EXPLICIT RECIPROCITY LAWS

A THESIS
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE INSTITUTE OF ENGINEERING AND SCIENCE
OF BILKENT UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE

By
Ali ADALI
July, 2010

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Alexander Klyachko (Supervisor)

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ahmet Muhtar Güloğlu

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ç̣etin Ürtiş

Approved for the Institute of Engineering and Science:

Prof. Dr. Levent Onural
Director of the Institute Engineering and Science

ABSTRACT

EXPLICIT RECIPROCITY LAWS

Ali ADALI
M.S. in Mathematics
Supervisors: Prof. Dr. Alexander Klyachko July, 2010

Quadratic reciprocity law was conjectured by Euler and Legendre, and proved by Gauss. Gauss made first generalizations of this relation to higher fields and derived cubic and biquadratic reciprocity laws. Eisenstein and Kummer proved similar relations for extension $\mathbb{Q}(\zeta_p, \sqrt[n]{a})$ partially. Hilbert identified the power residue symbol by norm residue symbol, the symbol of which he noticed the analogy to residue of a differential of an algebraic function field. He derived the properties of the norm residue symbol and proved the most explicit form of reciprocity relation in $\mathbb{Q}(\zeta_p, \sqrt[n]{a})$. He asked the most general form of explicit reciprocity laws as 9th question at his lecture in Paris 1900. Witt and Schmid solved this question for algebraic function fields. Hasse and Artin proved that the reciprocity law for algebraic number fields is equal to the product of the Hilbert symbol at certain primes. However, these symbols were not easy to calculate, and before Shafarevich, who gave explicit way to calculate the symbols, only some partial cases are treated. Shafarevich's method later improved by Vostokov and Brükner, solving the 9th problem of Hilbert. In this thesis, we prove the reciprocity relation for algebraic function fields as wel as for algebraic function fields, and provide the explicit formulas to calculate the norm residue symbols.

Keywords: Explicit Reciprocity, Norm Residue Symbol, Power Residue Symbol.

ÖZET

GENEL KARSILIKLILIK YASASI

Ali ADALI
Matematik, Yüksek Lisans
Tez Yöneticisi: Prof. Dr. Alexander Klyachko Temmuz, 2010

Karesel karşılıklılık yasası ilk olarak L. Euler ve A. Legendre tarafından iddia edildi ve Gauss tarafindan ispatlandı. Gauss daha yüksek alanlara bu ilişkinin ilk genellemelerini yapmış ve üçüncü ve dördüncü dereceden karşılıklılık yasalarını bulmuştur. Eisenstein ve Kummer bu yasaları $\mathbb{Q}(\zeta_p, \sqrt[n]{a})$ araştırmış ve benzer kısmi sonuçlar elde etmişlerdir. Hilbert, bu yasayı tanımlamaya yarayan sembolü cebirsel fonksiyon alanlarında diferansiyel kalana eşdeğer olan başka bir sembolle tanımlamış ve bu yeni sembolün özelliklerini kullanarak $\mathbb{Q}(\zeta_p, \sqrt[n]{a})$ alanındaki karşılıklılık yasasını en genel haliyle elde etmiştir. Sayı alanlarında en genel karşılıklılık yasası Hilbert'in 1900 yılında Paris'teki meşhur konferansında sorduğu 24 sorundan 9.'sudur. Witt ve Schmid cebirsel fonksiyon alanları için bu soruyu tüm yönleriyle çözdü. Hasse ve Artin bu cebirsel sayi alanlari için karşılıklılık yasasının belli asallardaki Hilbert sembollerinin çarpımına eşit olduğunu kanıtladı. Ancak bu sembollerin değerlerini hesaplamak kolay degildi ve açik bir şekilde sembolleri hesaplamak için ilk metodu geliştiren Shafarevich'ten önce sadece bazı kısmi durumlar için hesaplamalar yapıldı. Shafarevich'in yöntemi daha sonra Vostokov ve Brückner tarafindan geliştirildi. Bu gelişmelerle birlikte Hilbert'in 9. soru tamamen cevaplanmış oldu. Bu tezde, karşılıklılık ilişkisini hem cebirsel fonksiyon alanları için hem de cebirsel sayı alanları için ispatlayacağız. Hilbert sembollerinin hesaplaması için geliştirilen yöntemleri ele alacağız.

Anahtar sözcükler: Genel Karsiliklik Yasasi, Norm Kalan Sembolu, Kuvvet Kalan Sembolu.

Acknowledgement

I would like to express my sincere gratitude to my supervisor Prof. Alexander Klyachko for his excellent guidance, valuable suggestions, encouragement, patience, and conversations full of motivation. Without his guidance I can never walk that far in my studies and mathematics may not be this much delightful.

I would like to thank my parents, Fikret and Rukiye, my sisters Emel and Embiye who give countenance to me as this thesis would never be possible without their encouragement, support and love.

I would like to thank this adorable young lady, Filiz, who is the real heroine of this project hidden behind the scenes. Without her patience, her support, her love, her struggles for motivating me, her shoulders when I needed sometimes to put my head, her desserts prepared for me and everything about her I would never be able to finish this text.

The work that form the content of the thesis is supported financially by TÜBİTAK through the graduate fellowship program, namely ”TÜBİTAK-BİDEB 2228-Yurt İçi Yüksek Lisans Burs Programı”. I am grateful to the council for their kind support.

I dedicate this thesis to;

the Ground of all Being,
the One from Whom we have come,
and to Whom we shall return,
the Font of wisdom and the Light of lights,
the Maker, Renewer, and the Keeper of all things.

Contents

Chapter 1

Introduction

Leonard Euler and Adrien-Marie Legendre conjectured that for primes p and q, the solvability of the equation $x^2 \equiv p \pmod{q}$ is dependent on the solvability of $q \equiv x^2 (\text{mod } p)$ up to an arithmetical relation. This relation, also known as quadratic reciprocity law, was known by these two mathematicians, however, it was not proved until the work of Carl Friedrich Gauss. The quadratic residue symbol $\left(\frac{p}{q}\right)$ is defined as 1 or -1 depending on whether the equaiton $p \equiv x^2 \pmod{q}$ is solvable or not, respectively, and it equals zero in case $q \mid p$. The precise relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is the following:

Theorem 1.0.1 (Quadratic Reciprocity Law) *For odd primes p, q,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

and

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (\textit{supplementary laws})$$

Definition of the symbol can be extended multiplicatively to all rationals by

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n}\prod_{j=1}^{m}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\prod_{i=1}^{n}\left(\frac{-1}{q_j}\right)^{\alpha\beta_j}\prod_{i=1}^{n}\left(\frac{-1}{p_i}\right)^{-\beta\alpha_i}$$

for $a, b \in \mathbb{Q}$ with $a = (-1)^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $b = (-1)^{\beta} q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$, where p_i, q_j are different primes and $\alpha_i, \beta_j \in \mathbb{Z}$. The symbol $\left(\frac{a}{b}\right)$ is known as the Legendre symbol.

Gauss derived similar relations for cubic reciprocity and for biquadratic reciprocity for fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, respectively. Here, ζ_n denotes the primitive n-th root of unit. Eisenstein took the process one step further proving p-th power reciprocity relation for the cyclotomic extension $\mathbb{Q}(\zeta_p)$, where p is an odd prime. In this case, the formula looks considerably simpler; namely, it states that for non-zero integers a and b, both coprime to p, and $\alpha \in \mathbb{Z}[\zeta_p]$ with $\alpha \equiv b \left(\mathrm{mod}\ (1-\zeta_p)^2\right)$,

$$\left(\frac{a}{\alpha}\right)_p = \left(\frac{\alpha}{a}\right)_p .$$

In general, one defines n-th power residue symbol $\left(\frac{\cdot}{\cdot}\right)_n$ (see Chapter 6), for which one has a reciprocity law relating $\left(\frac{a}{b}\right)_n$ to $\left(\frac{b}{a}\right)_n^{-1}$ through a simple formula involving n-th roots of unity together with similar supplementary laws.

The reciprocity law of Eisenstein holds only for certain cases. E. Kummer achieved to prove the result of Eisenstein for a larger set of numbers by working on the fields $\mathbb{Q}(\zeta_p, \sqrt[p]{a})$, which inspired Hilbert to derive more explicit results by using these fields. One of Hilbert's most profound achievements was to define norm residue symbols in terms of which he was able to express n-th power residue symbols and thereby establish the p-th power reciprocity law for $\mathbb{Q}(\zeta_p, \sqrt[p]{a})$ in full generality. He noticed that this process can be generalized to larger algebraic number fields, which appeared as his 9th problem among the 24 problems he proposed in his famuos lecture in 1900, Paris.

Hilbert noticed that the norm residue symbol $\left(\frac{a}{b}\right)_n$ plays the same role in algebraic number fields as does the residue $Res(f\frac{dg}{g})$ in theory of algebraic function fields. The reciprocity laws in algebraic number fields has analogy to algebraic extensions of function fields, the relations which come out to be the natural results of the geometric structure of algebraic function fields. The explicit reciprocity laws for algebraic function fields were discovered in full generality before than that of algebraic number fields by the work of H. L. Schmid and E. Witt, both of whom are Ph.D students of Hasse.

E. Artin and H. Hasse achieved to derive certain properties of norm residue symbol by setting geometric-analytic structure on algebraic number fields which is analogous to that of algebraic function fields. Using these properties they not only proved the existance of the reciprocity relation in general but also that the quantity $\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1}$ is the product of Hilbert symbols at certain primes. Shafarevich proposed the most general formula for explicit calculations of the Hilbert symbols using the decomposition of numbers in certain basis. Bruckner and Vostokov built a comprehensive theory for explicit calculations of the Hilbert symbols without use of basis in Shafarevich's method, finishing the proof of the 9th Hilbert problem.

In this thesis, we explain the explicit reciprocity laws in algebraic function fields and algebraic number fields in full generality.

At Chapter 2 we start with the proof of quadratic reciprocity. We define the machinery (i.e. norm residue symbols, product formula, reciprocity laws) in order to show how how the general theory can be interpreted by this simplest case. Next, we switch to function fields, and prove the reciprocity law for polynomials over finite fields. This will suggest insight for reciprocity laws in function fields.

At Chapter 3 we define the machinery for algebraic function fields over a finite constant field and derive the explicit reciprocity laws. We derive two kinds of reciprocity laws, first is the multiplicative reciprocity law which corresponds to the case when characteristic is prime to exponent and second is additive law which corresponds to the character is equal to the exponent.

At Chapter 4 all the machinery that will be needed to settle reciprocity relation in general form will be introduced throughout the quadratic reciprocity. This chapter is illustration of the following chapter for quadratic case.

At Chapter 5 we define the machinery in general form. We introduce global fields. We define local and global analytic structures on global fields in order to define the symbols in explicit form and to derive the reciprocity relation in general. All the machinery except the definitions of symbols will be given, leaving the latter to next chapter.

At Chapter 6 we define of the power residue and norm residue symbols and derive some of their certain properties which are needed to obtain the reciprocity relation. We derive the reciprocity relation together with the supplementary laws. For illustration we prove the quadratic reciprocity formula from the main theorem. We continue with calculating the ‘simple formula’ for certain extensions, providing insight for generalization. As application we prove the cubic reciprocity and Eisenstein reciprocity laws.

At Chapter 7 we give the explicit formulas for algebraic number fields. We start with explaining the revolutionary work of Shafarevich, in which he explicitly calculated the values of the ‘simple formula’ up to choice of a certain basis. We then explain the work of Vostokov where he explicitly calculates the values of ‘simple formula’ without using a basis. We finish the theory by giving the most general explicit formulas due to Vostokov and Brückner.

Chapter 2

Quadratic Reciprocity and Reciprocity in Polynomials

In this chapter we start with proving the quadratic reciprocity law. We next prove the reciprocity law on polynomials over finite fields. We aim this section to provide examples in order to indicate how the reciprocity relations are treated for general cases.

2.1 Quadratic Reciprocity

Definition 2.1.1 *Let $a, p \in \mathbb{Z}$ with p prime. Define $\left(\frac{a}{p}\right) = 0$ if $p|a$, $\left(\frac{a}{p}\right) = 1$ if $a \equiv x^2 (mod\, p)$ solvable and $\left(\frac{a}{p}\right) = -1$ if $a \equiv x^2 (mod\, p)$ is not solvable. We call this symbol quadratic symbol (or Gauss symbol)*

Lemma 2.1.2 *Let $a, p \in \mathbb{Z}$ and p be an odd prime with coprime to a. Then quadratic symbol can be identified by $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\, p)$.*

Proof: If $(\frac{a}{p}) = 1$ then $\exists x \in \mathbb{Z}$ with $a \equiv x^2(\text{mod } p)$, hence $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1(\text{mod } p)$ by Euler's (or Fermat's) theorem. Now assume that $a^{\frac{p-1}{2}} \equiv$

1(mod p), let c be a primitive root in mod p and $a \equiv c^{a_1}(\text{mod } p)$.

$$1 \equiv a^{\frac{p-1}{2}} \equiv c^{\frac{a_1(p-1)}{2}}(\text{mod } p) \Leftrightarrow p-1|\frac{a_1(p-1)}{2} \Leftrightarrow 2|a_1 \Leftrightarrow a_1 = 2a_2$$

for some $a_2 \in \mathbb{Z}$, then $a \equiv (c^{a_2})^2(\text{mod } p)$ i.e. $(\frac{a}{p}) = 1$.

Theorem 2.1.3 (Quadratic Reciprocity Law) *Let p, q be odd primes.*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Theorem 2.1.4 (Supplementary Laws) *Let p be an odd prime, then*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$$

We follow a proof due to Gauss.

Lemma 2.1.5 (Gauss Lemma) *Let $a, p \in \mathbb{Z}$ with prime p coprime to a. Let $S = 1, 2, \cdots, \frac{(p-1)}{2}$ be set of half residues in mod p. Let v denote the number of elements in $a, 2a, \cdots, \frac{(p-1)}{2}a$ which are not in S, then $(\frac{a}{p}) = (-1)^v$.*

Proof: {Gauss Lemma} $ai \equiv (-1)^{v_i}i_1(\text{mod } p)$ for unique $i_1 \in S$ and for unique $v_i = 0$ or 1. On one hand;

$$a(2a)(\frac{(p-1)}{2}a) \equiv (-1)^{\sum_{i=1}^{\frac{p-1}{2}} v_i}1.2\cdots\frac{(p-1)}{2}(\text{mod } p)$$

on the other hand

$$a(2a)\cdots(\frac{(p-1)}{2}a) \equiv a^{\frac{(p-1)}{2}}1.2\cdots\frac{(p-1)}{2} \equiv (\frac{a}{p})1.2\cdots\frac{(p-1)}{2}(\text{mod } p)$$

, hence $(\frac{a}{p}) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} v_i} = (-1)^v$ as desired.

Proof: {Supplementary Laws} Take $a = -1$ in the Gauss lemma, then we have no elements of $\{-1, -2, \cdots, -\frac{(p-1)}{2}\}$ are in S, $v = \frac{(p-1)}{2}$ and $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}}$.

Take $a = 2$ in the Gauss lemma, we count the elements of the set $\{2.1, 2.2, \cdots, 2\frac{(p-1)}{2}\} = \{2, 4, \cdots, p-1\}$ which are not in S. Clearly v is the number of integers between $\frac{p}{4}$ and $\frac{p}{2}$. The first of these integers are either $\frac{p+3}{4}$ or $\frac{p+1}{4}$ (according to $p \equiv 1, 3(\text{mod } 4)$ respectively) and the last is $\frac{p-1}{2}$.
If $p \equiv 1(\text{mod } 8)$ then $v = \frac{p-1}{2} - \frac{p+3}{4} + 1 = \frac{p-1}{4} \equiv 0 \equiv \frac{(p^2-1)}{8}(\text{mod } 2)$.
If $p \equiv 3(\text{mod } 8)$ then $v = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4} \equiv 1 \equiv \frac{(p^2-1)}{8}(\text{mod } 2)$.
If $p \equiv 5(\text{mod } 8)$ then $v = \frac{p-1}{2} - \frac{p+3}{4} + 1 = \frac{p-1}{4} \equiv 1 \equiv \frac{(p^2-1)}{8}(\text{mod } 2)$.
If $p \equiv 7(\text{mod } 8)$ then $v = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4} \equiv 0 \equiv \frac{(p^2-1)}{8}(\text{mod } 2)$. Hence the relation $(\frac{2}{p}) = (-1)^{\frac{(p^2-1)}{8}}$.

Proof: {Quadratic Reciprocity} From Gauss lemma we have $(\frac{p}{q}) = (-1)^v$ where v is the numbers qx with $x = 1, 2, \cdots, \frac{(p-1)}{2}$ whose residue mod p is negative, i.e.

$$-\frac{p}{2} < qx - py < 0$$

has an integer solution y. On one hand $y > 0$ since $qx > 0$, on the other hand $py < qx + \frac{p}{2} < \frac{qp}{2} + \frac{p}{2} = p\frac{q+1}{2}$ thus $y \leq \frac{q-1}{2}$. In addition y is uniquely determined by x since $-\frac{p}{2} < qx - py' < 0$ then subtracting from the first equation we get $-p < p(y - y') < p$ thus $y = y'$. We can identify v by number of pairs of x, y such that $x = 1, 2, \cdots, \frac{(p-1)}{2}$, $y = 1, 2, \cdots, \frac{(q-1)}{2}$ and $-\frac{p}{2} < qx - py < 0$. Analogously, we have $(\frac{p}{q}) = (-1)^{v'}$ where v' is the numbers in the same sets satisfying $-\frac{q}{2} < py - qx < 0$ hence $0 < qx - py < \frac{q}{2}$. Therefore $(\frac{p}{q})(\frac{q}{p}) = (-1)^{v+v'}$ where $v + v'$ is the number of x, y in the sets defined above and satisfy $-\frac{p}{2} < qx - py < \frac{q}{2}$, because the equation $qx - py = 0$ has its smallest solution at $x = p$, $y = q$. We now prove that if a, b are in the same intervals with x and y respectively and is not the solution of $-\frac{p}{2} < qx - py < \frac{q}{2}$, then $\frac{p+1}{2} - a$ and $\frac{q+1}{2} - b$ are another integers in respective intervals which $-\frac{p}{2} < qx - py < \frac{q}{2}$ does not hold. To see this; $q(\frac{p+1}{2} - a) - p(\frac{q+1}{2} - b) = \frac{q}{2} - \frac{p}{2} - qa + pb$. If $qa - py > \frac{q}{2}$ then $\frac{q}{2} - \frac{p}{2} - qa + pb < -\frac{p}{2}$ and If $qa - py < -\frac{p}{2}$ then $\frac{q}{2} - \frac{p}{2} - qa + pb > \frac{q}{2}$. Thus, if we pair (a, b) with $(\frac{p+1}{2} - a, \frac{q+1}{2} - b)$, $(a, b) \neq (\frac{p+1}{2} - a, \frac{q+1}{2} - b)$ except perhaps $(a, b) = (\frac{p+1}{4}, \frac{q+1}{4})$, but (if both integers) $(\frac{p+1}{4}, \frac{q+1}{4})$ is solution to $-\frac{p}{2} < qx - py < \frac{q}{2}$. We can pair non-solutions and hence the number of solutions x, y with $x = 1, 2, \cdots, \frac{(p-1)}{2}$ and $y = 1, 2, \cdots, \frac{(q-1)}{2}$ is equivalent to $v + v'$ in mod 2. Since this number is equal to $\frac{(p-1)(q-1)}{4}$ thus $\frac{(p-1)(q-1)}{4} = v + v'(\text{mod } 2)$ hence $(\frac{p}{q})(\frac{q}{p}) = (-1)^{v+v'} = (-1)^{\frac{(p-1)(q-1)}{4}}$

as desired.

This quadratic symbol can be extended multiplicatively to all a, b in $\mathbb{Z}$ as following;

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n}\prod_{j=1}^{m}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\prod_{i=1}^{n}\left(\frac{-1}{q_j}\right)^{\alpha\beta_j}\prod_{i=1}^{n}\left(\frac{-1}{p_i}\right)^{-\beta\alpha_i}$$

for $a, b \in \mathbb{Q}$ with $a = -1^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, $b = (-1)^{\beta}q_1^{\beta_1}q_2^{\beta_2}\cdots q_m^{\beta_m}$ with p_i, q_j are different primes and $\alpha_i, \beta_j \in \mathbb{Z}$. This symbol has is called Legendre symbol. One may now derive the quadratic reciprocity law over all integers, which is the most general form;

Theorem 2.1.6 (General Quadratic Reciprocity Law) *Let a, b are odd relatively prime integers; then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{(a-1)(b-1)}{4} + \frac{(sqn(a)-1)(sqn(b)-1)}{4}},$$

with supplementary laws;

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2} + \frac{sgn(b)-1}{2}}, \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}.$$

Proof: These formulas hold when a and b are odd primes. We need only to check that formulas have multiplicative property. For reciprocity law this is equivalent to check $\frac{(aa'-1)(b-1)}{4} + \frac{(sqn(aa')-1)(sqn(b)-1)}{4} \equiv \frac{(a-1)(b-1)}{4} + \frac{(sqn(a)-1)(sqn(b)-1)}{4} + \frac{(a'-1)(b-1)}{4} + \frac{(sqn(a')-1)(sqn(b)-1)}{4} \pmod 2$ and this is evident by checking the cases for a,b in mod 4. For supplementary law it is equivalent to check $\frac{bb'^2-1}{8} \equiv \frac{b^2-1}{8}\frac{b'^2-1}{8} \pmod 2$ and $\frac{bb'-1}{2} + \frac{sgn(bb')-1}{2} \equiv \frac{b-1}{2} + \frac{sgn(b)-1}{2}\frac{b-1}{2} + \frac{sgn(b)-1}{2} \pmod 2$, which are evident in similar way.

2.2 Reciprocity Law in Polynomials

In this section we prove the reciprocity law for polynomials over a fixed finite field. We denote the finite field with q elements by $\mathbb{F}_q$, assuming that field has

characteristic p and $q = p^k$ for some integer k. $\mathbb{F}_q(t)$ be rational field of polynomial ring $\mathbb{F}_q[t]$. We can analogously define quadratic symbol for quadratic symbol $(\frac{f}{g})$ for polynomials $f, g \in \mathbb{F}_q[t]$ with g being prime (we assume primes are monic). Indeed, we can extend this definition to n-th power residue symbol in the following. $\mathbb{F}_q^*$ is cyclic hence has a generator c. We want to observe the roots of unity in $\mathbb{F}_q$. Let $n \in \mathbb{N}$, $x^n = 1 \Leftrightarrow c^{nx_1} = 1 \Leftrightarrow q-1|nx_1$ where $x = c^{x_1}$. Thus non-trivial roots of unity are n-th roots of unity with $n|q-1$. It is convenient to assume $n|q-1$ (note that we seek for a multiplicative form of reciprocity). Now let $f, g \in \mathbb{F}_q[t]$ and g prime. Residue field of mod g is a finite field with $q^{\deg(g)}$ elements (for simplicity we denote $q^{\deg(g)}$ by $|g|$), and mod g^* is cyclic with $|g|-1$ elements.
$f \equiv b^n (\text{mod } g) \Leftrightarrow g_c^{a_1} \equiv b^n (\text{mod } g) \Leftrightarrow n|a_1 \Leftrightarrow g_c^{\frac{a_1}{n}(|g|-1)} \equiv 1(\text{mod } g) \Leftrightarrow a^{\frac{q-1}{n}} \equiv 1(\text{mod } g)$ where g_c is the generator of mod g^* and $f \equiv g_c^{a_1}(\text{mod } g)$. It is convenient to define $\left(\frac{f}{g}\right)_n$ by;

Definition 2.2.1 *Let a, g, n be as above, n-th power residue symbol $\left(\frac{f}{g}\right)_n$ (or Legendre symbol) is defined to be the 0 if $g|f$ and the unique n-th root of unity satisfying*

$$\left(\frac{f}{g}\right)_n \equiv f^{\frac{|g|-1}{n}} (mod\ g)$$

if g coprime to f.

This definition makes sense because if we set $x = f^{\frac{|g|-1}{n}}$ then $x^n \equiv f^{|g|-1} \equiv 1(\text{mod } g)$, hence $x^n - 1 = \prod_{\omega^n=1}(x-\omega) \equiv 0(\text{mod } g)$, as g is prime, then it will divide unique factor $(x-\omega)$ with unique n-th root of unity ω.

Proposition 2.2.2 *Let $f, f', g \in \mathbb{F}_q[t]$, g prime and coprime to f and f'*

$$\left(\frac{ff'}{g}\right)_n = \left(\frac{f}{g}\right)_n \left(\frac{f'}{g}\right)_n$$

Proof: $(ff')^{\frac{|g|-1}{n}} \equiv (f)^{\frac{|g|-1}{n}} (f')^{\frac{|g|-1}{n}} (\text{mod } g)$ hence the proposition.

Theorem 2.2.3 (n-th Power Reciprocity Law) *Let k be finite field and $f, g \in k[t]$ prime polynomials. Then*

$$\left(\frac{f}{g}\right)_n \left(\frac{g}{f}\right)_n^{-1} = (-1)^{\deg(f)\deg(g)\frac{(q-1)}{n}}$$

We prove this theorem by identifying the power residue symbol with the resultant of of f with g. It is defined to be $Res(f,g) = \prod_{g(\beta)=0} f(\beta)$. Certain properties of this geometric object will give not only the proof of this theorem but also give the multiplicative formula, which is assumed to be the heart of the reciprocity relation for general forms.

Proof: Let β be root to g, we adjoint β to $\mathbb{F}_q$ and get a finite field $\mathbb{F}_q{}^{\beta}$ with $|g| = q^{\deg(g)}$ elements. $g(t)$ is decomposed into linear factors in $\mathbb{F}_q{}^{\beta}$. Due to the theory of finite fields we have that $\mathbb{F}_q{}^{\beta}/\mathbb{F}_q$ is cyclic of degree $\deg(g)$ and the Galois group is generated by automorphism $f \to f^p$(ref. Hasse Number theory, pg 41) Hence roots of g are permuted by this automorphism and thus all roots are g are $\beta, \beta^p, \cdots, \beta^{p^{\deg(g)-1}}$ and $g(t) = \prod_{i=0}^{\deg(g)-1}(t-\beta^i)$. Assume $f \in \mathbb{F}_q[t]$ coprime to g and consider the n-th power residue symbol $\left(\frac{f}{t-\beta}\right)_n'$ where the symbol is to be understood in $\mathbb{F}_q{}^{\beta}[t]$ instead of $\mathbb{F}_q[t]$. This symbol is characterized by

$$\left(\frac{f}{t-\beta}\right)_n' \equiv f^{\frac{q^{\deg(g)}-1}{n}} (\mathrm{mod}\ t-\beta)$$

since $|t-\beta| = q^{\deg(g)}$. On the other hand we have, $\left(\frac{f}{g}\right)_n \equiv f^{\frac{q^{\deg(g)}-1}{n}} (\mathrm{mod}\ g)$. As $(t-\beta)|g$ in $\mathbb{F}_q{}^{\beta}[t]$ then we have

$$\left(\frac{f}{g}\right)_n = \left(\frac{f}{t-\beta}\right)_n'$$

Since $t \equiv \beta(\mathrm{mod}\ t-\beta)$ then $f(t) \equiv f(\beta)(\mathrm{mod}\ t-\beta)$.

$$\left(\frac{f}{t-\beta}\right)_n' = f(\beta)^{\frac{q^{deg(g)}-1}{n}} = f(\beta)^{\frac{q^{deg(g)}-1}{q-1}\frac{q-1}{n}} = f(\beta)^{(1+q+\cdots+q^{\deg(g)-1})\frac{q-1}{n}} =$$

$$= \left(f(\beta)f(\beta^q)\cdots f(\beta^{q^{deg(g)}-1})\right)^{\frac{q-1}{n}}$$

The last equation is true due to $f(\beta)^p = f(\beta^p)$ since $\mathbb{F}_q$ has characteristic p. This gives us the following expression for n-th power residue symbol

$$\left(\frac{f}{g}\right)_n = \left(f(\beta)f(\beta^q)\cdots f(\beta^{q^{deg(g)}-1})\right)^{\frac{q-1}{n}}$$

This expression can be rewritten as

$$\left(\frac{f}{g}\right)_n = \left(\prod_{g(\beta)=0} f(\beta)\right)^{\frac{q-1}{n}}$$

We consider β is in the algebraic closure $\bar{\mathbb{F}}_q^{alg}$ of k. Now let $f \in \mathbb{F}_q[t]$ be another prime polynomial. Then

$$\left(\frac{f}{g}\right)_n = \left(\prod_{g(\beta)=0} f(\beta)\right)^{\frac{q-1}{n}} = \left(\prod_{g(\beta)=0}\prod_{f(\alpha)=0} (\alpha-\beta)\right)^{\frac{q-1}{n}} = \left(\prod_{g(\beta)=0}\prod_{f(\alpha)=0} (-1)(\beta-\alpha)\right)^{\frac{q-1}{n}} =$$

$$= (-1)^{\deg(f)\deg(g)\frac{q-1}{n}} \left(\prod_{g(\beta)=0}\prod_{f(\alpha)=0} (\beta-\alpha)\right)^{\frac{q-1}{n}} = (-1)^{\deg(f)\deg(g)\frac{q-1}{n}} \left(\prod_{f(\alpha)=0} g(\alpha)\right)^{\frac{q-1}{n}} =$$

$$= (-1)^{\deg(f)\deg(g)\frac{q-1}{n}} \left(\frac{g}{f}\right)_n$$

(α's and β's are in $\bar{\mathbb{F}}_q^{alg}$). Hence we proved the theorem.

We have a single supplementary law as follows;

Theorem 2.2.4 (Supplementary Law) *Let $g \in \mathbb{F}_q[t]$ prime polynomial and let $\epsilon \in \mathbb{F}_q$, then*

$$\left(\frac{\epsilon}{g}\right)_n = \epsilon^{\frac{q^{\deg(g)}-1}{n}}$$

Proof: $\left(\frac{\epsilon}{g}\right)_n$ is characterized by $\left(\frac{\epsilon}{g}\right)_n \equiv \epsilon^{\frac{q^{\deg(g)}-1}{n}} (\text{mod } g)$, set $x = \epsilon^{\frac{q^{\deg(g)}-1}{n}}$, then $x^n = \epsilon^{q^{\deg(g)}-1} = 1$ as $(q-1) | \left(q^{\deg(g)}-1\right)$ and thus $x = \epsilon^{\frac{q^{\deg(g)}-1}{n}}$ is itself an n-th root of unity and hence the theorem.

We can multiplicatively extend this symbol to all polynomials in $\mathbb{F}_q[t]$ by; setting its value to 0 if a, b are not coprime, and to

$$\left(\frac{a}{b}\right)_n = \left(\frac{a}{g_1}\right)_n^{\beta_1} \left(\frac{a}{g_2}\right)_n^{\beta_2} \cdots \left(\frac{a}{g_r}\right)_n^{\beta_r}$$

if a, b coprime and $b = \epsilon_b g_1^{\beta_1} g_2^{\beta_2} \cdots g_r^{\beta_r}$ with $\epsilon_b \in \mathbb{F}_q$ and $g_i \in \mathbb{F}_q[t]$. One can immediately get the most general form of the reciprocity formula for relatively prime polynomials a, b.

Theorem 2.2.5 *Let $a, b \in \mathbb{F}_q[t]$. Write $a = \epsilon_a f_1^{\alpha_1} f_2^{\alpha_2} \cdots f_l^{\alpha_l}$ and $b = \epsilon_b g_1^{\beta_1} g_2^{\beta_2} \cdots g_r^{\beta_r}$ where f_i, g_j are prime polynomials and $\epsilon_a, \epsilon_b \in \mathbb{F}_q$. Then;*

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = (-1)^{\frac{\deg(a)\deg(b)(q-1)}{n}} \left(\frac{\epsilon_a}{b}\right)_n^{\deg(b)} \left(\frac{\epsilon_b}{a}\right)_n^{-\deg(a)}$$

We observe now a local symbol (which will call the 'norm residue symbol') enters to the picture in the following. Let P be a point on $\mathbb{P}_1$ and f_P denote the minimal monic polynolial for P. One may define the symbol for $a, b \in \mathbb{F}_q[t]$ at P as;

$$\left(\frac{a, b}{P}\right) = (-1)^{\alpha\beta} \left(\frac{a}{f_P}\right)_n^{\beta} \left(\frac{b}{f_P}\right)_n^{-\alpha}$$

Where $a = f_P^{\alpha} A$ and $b = f_P^{\beta} B$ with $A, B \in \mathbb{F}_q[t]$ coprime to f_P.

One can identify the n-th power residue symbol by this symbol as;

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1}.$$

The symbol at $P = \infty$ is;

$$\left(\frac{a, b}{\infty}\right) = (-1)^{\frac{\deg(a)\deg(b)(q-1)}{n}} \left(\frac{\epsilon_a}{b}\right)_n^{-\deg(b)} \left(\frac{\epsilon_b}{a}\right)_n^{\deg(a)}$$

Combining these results with the reciprocity law, we get the formula

$$\prod_{P \in \mathbb{P}_1} \left(\frac{a, b}{P}\right) = 1.$$

the product is taken over all primes. This symbol is called norm residue symbol, and the formula called the product formula for norm residue symbol. We shall see in the context that these are very crucial notions.

Chapter 3

Reciprocity Laws in Algebraic Function Fields

3.1 Introduction

In this chapter we keep the notations of $\mathbb{F}_q$ and n from the previous chapter. We assume $n|q-1$. In the previous chapter it is showed that for prime $f, g \in \mathbb{F}_q(t)$ where $t \in \mathbb{P}_1$ the projective line, the solubility of $g \equiv u^n (\text{mod } f)$ for $u \in \mathbb{F}_q(t)$ is equivalent to the solubility of such equation locally at α where α is a root to f. By this, we mean that $g \equiv u^n (\text{mod } f)$ solvable if and only if $g(\alpha)$ is an n-th power in $\mathbb{F}_q(\alpha)$ and this is if and only if $N_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}(g(\alpha)) = Res(g, f)$ is an n-th power in $\mathbb{F}_q$. If we now define local ring $\mathcal{O}_\alpha$ at α as Taylor series in $x - \alpha$ with non-negative powers and with coefficients in $\mathbb{F}_q$, the solubility of the last is equivalent to the solubility of $g = u^n + fh$ where $u, h \in \mathcal{O}_\alpha$; this is as follows, one part is evident that putting α in equation we get $g(\alpha) = u(\alpha)^n + f(\alpha)h(\alpha) = u(\alpha)^n$ with $g(\alpha), u(\alpha) \in \mathbb{F}_q$. The inverse part is, we have $f(t) = (t-\alpha)(t-\alpha^q)\cdots(t-\alpha^{q^{l-1}})$ for some $l \in \mathbb{N}$ with $\alpha^{q^l} = 1$. $t - \alpha^{q^i}$ is in $\mathcal{O}_\alpha$ and is invertible for $i \neq 0$, hence $u = (t-\alpha^q)\cdots(t-\alpha^{q^{l-1}})$ can be written of the form $u(t) = u_0 + u_1(t-\alpha) + u_2(t-\alpha)^2 + \cdots$ where $u_i \in \mathbb{F}_q$, hence $u \in \mathcal{O}_\alpha$. Our aim is to find $u_i, h_i \in \mathbb{F}_q[t]$ such that $g \equiv u_i^n + fh_i$ where

$u_i \equiv u_{i+1}(\text{mod } (t-\alpha)^i)$ and $h_i \equiv h_{i+1}(\text{mod } (t-\alpha)^i)$ for all $i = 0, 1, 2, \cdots$. We follow by induction. Write $f = (x-\alpha)u$, now $g(\beta) = c^n$ for some $c \in \mathbb{F}_q$, set $u_0 = c$ and the induction step holds for $i = 0$. Now assume it holds for $0, 1, \cdots, k$. Hence we have $g \equiv u_k^n + fh_k(\text{mod } (x-\alpha)^k)$ for some $u_k, h_k \in \mathbb{F}_q[t]$, we choose $u_{k+1} = u_k + U(x-\alpha)^k$ and $h_{k+1} = h_k + H(x-\alpha)^k$ for $U, H \in \mathbb{F}_q$ as follows;

$$g - u_{k+1}^n \equiv g - (u_k + U(x-\alpha)^k)^n - fh_{k+1} \equiv$$

$$\equiv g - u_k^n - nu_k^{n-1}U(x-\alpha)^k - fh_k - fH(x-\alpha)^k(\text{mod } (x-\alpha)^{k+1}),$$

On the other hand by induction step $g = u_k^n + fh_k(\text{mod } (x-\alpha)^k)$, hence $g = u_k^n + fh_k = (x-\alpha)^k g_1$ with $g_1 \in \mathcal{O}_\alpha$ writing this above the equation becomes;

$$g - u_{k+1}^n - fh_{k+1} \equiv (x-\alpha)^k(g_1 - fH - nu_k^{n-1}U)(\text{mod } (x-\alpha)^{k+1})$$

we want RHS to be 0, or equivalently;

$$g_1 - fH - nu_k^{n-1}U \equiv 0(\text{mod } (x-\alpha))$$

or $g_1(\alpha) - f(\alpha)H - nu_k^{n-1}(\alpha)U = 0$ solvable in $\mathbb{F}_q$. Taking $U = g_1(\alpha)\left(nu_k^{n-1}(\alpha)\right)^{-1}$ which is legal since characteristic is prime to n and $u_k(\alpha) \neq 0$, gives a solution. Hence we prove the assertion.

We now ask for generalizations. One can directly notice that the elements of the algebraic extension of field of $\mathbb{F}_q(t)$ should have symbols which have similar characterizations and properties that of $\mathbb{F}_q(t)$ since the residue field of a prime rational function is finite. However, contrary to $\mathbb{F}_q(t)$ case, the global treatment of such symbols is complicated. In case, we follow with local treatment, i.e. the process what we just postulated for $\mathbb{F}_q(t)$, which is advantageous since we know how to treat algebraic function fields locally. In the polynomial case the symbol (which is free of arithmetic treatment) was defined as $(f,g)_P = (-1)^{v_P(f)v_P(g)}\frac{f^{v_P(g)}}{g^{v_P(f)}}(P)$. There is no reason to apply this local treatment of polynomials to that of algebraic extensions. We define the symbol to be the just the same; if $K/\mathbb{F}_q(t)$ is finite algebraic extension, f, g are elements of K i.e. f, g are rational functions on some curve X associated to K, and P be a point on X. Let t local uniformizer at P and v_P be the valuation at P, i.e. if $f = t^a u$ with u is free of t, then $v_P(f) = a$. Then the symbol $(f,g)_P = (-1)^{v_p(f)v_p(g)}\frac{f^{v_P(g)}}{g^{v_p(f)}}(P)$ is well defined in this case. In the context we shall see that this symbol is just the analogue to that of polynomials and has similar characterization properties.

3.2 Definitions

3.2.1 Algebraic Curves

Algebraic extensions of the field $\mathbb{F}_q(t)$ will be called algebraic function fields. One may identify these fields by curves in the following. Let X be an algebraic curve over an algebraically closed field $\mathbb{F}_q$, i.e. X is an algebraic variety of dimension 1. We also suppose X is irreducible, non singular and complete. Let $\mathbb{F}_q(X)$ be the field of the rational functions on X. It is an extension of finite type of $\mathbb{F}_q$ of transcendence degree 1. Conversely, there always exists a curve X associated any finite type extension $K/\mathbb{F}_q$ with transcendence degree 1, which is unique up to isomorphism (refer to [21]). The study of X is thus equivalent to the study of the extension of $K/\mathbb{F}_q$ when the dimension of the variety is 1, hence there is no reason to insist on the difference between the 'geometric' methods and 'algebraic' methods.

3.2.2 Local Rings

Let P be point on X. The local ring $\mathcal{O}_P$ of X at P is defined as follows: suppose X is embedded in a projective space $\mathbb{P}_r(\mathbb{F}_q)$, it is the set of functions induced by rational functions of the type R/S where R and S are homogeneous polynomials of the same degree and where $S(P) \neq 0$. It is a subring of $\mathbb{F}_q(X)$; by virtue of the general properties of algebraic varieties, it is a Noetherian local ring whose maximal ideal $\mathfrak{m}_P$ is formed by the functions f vanishing at P and we have $\mathcal{O}_P/\mathfrak{m}_P = \mathbb{F}_q$. Since X is a curve, $\mathcal{O}_P$ is a local ring of dimension 1, in the same sense of the dimension theory for the local rings: its only prime ideals are (0) and $\mathfrak{m}_P$. Since P is a simple point of X, its maximal ideal can be generated by a single element; such element t will be called the local uniformizer at P. These properties imply that $\mathcal{O}_P$ is a discrete valuation ring, the corresponding valuation will be denoted by v_P (for complete treatment of such rings refer to next chapter). If $f \in \mathbb{F}_q(X)$ is a non zero element, $v_P(f) = n$, $n \in \mathbb{N}$ means that f is of the form $f = t^n u$ where t is local uniformizer at P and u is an invertible element of $\mathcal{O}_P$.

Furthermore, the rings $\mathcal{O}_P$ are the only valuation rings of $\mathbb{F}_q(X)$ containing $\mathbb{F}_q$; indeed, if U is such a ring, U dominates one of the $\mathcal{O}_P$ since X is assumed to be complete, thus coincides with $\mathcal{O}_P$ since $\mathcal{O}_P$ is a valuation ring.

3.3 The Symbols

Let $K/\mathbb{F}_q(t)$ be an algebraic function field and X be the irreducible, non singular complete curve associated to K. Let $f, g \in K$, hence one may see f as homomorphism from X to $\mathbb{P}_1$, or removing a finite set S including zeros and poles of f, one may assume that f is a homomorphism from $X - S$ to the multiplicative group $G_m = \mathbb{F}_q{}^*$. Instead of G_m, we begin with any commutative group G and any homomorphism $f : X - S \to G$. f extends linearly to group of divisors of X which are prime to S, i.e. $D = \sum_{i=1}^k n_i P_i$ where $n_i \in \mathbb{Z}$ and $P_i \in X - S$ then $f(D) = \prod_{i=1}^k f(P_i)^{n_i}$. Let $g \in K$ and $P \in X$, we want to define the symbol $(f, g)_P$ which takes values in G. In order to do that we define the notion of "modulus". A divisor $\mathfrak{m}$ of X is said to be modulus for f if $1 - g \equiv 0(\text{mod } \mathfrak{m})$ implies that $(f, g)_P = 1_G$. The notion of modulus comes naturally since we expect that if $g \equiv 1(\text{mod } f)$ or $g = 1 + fh$ then $g \equiv u^n(\text{mod } f)$ is soluble, hence it is soluble locally at P, hence taking $\mathfrak{m}$ as the divisor of (f) it is convenient to expect $(f, g) = 1_G$ for $g \equiv 1(\text{mod } f)$. We call $(f, g)_P$ a "symbol assignment" if it satisfies the properties: i) linearity on the second coordinate (that of the first coordinate is followed by linearity of f) $(f, g_1 g_2)_P = (f, g_1)(f, g_2)$, ii) values at $P \in X - S$ equal to $(f, g)_P = f(P)^{v_P(g)}$, iii) $(f, g)_P = 1_G$ for all $1 - g \equiv 0(\text{mod } \mathfrak{m})$, and iv) $\prod_{P \in X} (f, g)_P = 1_G$ the product formula. The proof will be followed by showing that there exists a symbol assignment if and only if there exist a modulus for f.

In the special case when $G = G_m = \mathbb{F}_q{}^*$ we will derive the reciprocity law in multiplicative form which corresponds to the case n is prime to characteristic, indeed we suppose $n | q - 1$ in order to have $\zeta_n \in \mathbb{F}_q$. In the special case when $G = G_a$ the additive group of $\mathbb{F}_q$ we will derive the reciprocity law in additive form which corresponds to the case $n = p$, where p is the characteristic of $\mathbb{F}_q$. In the additive case it comes out to be that the symbol $(f, g)_P$ is equal to $Res_P(f \frac{dg}{g})$, and the product formula is the exact analogue of the sum of residues of a differential on a Riemann surface is 0. This geometric structure is the source of inspiration in order to introduce "geometric" methods for algebraic number fields and to derive similar explicit reciprocity laws.

3.4 Reciprocity Laws

Let $k = \bar{\mathbb{F}_q}^{alg}$ be algebraic closure of $\mathbb{F}_q$, X be an algebraic curve which is irreducible, non-singular and complete. $k(X)$ be the field of rational functions on X. If S is a finite subset of X, $\mathfrak{m}$ denote an effective divisor with support in S i.e. $\mathfrak{m} = \sum n_P P$ with $n_P > 0$ for $P \in S$ and $n_P = 0$ for remaining P. If $g \in k(X)$ we write $g \equiv 1(\text{mod } \mathfrak{m})$ if $v_P(1-g) \geq n_P$ for every $P \in S$.

Note that if $g \equiv 1(\text{mod } \mathfrak{m})$ the divisor (g) is prime to S. Let G be a group and $f : X - S \to G$ be a map. f extends linearly to a homomorphism from the group of divisors prime to S to the group G. In particular, if $g \equiv 1(\text{mod } \mathfrak{m})$ then the element $f((g)) = \prod_{P \in X-S} f(P)^{v_P(g)}$

Definition 3.4.1 $\mathfrak{m}$ *said to be **modulus** for f if $f((g)) = 1_G$ for every $g \in k(X)$ with $g \equiv 1(mod\ \mathfrak{m})$.*

Definition 3.4.2 *Let $\mathfrak{m}$ modulus supported on S, $f : X - S \to G$ be a map. The map $X \times k(X)^* \to G$ which is indicated as $(f,g)_P$ is called a **local symbol** associated to f and to $\mathfrak{m}$ if it satisfies following conditions:*

i) $(f, gg') = (f,g)(f,g')$

ii) $(f,g)_P = 0$ *for $P \in S$ and $g \equiv 1(mod\ \mathfrak{m})$*

iii) $(f,g)_P = f(P)^{v_P(g)}$ *if $P \in X - S$*

iv) $\prod_{P \in X} (f,g)_P = 1.$

Proposition 3.4.3 $\mathfrak{m}$ *is a modulus for* f *if and only if there exist a local symbol associated to* f *and to* $\mathfrak{m}$*, and this symbol is unique.*

Proof: if part: Suppose that a local symbol exists, and $g \equiv 1(\text{mod } \mathfrak{m})$, $f((g)) = \prod_{P \in X-S} f(P)^{v_P}$ (by iii this is equivalent to) $= \prod_{P \in X-S}(f,g)_P$ (by iv this is equivalent to) $= (\prod_{P \in X-S}(f,g)_P)^{-1}$ (and by ii) this product is equivalent to 1.

only if part: Let $\mathfrak{m}$ modulus for f, we shall define a local symbol. For $P \in X - S$ define $(f,g)_P = f(P)^{v_P(g)}$ to have iii. For $P \in S$, by approximation theorem for valuations, we can find $g_P \in k(X)^*$ such that $g_P \equiv 1(\text{mod } \mathfrak{m})$ at the points $S - P$ and $g/g_P \equiv 1(\text{mod } \mathfrak{m})$ at P. Define;

$$(f,g)_P = (\prod_{Q \in X-S} f(Q)^{v_Q(g_P)})^{-1}$$

We claim that this is a local symbol assignment. First of all we show that this is well defined since if g'_P is another such function then clearly $g_P/g'_P \equiv 1(\text{mod } \mathfrak{m})$; and $(f, g_P/g'_P) = 1$ as $\mathfrak{m}$ is modulus for f.
$(f, g_P/g'_P) = 1 = (\prod_{Q \in X-S} f(Q)^{v_Q(g_P/g'_p)})^{-1} = (\prod_{Q \in X-S} f(Q)^{v_Q(g_P)}/f(Q)^{v_Q(g'_P)})^{-1} = \frac{\prod_{Q \in X-S} f(Q)^{v_Q(g_P)}}{\prod_{Q \in X-S} f(Q)^{v_Q(g'_P)}}$

Verification of i) Let $g, g' \in k(X)^*$, choose g_P, g'_P respectively as above;
$(f, gg')_P = (\prod_{Q \in X-S} f(Q)^{v_Q(g_P g'_P)})^{-1} = (\prod_{Q \in X-S} f(Q)^{v_Q(g_P)})^{-1}(\prod_{Q \in X-S} f(Q)^{v_Q(g'_P)})^{-1} = (f,g)(f,g')$ Verification of ii) if $g \equiv 1(\text{mod } \mathfrak{m})$ then $g_P \equiv 1(\text{mod } \mathfrak{m})$ and as $\mathfrak{m}$ modulus for f we have $(f,g)_P = 1$. Verification of iii) is by definition. Verification of iv) $\prod_{P \in S}(f,g)_P = (\prod_{P \in S}\prod_{Q \in X-S} f(Q)^{v_Q(g_P)})^{-1} = (\prod_{Q \in X-S} f(Q)^{v_Q(h)})^{-1}$ with $h = \prod_P g_P$, $g/h \equiv 1(\text{mod } \mathfrak{m})$ and $\mathfrak{m}$ is modulus for f thus;

$$\prod_{Q \in X-S} f(Q)^{v_Q(g/h)} = 1$$

$\prod_{P \in S}(f,g)_P = (\prod_{Q \in X-S} f(Q)^{v_Q(g)})^{-1} \prod_{Q \in X-S} f(Q)^{v_Q(g/h)} = (\prod_{Q \in X-S} f(Q)^{v_Q(g)})^{-1} = \prod_{Q \in X-S}(f,g)_Q$ by iii), and we finally get $\prod_{P \in X}(f,g)_P = 1$.
The uniqueness: the symbol is uniquely defined on $X - S$, if $P \in S$ by above we must have (by ii) $(f,g)_P^{-1} = (f,g_P)_P^{-1} = (\prod_{Q \in X-P}(f,g_P)_P) = \prod_{Q \in X-S}(f,g_P)_P \prod_{Q \in S-P}(f,g_P)_P$ = (by ii) = $\prod_{Q \in X-S}(f,g_P)_P$ =(by iii) $\prod_{Q \in X-S} f(Q)^{v(g_P)}$. This finishes the proof.

3.4.1 Multiplicative Reciprocity Law

Theorem 3.4.4 *If G is the multiplicative group G_m, f has $\mathfrak{m} = \sum_{P \in S} P$ as a modulus with the corresponding local symbol;*

$$(f, g)_P = (-1)^{v_P(f)v_P(g)} \frac{f^{v_P(g)}}{g^{v_P(f)}}(P)$$

(This formula is well defined since this quantity is different than 0 and ∞.)

Proof: We must verify i, ii, iii, iv. Verification of i); $(f, gg')_P = (-1)^{v_P(f)v_P(gg')} \frac{f^{v_P(gg')}}{gg'^{v_P(f)}}(P) = (-1)^{v_P(f)(v_P(g)+v_P(g'))} \frac{f^{v_P(g)} f^{v_P(g')}}{g^{v_P(f)} g'^{v_P(f)}}(P) = (-1)^{v_P(f)v_P(g)} \frac{f^{v_P(g)}}{g^{v_P(f)}}(P)(-1)^{v_P(f)v_P(g')} \frac{f^{v_P(g')}}{g'^{v_P(f)}}(P) = (f, g)_P(f, g')_P$. Verification of ii); if $v_P(1 - g) > 0$ then $v_P(g) = 0$, $(f, g)_P = \frac{1}{g^{v_P(f)}}(P) = 1$. Verification f iii); if $P \in X - S$ then $v_P(f) = 0$ and $(f, g)_P = f(P)^{v_P(g)}$. Verification of iv) Let $\mathbb{P}^1$ projective line. If g is constant, $\prod_{P \in X} (f, g)_P = g^{-\sum v_P(f)} = g^0 = 1$. If g is not constant, then it is surjective which makes X a ramified covering of $\mathbb{P}^1$. Putting $F = k(X)$ and $E = k(\mathbb{P}^1)$ we have extension F/E with $F = k(g)$ and the norm $N_{F/E} : F^* \to E^*$ is well defined. Denote the identity map on $\mathbb{P}^1$ by t. First we prove the formula for $X = \mathbb{P}^1$. We may write $f = \alpha_0 \prod (t - \alpha)^{n_\alpha}$ and $g = \beta_0 \prod (t - \beta)^{n_\beta}$. For $\alpha \neq \beta$; $(t - \alpha, t - \beta)_{P_0} = 1$ for $P_0 \neq \alpha, \beta, \infty$, $(t - \alpha, t - \beta)_\alpha = \alpha - \beta$, $(t - \alpha, t - \beta)_\beta = 1/(\beta - \alpha)$, $(t - \alpha, t - \beta)_\infty = -1$,
for $\alpha = \beta$; $(t - \alpha, t - \alpha)_{P_0} = 1$ for $P_0 \neq \alpha, \infty$, $(t - \alpha, t - \alpha)_\alpha = -1$, $(t - \alpha, t - \alpha)_\infty = -1$, thus we get $\prod_{P_0 \in \mathbb{P}^1} (t - \alpha, t - \beta)_{P_0} = 1$, moreover by above, $\prod_{P_0 \in \mathbb{P}^1} (\alpha_0, g)_{P_0} = 1 = \prod_{P_0 \in \mathbb{P}^1} (f, \beta_0)_{P_0}$ and as symbol is multiplicative in both coordinates by definition, we get $\prod_{P_0 \in \mathbb{P}^1} (f, g)_{P_0} = 1$. To prove the general case, we are going to reduce it to a local result. Let $P_0 \in \mathbb{P}^1$ and $P \in X$ with $g(P) = P_0$. The symbol $(f', g')_{P_0}$ make sense when f' and g' are in the field $\hat{E}_{P_0}$ (the field of completion of E with respect to valuation v_{P_0}). For convenience we denote this symbol by $(f', g')_{\hat{E}_{P_0}}$. Similarly, define $\hat{F}_P$ to be the completion of F with respect to v_P and denote the corresponding symbol by $(.,.)_{\hat{F}_P}$. $\hat{F}_P/\hat{E}_{P_0}$ is finite extension and we have the formula $N_{F/E} f = \prod_{g(P)=P_0} N_P f$ with N_P is the norm $N_{\hat{F}_P/\hat{E}_{P_0}}$. By linearity of symbols we have

$$(N_{F/Ef}, t) = \prod_{g(P)=P_0} (N_P f, t).$$

Assume now we proved $(f,g)_{\hat{F}_P} = (N_P f, t)_{\hat{E}_{P_0}}$, consequently; $\prod_{P\in X}(f,g)_P = \prod_{P_0\in\mathbb{P}^1}(\prod_{g(P)=P_0}(f,g)_P) = \prod_{P_0\in\mathbb{P}^1}(\prod_{g(P)=P_0}(f,g)_{\hat{F}_P}) = \prod_{P_0\in\mathbb{P}^1}(N_{F/E}f,t)_{P_0} = 1$. (Since $N_{F/E}f \in k(\mathbb{P}^1)$ and the product formula holds for $X = \mathbb{P}^1$.) Thus we are reduced to prove $(f,g)_{\hat{F}_P} = (N_P f, t)_{\hat{E}_{P_0}}$. Since $(f,g)_{\hat{F}_P}$ and $(N_P f, t)_{\hat{E}_{P_0}}$ are multiplicative in f and in g by definition, it sufficies to do the proof when f and g are uniformizer of $\hat{F}_P$ and $\hat{E}_{P_0}$ respectively, (since every unit is quotient of two uniformizers and fields are multiplicatively generated by units and uniformizers). We thus have $\hat{F}_P = k((f))$ and $\hat{E}_{P_0} = k((g))$. $v_{\hat{E}_{P_0}}(N_P f) = v_{\hat{F}_P}(f) = 1$ hence $((N_P f, t)_{\hat{E}_{P_0}}) = -\frac{N_P f}{g}(P_0)$. On the other hand if the ramification index of f over $\hat{E}_{P_0}$ is e, then we have that $[\hat{F}_P : \hat{E}_{P_0}] = e$, and $v_{\hat{F}_P}(g) = e$, whence $(f,g)_{\hat{F}_P} = (-1)^e \frac{f^e}{g}(P)$. Comparing formula above we want this to be equal to $-\frac{N_P f}{g}(P_0)$ i.e $\frac{N_P f}{f^e} = (-1)^{e-1}$ at P (or P_0, it is the same).

As totally ramified with degree e, f has minimal polynomial for over $\hat{E}_{P_0}$ an Eisenstein polynomial of degree e i.e. minimal polynomial is of the form $f^e + a_1 f^{e-1} + \cdots + a_e = 0$ with $a_i \in \hat{E}_{P_0}$, $v_{\hat{E}_{P_0}}(a_0) = 1$ and $v_{\hat{E}_{P_0}}(a_i) \geq 1$. Clearly $a_e = (-1)^e N_P f(P)$. $v_{\hat{F}_P}(a_i f^{e-i}) = e v_{\hat{E}_{P_0}}(a_i) + e - i \geq 2e - i$, hence $v_{\hat{F}_P} \frac{a_i f^{e-i}}{f^e} \geq e - i > 0$. $v_{\hat{F}_P}(f^e + a_e) = v_{\hat{F}_P}(-a_1 f^{e-1} + \cdots + a_{e-1} f)$, dividing both sides by f^e; $v_{\hat{F}_P}(1 + \frac{a_e}{f^e}) = v_{\hat{F}_P}(-\frac{a_1}{f} - \cdots - \frac{a_{e-1}}{f^{e-1}}) > 0$ since all the monomials satisfy $v_{\hat{F}_P} \frac{a_i}{f^i} > 0$. Therefore, we have $v_{\hat{F}_P}(1 + \frac{a_e}{f^e})$ takes value 0 at P, hence $1 = \frac{-a_e}{f^e} = \frac{(-1)^{e-1} N_P f}{f^e}$ as desired.

Remark 3.4.5 *As with the quadratic norm residue symbol* $\left(\frac{a,b}{p}\right)$, *the symbol* $(f,g)_P$ *has the following properties* $(f,g)_P (g,f)_P = 1$, $(-f,f)_P = 1$ *and* $(1-f,f)_P = 1$. *These properties, indeed, hold for norm residue symbol (Hilbert symbol) in general.*

We get the following result which is due to A. Weil [26];

Proposition 3.4.6 (Weil Reciprocity Law) *If f and g are two functions on X with disjoint divisors then*

$$f((g)) = g((f))$$

Proof: By theorem 3.4.6 above we have $\prod P \in X(f,g)_P = 1$. $(f,g)_P$ is either $f(P)^{v_P(g)}$ or $g(P)^{-v_P(f)}$ thus $f((g))g(-(f)) = 1$ and $f((g)) = g((f))$ as desired.

3.4.2 Arithmetic

$(f,g)_P$ is the element of the field $\mathbb{F}_q(P)/\mathbb{F}_q$ which is non zero. We now want to define a multiplicative surjective map which sends $(f,g)_P$ to ζ_n satisfying $(f,g)_P \to 1$ if and only if $(f,g)_P$ is an n-th power in $\mathbb{F}_q(P)$. One may prove that a number $a \in \mathbb{F}_q(P)$ is an n-th power in $\mathbb{F}_q(P)$ is and only if $N_{\mathbb{F}_q(P)/\mathbb{F}_q}(a)$ is an n-th power in $\mathbb{F}_q$ (just by the same method used for polynomials). We follow a slightly different way;

Proposition 3.4.7 *$a \in \mathbb{F}_q(P)$ is an n-th power in $\mathbb{F}_q(P)$ is and only if $N_{\mathbb{F}_q(P)/\mathbb{F}_q}(a)$ is an n-th power in $\mathbb{F}_q$*

Proof: Let c_P be a generator of the multiplicative group $\mathbb{F}_q(P)^*$, since $N_{\mathbb{F}_q(P)/\mathbb{F}_q}$ is surjective homomorphism of $\mathbb{F}_q(P)^*$ onto ${\mathbb{F}_q}^*$, then $N_{\mathbb{F}_q(P)/\mathbb{F}_q}(c_G) = c$ is a generator of ${\mathbb{F}_q}^*$. If $a \in \mathbb{F}_q(P)^*$ with $a = c_G^{a_1}$, $a_1 \in \{0, 1, \cdots, q-1\}$, then

$$N_{\mathbb{F}_q(P)/\mathbb{F}_q}(a) = N_{\mathbb{F}_q(P)/\mathbb{F}_q}(c_G^{a_1}) = N_{\mathbb{F}_q(P)/\mathbb{F}_q}(c_G)^{a_1} = c^{a_1}$$

a is an n-th power in $\mathbb{F}_q(P)^*$ if and only if $n|a_1$ and this is if and only if $N_{\mathbb{F}_q(P)/\mathbb{F}_q}(a)$ is an n-th power in ${\mathbb{F}_q}^*$.

A number in ${\mathbb{F}_q}^*$ is determined to n-th power in ${\mathbb{F}_q}^*$ is determined up to taking the $\frac{q-1}{n}$-th power of the number. Combining all these results, we get the explicit form of multiplicative reciprocity;

Theorem 3.4.8

$$\left(\frac{f,g}{P}\right) = \left(N_{\mathbb{F}_q(P)/\mathbb{F}_q}((-1)^{v_P(f)v_P(g)}\frac{f^{v_P(g)}}{g^{v_P(f)}}(P))\right)^{\frac{q-1}{n}}.$$

where $\left(\frac{f,g}{P}\right)$ denotes the norm residue symbol for the field of rational functions on $\mathbb{F}_q(X)$.

As consequence, we have the reciprocity law as corollary;

Corollary 3.4.9 (Reciprocity Relation) *Let $f, g \in \mathbb{F}_q(X)$ with $supp(f) \cap supp(g) = S$, where supp denotes the set of poles of the function. Then;*

$$\left(\frac{f}{g}\right)_n \left(\frac{g}{f}\right)_n = \prod_{P \in S} \left(\frac{g, f}{P}\right)_n .$$

3.4.3 Additive Reciprocity Law

We are going to verify the theorem 3.4.4 in the case where the group $G = G_a$ additive group of $\mathbb{F}_q$. We assume that $f : X - S \to G_a$ being a regular map. We can consider f as a rational map from X to G regular away from S. We also suppose that S is the smallest subset of X having this property.

Theorem 3.4.10 *f has a modulus supported on S, the corresponding local symbol being $(f, g)_P = Res_P(f\frac{dg}{g})$.*

Remark 3.4.11 *$Res_P(f)$ is defined as follows; let t be a uniformizing element at P, write $f = \sum_{i>>-\infty}^{\infty} f_i t^i$ where f_i are in the residue field. Then $Res_P(f)$ defined to be $Res_P(f) = f_{-1}$. The formula $Res_P(f\frac{dg}{g})$ make sense since f is a scalar function on X with S as its set of poles. This definition, indeed, is independent of the choice of the uniformizing element t and is well defined. For proof we refer to [20], [6].*

Proof: If P belongs to S, we put $n_P = 1 - v_P(f)$; from the fact that P is a pole of f, we have $n_P > 1$. We are going to check that $Res_P(f\frac{dg}{g})$ is a local symbol associated to f and $\mathfrak{m} = \sum n_P P$.

Property i) is clear, from the fact that

$$\frac{d(gg')}{gg'} = \frac{dg}{g} + \frac{dg'}{g'}.$$

For ii), we remark that, if $v_P(1-g) \geq n_P$ then

$$v_P(dg) \geq n_P - 1 \geq -v_P(f);$$

as $v_P(g) = 0$ we deduce that $v_P(f\frac{dg}{g}) \geq 0$, whence $Res_P(f\frac{dg}{g}) = 0$. For iii), we remark that $\frac{dg}{g}$ has a simple pole at P, thus so does $f\frac{dg}{g}$ (since $P \notin S$) and we have

$$Res_P(f\frac{dg}{g}) = f(P)Res_P(\frac{dg}{g}) = f(P)v_P(g),$$

Finally, the formula iv):

$$\sum_{P\in X} Res_P(f\frac{dg}{g}) = 0$$

is just the residue formula $\sum_{P\in X} Res_P(f\frac{dg}{g}) = 0$ for any differential $f\frac{dg}{g}$ on $\mathbb{F}_q(X)$. We leave the proof of the residue formula to [20], [6].

Corollary 3.4.12

$$Res_P(f^p\frac{dg}{g}) = [Res_P(f\frac{dg}{g})]^p.$$

Where p is the characteristic of the field $\mathbb{F}_q$.

Proof: Indeed, the map $x \to x^p$ is a homomorphism $G_a \to G_a$ and we have that the local symbols are functorial.

3.4.4 Arithmetic

We have that $(f,g)_P = Res_P(f\frac{dg}{g}(P))$ is an element of $\mathbb{F}_p(P)$. The trace operator $Tr_{\mathbb{F}_p(P)/\mathbb{F}_p}$ is well defined and take values in $\mathbb{F}_p$. It comes out to be ([20], [21], [27]) that trace operator plays the same role for additive symbol as the norm operator for multiplicative symbol.

Theorem 3.4.13

$$\left(\frac{f,g}{P}\right) = Tr_{\mathbb{F}_p(P)/\mathbb{F}_p}\left(Res_P(f\frac{dg}{g})\right)$$

where $\left(\frac{f,g}{P}\right)$ denotes the norm residue symbol for the field of rational functions on $\mathbb{F}_p(X)$.

Remark 3.4.14 *One can define this symbol multiplicatively which assume values in p-th roots of unity in such way that setting*

$$\left(\frac{f,g}{P}\right) = \zeta_p^{Tr_{\mathbb{F}_p(P)/\mathbb{F}_p}\left(Res_P(f\frac{dg}{g})\right)}.$$

where $Tr_{\mathbb{F}_p(P)/\mathbb{F}_p}\left(Res_P(f\frac{dg}{g})\right)$ *is assumed to have a value in* $\{0, 1, 2, \cdots, p-1\}$.

Remark 3.4.15 *These formulas are due to H. L. Schmidt. [19]*

Chapter 4

Motivations Through the Quadratic Reciprocity

In the quadratic case, the quadratic residue symbol $\left(\frac{a}{p}\right)$ was identified with the solubility of $a \equiv x^2(\text{mod } p^k)$ for all $k \in \mathbb{N}$. The case where $p \not| 2$ or $p \not| a$, the solubility of $a \equiv x^2(\text{mod } p^k)$ for all k is equivalent to solubility of $a \equiv x^2(\text{mod } p)$. This follows by induction; assume $a \equiv x^2(\text{mod } p^k)$ soluble for $x = x_0$, set now $x = x_0 + cp^k$, hence $a - (x_0 + cp^k)^2 \equiv a - x_0^2 - 2x_0cp^k(\text{mod } p^{k+1})$, setting $c \equiv \frac{a-x_0^2}{p^k}\frac{1}{2x_0}(\text{mod } p)$ we have solution for p^{k+1}, inductively we get the assertion.

The idea of solubility of $a \equiv x^2$ equation in modulo powers of p is indeed equivalent to the solubility of $x^2 - ay^2 - bz^2 = 0$ in p-adic integers x, y, z with at least one is non-zero. We recall the p-adic numbers; $\mathbb{Q}_p = \{\sum_{i>>-\infty}^{\infty} a_i p^i : a_i \in \mathbb{Z}_p\}$ is called the p-adic field and elements of its ring of integers $\mathcal{O}_p = \{\sum_{i\geq 0}^{\infty} a_i p^i : a_i \in \mathbb{Z}_p\}$ are called the p-adic integers. Representing the rational numbers in power series of p with coefficients in $\mathbb{Z}_p$ has analogy with representing the rational functions of an algebraic function field by Taylor series in powers of uniformizer at some point P with coefficients from finite field $\mathbb{F}_p$. Consequently, the p-adic field impose a local analytic structure analogue to that of algebraic function fields over $\mathbb{F}_p$, and this structure provides certain tools for solubility of the equation above.

4.1 Norm Residue Symbol

On the other hand, the solubility of the equation $x^2 - ay^2 - bz^2 = 0$ itself suggest the solubility of $x^2 - ay^2 = bz^2$, equivalently; $(\frac{x}{z})^2 - a(\frac{x}{z})^2 = b = \left(\frac{x}{z} - \sqrt{a}\frac{y}{z}\right)\left(\frac{x}{z} + \sqrt{a}\frac{y}{z}\right)$ (assuming $z \neq 0$ without lost of generality) which is equivalent to the assertion 'b is a norm in the extension $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$'.

We now define the notion of quadratic norm residue symbol; Let p is a prime and a and b are integers coprime to p. $\left(\frac{a,b}{p}\right) = 1$ if $x^2 - ay^2 - bz^2 = 0$ is solvable in p-adic integers x, y, z with at least one is non-zero and $\left(\frac{a,b}{p}\right) = -1$ otherwise. First we note that this symbol can be extended multiplicatively to integers A, B which are not coprime to p in following; let $A = p^{A_p}a_p$ and $B = p^{B_p}b_p$ with a_p, b_p are coprime to p. Set

$$\left(\frac{A,B}{p}\right) = \left(\frac{p^{A_p}a_p, p^{B_p}b_p}{p}\right) = \left(\frac{p,p}{p}\right)^{A_pB_p}\left(\frac{a_p,p}{p}\right)^{B_p}\left(\frac{p,b_p}{p}\right)^{A_p}\left(\frac{a_p,b_p}{p}\right).$$

Assume now $p \neq 2$. One may calculate that $x^2 - py^2 - pz^2 = 0$ soluble then $p|x$, writing $x = px_1$ and dividing by p the equation becomes $x_1^2 = p(y^2 + z^2)$, then $p|y^2 + z^2$, assuming at least one y, z is not divisible by p (if so divide through powers p), hence this is equivalent to $y^2 \equiv -z^2 (\text{mod } p)$ or $-1 \equiv (\frac{y}{z})^2 (\text{mod } p)$ and this is if and only if $\left(\frac{-1}{p}\right) = 1$, hence we have $\left(\frac{p,p}{p}\right) = (-1)^{\frac{p-1}{2}}$. In addition, $\left(\frac{p,b_p}{p}\right) = \left(\frac{b_p,p}{p}\right) = \left(\frac{b_p,p}{p}\right)^{-1}$, combining these results we rewrite the norm residue symbol as:

$$\left(\frac{A,B}{p}\right) = \left(\frac{p^{A_p}a_p, p^{B_p}b_p}{p}\right) = (-1)^{A_pB_p\frac{p-1}{2}}\left(\frac{a_p,p}{p}\right)^{B_p}\left(\frac{b_p,p}{p}\right)^{-A_p}\left(\frac{a_p,b_p}{p}\right) =$$

$$= (-1)^{\frac{p-1}{2}a_pb_p}\left(\frac{a_p}{p}\right)^{B_p}\left(\frac{b_p}{p}\right)^{-A_p}.$$

since for $p \neq 2$ $\left(\frac{a_p,b_p}{p}\right) = 1$ and $\left(\frac{a_p,p}{p}\right) = \left(\frac{a_p}{p}\right)$. For $p = 2$, the solubility of $x^2 - py^2 - pz^2 = 0$ in 2-adic integers is not equivalent to solubility of this equation in mod 2, but rather is equivalent to solution of this equation in mod 8.

Writing $a \equiv 2^{a_1}(-1)^{a_1'}(1+2^2)^{a_2''} \pmod 8$ and $b \equiv 2^{b_1}(-1)^{b_1'}(1+2^2)^{b_2''} \pmod 8$, and setting

$$\left(\frac{a,b}{2}\right) = (-1)^{a_2 b_2'' + a_1' b_1' + a_2'' b_2},$$

one may easily check that this symbol is multiplicative, and for 16 values of $(a, b) \equiv (1, 1), (1, 3), (1, 5), (1, 7), \cdots, (7, 7) \pmod 8$ this symbol coincide with the solubility of $x^2 - ay^2 - bz^2 = 0$ in 2-adic integer, with at least one is non zero.

The p-adic field has the following absolute value; $|a|_p = p^{-a_1}$ if $a = p^{a_1}a_2$ with a_2 has no p divisor. $|\ |_p$ impose a topology on $\mathbb{Q}_p$ and hence a local analytic structure on $\mathbb{Q}$. In addition to local analytic structures, $\mathbb{Q}$ imposes a global analytic structure. The coordinates the global analytic structure consist of coordinates which are generated by p-adic absolute values plus the ordinary absolute value $|\ |$ of $\mathbb{R}$. For completeness, we shall also treat the latter field as p-adic identification of $\mathbb{Q}$ by a 'prime' which is called as 'infinite prime' and denoted by ∞. The norm residue symbol $\left(\frac{a,b}{\infty}\right)$ is determined by the solubility of $x^2 - ay^2 - bz^2 = 0$ in real numbers. Hence $\left(\frac{a,b}{\infty}\right) = 1$ if at least one of a, b is non negative, and $\left(\frac{a,b}{\infty}\right) = -1$ otherwise.

We have the following evident properties for the norm residue symbol;

$\left(\frac{a,b}{p}\right)$ depends only on residue classes a, b mod p and mod 8

$\left(\frac{a,b}{p}\right) \neq 1$ for finitely many p,

$\left(\frac{aa',b}{p}\right) = \left(\frac{a,b}{p}\right)\left(\frac{a',b}{p}\right)$

$\left(\frac{a,bb'}{p}\right) = \left(\frac{a,b}{p}\right)\left(\frac{a,b'}{p}\right)$

$\left(\frac{a,b}{p}\right)\left(\frac{b,a}{p}\right) = 1$

We have less evident property of the norm residue symbol known as the 'product formula';

Proposition 4.1.1 *For arbitrary non-zero integers a, b;*

$$\prod_{p\in\mathcal{P}\cup\{\infty\}}\left(\frac{a,b}{p}\right)=1.$$

where $\mathcal{P}$ denotes the set of primes.

Proof: By virtue of properties of multiplication and symmetry, it is sufficient to check the formula for $(-1,-1),(-1,2),(-1,q),(2,2),(2,q),(q,q),(q,q')$ where q and q' are distinct odd primes. Since $x^2+y^2-2z^2$ and $x^2-2y^2-2z^2$ has integer solution $1,1,1$ and $2,1,1$ respectively, $\left(\frac{-1,2}{p}\right)=1=\left(\frac{2,2}{p}\right)$ and for all p hence the product formula.

$\left(\frac{q,q'}{2}\right)=(-1)^{\frac{q-1}{2}\frac{q'-1}{2}}$, $\left(\frac{q,q'}{q}\right)=\left(\frac{q'}{q}\right)$, $\left(\frac{q,q'}{q'}\right)=\left(\frac{q}{q'}\right)$ and $\left(\frac{q,q'}{p}\right)=1$ for $p\neq 2,q$

$\left(\frac{-1,-1}{\infty}\right)=-1=\left(\frac{-1,-1}{2}\right)$ and $\left(\frac{-1,-1}{p}\right)=1$ for all odd prime p.

$\left(\frac{-1,q}{2}\right)=(-1)^{\frac{q-1}{2}}$, $\left(\frac{-1,q}{p}\right)=1$ for $p\neq 2,q$ and $\left(\frac{-1,q}{q}\right)=(-1)^{\frac{q-1}{2}}$.

$\left(\frac{2,q}{2}\right)=(-1)^{\frac{q^2-1}{8}}$,$\left(\frac{2,q}{q}\right)=(-1)^{\frac{q^2-1}{8}}$ and $\left(\frac{2,q}{p}\right)=1$ for $p\neq 2,q$

$\left(\frac{q,q}{2}\right)=(-1)^{\frac{q-1}{2}\frac{q-1}{2}}=(-1)^{\frac{q-1}{2}}$, $\left(\frac{q,q}{q}\right)=(-1)^{\frac{q-1}{2}}$ and $\left(\frac{q,q}{p}\right)=1$ for $p\neq 2,q$

hence the product formula holds.

We may now recover the quadratic reciprocity law from the properties of the norm residue symbol in following. Let a and b odd coprime integers, then $\left(\frac{a,b}{p}\right)$ is either $\left(\frac{a}{p}\right)^{\beta_p}$ or $\left(\frac{b}{p}\right)^{-\alpha_p}$ where α_p and β_p is the exact powers of p in a and b respectively. If we take the product over all odd primes we have $\prod_{p\in\mathbb{P}-\{2\}}\left(\frac{a,b}{p}\right)=\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}$ where $\mathbb{P}$ denotes the set of primes. Combining this fact with the product formula we get

$$\prod_{p\in\mathbb{P}\cup\{\infty\}}\left(\frac{a,b}{p}\right)=1=\prod_{p\in\mathbb{P}-\{2\}}\left(\frac{a,b}{p}\right)\left(\frac{a,b}{2}\right)\left(\frac{a,b}{\infty}\right)=\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}\left(\frac{a,b}{2}\right)\left(\frac{a,b}{\infty}\right)$$

or equivalently

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \left(\frac{b,a}{2}\right)\left(\frac{b,a}{\infty}\right) = (-1)^{\frac{(a-1)(b-1)}{4}}(-1)^{\frac{(sqn(a)-1)(sqn(b)-1)}{4}}$$

hence we get the reciprocity from properties of the norm residue symbol. In addition, we obtain the supplementary laws by putting $a = 2$ and $a = -1$ in the product formula.

This is a transparent illustration of how reciprocity relation is treated for general case. Definitions and the notations get more complicated, however the backbone of the theory remains the same. Norm residue symbol is generalized and its properties are proved by using the local techiques. Power residue symbol is identified by the norm residue symbol. This identification together with the product formula give the reciprocity relation in general.

4.2 Decomposition of Primes

We now return to identification of solubility $x^2 - ay^2 - bz^2 = 0$ is equivalent to 'b is a norm in the extension $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$'. The extension $\mathbb{Q}_p(\sqrt{a})$ is indeed a $\mathfrak{P}$-adic field of $\mathbb{Q}(\sqrt{a})$ for some prime ideal $\mathfrak{P}$ dividing (p). We hence need to know how primes of $\mathbb{Q}$ are decomposed into the primes of the extension $\mathbb{Q}(\sqrt{a})$. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Q}_p(\sqrt{a})$ with $\mathbb{Q}(\sqrt{a})(p) \subset \mathfrak{P}$, we say $\mathfrak{P}$ **divides** (or **above**) (p). Up to taking conjugates, we have that (p) either remains prime, or is product of two different prime ideals or is a square of a prime ideal of the field $\mathbb{Q}(\sqrt{a})$. We denote these situations by $(p) = \mathfrak{P}_0$, $(p) = \mathfrak{P}_1\mathfrak{P}_2$ and $(p) = \mathfrak{P}_3^2$ respectively. The residue field of $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3$ has p elements whereas that of $\mathfrak{P}_0$ has p^2 elements. This is the case in general; suppose K is number field and L/K is finite abelian extension of K. Let $\mathfrak{p}$ be a prime ideal of K, then $\mathfrak{p} = \mathfrak{P}_1^e\mathfrak{P}_2^e \cdots \mathfrak{P}_g^e$ where $\mathfrak{P}_i$ are distinct prime ideals of L and each residue field has $(N\mathfrak{p})^f$ elements where $N\mathfrak{p}$ is cardinality of the residue field of $\mathfrak{p}$. One has the relation $efg = n$ where $n = [L : K]$. We call $\mathfrak{p}$ is **unramified** in L if $e = 1$, and **ramified** if $e > 1$. The primes of $\mathbb{Q}$ which are ramified at $\mathbb{Q}(\sqrt{a})$ are, as we shall the proof in the 'Kummer Fields' section of the following chapter, those which divide 2 or a.

4.3 Localization

The field $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ is extension of local $\mathbb{Q}_p$, and is itself a local field. It's maximal ideal is constructed by a prime ideal $\mathfrak{P}$ of $\mathbb{Q}(\sqrt{a})$ which is above (p). $\mathfrak{P}$ is generated by an element π, and the field $\mathbb{Q}_p(\sqrt{a}) = \{\sum_{i>>-\infty}^{\infty} a_i\pi^i : a_i \in \mathfrak{R}\}$ where $\mathfrak{R}$ is the set representatives of residue field $\mathfrak{P}$.

When (p) is unramified at $\mathbb{Q}(\sqrt{a})$ and b is integer coprime to a, the identification of b being norm in the extension $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ has a transparent determination as follows. Rewrite the unramified cases $(p) = \mathfrak{P}_0$ and $(p) = \mathfrak{P}_1\mathfrak{P}_2$ by above. Let $b \in \mathbb{Q} \subset \mathbb{Q}_p$, we are interested in if b is a norm in the extension $\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p$ of some element $\gamma = a_0 + a_1\pi_\beta + a_2\pi_\beta^2 + \cdots \in \mathbb{Q}_p(\sqrt{a})$. In the first case the residue field has p^2 elements. The elements of the residue field can be chosen of the form $\{u + v\sqrt{a}\}$ where $u, v \in \{0, 1, \cdots, p-1\}$, and the uniformizer can be chosen $\pi = p$. Hence $b = N\gamma$ implies $b = (b_0 + b_1\pi + a_2\pi^2 + \cdots)(\bar{a}_0 + \bar{a}_1\pi + \bar{a}_2\pi^2 + \cdots)$. Checking the equation mod $\mathfrak{P}^k$, this amounts to the solution of $a \equiv x^2(\text{mod } p^k)$ for all $k \in \mathbb{N}$. In the second case, extension with respect to prime $\mathfrak{P}_1$ is isomorphic to the extension with respect to prime $\mathfrak{P}_2$ which is evident up to conjugation. Without loss of generality we may assume $\mathfrak{P} = \mathfrak{P}_1$. The residue field has p elements, and uniformizer is of the form $\pi = u + v\sqrt{a}$ where $N(\pi) = p$. $b = N\gamma$ implies $b = (a_0 + a_1\pi + a_2\pi^2 + \cdots)(a_0 + a_1\bar{\pi} + a_2\bar{\pi}^2 + \cdots)$ which amounts to the solution of $a \equiv x^2(\text{mod } \mathfrak{P}^k)$ for all $k \in \mathbb{N}$. The induction procedure introduced at the beginning of the chapter can be applied to this case without any difficulties, consequently b being norm is equivalent to the solution $b \equiv x^2(\text{mod } \mathfrak{P})$.

We can determine the solubility of $b \equiv x^2(\text{mod } \mathfrak{P})$ as follows. The residue field of $\mathfrak{P}$ is finite, hence its multiplicative group is cyclic and generated by some element c. Write $b \equiv c^B(\text{mod } \mathfrak{P})$ then

$$b \equiv x^2(\text{mod } \mathfrak{P}) \Leftrightarrow b \equiv x^2(\text{mod } p) \Leftrightarrow 2|B \Leftrightarrow b^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$$

In both unramified cases since $\mathfrak{P} \not| b$

$$b^{\frac{p-1}{2}} \equiv \sqrt{b}^{p-1} \equiv 1(\text{mod } \mathfrak{P}) \Leftrightarrow \sqrt{b}^{p} \equiv \sqrt{b}(\text{mod } \mathfrak{P}).$$

On the other hand, the Galois group $G(\mathbb{Q}_{\mathfrak{P}}(\sqrt{a})/\mathbb{Q}_p)$ comes out to be cyclic with a generator σ which is characterized by;

$$\sigma(\gamma) \equiv \gamma^p (\text{mod } \mathfrak{P})$$

for all γ in the ring of integers of $\mathbb{Q}_p(\sqrt{a})$. This automorphism is called the **Frobenius automorphism**. The quadratic norm residue symbol take the value of 2nd root of unity $\frac{\sigma(\sqrt{a})}{\sqrt{a}}$.

4.4 Globalization

The norm residue symbol is characterized by Frobenious automorphism in unramified primes, however, in ramified primes we don't have such explicit characterization. This is because in unramified cases the norm residue symbol acts on the multiplicative group of the residue field. This group is cyclic with a generator which allows the explicit determination of the symbol. In ramified cases, the norm residue symbol acts on additive group or on both multiplicative and additive groups, and since the additive group of the residue field is not acting so 'regularly' the explicit identification is not as direct as in the previous case. This is, indeed the reason why quadratic norm residue symbol is in a more complicated form at 2 than that of at odd primes. In general, as we shall see, such primes are the ones which divide the power n if we are to find n-th power reciprocity relation.

In the quadratic case, the only 'irregular' prime is 2 we treated this case by explicit definition of the symbol by using certain form of decomposition. In general case, we can not always have give such an explicit definition. To treat this problem we introduce the global analytic structure on field coordinates of which are generated by local p-adic fields. We next continuously extend the definition of the norm residue symbol to all primes which is equivalent to that of identified by the Frobenious automorphism at unramified primes. We briefly explain this process for quadratic case. Denoting the Frobenious automorphism for unramified prime p by $(p, \mathbb{Q}(\sqrt{a})/\mathbb{Q})$ we have $p \to (p, \mathbb{Q}(\sqrt{a})/\mathbb{Q})$ is a map from unramified prime ideals into $G(\mathbb{Q}_{\mathfrak{P}}(\sqrt{a})/\mathbb{Q}_p) \subset G(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ (this is evident since any automorphism of $\mathbb{Q}_{\mathfrak{P}}(\sqrt{a})$ fixing $\mathbb{Q}_p$ gives an automorphism of $\mathbb{Q}(\sqrt{a})$ fixing $\mathbb{Q}$). This map can be extended multiplicatively in obvious way to all ideals which contains no ramified primes. The extended map has a special name as the **global Artin map**. If principal ideal (b) has no ramified prime divisor and $(b) = \mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_r^{b_r}$ then set;

$$((b), \mathbb{Q}(\sqrt{a})/\mathbb{Q}) = (\mathfrak{p}_1, \mathbb{Q}(\sqrt{a})/\mathbb{Q})^{b_1}(\mathfrak{p}_2, \mathbb{Q}(\sqrt{a})/\mathbb{Q})^{b_2}\cdots(\mathfrak{p}_r, \mathbb{Q}(\sqrt{a})/\mathbb{Q})^{b_r}$$

and $((b), \mathbb{Q}(\sqrt{a})/\mathbb{Q})(\sqrt{a}) \equiv (-1)^i\sqrt{a}(\mathrm{mod}\ \mathfrak{P})$ for some $i \in \mathbb{N}$. The ratio $\frac{((b),\mathbb{Q}(\sqrt{a})/\mathbb{Q})(\sqrt{a})}{\sqrt{a}}$ comes out to be the quadratic residue symbol which is equal to $(-1)^i$.

We now indicate the global analytic structure. Let S denote the set of ramified primes of the abelian extension L/K plus the set of infinite primes. Denote the set of ideals of K which are coprime to primes of S by I^S, then the Artin symbol is a multiplicative map from I^S to $G(L/K)$. Define the coordinate system whose coordinates are identified by primes including infinite primes. We define an **idele** to be a vector of this coordinate system whose coordinates are in the multiplicative sets of corresponding fields. The set of ideles whose almost all coordinates are units impose a topology, which is called restricted product topology. The Artin symbol is considered to be a multiplicative map from the set of ideles J^S whose S components are 1 to $G(L/K)$ in canonical way. A theorem of Artin states that this multiplicative map extends continuously to all ideles in unique way. This map is called the **global Artin map** and denoted by $\psi_{L/K}$. The image of the ideles whose $\mathfrak{p}$th coordinate is x and other coordinates are 1 defines a map $\psi_{\mathfrak{p}}(x)$ what is called the **local Artin map**. We determine the most general form of norm residue symbol $\left(\frac{a,b}{\mathfrak{p}}\right)$ as the image of $\psi_{\mathfrak{p}}(b)$ in L/K. In the quadratic case, $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{a})$; and the norm residue symbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ coincide with $\psi_{\mathfrak{p}}(b)$ in the extension $L = \mathbb{Q}(\sqrt[n]{a})$.

Chapter 5

Global Fields

In this chapter we define the global fields, the general form of algebraic function fields and algebraic number fields. We show that the global fields admit local analytic structure which is similar to that of algebraic function fields, indeed, former is the generalization of the letter. Next, we generalize the global analytic structure of algebraic function fields to global fields.

5.1 Global Fields

We start with defining the general form of fields where we treat the algebraic function fields case and algebraic number fields case together. These fields are the rational fields of 'Dedekind domains'. In this section we define Dedekind domains and define the required machinery which is used in following chapter for the proof of the reciprocity relation.

5.1.1 Dedekind Domains

Definition 5.1.1 *K^* be the multiplicative group of the field K, $\mathbb{Z}$ denote the integers under addition, a map*

$$v : K \to \mathbb{Z} \cup \infty$$

is a ***discrete valuation*** *of K if*

i) *v defines a surjective homomorphism $K^* \to \mathbb{Z}$*

ii) *$v(0) = \infty$*

iii) *$v(x + y) \geq \inf v(x), v(y)$.*

The set $R_v = \{x \in K | v(x) \geq 0\}$ is an integral domain with quotient field K, the **valuation ring** of v, and the set $\mathfrak{p}_v = \{x \in K | v(x) > 0\}$ is a maximal ideal of R_v, is called the **valuation ideal**.

Remark 5.1.2 *Let F be a field let K be the field of formal series $\sum_{i>>-\infty}^{\infty} a_i t^i$, with $a_i \in F$. Then we have a discrete valuation v of K given by*

$$v(\sum_{i>>-\infty}^{\infty} a_i t^i) = \inf_{a_i \neq 0} i$$

The elements u with $v(u) = 0$ form a subgroup U_v of K, the group of units (invertible elements) of R_v. We now choose an element π with $v(\pi) = 1$. Then every $a \in K^*$ has a unique representation $a = \pi^{a_1} u$, $a_1 \in \mathbb{Z}$, $u \in U_v$, namely with $a_1 = v(a)$.

Let I be the fractional ideal of R_v, we define $v(I) = \inf_{x \in I} v(x)$, so $v(I) \in \mathbb{Z} \cup \infty \cup -\infty$. But $I = aJ$, where J is a non-zero ideal of R_v and $a \in K^*$. Hence $v(I) = v(J) + v(a) \in \mathbb{Z}$. Choose $b \in I$ with $v(b) = v(I)$, then $\pi^{v(b)} R_v = bR_v \subset I$. On the other hand $I \subset \{x \in K | v(x) \geq v(I)\}$ and if $v(x) \geq v(I)$ then $x = \pi^{v(I)} y$ with $y \in R_v$, thus $I \subset \pi^{v(I)} R_v = \pi^{v(b)} R_v$ hence $I = (\pi R_v)^{v(I)}$. In particular $p_v =$

πR_v. This equation shows that R_v has one and only one non-zero prime ideal, p_v, and R_v is a principal ideal domain. We now make the following definition: A **discrete valuation ring** R is a principal ideal domain with one and only one non-zero prime ideal.

Proposition 5.1.3 *The valuation ring R_v of a discrete v is a discrete valuation ring. Conversely, a discrete valuation ring R is the valuation ring R_v for a unique discrete valuation v of its quotient field K.*

Proof: We prove one side, the other is as follows; let $\mathfrak{p} = \pi R$ be the non-zero prime ideal of R. R is a unique factorization domain and hence each non-zero $x \in R$ has a unique representation $x = \pi^{x_1} u$, u is unit, $x_1 \geq 0$. Allow x_1 to vary over $\mathbb{Z}$ we get the corresponding statement for $x \in K^*$. But then $v(x) = x_1$ defines a discrete valuation of K with $R = R_v$. Uniqueness is obvious.

The field $R_{\mathfrak{p}} = \{xy^{-1} \in K | x, y \in R, y \notin \mathfrak{p}\}$ is called **localization** or **local field** of R at $\mathfrak{p}$. We now are ready to define the Dedekind domains;

Definition 5.1.4 *A Noetherian integral domain R said to be **Dedekind domain** if for every prime ideal $\mathfrak{p}$ of R, $R_{\mathfrak{p}}$ is a discrete valuation ring.*

Remark 5.1.5 *$\mathbb{F}_q$ being a finite field $\mathbb{F}_q[t]$ and $\mathbb{Z}$ are Dedekind domains.*

Definition 5.1.6 *A finite Galois extension of $\mathbb{F}_q(t)$ or $\mathbb{Q}$ is said to be **global field**.*

We will list a couple of properties of Dedekind domains without proving them. We refer (Serre Local fields Ch1, Cassels Frochlich Algebraic Number Theory ch1) for details.

Proposition 5.1.7 *Let $v_{\mathfrak{p}}$ denote the valuation of K defined by $A_{\mathfrak{p}}$, then for every $x \in K^*$ then $v_{\mathfrak{p}}(x)$ are zero for almost all $\mathfrak{p}$. ('almost' means 'for all but finitely many'). In addition, every fractional ideal $\mathfrak{a}$ of A can be written uniquely in the form $\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(a)}$ where the $v_{\mathfrak{p}}(\mathfrak{a})$ are almost all zero.*

This property enables to define the symbols on prime ideals, and is one of the reasons why we observe the theory on Dedekind domains. The next lemma, known as approximation lemma, is a common tool for approximating arbitrary ideals by using integral elements, and is frequently used in proofs. An analytic analogue will be given in the context.

Lemma 5.1.8 (Approximation lemma) *Let $\mathfrak{p}_1, \mathfrak{p}_2 \cdots, \mathfrak{p}_k$ are k distinct prime ideals of A, $x_1, \cdots, x_k \in K$ and $n_1, n_2, \cdots, n_k$ are integers. Then there exists $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all $i = 1, 2, \cdots, k$ and $v_{\mathfrak{q}}(x) \geq 0$ for all $\mathfrak{q}$ different than $\mathfrak{p}_i$.*

The next proposition points that the finite extension of the field of Dedekind domains is also a rational field of a Dedekind domain. Let L be a finite extension of K and $n = [L : K]$. Let A be a Dedekind domain with field of fractions are K, and B be its integral closure in L. Then

Proposition 5.1.9 *B is also a Dedekind domain.*

Remark 5.1.10 *$\mathbb{Z}$ is Dedekind domain with rational field $\mathbb{Q}$, so if L is a finite extension of $\mathbb{Q}$, then ring of algebraic integers of L is Dedekind domain. Moreover, $\mathbb{F}_q[t]$ proved to be a Dedekind domain with field of fractions $\mathbb{F}_q(t)$. Assuming $\mathbb{F}_q(t)(x)$ any finite algebraic extension of $\mathbb{F}_q(t)$, then the algebraic closure of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)(x)$ is also Dedekind domain. Hence, finite extensions of $\mathbb{Q}$ and $\mathbb{F}_q(t)$ enjoys the properties of Dedekind domains as well.*

We continue with definition of ramifications of L/K at primes of K;

Definition 5.1.11 *Let $\mathfrak{P}$ be a non-zero prime ideal of B, if $\mathfrak{p} = A \bigcap \mathfrak{P}$ we say $\mathfrak{P}$ **divides** (or **above**) $\mathfrak{p}$ and denote by $\mathfrak{P}|\mathfrak{p}$. Set $e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B)$ and $\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}$, $e_{\mathfrak{P}}$ is called **ramification index** of $\mathfrak{P}$ in L/K. As B is finitely generated over A, $B/\mathfrak{P}$ is finite extension of $A/\mathfrak{p}$. $f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}]$ is called the **residue degree** of $\mathfrak{P}$. If $e_{\mathfrak{P}} = 1$ and $B/\mathfrak{P}$ is separable over $A/\mathfrak{p}$ we say L/K is **unramified** at*

$\mathfrak{p}$. *If $e_{\mathfrak{P}} > 1$ we say L/K is ramified at $\mathfrak{p}$. When there is only one prime $\mathfrak{P}$ of L above $\mathfrak{p}$ and $f_{\mathfrak{P}} = 1$ we say L/K is* ***totally ramified*** *at $\mathfrak{p}$. We say L/K is* ***tamely ramified*** *at $\mathfrak{p}$ if it is ramified and $\mathfrak{p}$ does not divide the degree of the extension $[L : K]$.*

Now, we assume that L/K is Galois extension and denote the Galois group by $G(L/K)$.

Proposition 5.1.12 *$G(L/K)$ acts transitively on the set of prime ideals $\mathfrak{P}$ of B which are above the prime ideal $\mathfrak{p}$ of A.*

Definition 5.1.13 *$D_{\mathfrak{P}}(L/K) = \{\sigma \in G(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ is called the* ***decomposition group*** *of $\mathfrak{P}$ in L/K. $T_{\mathfrak{P}}(L/K) = \{\sigma \in G(L/K) : \sigma(\alpha) \equiv \alpha(mod\, \mathfrak{P}) \forall \alpha \in B\}$ is called the* ***inertia group*** *of $\mathfrak{P}$ in L/K.*

Assume now is (L/K) unramified at $\mathfrak{P}$ and $A/\mathfrak{p}$ has $N\mathfrak{p}$ elements. Then $T_{\mathfrak{P}} = \{1\}$ and there exists unique generator of $s_{\mathfrak{P}} \in D_{\mathfrak{P}}$ characterized by:

Definition 5.1.14 *$s_{\mathfrak{P}} \in (G/K)$ satisfying*

$$s_{\mathfrak{P}}(b) \equiv b^{N\mathfrak{p}}(mod\, \mathfrak{P})$$

for all $b \in B$ is called ***Frobenius automorphism*** *of $\mathfrak{P}$ and is denoted by $(\mathfrak{P}, L/K)$.*

By definition Frobenius automorphism generates $D_{\mathfrak{P}}$ and has order $f_{\mathfrak{P}}$.

Definition 5.1.15 *Assume L/K is abelian, $(\mathfrak{P}, L/K)$ depends only on $\mathfrak{p} = \mathfrak{P} \cap A$. It is denoted by $(\mathfrak{p}, L/K)$ and called the* ***Artin symbol*** *of $\mathfrak{p}$ in $G(L/K)$. If $\mathfrak{a}$ is a fractional ideal of A which contains no ramified primes, set*

$$(\mathfrak{a}, L/K) = \prod (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(\mathfrak{a})}$$

where $\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$. It is called the ***Artin symbol*** *of $\mathfrak{a}$ in $G(L/K)$.*

We note that only the extensions $L = K(\sqrt[n]{a})$, namely the Kummer fields, are our fields of interest throughout the reciprocity theory, hence we specialize to Kummer extensions and treat the ramification by Kummer theory.

5.2 Decomposition of Primes

In this section we define Kummer fields $L = K(\sqrt[n]{a})$ and determine the ramification the extension $K(\sqrt[n]{a})/K$ at primes of K.

Through this section, K is a field of characteristic p not dividing n (characteristic may be 0), in which $x^n - 1$ splits; and ζ_n will be a primitive root of unity. Let $a \in K^*$, if L is extension of K such that $x^n = a$ has root α in L, then all the roots $\alpha, \zeta_n\alpha, \zeta_n^2\alpha, \cdots, \zeta_n^{n-1}\alpha$ of $x^n = a$ are in L and any automorphism of L over K permutes them. We denote the minimal splitting field for $x^n = a$ by $K(\sqrt[n]{a})$.

Definition 5.2.1 *$K(\sqrt[n]{a})/K$ is called* ***Kummer extension*** *(or* ***Kummer field****).*

If σ is an element of Galois group $G(K(\sqrt[n]{a})/K)$, then, once we have chosen a root α of $x^n = a$, σ is determined completely by the image $\sigma(\alpha) = \zeta_n^b\alpha$. In particular, if a is of order n in the multiplicative group $K^*/(K^*)^n$, then a^r is an n-th power in K^* if and only if $n|r$, so $x^n - a$ is irreducible; in this case, the map $\sigma \to \zeta_n^b$ gives an isomorphism of $G(K(\sqrt[n]{a})/K)$ on to μ_n the multiplicative group of n-th roots of unity. We state all this as lemma;

Lemma 5.2.2 *If $a \in K^*$, there is a well defined normal extension $K(\sqrt[n]{a})$, the splitting field of $x^n - a$. If α is root of $x^n - a$, there is an injective map of $G(K(\sqrt[n]{a})/K) \to K^*$ given by $\sigma \to \frac{\sigma(\alpha)}{\alpha}$; in particular, if a is of order n in the multiplicative group $K^*/(K^*)^n$, the Galois group $G(K(\sqrt[n]{a})/K)$ is cyclic and generated by σ with $\sigma(\alpha) = \zeta_n\alpha$.*

We want to look at the factorization of primes $\mathfrak{p}$ of K in the extension $K(\sqrt[n]{a})$

in order to determine the ramified and unramified primes. The following theorem gives the answer for the general case:

Theorem 5.2.3 *Let S and R denote the Dedekind domains whose rational fields are L and K respectively. Assume L/K is finite Galois extension. A prime $\mathfrak{p}$ of K is unramified in L if and only if $\mathfrak{p}$ does not divide the discriminant δ of S/R.*

For proof we refer to [5].

As a consequence of this theorem we have the following identification for primes over Kummer fields;

Lemma 5.2.4 *The discriminant of $K(\sqrt{a})$ over K divides $n^n a^{n-1}$; $\mathfrak{p}$ is unramified if $\mathfrak{p} \not| na$. If $\mathfrak{p}|a$, $\mathfrak{p} \not| n$ and $\mathfrak{p}^n \not| a$ then $\mathfrak{p}$ is tamely ramified in $K(\sqrt{a})$; if $\mathfrak{p}|a$ and $\mathfrak{p}^2 \not| a$ then $\mathfrak{p}$ is totally ramified.*

Proof: Suppose $\alpha^n = a$; then, if $\mathcal{O}$ is the ring of integers of K, $\mathcal{O}[\alpha]$ is a submodule of the ring of integers of $K(\alpha)$, and its discriminant is $\prod_{\alpha^n=a} \frac{d(x^n-a)}{dx} = \prod_{\alpha^n=a} nx^{n-1} = na^{n-1}$. By theorem above $\mathfrak{p}$ is unramified if and only if $\mathfrak{p} \not| na$. If $\mathfrak{p}|a$ and $\mathfrak{p}^2 \not| a$ quite explicitly $\mathfrak{p} = (\mathfrak{p}, \alpha)^n$. If $\mathfrak{p} \not| n$, so that $\mathfrak{p}$ does not divide the degree of the extension then any ramification must certainly be tame. On the other hand if $\mathfrak{p}|a$ but $\mathfrak{p}^n \not| a$ then $\mathfrak{p}$ is certainly ramified since $(\mathfrak{p}, \alpha)|\mathfrak{p}|(\mathfrak{p}, \alpha)^n$.

There remains the case where $\mathfrak{p}^r|a$, $\mathfrak{p}^{r+1} \not| a$, $\mathfrak{p} \not| n$ with $2 \leq r \leq n-1$. If $(r, n) = 1$ then we have k, m so that $rk + nm = 1$ and choose $q \in K$ with $\mathfrak{p}|q$ and $\mathfrak{p}^2 \not| q$. Then $K[\sqrt[n]{a^k q^{-nm}}] = K(\sqrt[n]{a})$ and we got back to the case $r = 1$. If $(r, n) = s > 1$, the ramification is no longer total, and there may or may not be splitting as well. The ramification index is n/s: $\mathfrak{p}$ is unramified in the extension $K(\sqrt[s]{a})$ of K, and the factors of $\mathfrak{p}$ are totally ramified in the extension $K(\sqrt[n]{a})$ of $K(\sqrt[n]{a})$.

5.3 The Local Analytic Structure

Let R be Dedekind domain, $\mathfrak{p}$ its prime ideal, and $R_{\mathfrak{p}}$ is its localization at $\mathfrak{p}$. Let v be discrete valuation of $R_{\mathfrak{p}}$, π denote uniformizer. One may define an absolute value $|\ |_{\mathfrak{p}}$ on K by setting $|0|_{\mathfrak{p}} = 0$, $|x|_{\mathfrak{p}} = c^{-v(x)}$ for non-zero x and for a fixed $0 < c < 1$. This absolute value satisfies $|x+y|_{\mathfrak{p}} \leq |x|_{\mathfrak{p}} + |y|_{\mathfrak{p}}$, $|xy|_{\mathfrak{p}} = |x|_{\mathfrak{p}}|y|_{\mathfrak{p}}$ and $|x|_{\mathfrak{p}} = 0 \Leftrightarrow x = 0$, hence it is a metric. This metric imposes a topology on K. In this section, we show that different primes have different topologies and discuss certain properties of the analytic structure of K. We reverse the direction and investigate all absolute values satisfying the three conditions, in order to describe a global analytic structure. It comes out to be that all absolute values are of form $|\ |_{\mathfrak{p}}$ plus that are isomorphic to ordinary absolute value of $\mathbb{C}$ or $\mathbb{R}$ which will be called the infinite primes. We finish the section defining of the topology on the global analytic structure and deducing the local Artin maps.

We start with defining the absolute value;

Definition 5.3.1 *Let K be a field. A function $|\ | K \to \mathbb{R} \cup \{0\}$ is called **absolute value** if it satisfies*

1. $|0| = 0$ *and* $|a| > 0$ *for* $a \neq 0$
2. $|ab| = |a|\ |b|$
3. $|a+b| \leq |a| + |b|$

Remark 5.3.2 $|1| = 1$, $|-1| = 1$, $|a| = |-a|$ *and* $|a-b| \geq |\ |a| - |b|\ |$.

The valuation satisfying $|0| = 0$ and $|a| = 1$ for all $a \in K$ is called the trivial valuation and will be excluded from consideration.

The absolute values differ by the triangle inequality property $|x+y| \leq |x|+|y|$ such that either $|x+y| \leq \sup |x|, |y|$ for all $x, y \in K$ which resembles the case where absolute value is of form $|\ |_{\mathfrak{p}}$, or there always exits a $y \in K$ with $|x+y| > |x|$

for given x which resembles the case $| \ |$ is ordinary absolute value of $\mathbb{R}$ or $\mathbb{C}$. We explain it by;

Definition 5.3.3 *The absolute value $| \ |$ said to be non-archimedean if it satisfies $|x+y| \leq |x| + |y|$ for all $x, y \in K$ and said to be archimedean if it is not non-archimedean.*

Remark 5.3.4 *An equivalent but simpler version of the definition is if $|n| > 1$ for at least one $n \in \mathbb{N}$ then $| \ |$ is archimedean, if $|n| \leq 1$ for all $n \in \mathbb{N}$, $| \ |$ said to be non-archimedean valuation.*

Definition 5.3.5 *Absolute value $| \ |$ of field K said to be discrete if $\exists \delta > 0$ such that*

$$1 - \delta < |a| < 1 + \delta \Rightarrow |a| = 1$$

Lemma 5.3.6 *Let non trivial absolute value $| \ |$ of field K be non-archimedean. $| \ |$ is discrete if and only if the ideal $\mathfrak{p}_{| \ |} = \{x \in K : |x| < 1\}$ is a principal ideal.*

Proof: If $\mathfrak{p}$ is principal, then $\mathfrak{p} = (\pi)$ for some generating element $\pi \in K$. $|\pi| = P < 1$. Take $\delta = 1 - P$. Assume $P < |a| < 2 - P$, and $a = \pi^{a_1} u$ with u unit. Then $|a| = P^{a_1} > P$ thus $a_1 = 0$ and $|a| = 1$. Assume now $| \ |$ is discrete. Non-triviality guaranties $\exists \gamma \in K$ with $|\gamma| < 1$ and discrete property implies that there exists $\lambda < 1$ such that $|\gamma| < 1$ implies $|\gamma| < \lambda$. Assume now $\lambda = \sup_{|\gamma|<1}\{|\gamma|\}$. We first prove that $\exists \pi \in K$ with $|\pi| = \lambda$. Assume not, there exist a sequence γ_i in K with $|\gamma_i| \to \lambda$, hence $|\frac{\gamma_i}{\gamma_{i+1}}| \to 1$ $|\frac{\gamma_{i+1}}{\gamma_i}| \to 1$, hence there exists an i with either $\lambda < |\frac{\gamma_{i+1}}{\gamma_i}| < 1$ or $\lambda < |\frac{\gamma_i}{\gamma_{i+1}}| < 1$ which yields a contradiction. Let $|\pi| = \lambda$, and $a \in K$ with $|a| \leq 1$. $|\frac{a}{\pi^n}| \to \infty$ thus $\exists n_0$ with $|\frac{a}{\pi^{n_0}}| < 1 \leq |\frac{a}{\pi^{n_0+1}}|$. $|\frac{a}{\pi^{n_0}}| < 1 \Rightarrow |\frac{a}{\pi^{n_0}}| \leq \lambda = |\pi|$ and hence $|\frac{a}{\pi^{n_0+1}}| \leq 1$ which gives $|\frac{a}{\pi^{n_0+1}}| = 1$ therefore $a = \pi^{n_0+1} u$ for some unit, hence the lemma.

Let R be Dedekind domain with its quotient field K, and $\mathfrak{p}$ be prime ideal of R. Since $\mathfrak{p} = \mathfrak{p}_{| \ |_\mathfrak{p}}$ is principal ideal, by previous lemma $| \ |_\mathfrak{p}$ is a non-archimedean discrete absolute values of K. Conversely, given a non-archimedean discrete absolute value $| \ |$ of K, $\mathfrak{p}_{| \ |}$ is a prime ideal of K and $| \ |$ is equivalent to $| \ |_{\mathfrak{p}}$. In the achimedean case, the absolute value is as follows;

Theorem 5.3.7 (Gelfand-Tornheim) *Any field K with achimedean valuation is isomorphic to a subfield of $\mathbb{C}$, the valuation equivalent to that induced by absolute value on $\mathbb{C}$.*

Proof: Refer to [3]

Consequently, all types of valuations of K comes out to be either archimedean, or non-arhchimedean and discrete.

Different absolute values on K may give the same topological structure. Since we are interested in the kind of topology rather than that of valuation, we consider such valuations as equivalent.

Definition 5.3.8 *Two valuations of K; $| \ |_1$ and $| \ |_2$ said to be equivalent if $|a|_1 < |b|_1 \Leftrightarrow |a|_2 < |b|_2$. Equivalence is denoted by $| \ |_1 \simeq | \ |_2$.*

Remark 5.3.9 *Two valuations $| \ |_1$ and $| \ |_2$ are equivalent if and only if $\exists s > 0$ such that $| \ |_1 = | \ |_2^s$. In addition, $| \ |_1$ and $| \ |_2$ are equivalent if and only if both induce the same topology. For proofs we refer to [9].*

We call **place** to an equivalence class of absolute values. A place which of a non-archimedean discrete absolute value is determined by fixing the value $|\pi|$ at a uniformizer of $\mathfrak{p}_{| \ |}$. For measure theoretical reasons we set $|\pi| = P^{-1}$ where P is the cardinality of the residue field $K/\mathfrak{p}_{| \ |}$ (in order to have Haar measure 1 of the residue field).

Definition 5.3.10 *Let K be a field with absolute value $| \ |$ and residue field with $P < \infty$ elements. We say that $| \ |$ is normalized absolute value if*

$$|\pi| = \frac{1}{P}$$

where $\mathfrak{p}_{|\ |} = (\pi)$ *is the maximal ideal of* K *with respect to* $|\ |$.

We make some remarks on the analytic properties of absolute values and completion of fields with referring the proofs to [5].

Remark 5.3.11 *An absolute value* $|\ |$ *of field* K *induces a topology with metric* $d(x,y) = |x-y|$. *The topology induced by* $|\ |$ *makes* K *a topological field, i.e. sum, product, reciprocal are continuous.*

We continue with completion. We say that K is complete with respect to valuation $|\ |$ if every Cauchy sequence has a convergent point, or more precisely, for any given sequence a_n with $|a_n - a_m| \to 0$ as $m, n \to \infty$ there is $a^* \in K$ with $a_n \to a^*$ with respect to $|\ |$.

Theorem 5.3.12 *Every field* K *with valuation* $|\ |$ *can be embedded in a unique (up to isomorphism) complete field* $\bar{K}$ *with a valuation* $|\ |_{\bar{K}}$ *satisfying* $|\ |_{\bar{K}} = |\ |$ *on* K. *Moreover,* $|\ |$ *is non-archimedean if and only if* $|\ |_{\bar{K}}$ *is.*

The next theorem is the analytic analogue of the approximation lemma that we mentioned for fractional ideals. This is, too, a very useful tool to extend the properties inherited by principal ideals to properties of fractional ideals, and thus will frequently be used in proofs.

Theorem 5.3.13 (Artin-Whaples) *Let* $|\ |_1, |\ |_2, \cdots, |\ |_r$ *be inequivalent non-trivial valuations of* K, *then for arbitrary elements* $a_1, a_2, \cdots, a_r \in K$ *and* $\delta_1, \delta_2, \cdots, \delta_r > 0$ *there exists an element* $a \in K$ *with* $|a - a_i| < \delta_i$ *for all* $i = 1, 2, \cdots, r$.

Proof: Refer to [9]

Note that if $\mathfrak{p}$ is a prime ideal of R and $|\ |_{\mathfrak{p}}$ absolute value associated to $\mathfrak{p}$, then the completion $\bar{K}_{\mathfrak{p}}$ of the field K consist of elements of the form $\sum_{i>>-\infty}^{\infty} a_i \pi^i$ where a_i are elements in residue field $K/\mathfrak{p}$ and π is uniformizer.

5.4 The Global Analytic Structure

We now fix the notation. We start with definitions motivated by analytical structure. R is a Dedekind domain, K its quotient field. We say **prime** to an equivalence class of absolute value of K. We say **finite prime** to a non-archimedean discrete place and **infinite prime** to archimedean place. We denote finite and infinite primes by $\mathfrak{p}$ and ∞ respectively. We also use $\mathfrak{p}$ for prime ideal of R, and $|\ |_{\mathfrak{p}}$ for non-archimedean absolute value associated to $\mathfrak{p}$. Let $v = v_{\mathfrak{p}}$ denote the valuation, $\mathcal{O}_{\mathfrak{p}} = \{|a|_{\mathfrak{p}} \leq 1, a \in K\} = \{v_{\mathfrak{p}}(a) \geq 0, a \in K\}$ ring of integers, $K/\mathfrak{p}$ residue field $U_{\mathfrak{p}} = \{|u|_{\mathfrak{p}} = 1, u \in K\} = \{v_{\mathfrak{p}}(u) = 0, u \in K\}$ units, π uniformizer of $\mathfrak{p} = \{|a|_{\mathfrak{p}} < 1, a \in K\} = \{v_{\mathfrak{p}}(a) > 0, a \in K\}$, and $\bar{K}_{\mathfrak{p}}$ be completion of K with respect to $|\ |_{\mathfrak{p}}$. For convenience we set $U_\infty = K^*$.

We next fix the definitions motivated by ideal theoretic structure. Let S_∞ denote set of infinite primes and $\mathfrak{M}$ denote the set of all primes of K, i.e. set of all prime ideals of R plus S_∞. I_K denote the group of the fraction ideals of R, then there is a canonical isomorphism from I_K to free group generated by $\mathfrak{M} - S_\infty$ given by

$$\mathfrak{p}_1^{v_1}\mathfrak{p}_2^{v_2}\cdots\mathfrak{p}_k^{v_k} \to \mathfrak{p}_1^{v_1}\mathfrak{p}_2^{v_2}\cdots\mathfrak{p}_k^{v_k}.$$

We also fix L/K to be a finite abelian extension of K. Denote by S the set of primes of K which are ramified plus infinite primes and by I^S the set of fractional ideals of R which are coprime to S.

We now define the global analytical structure by introducing the restricted product topology:

Definition 5.4.1 *Let Ω_λ $(\lambda \in \Lambda)$ be a family of topological spaces and let $\Theta_\lambda \subset \Omega_\lambda$ be open subset for all $\lambda \in \Lambda$. Consider the space $\Omega = \{\{\alpha_\lambda\}_{\lambda\in\Lambda}, \alpha_\lambda \ \in \Theta_\lambda$ for almost all $\lambda\}$. We give Ω a topology by taking as basis for open sets $\prod_{\lambda\in\Lambda}\Gamma_\lambda$ where $\Gamma_\lambda \subset \Omega_\lambda$ is open for all λ and $\Gamma_\lambda = \Theta_\lambda$ for almost all λ. We call this topology as* ***restricted product topology*** *of Ω_λ with respect to Θ_λ.*

As we shall see, Ω_λ will be identified by primes, and the next corollary shows that the topology does not change if we remove a finite set S from Λ (this S will be consistent with the one defined above).

Corollary 5.4.2 *Let S be finite subset of Λ, and let $\Omega_S = \prod_{\lambda \in S} \Omega_\lambda \prod_{\lambda \notin S} \Theta_\lambda$. Then Ω_S is open in Ω and the topology induced in Ω_S as a subset of Ω is the same as the product topology.*

Definition 5.4.3 *The restricted product topology of the multiplicative groups $K_{\mathfrak{p}}^*$ with respect to the units $U_{\mathfrak{p}}$ of $\mathfrak{p}$ is called the **idele group** of K and denoted by J_K. An element(or vector) of J_K is called an **idele**. The set of elements of J_K which have value 1 at the $\mathfrak{p}$-th component is denoted by J_K^S.*

K^* can be embedded into the groups of ideles such that if $\alpha \in K$, $(.., \alpha, \alpha, \alpha, \cdots) = (\alpha)_{\mathfrak{p} \in \mathfrak{M}}$ is in J_K since α is unit for almost all primes. We set $\alpha \to (.., \alpha, \alpha, \alpha, \cdots)$. We call such ideles as **principal ideles**, and denote the set of principal ideles also by K^*.

Proposition 5.4.4 *The multiplicative group K^* is embedded as a discrete subgroup of J_K.*

Proof: Refer to [5] or [15].

If $x \in J_K$ it has a non-unit component at only a finite number of $\mathfrak{p}$ component $x_{\mathfrak{p}}$ of x in $n_{\mathfrak{p}} \in \mathbb{Z}$, we write

$$(x)^S = \prod_{\mathfrak{p} \notin S} n_{\mathfrak{p}} \mathfrak{p} \in I^S.$$

5.5 Global and Local Artin Maps

Theorem 5.5.1 *Let $\mathfrak{a} \in I^S$, recall the Artin symbol of $\mathfrak{a}$ with respect to L/K;*

$$(\mathfrak{a}, L/K) = \prod (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(\mathfrak{a})} \in G(L/K).$$

Then there exists $\epsilon > 0$ such that $a \in K^*$ and $|a-1|_{\mathfrak{p}} < \epsilon$ for all $\mathfrak{p} \in S$ implies

$$((a)^S, L/K) = \prod_{\mathfrak{p} \notin S} (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(a)} = 1$$

In other words, if $a \in K^*$ is sufficiently near to 1 at all primes in a large enough set S, then $((a)^S, L/K) = 1$.

We refer to [1], [5], [15], [25] for the proof.

We briefly indicate how this theorem is interpreted in the quadratic case. Let $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ be the quadratic extension. Then $S = \{p; p|2a\} \cup \infty$. I^S is fractional ideals prime to 2 and to a. Let p denote a prime dividing 2 or a. Let $\mathfrak{b} \in I^S$, since $\mathbb{Z}$ is principal ideal domain, we may assume $\mathfrak{b} = (b)$ with $b \in \mathbb{Q}$. $|b-1|_p < \epsilon$ means that $b \equiv 1 (\text{mod } p^k)$ for some large $k \in \mathbb{N}$. The theorem states that there exists an integer k_p such that $a \equiv 1(\text{mod } p^{k_p})$ implies that the quadratic norm residue symbol $\left(\frac{a,b}{p}\right) = 1$ i.e. b is a norm for the quadratic extension $\mathbb{Q}_{\mathfrak{P}}(\sqrt{a})/\mathbb{Q}_p$ for any $p|2a$. This is evident since $p = 2$ and $b \equiv 1(\text{mod } 8)$ implies that b is norm, and $p|a$, $p \neq 2$ and $b \equiv 1(\text{mod } p_i)$ implies b is norm. Hence taking $\epsilon = \min_{p|a}\{2^{-3}, p^{-1}\}$, $|a-1|_2 < \epsilon$ implies $\left(\frac{a,b}{p}\right) = 1$ for all $p|2a$.

Theorem 5.5.2 *Assume $G(L/K)$ is a topological group endowed with the Krull topology. Then there exists unique homomorphism $\psi_{L/K} : J_K \to G(L/K)$ such that*

i) *$\psi_{L/K}$ is continuous;*

ii) *$\psi_{L/K}(x) = 1$ for all $x \in K^*$;*

iii) *$\psi_{L/K}(x) = ((x)^S, L/K)$ for all $x \in J_K^S$.*

Proof: By approximation theorem we can find a sequence $a_n \in K^*$ such that $|a_n - x^{-1}|_{\mathfrak{p}} \to 0$ as $n \to \infty$ at all $\mathfrak{p} \in S$. We define $\psi_{L/K}(x)$ to be

$$\psi_{L/K}(x) = \lim_{n\to\infty} ((a_n x)^S, L/K)$$

The limit RHS is exists since $G(L/K)$ is complete. This is well defined as follows; if $b_m \in K^*$ is another sequence with $|b_m - x^{-1}|_{\mathfrak{p}} \to 0$, by triangle inequality of $|\ |_{\mathfrak{p}}$;

$$|\frac{a_n}{b_m} - 1|_{\mathfrak{p}} = \frac{1}{|b_m|_{\mathfrak{p}}}|a_n x - b_m x|_{\mathfrak{p}} \leq \frac{1}{|b_m|_{\mathfrak{p}}}(|a_n - x^{-1}|_{\mathfrak{p}} + |b_m - x^{-1}|_{\mathfrak{p}})$$

taking the limits as $m, n \to \infty$,
$|b_m|_{\mathfrak{p}} \to |x^{-1}|_{\mathfrak{p}} > 0$ and $(|a_n - x^{-1}|_{\mathfrak{p}} + |b_m - x^{-1}|_{\mathfrak{p}}) \to 0$, hence $|\frac{a_n}{b_m} - 1|_{\mathfrak{p}} \to 0$. Writing this in the equation;

$$\frac{((a_n x)^S, L/K)}{((b_m x)^S, L/K)} = ((\frac{a_n}{b_m})^S, L/K) \to 1 \in G(L/K)$$

by the previous theorem. For continuity, let the $\mathfrak{p}$-th component of x are units for $\mathfrak{p} \notin S$, then we have $\psi_{L/K}(x) = \lim_{n\to\infty}((a_n)^S, L/K)$ and if in addition $\mathfrak{p}$-th component of x are sufficiently close to 1 for $\mathfrak{p} \in S$, then so will be those of a_n for large n, and by previous theorem $((a_n)^S, L/K) = 1$ for sufficiently large n, proving i). Take $x \in K^*$ principle idele whose all components are a, set $a_n = a^{-1}$ we get $\psi_{L/K}(x) = \lim_{n\to\infty}((1)^S, L/K) = 1$ proving ii). Let $x \in J_K^S$, take now $a_n = 1$ for all n, thus we get $\psi_{L/K}(x) = \lim_{n\to\infty}((x)^S, L/K) = ((x)^S, L/K)$, proving iii).

Definition 5.5.3 *$\psi_{L/K}$ is called the **global Artin map**.*

We follow with the local artin maps.

Definition 5.5.4 *Denote the idele whose $\mathfrak{p}$-th component is x and other components are 1 by $(\cdots, 1, x, 1, \cdots)_{\mathfrak{p}}$. The homomorphism $\psi_{\mathfrak{p}} : K_{\mathfrak{p}}^* \to G(L/K)$ defined as follows; $x \to \psi_{L/K}((\cdots, 1, x, 1, \cdots)_{\mathfrak{p}})$ is on one hand in $G(L/K)$ since $\psi_{L/K}$ has image $G(L/K)$. On the other hand, by the choice of the idele this can be identified by an element of $G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. We set $\psi_{\mathfrak{p}} : K_{\mathfrak{p}} \to G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ as $x \to \sigma_x$ with $\sigma_x = \psi_{L/K}((\cdots, 1, x, 1, \cdots)_{\mathfrak{p}})$. We call $\psi_{\mathfrak{p}}$ the **local Artin map**.*

In the following remark we give the relation of local Artin maps to Global Artin map;

Remark 5.5.5 *If $x = (x_\mathfrak{p}) \in J_K$, then;*

$$x = \lim_S \{\prod_{\mathfrak{p} \in S} (\cdots, 1, x_\mathfrak{p}, 1, \cdots)_\mathfrak{p}\}$$

and by continuity

$$\psi_{L/K}(x) = \prod_\mathfrak{p} \psi_\mathfrak{p}(x_\mathfrak{p})$$

We end this chapter here, leaving the definition of the norm residue and power residue symbols to the next chapter.

Chapter 6

Symbols and The Reciprocity Relation

In this chapter we give the definition of power and norm residue symbols and prove the main theorem. At first section we define the power residue symbol and deduce a number of properties. We continue with definition and properties of the norm residue symbol at the second section. At the last the section we observe how both symbols are related, and finish by proving the main theorem of reciprocity theory.

6.1 Power Residue Symbol

We keep the notation of the previous chapter. Let R be Dedekind domain K be its field of fractions, n be a fixed natural number and let the group μ_n of n-th root of unity is contained in K. S denote the set of primes of K consisting of infinite primes and those dividing n. If $a_1, a_2, \cdots, a_r \in K^*$, we let $S(a_1, a_2, \cdots, a_r)$ denote the set of prime primes in S together with the primes such that $|a_i|_{\mathfrak{p}} \neq 1$ for some i. For $a \in K$, let $K(\sqrt[n]{a})$ denote the splitting field of $x^n = a$, and M denote the integral closure of R in $K(\sqrt[n]{a})$. Let $\mathfrak{b} \in I^{S(a)}$, its prime decomposition $\mathfrak{b} = \mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\cdots\mathfrak{p}_k^{b_k}$ where $b_i > 0$ and $\mathfrak{p}_i$ for $i = 1, 2, .., k$. Denote by $\mathfrak{P}_i$ to a prime in $K(\sqrt[n]{a})$ above $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ are unramified at $K(\sqrt[n]{a})$, and hence the Frobenius automorphism $(\mathfrak{p}, K(\sqrt[n]{a})/K)$ is characterized by

$$(\mathfrak{p}_i, K(\sqrt[n]{a})/K)(\gamma) \equiv \gamma^{N\mathfrak{p}_i} (\text{mod } \mathfrak{P})$$

for all $\gamma \in M$ (where $N\mathfrak{p}_i$ is the number of elements of the residue field $R/\mathfrak{p}_i$). This definition is independent of choice of root $\sqrt[n]{a}$ of $x^n - a$ since the automorphism is determined by its action on all elements of M and since it is unique. Extending this definition;

$$(\mathfrak{b}, K(\sqrt[n]{a})/K) = \prod_{i=1}^{k} (\mathfrak{p}_i, K(\sqrt[n]{a})/K)^{b_i}$$

is uniquely determined up to a.(i.e. independent of choice of $\sqrt[n]{a}$), and is an element of the Galois group $G(K(\sqrt[n]{a})/K)$.

$$[(\mathfrak{b}, K(\sqrt[n]{a})/K)(\sqrt[n]{a})]^n = (\mathfrak{b}, K(\sqrt[n]{a})/K)((\sqrt[n]{a})^n) = a = (\sqrt[n]{a})^n$$

$$[(\mathfrak{b}, K(\sqrt[n]{a})/K)(\sqrt[n]{a})]^n - (\sqrt[n]{a})^n = \prod_{i=0}^{n-1} [(\mathfrak{b}, K(\sqrt[n]{a})/K)(\sqrt[n]{a}) - \zeta_n^i \sqrt[n]{a}] = 0$$

Thus we have $(\mathfrak{b}, K(\sqrt[n]{a})/K)(\sqrt[n]{a}) = \zeta_n^{i_0} \sqrt[n]{a}$ for some $i_0 \in \{0, 1, \cdots, n-1\}$. We define n-th power residue symbol $\left(\frac{a}{\mathfrak{b}}\right)_n$ by

Definition 6.1.1

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \zeta_n^{i_0}$$

or more transparently

$$(\mathfrak{b}, K(\sqrt[n]{a})/K)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{b}}\right)_n \sqrt[n]{a}$$

is called the n-th power residue symbol associated to a and $\mathfrak{b}$.

We list the certain properties of this symbol, and leave the proofs to the end.

Theorem 6.1.2 i) *Assume $a, a' \in K^*$, and $\mathfrak{b} \in I^{S(a,a')}$ then;*

$$\left(\frac{aa'}{\mathfrak{b}}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n \left(\frac{a'}{\mathfrak{b}}\right)_n$$

ii) *Assume $a \in K^*$, and $\mathfrak{b}, \mathfrak{b}' \in I^{S(a)}$ then;*

$$\left(\frac{a}{\mathfrak{b}\mathfrak{b}'}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n \left(\frac{a}{\mathfrak{b}'}\right)_n$$

and hence

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p} \notin S(a)} \left(\frac{a}{\mathfrak{b}}\right)_n^{v_{\mathfrak{p}}(\mathfrak{b})}$$

iii) *{Generalized Euler Criterion} If $\mathfrak{p} \notin S(a)$ then $n | N\mathfrak{p} - 1$, where $N\mathfrak{p} = [R/\mathfrak{p}]$, and $\left(\frac{a}{\mathfrak{p}}\right)_n$ is the unique n-th root of unity such that*

$$\left(\frac{a}{\mathfrak{p}}\right)_n \equiv a^{\frac{N\mathfrak{p}-1}{n}} (mod\ \mathfrak{P})$$

iv) *Let $a \in K_{\mathfrak{p}}^*$ and $\mathfrak{p} \not| n$, then $\left(\frac{a}{\mathfrak{p}}\right)_n$ is the unique n-th root of unity satisfying*

$$\left(\frac{a}{\mathfrak{p}}\right)_n \equiv a^{\frac{N\mathfrak{p}-1}{n}} (mod\ \mathfrak{p}).$$

v) *For $\mathfrak{p} \in S(a)$, equivalently $\mathfrak{p} \not| n$ and $a \in K_{\mathfrak{p}}^*$, the following statements are equivalent*

1) $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$

2) $x^n \equiv a (mod\ \mathfrak{p})$ *solvable with* $x \in \mathcal{O}_{\mathfrak{p}}$.

3) $x^n = a$ *is solvable with* $x \in K_{\mathfrak{p}}$.

vi) *If $\mathfrak{b}$ is an integral ideal prime to n, and ζ_n be an n-th root of unity, then;*

$$\left(\frac{\zeta_n}{\mathfrak{b}}\right)_n = \zeta_n^{\frac{N\mathfrak{b}-1}{n}}$$

vii) *If a integral and $b \in I^{S(a)}$ integral ideal, and if $a' \equiv a (mod\ \mathfrak{b})$ then*

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \left(\frac{a'}{\mathfrak{b}}\right)_n$$

viii) *If $\mathfrak{b}, \mathfrak{b}' \in I^{S(a)}$ with $\mathfrak{b}'\mathfrak{b}^{-1} = (c)$ is the principal ideal with $c \in K^*$ such that $c \in (K_{\mathfrak{p}}^*)^n$ for all $\mathfrak{p} \in S(a)$, then*

$$\left(\frac{a}{\mathfrak{b}'}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n$$

We now prove these properties:

Proof: {Property i} If we show this for only prime ideals $\mathfrak{b} = \mathfrak{p}$, then by linearity we are done. Fix $\mathfrak{p}$, denote primes above $\mathfrak{p}$ of the fields $K(\sqrt[n]{a})$, $K(\sqrt[n]{a'})$, $K(\sqrt[n]{aa'})$ and $K(\sqrt[n]{a}, \sqrt[n]{a'})$ by $\mathfrak{P}_a$, $\mathfrak{P}_{a'}$, $\mathfrak{P}_{aa'}$ and $\mathfrak{P}$ respectively. Let M_a, $M_{a'}$, $M_{aa'}$ and M denote the integral closure of R in the respective fields. Denote the Frobenius automorphisms $(\mathfrak{p}, K(\sqrt[n]{a})/K)$, $(\mathfrak{p}, K(\sqrt[n]{a'})/K)$, $(\mathfrak{p}, K(\sqrt[n]{aa'})/K)$ and $(\mathfrak{p}, K(\sqrt[n]{a}, \sqrt[n]{a'})/K)$ by σ_a, $\sigma_{a'}$, $\sigma_{aa'}$ and σ respectively. Since $\mathfrak{p}$ is unramified at all these fields; σ is characterized by

$$\sigma(\gamma) = \gamma^{N\mathfrak{p}} (\text{mod } \mathfrak{P}), \forall \gamma \in M.$$

Putting $\gamma = \sqrt[n]{aa'}$ on one hand;

$$\sigma(\sqrt[n]{aa'}) \equiv \sqrt[n]{aa'}^{N\mathfrak{p}} (\text{mod } \mathfrak{P})$$

On the other hand $\sqrt[n]{aa'} \in M_{aa'}$ and $\mathfrak{P}$ is above $\mathfrak{P}_{aa'}$;

$$\sigma_{aa'}(\sqrt[n]{aa'}) \equiv \sqrt[n]{aa'}^{N\mathfrak{p}} (\text{mod } \mathfrak{P})$$

Doing the similar process for $\sqrt[n]{a'}$ and $\sqrt[n]{a'}$ we get $\sigma(\sqrt[n]{a}) \equiv \sigma_a(\sqrt[n]{a}) \equiv \sqrt[n]{a}^{N\mathfrak{p}} (\text{mod } \mathfrak{P})$ and $\sigma(\sqrt[n]{a'}) \equiv \sigma_{a'}(\sqrt[n]{a}) \equiv \sqrt[n]{a}^{N\mathfrak{p}} (\text{mod } \mathfrak{P})$, combinin these, we get $\sigma_{aa'}(\sqrt[n]{aa'}) \equiv \sigma_a(\sqrt[n]{a})\sigma_{a'}(\sqrt[n]{a'}) (\text{mod } \mathfrak{P})$. As $\sigma_{aa'}(\sqrt[n]{aa'})$, $\sigma_a(\sqrt[n]{a})$ and $\sigma_{a'}(\sqrt[n]{a'})$ are n-th root of 1, thus we have the lemma.

Proof: {Property ii} This is immediate from multiplicative property of the symbol.

Proof: {Property iii} First we prove that $\mathfrak{p} \notin S(a)$ then $n | N\mathfrak{p} - 1$. $\mathfrak{p} \notin S(a)$ implies $\mathfrak{p}$ is unramified and thus the inertia group

$$T_{\mathfrak{p}} = \{\sigma \in G(K(\sqrt[n]{a'})/K); \forall \alpha \in M, \sigma(\alpha) \equiv \alpha (\text{mod } \mathfrak{P})\} = (1).$$

Let $\sigma_{\mathfrak{p}}$ denote the Frobenius automorphism $(\mathfrak{p}, K(\sqrt[n]{a'})/K)$. Due to its characterization, we have

$$\sigma_{\mathfrak{p}}(\zeta_n) \equiv \zeta_n^{N\mathfrak{p}} (\text{mod } \mathfrak{P})$$

. The field $[M/\mathfrak{P} : R/\mathfrak{p}]$ has $N\mathfrak{p}$ elements, thus $\zeta_n^{N\mathfrak{p}-1} \equiv 1 (\text{mod } \mathfrak{P})$. Let d be smallest positive integer with $\zeta_n^d \equiv 1 (\text{mod } \mathfrak{P})$. We show that $d | n$ and $d | N\mathfrak{p} - 1$.

Assume $d_1 = (d, n)$, then $\exists k, l \in \mathbb{Z}$ such that $kd + ln = d_1$. $\zeta_n^{d_1} \equiv \zeta_n^{kd+ln} \equiv \zeta_n^{kd}\zeta_n^{ln} \equiv 1 (\text{mod } \mathfrak{P})$, thus $d_1 \geq d$, and by the choice of d_1, $d_1 \leq d$ so $d_1 = d$. Similar process works if we take $N\mathfrak{p} - 1$ instead of d, proving the assertion. We now prove $d = n$. $\zeta_n^d \equiv 1 (\text{mod } \mathfrak{P})$, $G(K(\sqrt[n]{a'})/K)$ is cyclic and generated by $\sigma_{gen} : \alpha \to \zeta_n \alpha$. Take σ_{gen}^d.

$$\sigma_{gen}^d(\alpha) \equiv \zeta_n^d \alpha \equiv \alpha (\text{mod } \mathfrak{P}), \forall \alpha \in M$$

hence $\sigma_{gen}^d \in T_\mathfrak{p} = (1)$ hence $d = n$ and $n | N\mathfrak{p} - 1$. For the second part;

$$\left(\frac{a}{\mathfrak{p}}\right)_n (\sqrt[n]{a}) \equiv \sqrt[n]{a}^{N\mathfrak{p}} \equiv a^{\frac{N\mathfrak{p}-1}{n}} \sqrt[n]{a} (\text{mod } \mathfrak{P})$$

hence the property.

Proof: {Property iv} The characterization of the symbol in the previous proof is independent of $\mathfrak{P}$. This allows us to define the symbol analogously for the field $K_\mathfrak{p}$. The residue field $\mathcal{O}/\mathfrak{p}$ is a finite field with $N\mathfrak{p}$ elements ($\mathcal{O}$ be ring of integers). Let $a \in K_\mathfrak{p}^*$, then $a^{\frac{N\mathfrak{p}-1}{n}}$ make sense, and if also $n | N\mathfrak{p} - 1$, is an n-th root of unity in $\mathcal{O}/\mathfrak{p}$ which is exactly the n-th root of unity determined by power residue symbol. We can derive the lemma above just in a similar manner up to slight modifications. The crucial point is $\mathfrak{p}$ is unramified in $K(\sqrt[n]{a})/K$, which equivalently, thanks to Kummer Theory, is $\mathfrak{p} \not| na$ or equivalently $a \in K_\mathfrak{p}^*$ and $\mathfrak{p} \not| n$.

Proof: {Property v} 1) $\Leftrightarrow$ 2); Let c be generator of the field $\mathcal{O}/\mathfrak{p}$, and $a \equiv c^{a_1} (\text{mod } \mathfrak{p})$. $\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \Leftrightarrow a^{\frac{N\mathfrak{p}-1}{n}} \equiv 1 (\text{mod } \mathfrak{p}) \Leftrightarrow c^{\frac{a_1(N\mathfrak{p}-1)}{n}} \equiv 1 (\text{mod } \mathfrak{p}) \Leftrightarrow n | a_1 \Leftrightarrow a_1 = na_2 \Leftrightarrow a \equiv c^{a_2 n} \equiv (c^{a_2})^n (\text{mod } \mathfrak{p}) \Leftrightarrow a \equiv x^n (\text{mod } \mathfrak{p})$ solvable in $\mathcal{O}_\mathfrak{p}$ since a_2 is arbitrary integer and c^{a_2} spans all the residue field when a_2 spans integers.

2) $\Leftrightarrow$ 3); the "$\Leftarrow$" part is obvious. Assume $x^n \equiv a (\text{mod } \mathfrak{p})$ solvable. we claim that we can find a_i $i = 1, 2, \cdots$ such that $(a_0 + a_1\mathfrak{p} + a_2\mathfrak{p}^2 + \cdots)^n \equiv a (\text{mod } \mathfrak{p}^k)$ for all $k \in \mathbb{N}$. We use induction. Set $a_0 = x$, this makes the assertion true for $k = 1$. Set $u_k = a_0 + a_1\mathfrak{p} + a_2\mathfrak{p}^2 + \cdots + a_{k-1}\mathfrak{p}^{k-1}$. $(u_k + a_k\mathfrak{p}^k)^n \equiv u_k^n + nu_k^{n-1}a_k\mathfrak{p}^{k-1} (\text{mod } \mathfrak{p}^k)$ thus $a - (u_k + a_k\mathfrak{p}^k)^n \equiv a - u_k^n - nu_k^{n-1}a_k (\text{mod } \mathfrak{p}^k)$. By induction step $a - u_k^n$ is divisible by $\mathfrak{p}^{k-1}$, thus equation becomes $\frac{a-u_k^n}{\mathfrak{p}^{k-1}} - nu_k^{n-1}a_k (\text{mod } \mathfrak{p})$. We are allowed

to set $a_k \equiv \frac{a-u_k^n}{nu_k^{n-1}\mathfrak{p}^{k-1}}(\text{mod } \mathfrak{p})$ since characteristic of the residue field is prime to n, hence n are u_k^{n-1} invertible. This choice of a_n proves the induction step hence the lemma.

Proof: {Property vi} Assume $\mathfrak{b} = \mathfrak{p}$ a prime ideal, then since $\mathfrak{p} \in S(a)$, $\left(\frac{\zeta_n}{\mathfrak{p}}\right)_n = \zeta_n^{\frac{N\mathfrak{p}-1}{n}}$, hence the property. Now write $\mathfrak{b} = \prod_{i=1}^k \mathfrak{p}_i^{b_i}$, on one hand

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \prod_{i=1}^k \left(\frac{a}{\mathfrak{p}_i}\right)_n^{b_i} = \zeta_n^{\sum_{i=1}^k b_i \frac{N\mathfrak{p}_i - 1}{n}}$$

On the other hand, setting $N\mathfrak{p}_i = 1 + nr_i$ then;

$$N\mathfrak{b} \equiv \prod_{i=1}^k (1+nr_i)^{b_i} \equiv \prod_{i=1}^k 1 + nr_ib_i \equiv 1 + n\sum_{i=1}^k r_ib_i(\text{mod } n^2)$$

hence

$$\frac{N\mathfrak{b}-1}{n} \equiv \sum_{i=1}^k b_i \frac{(N\mathfrak{p}_i - 1)}{n}(\text{mod } n)$$

and the property.

Proof: {Property vii} If $a' \equiv a(\text{mod } \mathfrak{b})$ then $\mathfrak{p} \in I^{S(a,a')}$. By ii)

$$\left(\frac{a'a^{-1}}{\mathfrak{b}}\right)_n = \left(\frac{a'}{\mathfrak{b}}\right)_n \left(\frac{a}{\mathfrak{b}}\right)_n^{-1}$$

and by property iv), this is equivalent to 1 since $a'a^{-1} \equiv 1(\text{mod } \mathfrak{b})$.

Proof: {Property viii} Artin theorem for the extension $K(\sqrt[n]{a}/K)$ implies that for all $\mathfrak{p}_i \in S(a)$ there exit $k_i \in \mathbb{N}$ such that $x \in K^*$ and $x \equiv 1(\text{mod } \mathfrak{p}_i)$ implies $(x, K(\sqrt[n]{a}/K)) = 1$. Now fix these k_i. The assumption of $c \in (K_{\mathfrak{p}}^*)^n$ implies that $c \equiv x_i^n(\text{mod } \mathfrak{p}_i^{k_i})$ is solvable with $x_i \in \mathcal{O}_i$ integer rinf of $\mathfrak{p}_i$. By approximation lemma we can find a c_0 such that $c_0 \equiv x_i(\text{mod } \mathfrak{p}_i^{k_i})$. By Artin's theorem we clearly have $(c/(c_0)^n, K(\sqrt[n]{a}/K)) = 1$. On the other hand

$$1 = (c/(c_0)^n, K(\sqrt[n]{a}/K)) = (c, K(\sqrt[n]{a}/K))(c_0, K(\sqrt[n]{a}/K))^{-n} = (c, K(\sqrt[n]{a}/K)) =$$

$$= (\mathfrak{b}'\mathfrak{b}^{-1}, K(\sqrt[n]{a}/K)) = (\mathfrak{b}', K(\sqrt[n]{a}/K))(\mathfrak{b}, K(\sqrt[n]{a}/K))^{-1}$$

Hence $(\mathfrak{b}', K(\sqrt[n]{a}/K))$ and $(\mathfrak{b}, K(\sqrt[n]{a}/K)$ are the same element of $G(K(\sqrt[n]{a}/K))$ and both send $\sqrt[n]{a}$ to the same number, thus $\left(\frac{a}{\mathfrak{b}'}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n$.

Now we specialize to the case $K = \mathbb{Q}$, $n = 2$. Let a, b denote arbitrary integers, and p, q denote positive odd primes. For $(a, p) = 1$ the quadratic residue symbol $\left(\frac{a}{p}\right) = \left(\frac{a}{(p)}\right) = 1$ is defined, is multiplicative in each argument separately, and satisfies; $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ by vii and $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ if $p \equiv q (\text{mod } 8a_0)$ by viii where a_0 is the odd part of a. The second follows from the fact that integers $\equiv 1 (\text{mod } 8)$ are 2-adic squares. We now get the classical form of quadratic reciprocity;

Theorem 6.1.3

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof: Taking $a = -1$ by property $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ if $p \equiv q (\text{mod } 8)$ we are reduced to check this for $p = 3, 5, 7, 17$, which evidently satisfy $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Taking $a = 2$, by similar property we are reduced to cases $p = 3, 5, 7, 17$ and these evidently satisfy $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. For the last one, define

$$< p, q >= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

If $p \equiv q (\text{mod } 8)$, writing $q = p + 8a$ then

$$\left(\frac{q}{p}\right) = \left(\frac{8a}{p}\right) = \left(\frac{8a}{q}\right) = \left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right).$$

hence we get $< p, q >= \left(\frac{-1}{q}\right)$ for $p \equiv q (\text{mod } 8)$. Now assume p, q arbitrary, then there is a prime r different than q with $rp \equiv q (\text{mod } 8)$, and another prime s different than q such that $s \equiv pr (\text{mod } 8)$ then

$$< p, q >< r, q >=< pr, q >=< s, q >= \left(\frac{-1}{q}\right).$$

We see that $< p, q >$ depends only on q modulo 8. by symmetry since $< p, q >< q, p >= 1$, we are reduced to check the cases for $p = 3, 5, 7, 17$ and $q = 3, 5, 7, 17$, which, up to a long calculation, evidently satisfy $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

6.2 Norm Residue Symbol

Let $a, b \in K^*$, let $\mathfrak{p}$ be an arbitrary prime. Let $\mathfrak{P}$ be a prime of the Kummer extension $K(\sqrt[n]{a})/K$ above $\mathfrak{p}$. Denote by $K(\sqrt[n]{a})_{\mathfrak{P}}$ the completion of $K(\sqrt[n]{a})$ with respect to $\mathfrak{P}$. $\psi_{\mathfrak{p}} : K_{\mathfrak{p}} \to G(K_{\mathfrak{P}}(\sqrt[n]{a})/K_{\mathfrak{p}})$ denote the local Artin map associated with $K(\sqrt[n]{a})/K$. The image of $G(K_{\mathfrak{P}}(\sqrt[n]{a})/K_{\mathfrak{p}})$ is identified by the decomposition group $D_{\mathfrak{P}}(K(\sqrt[n]{a})/K) \subset G(K(\sqrt[n]{a})/K)$, and is independent of the choice of the root $\sqrt[n]{a}$. Let $b \in K^*$ and (b) denote the its principal. If we consider a as element of $K_{\mathfrak{p}}^*$ then $\psi_{\mathfrak{p}}((b))(\sqrt[n]{a})$ makes sense, in fact;

$$[\psi_{\mathfrak{p}}((b))(\sqrt[n]{a})]^n = \psi_{\mathfrak{p}}((b))((\sqrt[n]{a})^n) = a = (\sqrt[n]{a})^n$$

since $G(K_{\mathfrak{P}}(\sqrt[n]{a})/K_{\mathfrak{p}})$ acts trivially on $K_{\mathfrak{p}}^*$, therefore

$$[\psi_{\mathfrak{p}}((b))(\sqrt[n]{a})]^n - (\sqrt[n]{a})^n = \prod_{i=0}^{n-1} [\psi_{\mathfrak{p}}((b))(\sqrt[n]{a}) - \zeta_n^i \sqrt[n]{a}]$$

for some $i_0 \in \mathbb{N}$, $\psi_{\mathfrak{p}}((b))(\sqrt[n]{a}) = \zeta_n^{i_0} \sqrt[n]{a}$. i_0 is independent of $\sqrt[n]{a}$, and depends only on a, b and $\mathfrak{p}$;

Definition 6.2.1

$$\left(\frac{a, b}{\mathfrak{p}}\right)_n = \zeta_n^{i_0}$$

or more transparently

$$(\psi_{\mathfrak{p}}((b))(\sqrt[n]{a}) = \left(\frac{a, b}{\mathfrak{p}}\right)_n \sqrt[n]{a}$$

is called the norm residue symbol associated to a and b at $\mathfrak{p}$.

Norm residue symbol also possesses certain properties similar to that of power reside symbol.

Theorem 6.2.2 *Let $a, a', b, b' \in K_{\mathfrak{p}}^*$, S denote the set of infinite primes, $S(a_1, \cdots, a_r)$ denote the set of primes $S \cup \{\mathfrak{p} : \exists i$ such that $v_{\mathfrak{p}}(a_i) \neq 0\}$. Then the following properties hold;*

i)

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{a,b'}{\mathfrak{p}}\right)_n = \left(\frac{a,bb'}{\mathfrak{p}}\right)_n$$

and

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{a',b}{\mathfrak{p}}\right)_n = \left(\frac{aa',b}{\mathfrak{p}}\right)_n$$

ii) *If one of a, $b \in (K_{\mathfrak{p}}^*)^n$, then;*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$$

iii) *If b is a norm for the extension $K_{\mathfrak{p}}(\sqrt[n]{a})/K_{\mathfrak{p}}$ then;*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1.$$

iv) *If $a + b \in (K^*)^n$ then*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$$

In particular; $(a, -a) = 1$ and $(a, 1 - a) = 1$.

v) *If $a, b \in K^*$ then*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n \left(\frac{b,a}{\mathfrak{p}}\right)_n = 1$$

vi) *If $\mathfrak{p}$ is infinite prime, then $\left(\frac{a,b}{\mathfrak{p}}\right)_2 = -1$ if both $a < 0$ and $b < 0$ in $K_{\mathfrak{p}}$, and for all other cases;*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$$

vii) *{Relation between norm-residue and power residue symbols} If $\mathfrak{p} \notin S(a)$ then*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(b)}$$

in particular, $\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$ for for $\mathfrak{p} \notin S(a, b)$.

viii) *If $\mathfrak{p} \notin S$ then;*

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n = \left(\frac{(-1)^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)}a^{v_{\mathfrak{p}}(b)}b^{-v_{\mathfrak{p}}(a)}}{\mathfrak{p}}\right)_n$$

ix) *{The Product formula} For $a, b \in K^*$, we have*

$$\prod_{\mathfrak{p} \in \mathfrak{M}} \left(\frac{a, b}{\mathfrak{p}} \right)_n = 1$$

where $\mathfrak{M}$ is the set of all primes of K (including the infinite primes).

We prove the properties;

Proof: {Property i} First one is immediate from norm residue symbol definition and the multiplicative property of local artin maps. The second part; let $\mathfrak{P}_a$, $\mathfrak{P}_{a'}$,$\mathfrak{P}_{aa'}$, $\mathfrak{P}$ denote the primes of $K(\sqrt[n]{a})$, $K(\sqrt[n]{a'})$, $K(\sqrt[n]{aa'})$, $K(\sqrt[n]{a}, \sqrt[n]{a'})$ above $\mathfrak{p}$ respectively, $K_{\mathfrak{P}_a}(\sqrt[n]{a})$, $K_{\mathfrak{P}_{a'}}(\sqrt[n]{a'})$, $K_{\mathfrak{P}_{aa'}}(\sqrt[n]{aa'})$, $K_{\mathfrak{P}}(\sqrt[n]{a}, \sqrt[n]{a'})$ denote respective closures, $\sigma_a \in G(K_{\mathfrak{P}_a}(\sqrt[n]{a})/K)$, $\sigma_{a'} \in G(K_{\mathfrak{P}_{a'}}(\sqrt[n]{a'})/K)$ $\sigma_{aa'} \in G(K_{\mathfrak{P}_{aa'}}(\sqrt[n]{a})/K)$ $\sigma \in G(K_{\mathfrak{P}}(\sqrt[n]{a}, \sqrt[n]{a'})/K)$ be respective elements of the respective Galois groups which correspond to local artin maps associated to a, b and respective primes. On one hand $\sigma(\sqrt[n]{a}) = \sigma_a(\sqrt[n]{a}) = \zeta_n^i \sqrt[n]{a}$ for some $i \in \mathbb{N}$ since $\sqrt[n]{a} \in K_{\mathfrak{P}_a}(\sqrt[n]{a})$. Similarly $\sigma(\sqrt[n]{a'}) = \sigma_{a'}(\sqrt[n]{a'}) = \zeta_n^j \sqrt[n]{a'}$ for some $j \in \mathbb{N}$ since $\sqrt[n]{a'} \in K_{\mathfrak{P}_{a'}}(\sqrt[n]{a'})$. On the other hand $\sigma(\sqrt[n]{aa'}) = \sigma(\sqrt[n]{a})\sigma(\sqrt[n]{a'}) = \zeta_n^{i+j} \sqrt[n]{aa'}$, but $\sigma(\sqrt[n]{aa'}) = \sigma_{aa'}(\sqrt[n]{aa'})$ since $\sqrt[n]{aa'} \in K_{\mathfrak{P}_{aa'}}(\sqrt[n]{aa'})$ hence i).

Proof: {Property ii} Assume $b \in (K_{\mathfrak{p}}^*)^n$, write $b = x^n$ with $x \in K_{\mathfrak{p}}^*$. The local Artin map associated with x, a and $\mathfrak{p}$ is identified by a decomposition group, and hence is a subgroup of a cyclic group of order n. This map's action on $\sqrt[n]{a}$ is uniquely determined by an element $\sigma \in G(K(\sqrt[n]{a})/K)$ by $\sqrt[n]{a} \to \sigma(\sqrt[n]{a})$. Due to linearity we have;

$$\left(\frac{a, b}{\mathfrak{p}} \right)_n \sqrt[n]{a} = \sigma^n(\sqrt[n]{a}) = \sqrt[n]{a}$$

Hence the property. Assume now $a \in (K_{\mathfrak{p}}^*)^n$; and let $x = \sqrt[n]{a}$ with $x \in K_{\mathfrak{p}}$. Local Artin map is identified by Galois group $G(K_{\mathfrak{P}}(\sqrt[n]{a})/K_{\mathfrak{p}})$ and acts trivially on $K_{\mathfrak{p}}^*$. Let σ as before; then

$$\left(\frac{a, b}{\mathfrak{p}} \right)_n \sqrt[n]{a} = \sigma(\sqrt[n]{a}) = \sqrt[n]{a}$$

hence the property.

We need a couple of lemma in order to prove iii.

Lemma 6.2.3 *Let L/K and L'/K' be abelian extensions with Galois groups G and G' respectively, such that $L' \supset L$ and $K' \supset K$, let θ be the natural map $G' \to G$ (every automorphism of L'/K' induces one of L/K). S denote finite set of primes of K including infinite primes and those ramified in L', let S' be the set of primes of K' above those in S. Then the diagram*

$$\begin{tikzcd} I^{S'} \arrow[r, "(,L'/K')"] \arrow[d, "N_{K'/K}"] & G' \arrow[d, "\theta"] \\ I^S \arrow[r, "(,L/K)"] & G \end{tikzcd}$$

is commutative, where N denotes norm.

Proof: By linearity, it is clear that it is enough to check that

$$\theta((\mathfrak{p}', L'/K')) = (N_{K'/K}\mathfrak{p}', L/K)$$

for an arbitrary prime $\mathfrak{p}'$ of K' such that $\mathfrak{p}' \notin S'$. Let $N_{K'/K}\mathfrak{p}' = \mathfrak{p}^f$, where $\mathfrak{p}$ is teh prime of K below $\mathfrak{p}'$; thus $f = [K_{\mathfrak{p}'} : K_{\mathfrak{p}}]$. Let $\sigma' = (\mathfrak{p}', L'/K')$ and $\sigma = (\mathfrak{p}, L/K)$. We must show $\theta(\sigma') = \sigma^f$. Now σ and σ' are determined by their effect on the residue fields. Let $\mathfrak{P}'$ be a prime of L' above $\mathfrak{p}'$ and let $\mathfrak{P}$ be the prime of L below $\mathfrak{P}'$. For $x \in K_{\mathfrak{P}} \subset K_{\mathfrak{P}'}$ we have

$$\sigma'(x) = x^{N\mathfrak{p}'} = x^{N\mathfrak{p}^f} = x^{\sigma^f}$$

as required.

Lemma 6.2.4 *Keeping the notations of previous lemma, and assuming that global Artin maps $\psi_{L/K}$ and $\psi_{L'/K'}$ exists for L/K and L'/K' respectively, then;*

$$\begin{tikzcd} J_{K'} \arrow[r, "\psi_{L'/K'}"] \arrow[d, "N_{K'/K}"] & G' \arrow[d, "\theta"] \\ J_K \arrow[r, "\psi_{L/K}"] & G \end{tikzcd}$$

is a commutative diagram.

Proof: Let S be finite set of primes of K including infinite primes and those ramified in L', and S' be set of primes of K' above S. We have the diagram;

$$\begin{tikzcd}
 & I_{K'}^{S'} \arrow[dr, "{(,L'/K')}"] \arrow[dd] & \\
J_{K'}^{S'} \arrow[ur] \arrow[rr, "\psi_{L'/K'}"] \arrow[dd, "N_{K'/K}"] & & G' \arrow[dd, "\theta"] \\
 & I_K^S \arrow[dr, "{(,L/K)}"] & \\
J_K^S \arrow[ur] \arrow[rr, "\psi_{L/K}"] & & G
\end{tikzcd}$$

The non-rectangular parallelograms are commutative by the compatibility of ideal and idele norms, and by previous lemma. The triangles are commutative by iii) property of the global Artin map (i.e. $\psi_{L/K}(x) = ((x)^S, L/K)$ for all $x \in J_K^S$). Thus the rectangle is commutative, i.e. the restrictions of $\psi_{L/K} \circ N_{K'/K}$ and $\theta \circ \psi_{L'/K'}$ to $J_{K'}^{S'}$ coincide. But those two homomorphisms take 1 on principal ideles by ii) property of global Artin maps, so the coincide on $(K')^* J_{K'}^{S'}$, which is a dense subset of $J_{K'}$ by the weak approximation theorem. Since the two homomorphism are continuous, the coincide on all of $J_{K'}$, proving the lemma.

Lemma 6.2.5 *Suppose the abelian extension L/K has a global Artin map $\psi_{L/K}$ and $K \subset M \subset L$ intermediate field. Then $\psi_{L/K}(N_{M/K}J_M) \in G(L/M)$ where $G(L/M)$ is the Galois groups of L/M.*

Proof: If we replace $L' = L$, $K' = M$ with the diagram in the previous proof we get $G' = G(L/M)$ and;

$$\begin{tikzcd}
 & I_M^{S'} \arrow[dr, "{(,L/M)}"] \arrow[dd] & \\
J_M^{S'} \arrow[ur] \arrow[rr, "\psi_{L/M}"] \arrow[dd, "N_{M/K}"] & & G(L/M) \arrow[dd, "\theta"] \\
 & I_K^S \arrow[dr, "{(,L/K)}"] & \\
J_K^S \arrow[ur] \arrow[rr, "\psi_{L/K}"] & & G(L/K)
\end{tikzcd}$$

It shows that $\psi_{L/K}(N_{M/K}J_M^{S'}) \subset G(L/M)$. Consequently the same is true with $J_M^{S'}$ replaced by $M^*J_M^{S'}$, and since this set is dense in J_M we are done.

Lemma 6.2.6 *Let L/K abelian extension, $\mathfrak{p}$ be prime of K, and $\mathfrak{P}$ be prime of L above $\mathfrak{p}$. Denote $K_\mathfrak{p}$ and $L_\mathfrak{P}$ the completion of K and L with respect to $\mathfrak{p}$ and $\mathfrak{P}$ respectively. Assume that the global Artin map $\psi_{L/K}$ exists for L/K, and let $\psi_\mathfrak{p}$ denote the local Artin map associated to extension $L_\mathfrak{P}/K_\mathfrak{p}$. If $\mathscr{M}$ is an intermediate field $K_\mathfrak{p} \subset \mathscr{M} \subset L_\mathfrak{P}$, then $\psi_\mathfrak{p}(N_{\mathscr{M}/K_\mathfrak{p}}\mathscr{M}^*) \subset G(L_\mathfrak{P}/\mathscr{M})$.*

Proof: Let $M = L\cap\mathscr{M}$ be the fixed field of $G(L_\mathfrak{P}/\mathscr{M})$ in L, so that $G(L/M)$ is identified with $G(L_\mathfrak{P}/\mathscr{M})$ under the identification of the decomposition group with the local Galois group. Then $\mathscr{M} = M_{\mathfrak{P}'}$, where $\mathfrak{P}'$ is a prime above $\mathfrak{p}$ and the diagram

$$\begin{tikzcd}
M_{\mathfrak{P}'} \arrow[r, "i_{\mathfrak{P}'}"] \arrow[d, "N_{\mathscr{M}/K_\mathfrak{p}}"] & J_M \arrow[d, "N_{M/K}"] \\
K_\mathfrak{p} \arrow[r, "i_\mathfrak{p}"] & J_K
\end{tikzcd}$$

is commutative where $i_\mathfrak{p}$ and $i_{\mathfrak{P}'}$ denote the natural injection. By the previous lemma we get

$$\psi_\mathfrak{p}(N_{\mathscr{M}/K_\mathfrak{p}}\mathscr{M}^*) \subset \psi_{L/K}N_{M/K} \subset G(L/M) \simeq G(L_\mathfrak{P}/\mathscr{M})$$

hence the lemma.

Proof: {Property iii} In the previous lemma taking $\mathscr{M} = L_\mathfrak{P}$ we get $\psi_\mathfrak{p}(N_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P})^*) = \{1\}$, hence the property.

Proof: {Property iv} Let $a + b = x^n$ and $\sqrt[n]{a}$ be an n-th root of a. The map $G(K(\sqrt[n]{a})/K) \to \mu_n$ given by $\sigma \to \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ is an isomorphism of the Galois group of $K(\sqrt[n]{a})/K$ onto a subgroup μ_d of μ_n, which is independent of choice of $\sqrt[n]{a}$ (μ_d and μ_n are groups of d-th and n-th root of unity respectively). If $(\zeta_n^{a_i})_{i=1}^{n/d}$ is a system of representatives of the co sets of μ_d in μ_n, we have then; $b = x^n - a = \prod_{\zeta_n\in\mu_m}(x - \zeta_n\sqrt[n]{a}) = N_{K(\sqrt[n]{a})/K}(\prod_{i=1}^{n/d} x - \zeta_n^{a_i}\sqrt[n]{a})$, hence if $y =$

$\prod_{i=1}^{n/d}(x-\zeta_n^{a_i}\sqrt[n]{a})$ then $b = N_{K(\sqrt[n]{a})/K}(y)$ and by iii) we have $\left(\frac{a,b}{\mathfrak{p}}\right)_n = 1$, as desired.

Proof: {Property v}

$$1=\left(\frac{ab,-ab}{\mathfrak{p}}\right)_n=\left(\frac{a,-a}{\mathfrak{p}}\right)_n\left(\frac{a,b}{\mathfrak{p}}\right)_n\left(\frac{b,-a}{\mathfrak{p}}\right)_n\left(\frac{b,-b}{\mathfrak{p}}\right)_n\left(\frac{b,-1}{\mathfrak{p}}\right)_n=\left(\frac{a,b}{\mathfrak{p}}\right)_n\left(\frac{b,a}{\mathfrak{p}}\right)_n$$

Proof: {Property vi} All primes of function fields are discrete, so are non-archimedean. The infinite primes can occur only in number field case, hence we consider K to be number field. For $n = 2$, there is

Proof: {Property vii} Since $\mathfrak{p}$ is unramified in $K(\sqrt[n]{a})$ both symbols, by definition, are determined by the action of corresponding Frobenious automorphisms on a up to power $v_{\mathfrak{p}}(b)$, hence the proposition is immediate.

Proof: {Property viii} Write $a = \pi^{v_{\mathfrak{p}}(a)}a_0$ with π is uniformizer for $\mathfrak{p}$ and $b = \pi^{v_{\mathfrak{p}}(b)}b_0$ with a_0 and b_0 are units.

$$\left(\frac{a,b}{\mathfrak{p}}\right)_n=\left(\frac{\pi^{v_{\mathfrak{p}}(a)}a_0,\pi^{v_{\mathfrak{p}}(b)}b_0}{\mathfrak{p}}\right)_n=\left(\frac{\pi^{v_{\mathfrak{p}}(a)},\pi^{v_{\mathfrak{p}}(b)}}{\mathfrak{p}}\right)_n\left(\frac{a_0,\pi^{v_{\mathfrak{p}}(b)}}{\mathfrak{p}}\right)_n\left(\frac{\pi^{v_{\mathfrak{p}}(a)},b_0}{\mathfrak{p}}\right)_n\left(\frac{a_0,b_0}{\mathfrak{p}}\right)_n=$$

$$=\left(\frac{\pi,\pi}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)}\left(\frac{a^{v_{\mathfrak{p}}(b)}b^{-v_{\mathfrak{p}}(a)}}{\mathfrak{p}}\right)_n$$

By linearity of symbol and by vii. We are reduced to show $\left(\frac{\pi,\pi}{\mathfrak{p}}\right)_n = -1$.

$$\left(\frac{\pi,\pi}{\mathfrak{p}}\right)_n=\left(\frac{-1,\pi}{\mathfrak{p}}\right)_n\left(\frac{-\pi,\pi}{\mathfrak{p}}\right)_n=\left(\frac{-1,\pi}{\mathfrak{p}}\right)_n=(-1)^{v_{\mathfrak{p}}(\pi)}=-1$$

as desired.

Proof: {Property ix} This is the direct consequence of the Artin's theorem 5.5.2

Hence we finish the proofs of the properties.

6.3 The General Power Reciprocity Law

Theorem 6.3.1 (The General Power Reciprocity Law) *Let $a, b \in K^*$, define the n-th power residue symbol of a with respect to b to be*

$$\left(\frac{a}{b}\right)_n = \prod_{\mathfrak{p} \notin S(a)} \left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(b)} = \left(\frac{a}{(b)^{S(a)}}\right)_n$$

Then we have

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p} \in S(a) \cap S(b)} \left(\frac{b,a}{\mathfrak{p}}\right)_n$$

in particular, if $S(a) \cap S(b) = S$ then

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p} \in S} \left(\frac{b,a}{\mathfrak{p}}\right)_n$$

and if $S(\lambda) = S$, then;

$$\left(\frac{\lambda}{b}\right)_n = \prod_{\mathfrak{p} \in S} \left(\frac{\lambda, b}{\mathfrak{p}}\right)_n$$

Remark 6.3.2 *The second particular case is analogue of the supplementary laws.*

Proof:

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p} \notin S(a)} \left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(b)} \prod_{\mathfrak{p} \notin S(b)} \left(\frac{b}{\mathfrak{p}}\right)_n^{-v_{\mathfrak{p}}(b)} = \prod_{\mathfrak{p} \notin S(a) \cap S(b)} \left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(b)} \left(\frac{b}{\mathfrak{p}}\right)_n^{-v_{\mathfrak{p}}(b)} =$$

$$= \prod_{\mathfrak{p} \notin S(a) \cap S(b)} \left(\frac{a,b}{\mathfrak{p}}\right)_n = \prod_{\mathfrak{p} \in S(a) \cap S(b)} \left(\frac{b,a}{\mathfrak{p}}\right)_n$$

hence the theorem. Particular cases are obvious.

We now apply this result to $\mathbb{Q}$ and obtain the classical quadratic reciprocity;

6.3.1 Quadratic Reciprocity Revisited

Let $K = \mathbb{Q}$ and $n = 2$. The infinite prime is the ordinary absolute value of $\mathbb{Q}$, which we denote by ∞, and the completion is $\mathbb{R}^+ \cup \{0\}$. The only ramified prime is $\mathfrak{p} = 2$ since this is the unique prime divisor $n = 2$. Then $S = \{2, \infty\}$. Let a, b are odd primes which are coprime, then by definition $\left(\frac{a}{b}\right)_2$ becomes the ordinary quadratic symbol. By the law we have;

$$\left(\frac{a}{b}\right)_2 \left(\frac{b}{a}\right)_2^{-1} = \left(\frac{a,b}{2}\right)_2 \left(\frac{a,b}{\infty}\right)_2$$

$\left(\frac{a,b}{\infty}\right)_2 = -1$ if both $a, b < 0$ and 1 otherwise, thus $\left(\frac{a,b}{\infty}\right)_2 = (-1)^{\frac{(sgn(a)-1)(sgn(b)-1)}{4}}$. By previous section, hence we get the reciprocity law;

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n = (-1)^{\frac{(a-1)(b-1)}{4} + \frac{(sgn(a)-1)(sgn(b)-1)}{4}}$$

and supplementary laws;

$$\left(\frac{-1}{p}\right)_n = (-1)^{\frac{p-1}{2}}, \left(\frac{2}{p}\right)_n = (-1)^{\frac{p^2-1}{8}}$$

where p is positive odd prime.

On the other hand, these formulas easily established working locally in $\mathbb{Q}_2$ in the following way;

Lemma 6.3.3 *b, c be non negative integers;*

$$(1 + 4c, b)_2 = (-1)^{v_2(b)c}$$

where $v_2(b)$ is the order of 2 dividing b.

Proof: Let p odd prime, then $x^2 \equiv 1 + 4c(\text{mod } p)$ solvable iff $x^2 - 1 \equiv (x-1)(x+1) \equiv 4c(\text{mod } p)$ solvable. Taking $x \equiv \frac{4+c}{2}(\text{mod } p)$ which is legal, hence $(1+4c, p)_2 = 1$. Now, $1+4c$ is a 2-adic square iff c is even, thus $(1+4c, 2)_2 = (-1)^c$ and by multiplicativity, $(1 + 4c, b)_2 = (-1)^{v_2(b)c}$.

Now $(3, 3)_2 = 1$ hence we can get the reciprocity law by just applying the multiplication formula. We see generalization in following section.

6.4 Generalizations

The localization idea and the properties of norm residue symbol suggest that it is enough to calculate the symbol only at certain numbers and get explicit form of the reciprocity law for all numbers. According to the reciprocity theorem only the primes divisors n is in our field of interest. We now begin to calculate the symbol starting with the simplest case. Assume p is an odd prime, $n = p$ and $K = \mathbb{Q}(\zeta_p)$. First we observe that p is totally ramified at K;

Lemma 6.4.1 *p is totally ramified at K. Let $\mathfrak{p}$ be the prime ideal above p, then $\pi = 1 - \zeta_p$ is uniformizer of $\mathfrak{p}$ and $(p) = \pi^{p-1}$.*

Proof: ζ_p is root to $X^p - 1 = 0 = \prod_{i=0}^{p-1}(X - \zeta_p^i)$, dividing by $X - 1$ and putting $X = 1$ we get $p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$. We now show that for relatively prime integers a and b with $p \not| ab$ the number $\frac{1-\zeta_p^a}{1-\zeta_p^b}$ is a unit in K. To prove it choose $k \in \mathbb{Z}$ such that $a \equiv bk (\text{mod } p)$ hence $\frac{1-\zeta_p^a}{1-\zeta_p^b} = \frac{1-\zeta_p^{bk}}{1-\zeta_p^b} = 1 + \zeta_p^b + \cdots + \zeta_p^{b(k-1)}$ which is in the ring of integers of K. Similar process works for $\frac{1-\zeta_p^b}{1-\zeta_p^a}$ and this is also in the ring of integers, hence both must be units. In particular $\frac{1-\zeta_p^i}{1-\zeta_p}$ is a unit, hence $p = \pi^{p-1}u$ for some unit u, proving $(p) = (\pi)^{p-1}$. On the other hand the degree of the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q} = p - 1$, by ramification theory we must have (π) is a prime ideal with p elements in in its residue field, hence $\mathfrak{p} = (\pi)$ and the lemma.

Set $K_\mathfrak{p}$ to be the completion of K with respect to $\mathfrak{p}$. Let U denote the units of $K_\mathfrak{p}$ and $U_i = \{u \in U : u \equiv 1 (\text{mod } \mathfrak{p}^i)\}$ for $i = 1, 2, \cdots$. We denote $\eta_i = 1 - \pi^i$. In the following we are going to prove that any nonzero number x of $K_\mathfrak{p}$ is of the form $x = x_1^p x_2$ where $x_1 \in K$ and x_2 is generated by $\pi, \eta_1, \eta_2, \cdots, \eta_p$. The advantage of this representation is that explicit calculation of the norm residue symbol amounts to calculation of this symbol only at certain numbers, i.e. at the numbers generated by π and η_i's. We will come to this point after proving the assertion.

Lemma 6.4.2 *η_i generates U_i/U_{i+1}, which is a cyclic group of order p.*

Proof: Let $U = 1 + \pi^{i+1}U_1 \in U_{i+1}$, we show $\exists u \in U_i$ such that $u = 1 + \pi^i u_1$ and $U = \eta_i^j u$ for some $j \in \{0, 1, 2, \cdots, p-1\}$. This is equivalent to

$$\eta_i^j u = (1 - \pi^i)^j (1 + \pi^i u_1) \equiv U \equiv 1 + \pi^{i+1}U_1 \equiv 1 (\text{mod } \mathfrak{p}^{i+1})$$

but this is if and only if $(1-\pi^i)^j(1+\pi^i u_1) \equiv 1+\pi^i(u_1+j) \equiv 1(\text{mod } \mathfrak{p}^{i+1})$. Choosing $j \equiv u_1(\text{mod } \mathfrak{p})$ gives the assertion. U_i/U_{i+1} is isomorphic to the multiplicative group of $\{1, \eta_i, \cdots, \eta_i^{p-1}\}$ where the powers are in mod p, hence it's cyclic of order p.

Lemma 6.4.3 *The image of* π *generates* $K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^p U_1$.

For proof we need another lemma;

Lemma 6.4.4

$$U_{p+1} \subset (K_{\mathfrak{p}}^*)^p.$$

Proof: Let $u = 1 + \pi^{p+1}a_1 + \pi^{p+2}a_2 + \cdots \in U_{i+1}$ with a_i's are in the representative set of mod $\mathfrak{p}$. We want to show existence of $x \in K_{\mathfrak{p}}^*$ such that $x^p = u$, which is equivalent to say that $x^p \equiv u(\text{mod } \mathfrak{p}^{p+k})$ solvable for all $k \in \mathbb{N}$. We show this by induction; for $k = 1$ this is evident. Let assume assertion holds for k, i.e. $x_k^p \equiv u(\text{mod } \mathfrak{p}^{p+k})$ for some $x_k \in K_{\mathfrak{p}}^*$, set $x_{k+1} = x + \pi^{k+1}c$ where c will be suitably chosen.

$$x_{k+1}^p \equiv (x+\pi^k c)^p \equiv x^p + p\pi^k c x^{p-1} \equiv x^p + u_0\pi^{k+p}cx^{p-1}(\text{mod } \mathfrak{p}^{p+k})$$

where $p = \pi^{p-1}u_0$ for fixed unit u_0. Choosing $c \equiv \frac{x^p-u}{u_0x^{p-1}}(\text{mod } \mathfrak{p})$, which is evidently legal, proves the assertion for $k+1$. By induction, hence the lemma.

Proof: {of the previous lemma} We now show that any $\gamma \in K_{\mathfrak{p}}^*$ is of the form $\gamma = \pi^k\gamma_1^p(1+l\pi)$ with $k \in \mathbb{Z}$ and $l \in \mathcal{O}$ (the ring of integers of $K_{\mathfrak{p}}$). We are reduced to show that every unit in $K_{\mathfrak{p}}$ is of the form $\gamma_1^p(1+l\pi) = (\bar{\gamma_0} + \bar{\gamma_1}\pi + \bar{\gamma_2}\pi^2 + \cdots)^p(1+l\pi)$, and this is equivalent to

$$u \equiv (\bar{\gamma_0} + \bar{\gamma_1}\pi + \bar{\gamma_2}\pi^2 + \cdots)^p(1+l\pi)(\text{mod } p^k)$$

is solvable for fixed $u \in U$ and every $k \in \mathbb{N}$. Choose $\bar{\gamma_0} \equiv u(\text{mod } \mathfrak{p})$, and thus $\bar{\gamma_0}^p \equiv \bar{\gamma_0}(\text{mod } \mathfrak{p})$. On the other hand $(\bar{\gamma_0} + \bar{\gamma_1}\pi + \bar{\gamma_2}\pi^2 + \cdots)^p = \bar{\gamma_0}^p + \tilde{\gamma_1}\pi^p + \tilde{\gamma_2}\pi^{p+1} + \cdots$, hence choosing $l = \frac{u-\bar{\gamma_0}^p}{\pi}$ works for $k \leq p$, for $k > p$, it is just the similar induction step that we used at the proof before.

Corollary 6.4.5 *Any element* $x \in K_{\mathfrak{p}}^*$ *is of the form* $x = \pi^{\alpha_0}\eta_1^{\alpha_1}\cdots\eta_p^{\alpha_p}x_1^p$ *where the representation is unique, hence, if* $y \in K_{\mathfrak{p}}^*$ *and of the form* $y = \pi^{\mathfrak{P}_0}\eta_1^{\mathfrak{P}_1}\cdots\eta_p^{\mathfrak{P}_p}y_1^p$ *then*

$$\left(\frac{x,y}{\mathfrak{p}}\right)_p = \prod_{i,j\in\{0,1,2,\cdots,p\}} \left(\frac{\eta_i,\eta_j}{\mathfrak{p}}\right)_p^{\alpha_i\mathfrak{P}_j}.$$

For convenience we set $\eta_0 = \pi$*.*

Proof: By above lemmas and bi linearity property of the norm residue symbol gives the corollary. The only thing to show is uniqueness. But this follows from checking x in mod $\mathfrak{p}^k$ for $k = 1, 2, 3, \cdots$ inductively, hence the corollary.

We now calculate the symbol explicitly at the basis, i.e. at η_i's and π.

Proposition 6.4.6 a) $\left(\frac{\eta_i,\eta_j}{\mathfrak{p}}\right)_p = \left(\frac{\eta_i,\eta_{i+j}}{\mathfrak{p}}\right)_p \left(\frac{\eta_{i+j},\eta_j}{\mathfrak{p}}\right)_p \left(\frac{\eta_{i+j},\pi}{\mathfrak{p}}\right)_p^{-j}.$

b) *If* $i + j \geq p + 1$*, then* $\left(\frac{a,b}{\mathfrak{p}}\right)_p = 1$ *for all* $a \in U_i$ *and* $b \in U_j$*.*

c) $\left(\frac{\eta_i,\pi}{\mathfrak{p}}\right)_p = 1$ *for* $1 \leq i \leq p-1$ *and* $\left(\frac{\eta_p,\pi}{\mathfrak{p}}\right)_p = \zeta_p$*.*

Proof: {a), b) and first part of c)} We have by definition that $\eta_{i+j} = \eta_j + \pi^j\eta_i$, hence $1 = \frac{\eta_j}{\eta_{i+j}} + \pi^j\frac{\eta_i}{\eta_{i+j}}$. By vi), i) and ii) properties of norm residue symbol respectively;

$$1 = \left(\frac{\eta_j/\eta_{i+j}, \pi^j\eta_i/\eta_{i+j}}{\mathfrak{p}}\right)_p = \left(\frac{\eta_j,\pi^j\eta_i}{\mathfrak{p}}\right)_p \left(\frac{\eta_j,\eta_{i+j}}{\mathfrak{p}}\right)_p^{-1} \left(\frac{\eta_{i+j},\eta_i\pi^j}{\mathfrak{p}}\right)_p \left(\frac{\eta_{i+j},\eta_{i+j}}{\mathfrak{p}}\right)_p^{-1}.$$

And by v), vi) properties equation becomes;

$$\left(\frac{\eta_i,\eta_j}{\mathfrak{p}}\right)_p = \left(\frac{\eta_j/\eta_{i+j},\pi^j}{\mathfrak{p}}\right)_p^{-1} \left(\frac{\eta_i,\eta_{i+j}}{\mathfrak{p}}\right)_p \left(\frac{\eta_{i+j},\eta_j}{\mathfrak{p}}\right)_p.$$

Thus we are reduced to calculate $\left(\frac{\eta_{i+j}/\eta_j,\pi^j}{\mathfrak{p}}\right)_p^{-1}$;

$$\left(\frac{\eta_{i+j}/\eta_j,\pi^j}{\mathfrak{p}}\right)_p^{-1} = \left(\frac{\eta_{i+j},\pi^j}{\mathfrak{p}}\right)_p^{-j} \left(\frac{\eta_j,\pi^j}{\mathfrak{p}}\right)_p = \left(\frac{\eta_{i+j},\pi}{\mathfrak{p}}\right)_p^{-j}$$

since $\eta_j + \pi^j = 1$ and by v), proving a).

For b) we are reduced to show this for $\left(\frac{\eta_i,\eta_j}{\mathfrak{p}}\right)_p = 1$ if $i+j \geq p+1$. $\eta_i + \eta_j \in U_{p+1} \subset (K_{\mathfrak{p}}^*)^p$ hence by v) we have the equality.

The first part of c) is also evident, since

$$\left(\frac{\eta_i,\pi}{\mathfrak{p}}\right)_p^i = \left(\frac{\eta_i,\pi^i}{\mathfrak{p}}\right)_p = 1.$$

by v), hence $\left(\frac{\eta_i,\pi}{\mathfrak{p}}\right)_p$ should be i-th root of unity, we also know that it is a p-th root of unity and $i < p$ so it should be 1.

The second part of c) is rather non trivial, and is not a direct consequence of the properties of the norm residue symbol. We introduce $\mathfrak{p}$-primary numbers.

Definition 6.4.7 *An element $a \in K$ is called $\mathfrak{p}$ **-primary** for n if $\mathfrak{p}$ is unramified at $K(\sqrt[n]{a})/K$.*

Note that in our case $n = p$.

Lemma 6.4.8

$$\frac{\pi^{p-1}}{p} \equiv -1(mod\ p).$$

Proof:

$$p = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \prod_{i=1}^{p-1}(1-\zeta_p)(1+\zeta_p+\cdots+\zeta_p^{i-1}) = \pi^{p-1}\prod_{i=1}^{p-1}(1+\zeta_p+\cdots+\zeta_p^{i-1})$$

hence

$$\frac{\pi^{p-1}}{p} \equiv \prod_{i=1}^{p-1}(1+\zeta_p+\cdots+\zeta_p^{i-1})^{-1} \equiv ((p-1)!)^{-1} \equiv -1(\text{mod } \mathfrak{p})$$

since $\zeta_p \equiv 1(\text{mod } \mathfrak{p})$ and by Wilson theorem.

Proposition 6.4.9 *Let $a \in K$ satisfy that $a = 1 + c\pi^p$, then a is $\mathfrak{p}$-primary and*

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \zeta_p^{-Tr_{\mathfrak{p}/\mathbb{F}_p}(c)v_{\mathfrak{p}}(b)}.$$

where Tr denotes the trace from $\mathfrak{p}$ to the prime field $\mathbb{F}_p$

Let $\alpha^p = a = 1 + c\pi^p$ for some $c \in \mathfrak{o}_\mathfrak{p}$. One one hand;

$$\alpha^p \equiv (1+\pi x)^p \equiv 1 + p\pi x + \frac{p(p-1)}{2}\pi^2 x^2 + \cdots + x^p \pi^p \equiv \pi^p(x^p - x)(\text{mod } \pi^{p+1}),$$

on the other hand

$$\alpha^p \equiv a \equiv 1 + c\pi^p(\text{mod } \pi^{p+1})$$

hence we get $x^p - x - c \equiv 0(\text{mod } \mathfrak{p})$. If $f(X) \in \mathfrak{o}_\mathfrak{p}[X]$ is the minimal polynomial for x, then $f(X) \equiv X^p - X - 1(\text{mod } \mathfrak{p})$. Since $f'(X) \equiv 1 \neq 0(\text{mod } \mathfrak{p})$, so $K_\mathfrak{p}(x) = K_\mathfrak{p}(\alpha)$ is indeed unramified, proving α is $\mathfrak{p}$-primary. Now $x^p \equiv x + c(\text{mod } \mathfrak{p})$, so if $N\mathfrak{p} = p^f$ and σ is the Frobenius automorphism associated to the unramified extension $K(\sqrt[n]{\alpha})/K$, then

$$\sigma(x) = x^{N\mathfrak{p}} \equiv x^{p^f} \equiv (x+c)^{p^{f-1}} \equiv x^{p^{f-1}} + c^{p^{f-1}} \equiv (x+c)^{p^{f-2}} + c^{p^{f-1}} \equiv x^{p^{f-2}} + c^{p^{f-2}} + c^{p^{f-1}} \equiv$$

$$\equiv \cdots \equiv x + c + c^p + \cdots + c^{p^{f-1}} \equiv x + Tr_{\mathfrak{p}/\mathbb{F}_p}(c)(\text{mod } \mathfrak{p}),$$

on the other hand, $\zeta_p\alpha = \zeta_p(1+\pi x) = \zeta_p + \zeta_p\pi x = 1 + (\zeta_p - 1) + \zeta_p\pi x = 1 - \pi + \zeta_p\pi x \equiv 1 = 1 + \pi x_1$, since $x_1 \equiv \zeta_p x - 1 \equiv x - 1(\text{mod } \mathfrak{p})$ then we have inductively that if $\zeta_p^k\alpha = 1 + \pi x_k$ then $x_k \equiv x - k(\text{mod } \mathfrak{p})$. On the other hand Frobenius automorphism σ determines the value of the symbol;

$$\sigma(\alpha) \equiv \zeta_p^l\alpha(\text{mod } \mathfrak{p}),$$

where $\zeta_p^l = \left(\frac{a,\pi}{\mathfrak{p}}\right)$ since $\sigma(x) = x + Tr_{\mathfrak{p}/\mathbb{F}_p}(c)$, then $k = -Tr_{\mathfrak{p}/\mathbb{F}_p}(c)$. We have $\left(\frac{a,\pi}{\mathfrak{p}}\right) = -Tr_{\mathfrak{p}/\mathbb{F}_p}(c)$, set $b = \pi^{v_p(b)}u_b$ with u_b is unit, hence we get by multiplicative property in the second coordinate that

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \zeta_p^{-Tr_{\mathfrak{p}/\mathbb{F}_p}(c)v_\mathfrak{p}(b)}$$

and hence the proposition.

Proof: {remaining part of c)} The proof of the remaining part of c) follows from the lemma when one takes $b = \pi$.

6.5 Applications

6.5.1 Cubic Reciprocity Law

We now specialize to $p = 3$. Let ζ_3 be 3rd roof of unity, first we determine the ring of integers R of $\mathbb{Q}(\zeta_3)$.

Lemma 6.5.1 $R = \mathbb{Z}(\zeta_3) = \mathbb{Z} + \zeta_3\mathbb{Z}$.

Proof: Let $a + b\zeta_3 \in R$ with $a, b \in \mathbb{Q}$, then we have $N(a + b\zeta_3) = (a + b\zeta_3)(a + b\zeta_3^2) = a^2 + b^2 - ab$ is in $\mathbb{Z}$ and $Tr(a + b\zeta_3) = (a + b\zeta_3) + (a - b\zeta_3) = 2a - b$ in $\mathbb{Z}$. $a^2 + b^2 - ab \in \mathbb{Z} \Rightarrow 4a^2 + 4b^2 - 4ab \in \mathbb{Z} \Leftrightarrow (2a - b)^2 + 3b^2 \in \mathbb{Z} \Leftrightarrow 3b^2 \in \mathbb{Z}$, since $b \in \mathbb{Q}$, this evidently implies $b \in \mathbb{Z}$ and hence $a \in \mathbb{Z}$ proving the lemma.

We next investigate how the integers are decomposed into product of powers of $\pi = 1 - \zeta_3$, $\eta_i = 1 - \pi^i$'s and certain units.

Proposition 6.5.2 *Any element $a \in R = \mathbb{Z}[\zeta_3]$ is of the form $\zeta_3^{a_1}\pi^{a_2}a_3$ where $a_3 = (-1)^i(1 + 3(m + n\zeta_3))$ with i, m, n are integers.*

Proof: Let $A + B\zeta_3 \in R$, $A, B \in \mathbb{Z}$. Write $A + \zeta_3 B = 3^k(A_1 + \zeta_3 B_1)$ where 3^k is the maximal power of 3 dividing both A and B. $3 = -\zeta_3^2(1 - \zeta_3)^2$. Hence we are reduced to show this for $A_1 + \zeta_3 B_1$ with at least one non divisible to 3, now if $A_1 \neq 0(\text{mod } 3)$ and $B_1 \equiv 0(\text{mod } 3)$ then $A_1 + \zeta_3 B_1$ of the form above. If, conversely $B_1 \neq 0(\text{mod } 3)$ and $A_1 \equiv 0(\text{mod } 3)$, writing $A_1 + \zeta_3 B_1 = \zeta_3^2(\zeta_3 A_1 + \zeta_3^2 B_1) = \zeta_3^2(-B_1 + \zeta_3(A_1 - B_1))$ and by previous result this is also in the desired form. Now assume both A_1 and B_1 are not divisible by 3, if $A_1 \equiv B_1(\text{mod } 3)$, by previous assertion we have $A_1 + \zeta_3 B_1 = \zeta_3^2(-B_1 + \zeta_3(A_1 - B_1))$ reducing to the previous case. If now $A_1 \neq B_1(\text{mod } 3)$ we have that $A_1 + \zeta_3 B_1 = (1 - \zeta_3)(\frac{a+b}{3} + \frac{2a-b}{3}\zeta_3)$, applying this step for finitely many will reduce to the previous cases, hence the proposition.

Theorem 6.5.3 (Cubic Reciprocity Law) *Let $a, b \in R$ with a and b are relatively prime and both are of the form $\pm(1 + 3(M + \zeta_3 N))$ i.e. $\equiv \pm 1(mod\ 3R)$. Then*

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right),$$

with supplementary laws;

$$\left(\frac{\zeta_3}{a}\right) = \zeta_3^{-m-n},\ \left(\frac{\pi}{a}\right) = \zeta_3^{m},$$

where $a = \pm(1 + 3(m + \zeta_3 m))$.

Proof: By main theorem of explicit reciprocity we have $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1}$ is equal to $\left(\frac{a,b}{\mathfrak{p}}\right)$ where $\mathfrak{p}$ is generated by $1-\zeta_3$. $a, b \equiv \pm 1(\mathrm{mod}\ 3R)$ hence both are 3-primary integers. Then by lemma above we have $\left(\frac{a,b}{\mathfrak{p}}\right) = \zeta_3^{Tr_{\mathfrak{p}/\mathbb{F}_3} v_{\mathfrak{p}}(b)} = 1$ since $v_{\mathfrak{p}}(b) = 0$, and hence the rule. For supplementary laws, first one is followed by iv) property of the power residue symbol hence $\left(\frac{\zeta_3}{a}\right) = \zeta_3^{\frac{N(a)-1}{3}} = \zeta_3^{\frac{(3m+1)^2+(3n)^2-(3m+1)3n}{3}} \equiv \zeta_3^{-m-n}$, and the second one is followed by the formula for 3-primary numbers taking $b = \pi = 1 - \zeta_3$ so $v_{\mathfrak{p}}(\pi) = 1$, and $Tr_{\mathfrak{p}/\mathbb{F}_3}(a) \equiv -2m \equiv m(\mathrm{mod}\ 3)$, thus $\left(\frac{\pi,a}{\mathfrak{p}}\right) = \left(\frac{a,\pi}{\mathfrak{p}}\right)^{-1} = \zeta_3^{Tr_{\mathfrak{p}/\mathbb{F}_3}(a) v_{\mathfrak{p}}(\pi)} = \zeta_3^{m}$.

6.5.2 Eisenstein Reciprocity Law

We now prove the Eisenstein reciprocity law;

Theorem 6.5.4 (Eisenstein Reciprocity Law) *Let p be an odd prime, ζ_p is primitive p-th root of unity, $K = \mathbb{Q}(\zeta_p)$ and R be the ring of integers of K. Let $\mathfrak{p} = (1 - \zeta_p)$ the prime ideal of $\mathbb{Q}(\zeta_p)$. Let $\alpha, a \in R$ relatively prime elements which are not divisible by $\mathfrak{p}$ such that a is integer and $\alpha \equiv b(mod\ (1-\zeta_p)^2)$. Then K has the reciprocity equation;*

$$\left(\frac{a}{\alpha}\right) = \left(\frac{\alpha}{a}\right).$$

Proof: a is integer, and relatively prime to p hence $a^{p-1} \equiv 1(\bmod p)$ hence $a^{p-1} = 1 + pa_1$, hence one may write it of the form $a^{p-1} = \eta_p u_p$ where $\eta_{p-1} = 1 - pi^{p-1}$ and $u_p \in U_p$. On the other hand, since $\alpha \equiv b(\bmod \pi^2)$ then $\alpha^{p-1} \equiv 1(\bmod \pi^2)$, hence we may write $\alpha = \eta_2 \eta_3^{c_3} \cdots \eta_{p-1}^{c_{p-1}} u'_p$ where $\eta_i = 1 - \pi^i$ and c_i are non negative integers. By the main theorem we have that

$$\left(\frac{a}{\alpha}\right)\left(\frac{\alpha}{a}\right)^{-1} = \left(\frac{a, \alpha}{\mathfrak{p}}\right).$$

by 6.4.6,

$$\left(\frac{a^{p-1}, \alpha^{p-1}}{\mathfrak{p}}\right) = \left(\frac{\eta_p u_p, \eta_2 \eta_3^{c_3} \cdots \eta_{p-1}^{c_{p-1}} u'_p}{\mathfrak{p}}\right) = \left(\frac{\eta_p, \eta_2}{\mathfrak{p}}\right)\left(\frac{\eta_p, \eta_3}{\mathfrak{p}}\right)^{c_3} \cdots \left(\frac{u_p, u'_p}{\mathfrak{p}}\right) = 1$$

On the other hand

$$\left(\frac{a^{p-1}, \alpha^{p-1}}{\mathfrak{p}}\right) = \left(\frac{a, \alpha}{\mathfrak{p}}\right)^{(p-1)^2},$$

, $\left(\frac{a,\alpha}{\mathfrak{p}}\right)$ is $(p-1)^2$-th root of unity and also p-th root of unity hence $\left(\frac{a,\alpha}{\mathfrak{p}}\right) = 1$.

Chapter 7

Explicit Reciprocity Laws

We begin with the explanation of the explicit reciprocity law of Shafarevich.

7.1 Explicit Reciprocity Law of Shafarevich

7.1.1 Introduction

Prime ideals in theory of algebraic numbers play the same part as points on the Riemann surface, etc. The problem arose of a systematic carrying over of results from the theory of algebraic functions which have been proved analytically, into the theory of algebraic numbers.

Hilbert pointed out that the formula $\prod_{\mathfrak{p}} \left(\frac{a,b}{\mathfrak{p}}\right) = 1$ plays the same role in the theory of algebraic numbers as does Cauchy's integral formula in the theory of abelian integrals. Further developments in theory abelian integrals as well as the theory of algebraic numbers show that the relation is more precisely the corollary of the integral formula namely that integral of the abelian differential $\alpha d\beta$ in all points of the Riemann surface is 0. From this point of view $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ is analogous to $\alpha d\beta$ at point $\mathfrak{p}$.

In spite of the fact that the norm residue symbol plays the part of a residue, its definition has nothing in common with the definition of the abelian differential.

Shafarevich gave a construction of the symbol $\left(\frac{a,b}{\mathfrak{p}}\right)_n$, which is exactly the analogous to the definition of the residue of an abelian differential.

In doing this he shows that the expansion of an algebraic function in a series in a neighborhood correspond to the decomposition of an algebraic number into a certain product (i.e. similar to that of the last chapter). One may apply to the product into which α and β decompose the same the same operations which are applied to to the series expansions of functions in calculating the residue, we get the value of the symbol. All the fundamental properties of abelian differentials are carried to the field of algebraic numbers.

By main theorem proved in previous chapter, explicit reciprocity law reduces the problem of calculating $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ at primes $\mathfrak{p}|n$. Shafarevich achieved to calculate this symbol explicitly by using the analogy between algebraic function fields to algebraic number fields.

We now describe the work of Shafarevich. We first fix some notations. Let K be a number field, i.e. finite Galois extension of $\mathbb{Q}$. We are interested in the value of the symbol at prime $\mathfrak{p} \subset K$ such that $\mathfrak{p}|n$. Let p be a prime integer below $\mathfrak{p}$ and degree of p at n be n_p i.e. $p^{n_p}|\,|n$, we always assume that ζ_n is in K, hence in particular we have $\zeta_{p^{n_p}}$ is in K. $K_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of K, π be a uniformizer of $\mathfrak{p}$, $v_\mathfrak{p}$ denote the valuation, $\mathcal{O}_\mathfrak{p}$ denote the ring of integers of $K_\mathfrak{p}$, p be the characteristic of the residue field $K/\mathfrak{p}$, Σ denote set of representatives of the residue field, then any $\alpha \in K_\mathfrak{p}$ is uniquely represented as $\alpha = \sum_{i>>-\infty}^{\infty} a_i\pi^i$ for $a_i \in \Sigma$. U denote the units and U_1 denote the units with $u \equiv 1(\text{mod } \mathfrak{p})$ which is also called the **principal units**.

$$p = u\pi^e$$

if $e = 1$ then we call $K_\mathfrak{p}$ is unramified. $K_\mathfrak{p}/\mathbb{Q}_p$ is finite Galois extension, hence there exist a maximal field T with $T/\mathbb{Q}_p$ is maximal unramified subfield of $K_\mathfrak{p}/\mathbb{Q}_p$. T is called the **inertia field** of $K_\mathfrak{p}$. The degree of $K_\mathfrak{p}/T = e$ and every number in T is of the form $\sum_{i>>-\infty}^{\infty} a_ip^i$ with $a_i \in \Sigma$. Let $\bar{T}$ be discrete unramified field with a valuation which is obtained from T by the algebraic closure of the residue class field. $\mathfrak{R}$, $\bar{\mathfrak{R}}$ denote the systems of representatives of $T/(p)$ and $\bar{T}/(p)$ and $\mathcal{O}_T$, $\mathcal{O}_{\bar{T}}$ denote the ring of integers of T and $\bar{T}$ respectively. Let F denote the Frobenious automorphism of $T/\mathbb{Q}_p$, define the map $\wp : \mathcal{O}_T \to \mathcal{O}_T$ given by $\wp(\alpha) = F(\alpha) - \alpha$, is an endomorphism of $\mathcal{O}_T^+$ onto $\mathcal{O}_T^+$ where $\mathcal{O}_T^+$ denotes the ring of integers which are not units of $\mathcal{O}_{\bar{T}}$. A number ω in $K_\mathfrak{p}^*$ is called p^{n_p}-primary if $K(\sqrt[p^{n_p}]{\omega})/K$ is unramified at $\mathfrak{p}$. Denote the set of p^{n_p}-primary numbers in K^* by Ω.

7.1.2 Shafarevich and Artin-Hasse Maps

In the ring of formal power series in x with coefficients in T we consider the series

$$L(\alpha, x) = \alpha x + p^{-1}\alpha^p x^p + p^{-2}\alpha^{p^2} x^{p^2} + \cdots$$

where $\alpha \in \mathcal{O}_T$. Obviously the series satisfy $L(\alpha_1 + \alpha_2, x) = L(\alpha_1, x) + L(\alpha_2, x)$ and $L(a\alpha_1, x) = aL(\alpha_1, x)$ for p-adic integer a. From this it follows that the series, which is also known as Shafarevich function,

$$E(\alpha, x) = e^{L(\alpha,x)}$$

has the properties $E(\alpha_1 + \alpha_2, x) = E(\alpha_1, x)E(\alpha_2, x)$ and $E(a\alpha, x) = E(\alpha, x)^a$. In case $\alpha \in \Sigma$ we have the following identity:

$$E(\alpha, x) = \prod (1 - \alpha^m x^m)^{-\frac{\mu(m)}{m}}$$

where $\mu(n)$ is the Möbius μ function i.e. $\mu(1) = 1$, $\mu(p_1 p_2 \cdots p_l) = (-1)^l$ for prime p_i's and $\mu(n) = 0$ if n is not square free integer. This identity shows that for $\alpha \in \Sigma$, $E(\alpha, x)$ has integral p-adic coefficients. In the view of above relations for $E(\alpha, x)$ this is true for any $\alpha \in T$. From this it follows that $E(\alpha, x)$ converges if we substitute for x any number of $K_\mathfrak{p}$ which is divisible by π. Moreover we have that

$$E(\alpha, x) \equiv 1 + \alpha x (\text{mod } x^2).$$

The function $E(1, \xi)$ has p-adic integral coefficients and the equation

$$1 + \eta = E(1, \xi)$$

is solvable in the power series of η with p-adic coefficients. Moreover,

$$\xi \equiv \eta (\text{mod } \eta^2).$$

Applying this to the case $\eta = \zeta_{p^{n_p}} - 1$ we see that for $\xi = Q(\zeta_{p^{n_p}} - 1)$ where $Q(\eta)$ is the p-adic representation, we will have

$$E(1, \xi) = \zeta_{p^{n_p}},$$

$$\xi = \zeta_{p^{n_p}} - 1 (\text{mod } (\zeta_{p^{n_p}} - 1)^2).$$

For every integer α of T, there exist an integer A in $\bar{T}$ such that

$$\wp(A) = \alpha,$$

We introduce the notation, also known as Artin - Hasse function,

$$E(p^{n_p} A, \xi) = E(\alpha).$$

This notation meaningful because it can be easily seen that different A's satisfying $\wp(A) = \alpha$ give the same $E(p^{n_p} A, \xi)$. It can be proved that $E(\alpha)$ is p^{n_p}-primary. It is clear that $E(\alpha)$ satisfies $E(\alpha + \beta) = E(\alpha)E(\beta)$ and $E(a\alpha) = E(\alpha)^a$ where a is p-adic integer. It can also be proved that every p^{n_p}-primary number ω is representable in the form

$$\omega = E(\alpha)\lambda^{p^{n_p}},$$

where α is an integer of $K_{\mathfrak{p}}$ and λ is any number in $K_{\mathfrak{p}}$.

7.1.3 Canonical Decomposition

Hensel found a very broad conditions for a system of units to be the system of generators the principal units group. We will give the formulation of the theorem and leaving the proof to Hensel's paper. Before that we note that $T(\zeta_{p^{n_p}})/T = (p-1)p^{n_p - 1}$, hence $p - 1 | e$ and we set $e_1 = e/(p-1)$.

Theorem 7.1.1 *Let us select for every i such that $i \neq 0 (mod\, p)$ for $1 \leq i < pe_1$ as well as for $i = pe_1$, and for every $\alpha \in \Sigma$ a principal unit $\epsilon_i(\alpha) \in U_1$,* *satisfying the condition $\epsilon_i(\alpha) \equiv 1 + \alpha\pi^i (mod\, \mathfrak{p}^{i+1})$. Then every principal unit ϵ can be represented in the form $\epsilon = \prod_{i,r} \epsilon_i(\alpha_{i,r})^{p^r}$, where the product extends over all i mentioned above and over all non negative integer r.*

Proof: Refer to [11]

Theorem 7.1.2 (Theorem on canonical decomposition) *Every principal unit $\epsilon \in U_1$ can be represented in the form $\epsilon = E(\alpha) \prod E(\alpha_i, \pi^i)$, where α and α_i are integer in $K_\mathfrak{p}$ and i goes over all the values between 1 to pe_1, which are not divisible by p. Moreover, this decomposition is unique in the sense if $E(\alpha) \prod E(\alpha_i, \pi^i) = E(\beta) \prod E(\beta_i, \pi^i)$ then $\alpha \equiv \beta + \wp(\eta) (mod\, p^{n_p})$ and $\alpha_i \equiv \beta_i (mod\, p^{n_p})$ for some $\eta \in \Sigma$.*

Proof: Refer to [22]

In what follows we shall be interested only in equalities up to a multiplier which is p^{n_p} power. We express by $\lambda \approx \mu$ if $\lambda = \mu\mu_1^{p^{n_p}}$ for $\mu_1 \in K_\mathfrak{p}$. To every ϵ in its canonical decomposition corresponds the first factor $E(\alpha)$ determined up to a $p^{p^{n_p}}$ power. We introduce

$$\delta(\epsilon) \approx E(\alpha).$$

It is clear that $\delta(\epsilon_1\epsilon_2) \approx \delta(\epsilon_1)\delta(\epsilon_2)$ and $\delta(\epsilon^{p^{n_p}}) \approx 1$. Therefore the mapping $\epsilon \to \delta(\epsilon)$ is a homomorphism of the group on the group $U_1/(U_1)^{p^{n_p}}$ on the group $\Omega/\Omega \cap (U_1)^{p^{n_p}}$. Note that $E(\alpha)$ does not only depend on ϵ but also on the choice of π. $K_\mathfrak{p}/\mathbb{Q}_p$ is a finite Galois extension. Let Tr denote the trace in $K_\mathfrak{p}/\mathbb{Q}_p$, then the mapping $\chi E(\alpha) = \zeta_{p^{n_p}}^{Tr(\alpha)}$ is an isomorphism of the group $\Omega/\Omega \cap (U_1)^{p^{n_p}}$ and the cyclic group generated by $\zeta_{p^{n_p}}$. This map is multiplicative since trace is additive, and $E(\alpha)$ is multiplicative. Since

$$Tr(\alpha^p - \alpha) = Tr(\alpha^p) - Tr(\alpha) = 0.$$

χ maps $\Omega/\Omega \cap (U_1)^{p^{n_p}}$ into units. The group $\Omega/\Omega \cap (U_1)^{p^{n_p}}$ is the center of the homomorphism since $Tr(\alpha) \equiv 0 (\text{mod}\ p^{n_p})$ and $\alpha \equiv \wp(\beta) (\text{mod}\ p^{n_p})$ (Refer to [27]). Since finite fields are seperable, χ gives a mapping over the whole group.

The expression of a p^{n_p}primary number ω in the form $E(\alpha)$ depends on the choice of $\zeta_p^{n_p}$, but Hasse [10] has shown that

$$\chi\omega = \zeta_{p^{n_p}}^{Tr(\alpha)}$$

does not depend on the choice of $\zeta_p^{n_p}$.

7.1.4 The Symbol (λ, μ)

Every number $\lambda \in K_{\mathfrak{p}}$ is of the form

$$\lambda = \pi^a w\epsilon$$

where a is an integer, $w \in \Sigma$ and ϵ is a principal unit. We are interested in equalities up to a multiple of a p^{n_p}-th power and we may disregard w since it is a p^{n_p}-th power, and will consider a in mod p^{n_p}. Then we have

$$\lambda \approx \pi^a E(\alpha) \prod E(\alpha_i, \pi^i).$$

Let μ be another number of $K_{\mathfrak{p}}$ represented in the same form

$$\mu \approx \pi^b E(\beta) \prod E(\beta_j, \pi^j).$$

We introduce the function

$$(\lambda, \mu) \approx E(a\beta - b\alpha + \gamma),$$

where $E(\gamma) \approx \delta(\prod_{i,j} E(i\alpha_i\beta_j, \pi^{i+j}))$.

The main work of Shafarevich was to prove that the norm residue symbol $\left(\frac{\lambda,\mu}{\mathfrak{p}}\right)$ coincide with the symbol $\chi(\lambda, \mu)$;

Theorem 7.1.3 *$\lambda, \mu \in K_{\mathfrak{p}}$, then*

$$\left(\frac{\lambda, \mu}{\mathfrak{p}}\right) = \chi(\lambda, \mu).$$

The proof of the theorem is based on the fact that the values of $\chi(\lambda,\mu)$ concide with $\left(\frac{\lambda,\mu}{\mathfrak{p}}\right)$ for the three cases $(\lambda,\mu) = (\pi, E(\alpha)), (\pi,\epsilon), (\epsilon_1,\epsilon_2)$ on the following four properties of the symbol (λ,μ)(which are similar to that of $\left(\frac{\lambda,\mu}{\mathfrak{p}}\right)$);

Theorem 7.1.4 I. Bilinearity: $(\lambda_1\lambda_2,\mu) \approx (\lambda_1,\mu)(\lambda_2,\mu)$ *and* $(\lambda,\mu_1\mu_2) \approx (\lambda,\mu_1)(\lambda,\mu_2)$.

II. Anti-symmetry: $(\lambda,\mu) \approx (\mu,\lambda)^{-1}$.

III. Separability: *If in the residue field not every element is of the form* $x^p - x$, *then*

$$(\lambda,\mu) \approx 1,\ \forall\mu \Rightarrow \lambda \approx 1.$$

$$(\lambda,\mu) \approx 1,\ \forall\lambda \Rightarrow \mu \approx 1.$$

Invariability (λ,μ) *is independent of the choice of* π.

that uniquely determines the value of the symbol.

We comment that proofs are based on carefully following of certain calculations, and leave the proofs to the paper of Shafarevich [22]. We continue with the formulation of explicit reciprocity of Shafarevich. We keep the notation above;

Theorem 7.1.5 *1.* $\chi(\pi, E(\alpha,\pi^i)) = 1$ *for* $p \not| i$, $\alpha \in \mathcal{O}_T$.

2. $\chi(\pi, E(\alpha)) = \zeta_{p^{n_p}}^{Tr(\alpha)}$ *if* $\alpha \in \mathcal{O}_T$.

3. $\chi(\pi,\pi) = \chi(\pi,-1)$.

4. $\chi(E(\alpha),\epsilon) = 1$ *for* $\alpha \in \mathcal{O}_T$ *and* $\epsilon \in U$.

5. If $p \neq 2$, *then* $\chi(E(\alpha,\pi^i), E(\beta,\pi^j)) = \chi(\pi^j, E(\alpha\beta,\pi^{i+j}))$, *If* $p = 2$ *then* $\chi(E(\alpha,\pi^i), E(\beta,\pi^j)) = \chi(-\pi^j, E(\alpha\beta,\pi^{i+j}))\prod_{s=1}^{\infty}\chi(-1, E(\alpha F^s(\beta),\pi^{i+jp^s}))$ $\prod_{r=1}^{\infty}\chi(-1, E(\alpha F^r(\beta),\pi^{ip^r+j}))$ *for* $\alpha,\beta \in \mathcal{O}_T$ *and* $p \not| i$, $p \not| j$.

6. If $p = 2$, *then* $\chi(-1, E(\alpha,\pi^i)) = \prod_{s=0}^{\infty}\chi(\pi, E(i2^sF^{s+1}(\alpha),\pi^{i2^{s+1}}))$ *for* $\alpha \in \mathcal{O}_T$ *and* $p \not| i$.

7.2 Explicit Reciprocity Laws of Brückner and Vostokov

The reciprocity law of Shafarevich is not as explicit as one would like since if one wants to compute the symbol (λ, μ) one has to write λ and μ of the form $\lambda \approx \pi^a E(\alpha) \prod E(\alpha_i, \pi^i)$ and $\mu \approx \pi^b E(\beta) \prod E(\beta_j, \pi^j)$, and then one has to write $E(\alpha_i \beta_j, \pi^{i+j})$ in such form if $p|(i+j)$. A more explicit general reciprocity law was found by Brückner (1967) and Vostokov (1978).

We follow from Vostokov. We start by the simpler case, we assume that $p > 2$ is odd prime. $p = 2$ case will be treated afterwards. Let $\mathcal{O}_T$ denote the ring of integers of T, $\mathfrak{R}$ system of representatives of the residue field of $K_{\mathfrak{p}}$ in $\mathcal{O}_T$. Suppose that $\zeta_{p^{n_p}}$ expanded into power series in π with coefficients in $\mathcal{O}_T$, that is $\zeta_{p^{n_p}} = 1 + c_1\pi + c_2\pi^2 + \cdots$ we then denote by $z(X)$ and $z_0(X)$ the following series; $z_0(X) = c_1X + c_2X^2 + \cdots$ and $z(X) = 1 + c_1X + c_2X^2 + \cdots$. By a formal series $\varphi(X)$ we shall understand a series of the form

$$\varphi(X) = \sum_{i=-\infty}^{\infty} d_i X^i, \ d_i \in \mathcal{O}_T$$

where $d_i \to 0$ if $i \to -\infty$. Such series, which we denote by $\mathcal{O}_T\{\{X\}\}$ forms a ring containing the formal power series $\mathcal{O}_T[[X]] = \{\sum_{i>>-\infty}^{\infty} d_i X^i, \ d_i \in \mathcal{O}_T\}$ as a sub ring. It is easy to verify that any $\varphi \in \mathcal{O}_T\{\{X\}\}$ is invertible if and only if at least one of its coefficients. We denote the inverse φ by φ^{-1}, if d_m the least coefficient of φ which is invertible, if $\varphi = d_m X^m(1 + \psi(X))$ then

$$\varphi^{-1} = (d_m X^m)^{-1}(1 - \psi + \psi^2 - \psi^3 + \cdots).$$

We define the action of the Frobenius automorphism F on the formal series $\varphi(X) = \sum_i a_i X^i$ as follows:

$$F(\varphi) = \sum_i F(a_i) X^{pi}.$$

7.2.1 The Functions l and E

We now introduce a kind of logarithm l and a kind of exponent E on formal power series both of which are analogous to that of on elements of $K_{\mathfrak{p}}$. Let $\mathcal{O}_T^0[[X]]$ denote the formal series of the form $\varphi = a_1X + a_2X^2 + \cdots$, $a_i \in \mathcal{O}_T$. Let $\epsilon(X) \in 1 + \mathcal{O}_T^0[[X]]$, we define the function $l(\epsilon)$ as follows;

$$l(\epsilon) = \left(1 - \frac{F}{p}\right) \log(\epsilon(X)).$$

where $\log(\varphi) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}\varphi^i}{i}$.

Lemma 7.2.1 *$l(\epsilon) \in \mathcal{O}_T^0[[X]]$, and $l(\epsilon\nu) = l(\epsilon) + l(\nu)$.*

Proof: Refer to [24].

Let us now define the inverse mapping from $\mathcal{O}_T^0[[X]] + 1$ to $\mathcal{O}_T^0[[X]]$. To do so we consider the Shafarevich function:

$$E(X) = \exp\left(\sum_{i=0}^{\infty} \frac{X^{p^i}}{p^i}\right).$$

By Möbius inversion formula we have

$$E(X) = \prod_{(m,p)=1} (1 - X^m)^{-\frac{\mu(m)}{m}}.$$

We connect E with the Frobenius automorphism F and define it for any series $\varphi \in \mathcal{O}_T^0[[X]]$ as follows;

$$E(\varphi) := \exp\left(\sum_{i=0}^{\infty} \frac{\varphi^{F^i}}{p^i}\right) = \exp\left(\left(1 + \frac{F}{p} + \frac{F^2}{p^2} + \cdots\right)(\varphi)\right).$$

Lemma 7.2.2 *$E(\varphi) \in 1 + \mathcal{O}_T^0[[X]]$, $E(\varphi + \psi) = E(\varphi)E(\psi)$. Moreover $E(\varphi)$ and $l(\epsilon)$ are inverse mappings i.e. $E(l(\epsilon)) = \epsilon(X)$ and $l(E(\varphi)) = \varphi(X)$.*

Proof: Refer to [24]

7.2.2 The Pairing $[A, B]$

In this section we define a symbol on formal power series. We consider the multiplicative group G of the formal power series

$$G = \{X^m \theta \epsilon(X); m \in \mathbb{Z}, \theta \in \mathfrak{R}, \epsilon(X) \in 1 + \mathcal{O}_T^0[[X]]\}$$

Let $A(X), B(X) \in G$ with $A = X^a \theta \epsilon(X)$ and $B = X^b \theta' \nu(X)$, we introduce the pairing in G with values in $\mathcal{O}_T$ as follows;

$$[A, B] = res_X \left(\Phi(X) W(X)\right),$$

where

$$\Phi(X) = l(\epsilon)\frac{dl(\mu)}{dX} - l(\epsilon)B^{-1}\frac{dB}{dX} + l(\mu)A^{-1}\frac{dA}{dX},$$

and $W(X)$ is formal series with coefficients in $\mathcal{O}_T$ having, in general, terms of negative powers such that

$$\frac{d}{dX}W(X) \equiv 0(\text{mod } p^{n_p}).$$

We are going to choose the function in most explicit and simple form in a while W, but before that we highlight some properties of the pairing $[A, B]$ which are similar to that of Shafarevich.

Theorem 7.2.3 *The pairing $[A, B]$ satisfies;*

Bilinearity: $[A_1 A_2, B] = [A_1, B] + [A_2, B]$ *and* $[A, B_1 B_2] = [A, B_1] + [A, B_2]$.

Skew-Symmetry: $[A, B] + [B, A] \equiv 0(mod\ p^{n_p})$.

Invariance: *The value of $[A, B]$ in mod p^{n_p} is independent of the choice of the function X.*

Proof: Refer to [24]

7.2.3 The Pairing $< \alpha, \beta >_\pi$

With the help of pairing $[A, B]$ we shall construct a pairing in $K_{\mathfrak{p}}^*$ with values in the group of p^{n_p}-th roots of unity. Let $\alpha = \pi^a \theta \epsilon$ and $\beta = \pi^b \theta' \eta$ elements of $K_{\mathfrak{p}}$, where $\theta, \theta' \in \mathfrak{R}$, and ϵ, η are principal units. Let $\epsilon = 1 + a_1 \pi + a_2 \pi^2 + \cdots$ be an expansion of ϵ into a series in π with $a_i \in \mathcal{O}_T$. We denote by $A(X)$ the series $X^a \theta \epsilon(X)$ where $\epsilon(X) = 1 + a_1 X + a_2 x^2 + \cdots$. The series $B(X)$ and $\eta(X)$ are defined similarly for β. Let $z(X)$ be the series obtained from the expansion of $\zeta_{p^{n_p}}$ into a power series π. Consider the following pairing;

$$< \alpha, \beta >_\pi = \zeta_{p^{n_p}}^{Tr[A,B]},$$

where $1/2 + \left(z^{p^{n_p}} - 1\right)^{-1}$ is taken for $W(X)$. By $\left(z^{p^{n_p}} - 1\right)^{-1}$ we mean the following Laurent series;

$$\left(z^{p^{n_p}} - 1\right)^{-1} = z_0^{-p^{n_p}} \left(1 + \sum_{i=0}^{p^{n_p}-1} C_{p^n}^i z_0^{-i}\right).$$

This pairing, too, satisfies similar properties that of $[A, B]$ and that of Shafarevich;

Theorem 7.2.4 $< \alpha, \beta >_\pi$ *is bilinear, skew symmetric and invariant under the choice of* π.

The first two properties are evident from that of $[A, B]$, but the last one is not direct and is a consequence of carefully followed calculations. We refer to Vos for the proofs. One of the most profound achievement of Vostokov's paper was to show that the value of the norm residue symbol $\left(\frac{\pi, \epsilon}{\mathfrak{p}}\right)_n$ is equal to the value of the symbol $< \alpha, \beta >_\pi$;

Theorem 7.2.5 *Let* $\epsilon = 1 + a_1 \pi + a_2 \pi^2 + \cdots$ *be a principal unit of* $K_{\mathfrak{p}}$, *then*

$$\left(\frac{\pi, \epsilon}{\mathfrak{p}}\right) = \zeta_{p^{n_p}}^{Tr(\gamma)},$$

where $\gamma = res_X \left(X^{-1} l(\epsilon) \left(z^{p^{n_p}} - 1\right)^{-1}\right)$.

Proof: Refer to [24].

This theorem states that

$$< \pi, \epsilon >_{\pi} = \left(\frac{\pi, \epsilon}{\mathfrak{p}} \right).$$

Let η also be a principal unit; then

$$< \epsilon, \eta >_{\pi} = < \pi\epsilon, \eta >_{\pi} < \pi, \eta >_{\pi}^{-1} = < \pi\epsilon, \eta >_{\pi\epsilon} < \pi, \eta >_{\pi}^{-1} = \left(\frac{\pi\epsilon, \eta}{\mathfrak{p}} \right) \left(\frac{\pi, \eta}{\mathfrak{p}} \right)^{-1} = \left(\frac{\epsilon, \eta}{\mathfrak{p}} \right).$$

And similarly, in general case for $\alpha = \pi^a \theta \epsilon$ and $\beta = \pi^b \theta' \eta$ we have

$$< \alpha, \beta >_{\pi} = < \pi, \eta >_{\pi}^{a} < \pi, \epsilon >_{\pi}^{-b} < \epsilon, \eta >_{\pi} = \left(\frac{\pi, \eta}{\mathfrak{p}} \right)^{a} \left(\frac{\pi, \epsilon}{\mathfrak{p}} \right)^{-b} \left(\frac{\epsilon, \eta}{\mathfrak{p}} \right) = \left(\frac{\alpha, \beta}{\mathfrak{p}} \right).$$

Hence, we have that $< \alpha, \beta >_{\pi} = \left(\frac{\alpha, \beta}{\mathfrak{p}} \right)$ everywhere, hence we have the theorem for explicit reciprocity law as follows;

Theorem 7.2.6 *Let $\alpha, \beta \in K_{\mathfrak{p}}$, $\alpha = \pi^a \theta \epsilon$, $\beta = \pi^b \theta' \eta$ with $\theta, \theta' \in \mathfrak{R}$, ϵ, η are principal units, write $\epsilon = 1 + a_1 \pi + a_2 \pi^2 + \cdots$ as expansion of ϵ into series in prime element π and coefficients in $\mathcal{O}_T$. Denote by $A(X)$ the series $X^a \theta \epsilon(X)$ where $\epsilon(X) = 1 + a_1 X + a_2 X^2 + \cdots$ and by $l(\epsilon)$ the function $\left(1 - \frac{F}{p}\right) \log(\epsilon(X))$. The series $B(X)$ and $l(\eta)$ are defined in similar way for β. Let $z(X)$ be the series obtained from the expansion of $\zeta_{p^{n_p}}$ into π. Then;*

$$\left(\frac{\alpha, \beta}{\mathfrak{p}} \right) = \zeta_{p^{n_p}}^{Tr(\gamma)},$$

where

$$\gamma = res_X \left(l(\epsilon) \frac{dl(\eta)}{dX} - l(\epsilon) B^{-1} \frac{dB}{dX} + l(\eta) A^{-1} \frac{dA}{dX} \right) \left(\frac{1}{2} + \frac{1}{z^{p^{n_p}} - 1} \right)$$

7.2.4 The Case $p = 2$

In this section we give the formula for special case $p = 2$. Although the calculations are highly technical, the same way of proof just works here. For a suitable function one may prove that the values of the function at principal units and prime elements coincide with that of Hilbert symbol, and finish the proof by bilinearity. We leave all the technical detail to [8] or to [4], and give the formula.

The first essential difference with the case $p > 2$ is that the pairing for formal series is not defined for all invertibe series in $\mathcal{O}_T^0((X))$ but series which belong to $Q := \{X^m c\epsilon(X) : \epsilon(X) \in 1 + \mathcal{O}_T^0[[X]],\ c \in {\mathcal{O}_T^0}^*,\ F(a) \equiv a^2(\text{mod } 4),\ m \in \mathbb{Z}\}$. For α, β in $K_\mathfrak{p}$, set $\alpha = \pi^a\theta\epsilon$, $\beta = \pi^b\theta'\eta$, $A(X) = X^a\theta\epsilon(X)$, $B(X) = X^b\theta'\eta(X)$, define

$$\Phi^{(1)} = \frac{d}{dX}\left(\frac{F}{2}\left(\frac{A^2 - F(A)}{2F(A)}\frac{B^2 - F(B)}{2F(B)}\right)\right),$$

$$\Phi^{(2)} = X^{-1}v_X(A)v_X(B)l(z(X)^{2^{n_2-1}}),$$

where v_X is the discrete valuation of $\mathcal{O}_T((X))$ correspond to X. We now introduce a series $h(X)$ and a polynomial $r(X)$ for $p = 2$. Define

$$h(X) = \frac{F(z(X)^{2^{n_2-1}} - 1) - (z(X)^{2^{n_2}} - 1)}{2^{n_2}}$$

Let $r_0(X)$ be a polynomial in $X\mathcal{O}_T[X]$ of degree $e - 1$ satisfying the condition:

$$F^2(r_0) + (1 + 2^{n_2-1}(z(X)^{2^{n_2-1}} - 1))F(r_0) + ((z(X)^{2^{n_2-1}} - 1))r_0 = \sum_{m\geq 0} a_m X^m$$

with $a_{2m} \equiv 0(\text{mod } 2)$. We have the following formula for $p = 2$

Theorem 7.2.7 $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = \zeta_{2^{n_2}}^{\gamma}$ *where*

$$\gamma = res_X\left(l(\epsilon)\frac{dl(\eta)}{dX} - l(\epsilon)B^{-1}\frac{dB}{dX} + l(\eta)A^{-1}\frac{dA}{dX} + \Phi^{(1)} + \Phi^{(2)}\right)r(X)\left(\frac{1}{2} + \frac{1}{z^{2^{n_2}} - 1}\right).$$

Proof: Refer to [8]

Bibliography

[1] Artin, E. (1927): Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Math. Semin. Univ. Hamb. 5, 353-363.

[2] Artin E., Tate, J. (1968): Class Field Theory. New York e.a.: Benjamin, 259pp.

[3] Artin E. (1956): Theory of algebraic numbers: Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter semester.

[4] Brückner, H. (1979): Hilbertsymbole zum Exponenten p^n und Pfaffsche Formen. Preprint Hamburg

[5] Cassels, J. W. S., Fröhlich, A. (1967): Algebraic Number Theory. New York-London Academic Press.

[6] Chevalley, C. (1951): Introduction to the Theory of Algebraic functions of One Variable. Amer. Math. Soc. Mathematical Surveys VI.

[7] Eisenstein, G. (1850): Beweis der allgemeinsten Reziprozitätsgesetze zwischen reellen und komplexen Zahlen. Ber. K. Akad. Wiss. Berlin, 189-198 (Mathematische Werke II, 712-721).

[8] Fesenko, I. B. Vostokov, S. V. (2002): Local Fields and Their Extensions.- 2nd Ed. Translations of Mathematical Monographs, Amer. Math. Soc.

[9] Hasse, H. (1979): Number Theory. Engl. Transl. of the 3rd ed. of Zahlentheorie. Berlin: Akademie-Verlag.

[10] Hasse, H. (1936): Die Gruppe der p^n-primären Zahlen für einen Primteiler $\mathfrak{p}$ von p, J. Reine Angew. Math. 176, 174-183

[11] Hensel, K. (1916): Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers, J. Reine Angew. Math 146, 189-215.

[12] Hilbert, D. (1895): The Theory of Algebraic Number Fields. Engl. Transl. of Die Theorie der algebraischen Zahlkörper, Berlin Heidelberg New York: Springer-Verlag.

[13] Iwasawa, K. (1986): Local Class Field Theory. Oxford Univ. Press New York.

[14] Koch, H. (1997): Algebraic Number Theory. Berlin Heidelberg New York: Springer-Verlag.

[15] Lang, S. (1970): Algebraic Number Theory. London: Addison-Wesley Publ. Comp.

[16] Neukirch, J. (1986): Class Field Theory. Berlin Heidelberg New York: Springer-Verlag.

[17] Roquette, P. (2000): Class Field Theory in Characteristic p. Its Origin and Development. Advanced Studies in Pure Mathematics vol. 30, Tokyo, 549 - 631.

[18] Rosen., M. I. (2002): Number Theory in Function Fields. Berlin Heidelberg New York: Springer-Verlag.

[19] Schmid, H. L., (1936): Über das Reziprozitätsgesetz in relativzyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper. Math. Zeit. 40, 94-109.

[20] Serre, J. P. (1988): Algebraic Groups and Class Fields. Transl. of the French Ed., Springer-Verlag.

[21] Serre, J. P. (1979): Local Fields. Transl. of French. Ed., Berlin Heidelberg New York: Springer-Verlag.

[22] Shafarevich, I. R. (1950): A General Reciprocity Law. Mat. Sb., Nov. Ser. 26 (68), 113-146, English transl.: Transl., II. Ser., Am. Math. Soc., 4, 73-106 (1956) and in Shafarevich, Collected Mathematical Papers. Berlin Heidelberg New York: Springer-Verlag 1989, 54-58.

[23] Stichtenoth, H. (1993): Algebraic Function Fields and Codes. Berlin Heidelberg New York: Springer-Verlag.

[24] Vostokov, S. V., (1978): The Explicit Form of The Reciprocity Law. Izv. Akad. Nauk SSSR, Ser. Mat. 42, No. 6, Englich Transl.: Math. USSR, Izv. 13, 557-588 (1979)

[25] Weil, A. (1967): Basic Number Theory. Berlin Heidelberg New York: Springer-Verlag.

[26] Weil, A. (1942): Oeuvres Scientifiques I, p. 291 (in Lettre à Artin, a 1942 letter to Artin, explaining the 1940 Comptes Rendus note Sur les fonctions algébriques à corps de constantes finis)

[27] Witt, E. (1936): Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. J. Crelle 176, 126-140.