relative Lubin-Tate extensions*. These are *totally ramified* extensions generalizing the construction of adjoining p-power roots of unity to $\mathbb{Q}_p$ to obtain totally ramified extensions. Composing the union of a tower of relative Lubin-Tate extensions with the maximal unramfied extension build up the abelian closure: this is the local Kronecker-Weber theorem. We end the discussion with a proof of theorem 1.0.1.

Chapter 2

p-adic Numbers, an Introduction

In this short chapter we explain the idea behind *the p-adic number* system. Throughout the discussion we will try to shed light on the motivation for this new number system and give some consequences of this informal definition.

2.1 Where does all this come from?

The use of p-adic methods to expand an algebraic integer as a sum of powers of a prime appears in Kummer's work on Fermat Last Theorem and even before. These ad-hoc methods, familiar to working number theorists, have found a formal setting since Kurt Hensel first viewed them as independent objects on their own. That is he considered *p-adic expansions*, i.e., expansions of the form $\sum_{n=m}^{\infty} a_n p^n$ where $m \in \mathbb{Z}$ and $a_n \in \{1, 2, \cdots, p-1\}$ a set of representatives of the residue field $\mathbb{Z}/p\mathbb{Z}$; independently of the rationals as such expansions don't come always from the p-adic expansion of a rational number. We will be more precise on the latter along our informal introduction to p-adic numbers. p-adic methods in number theory have become an important tool since Kurt Hensel and his predecessors have shown the advantage of applying the methods of series expansions from analysis to numbers.

Indeed, the p-adic numbers arise when one looks at analogies between the function field $\mathbb{C}(z)$ with the field of rational numbers $\mathbb{Q}$. For instance as $\mathbb{Z}$, $\mathbb{C}[z]$ is a unique factorization domain. In a standard course on Complex Analysis, one studies the Laurent series expansion of $f(z) \in \mathbb{C}(z)$ around a point $a \in \mathbb{C}$. In some region in $\mathbb{C}$ we have the unique expansion

$$f(z) = \sum_{n \geq m}^{\infty} c_n (z-a)^n$$

with $m \in \mathbb{Z}$ and $c_n \in \mathbb{C}$. This is what is known as local theory in Analysis since we are looking at the behavior of f around a given point a. For instance we can read if a is a zero or a pole of f and its multiplicity.

Now using the language of algebra, $z-a$ is a prime element in the field $\mathbb{C}(z)$. Any $f(z) \in \mathbb{C}(z)$ admits a unique expansion at the prime $z-a$ of the form

$$f(z) = \sum_{n \geqslant m}^{\infty} c_n (z-a)^n,$$

where the coefficients c_n are taken from a set of representative of the residue field $\mathbb{C} \cong \mathbb{C}[z]/(z-a)$.

We can achieve a similar expansion in $\mathbb{Q}$ using the analogy:

$$\begin{array}{rcl} \mathbb{C}(z) & \longleftrightarrow & \mathbb{Q} \\ \mathbb{C}[z] & \longleftrightarrow & \mathbb{Z} \\ z-a & \longleftrightarrow & p \\ \mathbb{C} \cong \mathbb{C}[z]/(z-a) & \longleftrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \displaystyle\sum_{n \geqslant m}^{\infty} c_n (z-a)^n & \longleftrightarrow & \displaystyle\sum_{n \geq l}^{\infty} a_n p^n. \end{array}$$

We immediately come across the problem of convergence of such a series. Obviously with respect to the usual absolute value on $\mathbb{Q}$ such series don't converge. Recall that the real numbers and many other concepts in Mathematics were rigorously defined only during the 19-th century. This problem of convergence was the main reason why the mathematicians contemporary to Kurt Hensel were cautious about this new system of numbers. It was some years later when the topological tools were ready that the Hungarian mathematician J. Kürschak proposed, by analogy with the construction of the real numbers from $\mathbb{Q}$, to view the p-adic numbers as the *completion* of the rational numbers with respect to the *p-adic absolute value*. This led to *Valuation Theory* where topological concepts help one to understand the arithmetic of certain fields. So, let us see how we can expand rational numbers at a prime number.

We first make the following definition

Definition 2.1.1. The formal set of numbers of the form $\sum_{n \geq m}^{\infty} a_n p^n$ with $a_n \in \{0, 1, \cdots, p-1\}$ and $m \in \mathbb{Z}$, is denoted by $\mathbb{Q}_p$ and called the *p-adic numbers*. The subset of these formal numbers of the form $a_0 + a_1 p + a_2 p^2 + \cdots$ is called the set of *p-adic integers* and denoted by $\mathbb{Z}_p$.

Let $a \in \mathbb{N}$ and p a prime number. From the Euclidean division we can write

$$a = r_0 + a_1 p$$

with $0 \leqslant r_0 \leqslant p-1$. Do the same with a_1, we have

$$a_1 = r_1 + a_2 p$$

with $0 \leqslant r_1 \leqslant p-1$. Thus we obtain

$$a = r_0 + r_1 p + a_2 p^2.$$

with $0 \leqslant r_1, r_2 \leqslant p-1$. Do the same with a_2 and so on. The process terminates, so we can write

$$a = r_0 + r_1 p + r_2 p^2 + \cdots + r_l p^l$$

with $r_i \in \{0, 1, 2, \cdots, p-1\}$.

On trying to do the same process with a negative integer we have to allow an infinite expansion. This is because of the formula

$$-1 = \frac{p-1}{1-p} = \sum_{n=0}^{\infty} (p-1)p^n.$$

So, for a negative integer a, one has

$$\begin{aligned} a &= r_0 + r_1 p + r_2 p^2 + \cdots + r_{n-1} p^{n-1} + (p-1)p^n + (-1)p^{n+1} \\ &= r_0 + r_1 p + r_2 p^2 + \cdots + r_{n-1} p^{n-1} + (p-1)p^n + (p-1)p^{n+1} + \cdots. \end{aligned}$$

The next step is to expand a rational number. To do so, we need first to describe how we can do arithmetic with these numbers. First we need to remark that unlike power series of functions; in the p-adic expansion the set of coefficients is not closed under addition and multiplication. This is similar to arithmetic with real numbers in their decimal expansion. Here is one way of doing the basic arithmetic operations with p-adic numbers. Without loss of generality we describe the arithmetic with the p-adic integers.

How to add p-adic integers:
Take $a = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$, and $b = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$, with $a_i,\ b_i \in \{0, 1, 2, \cdots, p-1\}$. We want to find

$$\begin{aligned} r &= a + b = (a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots) + (b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots \\ &= a_0 + b_0 + (a_1 + b_1)p + (a_1 + b_2)p^2 + \cdots. \end{aligned}$$

But perhaps the $a_i + b_i$ do not lie in $\{0, 1, 2, \cdots, p-1\}$. We write $a_0 + b_0 = c_1 p + r_0$ with $0 \leqslant r \leqslant p-1$. Thus r becomes

$$r = r_0 + (a_1 + b_1 + c_1)p + (a_2 + b_2)p^2 + (a_2 + b_3)p^3 + \cdots.$$

Repeat the same process for $a_1 + b_1 + c_1$, and so on. We see that we have

an algorithm to find the digits of r.

How to multiply p-adic integers:
Now we want to give a meaning to $m = (a_0+a_1p+a_2p^2+\cdots)(b_0+b_1p+b_2p^2+\cdots)$. We start with $m = a_0b_0 + (a_1b_0 + b_1a_0)p + \cdots + (\sum_{i+j=n} a_ib_j)p^n + \cdots$. And as above we write $a_0b_0 = c_1p + r_0$ with $0 \leqslant r_0 \leqslant p-1$, so that we have $m = r_0 + (a_1b_0 + b_1a_0 + c_1)p + \cdots$. Then write $a_1b_0 + b_1a_0 + c_1 = c_2p + r_1$; we have in this manner a process to obtain the digits of m. Having defined addition and multiplication we can now subtract and invert using addition and multiplication: $s = a - b = a + (-1)b$, to obtain $b = \frac{1}{a}$, we write $ba = 1$ and hence we can find the digits of b from those of a.

We can now represent every rational number r as an expansion in powers of p :

$$r = \sum_{n \geqslant m}^{\infty} a_n p^n,$$

with $a_n \in \{0, 1, 2, \cdots, p-1\}$ and m an integer. To see that this representation is unique, one introduces the following function.

Definition 2.1.2. For a rational number $0 \neq r = p^e \frac{a}{b}$, with $p \nmid ab$; one defines $v_p(r) = e$, and $v_p(0) = \infty$ with the conventions $e+\infty = \infty$, $\forall\ e \in \mathbb{Z}$, $\infty + \infty = \infty$. This function is called the *p-adic valuation.*

It satisfies the following properties.

Lemma 2.1.3. *Let $x, y \in \mathbb{Q}$. Then one has: $v_p(xy) = v_p(x) + v_p(y)$, $v_p(x + y) \geq inf\{v_p(x), v_p(y)\}$ with equality if $v_p(x) \neq v_p(y)$.*

Proof. This follows from the definition. □

Let $r \in \mathbb{Q}^*$. If we write $r = \sum_{n\geq m}^{\infty} a_np^n$ where $a_m \neq 0$, then $v_p(r) = m$. Next, if $r = \sum_{n\geq m}^{\infty} a_np^n = \sum_{i\geq j}^{\infty} b_ip^i$, with $b_j \neq 0$, it is immediate that $j = m$. On the other hand $(a_m - b_m)p^m + \sum_{n\geq m+1}^{\infty}(a_n - b_n)p^n = 0$. As $v_p(\sum_{n\geq m+1}^{\infty}(a_n - b_n)p^n) \geq m + 1$, we deduce that $v_p((a_m - b_m)p^m) = \infty$, i.e., $a_m = b_m$. Continuing this way , one sees that $a_n = b_n$ for all $n \geq m$ and hence follows the uniqueness of the p-adic expansion of a rational number.

Proposition 2.1.4. *With the addition and multiplication given above $\mathbb{Z}_p$ is an integral domain, and $\mathbb{Q}_p$ is its quotient field and $\mathbb{Q}$ can be embedded in $\mathbb{Q}_p$.*

Proof. This follows from the above discussion. □

The valuation v_p on $\mathbb{Q}$ extends naturally to $\mathbb{Q}_p$, and is denoted by v_p and called the p-adic valuation.

Remark 2.1.5. *By means of v_p, we have $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}$. From $v_p(x^{-1}) = -v_p(x)$, one deduces that $x \in \mathbb{Z}_p^*$, the group of units if and only if $v_p(x) = 0$. Thus the subset $\mathfrak{m} = \{x \in \mathbb{Z}_p : v_p(x) > 0\}$, is the only maximal ideal of $\mathbb{Z}_p$. This has a natural explanation as we shall see in the next chapter.*

Remark 2.1.6. *One sees that doing arithmetic with p-adic integers comes down to modular arithmetic. This is not a coincidence.*

With some little work we will be able to see that we have the strict embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and that $\mathbb{Q}_p$ is in fact a "big" field by a counting argument. To spell this out we shall make use of the following result which is a version of an important result that bears the standard name of *Hensel's lemma*. A more general version will appear in the sequel.

Proposition 2.1.7. (Hensel's lemma) *Let $f(X) = \sum_{r=0}^{d} c_r X^r \in \mathbb{Z}[X]$. Suppose that there is an integer a such that $f(a) \equiv 0 \pmod{p}$, $f'(a) \not\equiv 0 \pmod{p}$ with $f'(X)$ the formal derivative of $f(X)$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv a \pmod{p}$ and $f(\alpha) = 0$.*

Proof. The proof consists of finding by induction a sequence of integers $\{a_n\}_{n\in\mathbb{N}}$ such that $f(a_n) \equiv 0 \pmod{p^n}$ and $a_{n+1} \equiv a_n \pmod{p^n}$ which determines uniquely α. For $n = 1$, set $a_1 = a$. Now, suppose we have found $a_1, \cdots, a_n$ satisfying $a_{n-1} \equiv a_n \pmod{p^{n-1}}$ and $f(a_n) \equiv 0 \pmod{p^n}$, and hence the existence of $l_n \in \mathbb{Z}$ with $f(a_n) \equiv l_n p^n \pmod{p^{n+1}}$. Then we want a_{n+1} such that $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$ and $a_{n+1} \equiv a_n \pmod{p^n}$. Write $a_{n+1} = a_n + k_n p^n$. Hence $f(a_{n+1}) = f(a_n + k_n p^n) \equiv f(a_n) + k_n p^n f'(a_n) \pmod{p^{2n}}$ by Taylor expansion for polynomials. Thus $f(a_n) + k_n p^n \equiv 0 \pmod{p^{n+1}} \Leftrightarrow k_n f'(a_n) \equiv -l_n \pmod{p}$. Since $a_n \equiv a \pmod{p}$, we have $f'(a_n) \equiv f'(a) \not\equiv 0 \pmod{p}$, so we can solve for k_n and obtain a_{n+1}. To conclude set $\alpha = a + k_1 p + k_2 p^2 + \cdots \in \mathbb{Z}_p$. Then $\alpha \equiv a \pmod{p}$ and $f(\alpha) = 0$. □

Example 2.1.8. *Let p be an odd prime number. Take the polynomial $f(X) = X^2 - m$ with $p \nmid m$ not a square and is a quadratic residue modulo p. Say $a^2 \equiv m \pmod{p}$. Since $f'(a) = 2a \not\equiv 0 \pmod{p}$, the conditions of proposition 2.1.7 are satisfied. So there exist sequences $\{a_n\}_{n\geqslant 1}$ and $\{k_n\}_{n\geqslant 1}$ such that $a_{n+1} = a_n + k_n p^n$ with $k_n \in \{0, 1, 2, 3, \cdots, p-1\}$. Consider the p-adic integer $x = a + k_1 p + k_2 p^2 + \cdots + k_n p^n + \cdots$. It is a root of $f(X) = 0$ in $\mathbb{Q}_p$, i.e., $\sqrt{m} \in \mathbb{Q}_p$. This shows that for every odd prime p we have $\mathbb{Q} \subsetneqq \mathbb{Q}_p$.*

Example 2.1.9. *For the prime 2, consider the polynomial $f(X) = X^3 - m$ with $2 \nmid m$ a non-perfect cube. So, there is $x \in \mathbb{Q}_2$ such that $x^3 - m = 0$ in $\mathbb{Q}_2$, i.e., $\sqrt[3]{m} \in \mathbb{Q}_2$.*

Therefore for every p we have the strict embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Cantor's diagonal argument to prove that $\mathbb{R}$ is uncountable can be adapted to prove that the set of p-adic numbers $\mathbb{Q}_p$ is uncountable.

The real line $\mathbb{R}$ is an uncountable field containing $\mathbb{Q}$ as dense subfield. The density of $\mathbb{Q}$ in $\mathbb{Q}_p$ is an empty notion since we did not yet define any topology in $\mathbb{Q}_p$. This will be done with a satisfactory construction of $\mathbb{Q}_p$ from $\mathbb{Q}$, similarly as $\mathbb{R}$ is constructed from $\mathbb{Q}$, by *completing* $\mathbb{Q}$ with respect with the *p-adic absolute value.*

Chapter 3

Valued and Complete Fields

In this chapter the formalism that gives a rigorous treatment of the previous discussion among other things is introduced. We will start with the basic theory of absolute values and valuations on a field and the completion of that field. We will focus on the *ultrametric absolute values* and give the first properties of those fields complete with respect to such an absolute value. The references for this chapter are [1], [9], [23] or [7].

3.1 Absolute values and Valuations

3.1.1 Generalities

By analogy with Cantor's construction of the real numbers, any valued field K can be completed with respect to the metric induced by that absolute value.

Let us now turn to the basic theory of absolute values on a field K. From the properties of the usual absolute value $\mathbb{C}$ we abstract the definition

Definition 3.1.1. An absolute value on K is a function $|\,.\,|$: K $\to \mathbb{R}_{\geqslant 0}$ satisfying the following axioms

1. $|\,x\,| = 0 \Leftrightarrow x = 0$
2. $|\,xy\,| = |\,x\,||\,y\,|$
3. $|\,x + y\,| \leqslant |\,x\,| + |\,y\,|$, this is the triangle inequality.

From the second axiom we deduce that $|\,.\,|$ is a homomorphism from the multiplicative group K^* to the multiplicative group $\mathbb{R}^*$. The subgroup $|K^*|$ of $((\mathbb{R}_{>0})^*, .)$ is the *value group* of $|\,.\,|$.

Example 3.1.2. *The trivial absolute value has* $|\,x\,| = 1$ *if* $0 \neq x$.

Thus if $K = \mathbb{F}_q$, the finite field with q elements then every absolute value on $\mathbb{F}_q$ is trivial, because $\mathbb{F}_p^*$ is torsion and $\mathbb{R}^*$ is torsion free.

Example 3.1.3. *In* $\mathbb{C}$ *the usual absolute value is given by* $|z| = |x+iy| = \sqrt{x^2+y^2}$. *It is the only absolute value on* $\mathbb{C}$ *extending the usual absolute value on* $\mathbb{R}$ *as we will see in the sequel.*

Example 3.1.4. *Let* K *be a number field. If* $\sigma : K \to \mathbb{C}$ *is an embedding of* K, *then* $|\,x\,|_\sigma = |\sigma(x)|$ *is an absolute value on* K.

The p-adic absolute value on the rational numbers:
We know from commutative algebra that the localization of the integral domain $\mathbb{Z}$ at the prime ideal $(p) = p\mathbb{Z}$ is $\mathbb{Z}_{(p)} = \{\frac{r}{s} : r \in \mathbb{Z}, s \in \mathbb{Z} - p\mathbb{Z}\}$. This ring is principal and it has a unique prime ideal namely $p\mathbb{Z}_{(p)}$. A ring satisfying these properties is called a *discrete valuation ring.* Every $a \in \mathbb{Z}_{(p)}$ can be written uniquely as $a = p^n \frac{b}{c}$ with $p \nmid bc$ and $n \in \mathbb{N}$. Hence we have a function $v_p : \mathbb{Z}_{(p)} \to \mathbb{N} \cup \{\infty\}$ where one sets for $a \neq 0, v_p(a) = n,$ and $v_p(0) = \infty$. With the usual convention on ∞, *i.e,* $n+\infty = \infty$ and $\infty + \infty = \infty$, it satisfies the following properties

$$\begin{aligned} v_p(x+y) &\geqslant inf\{v_p(y), v_p(x)\} \\ v_p(xy) &= v_p(x) + v_p(y). \end{aligned}$$

We can extend v_p to $\mathbb{Q}$ as follows. Any $r \in \mathbb{Q}$ can be written $r = p^{v_p(r)}\frac{a}{b}$ with $p \nmid ab$ and $a,\ b,\ v_p(r) \in \mathbb{Z}$. Assign to $r \in \mathbb{Q}$ its valuation $v_p(r)$ at p. This is just the p-adic valuation of r that was defined in chapter 2, p 8. More generally we define

Definition 3.1.5. A *valuation* on a field K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ satisfying the following requirements:

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x+y) \geqslant inf\{\,v(x),\, v(y)\}$.

So v is a homomorphism from $(K^*, .)$ to $(\mathbb{R}, +)$. The subgroup $v(K^*)$ of $\mathbb{R}$ is called the *value group.* A valuation is called *discrete* when the value group is isomorphic to $\mathbb{Z}$ i.e., $v(K^*) = e\mathbb{Z}$ for some $0 \neq e \in \mathbb{R}$.

Example 3.1.6. *The trivial valuation* $v : K^* \to \mathbb{R}$, $v(x) = 0$ *for all* $x \in K^*$.

Example 3.1.7. *Our prototype of non-trivial valuation is the p-adic valuation on* $\mathbb{Q}$.

Example 3.1.8. *Each* $x \in \mathbb{Q}_p^*$ *is of the form* $x = \sum_{n \geqslant n_0}^{\infty} x_n p^n$ *with* $0 \neq n_0 \in \mathbb{Z}$. *Put* $v(x) = n_0$. *Then this defines a valuation on* $\mathbb{Q}_p$. *This is the extension of the p-adic valuation of* $\mathbb{Q}$ *to the p-adic field.*

Example 3.1.9. *In the field of formal Laurent series $K((X))$ in one indeterminate X over a field K, where each $f \in K((X))^*$ is of the form $f = \sum_{n \geqslant m}^{\infty} a_n X^n$, where $a_n \in K$, $a_m \neq 0$, the rule $v(f) = m$ defines a valuation on $K((X))$.*

These examples are instances of discrete valuations as the value group $v(K^*) \cong \mathbb{Z}$. If $v(K^*) = \mathbb{Z}$, then one says that the valuation v is *normalized*. Given a valuation v on a field K, then one can always define an absolute value.

Definition 3.1.10. Let $0 < c < 1$, then one defines $| x |_v = c^{v(x)}$ for $x \in K$.

When $K = \mathbb{Q}$, then the absolute value associated to the p-adic valuation is called *p-adic absolute value* and is denoted by $| \, . \, |_p$. From the property $v(x + y) \geq inf\{v(x), v(y)\}$, one sees that $|.|_v$ satisfies:

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

This inequality is called the *ultrametric inequality* . On the real line $\mathbb{R}$ the usual absolute value satisfies the *Archimedean postulate* :

$$\text{for each } x \in \mathbb{R}, \text{ there is } n \in \mathbb{Z} \text{ such that } | n | > | x |.$$

In general on a valued field K with absolute value $| \, . \, |$, if for each $x \in K$, there is $a \in \{n.1_K : n \in \mathbb{Z}\}$ such that $| a | > | x |$ then the absolute value is called *archimedean.*
This no longer holds with the p-adic absolute value on the rational numbers. Indeed the values $| x |_p$ for $x \in \mathbb{Z}$ are bounded as seen from the ultrametric inequality. Such an absolute value is called *non-archimedean.* In fact we have the following characterization of non-archimedean absolute values.

Proposition 3.1.11. *Let K be field with char $K \neq 0$. Put $A = \{n.1_K : n \in \mathbb{Z}\}$ the image of $\mathbb{Z}$ in K. Then an absolute value $| \, . \, |$ on K is non-archimedean if only if it is ultrametric.*

Proof. If $| \, . \, |$ is ultrametric then

$$|n.1_K| = |\underbrace{1_K + \cdots + 1_K}_{n \text{ times}}| \leqslant 1.$$

Conversely suppose that there is c such that $|x| \leqslant c$ for each $x \in A$. We have

$$|x + y|^l = |(x + y)^l| \quad = \quad |\sum_{k=0}^{l} \binom{l}{k} x^{l-k} y^k|$$

$$\begin{aligned} &\leqslant \sum_{k=0}^{l} |\binom{l}{k}||x^{l-k}||y^k| \\ &\leqslant c\sum_{k=0}^{l} |x^{l-k}||y^k| \\ &\leqslant c\sum_{k=0}^{l} (\max\{|x|, |y|)^l \\ &\leqslant c(l+1)(\max\{|x|, |y|\})^l \end{aligned}$$

Then taking l-th root and letting $l \to \infty$ give the ultrametric inequality. □

For upcoming use let us state

Proposition 3.1.12. *Let $|\,.\,|$ be an ultrametric absolute value on a field K. If $|\,x\,| \neq |\,y\,|$, then $|x+y| = max\{|\,x\,|, |\,y\,|\}$. Furthermore $|x_1 + x_2 + \cdots + x_n| = max\{|x_1|, |x_2|, \cdots, |x_n|\}$ if $|x_{i_0}| := max\{|x_1|, |x_2|, \cdots, |x_n|\} > |x_j|$ when $i_0 \neq j$.*

Proof. The second statement follows by induction from the first. So, if say $|\,x\,| > |\,y\,|$, then $|\,x\,| = |\,x + y - y\,| \leq max\{|\,x + y\,|, |\,y\,|\}$. This shows $|\,x\,| \leq |\,x + y\,|$ and from the ultrametric equality we have $|\,x + y\,| \leq |\,x\,|$. Hence $|\,x + y\,| = |\,x\,|$. □

As on the real line an absolute value on K defines a metric as follows. If $|\,.\,|$ is an absolute value on K, the function $d : K \times K \to \mathbb{R}_{\geqslant 0}$ $d(x, y) = |x-y|$ defines a metric on K. Thus the sets $B(a, \epsilon) = \{x : |a - x| < \epsilon\},\ \epsilon > 0$, form a fundamental system of neighborhoods of a. Hence this defines a topology on K induced by the metric d.

Definition 3.1.13. Let $|\,.\,|_1$, and $|\,.\,|_2$ be absolute values on K. They are said to be *equivalent* if their induced topologies are the same.

It is readily seen that this is an equivalence relation. Furthermore we have

Lemma 3.1.14. *If $|\,.\,|_1$ and $|\,.\,|_2$ are equivalent then $|\,x\,|_1 < 1 \Leftrightarrow |\,x\,|_2 < 1$*

Proof. Suppose $|\,.\,|_1$ and $|\,.\,|_2$ are equivalent. Then

$$|\,x\,|_1 < 1 \Leftrightarrow x^n \to 0 \ \text{ w.r.t } |\,.\,|_1 \Leftrightarrow x^n \to 0 \ \text{ w.r.t } |\,.\,|_2 \Leftrightarrow |\,x\,|_2 < 1.$$

□

The converse of lemma 3.1.14 also holds, see the proposition 3.1.17 below. Before we state it, we give two consequences of 3.1.14.

Corollary 3.1.15. *An archimedean absolute value cannot be equivalent to a non-archimedean absolute value.*

Proof. This is clear. □

Corollary 3.1.16. *If p and q are distinct primes then the $|\,.\,|_p$ and $|\,.\,|_q$ are inequivalent.*

Proof. If $|\,x\,|_q = c^{v_q(x)}$ with $0 < c < 1$, then $|\,q\,|_q < 1$ but $|\,q\,|_p = 1$. □

The equivalence class of a non-trivial absolute value is determined as follows.

Proposition 3.1.17. *The absolute values equivalent to $|\,.\,|$ are exactly the absolute values $|\,.\,|^s$ for some positive real number s. In the archimedean case we have $0 < s \leq 1$.*

Proof. When $|\,.\,|^s$ defines an absolute value then it is equivalent to $|\,.\,|$. To see the condition $0 < s \leq 1$ in the archimedean case, write $2^s = |\,1+1\,|^s \leq |\,1\,|^s + |\,1\,|^s = 2$.
Conversely suppose that $|\,.\,|_1$ is equivalent to $|\,.\,|_2$. By the lemma $|\,x\,|_1 < 1 \Leftrightarrow |\,x\,|_2 < 1$. Since $|\,.\,|_1$ is a non-trivial absolute value we can find $a \in K^*$ such that $|\,a\,|_1 < 1$. We want to show that $|\,.\,|_1 = |\,.\,|_2^s$ for some positive constant s. This comes down to showing that the ratio $s = \frac{\log(|x|_1)}{\log(|x|_2)}$ is independent of $x \in K^*$. For that fixed a we want to have $\frac{\log(|a|_1)}{\log(|a|_2)} = \frac{\log(|x|_1)}{\log(|x|_2)} \Leftrightarrow \frac{\log(|a|_1)}{\log(|x|_1)} = \frac{\log(|a|_2)}{\log(|x|_2)}$. For any rational number $r = \frac{m}{n}$ with $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ we have:

$$\begin{aligned} \frac{m}{n} < \frac{\log(|a|_1)}{\log(|x|_1)} &\Leftrightarrow |x^m a^{-n}|_1 < 1 \\ &\Leftrightarrow |x^m a^{-n}|_2 < 1 \\ &\Leftrightarrow \frac{m}{n} < \frac{\log(|a|_2)}{\log(|x|_2)} \end{aligned}$$

This implies that $\frac{\log(|a|_1)}{\log(|x|_1)} = \frac{\log(|a|_2)}{\log(|x|_2)}$. Indeed if we had $\frac{\log(|a|_1)}{\log(|x|_1)} < \frac{\log(|a|_2)}{\log(|x|_2)}$, then there is a rational $\frac{\log(|a|_1)}{\log(|x|_1)} < \frac{m}{n} < \frac{\log(|a|_2)}{\log(|x|_2)}$ which contradicts the above. Hence the result. □

Next we shall see that a finite number of inequivalent absolute values behave rather independently from each other.

Proposition 3.1.18. *Let $|\,.\,|_1, \cdots, |\,.\,|_n$ be pairwise inequivalent on K. Then there is a sequence $\{x_n\}_{n\in\mathbb{N}}$ in K that converges to 1 with respect to $|\,.\,|_1$ and to 0 with respect to $|\,.\,|_i$, $i \geqslant 2$.*

Proof. If we can find $a \in K^*$ such that $|\,a\,|_1 > 1$ and $|\,a\,|_i < 1$, $i \geqslant 2$ then $x_n = \frac{a^n}{1+a^n}$ will do. Indeed $|x_n - 1|_1 = |\frac{1}{1+a^n}|_1$ which converges to 0 and $|x_n - 0|_i = |\frac{a^n}{1+a^n}|_i$ which converges to 0 for $i \geqslant 2$. The existence of a is given by the following lemma. □

Lemma 3.1.19. *With the same hypotheses as above, we can find $a \in K^*$ such that $|\,a\,|_1 > 1$ and $|\,a\,|_i < 1$, $i \geqslant 2$.*

Proof. The proof is by induction on n. If $|\,.\,|_1$ and $|\,.\,|_2$ are inequivalent then there is a $b \in K^*$ with $|b|_1 > 1$ and $|b|_2 \leqslant 1$. Likewise we have $c \in K^*$ such that $|\,c\,|_1 \leqslant 1$ and $|\,c\,|_2 > 1$. Then $a = bc^{-1}$ is the desired element.
Now suppose that we have found $b \in K^*$ with $|\,b\,|_1 > 1$ and $|\,b\,|_i < 1$, $2 \leqslant i \leqslant n-1$. Since $|\,.\,|_1$ and $|\,.\,|_n$ are inequivalent there exists $c \in K^*$ with $|\,c\,|_1 > 1$ and $|\,c\,|_n < 1$.
If $|\,b\,|_n \leqslant 1$. Then $a = b^k c$ will do for k big enough to ensure that $|b^k c|_i < 1$, $2 \leqslant i \leqslant n-1$.
Otherwise, $|\,b\,|_n > 1$, then form $a_k = \frac{b^k}{1+b^k} c$. With respect to $|\,.\,|_1$ and $|\,.\,|_n$, a_k converges to c and with respect to $|\,.\,|_i$, $2 \leqslant i \leqslant n-1$, it converges to 0. So for k large enough and by continuity we have the desired a. □

Taking $d = a^{-1}$, we see that we have also found an element in K^* such that $|\,d\,|_1 < 1$ and $|\,d\,|_i > 1$, $2 \leqslant i \leqslant n$.

The proposition 3.1.18 illustrates the degree of freedom of a finite number of inequivalent absolute values. This fact does not generalize for infinitely many inequivalent absolute values as shown by theorem 3.1.30, p 21. We shall use proposition 3.1.18 to show a result known as the *approximation theorem*. This result can be interpreted as a Chinese Remainder Theorem as follows. Take n distinct prime numbers $p_1, \cdots, p_n$ and let $x_1, \cdots, x_n$ be integers. By the Chinese Remainder Theorem, for every $k \in \mathbb{N}$ there is an integer x such that

$$x \equiv x_i \pmod{p_i^k}.$$

Let $\epsilon > 0$, $\frac{1}{p_{i_0}} := \max_i\{\frac{1}{p_i}\}$. Choose k an integer such that $(\frac{1}{p_{i_0}})^k \leq \epsilon$. Next let $x \in \mathbb{Z}$ be a solution for the congruences $x \equiv x_i \pmod{p_i^k}$. Then we have $|\,x - x_i\,|_{p_i} \leq \epsilon$. So in terms of the p_i-adic absolute values on $\mathbb{Q}$, we may say that x is as "close" to x_i with respect to $|\,.\,|_{p_i}$ as we please. This interpretation has a weak analogue for K.

Theorem 3.1.20. (The Approximation Theorem) *Let $|\,.\,|_1, \cdots, |\,.\,|_n$ be pairwise inequivalent non-trivial absolute values on a field K. Let $x_1, \cdots, x_n \in K^*$. Then for any $\epsilon > 0$ there exists $x \in K^*$ such that $|\,x - x_i|_i < \epsilon$.*

Proof. By proposition 3.1.18 we can find a_i arbitrarily close to 1 with respect to $|\,.\,|_i$, and arbitrarily close to 0 with respect to $|\,.\,|_j$, $j \neq i$. More precisely for any $\epsilon > 0$ we have $|\,a_i - 1\,|_i < \frac{\epsilon}{n|\,x_i\,|_i}$ and $|\,a_i\,|_j < \frac{\epsilon}{n|\,x_i|_i}$, $i \neq j$. Form

$x = x_1a_1 + \cdots + x_na_n$, then

$$\begin{aligned} |\, x - x_i \,|_i &\leqslant |\, x_1 \,|_i |\, a_1 \,|_i + \cdots + |\, a_i - 1 \,|_i |\, x_i \,|_i + \cdots + |\, x_n|_i|a_n|_i \\ &< \frac{\epsilon |\, x_1|_i}{n |\, x_1 \,|_i} + \cdots + \frac{\epsilon |\, x_n \,|_i}{n |\, x_n \,|_i} \\ &= \epsilon. \end{aligned}$$

□

When dealing with non-archimedean absolute values, one translates this result by means of valuations using the correspondence between non-archimedean absolute values and valuations. One also has the following translation of equivalence for valuations via that correspondence. Two valuations v_1 and v_2 are equivalent if there is a positive real number s such that $v_1 = sv_2$. One may also translate the topology induced by an ultrametric absolute value in terms of its associated valuation.

In this thesis we will be mainly concerned with the absolute values and valuations analogous to the p-adic absolute values and the p-adic valuations on $\mathbb{Q}$.

Definition 3.1.21. Let $|\,.\,|$ be a non-archimedean absolute value on K and v its associated valuation. Put $A_{|\,.\,|} = \{x \in K : |\, x \,| \leqslant 1\} = \{x \in K : v(x) \geqslant 0\}$. This is called the *valuation ring.*

Remark 3.1.22. *The set $A_{|\,.\,|}$ is invariant up to equivalence of valuations or absolute values.*

For simplicity we shall drop the subscript $|\,.\,|$ if there is no possible confusion. It turns out from the ultrametric property that:

Proposition 3.1.23. *A is a ring. The subset $\mathfrak{m} = \{x \in K : |\, x \,| < 1\} = \{x \in K : v(x) > 0\}$ is the only maximal ideal of A. So A is a local ring.*

Proof. For $x,\ y \in A$, then $|\, x + y \,| \leqslant \max\{|\, x \,|,\ |y|\} \leqslant 1$. Clearly $xy \in A$. Now if $x \in A - \mathfrak{m}$ i.e. $|\, x \,| = 1$. Then $|\, x^{-1} \,| = 1$. Hence $x \in A^*$ the group of units of A. This implies that $\mathfrak{m}$ is the unique maximal ideal of A. □

Definition 3.1.24. The quotient $k = A/\mathfrak{m}$ which is a field is called the *residue field* of $(K, |\,.\,|)$.

Note that on a field K endowed with an ultrametric valuation or absolute value, the residue field may be infinite. Indeed assume that $char(K) \neq 0$ and consider the field of Laurent series in the variable T over K, $K((T))$ with the valuation defined in example 3.1.9, p 13. Then the valuation ring is $K[[T]]$ and its maximal ideal is $TK[[T]]$ so that its residue field $k = K[[T]]/TK[[T]] \cong K$. But at the same time we see that if we take K to be a finite field then the field $K((T))$ has finite residue field. Those fields

complete with respect to an ultrametric valuation or absolute value are the main object in this thesis. More precisely we will be concerned with those of characteristic zero. Before we specialize to this class of fields which are constructed from number fields as we will see in the sequel, see chapter 4, theorem 4.1.16, p 39; we have to see how one constructs an absolute value on a number field and rational function field.

3.1.2 Absolute value or valuation on number fields and rational function field

Following the construction of the p-adic absolute values on $\mathbb{Q}$, we construct ultrametric absolute values on number fields. To this end let K be a number field with ring of integers $\mathcal{O}$. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we have the discrete valuation ring $\mathcal{O}_{\mathfrak{p}} = \{\frac{x}{s} : x \in \mathcal{O},\ s \in \mathcal{O} - \mathfrak{p}\}$ which is the localization of $\mathcal{O}$ at $\mathfrak{p}$. We know from commutative algebra that the ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \{\frac{x}{s} : x \in \mathfrak{p},\ s \in \mathcal{O} - \mathfrak{p}\}$ is the unique maximal ideal of $\mathcal{O}_{\mathfrak{p}}$ and it is principal. Indeed, $\mathcal{O}_{\mathfrak{p}} \setminus \mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^*$, the units of $\mathcal{O}_{\mathfrak{p}}$. This means that up to units there is only one irreducible element in $\mathcal{O}_{\mathfrak{p}}$ say π, then $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} =< \pi >$. Therefore any element $r \neq 0$ in $\mathcal{O}_{\mathfrak{p}}$ can be written uniquely as $r = \pi^n u$ with $n \in \mathbb{N}$ and $u \in \mathcal{O}_{\mathfrak{p}}^*$. Since K is the field of fractions of $\mathcal{O}_{\mathfrak{p}}$ we see that every element $x \neq 0$ of K can be written uniquely as $x = \pi^n u$ with $n \in \mathbb{Z}$ and u a unit in $\mathcal{O}_{\mathfrak{p}}$. This defines a valuation $v_{\mathfrak{p}}(x) = n$ on K. We thus have a corresponding non-archimedean absolute value on K. In fact it turns out that up to equivalence all non-archimedean absolute values on a number field arise this way. To see this, we need the following fact which is interesting in its own right.

Lemma 3.1.25. *Let K be a number field with a non-archimedean absolute value $|\,.\,|$ on it. Let $\mathcal{O}$ be the ring of integers of K and let A be the valuation ring of K. Then, we have*

$$\mathcal{O} \subseteq A.$$

Proof. Take $x \in \mathcal{O}$. Then there are integers $a_i \in \mathbb{Z}, 0 \leqslant i \leqslant n-1$, with $n \geqslant 1$, such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Now suppose that x does not lie in A i.e., $|\,x\,| > 1$. Then from proposition 3.1.12 we would have $|\,x\,| > 1 \Rightarrow |\,x^n + a_{n-1}x^{n-1} + \cdots + a_0\,| = |\,x^n\,| \neq 0$ as $|\,x^n\,| > |\,a_i x^i\,|$ for $i = 0, \cdots, n-1$. A contradiction, and so our assumption is false. □

Theorem 3.1.26. *There is a* 1-1 *correspondence between the non-archimedean absolute values on K up to equivalence and the non-zero prime ideals of $\mathcal{O}$.*

Proof. Given a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we have the $\mathfrak{p}$-adic absolute value of K. Let $\mathfrak{p}$ and $\mathfrak{q}$ be two non-zero distinct prime ideals of $\mathcal{O}$. Then, $\mathfrak{p} + \mathfrak{q} = \mathcal{O}$, so that we have $x \in \mathfrak{p}$ and $y \in \mathfrak{q}$ such that $x + y = 1$. This means $|x|_{\mathfrak{p}} < 1$ and $|y|_{\mathfrak{q}} < 1$. If these absolute values were equivalent, then $|1 - y|_{\mathfrak{q}} < 1$, hence it follows that $1 - y \in \mathfrak{q}$ which gives the contradiction

$1 \in \mathfrak{q}$. This shows injectivity. Now let $|\,.\,|$ be a representative for a class of equivalent non-archimedean absolute values on K. The valuation ring A associated to $|\,.\,|$ with maximal ideal $\mathfrak{m}$ contains the ring of integers $\mathcal{O}$ of K. So, $\mathcal{O} \cap \mathfrak{m} = \mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}$. By definition of $\mathfrak{m}$, $|\,.\,|$ is trivial on $\mathcal{O} \setminus \mathfrak{p}$. Hence in the localized ring $\mathcal{O}_\mathfrak{p}$ the units $\mathcal{O}_\mathfrak{p}^*$ have absolute value 1. As the prime ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is principal, there is $\pi \in \mathcal{O}_\mathfrak{p}$ such that $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$. Hence every element $x \in K$ can be uniquely written as $u\pi^k$ with $k \in \mathbb{Z}$ and $u \in \mathcal{O}_\mathfrak{p}^*$. Therefore $|\,x\,| = |\,\pi\,|^k = |\,x\,|_\mathfrak{p}$. □

In contrast with the above result, the proposition 3.2.9, p 25, shows that there are only finitely many archimedean absolute values on K. Here is how they are constructed.

Let K be a number field, there are $n = [K : \mathbb{Q}]$ embeddings $\gamma : K \longrightarrow \mathbb{C}$. If $\gamma(K) \subseteq \mathbb{R}$, then γ is called real, otherwise γ is called complex. The complex embeddings come in pairs, $\gamma,\ \overline{\gamma}$ with $\overline{\gamma}(x) = \overline{\gamma(x)}$ (the bar denotes the complex conjugation in $\mathbb{C}$). So if r is the number of real embeddings and s is the number of pairs of complex embeddings, then $n = r + 2s$. Now let $|\,.\,|$ be the usual absolute value on $\mathbb{C}$.
For every embedding γ of K in $\mathbb{C}$ define $|\,x\,|_\gamma = |\,\gamma(x)\,|$. It is clear that $|\,x\,|_\gamma$ defines an archimedean absolute value, and furthermore $|\,.\,|_\gamma = |\,.\,|_{\overline{\gamma}}$. Up to conjugation we will see that the $|\,.\,|_\gamma$ are inequivalent absolute values. Hence we have constructed $n - s$ inequivalent absolute values on K where n is the number of embeddings of K and s the number of pairs of the complex ones. We will show that any archimedean absolute value on K is equivalent to one of these. So this will classify all the absolute values on a number field K. For $K = \mathbb{Q}$, this result was first established by S. Ostrowsky.

Theorem 3.1.27. (Ostrowsky) *Any absolute value ψ on $\mathbb{Q}$ is either equivalent to a p-adic absolute value or to the usual absolute value.*

Proof. If ψ is non-archimedean, then the above theorem 3.1.26 applies and we are done in this case.
Now suppose that ψ is archimedean. As every rational number is a quotient of integers, $\psi(-1) = 1$ and ψ is multiplicative, it is enough to show that for $n \in \mathbb{N}$, $\psi(n) = n^a$ with $0 < a \leq 1$. That is to say $\mathbb{N} \ni n \mapsto \frac{\log(\psi(n))}{\log(n)}$ is a constant function. By the triangle inequality, every $n \in \mathbb{N}$ satisfies $\psi(n) \leq n$. Hence $\psi(n) = n^b$ with b a positive real number so that $\psi(n) \geq 1$. Let $n,\ m \in \mathbb{N}$ arbitrary. We can write any integer power of m as

$$m^l = \sum_{i=0}^{r} a_i n^i$$

with $a_i \in \{0, \cdots n-1\}$, $a_r \neq 0$ and r is the integer part of $\log(m^l)/\log(n) =$

$l\log(m)/\log(n)$. This gives $r/l \leq \log(m)/\log(n)$. We then have

$$\begin{aligned}
\psi(m)^l &\leq \sum_{i=0}^{r} \psi(a_i)\psi(n)^i \\
&\leq \sum_{i=0}^{r} n\psi(n)^i \quad (\text{since } \psi(a_i) < n) \\
&\leq (r+1)n\,(max\{1,\ \psi(n)^r\}) \quad (\text{because } \psi(n)^i \\
&\leq max\{1, \psi(n)^r\} \text{ for } 0 \leq i \leq r) \\
&= (r+1)n(max\{1,\ \psi(n)\})^r \\
\Longrightarrow \psi(m) &\leq \{(r+1)n\}^{\frac{1}{l}}(max\{1,\ \psi(n)\})^{\frac{r}{l}} \\
&\leq \{(r+1)n\}^{\frac{1}{l}}(max\{1,\ \psi(n)\})^{\frac{\log(m)}{\log(n)}}.
\end{aligned}$$

As $\psi(n) \geq 1$ and let $l \to \infty$, we obtain that

$$\psi(m)^{\frac{1}{\log(m)}} \leq \psi(n)^{\frac{1}{\log(n)}}.$$

Since the roles of m and n are symmetric we see that $\psi(m)^{\frac{1}{\log(m)}} = \psi(n)^{\frac{1}{\log(n)}}$ with $m,\ n$ arbitrary integers. Hence $\frac{\log(\psi(n))}{\log(n)} =: a$ is a constant $\in (0,\ 1]$ so that $\psi(n) = n^a$. This is what we wanted. □

Having this in hand, we shall now consider instead of $\mathbb{Q}$ the rational function field in one variable over a field F, $F(X)$. This shows one aspect of the analogy between $F(X)$ and $\mathbb{Q}$. Let $f \in F(X)$, $f = \frac{h}{g}$ with $g,\ h \in F[X]$. Define the degree of f to be $deg(f) = deg(h) - deg(g) \in \mathbb{Z}$ with the usual convention $deg(0) = -\infty$.

Definition 3.1.28. Take a real number $a > 1$. Define the degree absolute value $|\,.\,|_{deg}$ as:

$$\begin{aligned}
|\,.\,|_\infty : F(X) &\longrightarrow \mathbb{R}_{\geq 0} \\
f &\mapsto a^{deg(f)}
\end{aligned}$$

This is indeed an absolute which is trivial on F and hence non-archimedean.

We next associate to each irreducible polynomial p in $F[X]$ an absolute value as we did for the rational primes. Let p be irreducible in $F[X]$ and $f = \frac{h}{g} \in F(X)$. Then we can write $f = \mathsf{p}^{v_\mathsf{p}(f)}\frac{h_1}{g_1}$ with p coprime with $h_1 g_1$ and $v_\mathsf{p}(f) \in \mathbb{Z}$. Now let c be real a number such that $0 < c < 1$, put $|\,f\,|_\mathsf{p} := c^{v_\mathsf{p}(f)}$. Similarly as for the p-adic absolute value on $\mathbb{Q}$, one verifies that $|\,.\,|_\mathsf{p}$ is a non-archimedean absolute value independent of the choice of c. Hence we have defined infinitely many inequivalent absolute values coming from the irreducible polynomials $\mathsf{p} \in F[X]$. The next result shows that we have an exhaustive list of the absolute values on $F(X)$ trivial on F.

Theorem 3.1.29. *We fix the rational function field $F(X)$. Then a non-trivial absolute value $|\,.\,|$ on $F(X)$ which trivial on F is either equivalent to $|\,.\,|_\infty$ or $|\,.\,|_{\mathfrak{p}}$ for some irreducible polynomial $\mathfrak{p} \in F[X]$.*

Proof. By assumption $|\,.\,|$ is non-archimedean. It is enough to consider $|\,f\,|$ for f a non-constant polynomial in the ring $F[X]$. So, let $f = a_nX^n + \cdots + a_0 \in F[X]$ with $a_n \neq 0$. By the ultrametric inequality we have $|\,f\,| \leq \max\{|\,X\,|^n, \cdots, |\,a_0\,|\}$. Therefore if $|\,X\,| > 1$, we obtain that $|\,f\,| = |\,X\,|^n$. Thus $|\,.\,|$ is equivalent to $|\,.\,|_\infty$ in this case.
Now if $|\,X\,| \leq 1$, $F[X]$ lies inside the valuation ring $A = \{f \in F(X) : |\,f\,| \leq 1\}$. And one concludes similarly to the number field case. □

Next we consider all possible absolute values on $\mathbb{Q}$ and on a rational function field $F(X)$ and state a result that gives a relation between them. This result is known as *the product formula* and is obtained after normalizing the absolute values on these prime fields. Before stating it, we shall mention that the product formula holds in a more general context. That is to say that this important formula holds when instead of $\mathbb{Q}$ or $F(X)$ one has a number field or a function field. In this context, the product formula is a consequence of the one given below , for the details see [18, pp 184-185]. The normalization of absolute values is done as follows.

In the general setting of a number field K, one has a natural choice for the base a of a non-archimedean absolute value $|\,.\,|_{\mathfrak{p}}$ on K. Indeed, the prime ideal $\mathfrak{p}$ has a finite residue field $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Hence the base $a := q^{-1}$ where $q = card(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$. When $K = \mathbb{Q}$, then the residue field is the finite field with p elements, so that $|\,x\,|_p = p^{-v_p(x)}$ for $x \in \mathbb{Q}$. For an archimedean absolute $|\,.\,|$ value on K, we know that $|\,x\,| = |\,\sigma(x)\,|$ with $\sigma : K \to \mathbb{C}$, an embedding. Then one puts $|\,x\,|_1 = |\,x\,|$ if σ is real or $|\,x\,|_1 = |\,x\,|^2$ otherwise. Note that the latter is not an absolute value, but this is needed in order to obtain the product formula in general context, see again [18, pp 184-185]. The resulting absolute values are called *normalized* absolute values.

In the context of a rational function field $F(X)$, the absolute value associated to an irreducible polynomial $\mathfrak{p}$ is normalized as follows. We fix $c \in (0,\ 1)$, and put $|\,x\,|_{\mathfrak{p}} = c^{deg(\mathfrak{p})v_{\mathfrak{p}}(x)}$ and $|\,f\,|_\infty = (c^{-1})^{deg(f)}$.
The importance of normalization of absolute values lies in what follows.

Theorem 3.1.30. (Product Formula) *Let $0 \neq x \in F(X),$ or $\mathbb{Q}$. Then*

$$\prod |\,x\,| = 1,$$

where the product runs over the normalized archimedean absolute value and the non-archimedean absolute values in the case of $\mathbb{Q}$ and in the case of $F(X)$ the product runs over the normalized non-archimedean absolute values that are defined above.

Proof. We first have to check that this infinite product is well defined in both cases. Note that only a finite number of primes or irreducible polynomials occurs in the factorization of x. This says that almost all the factors in the infinite product are 1. The normalization is chosen so that the formula holds. □

After having classified the absolute values and valuations on the most relevant fields in number theory, namely number fields and rational function fields, we shall now turn to the important concept of *completion*.

3.2 Complete Fields

As a prototype for completing fields one takes the example of the construction of the real numbers from the rationals by using the usual absolute value $|\,.\,|_\infty$. Here the notion of *Cauchy sequence* plays a fundamental role. We shall do it for a general valued field K.

Definition 3.2.1. Let $|\,.\,|$ be an absolute value on K and $\{a_n\}_{n\in\mathbb{N}}$ a sequence in K. Then $\{a_n\}$ is called a *Cauchy sequence* if for every $\epsilon > 0$ there is $l \in \mathbb{N}$ such that if $m > n \geq l$ then $|\, a_m - a_n \,| < \epsilon$.

There is of course an equivalent definition of Cauchy sequence by means of a valuation defined on K. This reads as follows. Let $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ be a valuation and $\{a_n\}_{n\in\mathbb{N}}$ a sequence in K. Then $\{a_n\}_{n\in\mathbb{N}}$ is Cauchy with respect to v if:

$$\forall\, m \in \mathbb{N},\, \exists\, N \in \mathbb{N},\, \forall\, n \geq N,\, \forall\, l \in \mathbb{N};\ v(a_{n+l} - a_n) \geq m.$$

In other words in a Cauchy sequence the terms become arbitrarily close with respect to an absolute value from a certain step. So, one would expect Cauchy sequences to converge to a limit in their underlying field with respect to the metric topology coming from the absolute value. If this is the case the field is said to be *complete*, otherwise it is *incomplete*. Every field is complete with respect to the trivial absolute values. In general with respect to a non-archimedean absolute value, the values of the terms in a Cauchy sequence which does not converge to zero become stationary at a certain step. Indeed we have the proposition.

Proposition 3.2.2. *Let K be a field equipped with an ultrametric absolute value $|\,.\,|$ and let $\{x_n\}$ be a Cauchy sequence not converging to zero. Then there exists $m \in \mathbb{N}$ such that for all $n \geq m$ we have $|\, x_n \,| = |\, x_m \,|$.*

Proof. Since $\{x_n\}$ is a Cauchy sequence not converging to zero, we can find a positive real number δ such that for infinitely many n we have $|\, x_n \,| \geq \delta$. This means that the sequence of positive real numbers $\{|\, x_n \,|\}$ which is Cauchy has a limit greater or equal to δ. Therefore there is $N \in \mathbb{N}$ such

that for all $n \geq N$ we have $|\, x_n \,| > \frac{2}{3}\delta$ and $|\, x_{n+p} - x_n \,| < \frac{\delta}{2}$ for all $p \in \mathbb{N}$ so that $|\, x_{n+p} - x_n \,| < |\, x_n \,|$. Now from the ultrametric inequality we have $|\, x_{n+p} \,| = |\, x_{n+p} - x_n + x_n \,| = max\{|\, x_{n+p} - x_n \,|,\ |\, x_n \,|\} = |\, x_n \,|$ for all $p \in \mathbb{N}$ and $n \geq N$. This ends the proof. □

The rational numbers endowed with the usual topology are incomplete and its completion is just the usual field of real numbers. This is a "well known" fact, so, we shall not discuss it here. We shall instead show that the rational numbers are also incomplete with respect to a p-adic topology.

We fix a rational prime p and as usual $|\,.\,|_p$ is the p-adic absolute value on $\mathbb{Q}$. We also choose a polynomial f in $\mathbb{Z}[X]$ satisfying the following properties:

1. f is irreducible in $\mathbb{Q}[X]$ of degree ≥ 2
2. There is $s \in \mathbb{Z}$ such that $f(s) \equiv 0 \pmod{p}$
3. $f'(s) \not\equiv 0 \pmod{p}$ where f' is the formal derivative of f.

By the Hensel's lemma, proposition 2.1.7, there is a sequence of integers $\{a_n\}_{n\in\mathbb{N}}$ such that $f(a_n) \equiv 0 \pmod{p^n}$ and $a_{n+1} \equiv a_n \pmod{p^n}$. The sequence $\{a_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence in $\mathbb{Q}$ with respect to the p-adic topology and converges to an irrational (not in $\mathbb{Q}$) element in $\mathbb{Q}_p$. Indeed, on one hand for $m > n$ we have $|\, a_m - a_n|_p \leqslant p^{-n}$, which shows that it is Cauchy. Thus p-adically the sequence $\{a_n\}_{n\in\mathbb{N}}$ converges to a. But, a is not rational by 1. This establishes the incompleteness of the rational numbers with respect to the p-adic absolute value.

The general setting when we are given a field K with absolute value $|\,.\,|$, we can construct the completion of K by imitating Cantor's method of construction of the real numbers $\mathbb{R}$ from the rational numbers $\mathbb{Q}$. To this end we set $\mathcal{C}$ the set of all Cauchy sequences with entries in K. For $\{a_n\},\ \{b_n\} \in \mathcal{C}$ define $\{a_n\} + \{b_n\} = \{a_n + b_n\}$ and $\{a_n\} \times \{b_n\} = \{a_n b_n\}$.

Lemma 3.2.3. *With these operations $\mathcal{C}$ is a commutative ring with unit element the sequence $\{1\}_{n\in\mathbb{N}}$ and the zero element $\{0\}_{n\in\mathbb{N}}$.*

Proof. By the the triangle inequality, if $\{a_n\},\ \{b_n\} \in \mathcal{C}$, then $\{a_n + b_n\} \in \mathcal{C}$ as well. From the identity $a_m b_m - a_n b_n = a_n(b_m - b_n) + b_m(a_m - a_n)$ we obtain $|\, a_m b_m - a_n b_n \,| \leq |\, a_n \,||\, b_m - b_n \,| + |\, b_m \,||\, a_m - a_n \,|$. This implies that for $\{a_n\},\ \{b_n\} \in \mathcal{C}$ we have $\{a_n b_n\} \in \mathcal{C}$. Indeed, $\{|\, a_n \,|\},\ \{|\, b_n \,|\}$ have upper bounds as they are Cauchy. □

Consider the subset $\mathcal{N} \subset \mathcal{C}$ of all the sequences that converge to zero in K called the set of null sequences.

Lemma 3.2.4. *$\mathcal{N}$ is the only maximal ideal of the ring $\mathcal{C}$.*

Proof. It is easy to check that $\mathcal{N}$ is an ideal. We check the maximality of $\mathcal{N}$. For $\{b_n\} \in \mathcal{C} \setminus \mathcal{N}$, from a certain step l the terms of a non-null sequence are non-zero. So, set $c_n = 0$ for $n < l$ and $c_n = b_n^{-1}$ otherwise. Then the sequence $\{c_n\}$ is Cauchy and $\{b_n c_n\}$ converges to 1. This shows that $\{b_n\}$ is a unit of $\mathcal{C}$ and $\mathcal{N}$ is indeed the only maximal ideal of $\mathcal{C}$. □

Now, we can prove:

Theorem 3.2.5. *Let K be a valued field with absolute value $|\ |$. Then there is a field $\hat{K}$ with the following properties:*

1. *There is an embedding $\phi : K \hookrightarrow \hat{K}$; hence $\hat{K}$ is an extension of K.*
2. *There is an absolute $|\,.\,|_{\hat{K}}$ on $\hat{K}$ that extends $|\,.\,|$.*
3. *In the topology induced by $|\,.\,|_{\hat{K}}$ K is dense in $\hat{K}$ and $\hat{K}$ is complete*
4. *$\hat{K}$ is unique up to topological isomorphism.*

Proof. **Existence:** We put $\hat{K} = \mathcal{C}/\mathcal{N}$. For each $a \in K$ the stationary sequence $\{a\}_{n\in\mathbb{N}}$ is Cauchy and so we have $\phi : K \hookrightarrow \hat{K}$. Define $|\,.\,|_{\hat{K}} : \hat{K} \longrightarrow \mathbb{R}_{\geq 0}$, $\alpha \equiv \{a_n\} \pmod{\mathcal{N}} \longmapsto |\,\alpha\,|_{\hat{K}} = \lim_{n\to\infty} |\,a_n\,|$. First note that since $\{a_n\}$ is Cauchy then $\{|\,a_n\,|\}$ is Cauchy in the complete field $\mathbb{R}$, hence $\lim_{n\to\infty} |\,a_n\,|$ is well defined. It is clear that if $\alpha \equiv \beta \pmod{\mathcal{N}}$ then $|\,\alpha\,|_{\hat{K}} = |\,\beta\,|_{\hat{K}}$. All the other axioms follow easily and $|\,.\,|_{\hat{K}}$ restricted to K is $|\,.\,|$.
Density: Take $\alpha \equiv \{a_n\} \pmod{\mathcal{N}}$. We identify K with its image in $\hat{K}$, we have by definition $|\,a_n - \alpha|_{\hat{K}} = \lim_{l\to\infty} |\,a_l - a_n\,|$. Since $\{a_n\}$ is Cauchy we see that the sequence $\{a_n\} \in K$ converges to $\alpha \in \hat{K}$.
Completeness: Suppose that $\{\alpha_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence in $\hat{K}$. For each α_n let $\{a_{n,k}\}_{k\in\mathbb{N}}$ be a Cauchy sequence in K with $\alpha_n \equiv \{a_{n,k}\} \pmod{\mathcal{N}}$. Consider the sequence $a_{1,1}, a_{2,2}, \cdots, a_{n,n}, \cdots$. The sequence $\{a_{n,n}\}$ is Cauchy. Indeed, since $\lim_{k\to\infty} a_{n,k} = \alpha_n$, $\exists l \in \mathbb{N}$, $\forall k \geq l$, $|\,a_{n,k} - \alpha_n|_{\hat{K}} \leq \min\{\frac{1}{n}, \frac{1}{k}\}$. Therefore, $|\,a_{n,n} - a_{m,m}\,|_{\hat{K}} = |\,a_{n.n} - a_{m,m}\,| \leq |\,a_{n,n} - \alpha_a\,|_{\hat{K}} + |\,a_{m,m} - \alpha_m|_{\hat{K}} + |\alpha_m - \alpha_m\,|$. So, let α be the image of $\{a_{n,n}\}_{n\in\mathbb{N}}$ in $\hat{K}$, hence $|\,\alpha - \alpha_n\,|_{\hat{K}} \leq |\,\alpha - a_{n,n}\,|_{\hat{K}} + |\,a_{n,n} - \alpha_n|_{\hat{K}}$. The completeness of $\hat{K}$ is established.
Uniqueness: Suppose $(F, |\,.\,|_F) \supset (K, |\,.\,|)$ with the above properties. Then we define a surjective ring homomorphism ψ: $\mathcal{C} \to F$, $\psi(\alpha) = \lim_{n\to\infty} a_n$ where $\alpha \equiv \{a_n\} \pmod{\mathcal{N}}$. This is continuous by definition. Therefore we have a continuous isomorphism $\hat{K} = \mathcal{C}/\mathcal{N}$. Suppose there is another continuous isomorphism $\phi : \hat{K} \to F$. Then $\phi = \psi$ on K, and hence we have equality on $\hat{K}$ since K is dense in $\hat{K}$. □

Example 3.2.6. *The completion of $\mathbb{Q}(i)$ with respect to the usual absolute value on the complex numbers is $\mathbb{R}(i) = \mathbb{C}$.*

Example 3.2.7. *We shall soon see that the completion of the rational numbers that with respect the p-adic absolute values is the p-adic field $\mathbb{Q}_p$.*

Given an absolute value $|\,.\,|$ on a field K, we can characterize the completion of K with respect to $|\,.\,|$. To start with suppose the absolute value is archimedean. Necessarily K is of characteristic zero as there is no archimedean absolute value on a field of positive characteristic. Hence, we have $\mathbb{Q} \subseteq K$. Let F be the completion of K with respect to $|\,.\,|$. We therefore have $\mathbb{R} \subseteq F$. The next theorem says that in the case of strict inclusion, then, F is the field of complex number $\mathbb{C}$. This fundamental fact was first proved by Ostrowsky.

Theorem 3.2.8. (Ostrowsky). *The only complete archimedean fields are the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$.*

Proof. See [1, p 24], [18, p 124], or [23, p 13]. □

Ostrowsky's theorem has the following important consequence for archimedean absolute values on a number field.

Proposition 3.2.9. *Let K be a number field. To an embedding $\sigma : K \to \mathbb{C}$ corresponds an absolute value $|\,x\,|_\sigma = |\,\sigma(x)\,|$ on K. This induces a 1-1 correspondence between absolute values on K extending the usual absolute value on $\mathbb{Q}$, modulo conjugation.*

Proof. Let $\sigma : K \to \mathbb{C}$ be an embedding. Define the absolute value $|\,.\,|_\sigma$ on K by $|\,x\,|_\sigma = |\,\sigma(x)\,|$, taking the usual absolute value of $\sigma(x) \in \mathbb{C}$. This defines an archimedean absolute value on K extending the usual absolute value on $\mathbb{Q}$. For surjectivity, suppose $|\,.\,|$ is any absolute value on K extending the usual absolute value on $\mathbb{Q}$. Let F be the the completion of K with respect to $|\,.\,|$. As F is either $\mathbb{R}$ or $\mathbb{C}$ we have an embedding $\sigma : K \to \mathbb{C}$ and $|\,x\,| = |\sigma(x)|$. For injectivity, let σ_1, σ_2 be two embeddings such that the absolute values $|\,.\,|_{\sigma_1}$, $|\,.\,|_{\sigma_2}$ are equivalent. Let $\hat{K}_{\sigma_i}$ be the completion of K with respect to $|\,.\,|_{\sigma_i}$. For $i = 1, 2$, define the embeddings $\hat{\sigma_i} : \hat{K}_{\sigma_i} \to \mathbb{C}$ by $\hat{\sigma_i}(x) = \lim_{n\to\infty} \sigma_i(x_n)$ where $\{x_n\}$ is a sequence in K converging to x. Each $\hat{\sigma_i}$ fixes the completion $\mathbb{R}$ of $\mathbb{Q}$ and we have a commutative diagram

$$\begin{array}{ccc} K & & \\ {\scriptstyle\sigma_1}\downarrow & \searrow^{\sigma_2} & \\ \mathbb{C} \supseteq \hat{K_{\sigma_1}} & \longrightarrow & \hat{K}_{\sigma_2} \subseteq \mathbb{C} \end{array}$$

giving a continuous isomorphism $\hat{K}_{\sigma_1} \mapsto \hat{K}_{\sigma_2}$ fixing $\mathbb{R}$. Either both $\hat{K}_{\sigma_1}, \hat{K}_{\sigma_2}$ are $\mathbb{R}$ or both are $\mathbb{C}$. Hence σ_1 and σ_2 are equal to the identity or are conjugate of each other [1] . This shows injectivity since a complex embedding σ and its conjugate $\bar{\sigma}$ induces the same absolute value. □

[1] In fact there is no non-trivial automorphism of $\mathbb{R}$ at all, continuous or not. If we

The proposition 3.2.9 and theorem 3.1.26 give the complete list of absolute values on a number field $K/\mathbb{Q}$.

We just saw that the complete archimedean fields arising from number fields have a much simpler characterization. Now what about the non-archimedean complete fields?

Let K be a valued field with a non-archimedean absolute value $|\,.\,|$. Let $v(\,.\,) = -\log(|\,.\,|)$ be the corresponding valuation. For our purposes, we shall be concerned with discrete valuations $v : K^* \to e\mathbb{Z}$ with $e \in \mathbb{N}$ and surjective. As usual we call A the discrete valuation ring of v, $\mathfrak{m}$ its only maximal ideal and $k = A/\mathfrak{m}$ its residue field. Let $\pi \in A$ with minimal positive v-value, then it is easy to see that $\mathfrak{m} =< \pi >$. A generator π of $\mathfrak{m}$ is called a *prime* of K or *uniformizer* , it is characterized by $v(\pi) = e$. As A is a discrete valuation ring, one knows all the ideals $\mathfrak{p}$ are of the form $\mathfrak{p} = \pi^n A = \mathfrak{m}^n$ for some positive integer n. Hence we have the filtration of ideals of A

$$A \supset \pi A \supset \pi^2 A \supset \cdots \supset \pi^n A \supset \cdots.$$

Note that the $\pi^n A$ are both open and closed in the v-topology as $x \in \pi^n A \Leftrightarrow v(x) \geq nv(\pi) \Leftrightarrow v(x) > (n-1)v(\pi)$ and they form a fundamental system of neighborhoods of zero.

In the multiplicative group K^*, inside the group of units A^*, we have the group of *principal units* $U_1 = 1+\pi A$ and the n-th higher unit group $U_n = 1 + \pi^n A$. These are both closed and open and form a fundamental system of neighborhoods of 1. We also have the filtration of subgroups

$$A^* \supset 1 + \pi A \supset 1 + \pi^2 A \supset \cdots \supset 1 + \pi^n A \supset \cdots.$$

The successive quotients in this filtration are computed as follows.

Proposition 3.2.10. *With the above notation one has*

$$A^*/U_n \cong (A/\pi^n A)^*,\ U_n/U_{n+1} \cong A/\pi A \cong \pi^n A/\pi^{n+1} A,\ \textit{for}\ n \geq 1.$$

Proof. The surjective ring homomorphism $A \mapsto A/\pi^n A$ induces the homomorphism of groups of units $\phi : A^* \to (A/\pi^n A)^*$, $u \in A^* \mapsto \phi(u) := u \pmod{\pi^n}$. ϕ is surjective and has kernel U_n, hence $A^*/U_n \cong (A/\pi^n A)^*$. Next, define $\chi : U_n \to A/\pi A$, $u = 1 + a\pi^n \in U_1 \mapsto \chi(u) := a \pmod{\pi}$.

---

suppose the automorphism to be continuous, then it is the identity on the dense set $\mathbb{Q}$; thus it is the identity on $\mathbb{R}$. But we can get rid of the continuity hypothesis by using the fact that $\mathbb{R}$ is totally ordered. Indeed, let ψ be an automorphism of $\mathbb{R}$, then ψ preserves the order on $\mathbb{R}$. Indeed let $x < y$ be real numbers. Then there is $w \in \mathbb{R}$ with $y - x = w^2$. Thus $\psi(y) - \psi(x) = \psi(w)^2$. Now choose $a \in \mathbb{R}$ such that $a < \psi(a) = b$. Hence there is a rational number r with $a < r < b$, this gives $\psi(a) < \psi(r) = r < \psi(b)$, and this is absurd. For the automorphisms of $\mathbb{C}$, the identity and the complex conjugation are the only continuous automorphisms while there are uncountably many discontinuous automorphisms, see [24] for the details.

This is a surjective homomorphism with kernel U_{n+1}. Lastly, define $\psi : A/\pi A \to \pi^n A/\pi^{n+1},\ a + \pi A \mapsto \pi^n a + \pi^{n+1} A$. This is also onto and injective. □

Let now $(\hat{K}, \hat{v})$ be the completion of (K, v). In contrast with $(\mathbb{R}, |\,.\,|_\infty)$, $(\mathbb{Q}, |\,.\,|_\infty)$ where the value group $|\,\mathbb{R}^*\,|_\infty = \mathbb{R}_{>0} \supset |\,\mathbb{Q}^*\,|_\infty = \mathbb{Q}_{>0}$, the value group of K and its completion $\hat{K}$ are the same.

Lemma 3.2.11. *Let $(\hat{K}, \hat{v})$ be the completion of (K, v), then $v(K^*) = \hat{v}(\hat{K}^*)$.*

Proof. It is clear that $v(K^*) \subset \hat{v}(\hat{K}^*)$. Now let $x \in \hat{K}^*$. Then there is a v-Cauchy sequence $\{x_n\}$ in K that converges to x. So there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ we have $\hat{v}(x - x_n) > \hat{v}(x)$. Then we have $\hat{v}(x_n - x + x) = min\{\hat{v}(x_n - x),\ \hat{v}(x)\} = \hat{v}(x)$. □

In other words, the value group of a discrete valued field K is invariant under completion. The residue field is also invariant under completion.

Proposition 3.2.12. *Let $(\hat{K}, \hat{v})$ be the completion of $(K,\ v)$ with respective valuation rings $\hat{A}$, A, maximal ideals $\hat{\mathfrak{m}}$, $\mathfrak{m}$ and residue fields $\hat{k}$, k. Then*

$$A/\mathfrak{m}^n \cong \hat{A}/\hat{\mathfrak{m}}^n \ \textit{for}\ n \geq 1.$$

In particular $k \cong \hat{k}$.

Proof. Since $\hat{m}^n \cap A = \mathfrak{m}^n$ we have an embedding $\phi : A/\mathfrak{m}^n \hookrightarrow \hat{A}/\hat{\mathfrak{m}}^n$. For surjectivity, let $x \in \hat{A}$, then there is a Cauchy sequence $\{x_m\}$ in K such that $x = \lim\limits_{m\to\infty} x_m$. We have $\hat{v}(x) \geq 0$, hence by continuity of $\hat{v}$, $v(x_m) \geq 0$ for large m. So, for large m, $x_m \in A$ and $x_m \equiv x \pmod{\hat{\mathfrak{m}}^n}$. This gives $\phi(x_m) = x$. □

We shall next see that our informal definition of the p-adic number field in the previous chapter is a special case of a general fact, that is to say that the elements in a complete non-archimedean field admit a representation as a convergent Laurent series in a prime element. Let R be a subset of A such that the restriction of the canonical projection $A \to A/\mathfrak{m}$ is bijective and $0 \in R$. R is called a *system of representatives* of $k = A/\mathfrak{m}$ in A. By definition of R we have $A = \bigcup_{r\in R}\{r + \mathfrak{m}\} = \{r + \mathfrak{m} : r \in R\}$. Hence one has $A = R + \mathfrak{m}$. For $n \in \mathbb{Z}$, let π_n be such that $v(\pi_n) = n$.

Theorem 3.2.13. *Let $(\hat{K}, \hat{v})$ be the completion of (K, v) and let $\pi_n \in K$ be as above. Then any $x \in \hat{K}$ has a unique representation as a convergent Laurent series expansion:*

$$x = \sum_{n \geq n_0} r_n \pi_n, \quad \textit{with}\ n_0 \in \mathbb{Z},\ \ r_n \in R.$$

Proof. **Existence:** From the equality $\hat{A} = R + \hat{\mathfrak{m}}$, and by noting that $\pi_n \hat{A} = \hat{\mathfrak{m}}^n$, one has $\hat{\mathfrak{m}}^n = \pi_n R + \pi_{n+1} R + \cdots + \pi_m R + \hat{\mathfrak{m}}^{m+1}$ for $m \geq n$. Hence for any $x \in \hat{\mathfrak{m}}^n$, and for $m \geq n$ there exist $r_n, r_{n+1}, \cdots, r_m \in R$ such that

$$x \equiv r_n \pi_n + \cdots + \pi_m \pmod{\hat{\mathfrak{m}}^{m+1}}.$$

This gives $x = \sum_{n \geq n_0}^{\infty} \pi_n r_n$.
Uniqueness: Suppose that we have $0 \neq x = \sum_{n \geq n_0} r_n \pi_n = \sum_{i \geq i_0} a_i \pi_i$ with $a_{i_0}, r_{n_0} \neq 0$ and $a_i \in R$. Then $i_0 = v(x) = n_0$. From $0 = (a_{i_0} - r_{i_0})\pi_{i_0} + \sum_{i \geq i_0 + 1}(a_i - r_i)\pi_i$, one sees that we must have $v(a_{i_0} - r_{i_0}) = \infty$, that is $a_{i_0} = r_{i_0}$. Therefore one obtains that $a_i = r_i$ for all $i \geq i_0$ and so one gets the uniqueness of the expansion of x. □

In particular, if we take $K = \mathbb{Q}$, and $\pi_n = p^n$, we see that the completion of $\mathbb{Q}$ with respect to the p-adic valuation is just $\mathbb{Q}_p$ the field of p-adic numbers.

This representation of complete discrete valued fields leads to an alternative way of viewing them. Let π be a prime of K, then one can take $\pi_n = \pi^n$. Therefore any $a \in \hat{A}$ can be written as $a = \sum_{i=0}^{\infty} a_n \pi^n$. Consider now the partial sums $s_n = \sum_{i=0}^{n-1} a_n \pi^n$, we have $s_{n+1} \equiv s_n \pmod{\pi^n}$. Hence, $(s_1 \pmod{\mathfrak{m}}, s_2 \pmod{\mathfrak{m}^2}, \cdots, s_n \pmod{\mathfrak{m}^n}. \cdots) \in \lim_{\leftarrow n} A/\mathfrak{m}^n$, the projective limit. Thus we have an homomorphism

$$\begin{aligned} \psi : \hat{A} &\rightarrow \lim_{\leftarrow n} A/\mathfrak{m}^n \\ \psi(a = \sum_{i=0}^{\infty} a_n \pi^n) &\mapsto (s_1 \pmod{\mathfrak{m}}, \cdots, s_n \pmod{\mathfrak{m}^n}, \cdots). \end{aligned}$$

Proposition 3.2.14. *ψ is an isomorphism of topological rings. Here $\hat{A}$ is endowed with the topology induced by the valuation and the projective limit is endowed with the topology induced by the product topology of $\prod_n A/\mathfrak{m}^n$ where the finite rings $A/\mathfrak{m}^n$ are endowed with the discrete topology. Taking units yields the isomorphism:*

$$(\hat{A})^* \cong (\lim_{\leftarrow n} A/\mathfrak{m}^n)^* \cong \lim_{\leftarrow n} (A/\mathfrak{m}^n)^* \cong \lim_{\leftarrow n} A^*/U_n.$$

Proof. See [18, p 128]. □

This proposition 3.2.14 is a special case of the more general notion of $\mathfrak{m}$-*adic completion*. See [2], [4] or [6] for the details on this notion. One important advantage of using projective limits is that arithmetic in $\lim_{\leftarrow i} A/\mathfrak{m}^i$ is easier as it comes down to arithmetic modulo $\mathfrak{m}^i$ for all $i \geq 1$.

We shall now turn to the task of finding roots of polynomials over a discrete valued field. We divert briefly to the similar problem in $\mathbb{R}$ because the notion that follows is similar to what we know for $\mathbb{R}$. Let $f(X)$ be a

polynomial of $\mathbb{R}[X]$. We ask for a real root of f if it exists. As finding a root is a hard exercise, one is often satisfied with an approximation to such a root. One has at hand Newton's method for this problem. Newton's method relies on the sequence of real numbers $\{x_n\}_{n\in\mathbb{N}}$ where $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, with f' the derivative of f and $f'(x_n) \neq 0$ for each $n \in \mathbb{N}$. It easy to see that in the case where the Newton sequence converges in $\mathbb{R}$, then its limit is a root of f. Unfortunately, this sequence does not always converge in $\mathbb{R}$ see [12, p 166]
On the other hand, when $f(X)$ is a polynomial in $\mathbb{Z}_p[X]$, we saw that from a simple root α of f modulo p, we can lift it to a root of f in $\mathbb{Z}_p$. We take α as first approximation of the root and form the Newton sequence $\{x_n\}$ with $x_0 = \alpha$, it will necessarily converge in $\mathbb{Z}_p$ as already seen in the proof of proposition 2.1.7. We shall give this method of lifting a root in a more general context.

Proposition 3.2.15. (Hensel's lemma: Root Form) *Let $(K, |.|)$ be a complete discrete valued field with valuation ring A and maximal ideal $\mathfrak{m}$. Let $f(X) = \sum_{i=0}^{m} a_m X^m \in A[X]$ and suppose that there is $\alpha_0 \in A$ such that $|f(\alpha_0)| < |f'(\alpha_0)^2|$. The following holds:*

1. *There exists an $\alpha \in A$ with $f(\alpha) = 0$ and $|\alpha - \alpha_0| < 1$.*
2. *Furthermore if $|f'(\alpha_0)| = 1$, then such an α is unique.*

Proof. 1. For $n \geq 0$, consider Newton's sequence $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$. Introduce also, the sequence of positive real numbers $u_n = |\frac{f(\alpha_n)}{f'(\alpha_n)}|$. Firstly for $n \geq 0$, we have $|f(\alpha_n)| < |f'(\alpha_n)^2|$. Indeed, this is true for $n = 0$, by assumption, suppose then that $|f(\alpha_n)| < |f'(\alpha_n)^2|$. By Taylor's expansion theorem we have $f(\alpha_{n+1}) = f(\alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}) = f(\alpha_n) - \frac{f(\alpha_n)}{f'(\alpha_n)} f'(\alpha_n) + \frac{f(\alpha_n)^2}{f'(\alpha_n)^2} \frac{f''(\alpha_n)}{2!} + \cdots + (-1)^m \frac{f(\alpha_n)^m}{f'(\alpha_n)^m} \frac{f^{(m)}(\alpha_n)}{m!} = f(\alpha_n)h_n$ where $h_n \in A$. Hence $|f(\alpha_{n+1})| \leq |f(\alpha_n)|$. Also by Taylor's theorem we have $f'(\alpha_{n+1}) = f'(\alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}) = f'(\alpha_n) - \frac{f(\alpha_n)}{f'(\alpha_n)} f''(\alpha_n) + \cdots + (-1)^{m-1} \frac{f(\alpha_n)^{m-1}}{f'(\alpha_n)^{m-1}} \frac{f^{(m)}(\alpha_n)}{(m-1)!} = f'(\alpha_n)(\frac{1}{f'(\alpha_n)} + h'_n)$, with $h'_n \in A$. Thus we have $|f'(\alpha_{n+1})| \geq |f'(\alpha_n)|$. So, we obtain that $|\frac{f(\alpha_{n+1})}{f'(\alpha_{n+1})^2}| \leq |\frac{f(\alpha_n)}{f'(\alpha_n)^2}| < 1$. We deduce at the same time that the sequence α_n is well defined that is to say $f'(\alpha_n) \neq 0$ for $n \geq 0$ and also that the sequence u_n is a decreasing sequence which is bounded below by zero and so u_n converges. Therefore, $\{\alpha_n\}$ is a Cauchy sequence in the complete valuation ring A, so it converges say to $\alpha \in A$ and we have $f(\alpha) = 0$. Next for $n \geq 1$, write $\alpha_n = \alpha_0 - (\frac{f(\alpha_0)}{f'(\alpha_0)} + \cdots + \frac{f(\alpha_n)}{f'(\alpha_n)})$. Hence $|\alpha_n - \alpha_0| \leq |\frac{f(\alpha_0)}{f'(\alpha_0)}| < 1$ for all $n \geq 1$. Taking limit as $n \to \infty$ we get $|\alpha - \alpha_0| < 1$

2. Now suppose that there is $\beta \in A$ such that $f(\beta) = 0$ and $|\beta - \alpha_0| < 1$ [1] . By Taylor's theorem we have:
$0 = f(\alpha_0 + \alpha - \alpha_0) = f(\alpha_0) + \frac{(\alpha-\alpha_0)f'(\alpha_0)}{1!} + \cdots + \frac{(\alpha-\alpha_0)^m f^{(m)}(\alpha_0)}{m!}$
$0 = f(\alpha_0 + \beta - \alpha_0) = f(\alpha_0) + \frac{(\beta-\alpha_0)f'(\alpha_0)}{1!} + \cdots + \frac{(\beta-\alpha_0)^m f^{(m)}(\alpha_0)}{m!}$. By the formula $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$, noting that $\alpha - \alpha_0,\ \beta - \alpha_0 \in \mathfrak{m}$ and after subtracting the second equation from the first, we obtain the equation

$$(\alpha - \beta)(f'(\alpha_0) + \omega) = 0$$

with $\omega \in \mathfrak{m}$. Since $f'(\alpha_0)$ is a unit, we deduce that we must have $\alpha = \beta$.

□

As a corollary we have

Corollary 3.2.16. *Let $f(X) \in A[X]$ and suppose that f has a simple root $\bar{\lambda}$ modulo $\mathfrak{m}$. Then, f has a root $\alpha \in A$ with $\bar{\alpha} = \bar{\lambda}$.*

Proof. Let α_0 be a lift of $\bar{\lambda}$ in A. As $\bar{\lambda}$ is a simple root of $\bar{f}$ we have $f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{m}}$. Hence $|f'(\alpha_0)| = 1$ and $|f(\alpha_0)| < |f'(\alpha_0)^2| = 1$. □

Remark 3.2.17. *In fact proposition 3.2.15 and corollary 3.2.16 are equivalent. These are two of the various equivalent formulations of Hensel's lemma to be found in the literature. One other formulation of Hensel's lemma that we shall see in the sequel is the uniqueness of an extension of a non-archimedean absolute value on K to any of its algebraic extensions, for more details see [14].*

Keeping the same notation as in proposition 3.2.15, suppose in addition that K has finite residue field with $q = card(k)$. Then the polynomial $X^q - X$ has $q-1$ non-zero simple roots in k and hence by Hensel's lemma it has $q-1$ distinct roots in A. Therefore A contains the $(q-1)$-th roots of unity and so A contains a primitive $(q-1)$-th root of unity as any finite subgroup of $(K^*, .)$ is cyclic. In particular $\mathbb{Z}_p$ contains a primitive $(p-1)$-th root of unity. Thus we have proved

Proposition 3.2.18. *If the discrete valuation ring A has finite residue field with q elements then A contains a primitive $(q-1)$-th root of unity.*

Keeping the same assumption as in the above proposition 3.2.18, let π be a prime in A and let K be the field of fractions of A. Let ζ be a primitive $(q-1)$-th root of unity. Consider the set $R := < \zeta > \cup \{0\}$. Then R is a set of

[1] Once we know that the absolute value on K can be extended on any algebraic extension of K, then we don't need to impose $\beta \in A$. The same argument holds for β lying in an algebraic extension of K.

representatives for $A/\pi A$. It is closed under multiplication and each element $x \in K^*$ can be written as $x = \sum_{n \geq n_0}^{\infty} \omega_n \pi^n$ with $\omega_n \in R$ from the expansion theorem. The set R is called the set of the *Teichmüller representatives*.

Chapter 4

Algebraic extensions of complete valued fields

In this chapter, we start with the question of extending an absolute value to an algebraic extension of a complete valued field. Then, we will define and focus on the main object of this thesis, *local fields* by giving an account of their Galois and ramification theory. The last section is concerned with the *norm group* of a local field. The content for this chapter is inspired from [18], [1], [23] or [8].

4.1 Extending absolute values

Let K be a complete field with absolute value $|\,.\,|_K$. Here we are concerned with the problem of extending the absolute value $|\,.\,|_K$ of K to an algebraic extension E/K. As an infinite algebraic extension is the union of its finite algebraic subextensions, we first restrict to finite extensions. So, we assume that E/K is finite. The case where $|\,.\,|_K$ is archimedean, is handled as follows. $\mathbb{C}$ is algebraically closed, so the algebraic extensions of $\mathbb{R}$ are $\mathbb{C}$ or $\mathbb{R}$. So, by Ostrowsky's theorem 3.2.8, p 25, we are done.
We now suppose that the absolute value $|\,.\,|_K$ is non-archimedean and discrete. By the following remark we can assume the finite algebraic extension E/K to be separable.

Remark 4.1.1. *We have to worry about separability only in characteristic p when E/K is purely inseparable. Then $[E : K] = q$, a power of p, and $\forall\, x \in E, x^q \in K$. Hence the rule $|\,x\,|_E = (|\,x^q\,|_K)^{\frac{1}{q}}$ defines the extension of $|\,.\,|_K$.*

So, our finite algebraic extensions E/K are assumed to be separable unless otherwise stated. We assume in addition that K has finite residue field. We first remark

Remark 4.1.2. *Let A be the valuation ring of K and $\mathfrak{m}$ its maximal ideal. Then, the quotients $A/\mathfrak{m}^n$ for $n \geq 2$ are finite because of the finiteness of the residue field $A/\mathfrak{m}$. Indeed, let $\pi \in A$ be a prime and let R be a set of representatives for $A/\mathfrak{m}$ in A. Then for $n \geq 2$, each $\alpha \in A$ can be uniquely written as $\alpha = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}$ with $a_i \in R$. Therefore we have a bijection $A/\mathfrak{m}^n \to (A/\mathfrak{m})^n$ and so $A/\mathfrak{m}^n$ is finite with cardinal q^n where q is the cardinal of $A/\mathfrak{m}$.*

Then for the ground field K, we have

Proposition 4.1.3. *Let K be a complete discrete valued field with finite residue field, valuation ring A and maximal ideal $\mathfrak{m}$. Then*

(a). A is compact;

(b). K is locally compact.

Proof. The local compactness of K is a consequence of the compactness of A since for each $\alpha \in K$, $\alpha + A$ will be a compact neighborhood of α. From the homeomorphism $A \cong \lim_{\leftarrow n} A/\mathfrak{m}^n$, we have that A is compact since $\lim_{\leftarrow n} A/\mathfrak{m}^n$ is closed in the compact space $\prod_{n=1}^{\infty} A/\mathfrak{m}^n$ (product of finite rings, hence compact spaces), so it is also compact. □

We shall show that there exists an extension of $|\,.\,|_K$ to E and it is unique. Suppose that we have a unique extension $|\,.\,|_E$ of $|\,.\,|_K$, and assume that E/K is Galois. Then for $\sigma \in Gal(E/K)$, $|\,.\,|_\sigma = |\,.\,|_E$ and hence we have the formula $|\,x\,|_E = |\,N_{E/K}(x)|_K^{\frac{1}{n}}$ with $[E : K] = n$. This means that if a unique extension of $|\,.\,|_K$ to E exists, then it is defined by this formula. We are left to show now that $|\,x\,|_E = |\,N_{E/K}(x)\,|_K^{\frac{1}{n}}$ is indeed the unique extension of $|\,.\,|_K$ to E.

Theorem 4.1.4. *With the above notations, then $|\,x\,|_E = |\,N_{E/K}(x)\,|_K^{\frac{1}{n}}$ is the unique absolute value on E extending $|\,.\,|_K$.*

Proof. We first check that this is an absolute value. For $x, y \in E$, $|\,xy\,|_E = |\,x\,|_E|\,y\,|_E$ from the definition and $|\,x\,|_E = 0 \Leftrightarrow x = 0$ similarly. Now, we have to verify that $|\,.\,|_E$ satisfies the ultrametric inequality $|\,x + y\,|_E \leq \max\{|\,x\,|_E, |\,y\,|_E\}$ or equivalently that $|\,\gamma + 1\,|_E \leq 1$ if $|\,\gamma\,|_E \leq 1$. So, let $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_o$ be the minimal polynomial of γ over K. Consider the extension $K(\gamma)/K$. From $N_{E/K}(x) = N_{K(\gamma)/K}(N_{E/K(\gamma)}(x))$, one has $N_{E/K}(\gamma) = (N_{K(\gamma)/K}(\gamma))^{[E:K(\gamma)]}$. Therefore $|\,N_{E/K}(\gamma)\,|_K \leq 1 \Leftrightarrow |\,N_{K(\gamma)/K}(\gamma)|_K \leq 1$. So, it comes down to showing the inequality for $K(\gamma)/K$. To this end, the minimal polynomial of $\gamma+1$ is then $g(X) = f(X-1)$ so that $N_{E/K}(\gamma+1) = \pm g(0) = \pm((-1)^d + a_{d-1}(-1)^{d-1} + \cdots + a_1(-1) + a_0)$. We need the implication $|\,a_0\,|_K = |\,N_{K(\gamma)/K}(\gamma)\,|_K \leq 1 \Rightarrow |\,(-1)^d + a_{d-1}(-1)^{d-1} + \cdots + a_1(-1) + a_0\,|_K = |\,N_{K(\gamma)/K}(\gamma + 1)\,|_K \leq 1$ to hold. This is a consequence of

the lemma 4.1.5 below, a corollary of Hensel's lemma.
For the uniqueness part, let A be the valuation ring of K and let $\mathcal{O}$ be the integral closure of A in E. Then $\mathcal{O}$ is the valuation ring for $|\,.\,|_E$. Indeed by definition of the integral closure any $a \in \mathcal{O}$ satisfies $N_{E/K}(a) \in A$. On the other hand if $x \in E$ has minimal polynomial $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ over K, then $N_{E/K}(x) = \pm a_0^{[E:K(x)]}$. So, if $N_{E/K}(x) \in A$ then so is a_0. By lemma 4.1.5 we obtain $f(X) \in A[X]$. This shows $\mathcal{O} = \{x \in E : N_{E/K}(x) \in A\} = \{x \in E : |\,x\,|_E \leq 1\}$. Now suppose $|\,.\,|'$ is another absolute value on E extending $|\,.\,|_K$ and let $\mathcal{O}'$ be its valuation ring, we next show that $\mathcal{O} \subset \mathcal{O}'$ as this implies that $|.| = |.|'$. Indeed the inclusion $\mathcal{O} \subset \mathcal{O}'$ is equivalent to the statement $|x| \leq 1 \Leftrightarrow |x|' \leq 1$ and so their equivalence as absolute values. Since they have the same restriction on K, one deduces that $|.| = |.|'$. So, to see the inclusion $\mathcal{O} \subset \mathcal{O}'$ suppose that there exists $x \in \mathcal{O} \smallsetminus \mathcal{O}'$. As x is integral over A, there exist $a_0, \cdots, a_{n-1} \in A$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Also $x \notin \mathcal{O}'$, so $x^{-1} \in \mathfrak{m}'$, the maximal ideal of $\mathcal{O}'$. Therefore, $1 + a_{n-1}x^{-1} + \cdots + a_0(x^{-1})^n = 0$, which gives the contradiction $1 \in \mathfrak{m}'$. Thus, we must have $\mathcal{O} \subset \mathcal{O}'$. □

Lemma 4.1.5. *Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, be an irreducible polynomial in $K[X]$. Then $|\,a_n + a_{n-1} + \cdots + a_1 + a_0\,|_K = max\{|\,a_n\,|_K, \ |\,a_0\,|_K\}$.*

Proof. By contradiction suppose the statement is false and let a_r be the first from $a_1, \cdots, a_{n-1}$ with $|\,a_r\,|_K = max\{|\,a_1\,|_K, \cdots, |a_{n-1}|_K\}$. Then $a_r^{-1}f(X) \in A[X]$. Let $u \in A^*$ be any unit and set $g(X) = a_r^{-1}f(X) - uX$. Then $g(X) \equiv X(a_na_r^{-1}X^{n-1} + \cdots - u) \pmod{\mathfrak{m}}$ so that 0 is simple root of $g(X)$ modulo $\mathfrak{m}$ and hence by corollary 3.2.15, p 29, there are $\alpha \in \mathfrak{m}$, $h(X) \in A[X]$ such that $g(X) = (X - \alpha)h(X)$. Hence, $a_r^{-1}f(X) = (X - \alpha)h(X) + uX$. We then obtain $a_r^{-1}f'(X) = h(X) + (X - \alpha)h'(X) + u$. Note that the constant term of $h(X)$ is $b_0 := a_r^{-1}a_0\alpha^{-1}$, so we have finitely many possibilities for b_0. If b_0 is not a unit, then $a_r^{-1}f'(0) = b_0 + (-\alpha)h'(0) + u$ is unit. Hence by proposition 3.2.15, p 29, we see that $a_r^{-1}f(X)$ is has a zero in A contradicting the fact that $f(X)$ is irreducible. Next if b_0 is a unit we choose u such that $b_0 + u$ is a unit and we apply proposition 3.2.16 to deduce that $f(X)$ would be reducible. So, in all cases we obtain a contradiction and this completes the proof of the lemma. □

Remark 4.1.6. *From the definition of $|\,.\,|_E$, we see that if $|\,.\,|_K$ has associated valuation v, then v has as unique extension w given by the formula $w(x) = \frac{1}{[E:K]}v(N_{E/K}(x))$, for each $x \in E$, and w is also discrete.*

Continuing this discussion we shall next see that the field E is complete with respect to $|\,.\,|_E$. In fact, we shall prove the completeness of E from local compactness of E. In the archimedean case we know already that the finite algebraic extensions are complete, so we assume that the absolute values are

discrete as usual. Let B be the discrete valuation ring of E which is also the integral closure of A in E as saw in the proof of theorem 4.1.4, p 34. Since the extension E/K is finite of degree $n = [E : K]$, B is a free A-module of rank n, see [18, p 12] for the details.

Proposition 4.1.7. *Let E/K be a finite extension of discrete valued fields with $|\,.\,|_E$ the unique absolute value on E extending $|\,.\,|_K$ and K complete. Let B, A be the valuation rings of E, K respectively. Then E is locally compact which implies that it is complete.*

Proof. **Local compactness:** Similarly as in proposition 4.1.3, local compactness of E follows from the compactness of B. To see that B is compact, fix a basis $\beta_1, \cdots, \beta_n$ of B over A. Define the map:

$$\begin{aligned} \psi : A^n &\rightarrow B \\ \psi((\alpha_1, \cdots, \alpha_n)) &= \alpha_1\beta_1 + \cdots + \alpha_n\beta_n \end{aligned}$$

A^n endowed with the norm $|\,(\alpha_1, \cdots, \alpha_n)\,| := max\{|\,\alpha_1\,|_K, \cdots, |\,\alpha_n|_K\,\}$ becomes a topological space. It's in fact the product topology on A^n. Next B is endowed with the topology induced by the absolute value of B extending that of A. Then, ψ is continuous and bijective. Hence B is compact as the image of the compact space A^n under ψ. Therefore, E is locally compact.
Completeness : Recall that for $r \in \mathbb{R}_{>0}$, the sets $V_r = \{x \in E : |\,x\,|_E < r\}$ form a fundamental system of neighborhoods of zero in E. Let $\{x_n\}$ be a Cauchy sequence in E. Then we know that it is bounded, that is there exists $M \in \mathbb{R}_{>0}$ such that $|\,x_n\,| \leq M$ for all $n \in \mathbb{N}$. Consider the subset $S = \{x \in E : |\,x\,|_E \leq M\}$. By the local compactness of E, there exists $C_r = \{x \in E : |\,x\,|_E \leq r\}$, a compact neighborhood of zero.Therefore by choosing $\alpha \in E^*$ with $|\,\alpha\,|_E \geq r^{-1}M$, we see that S is contained in the compact set αC_r. Thus $\{x_n\}$ is a Cauchy sequence inside a compact subspace, so x_n converges. □

Remark 4.1.8. *Commonly, the completeness of a finite extension E/K of a complete field K is deduced from a general result on normed vector spaces over complete fields: Let V be a finite dimensional vector space over a complete field K; it is a theorem that all the norms on V are equivalent to the sup-norm, see [18, p 132] for the details.*

We now turn to a converse of proposition 4.1.3. Let us first define the main object of study in this thesis.

Definition 4.1.9. A *local field* is a complete discrete valued field with finite residue field.

Example 4.1.10. *1. The p-adic field $\mathbb{Q}_p$ is the prototype of a local field of characteristic zero.*

2. *More general than $\mathbb{Q}_p$, the completion of a number field K at a prime ideal $\mathfrak{p}$, $K_\mathfrak{p}$, is a local field.*

3. *The field of formal Laurent series $\mathbb{F}_q((X))$ in the variable X over a finite field $\mathbb{F}_q$, is a local field of positive characteristic.*

Soon, we will see that the local fields are exactly the finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_q((X))$. To this end, we will need the following result, which gives a topological criterion for a field to be local.

Theorem 4.1.11. *Let K be a field with a valuation v, not necessarily discrete. Then K is locally compact if and only if the following hold:*

1. *K is complete;*

2. *the valuation ring A is compact and the residue field is finite;*

3. *v is a discrete valuation.*

Proof. We have proved in proposition 4.1.3 that the enumerated properties imply that K is locally compact.
For the converse let K be locally compact. We have showed in proposition 4.1.7 that K is complete. By local compactness, there exists W a compact neighborhood of zero. Hence, there exists $\alpha \in K$ such that $\alpha A \subset W$. Since A is closed, αA is closed in the compact subset W, so it is compact. We deduce that A is compact. As each ideal $\mathfrak{a}$ of A is at the same time open and closed, the quotient topology on the ring $A/\mathfrak{a}$ is the discrete topology. This, with the compactness of A implies that $A/\mathfrak{a}$ is compact and discrete, hence finite. In particular, the residue field $A/\mathfrak{m}$ is a finite field. For $\alpha \in A$, the ring $A/\alpha A$ is finite, this means that there are only a finite number of ideals of A that contain α. So the set $P_{v(\alpha)} = \{v(x) : x \in A,\ 0 < v(x) < v(\alpha)\}$ must be finite. Otherwise, we would have infinitely many xA with $A \supsetneq xA \supsetneq \alpha A$. Therefore, $P_{v(\alpha)}$ has a least element, say λ. Choose $\pi \in A$ with $v(\pi) = \lambda$. For each $x \in A$ with $v(x) > 0$, we obtain $v(\pi) \leq v(x)$, so that $v(\pi) = \lambda$ is the least element in the set $\{v(x) > 0 : x \in A\}$. Now, let $m \in \mathbb{N}$ be the greatest integer such that $mv(\pi) \in P_{v(\alpha)}$. Then $m\lambda < v(\alpha) < (m+1)\lambda$, which gives $0 < v(\alpha) - m\lambda < \lambda$. Therefore, by the definition of λ, we must have $v(\alpha) = m\lambda$. And hence $v(K^*) = \lambda\mathbb{Z}$. □

From now on, unless otherwise stated, all fields are local. Next we define some invariants for an extension of local fields E/K. From the inclusion $E^* \supset K^*$, we get that $v_K(K^*)$ is a subgroup of $v_E(E^*)$ where v_E is the unique valuation extending v_K. As $v_E(E^*)$ is discrete, the index $(v_E(E^*) : v_K(K^*))$ is finite as nontrivial subgroups of $\mathbb{Z}$ have finite index. Define $e(E/K)$ to be the index $(v_E(E^*) : v_K(K^*))$. Also, the residue fields are finite so $[k_E : k_K]$ is finite. Set $f(E/K) = [k_E : k_K]$. So $e(E/K)$ and $f(E/K)$ are finite for any extension E/K of local fields.

Definition 4.1.12. $e(E/K)$ is called the *ramification index* of the extension E/K. $f(E/K)$ is the *residue degree* of the extension E/K.

Remark 4.1.13. *If we fix prime elements π_K, π_E of K, E respectively, then $e = e(E/K)$ is the integer such that $\pi_K B = \pi_E^e B$.*

Lemma 4.1.14. *For an intermediate field $K \subseteq F \subseteq E$ one has*

$$f(E/K) = f(E/F)f(F/K), \;\; e(E/K) = e(E/F)e(F/K).$$

Proof. These relations follows from the definition. □

Given an extension E/K of local fields, let A, B, be the valuation rings of K, E respectively. The expansion theorem 3.2.13, p 27, allows one to find an explicit integral basis for B over A. Then it follows that any extension E/K of local fields is finite since a basis for B over A is also a basis for E over K.

Proposition 4.1.15. *Let E/K be an extension of local fields. We write $f = f(E/K), \; e = e(E/K)$. Take $u_1, \cdots, \; u_f \in B$ such that their reductions modulo $\mathfrak{m}_E$ is a basis for k_E over k_K. Fix a prime element $\pi_E \in B$. Then, the elements $\pi_E^j u_i, \; 0 \leq j \leq e-1, \; 1 \leq i \leq f$, form an integral basis for B over A, so that $ef = [E : K]$.*

Proof. For $n \geq 0$, write $n = qe + s$ with $0 \leq s < e$ and set $\pi_n = \pi_K^q \pi_E^s$. Then $v_E(\pi_n) = qe + s = n$. Let also R_A be a set of representatives for k_K in A. The set $R_B = R_A u_1 + \cdots + R_A u_f$ is a set of representatives for k_E in B. Indeed, $card(R_B) = (card(k_K))^f$ and each element in B is congruent modulo $\mathfrak{m}_E$ to some $\beta \in R_B$. Therefore by the expansion theorem, for $\beta \in B$ we have

$$\begin{aligned} \beta &= \sum_{q=0}^{\infty} \sum_{s=0}^{e-1} \pi_K^q \pi_E^s (\sum_{i=0}^{f} r_{q,r,i} u_i), \text{ with } r_{q,s,i} \in R_A \\ &= \sum_{i=1}^{f} \sum_{s=0}^{e-1} \pi_E^s u_i \sum_{q=0}^{\infty} \pi_K^q r_{q,s,i}. \end{aligned}$$

Each $\sum_{q=0}^{\infty} \pi_K^q r_{q,s,i} \in A$, so B is finitely generated as an A-module. Hence E/K is a finite extension. But A is a principal ideal domain and B is the integral closure of A in E. So we know that B is a free A-module of rank $n = [E : K]$. Also $B/\pi_K B \cong B/\pi_E^e B$ so that $card(B/\pi_K B) = (card(k_K))^{ef}$. Therefore, one has $ef = n$. It follows that $\pi_E^j u_i$ with $j = 0, \cdots, e-1, \; i = 1, \cdots, f$, form an integral basis for B over A. This completes the proof of the proposition. □

We can now give the characterization theorem for local fields.

Theorem 4.1.16. *A local field is a finite extension either of $\mathbb{Q}_p$ or of the field of formal Laurent series $\mathbb{F}_p((X))$.*

Proof. It is clear that $\mathbb{Q}_p$ and $\mathbb{F}_p((X))$ are local fields. From theorem 4.1.11 any finite extension K of one of the local fields $\mathbb{Q}_p$ or $\mathbb{F}_q((X))$ is a local field.

Conversely, let K be a local field. If K is of characteristic zero, then K contains the prime field $\mathbb{Q}$. Let p be the characteristic of the residue field $A/\mathfrak{m}_K$, where A is the valuation ring of K, and $\mathfrak{m}_K$ its maximal ideal, then we have $p \in \mathfrak{m}_A$. Therefore the restriction of the valuation v of K to $\mathbb{Q}$ is equivalent to the p-adic valuation v_p, hence the closure of $\mathbb{Q}$ in K is $\mathbb{Q}_p$. Thus we have an extension $K/\mathbb{Q}_p$ of local fields. From proposition 4.1.15, $K/\mathbb{Q}_p$ is finite [1] . Now, if K is of positive characteristic p, then p is also the characteristic of its residue field $k_K = \mathbb{F}_q$ ($p = 0$ in $K \Rightarrow p = 0$ in k_K), with $q = p^f, f = [\mathbb{F}_q : \mathbb{F}_p]$. Then $K \cong \mathbb{F}_q((X)) \supset \mathbb{F}_p((X))$. Indeed, let $R = \{\zeta_{q-1}^n : n \in \mathbb{Z}\} \bigcup \{0\} = \{\text{roots of } X^q - X\}$ be the set of the Teichmüller representatives of $k_K = \mathbb{F}_q$ in A, see p 30. But also we have $\mathbb{F}_q \cong \{\text{roots of } X^q - X\}$ in A. Therefore, $R \cong \mathbb{F}_q$. Fixing a prime $\pi \in K$ and using the expansion theorem, we see that K is isomorphic to $\mathbb{F}_q((X))$ with $\pi \leftrightarrow X$. So, K is a finite extension of $\mathbb{F}_p((X))$. □

We shall now turn to the study of Galois extensions of local fields.

4.2 Galois theory and the norm group of local fields.

In this section we gather the basic facts concerning ramification theory for local fields. We introduce the *higher ramification groups* for a Galois extension of local fields and finish with the basic facts about the norm group of a local field.

4.2.1 Ramification in an extension of a local field.

Let E/K be a finite extension of local fields.

Definition 4.2.1.

1. If $e = e(E/K) = 1$, the extension E/K is said to be *unramified.* We then have $f = [k_E : k_K] = [E : K]$ and $\pi_K = \pi_E u$ with $u \in A_E^*$.
2. If $e = [E : K]$ so that $f = [k_E : k_K] = 1$, we say that the extension E/K is *totally ramified.*
3. If the characteristic of the residue field is $p > 0$ and does not divide the ramification index e, then, the extension E/K is said to be *tamely*

[1] The fact that $[K : \mathbb{Q}_p]$ is finite is a general property of locally compact topological vector spaces, theorem 3 in [3, p TVS I.15].

ramified. We see immediately that an unramified extension is tamely ramified and a totally ramified extension may not be tamely ramified.

4. An extension which is not tamely ramified is said to be *wildly ramified.*

Remark 4.2.2. *An extension E/K of local fields is unramified if and only if a prime $\pi_K \in K$ is also prime in E.*

For an extension E/K of local fields, let π_E, π_K be primes of E, K respectively. From $\pi_K = \pi_E^e u$ where $u \in A_E^*$, we obtain $\pi_K^{[E:K]} = N_{E/K}(\pi_K) = (N_{E/K}(\pi_E))^e N_{E/K}(u)$. Therefore after normalizing v_K, we have $ef = ev_K(N_{E/K}(\pi_E))$. From $f = v_K(N_{E/K}(\pi_E))$ we deduce that E/K is totally ramified if and only if the norm of a prime in E is prime in K.

An infinite algebraic extension E/K of valued fields is in one of the classes 1-4 above if all its finite subextensions are.

Proposition 4.2.3. *Let E/K be a finite extension of local fields. Then $A_E = A_K[\alpha]$ with some $\alpha \in A_E$.*

Proof. Since k_E/k_K is separable and finite, $k_E = k_K[\beta]$, for some $\beta \in k_E$. Let $f(X) \in k_K[X]$ be the minimal polynomial of β over k_K. Let $g(X) \in A_K[X]$ be monic such that its reduction modulo $\mathfrak{m}_K$ is $f(X)$. As β is a simple root of $g(X)$ modulo $\mathfrak{m}_K$, by Hensel's lemma there exists $\alpha \in A_E$ with $\bar{\alpha} = \beta$ in k_E and $g(\alpha) = 0$. Let $\alpha_1 = \alpha + a\pi_E$ with $a \in A_E$ and π_E a prime of A_E. We have $g(\alpha_1) \equiv g(\alpha) + a\pi_E g'(\alpha) \pmod{\pi_E^2}$. As $g'(\alpha) \neq 0$ modulo $\mathfrak{m}_E$, we see that we cannot have both $g(\alpha_1),\ g(\alpha) \equiv 0 \pmod{\pi_E^2}$. Hence by renaming if necessary, we can assume that $g(\alpha)$ is a prime element of A_E. Hence from proposition 4.1.15, $\alpha^i g(\alpha)^j$ with $0 \leq i \leq f-1,\ 0 \leq j \leq e-1$, is an A_K basis for A_E. □

Unramified extensions:

Let (K, v) be a complete discrete valued field with k_K as residue field. Then we have

Theorem 4.2.4. *1. For each positive integer n there exists a field extension F/K with $[F : K] = n = f(F/K),\ e(F/K) = 1$.*

2. Such an extension F is unique inside an algebraic closure $\bar{K}$ of K.

Proof. **Existence:** Let F be the splitting field of $X^{q^n-1} - 1$ over K. Let ζ be a primitive $(q^n - 1)$-th root unity and let $f(X)$ be the minimal polynomial of ζ over K. $f(X)$ is a factor of $X^{q^n-1} - 1$ and $\bar{f}(X)$ is irreducible over $k_K[X]$ since otherwise Hensel's lemma will show that $f(X)$ is not irreducible. We obtain $[F : K] = deg(f) = deg(\bar{f}) \leq [k_F : k_K] \leq [F : K]$, so F/K is unramified.

Uniqueness: Let $n = [E : K]$. $e(E/K) = 1$ so that $[k_E : k_K] = n$. Write $k_K = \mathbb{F}_q$, $k_E = \mathbb{F}_{q^n}$. $\mathbb{F}_{q^n}$ is the splitting field of $X^{q^n-1} - 1$. By Hensel's lemma, there exists $\zeta \in E$ a primitive $(q^n - 1)$-th root of unity. Then $K \subset K(\zeta) \subset E$. Hence $k_{K(\zeta)} = k_E$. Therefore $[K(\zeta) : K] \geq [k_E : k_K] = [E : K]$ and thus $E = K(\zeta)$. □

Corollary 4.2.5. *Let E/K be a finite extension of local fields. Then there exists a unique subextension L/K such that L/K is unramified and E/L is totally ramified.*

Proof. Let $f = f(E/K)$. We take L as the unique unramified extension of K of degree f. □

Definition 4.2.6. This maximal unramified extension L/K is called the *inertia field* of the finite extension E/K.

Corollary 4.2.7. *Let E'/K and L/K be algebraic extensions of a local field K. Let $E = E'L$. Then if L/K is unramified so is E/E'. The composite of unramified extensions of a local field K is also unramified. Furthermore, the subextensions of an unramified E/K are unramified.*

Proof. Without loss of generality, we can assume all extensions finite. We have to check that $[E : E'] = [k_E : k_{E'}]$. As the extension L/K is unramified, we know that $L = K(\alpha)$ with α such that its reduction generates k_L. We thus obtain $E = E'K(\alpha) = E'(\alpha)$. So, let $h(X) \in A_{E'}[X]$ be the minimal polynomial of α over $A_{E'}$. Let $l(X) \in k_{E'}[X]$ be the minimal polynomial of the reduction of α over $k_{E'}$. We have $deg(h) = deg(l)$. Indeed, any root of $h(X)$ reduces to a root of $l(X)$ and since $l(X)$ is separable, it follows that two distinct roots of $h(X)$ reduces to two distinct roots of $l(X)$. Therefore we have

$$[k_E : k_{E'}] \leq [E : E'] = deg(h) = deg(l) \leq [k_E : k_{E'(\alpha)}] \leq [k_E : k_{E'}].$$

This means $[E : E'] = [k_E : k_{E'}]$ and hence E/E' is unramified.
Let now L/K, L'/K, be unramified and put $T = LL'$. Then T/L' is unramified, and from $e(T/K) = e(T/L')e(L'/K)$, we deduce that T/K is unramified. Next let L/K be an subextension of an unramified extension E/K. From $1 = e(E/K) = e(E/L)e(L/K)$, we see that $e(L/K) = 1$, i.e., L/K is unramified. □

From the above we see that the union of all the unramified extensions of a local field K inside an algebraic closure $\bar{K}$ of a K is a field. It is denoted by K^{ur} and by construction it is the *maximal unramified extension* of K. It is a natural object to consider as it allows one to handle the finite unramified extensions of K at once. From its definition we see that K^{ur} is not a local field as it is of infinite degree over K. Furthermore it fails to be complete

with respect to the unique discrete valuation extending v_K, the valuation of K. Nonetheless, the Hensel's lemma does hold. This is an example of what is called a *Henselian field*. For an introduction to the theory of Henselian fields, consult [18], [10], or [9].

Totally and wildly ramified extensions:

Let E/K be a totally ramified extension of local fields. We know from proposition 4.1.15, that $A_E = A_K[\pi_E]$ with π_E a prime element of A_E. Now $[E : K] = e = e(E/K)$. The minimal polynomial of π_E over K is say $P(X) = X^e + a_{e-1}X^{e-1} + \cdots + a_0$ with $a_i \in A_K$. Since the extension E/K is totally ramified, $v_K(N_{E/K}(\pi_E)) = v_K(\pm a_o) = f(E/K) = 1$, that is a_0 is a prime in A_K. From lemma 4.1.5, p 35 we deduce that all $a_i \in \mathfrak{m}_K$. Such a polynomial is known as an *Eisenstein polynomial.*
Conversely let π be a root of an Eisenstein polynomial $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ over A_K with $n \geq 2$. Let v_K be the valuation on K. Consider the extension $K(\pi)$ and let w be the unique extension of v_K to $K(\pi)$. Then from the integral relation

$$\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1\pi + a_0 = 0,$$

it follows that two of the terms must have the same minimal w value. As all $v_K(a_i) > 0$, we have $w(\pi) > 0$ and $w(a_i\pi^i) > w(a_0)$ for all $i = 1, \cdots, n-1$. This is because $P(X)$ is Eisenstein. Therefore we deduce $w(\pi^n) = w(a_0)$ which is equivalent to $nw(\pi) = e$. But we know that $e \leq n$ and hence we have $w(\pi) = 1,\ e = n$. This means that $K(\pi)/K$ is totally ramified and that π is a prime in $K(\pi)$. We have proved.

Proposition 4.2.8. *A finite algebraic extension E/K of local fields is totally ramified if and only if $E = K(\pi)$ for a prime π in A_E which is a root of an Eisenstein polynomial in $A_K[X]$.*

In the case of $\mathbb{Q}_p$, a totally ramified extension is constructed as follows.

Example 4.2.9. *Let $q = p^n$ with p a prime, and ζ_q be a primitive q-th root of unity. Consider the extension $K = \mathbb{Q}_p(\zeta_q)$. Write $X^{p^n} - 1 = (X^{p^{n-1}} - 1)(X^{(p-1)p^{n-1}} + \cdots + X^{p^{n-1}} + 1)$. Then ζ_q is a root of $h(X) = X^{(p-1)p^{n-1}} + \cdots + X^{p^{n-1}} + 1$. By the change of variable $X \leftrightarrow X + 1$, we see that $h(X+1)$ is Eisenstein over $\mathbb{Z}_p$. Therefore $K/\mathbb{Q}_p$ is totally ramified with degree $(p-1)p^{n-1} = \phi(p^n)$. We also have $A_K = \mathbb{Z}_p[\zeta_q]$. Indeed $\lambda = \zeta_q - 1$ is a root of the Eisenstein polynomial $h(X+1)$, so it is a prime. Therefore we have $A_K = \mathbb{Z}_p[\lambda] = \mathbb{Z}_p[\zeta_q]$.*

Next we shall see that a totally ramified extension E/K of local fields contains a maximal tamely ramified subextension. So a ramified extension may be split into a tamely and a wildly ramified extension.

Proposition 4.2.10. *Let E/K be a totally ramified extension of local fields with p the characteristic of the residue field k_K. Let $n = [E : K] = n_0 p^k$ with $(n_0, p) = 1$. Then there exists a unique subextension T/K inside E given by $T = K(\sqrt[n]{\pi})$ for some prime $\pi \in K$ and $[T : K] = n_0$.*

Proof. **Existence:** As E/K is totally ramified, we have $\pi_E^n = u\pi_K$ with $u \in A_E^*$ and π_E, π_K prime elements from A_E, A_K respectively. Since $k_E = k_K$, there exists $v \in A_K^*$ such that $u \equiv v \pmod{\mathfrak{m}_E}$. Let $\alpha := v\frac{\pi_K}{(\pi_E^{p^k})^{n_0}}$. The polynomial $f(X) = X^{n_0} - \alpha$ has $\bar{1}$ as simple root modulo $\mathfrak{m}_E$, whence by Hensel's lemma there exists a unique $\beta \in A_E$ such that $f(\beta) = 0$ and $\beta \equiv 1 \pmod{\mathfrak{m}_E}$. Hence $\beta(\pi_E)^{p^k}$ is a root of the Eisenstein polynomial $X^{n_0} - v\pi_K \in A_K[X]$. That is the extension $T = K(\beta\pi_E^{p^k}) = K(\sqrt[n_0]{v\pi_K})/K$ is totally and tamely ramified extension of degree n_0.
Uniqueness: Suppose that we have T_1, T_2 two tamely ramified extensions of K inside E of degree n_0. By the above, we see that there exist π_1, π_2 primes of T_1 and T_2 respectively and $\pi_1^{n_0} = \pi_K$, $\pi_2^{n_0} = v\pi_K$ for some prime $\pi_K \in A_K$ and $v \in A_K^*$. Then $x = \frac{\pi_1}{\pi_2} \in A_E^*$ and $x^{n_0} \in A_K$. From $k_E = k_K$, there exists $w \in A_K^*$ such that $x \equiv w \pmod{\mathfrak{m}_E} \Leftrightarrow xw^{-1} \in 1 + \mathfrak{m}_E$, *i.e*, $|xw^{-1} - 1|_E < 1$. We first observe that xw^{-1} is a root the polynomial $f(X) := X^{n_0} - x^{n_0}w^{-n_0} \in A_K[X]$ with $|xw^{-1} - 1|_E < 1$, but also the polynomial $f(X)$ has 1 as simple root modulo $\mathfrak{m}_K$ and hence by corollary 3.2.16, it has a root $\beta \in A_K$ with $|\beta - 1|_K < 1$. Since $f'(1)$ is a unit, proposition 3.2.15 says that $xw^{-1} = \beta \in 1 + \mathfrak{m}_K$. This means that $x = \frac{\pi_1}{\pi_2} \in A_K^*$ and hence $T_1 = T_2$. □

Corollary 4.2.11. *Let T/K, T'/K be two extensions of K. Let $E = TT'$. Then one has: T/K is tamely ramified $\Rightarrow E/T'$ is a tamely ramified extension. The composite of tamely ramified extensions is also tamely ramified and any subextension of a tamely ramified extension is tamely ramified.*

Proof. We can assume the extensions to be finite. To simplify matters, we assume that T'/K is Galois and $[T : K]$ is prime to p [2] . It is clear that any subextension of a tamely ramified extension is also tamely ramified. Now T/K is tamely ramified, since $[E : T'] = [T : T \cap T']$, then E/T' is also tamely ramified. Next, let T_1, T_2 be tame ramified extensions of K. Then T_1T_2/T_2 is tamely by the preceding argument and so from $e(T_1T_2/K) = e(T_1T_2/T_2)e(T_2/K)$, we deduce that T_1T_2/K is also tamely ramified. □

As a consequence, we see that the union inside a fixed algebraic closure of all finite tamely ramified extensions of a local field K is a field. This field is denoted by K^{tame} and is of infinite degree over K^{ur}. K^{tame} is called the maximal tamely ramified extension of K. This is also a Henselian field. Having this, we next give the Galois theory of extensions of local fields.

[2]This proposition is also true without these assumptions, the reader may consult [18, pp 155-157] or [10, p 45] for a precise description of a tame extension of a local field.

4.2.2 Galois theoretical aspects for local fields.

Let $K \subset L \subset T \subset E$ be the tower of local fields with L, T being respectively the maximal unramified and the maximal tamely ramified extension of K inside E. When the extension E/K is Galois, we shall give the Galois groups corresponding to these subfields. After this we will give a brief account of the *higher ramification* subgroups inside $Gal(E/K)$.

Let E/K be Galois with Galois group $Gal(E/K)$. We know that conjugate elements have the same valuation, hence we have $\sigma(A_E) = A_E, \sigma(\mathfrak{m}_E) = \mathfrak{m}_E$. This means that any $\sigma \in Gal(E/K)$ induces an automorphism $\bar{\sigma} \in Gal(k_E/k_K)$ by $\bar{\sigma}(\bar{\alpha}) := \overline{\sigma(\alpha)}$. Hence we can define

$$\begin{aligned} \psi : Gal(E/K) &\rightarrow Gal(k_E/k_K) \\ \psi(\sigma) &= \bar{\sigma}. \end{aligned}$$

This is a group homomorphism.

Proposition 4.2.12. *Let E/K an unramified extension of local fields. Then E/K is cyclic Galois. Furthermore the homomorphism ψ is an isomorphism.*

Proof. By construction of the extension E/K, see theorem 4.2.4, E/K is cyclic Galois. We are left to prove that ψ is an isomorphism. We have $k_K = \mathbb{F}_q$ and $k_E = \mathbb{F}_{q^n}$ with $n = f(E/K) = [E : K]$. Also there is a primitive $(q^n - 1)$-th root of unity $\zeta \in E$ with $E = K(\zeta)$. Furthermore, the reduction $\bar{\zeta} \in k_E$ of ζ modulo $\mathfrak{m}_E$ is such that $\bar{\zeta}$ is a primitive $(q^n - 1)$-th root of unity in k_E. So $k_E = k_K(\bar{\zeta})$. Now for $\sigma \in Gal(E/K)$, $\psi(\sigma)(\bar{\zeta}) = \bar{\zeta} \Leftrightarrow \bar{\sigma}(\bar{\zeta}) \equiv \zeta \pmod{\mathfrak{m}_E} \Leftrightarrow \sigma(\zeta) = \zeta$. Therefore ψ is injective. Since both Galois groups have the same order $f = [k_E : k_K] = [E : K]$, ψ is an isomorphism. □

Corollary 4.2.13. *Let E/K be a finite Galois extension. Then ψ is surjective and the maximal unramified extension L/K inside E is the fixed field of $ker(\psi)$.*

Proof. We can write ψ as the composite $Gal(E/K) \rightarrow Gal(L/K) \rightarrow Gal(k_E/k_K) = Gal(k_L/k_K)$, where the first arrow is the restriction map. We obtain

$$Gal(E/K)/ker(\psi) \cong Gal(L/K).$$

Thus by Galois theory we have $Gal(E/L) = Ker(\psi)$, i.e., $L = E^{ker(\psi)}$. □

The subgroup of $Gal(E/K)$ corresponding to the inertia field is called the inertia subgroup of $Gal(E/K)$ and it is denoted by $I_{E/K} := ker\psi$. Since $k_K = \mathbb{F}_q$, $k_E = \mathbb{F}_{q^f}$ where $f = [k_E : k_K]$, $Gal(k_E/k_K)$ is a cyclic group generated by the *Frobenius k_K-automorphism*

$$\bar{\varphi} : k_E \rightarrow k_E, \bar{\varphi}(\bar{\alpha}) = (\bar{\alpha})^q.$$

By the isomorphism $Gal(L/K) \cong Gal(k_E/k_K)$, there exists a unique K-automorphism φ of L that corresponds to $\bar{\varphi}$. It generates $Gal(L/K)$ and is characterized by

$$\varphi(a) \equiv a^q \pmod{\mathfrak{m}_L}, \forall a \in A_L.$$

Definition 4.2.14. This automorphism $\varphi \in Gal(L/K)$ of an unramified extension L/K is called the *Frobenius automorphism* of L/K.

For a finite Galois extension of local fields E/K, we wish to complete the Galois correspondence

$$\begin{array}{ccc}
E & \longleftrightarrow & 1 \\
\uparrow & & \downarrow \\
T & \longleftrightarrow & Gal(E/T) =? \\
\uparrow & & \downarrow \\
L & \longleftrightarrow & Gal(E/L) = ker[Gal(E/K) \to Gal(k_E/k_K)] \\
\uparrow & & \downarrow \\
K & \longleftrightarrow & Gal(E/K)
\end{array}$$

where respectively T, L are the maximal tamely ramified and maximal unramified extensions of K inside E. Let then $e = e(E/K) = n_0 p^k = [E : L]$ with $(n_0, p) = 1$ with $n_0 = [T : L]$ and $p^k = [E : T]$. By Galois theory we see that the subgroup $Gal(E/T)$ is of order p^k inside $I_{E/K}$. Hence it is a p-Sylow subgroup of $I_{E/K}$. If there were more than one p-Sylow subgroups of $I_{E/K}$, by Galois correspondence we would have a field $T_1 \neq T$ with $[T_1 : L] = n_0$ contradicting the uniqueness of the maximal tamely ramified subextension of E/K. Therefore, there is a unique p-Sylow subgroup of $I_{E/K}$, and it is the subgroup of $Gal(E/K)$ that fixes the maximal tamely ramified extension. From the maximality of the extension T/K, inside E, one sees that it must be Galois. We would like to have a more precise description of $Gal(E/T)$, so let us carry on this discussion. Put $S = Gal(E/T) \subset I_{E/K}$.

For $\sigma \in I_{E/K}$, we obtain $\frac{\sigma(\pi)}{\pi} \in A_E^*$ for a prime $\pi \in A_E$. For another $\pi_1 = u\pi$ with $u \in A_E^*$, we have that $\frac{\sigma(\pi_1)}{\pi_1} = \frac{\sigma(u)\sigma(\pi)}{u\pi}$, and also $\frac{\sigma(u)}{u} \in 1 + \mathfrak{m}_E = U_1$. Whence $\frac{\sigma(\pi_1)}{\pi_1} \equiv \frac{\sigma(\pi)}{\pi} \pmod{U_1}$. That is the map

$$\begin{aligned}
\theta : I_{E/K} &\to A_E^*/U_1, \\
\sigma &\mapsto \frac{\sigma(\pi)}{\pi} \pmod{U_1}
\end{aligned}$$

is independent of π. On the other hand $\theta(\sigma\tau) = \frac{\sigma(\tau(\pi))}{\pi} = \frac{\sigma(\tau(\pi))\tau(\pi)}{\tau(\pi)\pi} \equiv$

$\theta(\sigma)\theta(\tau) \pmod{U_1}$, i.e., θ is a homomorphism of groups and its kernel is

$$ker(\theta) = \{\sigma \in I_{E/K} : \sigma(\pi) - \pi \in \mathfrak{m}_E^2\}.$$

We can thus identify $I_{E/K}/ker(\theta)$ with a subgroup of $A_E^*/U_1 \cong k_E^*$. This implies that the index $(I_{E/K} : ker(\theta))$ is coprime with p the characteristic of k_E and so $ker(\theta)$ contains the unique p-Sylow S of $I_{E/K}$.
Conversely, since T/L is tamely ramified of degree n_0, there exists a prime $\pi_T \in T$ such that $\pi_T^{n_0} = \pi_L$ for some prime of L. Then $\frac{\sigma(\pi_T)}{\pi_T}$ is a n_0-th root of unity for $\sigma \in I_{E/K}$. On the other hand the extension E/T is totally ramified of degree p^k so that $\pi_T = v\pi_E^{p^k}$ for some π_E of E prime and a unit v of A_E. This means $\frac{\sigma(\pi_T)}{\pi_T} \equiv (\frac{\sigma(\pi_E)}{\pi_E})^{p^k} \pmod{\mathfrak{m}_E}$ for $\sigma \in I_{E/K}$. We then have

$$\sigma \in ker(\theta) \Rightarrow (\frac{\sigma(\pi_E)}{\pi_E})^{p^k} \equiv 1 \pmod{\mathfrak{m}_E} \Leftrightarrow \frac{\sigma(\pi_T)}{\pi_T} \equiv 1 \pmod{\mathfrak{m}_E}.$$

But $\frac{\sigma(\pi_T)}{\pi_T}$ is a n_0-th root of unity so we must have $\sigma(\pi_T) = \pi_T$. Indeed, we have $(\frac{\sigma(\pi_T)}{\pi_T})^{n_0} = 1$ and if $\frac{\sigma(\pi_T)}{\pi_T} = 1 + a\pi_E^r$ with $a \in A_E^*$ then $1 = (1 + a\pi_E^r)^{n_0} \equiv 1 + n_0 a\pi_E^r \pmod{\pi_E^{r+1}}$. But also $(n_0, p) = 1$, so we must have $a = 0$. This gives

$$S = ker(\theta) = \{\sigma \in I_{E/K} : \sigma(\pi_E) - \pi_E \in \mathfrak{m}_E^2\}.$$

More generally, one observes first that for $\sigma \in G = Gal(E/K)$ we have $\sigma(A_E) = A_E$, $\sigma(\mathfrak{m}_E^i) = \mathfrak{m}_E^i$ for $i \geq 1$. So, there is an induced map $\bar{\sigma} : A_E/\mathfrak{m}_E^i \to A_E/\mathfrak{m}_E^i$ with $\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)}$ where $\bar{\alpha} = \alpha + \mathfrak{m}_E^i$. Hence we can define group homomorphisms

$$\begin{array}{rcl} \psi_i : G & \to & Aut(A_E/\mathfrak{m}_E^{i+1}) \\ \sigma & \mapsto & \bar{\sigma} \end{array}$$

For $i \geq 0$, define $G_i := ker(\psi_i)$ so that $I_{E/K} = G_0$ and $S = G_1$.

Definition 4.2.15. The subgroups G_i, $i \geq 0$, are called the *higher ramification subgroups in lower numbering* associated with the Galois extension E/K.

These higher ramifications subgroups form a decreasing filtration on G :

$$1 = \cdots = G_l \subset G_{l-1} \subset \cdots \subset G_1 \subset G_0 \subset G_{-1} = G.$$

By Galois correspondence they give rise to the tower of fields:

$$E \supset \cdots \supset T_i \supset \cdots \supset T \supset L \supset K.$$

T_i is called the *i-th ramification subfield* for the extension E/K. From proposition 4.2.3, p 40, we have $A_E = A_K[\alpha]$ for some $\alpha \in A_E$. Then these higher ramification subgroups can be described in terms of α. We have

Lemma 4.2.16. *Take $\alpha \in A_E$ such that $A_E = A_K[\alpha]$ and $\sigma \in Gal(E/K)$. Then $v_E(\sigma(\alpha) - \alpha) = Inf_{a \in A_E} v_E(\sigma(a) - a)$.*

Proof. Let $a \in A_E$, we have $a = a_{n-1}\alpha^{n-1} + \cdots + a_0$, with $a_i \in A_K$. We obtain $\sigma(a) - a = a_{n-1}(\sigma(\alpha)^{n-1} - \alpha^{n-1}) + \cdots + a_1(\sigma(\alpha) - \alpha)$. Since $\sigma(\alpha)^k - \alpha^k$ is divisible by $\sigma(\alpha) - \alpha$ for $k \geq 1$, we obtain that $\sigma(a) - a$ is a multiple of $\sigma(\alpha) - \alpha$, and hence the relation follows. □

One then defines $i_{E/K}(\sigma) = v_E(\sigma(\alpha) - \alpha)$ for α a generator of the valuation ring A_E over A_K. From lemma 4.2.16, we see that $i_{E/K}(\sigma)$ is independent of the choice of α. We have $G_i = \{\sigma \in G : i_{E/K}(\sigma) \geq i + 1\}$. As the extension E/L is totally ramified, one has $A_E = A_L[\pi]$ with π a prime of A_E, so one can compute the successive quotients in the filtration as follows. The computation establishes that a finite Galois extension of local fields is solvable. It provides also a short argument to see that G_1 is the unique p-Sylow of the inertia subgroup $I_{E/K}$. We observe as well that in contrast with the number fields where the roots of a polynomial of degree greater or equal to 5 cannot be given by radicals in general, roots of a polynomial over local fields can be expressed with radicals.

So, let E/K be a totally ramified Galois extension of local fields with $A_E = A_K[\pi]$, where π a prime of A_E. We have $G_i = \{\sigma \in Gal(E/K) : \sigma(\pi) - \pi \in \mathfrak{m}_E^{i+1}\}$. Therefore for $\sigma \in G_i$, we obtain $\frac{\sigma(\pi)}{\pi} \in 1 + \mathfrak{m}_E^i = U_i$. If $\pi_1 = u\pi$ with $u \in A_E^* = U$, the group of units of A_E, we get $\frac{\sigma(\pi_1)}{\pi_1} = \frac{\sigma(u)}{u}\frac{\sigma(\pi)}{\pi}$. Thus $\frac{\sigma(\pi_1)}{\pi_1} \equiv \frac{\sigma(\pi)}{\pi} \pmod{U_{i+1}}$. Therefore we can define maps that are independent of π :

$$\begin{aligned} \phi_i : G_i &\to U_i/U_{i+1} \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} \pmod{U_{i+1}}. \end{aligned}$$

Recall from proposition 3.2.10, p 26, the isomorphisms $U/U_1 \cong k_E^*$, $U_i/U_{i+1} \cong k_E$ for $i \geq 1$. Then one has

Theorem 4.2.17. *1. ϕ_i is a homomorphism with kernel G_{i+1}.*

2. G_0/G_1 is cyclic of order prime with p and $G_i/G_{i+1}, i \geq 1$ are elementary abelian p-groups.

3. $G = Gal(E/K)$ is a solvable group.

Proof. This follows from the above discussion, for more details see [20, p 65]. □

Remark 4.2.18. *The second statement of theorem 4.2.17 clearly gives another argument to see that G_1 is the unique p-Sylow of $I_{E/K}$.*

The ramification subgroups carry non-trivial information concerning the arithmetic of Galois extensions of local fields E/K. So, it is natural to ask how the ramification groups behave under the operation of restricting to a subgroup H of $G = Gal(E/K)$ or the operation of taking quotients G/H when H is normal in G. In other words given a tower of fields $E \supset L \supset K$ with L/K Galois, what are the relations between G_i, $H_i = Gal(E/L)_i$ and $Gal(L/K)_i = (G/H)_i$. For subgroups this is clear:

Proposition 4.2.19. $H_i = G_i \cap H$.

Proof. This follows from the definition. □

On the other hand when taking quotients things are not so simple. By the canonical projection G_i maps to G_iH/H, but in general $(G/H)_i \neq G_iH/H$. Thus, the numbering changes by passage to quotient. Writing G_iH/H, and $(G/H)_j$, for respectively the image of G_i modulo H and a ramification subgroup of G/H, we seek a relation between i and j. To this end a slight modification of the definition of the ramification groups is needed. The indexing set is made to be continuous as follows. For a real number $t \in [-1, +\infty)$, one defines

$$G_t = \{\sigma \in G = Gal(E/K) : i_{E/K}(\sigma) \geq t + 1\}.$$

Then we have $G_{-1} = G$, $G_t = G_0$ for $-1 < t \leq 0$, $G_t = G_1$ for, $0 < t \leq 1$ and in general $G_t = G_n$ for $n - 1 < t \leq n$. Given a normal subgroup H of G, let $L = E^H$. For $\tau \in G$, and $\sigma \in G/H = Gal(L/K)$, we write $\tau \to \sigma$ to mean that the restriction of τ to L gives σ. Then we have

Proposition 4.2.20. *Let H be a normal subgroup of G, and $L = E^H$. Then for $\sigma \in Gal(L/K)$, one has*

$$i_{L/K}(\sigma) = \frac{1}{e(E/L)} \sum_{\tau \to \sigma} i_{E/K}(\tau).$$

Proof. Write $A_E = A_K[\alpha]$, $A_L = A_K[\beta]$ for $\alpha \in A_E$, $\beta \in A_L$. By definition for $\sigma \in Gal(L/K)$, we have $i_{L/K}(\sigma) = v_L(\sigma(\beta) - \beta)$ and for $\tau \in Gal(E/K)$ we have $i_{E/K}(\tau) = v_E(\tau(\alpha) - \alpha)$. Suppose $\tau \to \sigma$, the other elements in $Gal(E/K)$ which restrict to σ are of the form τh with $h \in H$. As for $y \in L$ we have $v_E(y) = e(E/L)v_L(y)$, we see that we need to check that

$$v_E(\sigma(\beta) - \beta) = v_E(\prod_{h \in H} (\tau h(\alpha) - \alpha)).$$

If $\sigma = 1$, both sides have valuation equal to ∞. So, suppose $\sigma \neq 1$ and put $a = \tau(\beta) - \beta$, and $b = \prod_{h \in H}(\tau h(\alpha) - \alpha)$. Next observe that a, b, have the

same valuation if and only if they generate the same ideal in A_E. Let $f(X) = \prod_{h\in H}(X - h(\alpha))$ be the minimal polynomial of α over L. We let τ acts on the coefficients of $f(X) \in A_L[X]$ and we write $\tau(f)(X) = \prod_{h\in H}(X - \tau h(\alpha))$ the resulting polynomial. Each coefficient of $\tau(f)(X) - f(X)$ is of the form $\sum_{i\geq 1} a_i(\tau(\beta^i) - \beta^i)$ with $a_i \in A_K$. These coefficients are all divisible by $a = \tau(\beta) - \beta$. Plugging $X = \alpha$ in $\tau(f)(X) - f(X)$ we see that $b = \pm\tau(f)(\alpha)$ is divisible by a. Conversely, writing $\beta = a_l\alpha^l + \cdots + a_0 = g(\alpha) \in A_K[\alpha]$, we obtain that α is a zero of the polynomial $g(X) - \beta$. Therefore $g(X) - \beta = f(X)p(X)$ with $p(X) \in A_E[X]$. Now $\tau(g)(X) - \tau(\beta) = g(X) - \tau(\beta) = \tau(f)(X)\tau(p)(X)$. Plugging $X = \alpha$ in $g(X) - \tau(\beta)$ we obtain

$$-a = \beta - \tau(\beta) = \pm b\tau(p)(\alpha).$$

And the proposition follows. □

Next one associates a real valued function $\psi_{E/K}$ defined on $[-1, \infty)$ with the filtration G_i as follows. For $s \in [-1, \infty)$ one puts

$$\psi_{E/K}(s) = \int_0^s \frac{dt}{(G_0 : G_t)}$$

with the convention that if $t = -1$, then $(G_0 : G_t) = (G : G_0)^{-1}$, and for $-1 < t \leq 0$, $(G_0 : G_t) = (G_0 : G_0)^{-1} = 1$. The map $f(t) := (G_0 : G_t)^{-1}$ on $[-1, \infty)$ satisfies: $f(-1) = (G : G_0)$, $f(t) = 1$ for $-1 < t \leq 0$ and $f(t) = (G_0 : G_n)^{-1}$ for $n - 1 < t \leq n$ and $n \geq 1$. So f is a step function discontinuous at 0, 1, 2, 3, $\cdots$. Therefore $\psi_{E/K}$ is continuous piecewise linear function. For an integer m, with $0 < m \leq s \leq m + 1$, we have

$$\psi_{E/K}(s) = \int_0^1 \frac{dt}{(G_0 : G_t)} + \cdots + \int_m^{m-1} \frac{dt}{(G_0 : G_t)} + \int_m^s \frac{dt}{(G_0 : G_t)}.$$

This gives

$$\psi_{E/K}(s) = \frac{1}{g_0}(g_1 + g_2 + \cdots + g_m + (s - m)g_{m+1}), \text{ with } g_i = card(G_i).$$

The relation between this function and the integers $i_{E/K}(\sigma)$ is as follows.

Proposition 4.2.21. *Let E/K be a Galois extension of local fields with Galois group G. Then one has*

$$\psi_{E/K}(s) = \frac{1}{g_0}\sum_{\sigma\in G} inf\{i_{E/K}(\sigma), s + 1\} - 1.$$

Proof. Let $\theta(s)$ be the function on the right hand side. Both θ and $\psi_{E/K}$ are continuous and piecewise linear real functions defined on $[-1, \infty)$. One has $\psi_{E/K}(0) = \theta(0) = 0$. On one hand for $s \in (m, m + 1)$ with $m \in \mathbb{Z}$, we

have $inf\{i_{E/K}(\sigma), s+1\} = s+1$ if $\sigma \in G_{m+2}$ and it is the constant $i_{E/K}(\sigma)$ otherwise. Therefore for $s \in (m, m+1)$,

$$\theta'(s) = \frac{1}{g_0} card\{\sigma \in G : i_{E/K}(\sigma) \geq m+2\} = \frac{1}{(G_0 : G_{m+1})}.$$

On the other hand it is clear that $\psi'_{E/K}(s) = \frac{1}{(G_0:G_{m+1})}$ for $s \in (m, m+1)$. Hence we deduce that we must have $\psi_{E/K}(s) = \theta(s)$. □

Now via the function $\psi_{E/L}$ one has the following result known as *Herbrand's theorem.*

Theorem 4.2.22. (Herbrand) *Let E/K be a Galois extension of local fields with $G = Gal(E/K)$. Let H be normal in G, and let $L = E^H$ so that L/K is Galois with $Gal(L/K) = G/H$. Lastly, let $r = \psi_{E/L}(s)$. Then one has*

$$G_sH/H = (G/H)_r$$

Proof. To start let us first observe that $\psi_{E/L}$ is an increasing function. Next let $\sigma \in G_sH/H$ and any $\tau \in G$ such that $\tau|_L = \sigma$. Then $\sigma \in G_sH/H \Leftrightarrow i_{E/K}(\tau) \geq s+1$ for some τ. So, if we define $j(\sigma) = \sup_{\tau|_L=\sigma} i_{E/K}(\tau)$, and by using the fact that $\psi_{E/L}$ is an increasing function, we can write

$$\sigma \in G_sH/H \Leftrightarrow j(\sigma) - 1 \geq s \Leftrightarrow \psi_{E/L}(j(\sigma) - 1) \geq \psi_{E/L}(s).$$

On the other hand, we have

$$\sigma \in (G/H)_{\psi_{E/L}(s)} \Leftrightarrow i_{L/K}(\sigma) \geq \psi_{E/L}(s) + 1.$$

So, in order to prove $G_sH/H = (G/H)_r$, we are led to show the statement

$$\psi_{E/L}(j(\sigma) - 1) \geq \psi_{E/L}(s) \Leftrightarrow i_{L/K}(\sigma) - 1 \geq \psi_{E/L}(s),$$

that is we need to establish

$$\psi_{E/L}(j(\sigma) - 1) = i_{L/K}(\sigma) - 1.$$

To this end we fix $\tau_0 \in G$ with $\tau_0|_L = \sigma$ and $j(\sigma) = i_{E/K}(\tau_0)$. By proposition 4.2.20 we have

$$i_{L/K}(\sigma) = \frac{1}{e(E/L)} \sum_{\tau|_L=\sigma} i_{E/K}(\tau) = \frac{1}{e(E/L)} \sum_{h \in H} i_{E/K}(\tau_0 h).$$

Let $\alpha \in A_E$ be a primitive element, i.e., $A_E = A_K[\alpha]$, then $i_{E/K}(\tau_0 h) = v_E(\tau_0(h(\alpha)) - \alpha) = v_E(\tau_0(h(\alpha) - \alpha) + \tau_0(\alpha) - \alpha)$. Hence $i_{E/K}(\tau_0 h) \geq \inf\{i_{E/K}(h), j(\sigma)\}$. By definition of $j(\sigma)$, we have $i_{E/K}(\tau_0 h) \leq j(\sigma) = i_{E/K}(\tau_0)$. Whence if $i_{E/K}(h) \geq j(\sigma)$, then $i_{E/K}(\tau_0 h) = j(\sigma)$. Also in the case

$i_{E/K}(h) < j(\sigma)$, then the ultrametric inequality gives $i_{E/K}(\tau_0 h) = i_{E/K}(h)$. Thus we obtain $i_{E/K}(\tau_0 h) = \inf\{i_{E/K}(h), j(\sigma)\}$. Next, by proposition 4.2.21 we have

$$\psi_{E/L}(s) + 1 = \frac{1}{e(E/L)} \sum_{h \in H} inf\{i_{E/L}(h), s+1\}.$$

So after noting that $i_{E/L}(h) = i_{E/K}(h)$, we deduce $i_{L/K}(\sigma) - 1 = \psi_{E/L}(j(\sigma) - 1)$. This is what we needed. □

$\psi_{E/K}$ is strictly increasing so it has an inverse say $\phi_{E/K} : [-1, \infty) \to [-1, \infty)$. Then the *upper numbering* for the ramification groups is defined as follows.

Definition 4.2.23. For $\phi_{E/K}(r) = s$, one puts $G^r := G_s$.

One can also write $\phi_{E/K}$ by means of an integral. Indeed on one hand for r and $\phi_{E/K}(r)$ non-integers, $\phi'_{E/K}(r) = \frac{1}{\psi'_{E/K}(\phi_{E/K}(r))}$. On the other hand the function $\omega(s) = \int_0^s (G^0 : G^t) dt$, satisfies $\omega'(s) = \frac{1}{\psi'_{E/K}(\phi_{E/K}(r))}$ and $\omega(0) = \phi_{E/K}(0) = 0$. Hence

$$\phi_{E/K}(r) = \int_0^r (G^0 : G^t) dt.$$

In a tower of fields these functions verify the following relations.

Proposition 4.2.24. *Let L/K be a Galois subextension of E/K and $H = Gal(E/L)$. Then*

$$\psi_{E/K} = \psi_{L/K} \circ \psi_{E/L}, \ \phi_{E/K} = \phi_{E/L} \circ \phi_{L/K}.$$

Proof. We take derivatives when it makes sense, that is at the points of continuity of all the functions involved. The two functions on both sides of the first relation take the same value zero at zero. We have $\psi'_{E/K}(s) = \frac{1}{e(E/K)} card(G_s)$. Also $(\psi_{L/K} \circ \psi_{E/L}(s))' = \frac{card((G/H)_t) card(H_s)}{e(E/L)e(L/K)}$ with $t = \psi_{E/L}(s)$. This is because we have $\psi'_{E/L}(s) = \frac{card(H_s)}{e(E/L)}$ and $\psi'_{L/K}(t) = \frac{(G/H)_t}{e(L/K)}$. Hence it suffices to see that $card(G_s) = card((G/H)_t) card(H_s)$. And this follows by Herbrand theorem, $(G/H)_t = G_s H/H$, and the surjective group homomorphism $\rho : G_s \to G_s H \to G_s/H$ with kernel $G_s \bigcap H = H_s$ which induces the isomorphism $G_s H/H \cong G_s/H_s$. Since $\psi_{E/K}$ and $\phi_{E/K}$ are inverse of each other, the second relation follows from the first. □

Now putting all of this together one has the following.

Proposition 4.2.25. *Let L/K be a Galois subextension of E/K with $H = Gal(E/L)$. Then*

$$G^r H/H = (G/H)^r.$$

Proof. By definition of the upper numbering $G^rH/H = G_{\phi_{E/K}(r)}H/H = (G/H)_{\psi_{E/L}(\phi_{E/K}(r))}$ by Herbrand's theorem. And since $\phi_{E/L}$ is the inverse of $\psi_{E/L}$ we obtain $\psi_{E/L}(\phi_{E/K}(r)) = \phi_{L/K}(r)$. Hence

$$G^rH/H = (G/H)_{\phi_{L/K}(r)} = (G/H)^r.$$

□

Thus we see that the lower numbering for the ramification groups is invariant when changing the base field while the upper numbering is invariant when passing to a Galois subextension.

4.2.3 The group of norms

In this last part of this long chapter, we shall give the basic properties concerning the *norm group* in a finite extension of local fields. This section is very brief so the reader is invited to consult the references namely [10] or [15], for a satisfactory treatment of the norm group which plays a fundamental role in local class field theory as we will see in the next chapter.

So, let E/K be a Galois extension of local fields with $G = Gal(E/K)$. Recall, the norm $N_{E/K}$ and the trace $Tr_{E/K}$ are the group homomorphisms defined by:

$$\begin{aligned} N_{E/K} : E^* &\to K^* \\ x &\mapsto \prod_{\sigma\in G} \sigma(x); \\ Tr_{E/K} : E &\to K \\ x &\mapsto \sum_{\sigma\in G} \sigma(x). \end{aligned}$$

From their definitions we deduce the norm and the trace maps are continuous since each $\sigma \in Gal(E/K)$ is continuous. Particularly for the norm, this implies

Proposition 4.2.26. *Let A_E^*, A_K^* be the unit groups. Then $N_{E/K}(A_E^*)$ is a compact subgroup of A_K^*, hence closed in the compact Hausdorff group A_K^*. Furthermore $N_{E/K}(E^*)$ is closed in K^*.*

Proof. A_E^* is closed in the compact A_E so it is also compact. From the continuity of the norm $N_{E/K}$ follows that $N_{E/K}(A_E^*)$ is compact and hence closed in A_K^*. Next take a prime π_E of E. Then we have $E^* =< \pi_E > \times A_E^*$. Therefore $N_{E/K}(E^*) =< N_{E/K}(\pi_E) > \times N_{E/K}(A_E^*)$. Now $< N_{E/K}(\pi_E) >$ is discrete in K^* hence closed in K^*. Thus $N_{E/K}(E^*)$ is a product of groups both closed in K^* so $N_{E/K}(E^*)$ is closed in K^*. □

In the situation where E/K is not necessarily finite, one defines the norm group $N(E/K)$ and the *unit norm group* $N(U_{E/K})$ as follows. For L/K running over the finite subextensions of E/K, one puts $N(E/K) = \cap_L N_{L/K}(L^*)$, $N(U_{E/K}) = \cap_L N(U_L)$ where U_L is the unit group of L.

Let E/K be finite unramified. We know that a prime π_K of K is also a prime of E. Hence we can write the higher unit groups as follows: $U_{E,i} = 1 + \pi_K^i A_E$, $U_{K,i} = 1 + \pi_K^i A_K$. For $u = 1 + \pi_K^i a \in U_{E,i}$, we have

$$N_{E/K}(u) = \prod_{\sigma \in G} (1 + \pi_K^i \sigma(a)) \equiv 1 + \pi_K^i Tr_{E/K}(a) \pmod{\pi_K^{i+1}}. \qquad (4.1)$$

Thus

Lemma 4.2.27. *For $i \geq 1$ we have $N_{E/K}(U_{E,i}) \subset U_{K,i}$.*

Besides, we can define surjective homomorphisms

$$\begin{aligned} \theta_{E,i} : U_{E,i} &\to k_E \\ 1 + \pi_K^i a &\mapsto a; \\ \theta_{K,i} : U_{K,i} &\to k_K \\ 1 + \pi_K^i a &\mapsto a. \end{aligned}$$

By the congruence (4.1), one has

Proposition 4.2.28. *The following diagram is commutative*

$$\begin{array}{ccc} U_{E,i} & \xrightarrow{\theta_{E,i}} & k_E \\ {\scriptstyle N_{E/K}}\downarrow & & \downarrow{\scriptstyle Tr_{k_E/k_K}} \\ U_{K,i} & \xrightarrow{\theta_{K,i}} & k_K \end{array}$$

Furthermore $N_{E/K}(U_{E,i}) = U_{K,i}$ for $i \geq 1$.

Proof. We have $\theta_{E,i}(1 + \pi_K^i a) \equiv a \pmod{\pi_K}$, and from the isomorphism $Gal(E/K) \cong Gal(k_E/k_K)$, we see that $\overline{Tr_{E/K}(x)} = Tr_{k_E/k_K}(\bar{x})$. Combining this with the congruence for the norm makes the diagram commutative. We have the said equality from the surjectivity of the trace map Tr_{k_E/k_K}. To see this, recall that $Gal(k_E/k_K)$ is cyclic generated by the Frobenius automorphism $x \mapsto x^q$ with $q = card(k_K)$. So, the trace is the polynomial map $T(X) = X^{q^{n-1}} + \cdots + X^q + X$ on k_E, where $n = [k_E : k_K] = [E : K]$. Hence the kernel of Tr_{k_E/k_K} is the set of the zeros of $T(X)$. Thus $card(ker(Tr_{k_E/k_K})) \leq q^{n-1}$, and hence $card(im(Tr_{k_E/k_K})) \geq \frac{q^n}{q^{n-1}} = q = card(k_K)$. □

Corollary 4.2.29. $N_{E/K}(A_E^*) = A_K^*$.

Proof. Recall from proposition 3.2.18, p 30 that A_E^* contains the (q^n-1)-th roots of unity and A_K contains $(q-1)$-th roots of unity. Then write $A_E^* =< \zeta_{q^n-1} > \times U_{E,1}$, where $< \zeta_{q^n-1} >$ is the cyclic group generated by a primitive (q^n-1)-th root of unity ζ_{q^n-1}. From proposition 4.2.28 we have $N_{E/K}(U_{E,1}) = U_{K,1}$ and $N_{E/K}(\zeta_{q^n-1})$ is a primitive $(q-1)$-th root of unity so that $N_{E/K}(< \zeta_{q^n-1} >) =< \zeta_{q-1} >$. Since $A_K^* =< \zeta_{q-1} > U_{K,1}$, we can conclude. □

In the totally ramified situation we have the following useful criterion.

Proposition 4.2.30. *An extension E/K is totally ramified if and only if $N_{E/K}(E^*)$ contains a prime element.*

Proof. We assume the extension to be finite; for the infinite case see [15]. So if E/K is totally ramified, then we know that for a prime $\pi_E \in A_E$ $N_{E/K}(\pi_E)$ is prime in K.
Conversely, suppose that $N_{E/K}(E^*)$ contains a prime π_K. If E/K was not totally ramified, then we would have that E contains the unramified extension of K_n^{ur}/K of degree $n \geq 2$. We then obtain $N_{E/K}(E^*) \subset N_{K_n^{ur}/K}((K_n^{ur})^*) =< \pi_K^n > \times A_{K_n^{ur}}^*$ since π_K is a prime in K_n^{ur}. A contradiction and so the proposition follows. □

Chapter 5

Formal group law, Lubin-Tate extensions and Local Class Field Theory

For the sake of giving the main theorem of the explicit description of the class field theory of a local field, this chapter introduces the notion of a formal group law, with emphasis on Lubin-Tate formal group laws. By means of the latter we will define Lubin-Tate modules. We next give the construction of the Lubin-Tate extensions which are obtained by adjoining torsion points on Lubin-Tate modules to a complete unramified extension of a local field. And lastly local class field theory will follow. The main references here are [15], [25], [17] and [13].

5.1 Introduction

Let K be a local field with A_K as ring of integers and $\mathfrak{m}_K$ the prime ideal of A_K. We fix an algebraic closure K^{al} of K and we write $\hat{K}^{al}$, A, $\mathfrak{m}$ for respectively the completion of K^{al} with respect to the unique extension of the valuation of K to K^{al}, the valuation ring and the maximal ideal of $\hat{K}^{al}$. Originally, explicit local class field for K relies on the notion of *Lubin-Tate formal groups* over A_K, for the definition of formal groups see definition 5.2.1 below. These Lubin-Tate groups give rise to an A_K-module structure on $\mathfrak{m}$, see example 5.2.10 where the case $K = \mathbb{Q}_p$ is illustrated. Then a tower of totally ramified extensions of K generalising the cyclotomic extensions for $\mathbb{Q}_p$ is constructed by adjoining torsion points of the A_K-module $\mathfrak{m}$ to K. These generalised cyclotomic extensions are called Lubin-Tate extensions. This is Lubin-Tate theory as exposed in [16] and [21].

Now, let n be a positive integer and let L/K be the unique unramified extension of degree n of K. In [22], *relative Lubin-Tate groups* are constructed, these encompass the Lubin-Tate groups as a special case. Similar as in the

classical case, in [15] and more recently in [25], a treatment of explicit local class field theory for K is given by means of relative Lubin-Tate groups. Here, one constructs *relative Lubin-Tate* extensions of L by adjoining torsion points of the A_K-module structure on $\mathfrak{m}$ induced by relative Lubin-Tate groups. As this approach is a generalisation of the original treatment, we choose to adopt it in our presentation of explicit local class field theory.

5.2 Relative Lubin-Tate formal group law

In this section, the concept of formal group law is introduced. We are mainly interested in a special class of formal group law that is the Lubin-Tate formal group law.

5.2.1 Generalities

Classically, by a group G one means a set G and a group law defined on G. By a formal group law, one is given a law without having a priori a set on which the law acts.

To start with we first recall some basic rules concerning formal power series which is the formalism in which formal group laws are defined. Let $B = A[[X, Y]]$ be the ring of formal power series in the variables X, Y over a ring A. Let $F \in B$. For $a = (a_1, a_2) \in A^2$, recall that evaluating F at a is not always defined. But for $G(X, Y)$, $f(X) \in B$ with $F(0) = 0$, then we can substitute $G \circ f := G(f(X), f(Y))$. On the subring $A[[X]]$ of B, composing $f(X)$, $g(X) \in XA[[X]]$ defines a structure of semi-group (not necessarily commutative) with X as neutral element. $f(X) \in XA[[X]]$ has an inverse $g(X) \in XA[[X]]$ for composition that is $f \circ g = g \circ f = X$, if and only if the coefficient of X in f is a unit.

For power series, the notation $F \equiv G \pmod{(deg\ n)}$ signifies that the power series $F - G$ has all terms of degree greater or equal to n.

Definition 5.2.1. A *formal group law* over a ring A is a formal power series $F(X, Y) \in A[[X, Y]]$ satisfying the following axioms:

(a) $F(X, Y) \equiv X + Y \pmod{(deg\ 2)}$,

(b) $F(X, F(Y, Z)) = F(F(X, Y), Z)$ (Associativity),

(c) $F(X, Y) = F(Y, X)$ (Commutativity).

Example 5.2.2. *We have the additive formal group law given by* $G_a(X, Y) := X + Y$ *and the multiplicative formal group law defined by* $G_m(X, Y) := X + Y + XY = (1 + X)(1 + Y) - 1$.

From (a) and (b), one sees that a formal group law $F(X, Y)$ is of the form $F(X, Y) = X + Y + \sum_{i,j \geq 1} X^i Y^j$. Hence the equation $F(X, Y) = 0$ can be

solved for $Y \in XA[[X]]$. Denote by $\iota_F(X)$ its solution. For $f,\ g \in XA[[X]]$, the law $f +_F g = F(f(X), g(X))$, defines an abelian group on $XA[[X]]$. From $F(X, \iota_F(X)) = 0$, we have $f +_F \iota_F(f) = F(f(X), \iota_F(f(X))) = 0$, so $\iota_F(f)$ is the inverse of f. When A is a complete valuation ring with maximal ideal $\mathfrak{m}$, then for $a,\ b \in \mathfrak{m}$, the law $a +_F b = F(a, b)$ is well defined and makes $(\mathfrak{m},\ +_F)$ an abelian group.

We also have a notion of homomorphism of formal group laws. It is defined as follows.

Definition 5.2.3. Let $F, G \in A[[X, Y]]$, be formal group laws. We say that a power series $f(X) \in XA[[X]]$ is a homomorphism from F to G if:

$$f(F(X, Y)) = G(f(X), f(Y)).$$

It is an isomorphism if in addition there exists $g(X) = f^{-1}(X) \in XA[[X]]$ such that:

$$g(G(X, Y)) = F(g(X), g(Y)).$$

If $f(X)$ admits an inverse $g(X)$ for composition, then we have $f(F(g(X), g(Y))) = G(X, Y) \Leftrightarrow g(G(X, Y)) = F(g(X), g(Y))$. Therefore f is an isomorphism of formal group laws if and only if the coefficient of X in f is a unit in A. Denote by $\mathrm{Hom}_A(F, G)$, the set of homomorphism from F to G. With the operation $f +_G g$, $\mathrm{Hom}_A(F, G)$ is a subgroup of $(XA[[X]], +_G)$. Furthermore, with the multiplication $f \circ g$, $\mathrm{End}_A(F) := Hom_A(F, F)$ has a ring structure.
Having at hand the basic language of formal group laws, we shall now turn to the study of Lubin-Tate formal group laws which are formal groups over a discrete valuation ring.

5.2.2 Relative Lubin-Tate formal group laws

Let $E := \hat{K}^{ur}$ be the completion of the maximal unramified extension of a local field K with v_E the unique valuation on E extending v_K of K. The Frobenius automorphism $\varphi_K \in Gal(K^{ur}/K)$ is extended by continuity to E and we will denote it by φ_K. We write as usual $A_E,\ \mathfrak{m}_E, A_K,\ \mathfrak{m}_K$ for the valuation rings and maximal ideals of E, K respectively. Lastly let $q = card(k_K)$. We start by defining

Definition 5.2.4. Let π be a prime of E. A power series $e(X) \in A_E[[X]]$ is called a *Lubin-Tate power series* for π when the following conditions are satisfied:

$$e(X) \equiv \pi X \pmod{(deg\ 2)},\ e(X) \equiv X^q \pmod{\pi}.$$

In particular a *Lubin-Tate polynomial* $e(X)$ for π is of degree q and satisfies these conditions. A Lubin-Tate polynomial is not necessarily a monic polynomial.

Recall that φ_K acts on the ring $A_E[[X]]$ as follows. For $f \in A_E[[X]]$, f^{φ_K} is the power series obtained from the action of φ_K on the coefficients of f. We next show that the Lubin-Tate power series arise as homomorphisms of certain formal group laws. In light of definition 5.2.3, for a power series $F(X_1, \cdots, X_n) \in A_E[[X_1, \cdots, X_n]]$ and a power series $f(X) \in A_E[[X]]$ we define $F \circ f := F(f(X_1), \cdots, f(X_n)) \in A_E[[X_1, \cdots, X_n]]$.

Proposition 5.2.5. *Let $e(X)$, $e'(X) \in A_E[[X]]$ be Lubin-Tate power series for the primes π, π' respectively. Let $\mathfrak{L}(X_1, \cdots, X_n) = a_1X_1 + \cdots + a_nX_n \in A_E[[X_1, \cdots, X_n]]$ such that $\pi'\mathfrak{L}(X_1, \cdots, X_n) = \pi\mathfrak{L}^{\varphi_K}(X_1, \cdots, X_n)$, i.e., $\pi' a_i = \pi a_i^{\varphi_K}$ for all i. Then there exists a unique power series $F(X_1, \cdots, X_n) \in A_E[[X_1, \cdots, X_n]]$ such that:*

$$F(X_1, \cdots, X_n) \equiv \mathfrak{L}(X_1, \cdots, X_n) \pmod{deg\ 2} \text{ and } e' \circ F = F^{\varphi_K} \circ e.$$

Proof. A power series $F(X_1, \cdots, X_n)$ with non constant term can be written as $F(X_1, \cdots, X_n) = \sum_{r=1}^{\infty} H_r(X_1, \cdots, X_n)$ with $H_r(X_1, \cdots, X_n) \in A_E[X_1, \cdots, X_n]$, a homogeneous polynomial of degree r. Put $F_m = \sum_{r=1}^{m} H_r$. We seek polynomials $F_m, m \geq 1$, such that $e' \circ F_m \equiv F_m^{\varphi_K} \circ e \pmod{deg\ m+1}$. Then, $F = \lim_{m \to \infty} F_m$ is the desired power series. For $m = 1$, we take $F_1 = \mathfrak{L}$ as $\mathfrak{L}$ satisfies the conditions by hypothesis. Suppose we have uniquely found $F_1, \cdots, F_m$ satisfying our requirement. Write $F_{m+1} = F_m + H_{m+1}$, we have $e' \circ F_{m+1} \equiv e' \circ F_m + \pi' H_{m+1} \pmod{deg\, m+2}$ and also $F_{m+1}^{\varphi_K} \circ e \equiv F_m^{\varphi_K} \circ e + \pi^{m+1} H_{m+1}^{\varphi_K} \pmod{deg\, m+2}$. Indeed, write $e'(X) = \pi' X + \sum_{i=1}^{\infty} a_i X^i$. Then

$$\begin{aligned} e' \circ F_{m+1} &= \pi' F_{m+1} + \sum_{i=1}^{\infty} a_i F_{m+1}^i \\ &= \pi' F_m + \pi' H_{m+1} + \sum_{i=1}^{\infty} a_i \Big(\sum_{j=0}^{i} \binom{i}{j} F_m^{i-j} H_{m+1}^j\Big) \\ &= \pi' F_m + \sum_{i=0}^{\infty} a_i F_m^i + \pi' H_{m+1} + (\text{ terms of degree} \geq m+2). \end{aligned}$$

For the second equation write $e(X) = \pi X + \sum_{i=1}^{\infty} b_i X^i$ and use the fact that $H_{m+1} \circ e = \pi^{m+1} H_{m+1} + (\text{terms of degree} \geq m+2)$. Let $G_{m+1} = e' \circ F_m - F_m^{\varphi_K} \circ e$. Then to satisfy our conditions we must have $G_{m+1} + \pi' H_{m+1} - \pi^{m+1} H_{m+1}^{\varphi} \equiv 0 \pmod{deg\ m+2}$. On one hand, by definition of G_{m+1}, we have $G_{m+1} \equiv 0 \pmod{deg\ m+1}$. On the other $F_m(X_1, \cdots, X_n) = \sum a_{i_1, \cdots, i_n} X_1^{i_1} \cdots X_n^{i_n}$, so that, $F_m^q(X_1, \cdots, X_n) \equiv \sum a_{i_1, \cdots, i_n}^q (X_{i_1}^{i_1})^q \cdots (X_n^{i_n})^q \equiv F_m^{\varphi_K}(X_1^q, \cdots, X_n^q) \pmod{\pi'}$ since by definition of φ_K we have $a^{\varphi_K} \equiv a^q \pmod{\pi'}\ \forall a \in A_E$. From $e'(X) \equiv X^q \pmod{\pi'}$ we obtain $e' \circ F_m \equiv F_m^q \pmod{\pi'}$ and similarly from $e(X) \equiv X^q \pmod{\pi}$, we deduce that $F_m^{\varphi_K} \circ e \equiv F_m^{\varphi_K}(X_1^q, \cdots, X_n^q) \pmod{\pi'}$. Therefore we have $G_{m+1}(X_1, \cdots, X_n) \equiv$

$F_m^q(X_1,\cdots,X_n) - F_m^{\varphi_K}(X_1^q,\cdots,X_n^q) \equiv 0 \pmod{\pi'}$, that is all the coefficients in G_{m+1} are multiples of π'. So, let $\pi'\beta,\ \pi'\alpha, \pi^{m+1}\alpha^{\varphi_K}$ be the coefficient of a monomial $X_1^{i_1}\cdots X_n^{i_n}$ of degree $m+1$ in $G_{m+1}, \pi' H_{m+1}$, and $\pi^{m+1}H_{m+1}^{\varphi_K}$ respectively. Then we must solve for α the equation $\pi'\beta + \pi'\alpha - \pi^{m+1}\alpha^{\varphi_K} = 0$. This gives, with $\omega = \pi'^{-1}\pi^{m+1}$, $\alpha = -\beta + \omega\alpha^{\varphi_K} = -\beta - \omega\beta^{\varphi_K} + \omega^{\varphi_K+1}\alpha^{\varphi_K^2} = \cdots = -\beta - \omega\beta^{\varphi_K} - \omega^{\varphi_K+2}\beta^{\varphi_K^2} - \cdots$. By the completeness of A_E, we have $\alpha \in A_E$ and it is unique. Indeed, if say α' is another solution, then $v_E(\alpha-\alpha') = v_E(\omega) + v_E((\alpha-\alpha')^{\varphi_E}) = v_E(\omega) + v_E(\alpha-\alpha')$. Since $v_E(\omega) \geq 1$, we must have $v_E(\alpha-\alpha') = \infty$. This uniquely determines H_{m+1}, and hence F_{m+1} is uniquely determined which implies that F is uniquely determined. □

Corollary 5.2.6. *Let $e(X) \in A_E[[X]]$ be a Lubin-Tate power series for a prime π. Then there exists a unique formal group law F_e over A_E such that $e(X) \in Hom_{A_E}(F_e,\ F_e^{\varphi_K})$.*

Proof. Applying the proposition for $\pi = \pi',\ e = e',\ \mathfrak{L}(X,Y) = X+Y$, we obtain a unique power series $F_e(X,Y) \in A_E[[X,Y]]$ such that $e \circ F_e = F_e^{\varphi_K} \circ e$. To see that $F_e(X,Y)$ is a formal group law, we have $e\circ(F_e(X,F_e(Y,Z))) = F_e^{\varphi_K}(e(X), F_e^{\varphi_K}(e(Y),\ e(Z))) = (F_e(X,F_e(Y,Z))^{\varphi_K} \circ e$. Similarly $e\circ(F_e(F_e(X,Y),Z)) = (F_e(F_e(X,Y),Z))^{\varphi_K}\circ e$. Therefore $F_e(X,F_e(Y,Z))$ and $F_e(F_e(X,Y),Z) \in A_E[[X,Y,Z]]$ satisfy the conditions of proposition 5.2.5 with $\pi = \pi',\ e = e',\ \mathfrak{L}(X,Y,Z) = X+Y+Z$. Hence they must be equal by the uniqueness of such a power series. The equality $F(X,Y) = F(Y,X)$ is obtained in the same fashion. □

Let $A^E_{\pi,\pi'} = \{a \in A_E : \pi' a = \pi a^{\varphi_K}\}$, then from the proposition 5.2.5, for each $a \in A^E_{\pi,\pi'}$, there exists a unique power series $[a]_{e,e'}(X) \in A_E[[X]]$ such that $e' \circ [a]_{e,e'} = [a]_{e,e'}^{\varphi_K} \circ e$, $[a]_{e,e'}(X) \equiv aX \pmod{deg\ 2}$. Let also $F_e,\ F_{e'}$ be formal group laws over A_E arising from Lubin-Tate power series $e(X)$, $e'(X)$.

Proposition 5.2.7. *Keeping the same notations as above, one has*

1. $[a]_{e,e'} \circ F_e = F_{e'} \circ [a]_{e,e'}$, *i.e.,* $[a]_{e,e'} \in Hom_{A_E}(F_e, F_{e'})$,
2. $[a+b]_{e,e'}(X) = F_e([a]_{e,e'}(X), [b]_{e,e'}(X))$,
3. *If e'' is a Lubin-Tate power series for a prime π'' of A_E, then* $[ab]_{e,e''}(X) = [a]_{e,e'}([b]_{e',e''}(X))$,
4. *If π is a prime of A_K (which is also a prime of A_E,) $e(X) \in A_E[[X]]$, the corresponding Lubin-Tate power series then $\pi \in A^E_{\pi,\pi}$ and* $[\pi]_e := [\pi]_{e,e} = e(X)$.

Proof. These equalities are obtained by verifying in each case that the terms satisfy the conditions of proposition 5.2.5. For instance to check the first equality, let $\mathfrak{L}(X,Y) = a(X+Y)$. As $[a]_{e,e'}(X) \equiv aX \pmod{deg\,2}$ and $F_e \equiv X+Y \equiv F_e^{\varphi_K} \pmod{deg\,2}$, we see that we have $[a]_{e,e'} \circ F_e \equiv F^{\varphi_K} \circ [a]_{e,e'} \equiv \mathfrak{L} \pmod{deg\,2}$. Next, $e' \circ [a]_{e,e'} \circ F_e = [a]_{e,e'}^{\varphi_K} \circ e \circ F_e = ([a]_{e,e'} \circ F_e)^{\varphi_K} \circ e$. Similarly, one gets $e' \circ F_{e'} \circ [a]_{e,e'} = (F_{e'} \circ [a]_{e,e'})^{\varphi_K} \circ e$. □

Corollary 5.2.8. *We have an injective ring homomorphism*

$$A_K \to End_{A_E}(F_e), a \mapsto [a]_e := [a]_{e,e}.$$

Proof. The first three equations in proposition 5.2.7 show that this is a well defined ring homomorphism and the property $[a]_e \equiv aX \pmod{deg\,2}$ implies injectivity. □

This leads to the following concept of *formal Lubin-Tate module*. It is precisely defined as follows.

Definition 5.2.9. For any local field K a *formal A_K-module* is a couple $\mathfrak{F} = (F(X,Y),[.])$ where F is a formal group law over A_K and $[.]$ is a ring homomorphism:

$$\begin{array}{rcl} A_K & \to & \mathrm{End}_{A_K}(F) \\ a & \mapsto & [a](X) \end{array}$$

such that $[a](X) \equiv aX \pmod{deg\ 2}$. When a prime $\pi \in A_K$ is fixed, then it is called a *formal Lubin-Tate module* over A_K for the prime π if in addition $[\pi](X) \equiv X^q \pmod{\pi}$ with $q = card(k_K)$.

When F defines a group law on a set S as it is the case for the prime ideal of a discrete valuation ring, then we can defines on S a module structure as follows. For $s \in S$, $a \in A_K$ the action of a is defined by $a.s := [a](s)$, in the case where $[a](s)$ converges.

Example 5.2.10. (The case $\mathbf{K = Q_p}$) Let p be a rational prime number as usual, take $e(X) = (1+X)^p - 1 \in \mathbb{Z}_p[X]$, a Lubin-Tate polynomial for p. E is the completion of the maximal unramified extension of $\mathbb{Q}_p$. Let $G_m(X,Y) = (1+X)(1+Y) - 1 \in \mathbb{Z}_p[X,Y]$ be the multiplicative formal group law defined over $\mathbb{Z}_p$. Then

$$e \circ G_m(X,Y) = (1+X)^p(1+Y)^p - 1 = G_m(e(X), e(Y)).$$

So, G_m is the Lubin-Tate formal group law over $\mathbb{Z}_p$ corresponding to e. For any $n \geq 1$, let us define $[n](X) := (1+X)^n - 1 \in \mathbb{Z}[X]$. It is also clear that we have $e \circ [n] = [n] \circ e$. Now any $a \in \mathbb{Z}_p$ is the limit of a sequence of integers $\{a_i\}$. One then defines $[a](X) := (1+X)^a - 1 = \lim_{i \to \infty} (1+X)^{a_i} - 1 = \sum_{i=1}^{\infty} \binom{a}{i} X^i$

with $\binom{a}{i} = \frac{a(a-1)\cdots(a-i+1)}{i!} \in \mathbb{Z}_p$, the extension of the binomial coefficient to $\mathbb{Z}_p$. For each i we have that $e \circ [a_i] = [a_i] \circ e$ and by continuity one has that $e \circ [a] = [a] \circ e$. This says that $[a] \in End_{\mathbb{Z}_p}(G_m)$, and moreover $\mathcal{F} = (G_m(X,Y), [.])$ defines a formal Lubin-Tate module for p. Let us denote by A the completion of the ring of algebraic integers over $\mathbb{Z}_p$. Put $\mathfrak{m}_A = \{a \in A : v(a) > 0\}$ with v the extension of the p-adic valuation to A. Then one endowed $\mathfrak{m}_A$ with a structure of $\mathbb{Z}_p$-module by $a.x = [a](x) = (1+x)^a - 1$. This $\mathbb{Z}_p$-module has torsion points and for $n \geq 1$ the p^n-torsion points are :

$$\{\zeta : [p^n](\zeta - 1) = 0\} = \{\zeta : \zeta^{p^n} = 1\}.$$

So, we see that adjoining p^n-th root of unity to $\mathbb{Q}_p$ amounts to adjoining p^n-torsion points of the $\mathbb{Z}_p$-module $\mathfrak{m}_A$.

We shall next see that this construction can be carried in a more general context. More precisely adjoining torsion points on Lubin-Tate modules to a complete unramified extension L/K of a local field K is the main construction that we shall study now.

5.3 Relative Lubin-Tate extensions

Let p be a rational prime number and let $n \geq 1$ be an integer. To obtain totally ramified extensions of $\mathbb{Q}_p$, one adjoins *p^n-th* roots of unity. We saw that these are roots of an Eisenstein polynomial over $\mathbb{Q}_p$ and also that the Galois groups are isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^*$, see example 4.2.9. The content of this section is to see how the theory of formal group laws is used to generalize that situation. Any local field in the sequel is of characteristic zero.

Let L/K be a complete unramified extension of a local field K and Galois. We can think of L as the completion of the maximal unramified extension of K or a finite extension of K. Let $e(X) \in A_L[X]$ be a Lubin-Tate polynomial for a prime π of A_L and let φ_K be the Frobenius of $Gal(K^{ur}/K)$. For $m \geq 1$, form the polynomial $e_m = e^{\varphi_K^{m-1}} \circ \cdots \circ e^{\varphi_K} \circ e$. Let $h_m(X) = e_m(X)/e_{m-1}(X) = e^{\varphi_K^{m-1}}(e_{m-1}(X))/e_{m-1}(X)$.

Lemma 5.3.1. *$h_m(X)$ is an Eisenstein polynomial of degree $(q-1)q^{m-1}$. Furthermore $h_m(X)$ is irreducible and separable over L.*

Proof. Let $j(X) = e^{\varphi_K^{m-1}}(X)/X$, then as $e^{\varphi_K^{m-1}}(X) \equiv \pi^{\varphi_K^{m-1}} X \pmod{deg\ 2}$, we have $j(X) \equiv \pi^{\varphi_K^{m-1}} \pmod{deg\ 1}$. Since $h_m(X) = j(e_{m-1}(X))$, the claims follow by noting that $j(X) \equiv X^{q-1} \pmod{\pi}$ and recalling that in characteristic zero irreducibility implies separability. □

As a consequence we next obtain that the polynomial $e_m(X) \in A_L[X]$ is separable. This follows from the separability of the Lubin-Tate polynomial $e(X)$.

Lemma 5.3.2. *$e(X)$ is separable over A_L. Furthermore $e_m(X)$ is also separable.*

Proof. By definition of $e(X)$, it is a polynomial of degree q satisfying $e(X) \equiv X^q \pmod{\pi}$ and $e(X) \equiv \pi X \pmod{deg\ 2}$. Hence, $e(X)/X$ is an Eisenstein polynomial, so it is irreducible and since we are in characteristic zero it is separable. By $e(X) = Xe(X)/X$, we deduce that $e(X)$ is separable. We get the separability of $e_m(X)$ by induction on m. We just saw the case $m = 1$ as $e_1 = e$. Suppose then e_{m-1} is separable. From $e_m(X) = e_{m-1}(X)h_m(X)$, one deduces the separability of $e_m(X)$ since the product of distinct polynomials all separable is separable. □

Set $\mu_{e,m} = \{\alpha : e_m(\alpha) = 0\}$. Put $L' = L(\mu_{e,m})$, the splitting field of $e_m(X)$.

Definition 5.3.3. The extension L'/L is called a *relative Lubin-Tate extension.*

Proposition 5.3.4. *1. The set $\mu_{e,m}$ is an A_K-module by $+_{F_e}$ and $[.]_e$. For any $\alpha \in \mu_{e,m}$, we have an A_K-module homomorphism:*

$$\psi : A_K \to \mu_{e,m},\ a \mapsto [a]_e(\alpha).$$

It induces an isomorphism of A_K-modules:

$$\begin{array}{rcl} A_K/\mathfrak{m}_K^m & \to & \mu_{e,m} \\ a & \mapsto & [a]_e(\alpha) \end{array}$$

for $\alpha \in \mu_{e,m} \setminus \mu_{e,m-1}$.

2. $L' = L(\alpha)$ where α is a zero of the Eisenstein polynomial $h_m(X) \in A_L[X]$ so that L'/L is totally ramified of degree $(q-1)q^{m-1}$.

Proof. 1. It is easy to see $\mu_{e,1} \subset \mathfrak{m}_{L'}$. Any $\alpha \in \mu_{e,m-i} \setminus \mu_{e,m-i-1}$ is a zero of the Eisenstein polynomial $h_{m-i}(X) \in A_L[X]$ for $0 \le i \le m-2$. Thus $\alpha \in \mathfrak{m}_{L'}$. Writing $\mu_{e,m} = \bigcup_{i=0}^{m-2} \mu_{e,m-i} \setminus \mu_{e,m-i-1} \bigcup \mu_{e,1}$, we obtain $\mu_{e,m} \subset \mathfrak{m}_{L'}$. Therefore, $[a]_e(\alpha)$, $F_e([a]_e(\alpha), [a]_e(\beta)) \in \mu_{e,m}$ for $\alpha,\ \beta \in \mu_{e,m}$ and $a \in A_K$. Indeed by induction one has $e_m \circ [a]_e = [a]_e \circ e_m$ and $e_m \circ F_e = F_e \circ e_m$. Hence $(e_m \circ [a]_e)(\alpha) = [a]_e(e_m(\alpha)) = [a]_e(0) = 0$. Similarly $e_m \circ F_e([a]_e(\alpha),\ [a]_e(\beta)) = F_e(e_m([a]_e(\alpha), e_m([a]_e(\beta))) = F_e(0,\ 0) = 0$.
Now, from proposition 5.2.5, we obtain $e(X) = [\pi]_e(X)$. Thus $e_m(X) = [\pi^{\varphi_K^{m-1}+\cdots+\varphi_K+1}]_e(X) = [u\pi_K^m]_e(X)$ with $u \in A_L^*$. Writing $e_m(X) = [u]_e(X) \circ [\pi_K^m]_e(X)$, one sees that: $e_m(\alpha) = 0 \iff [\pi_K^m]_e(\alpha) = 0$. This means that any $\alpha \in \mu_{em} \setminus \mu_{e,m-1}$ is exactly annihilated by $[\pi_K^m]_e(X)$, that is to say $[\pi^k]_e(\alpha) \neq 0$ for $1 \le k \le m-1$. This implies that the

induced homomorphism has kernel $\mathfrak{m}_K^m$ and hence the isomorphism follows. This ends the proof of the first part of the proposition.

2. We have $L' = L(\mu_{e,m})$. As $\mu_{e,m} = \{[a]_e(\alpha) : a \in A_K\}$, for any $\alpha \in \mu_{e,m} \setminus \mu_{e,m-1}$, it follows that $L' = L(\alpha)$, with α a root of the Eisenstein polynomial $h_m(X)$. Therefore L'/L is totally ramified of degree $deg(h_m) = (q-1)q^{m-1}$.

□

Let $\alpha \in \mu_{e,m} \setminus \mu_{e,m-1}$ be fixed. The Galois group $Gal(L'/L)$ is computed as follows. By Galois theory we have $Gal(L'/L) \subset Aut(\mu_{e,m}) \cong Aut(A_K/\mathfrak{m}_K^m) \cong (A_K/\mathfrak{m}_K^m)^*$ where $[u]_e(\,.\,) \in Aut(\mu_{e,m})$ maps to $u \in (A_K/\mathfrak{m}_K^m)^*$. This homomorphism is clearly onto and since $card(Gal(L'/L)) = (q-1)q^{m-1} = card((A_K/\mathfrak{m}_K^m)^*)$, one has an isomorphism:

$$\begin{array}{rcl} \rho_{e,m} : Gal(L'/L) & \to & (A_K/\mathfrak{m}_K^m)^* \\ (\sigma : \sigma(\alpha) = [u]_e(\alpha)) & \mapsto & u. \end{array}$$

This isomorphism does not depend on the choice of a primitive element $\alpha \in \mu_{e,m} \setminus \mu_{e,m-1}$. Indeed, let $\sigma(\alpha) = [u]_e(\alpha)$ and $\alpha' = [u']_e(\alpha)$ be a conjugate of α. Note that $[u]_e(X) \in A_L[[X]]$ and hence $\sigma([u']_e(\alpha)) = [u']_e(\sigma(\alpha)) = [u']_e([u]_e(\alpha)) = [u]_e([u']_e(\alpha))$. We have proved the following

Proposition 5.3.5. *The Galois group $Gal(L'/L)$ is isomorphic to $(A_K/\mathfrak{m}_K^m)^*$. The isomorphism being given by $\rho_{e,m} : Gal(L'/L) \to (A_K/\mathfrak{m}_K^m)^*$; $[u]_e(.) \mapsto u \pmod{\mathfrak{m}^m}$ and is independent of α.*

5.3.1 Isomorphism of Lubin-Tate extensions

Let $E = \hat{K}^{ur}$, be the completion of the maximal unramified extension of K. Let $e(X), e'(X) \in A_E[[X]]$ be Lubin-Tate power series for the primes $\pi,\ \pi' \in A_E$ respectively. Let $F_e(X,Y), F_{e'}(X,Y) \in A_E[[X,Y]]$ be the formal group laws corresponding to $e(X), e'(X)$ respectively. For $a \in A^E_{\pi,\pi'} = \{a \in A_E : \pi' a = \pi a^{\varphi_K}\}$, consider $[a]_{e,e'}(X) \in A_E[[X]] \in \mathrm{Hom}(F_e, F_{e'})$. Finally, φ_K denotes the extension of the Frobenius automorphism of $Gal(K^{ur}/K)$ to E.

We first prove that in this setting, the Lubin-Tate formal group laws $F_e, F_{e'}$ over E are in fact isomorphic.

Lemma 5.3.6. *The map*

$$\begin{array}{rcl} \psi : A_E^* & \to & A_E^* \\ u & \mapsto & u^{\varphi_K}/u \end{array}$$

is surjective.

Proof. As $A_E^* \cong \lim_{\leftarrow m}(A_E/\mathfrak{m}_E^{m+1})^*$, it suffices to verify that for $v \in A_E$ and for all $m \geq 0$, there exists u_m such that $u_m^{\varphi_K}/u_m \equiv v \pmod{\pi_E^{m+1}}$. When $m = 0$, then $(A_E/\mathfrak{m}_E)^* \cong \overline{\mathbb{F}}_q^*$. Thus $\bar{\psi}(\bar{u}) = \bar{u}^{\varphi_K}/\bar{u} = \bar{u}^{q-1}$, and this is a surjective map as we are in the algebraic closure of $\mathbb{F}_p$. Suppose then that we have found u_m such that $v/(u_m^{\varphi_K}/u_m) = 1+\alpha\pi_K^{m+1}$ with π_K a prime of K and $\alpha \in A_E$. On $A_E/\mathfrak{m}_E \cong \overline{\mathbb{F}_q}$, the map $\bar{u} \mapsto u^{\bar{\varphi}_K} - \bar{u} = \bar{u}^q - \bar{u}$ is surjective so that there exists $\beta \in A_E$ such that $\beta^{\varphi_K} - \beta \equiv \alpha \pmod{\mathfrak{m}_E}$. Then, setting $u_{m+1} = u_m(1 + \beta\pi^{m+1})$, gives $u_{m+1}^{\varphi_K}/u_{m+1} \equiv v \pmod{\mathfrak{m}_E^{m+2}}$. □

This gives

Proposition 5.3.7. *Let $e, e', F_e, F_{e'}$ be as above. Then $a \in A_{\pi,\pi'}^E \bigcap A_E^*$ gives rise to an isomorphism of the Lubin-Tate formal group laws over E :*

$$[a]_{e,e'} : F_e \cong F_{e'}.$$

Proof. We know that $[a]_{e,e'} \equiv aX \pmod{deg\ 2}$. Hence $[a]_{e,e'} \in XA_E[[X]]$ is invertible, and so the homomorphism $[a]_{e,e'}$ is an isomorphism over E. □

The extension L/K is still complete unramified inside E. As a prime in L is also a prime in E, a Lubin-Tate polynomial over A_L is also a Lubin-Tate polynomial over A_E.

Next, take $e(X), e'(X) \in A_L[X]$, Lubin-Tate polynomials for the primes $\pi, \pi' \in L$ and $[a]_{e,e'} \in Hom_E(F_e, F_{e'})$. An isomorphism $[a]_{e,e'} : F_e \cong F_{e'}$ over E gives rise to an isomorphism of A_K-modules $\mu_{e,m},\ \mu_{e',m}$ as follows. For $a \in A_{\pi,\pi'}^E \bigcap A_E^*$, we have $[a]_{e,e'}(X) \in A_E[[X]]$ such that $[a]_{e,e'}^{\varphi_K} \circ e = e' \circ [a]_{e,e'}$. Hence for $m \geq 1$, we get $e'_m \circ [a]_{e,e'} = [a]_{e,e'}^{\varphi_K^m} \circ e_m$. Then for $\alpha \in \mu_{e,m}$, we see that $[a]_{e,e'}(\alpha) \in \mu_{e',m}$. Therefore, we have a map:

$$\begin{array}{rcl} [a]_{e,e'} : \mu_{e,m} & \to & \mu_{e',m} \\ \alpha & \mapsto & [a]_{e,e'}(\alpha). \end{array}$$

From the properties of $[a]_{e,e'}(X)$, one deduces that this is a homomorphism of A_K-modules and hence that this is an isomorphism since a is a unit. If in addition we suppose that $[a]_{e,e'}(X) \in A_L[[X]]$, then we have $L(\mu_{e,m}) = L(\mu_{e',m})$ and $\rho_{e,m} = \rho_{e',m}$. Indeed, because L is complete then $L(\mu_{e,m})$ is complete and so $\mu_{e',m} = [a]_{e,e'}(\mu_{e,m}) \subset L(\mu_{e,m})$ so that $L(\mu_{e',m}) \subset L(\mu_{e,m})$. The reverse inclusion follows similarly since $\mu_{e,m} = [a^{-1}]_{e',e}(\mu_{e',m})$. From proposition 5.3.5 and for $\alpha \in \mu_{e,m}$, we have an isomorphism:

$$\begin{array}{rcl} \rho_{e,m} : Gal(L(\mu_{e,m})/L) & \to & (A_K/\mathfrak{m}_K^m)^* \\ (\alpha \mapsto [u]_{e,e'}(\alpha)) & \mapsto & u \pmod{\mathfrak{m}_K^m}. \end{array}$$

Hence, the automorphism $[u]_{e,e'}(\alpha)$ maps to $[u.a]_{e,e'}(\alpha)$ under the isomorphism $[a]_{e,e'}(.) : \mu_{e,m} \cong \mu_{e',m}$. From $[a.u]_{e,e'}(\alpha) = [u]_{e'}([a]_{e,e'}(\alpha))$, one sees

that $\rho_{e,m} = \rho_{e',m}$. Summarizing this discussion we have

Proposition 5.3.8. *Let L/K be a complete unramified extension of a local field K. Let $e(X), e'(X) \in A_L[X]$ be Lubin-Tate polynomials for the primes $\pi, \pi' \in L$ respectively. Let $a \in A^E_{\pi,\pi'} \bigcap A^*_E$ so that $[a]_{e,e'}(X) \in A_E[[X]]$ defines an isomorphism: $F_e \cong F_{e'}$ of formal groups law over A_E. Then we have an isomorphism of A_K-modules*

1. *$[a]_{e,e'}(.) : \mu_{e,m} \cong \mu_{e',m}$, and*
2. *Furthermore if $[a]_{e,e'} \in A_L[[X]]$, then $L(\mu_{e,m}) = L(\mu_{e',m})$ and $\rho_{e,m} = \rho_{e',m}$.*

We now make the hypothesis that the extension L/K is finite inside $E = \hat{K}^{ur}$. The following result gives a criterion that allows one to decide whether $[a]_{e,e'}(X) \in A_L[[X]]$ or not. We need the following. For a Lubin-Tate power series $e(X) \in A_L[[X]]$, the map :

$$\begin{array}{rcl} \cdot \circ e : A_L[[X]] & \to & A_L[[X]] \\ h & \mapsto & h \circ e \end{array}$$

is well defined since $e(0) = 0$.

Lemma 5.3.9. *This map is an injection.*

Proof. Let π be a prime of L and $q = card(k_L)$. The injectivity follows from the statement $h \circ e \equiv 0 \pmod{\pi^m} \Rightarrow h \equiv 0 \pmod{\pi^m}$ for $m \geq 0$. One sees this by induction on m. For $m = 0$, this is clear. Suppose then that this is true up to $m-1$. If $h \circ e = \pi^m g$, then by induction hypothesis $h = \pi^{m-1} h'$ so that $h' \circ e = \pi g$. Reduction modulo π, leads $h'(X^q) \equiv (h'(X))^q \equiv h'(X) \equiv 0 \pmod{\pi}$. This gives $h(X) \equiv 0 \pmod{\pi^m}$. Therefore if $(h_1 - h_2) \circ e \equiv 0 \pmod{\pi^m}$ for $m \geq 0$, one deduces that we must have $h_1 = h_2$ by taking limit. □

Then we can state

Proposition 5.3.10. *Let L/K be a finite unramified extension of degree n. Let $e(X)$, $e'(X)$ be Lubin-Tate polynomials for the primes $\pi, \pi' \in L$ respectively. Let $[a]_{e,e'}(X) \in Isom_{A_E}(F_e, F_{e'})$ and let φ_K be the Frobenius in $Gal(K^{ur}/K)$. Then $[a]^{\varphi^n_K}_{e,e'} = [a]_{e,e'} \circ [N_{L/K}(\pi'/\pi)]_e$. Furthermore, if $N_{L/K}(\pi) = N_{L/K}(\pi')$, then $[a]_{e,e'}(X) \in A_L[[X]]$.*

Proof. By definition of e_n, one has $e_n \equiv \pi^{\varphi_K^{n-1}} \cdots \pi^{\varphi_K} \pi X \equiv N_K(\pi) X \pmod{deg\ 2}$. On one hand, since φ^n_K is the identity on L, one gets $e \circ e_n = e_n \circ e$. On the other, $[N_{L/K}(\pi)]_e$ clearly satisfies: $[N_{L/K}(\pi)]_e \equiv N_{L/K}(\pi) X \pmod{deg 2}$ and $e \circ [N_{L/K}(\pi)]_e = [N_{L/K}(\pi)]_e \circ e$. Hence, $e_n(X) = [N_{L/K}(\pi)]_e(X)$ by proposition 5.2.5. Similarly, one gets $e'_n = [N_{L/K}(\pi')]_{e'}$. As $e' \circ [a]_{e,e'} =$

$[a]_{e,e'}^{\varphi_K} \circ e$, we obtain $e'_n \circ [a]_{e,e'} = [a]^{\varphi_K^n} \circ e_n$. Thus $[a]^{\varphi_K^n} \circ e_n = [N_{L/K}(\pi')]_{e'} \circ [a] = [a.N_{L/K}(\pi')]_{e,e'} = [a]_{e,e'} \circ [N_{L/K}(\pi')]_e = [a]_{e,e'} \circ [N_{L/K}(\pi'/\pi)]_e \circ e_n$. Now to conclude the equality use the above lemma successively for $e, e^{\varphi_K}, \cdots, e^{\varphi_K^{n-1}}$. Next if $N_{L/K}(\pi') = N_{L/K}(\pi)$, then one has $[a]_{e,e'}^{\varphi_K^n} = [a]_{e,e'}$, this means that $[a]_{e,e'}(X) \in A_L[X]$. □

From the above discussion, we see that when L/K is a finite unramified extension, then the Lubin-Tate extensions $L(\mu_{e,m})$ are dependent only on $N_{L/K}(\pi) = x \in K^*$ with π a prime in L defining the Lubin-Tate polynomial $e(X) \in A_L[X]$. So, let us denote $L(\mu_{e,m})$ by K_x^m. The maps $\rho_{e,m}$ depend also only on $N_{L/K}(\pi)$ and so we will write ρ_m for $\rho_{e,m}$.

Let $[L : K] = n$. Let $\pi_K \in K$ be a prime. It is also a prime in L. Now any prime π of L can be written as $\pi = u\pi_K$ with $u \in A_L^*$. Hence $N_{L/K}(\pi) = N_{L/K}(u)\pi_K^n$. Thus we have $v_K(N_{L/K}(\pi)) = n$. So if $x \in K^*$ with $v_K(x) = n$ then we have $x = yN_{L/K}(\pi)$ with $y \in A_K^*$. Next as $N_{L/K}$ maps A_L^* onto A_K^* since L/K is unramified, there is $w \in A_L^*$ with $N_{L/K}(w) = y$. Whence $x = N_{L/K}(w\pi)$. This means that if $x \in K^*$ with $v_K(x) = n$, then there exists a prime $\pi' \in L$ such that $x = N_{L/K}(\pi')$.

For $m, m' \geq 1$, say $m \leq m'$, then $e_m \mid e_{m'}$ and hence $K_x^m \subset K_x^{m'}$. Thus $\bigcup_{m\geq 1} K_x^m$ is a totally ramified extension of L. It is denoted by K_x^{ram}. The canonical projection $Gal(K_x^{m'}/L) \to Gal(K_x^m/L)$ gives rise to the projective system $(Gal(K_x^m/L), m \in \mathbb{N})$. Let us recall also that $Gal(K_x^m) \cong (A_K/\mathfrak{m}_K^m)^*$. This gives rise to an isomorphism:

$$Gal(K_x^{ram}/L) \cong \lim_{\leftarrow m} Gal(K_x^m/L) \cong \lim_{\leftarrow m}(A_K/\mathfrak{m}_K^m)^* \cong A_K^*.$$

For the maximal unramified extension $K^{ur} = \bigcup_{n\geq 1} K_n^{ur}$, where K_n^{ur} is the unique unramified extension of degree n of K, we have $Gal(K_n^{ur}/K) \cong Gal(k_{K_n^{ur}}/k_K) \cong \mathbb{Z}/n\mathbb{Z}$. Then if $n' \mid n$, we have restriction: $Gal(K_n^{ur}/K) \to Gal(K_{n'}^{ur}/K)$. Hence, one has $Gal(K^{ur}/K) \cong \lim_{\leftarrow n} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$, the isomorphism being given by $\varphi_K \leftrightarrow 1$, where φ_K is the Frobenius of $Gal(K^{ur}/K)$. From the equality $L^{ur} = K^{ur}$, one has $Gal(K^{ur}/L) = Gal(L^{ur}/L) = \hat{\mathbb{Z}}$, the isomorphism is given by $\varphi_K^n \mapsto 1$ with $n = [L : K]$.

Now define the extension $K_x^{LT} = K_x^{ram}K^{ur}$ of L. This is an abelian extension of L. Since K_x^{ram}/L is totally ramified and K^{ur}/L is unramified, one sees that $K^{ram} \bigcap K^{ur} = L$. Therefore by Galois theory we have

$$\begin{array}{ccccc} Gal(K_x^{LT}/L) \cong Gal(K^{ram}/L) & \times & Gal(K^{ur}/L) \cong A_K^* \times \hat{\mathbb{Z}} \\ (\alpha \mapsto [u](\alpha),\ \varphi_L^b) & \mapsto & (u, b). \end{array}$$

Then a map $N_{L/K}(L^*) = A_K^* \times < x > \to Gal(K_x^{LT}/K)$ is defined as follows.

Definition 5.3.11. (Artin maps) The *Artin map* associated to x and

denoted by Art_K^x is the map:

$$Art_K^x : N_{L/K}(L^*) \to Gal(K_x^{LT}/K)$$

with $Art_K^x(ux^b)$ acting as $[u^{-1}]$ on each K_x^m and like φ_L^b on K^{ur} where φ_L is the Frobenius in $Gal(L^{ur}/L)$ which is φ_K^n with $n = [L : K]$ and φ_K the Frobenius in $Gal(K^{ur}/K)$.

Remark 5.3.12. *Using $[u^{-1}]$ and not $[u]$ is precisely because we want it to be independent of x.*

In what follows, we will see that the extension $K_x^m K^{ur}$ is independent of the choice of x with $v_K(x) = n = [L : K]$ and that the Artin map Art_K^x is independent of x and is a restriction of a certain map $Art_K : K^* \to Gal(K^{LT}/K)$. On the way to these statements we need the following lemma.

Lemma 5.3.13. *Let K be a local field with K^{al} as algebraic closure. Let S be any extension of K inside K^{al}. Lastly, let E', E'' be algebraic extensions of S. Then the following holds*

1. *If E'/S is finite then $E'\hat{S} = \hat{E'}$,*
2. *$\hat{S} \bigcap E' = S$,*
3. *$\hat{E'} = \hat{E''} \Rightarrow E' = E''$.*

Proof. 1. Let E'/S be finite. Therefore $E'\hat{S}/\hat{S}$ is finite. Hence $E'\hat{S}$ is complete in $\hat{K^{al}}$, the completion of the algebraic closure of K, by recalling that a finite extension of a complete field is also complete. Then $E'\hat{S} = \hat{E'\hat{S}} = \hat{E'}\hat{S} = \hat{E'}$.

2. To prove $\hat{S} \cap E' = S$, we can assume that the extension E'/S is finite Galois. Indeed, we can take the normal closure R of E'/S and verify that $R \cap \hat{S} = S$. So, let E'/S be Galois so that $E'\hat{S}/\hat{S}$ is also Galois. Now any automorphism $\sigma \in Gal(E'/S)$ can be extended uniquely by continuity to an automorphism $\hat{\sigma} \in Gal(\hat{E'}/\hat{S})$. Therefore

$$[E' : S] \leq [\hat{E'} : \hat{S}] = [E'\hat{S} : \hat{S}] = [E' : \hat{S} \cap E'].$$

This means that $\hat{S} \cap E' = S$. Now if E'/S is an infinite extension we can write $E' = \cup E_i$ with E_i/S finite so that $\hat{S} \bigcap E_i = S$. Then $\hat{S} \bigcap E' = \bigcup(\hat{S} \cap E_i) = S$.

3. Applying the second part to $E'E''$, E', and E'', one has $E'E'' \bigcap \hat{E'} = E'$, and $E'E'' \bigcap \hat{E''} = E''$. Thus, the condition $\hat{E'} = \hat{E''}$ implies $E' = E''$.

□

Then

Theorem 5.3.14. *1. The fields $K_x^m K^{ur}$ for $m \geq 1$ and hence their union K_x^{LT} are independent of the choice of $x \in \mathfrak{m}_K \cap K^*$ with $v_K(x) = n$.*

2. The Artin map Art_K^x is independent of x with $v_K(x) = n$. Furthermore if $v_K(x) = 1$, then $Art_K^x =: Art_K : K^* \to Gal(K^{LT}/K)$ is such that for $y \in K^*$ with $v_K(y) = n$, we have $Art_K^y = Art_K|_{N_{L/K}(L^*)}$ with L/K the finite unramified extension of degree n.

Proof. 1. Let x, $x' \in K^*$ with $v_K(x) = v_K(x') = n$, and let π, π' be primes in L such that $N_{L/K}(\pi) = x$ and $N_{L/K}(\pi') = x'$. We consider also the Lubin-Tate polynomials $e(X)$, $e'(X) \in A_L[X]$ for π and π' respectively. We write also $\mu_{e,m}$, $\mu_{e',m}$ for the set of roots of the polynomials $e_m(X)$, $e'_m(X)$ as defined before lemma 5.3.1, p 61. By proposition 5.3.7, p 64, there exists an isomorphism $[a]_{e,e'} : \mu_{e,m} \cong \mu_{e',m}$, so that $\mu_{e',m} = [a]_{e,e'}(\mu_{e,m})$ where $[a]_{e,e'}(X) \in \hat{K^{ur}}[[X]]$. We have $K_{x'}^m = L(\mu_{e',m})$ so that $K_{x'}^m \hat{K^{ur}} = \hat{K^{ur}}(\mu_{e',m})$. Similarly one obtains that $K_x^m \hat{K^{ur}} = \hat{K^{ur}}(\mu_{e,m})$. Then since we have $\mu_{e',m} = [a]_{e,e'}(\mu_{e,m})$ with $[a]_{e,e'}(X) \in \hat{K^{ur}}[X]$, one deduces that $\hat{K^{ur}}(\mu_{e',m}) = \hat{K^{ur}}(\mu_{e,m})$. Now $K_{x'}^m K^{ur}/K^{ur}$ is a finite extension so by applying the first part of lemma 5.3.13 we have $K_{x'}^m K^{ur} \hat{K^{ur}} = (\hat{K_{x'}^m K^{ur}}) = \hat{K^{ur}}(\mu_{e',m})$. Similarly we have $K_x^m K^{ur} \hat{K^{ur}} = (\hat{K_x^m K^{ur}}) = \hat{K^{ur}}(\mu_{e,m})$. So, the fields K_x^m and $K_{x'}^m$ have the same completion. From the last part of lemma 5.3.13, we obtain $K_x^m K^{ur} = K_{x'}^m K^{ur}$. This means that $K_x^m = K_{x'}^m$.

2. We are still in the same setting. We need to show that $Art_K^x(x') = Art_K^{x'}(x')$. By definition $Art_K^x(x')$ acts as φ_K^n on K^{ur} where φ_K the Frobenius of $Gal(K^{ur}/K)$. So, we have that $Art_K^x = Art_K^{x'}$ on K^{ur}. Next we prove that $Art_K^x(x')$ is the identity on $K_{x'}^{ram}$. To this end, let $[a]_{e,e'}(X) = \sum a_i X^i \in \hat{K^{ur}}[[X]]$ and write $x' = \frac{x'}{x} x = ux$. Then, by definition $Art_K^x(x')$ acts as $\alpha \mapsto [u^{-1}]_e(\alpha)$ with $\alpha \in \mu_{e,m} \setminus \mu_{e,m-1}$. Hence, we have $Art_K^x(x')([a]_{e,e'}(\alpha)) = \sum Art_K^x(x')(a_i)(Art_K^x(x')(\alpha))^i = \sum a_i^{\varphi_K^n}([u^{-1}]_e(\alpha))^i = ([a]_{e,e'}^{\varphi_K^n} \circ [u^{-1}]_e)(\alpha)$. From proposition 5.3.10, we obtain

$$Art_K^x(x')([a]_{e,e'}(\alpha)) = ([a]_{e,e'} \circ [u]_e \circ [u^{-1}]_e)(\alpha) = [a]_{e,e'}(\alpha).$$

Thus, $Art_K^x(x')$ is the identity on $K_{x'}^{ram}$ since it is so on $\mu_{e',m}$ for all $m \geq 1$. Similarly for any $x'' \in K^*$ with $v_K(x'') = n$, we obtain $Art_K^{x'}(x'') = Art_K^{x''}(x'') = Art_K^x(x'')$, that is $Art_K^x = Art_K^{x'}$. Now, if $v_K(x) = 1$, we have $K_x^m = K(\mu_{e,m})$. Then for an unramified extension L/K of degree $n = v_K(x^n)$, one gets $K_{x^n}^m = L(\mu_{e,m}) = K_x^m L$ and from the definition of the Artin maps we have $Art_K^{x^n} = Art_K^x|_{N_{L/K}(L^*)}$.

□

Having this at hand we make the following definition.

Definition 5.3.15. 1. Let π be a prime of K and let φ_K be the Frobenius automorphism in $Gal(K^{ur}/K)$. The *Artin map* of K is the homomorphism

$$\begin{array}{rcl} Art_K : K^* & \to & Gal(K^{LT}/K) \\ u\pi^l & \mapsto & [u^{-1}]_e \varphi_K^l. \end{array}$$

2. Let E/K be an algebraic extension that contains K^{ur}. The *Weil group* $W(E/K)$ of the extension E/K is

$$W(E/K) = \{\sigma \in Gal(E/K) : \sigma|_{K^{ur}} \in \varphi_K^{\mathbb{Z}}\}.$$

Then theorem 5.3.14 has the following corollary.

Corollary 5.3.16. *If $x \in K^*$, then $\sigma = Art_K(x) \in Gal(K^{LT}/K)$ is characterized by $\sigma|_{K^{ur}} = \varphi_K^{v_K(x)}$ and $\sigma|_{K_x^{ram}} = 1$. By the Artin map we have $Art_K : K^* \to W(K^{LT}/K)$ isomorphically.*

Proof. The first statement is just a rewriting of the definition of the Artin map. The last statement is clear from the definition of the Weil group and the fact that for $x \in K^*$, $Art_K(x)|_{K^{ur}} = \varphi_K^{v_K(x)}$. □

Next come the classical theorems for local class field theory.

5.4 Local class field theory

Let K be local field, we prove that by the Artin map $Art_K : K^* \to Gal(K^{LT}/K)$, one classifies the abelian extensions of K. To this end, we first establish that the extension K^{LT} is in fact the abelian closure of K. This is the local Kronecker-Weber theorem for K.

5.4.1 The local Kronecker-Weber theorem

We follow here a classical argument that uses the Hasse-Arf theorem . So, let us start by recalling the statement of the said theorem.

Let F/K be a Galois extension of local fields with Galois group G. Let G_i be the ramification groups in the lower numbering and the let $\psi_{F/K}(s) = \frac{1}{g_0}(g_1 + \cdots + g_m + (s-m))$ with $s \in [-1, \infty)$, $0 < m \leq s \leq m+1$ and $g_i = card(G_i)$, be the real valued function associated with the groups G_i as defined in 4.2.15, p 46. Recall also that the ramification groups in upper number numbering are $G^m = G_{\psi_{F/K}^{-1}(m)}$. Then the Hasse-Arf theorem reads as follows.

Theorem 5.4.1. *(***Hasse-Arf***) If G is abelian, $n \in \mathbb{Z}_{\geq 0}$ and $G_n \neq G_{n+1}$, then $\psi_{F/K}(n) \in \mathbb{Z}_{\geq 0}$.*

Proof. See [20], or [25]. □

We also need the following result concerning the computation of the ramification groups in upper numbering of the totally ramified extensions K_x^m/K for $m \geq 1$.

Proposition 5.4.2. *Let G be the Galois group of the extension K_x^m/K for $m \geq 1$. Then*

1. $G_0 = G$, $G_1 = G_2 = \cdots = G_{q-1}$, $G_q = \cdots = G_{q^2-1}$, $\cdots$, $G_{q^m-1} = 1$;
2. $G^0 = G_0$, $G^1 = G_{q-1}$, $\cdots, G^m = G_{q^m-1} = 1$.

Proof. See [17, pp 31-32]. □

We will make use as well of the

Proposition 5.4.3. *1. Let G be the Galois group of a totally ramified abelian extension of local fields F/K, and let $q = card(k_K)$ where k_K is the residue field of K. Then $(G : G^m)$ divides $(q-1)q^{m-1}$ with m a positive integer.*

2. Let K'/K and K''/K be two Galois extensions with $K'K''/K$ totally ramified. If $Gal(K'/K)^m = Gal(K''/K)^m = 1$, then $Gal(K'K''/K)^m = 1$.

Proof. 1. We write ψ for $\psi_{F/K}$. Recall first that we have embeddings $G_0/G_1 \hookrightarrow k_K^*$, and $G_i/G_{i+1} \hookrightarrow k_K$ for $i \geq 1$, see 4.2.17, p 47. As $G^m = G_{\psi^{-1}(m)}$, we know that for $n \in \mathbb{Z}_{\geq 0}$ if $n-1 < \psi^{-1}(m) \leq n$, i.e., $\psi(n-1) < m \leq \psi(n)$ (ψ is an increasing function), then $G^m = G_n$. As $(G : G_n) = (G : G_1)(G_1 : G_2) \cdots (G_{n-1} : G_n)$, by the Hasse-Arf theorem, if $1 \leq i \leq n$, then $G_{i-1} \neq G_i$ occurs only when $\psi(i-1) \in \mathbb{Z}_{\geq 0}$. $(G : G_1)$ divides $q-1$ and for $i \geq 2$ we have that $G_{i-1} \neq G_i$ occurs at most $m-1$ times as $\psi(i-1) \leq \psi(n-1) < m$. Hence as $(G_{i-1} : G_i)$ divides q we see that $(G : G^m)$ divides $(q-1)q^{m-1}$.

2. Put $S = Gal(K'K''/K)$ and let $H = Gal(K'K''/K'')$ so that $Gal(K''/K) = S/H$. We know that $S^m H/H = (S/H)^m = 1$, hence $S^m \subset H = Gal(K'K''/K'')$. Similarly $S^m \subset Gal(K'K''/K')$. Thus $S^m \subset Gal(K'K''/K') \bigcap Gal(K'K''/K'') = 1$.

□

Let now π be a prime of a local field K and consider the extension $K_\pi^{ram} = \bigcup_{m \geq 1} K_\pi^m$.

Lemma 5.4.4. *K_π^{ram} is a maximal totally ramified extension of K inside K^{ab}.*

Proof. Let E be an intermediate field of K^{ab}/K_π^{ram} and totally ramified over K. As each finite subextension E' of E/K is totally ramified, we have to show that $E' \subset K_\pi^m$ for some $m \geq 1$. So, let E'/K as said with $G = Gal(E'/K)$. For m large enough we have $G^m = \{id\}$. Combining this with proposition 5.4.2, 2., and 5.4.3, 2., one gets $Gal(E'K_\pi^m)^m = 1$. From proposition 5.4.3, 1., we have $[E'K_\pi^m : K] \mid (q-1)q^{m-1} = [K_\pi^m : K]$. Therefore $E' \subset K_\pi^m$. □

Then we have the following statement.

Theorem 5.4.5. (Local Kronecker-Weber theorem) *Every abelian extension of a local field K lies inside K^{LT}, i.e., $K^{LT} = K^{ab}$.*

Proof. Let φ_K be the Frobenius element of $Gal(K^{ur}/K)$, and let $\sigma \in Gal(K^{ab}/K)$ be any extension of φ_K. Set F the fixed field of σ. By definition $F \bigcap K^{ur} = K$, hence F/K is totally ramified. The rule $Gal(K^{ab}/F) \to \hat{\mathbb{Z}}, \sigma \mapsto 1$ gives an isomorphism $Gal(K^{ab}/F) \cong \hat{\mathbb{Z}}$. In fact, it is easy to see that $Gal(K^{ab}/F) \cong Gal(K^{ur}/K)$ by mapping σ to φ_K. Since $\hat{\mathbb{Z}}$ has a unique closed subgroup of index n, namely $n\hat{\mathbb{Z}}$, there exits only one intermediate field of K^{ab}/F of degree n. Since $F \bigcap K^{ur} = F \bigcap K_n^{ur}$ where K_n^{ur} is the unique unramified extension of degree n over K, FK_n^{ur}/F is the subextension of degree n over F. Hence we obtain $K^{ab} = \bigcup_{[F':F]<\infty} F'/F = \bigcup_{n\geq 1} FK_n^{ur} = FK^{ur}$. One the other hand, let π be a prime of K. By definition $Art_K(\pi)|_{K^{ur}} = \varphi_K$, and $Art_K(\pi)|_{K_\pi^{ram}} = id$. Thus one sees that $K_\pi^{ram} \subset F$, which implies $F = K_\pi^{ram}$ by the maximality of K_π^{ram}. □

5.4.2 The theorems of local class field theory

For a local field K, we have $Art_K : K^* \to Gal(K^{ab}/K)$. Let K'/K be an extension of local fields. Obsverve that $K^{ab} \subset K'^{ab}$ so that the restriction map $res : Gal(K'^{ab}/K') \to Gal(K^{ab}/K)$ is well defined. We shall next see how the Artin map behaves with respect to a change of the ground field from K to K'. We begin with the following result concerning the norm group of the extension K_x^m/K. So let L/K be a finite unramified extension and π a prime of L with $x = N_{L/K}(\pi)$ so that $v_K(x) = [L : K]$. Also for an infinite extension E/K we write $N(E/K)$ to denote $\cap N_{E_i/K}(E_i^*)$ with E_i/K finite subextensions of E/K.

Lemma 5.4.6. *Let K be a local field and let $x \in K^*$ as above. Then $N_{K_x^m/K}((K_x^m)^*) = (1 + \mathfrak{m}_K^m) \times < x >$. Furthermore, if E/K is a totally ramified extension and $E \supset K_x^{ram}$, then $N(E/K) =< x >$.*

Proof. See [25, p 11]. □

Theorem 5.4.7. *Let K'/K be an extension of local fields. The following diagram is commutative:*

$$\begin{array}{ccc} K'^{*} & \xrightarrow{Art_{K'}} & Gal(K'^{ab}/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle res} \\ K^{*} & \xrightarrow{Art_{K}} & Gal(K^{ab}/K) \end{array}$$

Proof. Let π' be a prime of K', and let φ' be the Frobenius of K'^{ur}. By definition of $Art_{K'}(\pi') \in Gal(K'^{ab}/K')$ it verifies $Art_{K'}(\pi')|_{K'^{ur}} = \varphi'_{K'}$ and $Art_{K'}(\pi')|_{K'^{ram}_{\pi'}} = 1$. Hence the fixed field of $Art_{K'}(\pi')$ is K'^{ram}_{π}. As $K'^{ram}_{\pi'}/K'$ is totally ramified, from lemma 5.4.6, $N(K'^{ram}_{\pi'}/K') =< \pi' >$. Therefore by the transitivity of the norm we have $N(K'^{ram}_{\pi'}/K) =< N_{K'/K}(\pi') >$. Then set $\pi = Art_K^{-1}(Art_{K'}(\pi')|_{K^{ab}}) \in K^*$ and let L be the maximal unramified subextension of K'/K i.e., $L = K' \bigcap K^{ur}$. As $K'^{ram}_{\pi'}/L$ is totally ramified and $K^{ram}_{\pi} \subset K'^{ram}_{\pi'}$ (by the maximality of $K'^{ram}_{\pi'}$), from lemma 5.4.6 we get $N(K'^{ram}_{\pi'}/K) =< \pi >$. Hence as π and $N_{K'/K}(\pi')$ generate the same group, they must be associate. By changing the prime π if necessary we may write $\pi = N_{K'K}(\pi')$. Thus $Art_{K'}(\pi')|_{K^{ab}} = Art_K(N_{K'/K}(\pi'))$. Now use the fact that as a group K'^{*} is generated by the primes to conclude that $Art_{K'} \circ res = Art_K \circ N_{K'/K}$. □

By theorem 5.4.7, we see that if K'/K is a finite abelian extension then $Art_K(N_{K'/K}K'^{*})|_{K'} = 1$. We also know that for a prime $\pi \in K^*$ we have $Art_K(\pi)|_{K^{ur}} = \varphi_K$ with φ_K the Frobenius of $Gal(K^{ur}/K)$ and $Art_K(\pi)|_{K^{ram}_{\pi}}$
$= 1$. Now suppose that we have $\psi : K^* \to Gal(K^{ab}/K)$ another homomorphism satisfying all these properties. Let $\pi \in K$ be a prime and consider the extension K^{ram}_{π}. Then $\pi \in N(K^{ram}_{\pi}/K)$ so that $Art_K(\pi)|_{K^{ram}_{\pi}} = 1$ by definition. This means that $Art_K(\pi)|_{K^{ur}} = \varphi_K = \psi(\pi)|_{K^{ur}}$ and also $Art_K(\pi)|_{K^{ram}_{\pi}} = 1 = \psi(\pi)|_{K^{ram}_{\pi}}$. Therefore, one has $Art_K(\pi) = \psi(\pi)$. Since K^* is generated by the primes as a group we conclude that $Art_K = \psi$. In other words the homomorphism $Art_K : K^* \to Gal(K^{ab}/K)$ is uniquely characterized by:

$$Art_K(N_{K'/K}K'^{*})|_{K'} = 1 \text{ and } Art_K(\pi)|_{K^{ur}} = \varphi_K.$$

We also have

Theorem 5.4.8. *Let K'/K be a finite extension of local fields. Then we have an isomorphism*

$$K^*/N_{K'/K}(K'^{*}) \cong Gal((K' \cap K^{ab})/K).$$

Proof. We have $Art_K : K^* \cong W(K^{ab}/K)$ and $K'^{*} \cong W(K'^{ab}/K')$ by Art'_K

as well. Therefore, one has $K^*/N_{K'/K}(K'^*) \cong W(K^{ab}/K)/res(W(K'^{ab}/K'))$. Next observe that we have a surjection $res : W(K^{ab}/K) \twoheadrightarrow Gal((K' \cap K^{ab})/K)$ with kernel $res(W(K'^{ab}/K'))$. Indeed $H = Gal(K' \cap K^{ab}/)$ is finite and every $\sigma \in H$ extends to an element in $Gal(K^{ab}/K)$ whose restriction to K^{ur} lies in $< \varphi_K >$ an so we have surjectivity. Now any $\sigma \in res(W(K'^{ab}/K'))$ maps to identity in H since it fixes K', and any $\tau \in W(K^{ab}/K)$ that fixes $K' \cap K^{ab}$ is a restriction of some element in $W(K'^{ab}/K')$ so lies in $res(W(K'^{ab}/K'))$. This ends the proof. □

Putting together these results, we have

Theorem 5.4.9. (Local Class Field Theory) *Let K be a local field. Then,*

1. *There is a unique homomorphism $Art_K : K^* \to Gal(K^{ab}/K)$ characterized by the following properties:*
   - *For a prime $\pi \in K$, then $Art_K(\pi)|_{K^{ur}} = \varphi_K$ with φ_K the Frobenius of $Gal(K^{ur}/K)$.*
   - *For an abelian extension K'/K, we have $Art_K(N(K'/K))|_{K'} = 1$.*
2. *For a finite abelian extension K'/K, the Artin map induces the exact sequence:*

$$1 \to N_{K'/K}(K'^*) \to K^* \to Gal(K'/K) \to 1.$$

Bibliography

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, AMS CHELSEA PUBLISHING 2005.

[2] N. Bourbaki. *Commutative Algebra*; ADDISON-WESLEY 1972.

[3] N. Bourbaki, *Topological Vector Spaces*, Chapter 1-5, Springer, Berlin Heidelberg New York 1987.

[4] C. Chevalley, *On the theory of local rings*, Ann. of Math., Vol. 44 (1943) pp. 690-708; available at: http://www.jstor.org.

[5] Henri Cohen; Xavier-François Roblot, *Computing the Hilbert class field of real quadratic fields* , available at: http://www.ams.org/mcom/2000-69-231/S0025-5718-99-01111-4/home.html.

[6] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc., Vol. 59, 1946, pp. 54-106; available at: http://www.jstor.org.

[7] P. Colmez *Les Nombres p-adiques, Notes du Cours de M2* available at: http://people.math.jussieu.fr/∼colmez/.

[8] P. Colmez *Corps Locaux, Notes du Cours de M2* available at: http://people.math.jussieu.fr/∼colmez/.

[9] A. J. Engler, A. Prestel, *Valued Fields* , Springer, Berlin Heidelberg 2005.

[10] I. B. Fesenko, S. V. Vostokov, *Local Fields and Their extensions*, AMS, second edition 2002.

[11] A. Frohlich, *Local fields* in *Algebraic Number theory*, Academic Press 1967.

[12] S R. Ghorpade, Balmohan V. Limaye, *A Course in Calculus and Real Analysis*, Springer, New York 2006.

[13] M. Hazewinkel, *Formal groups and applications*, Acad. Press, 1978.

[14] Franz-Viktor Kuhlmann, *Valuation Theory*, available at: http://math.usask.ca/∼fvk/Fvkbook.htm.

[15] Kenkichi. Iwasawa, *Local Class Field Theory*, Oxford University Press. New York 1986.

[16] J. Lubin and J. Tate, Formal complex multiplication in local fields, Ann. of Math. (2) 81 (1965), 380-387.

[17] J. S. Milne, *Class Field Theory*, Course notes available at: http://www.math.lsa.unich.edu/∼jmilne.

[18] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin Heidelberg New York 1999.

[19] Xavier-François Roblot, *Stark's Conjectures and Hilbert's Twelfth Problem*, available at: http://citeseer.ist.psu.edu/roblot99starks.html.

[20] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, New York Heidelberg Berlin 1979.

[21] Jean-Pierre Serre, *Local class field theory*, Algebraic Number Theory (Cassels and Frohlich, eds), Academic Press, New York, 1967.

[22] Ehud de Shalit, *Relative Lubin-Tate Groups*, available at http://www.jstor.org/stable/2045561

[23] J. Stevenhagen, *Local fields*, available at: http://websites.math.leidenuniv.nl/algebra/localfields.pdf.

[24] Paul B. Yale, *Automorphisms of Complex Numbers*, Mathematics Magazine, Vol. 93, No. 3 (1966), pp. 135-141; available at: http://www.jstor.org.

[25] T. Yoshida, *Local Class Field Theory via Lubin-Tate Theory*, available at: http://www.math.harvard.edu/∼yoshida/.

Index

i-th ramification subfield, 47
p-adic absolute value, 13

absolute values, 11
discrete valuation ring, 12
system of representatives, 27
upper numbering, 51

approximation theorem, 16
Archimedean, 13
Archimedean postulate, 13

complete, 22

formal A_K-module, 60
Frobenius k_K-automorphism, 44

Hasse-Arf theorem, 69
Herbrand's theorem, 50
higher ramification subgroups in lower numbering, 46

incomplete, 22

local field, 36

non-archimedean, 13
norm group, 52
normalized, 13

p-adic valuation, 8
prime, 26

ramification index, 38
relative Lubin-Tate extension, 62
residue degree, 38
residue field, 17

tamelyramified, 40
Teichmüller representatives, 31
the product formula, 21
totally ramified, 39

ultrametric absolute values, 11
ultrametric inequality, 13
uniformizer, 26
unit norm group, 53
unramified, 39

valuation, 12
valuation ring, 17
value group, 11, 12

wildly ramified, 40