PMATH 940 - Local Fields!

https://sachink003.github.io

Sachin Kumar
University of Waterloo

Winter 2024

Preface

This class taught by Jerry (Xiaoheng) Wang in Winter 2024. The topics covered are:

1. **Absolute Values:** Absolute values, Topology, Classifying local fields, Hensel's lemma, Newton polygon, Extensions of absolute values for complete valued fields.

2. **Ramification:** Totally ramified, Tamely ramified, Unramified extensions, item Ramification groups, Discriminant, Upper numbering ramification groups, Local Kronecker-Weber, Serre's mass formula.

3. **Absolute values over Global fields:** Places of global fields, Product formula, Discriminant again, Decomposition groups, Inertia and Frobenius, Chebotarev density theorem, Cyclotomic extensions, global Kronecker-Weber.

4. **Local Class Field Theory via Lubin-Tate theory:** Main theorems of LCFT, Formal groups, Lubin-Tate extension, little-bit of GCFT.

The main prerequisites are commutative algebra, Real Analysis, General (Point-set) Topology and Algebraic Number Theory, but it is recommended to know basic algebraic geometry (but not mandatory).

1 Absolute Values

§1.1 Introduction

The main objects of interest of algebraic number theory are the algebraic extensions of $\mathbb{Q}$. By Galois theory, this amounts to studying the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and its closed subgroups. This turns out to be way too difficult! If we restrict our attention to abelian extensions (i.e. Galois extensions with abelian Galois groups), things are a lot cleaner.

Theorem 1.1.1

(Kronecker-Weber) Every finite abelian extension of $\mathbb{Q}$ lies in a cyclotomic extension $\mathbb{Q}(\zeta_m)$.

We will prove this result in this course. Let's look at some toy examples first. Notice that The icosahedron problem in 2023 Putnam A4 is related to $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$ with

$$\sqrt{5} = 2(\zeta_5 + \zeta_5^{-1}) + 1.$$

Similar to 3, one can check that $\sqrt{7} \notin \mathbb{Q}(\zeta_7)$ as the real subfield of $\mathbb{Q}(\zeta_7)$ has odd degree over $\mathbb{Q}$. Instead, we use

$$\prod_{1 \le i < j \le p-1} (\zeta_p^i - \zeta_p^j)^2 = p^* \cdot p^{p-3}$$

where $p^* = (-1)^{(p-1)/2}p$. This means that $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$. By throwing in ζ_4 if needed, we have

$$\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p, \zeta_4) = \mathbb{Q}(\zeta_{4p}).$$

Since every quadratic extension of $\mathbb{Q}$ is a compositum of $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-1})$, we have proved Theorem **??** in the degree 2 case. The degree 3 case also has some very interesting examples. A C_3-extension of $\mathbb{Q}$ is of the form $\mathbb{Q}[x]/(f(x))$ where $f(x) \in \mathbb{Q}[x]$ is irreducible with square discriminant. For example, for $f(x) = x^3 - 3x + 1$, we have

$$\Delta(f) = -4(-3)^3 - 27(1)^2 = 81.$$

My 145 students/TAs would recognize $x^3 - 3x + 1$ as the minimal polynomial of $\zeta_9 + \zeta_9^{-1}$. So

$$\mathbb{Q}[x]/(x^3 - 3x + 1) \cong \mathbb{Q}(\zeta_9 + \zeta_9^{-1}) \subseteq \mathbb{Q}(\zeta_9).$$

Exercise: If you are told that the discriminant of $x^3 + x^2 - 2x - 1$ is 49, what would you guess the field $\mathbb{Q}[x]/(x^3 + x^2 - 2x - 1)$ to be? This is $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. You can check this, and the $x^3 - 3x + 1$ example, by computing $f(x + x^{-1})$.

As another example, we take $g(x) = x^3 - 9x + 9$ which has discriminant $-4(-9)^3 - 27(9)^2 = 9^3 = 3^6$. Which cyclotomic extension contains $\mathbb{Q}[x]/(x^3 - 9x + 9)$? Testing some small values gives

$$g(-1) = 17, \qquad \text{and} \qquad g(-2) = 19.$$

This implies that $g(x)$ factors mod 17 and mod 19. Since $\mathbb{Q}[x]/(g(x))$ is Galois, we see that $g(x)$ splits completely mod 17 and mod 19. Trying more values leads one to conjecture that $g(x)$ splits completely mod p if and only if $p = 3$ or $p \equiv \pm 1 \pmod 9$. A couple of results we will prove in this course say that Galois extensions are uniquely determined by the set of primes that split completely; and that the primes that split completely in $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ are exactly these as well. So this suggests as well that

$$\mathbb{Q}[x]/(x^3 - 9x + 9) \cong \mathbb{Q}(\zeta_9 + \zeta_9^{-1}).$$

It is then not to hard to do some calculation to find that $x^3 - 9x + 9$ is the minimal polynomial of $\zeta_9 + \zeta_9^{-1} - \zeta_9^2 - \zeta_9^{-2}$. So the above is in fact true as $\mathbb{Q}(\zeta_9 + \zeta_9^{-1} - \zeta_9^2 - \zeta_9^{-2})$ is a subfield of $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ of the same degree over $\mathbb{Q}$.

There are some important observations from these examples:

- The discriminant gives us information on which cyclotomic extension $\mathbb{Q}(\zeta_m)$ to consider and which mod to consider.

- The set of primes that split completely are given by congruence conditions mod the above.

We will see that these are the artifacts of abelian extensions! There is an even more important idea to be learnt here: we should study the extension one prime at a time. The process of "localizing" $\mathbb{Z}$ so that only the prime (p) matters is called localization. The ring $\mathbb{Z}_{(p)}$ is formed by adjoining the inverses of every integer not divisible by p. The ring $\mathbb{Z}_p$ of p-adic integers is formed by taking its (ring-theoretic) completion at (p):

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(b_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \colon b_{n+1} \equiv b_n \pmod{p^n}\}.$$

More concretely, we can write every element of $\mathbb{Z}_p$ as the formal infinite series

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

where each $a_i = 0, \ldots, p-1$ so that $a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \equiv b_n \pmod{p^n}$. The field $\mathbb{Q}_p$ of p-adic numbers is the field of fraction of $\mathbb{Z}_p$. It is an example of a local field and we will be studying extensions of it. For example, we will prove the local version of Kronecker-Weber: every finite abelian extension of $\mathbb{Q}_p$ is contained in some $\mathbb{Q}_p(\zeta_m)$. We will then use this to prove the global version after studying how the Galois group of the local extension and the Galois group of the global extension relate to each other.

How does the field $\mathbb{Q}_p$ relate to the field $\mathbb{Q}$? The field $\mathbb{Q}_p$ is uncountable, and so is not algebraic over $\mathbb{Q}$. One can show that the p-adic integer

$$\sum_{n=0}^{\infty} p^{n!}$$

is transcendental over $\mathbb{Q}$. The proof of this is very similar to the proof that the real number $\sum_{n=0}^{\infty} 10^{-n!}$ is transcendental over $\mathbb{Q}$: that it can be approximated too well by a rational number. Now to say that a real number α is approximated well by a rational number r, we are saying that the absolute value $|r - \alpha|$ is small. Can we define a notion of p-adic absolute value on $\mathbb{Q}$ (and extend naturally to $\mathbb{Q}_p$)? Yes! We can define it using the p-adic valuation. For any nonzero integer a, we define its **p-adic valuation** $\mu_p(a)$ as the largest integer k such that $p^k \mid a$ and we extend it to $\mathbb{Q}$ via $\mu_p(a/b) = \mu_p(a) - \mu_p(b)$ and $\mu_p(0) = \infty$. It behaves fairly well with respect to addition and multiplication: for any $r, s \in \mathbb{Q}$,

$$\mu_p(rs) = \mu_p(r) + \mu_p(s), \qquad \text{and} \qquad \mu_p(r+s) \geq \min\{\mu_p(r), \mu_p(s)\}.$$

We then define the multiplicative p-adic absolute value by $|r|_p = p^{-\nu_p(r)}$ for any $r \in \mathbb{Q}$. It is multiplicative $|rs|_p = |r|_p|s|_p$ and satisfies the ultrametric inequality:

$$|r+s|_p \leq \max\{|r|_p, |s|_p\}$$

which is stronger than the triangle inequality

$$|r+s|_p \leq |r|_p + |s|_p.$$

We now have the p-adic metric on $\mathbb{Q}$: $d_p(r,s) = |r-s|_p$ so that two rational numbers are close p-adically if and only if their difference is highly divisible by p. Just as $\mathbb{R}$ can be defined as the completion of $\mathbb{Q}$ with respect to the usual archimedean distance $d_\infty(r,s) = |r-s|_\infty$, the field $\mathbb{Q}_p$ can be defined as the completion of $\mathbb{Q}$ with respect to the p-adic metric $d_p(r,s)$.

Are there any other interesting absolute values on $\mathbb{Q}$? To answer this, we should properly define the notion of absolute values on fields.

§1.2 Absolute values

Let K be a field. An **absolute value** on K is a function $|.| : K \to \mathbb{R}$ such that for any $x, y \in K$:

1. (Positivity) $|x| \geq 0$ with equality if and only if $x = 0$;
2. (Multiplicativity) $|xy| = |x||y|$;
3. (Triangle inequality) $|x+y| \leq |x| + |y|$.

Absolute values that satisfy the stronger **ultrametric inequality**:

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

are said to be **non-archimedean**.

Example: What are the absolute values of a finite field $\mathbb{F}_q$? From multiplicativity, we see that $|1| = 1$ and so for any root of unity u with $u^m = 1$, we have $|u| = 1$. Every nonzero element of a finite field is a root of unity and so the only absolute value on $\mathbb{F}_q$ is the trivial one: sending 0 to 0, and everything else to 1.

Our first goal is to classify all absolute values on $\mathbb{Q}$. Let's make some general observations first.

1. Every field has the trivial absolute value defined by $|x| = 1$ for all $x \neq 0$.
2. For any absolute value $|.|$, we have $|1| = |-1| = 1$, and $|\zeta| = 1$ if $\zeta \in K$ is a root of unity.
3. For any positive integer n, we have $|n| \leq |1+1+\cdots 1| \leq n$.
4. If $|.|$ is an absolute value on K, then for any $a \in (0,1]$, $|.|^a$ is also an absolute value.
5. If $|.|$ is a non-archimedean absolute value on K, then for any $a > 0$, $|.|^a$ is also a non-archimedean absolute value.
6. On $\mathbb{Q}$, $|.|_\infty^a$ is not an absolute value if $a > 1$ and $|.|_p^a$ is not an absolute value if $a < 0$.

Theorem 1.2.1

(Ostrowski) Every nontrivial absolute value on $\mathbb{Q}$ is of the form $|.|_\infty^a$ for some $a \in (0,1]$ or of the form $|.|_p^a$ for some prime p and some $a > 0$.

Proof. We make the following comparison between $|m|$ and $|n|$ for any two integers $m, n > 1$. For any $k \in \mathbb{N}$, we express m^k in base n to get

$$m^k = a_0 + a_1 n + \cdots + a_r n^r$$

with $a_i = 0, \ldots, n-1$ and $r \leq k \log m / \log n$. So

$$|m|^k \leq (a_0 + a_1 + \cdots + a_r) \max\{1, |n|\}^r \leq n(1+r) \max\{1, |n|\}^r.$$

Taking k-th root and letting $k \to \infty$, we get

$$|m| \leq \max\{1, |n|\}^{\log m / \log n}. \tag{1.1}$$

Suppose first that $|p| > 1$ for all primes $p > 1$, and so also for all integers $n > 1$. Then (**??**) gives

$$|m|^{1/\log m} \leq |n|^{1/\log n}$$

for any integers $m, n > 1$. Swapping m and n shows that they are all equal. Let $c > 1$ be the common value. Then

$$|m| = c^{\log m} = |m|_\infty^{\log c}.$$

This completes the case of archimedean absolute values.

Suppose now that $|p| \leq 1$ for some prime p. Then by (**??**), $|q| \leq 1$ for all primes q. Hence $|n| \leq 1$ for every integer n. Suppose further than $|p| < 1$. Suppose for a contradiction that there is a prime q with $|q| < 1$ and $q \neq p$. Then there exist integers a, b such that $ap + bq = 1$. Then

$$1 \leq \max\{|a||p|, |b||q|\} < 1.$$

Contradiction. Therefore, $|.| = |.|_p^a$ where $a = \log_{1/p} |p| > 0$. □

What about the field $\mathbb{F}_q(t)$? As the following results show, we only need to consider the non-archimedean ones.

Proposition 1.2.2

An absolute value $|.|$ on K is non-archimedean if and only if the set $\{|n| \colon n \in \mathbb{Z}\}$ is bounded (and so by 1).

Proof. ($\Rightarrow$) is easy: $|n| = |1 + \cdots + 1| \leq \max\{|1|, \ldots, |1|\} = 1$.

($\Leftarrow$): Suppose $|n| \leq M$ for some $M > 0$ for all $n \in \mathbb{Z}$. Then for any $x, y \in K$ and any $k \in \mathbb{N}$,

$$|x+y|^k \leq \sum_{i=0}^{k} |\binom{k}{i}||x|^i |y|^{k-i} \leq (k+1) \max\{|x|^k, |y|^k\}.$$

Take k-th root and take limit as $k \to \infty$. □

Corollary 1.2.3

If K has positive characteristic, then all absolute values on K are non-archimedean.

We can now classify the absolute values on $\mathbb{F}_q(t)$ in the same way as non-archimedean absolute values on $\mathbb{Q}$. Suppose first that $|t| > 1$. Then for any polynomial, we have

$$|a_d t^d + \cdots + a_0| = |t|^d$$

by Proposition **??**(a), since every summand has a different absolute value . Let $|.|_\infty$ be the absolute value on $\mathbb{F}_q(t)$ defined by $|f(t)|_\infty = q^{\deg(f)}$ for any nonzero polynomial $f(t)$ and then extended by multiplicativity. Then $|.| = |.|_\infty^a$ for $a = \log_q |t| > 0$.

Suppose now $|t| \leq 1$. Then for any polynomial $f(t)$, we have $|f(t)| \leq 1$. We can then use the same argument to conclude that there is a unique irreducible polynomial $\pi(t)$ such that $|\pi(t)| < 1$. Let $|.|_{\pi(t)}$ be the absolute value on $\mathbb{F}_q(t)$ defined by $|\pi(t)|_{\pi(t)} = q^{-\deg(\pi)}$ and $|f(t)|_{\pi(t)} = 1$ for any other irreducible polynomial $f(t)$ and then extended by multiplicativity. Then $|.| = |.|_{\pi(t)}^a$ for $a = \log_{q^{-\deg(\pi)}} |\pi(t)| > 0$.

Theorem 1.2.4

Absolute values on $\mathbb{F}_q(t)$ are all of the form $|.|_\infty^a$ or $|.|_{\pi(t)}^a$ for some irreducible polynomial $\pi(t)$ and some $a > 0$.

There is also a ring-theoretic treatment of non-archimedean absolute values.

Proposition 1.2.5

Let $|.|$ be a non-archimedean absolute value on K. Then:

(a) If $x, y \in K$ with $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

(b) The set $\mathcal{O} = \{x \in K : |x| \leq 1\}$ is a local ring with group of units $\mathcal{O}^\times = \{x \in K : |x| = 1\}$ and maximal ideal $\mathfrak{m} = \{x \in K : |x| < 1\}$.

Suppose now $|.|$ is a nontrivial absolute value on K where $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$. Let $R = \mathbb{Z}$ or $\mathbb{F}_q[t]$ and we suppose that $R \subseteq \mathcal{O}$. Then $\mathfrak{m} \cap R$ is a proper nonzero prime ideal of R. Since R is a PID, we have $\mathfrak{m} \cap R = (\pi)$ for some irreducible $\pi \in R$ and $|.|$ is some power of $|.|_\pi$.

§1.3 Topology

Absolute values on a field K define metrics by $d(x, y) = |x - y|$ and then topologies on K. Two absolute values are **equivalent** if they define the same topology. One important property about equivalent absolute values is that

$$|x|_1 < 1 \iff |x|_2 < 1 \iff \lim_{n\to\infty} x^n = 0.$$

Note also that

$$|x|_1 > 1 \iff |x^{-1}|_1 < 1 \iff |x^{-1}|_2 < 1 \iff |x|_2 > 1$$

and that $|x|_1 = 1 \iff |x|_2 = 1$. Only the trivial absolute value is equivalent to the trivial absolute value, which defines the discrete topology.

Proposition 1.3.1

Two absolute values $|.|_1, |.|_2$ on K are equivalent if and only if $|.|_2 = |.|_1^a$ for some $a > 0$.

Proof. The backwards direction is obvious. Suppose now $|.|_1, |.|_2$ are equivalent and suppose they are nontrivial. The key is that for $m_1, m_2, n_1, n_2 \in \mathbb{N}$ and $x, y \in K^\times$, we have

$$|x|_1^{m_1/n_1} < |y|_1 < |x|_1^{m_2/n_2} \iff |x|_2^{m_1/n_1} < |y|_2 < |x|_2^{m_2/n_2}.$$

This follows by considering y^{n_1}/x^{m_1} and y^{n_2}/x^{m_2}. For any positive real number b, by choosing $m_1, m_2, n_1, n_2 \in \mathbb{N}$ so that $m_1/n_1 \to b^-$ and $m_2/n_2 \to b^+$, we see that

$$|y|_1 = |x|_1^b \iff |y|_2 = |x|_2^b.$$

Hence $\log|x|_2/\log|x|_1$ is constant over $x \in K^\times$ with $|x|_1 \neq 1$. □

When $K = \mathbb{Q}$, the absolute values equivalent to $|.|_\infty$ induce the usual Euclidean topology, and the absolute values equivalent to $|.|_p$ induce the **p-adic topology**. Since only powers of p are possible values of $|x|_p$ for $x \neq 0$, we see that $|\mathbb{Q}^\times|_p$ is a discrete subgroup of $\mathbb{R}^\times$ and open balls and closed balls are the same thing and they are of the form $r + p^n\mathbb{Z}$ for some $r \in \mathbb{Q}$ and some $n \in \mathbb{Z}$.

An absolute value $|.|$ on a field K turns K into a metric space which can then be completed into a complete metric space $\hat{K}$ in which K is dense. Recall that the completion $\hat{K}$ of K can be constructed as the set of equivalence classes of Cauchy sequences in K. It is easy to check that term-wise addition, multiplication, negation, inversion give $\hat{K}$ the structure of a field and the map $K \to \hat{K}$ sending x to $(x, x, \ldots)$ is a field homomorphism. The absolute value $|.|$ extends naturally to $\hat{K}$ making it a **complete valued field**. It is universal in the sense that if $(L, |.|)$ is a complete valued field, then any homomorphism $(K, |.|) \to (L, |.|)$ preserving the absolute value extends uniquely to $(\hat{K}, |.|)$.

The completion of $(\mathbb{Q}, |.|_\infty)$ is $\mathbb{R}$. The completion of $(\mathbb{Q}, |.|_p)$ is the field $\mathbb{Q}_p$ of p-adic numbers. If (x_n) is a Cauchy sequence in $\mathbb{Q}$ such that $\lim |x_n|_p \neq 0$, then eventually, $|x_n - x_m|_p < |x_n|_p$ causing $|x_n|_p$ to be eventually constant. Elements in $\mathbb{Q}_p$ can be viewed as formal series of the form

$$a_{-n}p^{-n} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots + a_m p^m + \cdots$$

with $0 \leq a_i < p$ and $1 \leq a_{-n} < p$. Its p-adic absolute value is p^n. The ring $\mathbb{Z}_p$ of p-adic integers is the subset of $\mathbb{Q}_p$ consisting of elements with $|.|_p \leq 1$. It is a local ring containing $\mathbb{Z}$, with maximal ideal $p\mathbb{Z}_p$ and residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. Given any positive integer n, $\mathbb{Z}_p$ can be covered by p^n open balls of the form $r + p^n\mathbb{Z}_p$. Hence $\mathbb{Z}_p$ is totally bounded, and since it is a complete metric space, it is also compact. As a result, $\mathbb{Q}_p$ is locally compact.

The completion of $(\mathbb{F}_q(t), |.|_\infty)$ is $\mathbb{F}_q((1/t))$. The completion of $(\mathbb{F}_q(t), |.|_t)$ is $\mathbb{F}_q((t))$. For any irreducible polynomial $\pi(t) \in \mathbb{F}_q[t]$, we will show below that the completion is isomorphic to $k((t))$ where $k = \mathbb{F}_q[t]/(\pi(t))$. They are all locally compact for the same reason that $\mathbb{Z}_p$ is compact: finite residue field.

A **local field** is a locally compact valued field $(K, |.|)$. It is automatically complete, since completeness is a local property and a compact metric space is complete. Since scaling is a homeomorphism, the locally compact condition is also equivalent to saying that the closed unit ball (or any closed ball of finite radius) is compact.

Theorem 1.3.2

Every local field is isomorphic to:

1. (Archimedean) $\mathbb{R}$ or $\mathbb{C}$ with the usual absolute value;
2. (Non-archimedean) a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.

Suppose first that K is an archimedean local field with absolute value $|.|$. Then K contains $\mathbb{Q}$ and $|.|$ restricts to an absolute value on $\mathbb{Q}$, which must be archimedean since being archimedean or not can be checked on $\mathbb{Z}$. Since K is complete, K will also contain $\mathbb{R}$. Suppose for any $r \in \mathbb{R}$, $|r| = |r|_\infty^a$ for some $a \in (0,1]$. Viewing K as an $\mathbb{R}$-vector space, we see that its local compactness implies that K is finite-dimensional over $\mathbb{R}$. Then by the fundamental theorem of algebra, we see that $K = \mathbb{R}$ or $K = \mathbb{C}$.

There is a little subtlety in the above argument. Since the absolute value on K may not restrict to the usual absolute value on $\mathbb{R}$, we need to be a bit careful in applying the usual results from analysis. In this case, we are using Riesz's Lemma to construct, in the case $\dim_{\mathbb{R}} K = \infty$, an infinite sequence $(x_n) \subseteq K$ such that each $|x_n| = 1$ and $|x_n - x_m| \geq r$ for any fixed $r < 1$. Indeed, suppose we have $x_1, \ldots, x_n$ constructed. Let $U = \mathrm{Span}_{\mathbb{R}}\{x_1, \ldots, x_n\}$ which is a closed proper subspace in K (note that this uses the completeness of $\mathbb{R}$). Take any $y \notin U$. Let $R = \inf_{x \in U} |x - y|$. Fix any $\epsilon > 0$ and let $z \in U$ be such that $|y - z| \leq R + \epsilon$. Let $t \in \mathbb{R}$ be a positive real number such that $|t| = 1/|y - z|$. Take $x_{n+1} = t(y - z)$. Then for any $x \in U$,

$$|x - x_{n+1}| = |t(x/t - (y - z))| = |t||(x/t + z) - y| \geq \frac{R}{R + \epsilon} \geq r$$

for ϵ small enough. The sequence (x_n) has no convergent subsequence and so K is not locally compact.

We now focus on the non-archimedean case. We define some adjectives.

- A **non-archimedean complete valued field** is a field K equipped with a non-archimedean absolute value with respect to which K is complete.
- A **complete discrete valued field** is a field K equipped with a discrete absolute value with respect to which K is complete.
- An absolute value $|.|$ on K is **discrete** if $|K^\times| = \{|a| \colon a \in K^\times\}$ is discrete in $\mathbb{R}_{>0}$.

Exercise: Prove that a discrete absolute value is non-archimedean.

Proposition 1.3.3

If $(K, |.|)$ is a non-archimedean local field, then $|K^\times|$ is discrete in $\mathbb{R}_{>0}$.

Proof. Similar to the analysis of Cauchy sequences in $\mathbb{Q}$, non-archimedean absolute values have the important property that if (x_n) converges to some nonzero limit x, then the absolute values $|x_n|$ are eventually constant. If $a \neq 0$ is an accumulation point of $|K^\times|$, then there exists a sequence (x_n) with distinct absolute values such that $|x_n| \to a$. Then eventually x_n belongs to the closed ball of radius $2a$ centered at 0, which is compact, but (x_n) has no convergent subsequence. □

In other words, we have the following containments:

$$\{\text{non-archi. complete valued fields}\} \supseteq \{\text{complete discrete valued fields}\} \supseteq \{\text{non-archi. local fields}\}.$$

For example, $\mathbb{C}((t))$ where we define $|\lambda| = 1$ for every $\lambda \in \mathbb{C}^\times$ and $|t| = 1/69$ is a complete discrete valued field that is not a local field, because it is not compact. Its algebraic closure is the field

$$K = \bigcup_{n\geq 1} \mathbb{C}((t^{1/n}))$$

of Puiseux series over $\mathbb{C}$ where we extend the absolute value by $|t^{1/n}| = 69^{-1/n}$. By HW1 P1, K will not be complete, but its completion will be a non-archimedean complete valued field with a non-discrete absolute value.

Proposition 1.3.4

Suppose $|.|$ is a discrete absolute value on K and K is complete. Then $\mathfrak{m}$ is principal. In other words, $\mathcal{O}$ is a discrete valuation ring. Moreover, $\mathcal{O}$ is compact if and only if the residue field $k = \mathcal{O}/\mathfrak{m}$ is finite.

Proof. Since $|.|$ is discrete, there exists $\pi \in \mathfrak{m}$ with the largest absolute value. Then for any $a \in \mathfrak{m}$, $|a/\pi| \leq 1$ and so $a \in (\pi)$.

Since $\mathfrak{m}$ is open and $\mathcal{O}$ can be covered by $\#(\mathcal{O}/\mathfrak{m})$ cosets of $\mathfrak{m}$, we see that if $\mathcal{O}$ is compact, then the residue field is finite. Suppose conversely that $\mathcal{O}/\mathfrak{m}$ is finite. Let $S \subset \mathcal{O}$ be a complete set of representatives for $\mathcal{O}/\mathfrak{m}$. Then every element $a \in \mathcal{O}$ can be written uniquely as

$$a = a_0 + a_1\pi + a_2\pi^2 + \cdots$$

with $a_i \in S$. Note that completeness implies that the above sum converges and

$$\mathcal{O} \cong \varprojlim_n \mathcal{O}/\mathfrak{m}^n.$$

The same argument for $\mathbb{Z}_p$ now proves that $\mathcal{O}$ is totally bounded and so compact. □

Note that if we have a ring homomorphism $\alpha : \mathcal{O}/\mathfrak{m} \to \mathcal{O}$ such that the composition $\mathcal{O}/\mathfrak{m} \to \mathcal{O} \to \mathcal{O}/\mathfrak{m}$ is the identity map, then we have $\mathcal{O} \cong (\mathcal{O}/\mathfrak{m})[[t]]$. Such a ring homomorphism certainly doesn't exist if char$(\mathcal{O}/\mathfrak{m})= p$ but char$(\mathcal{O})= 0$, for example when $\mathcal{O} = \mathbb{Z}_p$. We call this the mixed characteristic case. The issue here is that no additive map α can exist. However, it is posible to define α to be multiplicative.

Consider the example of $\mathcal{O} = \mathbb{Z}_p$. Then we are looking for a group homomorphism $\alpha : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$. In other words, for any integer j such that $p \nmid j$, we need an element $\alpha(j)$ of $\mathbb{Z}_p$ that is congruent to j mod p and is a root of $f(x) = x^{p-1} - 1$. The standard method is Hensel's lift, in other words, p-adic Newton's method. We note that for any $a \in \mathbb{Z}$ such that $p \nmid a$,

$$f'(a) = (p-1)a^{p-2} \equiv -a^{-1} \pmod{p}$$

and

$$a - \frac{f(a)}{-a^{-1}} = a + (a^{p-1} - 1)a = a^p.$$

Hence, we have

$$\alpha(j) = \lim_{n\to\infty} j^{p^n}.$$

This is the Teichmüller lift.

In general, we have $\mathcal{O}/\mathfrak{m} \cong \mathbb{F}_q$ where q is some power of p. For any $j \in \mathbb{F}_q^\times$, we lift it arbitrarily to some $a_j \in \mathcal{O}$ and then apply Hensel's lift to find a root of $x^{q-1} - 1$ that is congruent to a_j mod $\mathfrak{m}$ by taking

$$\alpha(j) = \lim_{n\to\infty} a_j^{q^n}.$$

We note first that $\alpha(j)$ is independent on the choice of the lift a_j. Let π be a uniformizer, so that $\mathfrak{m} = (\pi)$. Then $p \in (\pi)$. Hence if $a_j \equiv b_j \pmod{\pi}$, we have

$$a_j^p \equiv b_j^p + p(a_j - b_j)b_j^{p-1} \equiv b_j^p \pmod{\pi^2}.$$

Hence the sequences $a_j^{q^n}$ and $b_j^{q^n}$ have the same limits. It then follows that α is multiplicative. If $\mathcal{O} = p$, then α is also additive, in which case α is a ring homomorphism and $\mathcal{O} \cong \mathbb{F}_q[[t]]$.

Remark 1: We don't actually need $\mathcal{O}/\mathfrak{m}$ to be finite to define α. All that is needed is that $\mathcal{O}/\mathfrak{m}$ is perfect, so that the Frobenius map $x \mapsto x^p$ is an automorphism. Fix any $\lambda \in \mathcal{O}/\mathfrak{m}$. For every integer $n \geq 1$, there exists a unique $\lambda_n \in \mathcal{O}/\mathfrak{m}$ such that $\lambda_n^{p^n} = \lambda$. Let a_n be any element in $\mathcal{O}$ lifting λ_n and define

$$\alpha(\lambda) = \lim_{n\to\infty} a_n^{p^n}.$$

For any $m > n$, since $a_m^{p^{m-n}} \equiv a_n \pmod{\pi}$, we have $a_m^{p^m} \equiv a_n^{p^n} \pmod{\pi^{n+1}}$. Hence the limit exists. The independence on the lift a_n and the multiplicativity (and additivity in the equal characteristic case) follow as before.

Remark 2: When the residue field $k = \mathcal{O}/\mathfrak{m}$ has characteristic 0, it is also true that $\mathcal{O} \cong k[[t]]$. This is treated in more detail in Serre's Local Field p.34. Here is a sketch. The natural map $\mathbb{Z} \to \mathcal{O}$ sends nonzero integers to units since it is injective to k, so $\mathbb{Q}$ is a subring of $\mathcal{O}$. Let S be the maximal subfield of $\mathcal{O}$ containing $\mathbb{Q}$, which exists by Zorn's Lemma. Then prove that the composition of the natural maps $S \hookrightarrow \mathcal{O} \to k$ is an isomorphism.

We focus on the case $\text{char}(\mathcal{O}) = 0$. In this case, $\mathbb{Q} \hookrightarrow K$ and by completeness, K is an extension of $\mathbb{Q}_p$, of finite dimension n by compactness. The ring $\mathcal{O}$ is a finite $\mathbb{Z}_p$-module free of rank n since it is torsion-free. We fix a uniformizer π so that $\mathfrak{m} = (\pi)$. The **ramification degree** e is defined to be the positive integer such that $(p) = (\pi)^e$. The **residue degree** f is defined to be degree of the residue field extension $[\mathcal{O}/\mathfrak{m} : \mathbb{F}_p]$. Let $b_1, \ldots, b_f$ be elements in $\mathcal{O}$ such that their images in $\mathcal{O}/\mathfrak{m}$ form an $\mathbb{F}_p$-basis. Let

$$S = \{b_i\pi^j : 1 \leq i \leq f, 0 \leq j \leq e-1\} \subset \mathcal{O}.$$

Then S forms a basis for the $\mathbb{F}_p$-module $\mathcal{O}/(p)$. Hence by Nakayama's lemma, S forms a basis for the $\mathbb{Z}_p$-module $\mathcal{O}$. Hence, we have $n = ef$.

What about the structure of $K^\times$? Using the uniformizer π and the multiplicative $\alpha : \mathbb{F}_q^\times \to \mathcal{O}^\times$ where $\mathbb{F}_q \cong \mathcal{O}/\mathfrak{m}$, we have

$$K^\times \cong \langle\pi\rangle \times \mathbb{F}_q^\times \times (1 + \mathfrak{m}) \cong \mathbb{Z} \times \langle\zeta_{q-1}\rangle \times (1 + \pi\mathcal{O}).$$

The group $1 + \mathfrak{m}$ admits a filtration by $U_n = 1 + \pi^n\mathcal{O}$. Consider the case of $\mathcal{O} = \mathbb{Z}_p$. Then we have

$$\begin{aligned}(1 + p^n a)^p &= 1 + p^{n+1}a + \text{higher order terms} + p^{np}a^p \\ &= 1 + p^{n+1}a \pmod{p^{n+2}} \qquad \text{if} \qquad n > \frac{1}{p-1}.\end{aligned}$$

Hence if p is odd, we have isomorphisms $\mathbb{Z}/p^\ell\mathbb{Z} \cong U_1/U_{\ell+1}$ sending m to $(1+p)^m$; and when $p=2$, we have isomorphisms $\mathbb{Z}/2^\ell\mathbb{Z} \cong U_2/U_{\ell+2}$ sending m to $(1+4)^m$. Taking inverse limits gives isomorphisms

$$\mathbb{Z}_p \cong 1 + p\mathbb{Z}_p, \qquad \text{and} \qquad \mathbb{Z}_2 \cong 1 + 4\mathbb{Z}_2.$$

Putting things together:

$$\begin{aligned} \mathbb{Q}_p^\times &\cong \mathbb{Z} \times \langle \zeta_{p-1} \rangle \times \mathbb{Z}_p, \quad \text{for } p > 2, \\ \mathbb{Q}_2^\times &\cong \mathbb{Z} \times \langle -1 \rangle \times \mathbb{Z}_2. \end{aligned}$$

Remark 1: In HW 2 P6, using p-adic logarithms, one can show that $1+\pi^n\mathcal{O} \cong \mathcal{O}$ for $n > e/(p-1)$.
Remark 2: In fact, $\mathbb{Q}_2^\times$ is a special case of

$$\mathbb{Q}_p(\zeta_p)^\times \cong \mathbb{Z} \times \langle \zeta_{p-1} \rangle \times \langle \zeta_p \rangle \times \mathbb{Z}_p^{p-1}.$$

The minimal polynomial of $\zeta_p - 1$ over $\mathbb{Q}_p$ is

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p,$$

which is irreducible in $\mathbb{Q}_p[x]$ since it is Eisenstein. Since $\zeta_p - 1$ is a root of this polynomial, we see that in $\mathbb{Q}_p(\zeta_p)$ (assuming that the p-adic absolute value of $\mathbb{Q}_p$ extends),

$$|\zeta_p - 1|^{p-1} = |p|.$$

Since $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p-1$. We see that $\zeta_p - 1$ is a uniformizer so that $\zeta_p \in U_1$, the ramification degree $e = p-1$ so that $U_2 \cong \mathcal{O} \cong \mathbb{Z}_p^{p-1}$ and the residue degree $f = 1$ so that $(\mathcal{O}/\mathfrak{m})^\times \cong \langle \zeta_{p-1} \rangle$. This is an example of a totally ramified extension.
Exercise: Prove that an absolute value on $\mathbb{Q}_p(\zeta_p)$ exists where $|\zeta_p - 1|^{p-1} = |p|$. Note from the theory of normed vector spaces over a complete field, any two nontrivial absolute values on $\mathbb{Q}_p(\zeta_p)$ are equivalent.
Exercise: Prove that $\mathbb{Z}_p \cong \mathbb{Z}[[x]]/(x-p)$. How much can you generalize this?

§1.4 Hensel's Lemma and Non-archimedean complete valued field

Our next goal is to understand what finite extensions of $\mathbb{Q}_p$ look like. We say a field K is a **non-archimedean complete valued field** if it is equipped with a non-archimedean absolute value $|.|$ with respect to which K is complete. We then have the associated valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{m}$ and residue field $k = \mathcal{O}/\mathfrak{m}$:

$$\begin{aligned} \mathcal{O} &= \{a \in K \colon |a| \leq 1\}, \\ \mathfrak{m} &= \{a \in K \colon |a| < 1\}. \end{aligned}$$

We do not assume that the absolute value is discrete so $\mathfrak{m}$ may not be principal. We do not assume that the residue field k is finite so $\mathcal{O}$ may not be compact. For any $f(x) \in \mathcal{O}[x]$, let $\bar{f}(x)$ denote its image in $k[x]$. We say $f(x) \in \mathcal{O}[x]$ is **primitive** if $\bar{f} \neq 0$.

Theorem 1.4.1

(Hensel's Lemma) Suppose $f(x) \in \mathcal{O}[x]$ is primitive and $\bar{f}(x)$ factors as a product $g_0 h_0$ of coprime polynomials g_0, h_0 in $k[x]$. Then there exist polynomials $g, h \in \mathcal{O}[x]$ such that $f = gh$, $\deg(g) = \deg(g_0)$ and $\bar{g} = g_0, \bar{h} = h_0$. Moreover, $(g, h) = \mathcal{O}[x]$ and the factorization is unique up to scaling by elements in $1 + \mathfrak{m}$.

Proof. We note first that since $\deg(g) = \deg(g_0)$, the leading coefficient of $g(x)$ is a unit and so $\mathcal{O}[x]/(g, h)$ is a finite $\mathcal{O}$-module and so is trivial by Nakayama's Lemma. We construct g, h by induction. We lift g_0, h_0 arbitrarily to $\mathcal{O}[x]$. There exist polynomials $a, b \in \mathcal{O}[x]$ such that $ag_0 + bh_0 - 1 \in \mathfrak{m}[x]$. Let π be the coefficient of minimal valuation among those of $f - g_0 h_0$ and $ag_0 + bh_0 - 1$. Then $f - g_0 h_0 \in \pi\mathcal{O}[x]$ and $ag_0 + bh_0 - 1 \in \pi\mathcal{O}[x]$. Suppose we have constructed monic polynomials $g_n, h_n \in \mathcal{O}[x]$ with $g_n - g_{n-1} \in \pi^n \mathcal{O}[x]$, $h_n - h_{n-1} \in \pi^n\mathcal{O}[x]$ and such that $f - g_n h_n \in \pi^{n+1}\mathcal{O}[x]$. We seek polynomials $u, v \in \mathcal{O}[x]$ with $\deg u < \deg g_0$, $\deg v < \deg h_0$ such that

$$f - (g_n + \pi^{n+1}u)(h_n + \pi^{n+1}v) \in \pi^{n+2}\mathcal{O}[x].$$

This amounts to $g_n v + h_n u - (f - g_n h_n)/\pi^{n+1} \in \pi\mathcal{O}[x]$. This can be achieved with

$$v = a(f - g_n h_n)/\pi^{n+1}, \qquad u = b(f - g_n h_n)/\pi^{n+1}$$

without the requirement on their degrees. If $\deg u \geq \deg g_0$, we apply the division algorithm to write $u = g_n q + r$ with $\deg r < \deg g_0$. Then

$$g_n v + h_n u = g_n(v + h_n q) + h_n r$$

and we replace u, v by $r, v + h_n q$. Taking $g = \lim g_n$ and $h = \lim h_n$ does the job.

To prove uniqueness, suppose (g', h') is another coprime factorization. Then $(g, h') = \mathcal{O}[x]$ since $(\bar{g}, \bar{h'}) = k[x]$. So $gr + h's = 1$ for some $r, s \in \mathcal{O}[x]$. Multiply by g' to get $g \mid g'$. Similarly, we have $g' \mid g$ and so they differ by a scalar that reduces to 1 in k. □

The condition that g_0 and h_0 are coprime is important. The polynomial $x^8 + x^2 + 1$ factors as $(x^4 + x + 1)^2$ in $\mathbb{F}_2[x]$, but it is a simple bash to show that it doesn't factor as a product of two quartics in $(\mathbb{Z}/4\mathbb{Z})[x]$ so it is irreducible in $\mathbb{Q}_2[x]$. (**Exercise**:) Prove that $x^8 + x^2 + 1$ factors in $\mathbb{Q}_p[x]$ for every prime p. Indeed, its discriminant $2^8 \cdot 229^2$ is a square but the discriminant of an irreducible polynomial in $\mathbb{F}_p[x]$ of degree d is a quadratic residue mod p if and only if d is odd. This implies that it factors in $\mathbb{F}_p[x]$. For $p \neq 229$, since it has no repeated factors in $\mathbb{F}_p[x]$, the factorization in $\mathbb{F}_p[x]$ lifts to $\mathbb{Z}_p[x]$. When $p = 229$, Wolfram alpha gives

$$x^8 + x^2 + 1 = (x + 103)^2(x + 126)^2(x^2 + 110x + 171)(x^2 + 119x + 171) \in \mathbb{F}_{229}[x].$$

Hensel's lemma lifts this to a product of 4 polynomials of degree 2 in $\mathbb{Z}_{229}[x]$. Note also that if c is a root of $x^8 + x^2 + 1$, then so is $-c$. Hence for any p, the polynomial $x^8 + x^2 + 1$ has no irreducible factors of degree 5 or 7. The Galois group of the splitting field of $x^8 + x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{F}_2^3 \rtimes S_4$, where the action of S_4 on $\mathbb{F}_2^3$ is via its 3-dimensional regular representation. When viewed as permutations on the 8 roots, we see that there are no 5-cycles or 7-cycles. The underlying principle here is the Chebotarev density theorem.

For another example, the polynomial $x^{p-1} - 1 \in \mathbb{Z}_p[x]$ factors as $(x-1)\cdots(x-(p-1)) \in \mathbb{F}_p[x]$. Hence it must also split completely over $\mathbb{Z}_p[x]$.

Corollary 1.4.2

Suppose $f(x) \in \mathcal{O}[x]$ with $\bar{f} \neq 0$ and suppose $a_0 \in k$ is a simple root of $\bar{f}(x)$. Then a_0 lifts to a root a of $f(x)$.

Proof. Simple root means that $\bar{f}(x) = (x - a_0)h(x)$ where $x - a_0$ and h are coprime. □

Corollary 1.4.3

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ is irreducible and $a_n a_0 \neq 0$. Let $r = 0, \ldots, n$ be such that $|a_r|$ is maximal. Then $r = 0$ or $r = n$. In other words, if $f(x) \in \mathcal{O}[x]$ is primitive and irreducible in $K[x]$, then a_0 or a_n is a unit. In particular, if $f(x) \in K[x]$ is irreducible with $a_n = 1$ and $a_0 \in \mathcal{O}$, then $f(x) \in \mathcal{O}[x]$.

Proof. Suppose $f(x) \in \mathcal{O}[x]$ is primitive with $a_0 \in \mathfrak{m}$ and $a_n \in \mathfrak{m}$. Then $\bar{f} = x^r h_0(x)$ for some $h_0(x) \in k[x]$ with $h_0(0) \neq 0$. The condition $a_0 \in \mathfrak{m}$ implies $r \geq 1$. The condition $a_n \in \mathfrak{m}$ implies $r < n$. Hence the factor x^r lifts to a nontrivial factor of f.. □

Proposition 1.4.4

Suppose $f(x) \in \mathcal{O}[x]$ and suppose $a_0 \in \mathcal{O}$ satisfies $|f(a_0)| < |f'(a_0)|^2$. Then there is a unique root $a \in \mathcal{O}$ of $f(x)$ with $|a - a_0| \leq |f(a_0)|/|f'(a_0)| < |f'(a_0)|$.

Proof. Define

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

It is easy to check that

$$|f(a_{n+1})| \leq \frac{|f(a_n)|^2}{|f'(a_n)|^2} < |f(a_n)|, \qquad |f'(a_{n+1})| = |f'(a_n)|$$

and

$$|a_{n+m} - a_n| = \frac{|f(a_n)|}{|f'(a_n)|} = \frac{|f(a_n)|}{|f'(a_0)|} \to 0.$$

Hence the sequence (a_n) converges to a desired root a. Note that the inequality $|a - a_0| < |f'(a_0)|$ implies that $|f'(a)| = |f'(a_0)|$.

Suppose now $b \in \mathcal{O}$ is another root with $|b - a_0| < |f'(a_0)|$ and $|b - a| \neq 0$. Then

$$0 = f(b) - f(a) \equiv (b - a)f'(a) \pmod{(b-a)^2}$$

but since $|b - a| < |f'(a_0)|$, we have

$$|(b - a)^2| < |b - a||f'(a_0)| = |(b - a)f'(a)|.$$

Contradiction. □

Corollary 1.4.5

Suppose m is a positive integer not divisible by $\mathrm{char}(\mathcal{O})$. Then every unit sufficiently close to 1 has an m-th root in $\mathcal{O}$.

Proof. Take $a_0 = 1$ and $f(x) = x^m - u$. Then we just need $|u - 1| < |m|^2$. □

Corollary 1.4.6

For any positive integer n, the equation $x^n + 1 = z^n$ has nonzero solutions in $\mathbb{Z}_p$. In other words, Fermat's Last Theorem can't be proved by purely local methods.

For which m does $\sqrt{m}$ exist in $\mathbb{Z}_2$? Clearly any m with $\mu_2(m)$ odd is not a square and if $\mu_2(m)$ is even, we may divide m by powers of 4. So it suffices to consider $m \in \mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$. Since odd squares are all 1 mod 8. We see that $m \in 1 + 8\mathbb{Z}_2$ in order to be a square. Now if $m \in 1 + 8\mathbb{Z}_2$, then consider $f(x) = x^2 - m$ with $a_0 = 1$. We have $f(a_0) \in 8\mathbb{Z}_2$ and $f'(a_0) = 2$ and so $|f(a_0)| < |f'(a_0)|^2$. Hence m has a square root in $1 + 4\mathbb{Z}_2$. Alternatively, one can show that $2n^2 + n = k$ is always solvable in $\mathbb{Z}_2$ by lifting the root k in $\mathbb{F}_2$. In other words,

$$\mathbb{Z}_2^\times/\mathbb{Z}_2^{\times 2} \cong (1 + 2\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Consider now $f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34)$. We know 17 is a square in $\mathbb{Z}_2$ and 2 is a square in $\mathbb{F}_{17}$ and so also in $\mathbb{Z}_{17}$. For any other prime p, at least one of $2, 17, 34$ is a square in $\mathbb{F}_p$ and so a square in $\mathbb{Z}_p$. In other words, $f(x) = 0$ is solvable in $\mathbb{Z}_p$ for all primes p (called *locally soluble*), but not solvable in $\mathbb{Z}$. Other examples include $(x^3+x+1)(x^2+31)$ and $(x^3 - 19)(x^2 + x + 1)$. We will see later that such polynomials can't be irreducible in $\mathbb{Z}[x]$. It is not hard to check it can't be a product of two irreducible degree 2 polynomials.
Exercise: Prove that the Dedekind polynomial $f(x) = x^3 - x^2 - 2x - 8$ splits completely in $\mathbb{Q}_2[x]$.
Exercise: (Weierstrass preparation) Let $f(x) \in \mathcal{O}[[x]]$ be primitive and let $d \geq 0$ be the smallest integer such that the coefficient of x^d in $f(x)$ is a unit. Then there exist a unique polynomial $g(x)$ of degree d such that $\bar{g} = x^d$ and a unit $h(x) \in \mathcal{O}[[x]]^\times$ such that $f = gh$. As a consequence, a primitive power series has finitely many roots in $\mathfrak{m}$.

Even though the statement looks just like Hensel's lemma. The proof (that I know) is quite different!
Exercise: Consider the field

$$K = \bigcup_{n \geq 1} \mathbb{C}((t^{1/n}))$$

of Puiseux series over $\mathbb{C}$. Define a non-archimedean absolute value on K by $|t^{1/n}| = 69^{-1/n}$ and $|\lambda| = 1$ for every $\lambda \in \mathbb{C}^\times$. Prove that K is algebraically closed.

For non-archimedean absolute values, we often also consider the asociated **additive valuations**, defined by $\mu(a) = -\log_\rho(|a|)$ for some fixed $\rho > 1$. The additive valuation μ satisfies

1. $\mu(0) = \infty$;
2. $\mu(xy) = \mu(x) + \mu(y)$;
3. $\mu(x + y) \geq \min\{\mu(x), \mu(y)\}$, with equality when $\mu(x) \neq \mu(y)$;
4. $\mathcal{O} = \{a \in K \colon \mu(a) \geq 0\}$ and $\mathfrak{m} = \{a \in K \colon \mu(a) > 0\}$.

Consider now a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ with a root $\alpha \in K$. Then

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_i\alpha^i + \cdots + a_j\alpha^j + \cdots + a_n\alpha^n.$$

We note that the minimal $\mu(a_m\alpha^m)$ must be achieved at least twice, say at i and j. That is,

$$\mu(a_i) + i\mu(\alpha) = \mu(a_j) + j\mu(\alpha) \leq \mu(a_m) + m\mu(\alpha).$$

Hence every point $(m, \mu(a_m))$ lies above or on the line joining $(i, \mu(a_i))$ and $(j, \mu(a_j))$, which has slope $-\mu(\alpha)$. We define the **Newton polygon** of f as the lower convex hull of the points $(m, \mu(a_m))$ for $m = 0, 1, \ldots, n$ and $(0, \infty), (n, \infty)$ on the plane. Its lower edges consist of multiple segments of increasing slope.

Theorem 1.4.7

Suppose K is a non-archimedean (complete) valuation field. Suppose $f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$ splits completely in K. If exactly m of the α_i's have additive valuation s, then the Newton polygon of f has a segment of length m and slope $-s$.

Proof. Since the leading coefficient only has the effect of shifting the Newton polygon up or down, we may assume $a_n = 1$. Suppose first that all n roots of $f(x)$ have additive valuation s. Then for $i = 1, \ldots, n-1$, a_{n-i} is the sum of the i-fold products of the α_j and so is a sum of elements with additive valuation is. Hence $\mu(a_{n-i}) \geq is$. Since $\mu(a_n) = 0$ and $\mu(a_0) = ns$, we see that the Newton polygon of f consists of one segment of length n and slope $-s$.

We now proceed by induction on the number of different valuations of the roots. The base case is proved above. In general, suppose $\alpha_1, \ldots, \alpha_m$ have the highest additive valuations s. Let

$$g(x) = (x - \alpha_1) \cdots (x - \alpha_m) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

with $\mu(b_{m-i}) \geq is$ and $\mu(b_0) = ms$. Let $h(x) = f(x)/g(x) = x^{n-m} + c_{n-m-1}x^{n-m-1} + \cdots + c_0$. Since the slopes for the Newton polygon of h are all bigger than $-s$, we see that $\mu(c_{j+k}) > \mu(c_j) - ks$ for any j and any $k \neq 0$. This implies that $\mu(c_{j+k}b_{m-k}) > \mu(c_j)$ and so

$$a_{j+m} = c_j + c_{j+1}b_{m-1} + \cdots$$

has valuation $\mu(c_j)$. In other words, the points $(i, \mu(a_i))$ for $i = m, \ldots, n$ are obtained from the points $(i, \mu(c_i))$ for $i = 0, \ldots, n-m$ by shifting m units to the right. For any $i = 0, \ldots, m$, we have

$$a_i = c_0 b_i + c_1 b_{i-1} + \cdots + c_i b_0$$

with

$$\mu(c_j b_{i-j}) \geq \mu(c_0) - js + (m - (i-j))s = \mu(c_0) + (m-i)s$$

and $\mu(c_0 b_0) = \mu(c_0) + ms$. Hence we have an extra segment of length m and slope $-s$ from $(0, \mu(a_0))$ to $(m, \mu(a_m))$. □

Of course polynomials rarely split completely. Theorem **??** is the most useful after we extend valuations to field extensions.

Theorem 1.4.8

Let K be a non-archimedean complete valuation ring with absolute value $|.|_K$ and let L be a finite extension of K of degree n. Then the absolute value $|.|_K$ extends uniquely to an absolute value $|.|_L$ on L, and L is complete with respect to $|.|_L$. Moreover, for any $\beta \in L$,

$$|\beta|_L = |N_{L/K}(\beta)|_K^{1/n}.$$

Here, $N_{L/K}(\beta)$ is the determinant of the multiplication by β map on L.

Proof. Uniqueness of the extension and completeness of L follow from general topology, via the theory of finite dimensional normed vector spaces over a complete metric space. It only remains to prove that the ultrametric inequality for $|N_{L/K}(\beta)|_K^{1/n}$. That is, given nonzero $\beta_1, \beta_2 \in L$, we have

$$|N_{L/K}(\beta_1 + \beta_2)|_K \leq \max\{|N_{L/K}(\beta_1)|_K, |N_{L/K}(\beta_2)|_K\}.$$

Without loss of generality, suppose that $|N_{L/K}(\beta_1\beta_2^{-1})|_K \leq 1$. Hence we see that it suffices to prove that

$$|N_{L/K}(\beta)|_K \leq 1 \quad \Longrightarrow \quad |N_{L/K}(\beta + 1)|_K \leq 1.$$

Let $\mathcal{O}_K$ denote the valuation ring of K and let $\mathcal{O}_L$ denote its integral closure in L. In other words, $\mathcal{O}_L$ consists of $\beta \in L$ whose minimal polynomial over K lies in $\mathcal{O}_K[x]$. Recall that

$$\text{char poly of } \cdot\beta \text{ on } L = (\text{char poly of } \cdot\beta \text{ on } K(\beta))^{[L:K(\beta)]} = (\text{min poly of } \beta)^{[L:K(\beta)]}.$$

We see that if $\beta \in \mathcal{O}_L$, then its minimal polynomial is in $\mathcal{O}_K[x]$ and so $N_{L/K}(\beta) \in \mathcal{O}_K$. Conversely, if $N_{L/K}(\beta) \in \mathcal{O}_K$, then the minimal polynomial of β over K is an irreducible polynomial of the form $x^d + \cdots + a_0$ with $a_0 \in \mathcal{O}_K$, and so lies in $A[x]$ by Corollary **??**. Hence

$$\mathcal{O}_L = \{\beta \in L \colon N_{L/K}(\beta) \in \mathcal{O}_K\}.$$

We are now done because $\mathcal{O}_L$ is a ring. □

Corollary 1.4.9

Let K be a complete field with a non-archimedean absolute value $|.|_K$. Let Ω denote an algebraic closure of K. Then $|.|_K$ extends uniquely to an absolute value $|.|_\Omega$ on Ω.

Note the absolute value $|.|_\Omega$ is still non-archimedean, but it is not discrete and Ω is not necessarily complete unless $|.|_K$ is trivial. Consider $K = \mathbb{Q}_p$ with $|.|_p$ and we also denote by $|.|_p$ for its extension to $\bar{\mathbb{Q}}_p$. Then for any positive integer n, we have $p^{1/n} \in \bar{\mathbb{Q}}_p$ and $|p^{1/n}|_p = p^{-1/n}$ which can be arbitrarily close to 1 as n goes to infinity. Since $\bar{\mathbb{Q}}_p$ has countable dimension over $\mathbb{Q}_p$, we know from the Baire Category Theorem (any complete metric space is not a countable union of nowhere dense subsets) that $\bar{\mathbb{Q}}_p$ is not complete. The completion of $\bar{\mathbb{Q}}_p$ is $\mathbb{C}_p$. Krasner's Lemma can also be used to prove that $\mathbb{C}_p$ is algebraically closed. In fact, $\mathbb{C}_p$ is (non-canonically) isomorphic to $\mathbb{C}$ assuming the axiom of choice.

Theorem 1.4.10

Suppose K is a non-archimedean complete valued field. Let $f(x) = a_n(x-\alpha_1)\cdots(x-\alpha_n) \in K[x]$ with $\alpha_1, \ldots, \alpha_n \in \bar{K}$. If exactly m of the α_i's have additive valuation s (under the extension of the valuation on K to $\bar{K}$), then the Newton polygon of f has a segment of length m and slope $-s$.

Proof. Let L be a finite extension of K over which f splits. The extension of $|.|_K$ to L also extends μ to L. Apply Theorem **??** to L. □

Corollary 1.4.11

Suppose K is a non-archimedean complete valued field and suppose $f(x) = a_n x^n + \cdots + a_0 \in K[x]$ is irreducible with $a_n a_0 \neq 0$. Then all the roots of $f(x)$ have the same valuation.

Proof. For any root β of $f(x)$ in $\bar{K}$, we have $|\beta|_{\bar{K}} = |\beta|_{K(\beta)} = |a_0/a_n|_K^{1/n}$. □

Corollary 1.4.12

Let K be a complete field and an additive valuation μ. Let $f(x) \in K[x]$ and suppose that the Newton polygon of f has a segment of length m and slope $-s$. Then there exists $\alpha_1, \ldots, \alpha_m \in \bar{K}$ with valuation s such that $(x - \alpha_1) \cdots (x - \alpha_m) \in K[x]$ and divides $f(x)$.

Proof. When $f(x)$ is factored into a product of irreducible polynomials over K, the roots of each irreducible factor have the same valuations. □

2 Ramification

Suppose now K is a complete discrete valued field with valuation ring A, maximal ideal $\mathfrak{p} = (\pi)$, and residue field k. We normalize μ on K so that $\mu(\pi) = 1$. Let L be an algebraic extension of K. Then the absolute value $|.|$ on K extends uniquely to an absolute value $|.|$ on L, with valuation ring B, maximal ideal $\mathfrak{q}$, and residue field ℓ. From the proof of Theorem **??**, we know that B is the integral closure of A in L. The ring A is a discrete valuation ring. We say L/K is **unramified** if ℓ/k is separable and $\mathfrak{q} = \mathfrak{p}B$. In other words, the ramification degree $e = 1$. We say L/K is **totally ramified** if $\ell = k$. In other words, the residue degree $f = 1$. Note that if L/K is finite of degree n, then B is also a discrete valuation ring and recall that the ramification degree e and residue degree f are defined more generally as

$$\mathfrak{q}^e = \mathfrak{p}B, \qquad \text{and} \qquad f = [\ell : k], \qquad \text{with} \qquad n = ef.$$

§2.1 Interlude on Dedekind domains and Discrete Valuation Rings

A **discrete valuation ring** (DVR) is a PID with a unique nonzero prime ideal. The localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at a prime ideal (p), so that integers not divisible by p are invertible, is a DVR. If A is a DVR with maximal ideal $\mathfrak{m} = (\pi)$ and field of fraction K, then every element $a \in K^\times$ can be written uniquely as $\pi^n u$ for some $n \in \mathbb{Z}$ and $u \in A^\times$ and we define an additive valuation $\mu : K^\times \to \mathbb{Z}$ by $\mu(a) = n$.

Proposition 2.1.1

Suppose A is a local Noetherian integral domain whose maximal ideal is principal. Then A is a DVR.

Proof. Suppose $\mathfrak{m} = (\pi)$ for some $\pi \in A$. Suppose there exists $y \in \bigcap \mathfrak{m}^n$ with $y \neq 0$. Then there is an infinite ascending chain

$$(y) \subsetneq (y\pi^{-1}) \subsetneq (y\pi^{-2}) \subsetneq \cdots$$

contradicting Noetherian-ness. Hence every element in A can be written in the form $\pi^n u$ for some non-negative integer n and unit u and if an ideal contains $\pi^n u$, it also contains π^n. For any nonzero ideal I, let n be the smallest integer such that $\pi^n \in I$, then $I = (\pi^n)$. □

Proposition 2.1.2

A Noetherian integral domain is a DVR if and only if it is integrally closed and has a unique nonzero prime ideal.

Proof. Suppose A is a DVR with field of fraction K. We need to prove it is integrally closed. Let $x \in K$ be integral over A. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in A$. If $\mu(x) = -m < 0$, then $\mu(a_{n-1}x^{n-1} + \cdots + a_0) \geq -(n-1)m > \mu(x^n)$.

To prove the converse, suppose A is integrally closed and has a unique nonzero prime ideal $\mathfrak{m}$. It suffices to show that $\mathfrak{m}$ is principal. Fix some arbitrary nonzero $c \in \mathfrak{m}$. For each $b \notin (c)$, let

$$I_b = \{a \in A\colon ab \in (c)\}.$$

Then each I_b is a nonzero proper ideal of A. Since A is Noetherian, let $b \notin (c)$ be such that I_b is maximal among all such ideals. Suppose $x, y \in A$ with $xy \in I_b$. Then $(x, I_b) \subset I_{yb}$. Hence $y \notin I_b \Rightarrow yb \notin (c) \Rightarrow x \in I_b$. Therefore, $I_b = \mathfrak{m}$ is the unique nonzero prime ideal of A.

Since $I_b(b) \subset (c)$, we have $I_b(b/c) \subset A$. If $I_b(b/c) \subset I_b$, then b/c is integral as it preserves a finitely generated A-module, which implies that $b/c \in A$ since A is integrally closed. This contradicts the assumption that $b \notin (c)$. Hence $I_b(b/c) = A$ and so $I_b = (c/b)$ is principal. □

§2.2 Extensions of non-archimedean absolute values

Recall that we have shown that every local field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{F}_q((t))$ or a finite extension of $\mathbb{Q}_p$. What do finite extensions of $\mathbb{Q}_p$ look like?

Theorem 2.2.1

Let A be a complete DVR with field of fraction K and absolute value $|.|_K$. Let L be a finite extension of K of degree n. Then the integral closure B of A in L is finitely generated as an A-module. The absolute value $|.|_K$ extends uniquely to a discrete absolute value $|.|_L$ on L, and L is complete with respect to $|.|_L$. Moreover, for any $\alpha \in L$,

$$|\alpha|_L = |N_{L/K}(\alpha)|_K^{1/n}.$$

Proof. We note that the completeness of L follows from standard argument after the extension is proven. Namely, fix a K-basis $\{e_1, \ldots, e_n\}$. Given any Cauchy sequence in L, when each term is expressed in the above K-basis, each coefficient forms a Cauchy sequence in K.

Let $\mathfrak{p}$ denote the unique nonzero prime ideal of A. We suppose first that L/K is separable. Then B is a Dedekind domain since A is. All nonzero prime ideals of B lie above $\mathfrak{p}$ and they each define in-equivalent absolute values on L. There are multiple ways to prove that B has only one nonzero prime ideal, which implies that B is a DVR and that $|.|_K$ extends uniquely to L.

(Proof 1): Since K is complete, any norm on a finite dimensional K-vector space is equivalent (i.e. define the same topology) to the sup norm (defining the product topology). (Cassels-Frohlich page 52)

(Proof 2): Suppose $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are two prime ideals of B over $\mathfrak{p}$. Take $\beta \in \mathfrak{q}_1 \backslash \mathfrak{q}_2$. Then $\mathfrak{q}_1 \cap A[\beta]$ and $\mathfrak{q}_2 \cap A[\beta]$ are two distinct prime ideals containing $\mathfrak{p}$. They then give two distinct prime ideals in $A[\beta]/\mathfrak{p} \cong k[x]/(\bar{f}(x))$ where $f(x) \in A[x]$ is the minimal polynomial of β. By Hensel's Lemma, since $f(x)$ is irreducible, we see that $\bar{f}(x) = g(x)^m$ for some irreducible polynomial $g \in k[x]$. However, $k[x]/(g(x)^m)$ only has one prime ideal, contradiction.

To prove the explicit formula for $|.|_L$, let L' denote the Galois closure of L/K. The absolute value $|.|_K$ also extends uniquely to $|.|_{L'}$. For any $\sigma \in \mathrm{Gal}(L'/K)$, $x \mapsto |\sigma(x)|_{L'}$ is a discrete absolute value on L' extending $|.|_K$. Hence $|\sigma(x)|_{L'} = |x|_{L'}$. In other words, for any $\alpha \in L$, the conjugates of α all have the same valuation. Let $\alpha_1, \dots, \alpha_d$ be all the conjugates of α. Then

$$|N_{L/K}(\alpha)|_K = |(\alpha_1 \cdots \alpha_d)^{n/d}|_K = |(\alpha_1 \cdots \alpha_d)^{n/d}|_{L'} = |\alpha|_L^n.$$

Suppose now L/K is inseparable. Then there exists an intermediate field E such that L/E is purely inseparable and E/K is separable. Applying the above to the extension E/K, we may assume L/K is purely inseparable. Then exists a prime power $q = p^m$ where p is the characteristic of K such that $\alpha^q \in K$ for all $\alpha \in L$. The extention of $|.|_K$ to $|.|_L$ is then forced to be $|\alpha|_L = |\alpha^q|_K^{1/q}$. The ultrametric inequality for $|.|_L$ and the norm formula can be checked easily.

Finally, we prove that B is finite over A. This argument doesn't use any separable assumption. We claim first that $B/\mathfrak{p}B$ is finite over $A/\mathfrak{p}$. Indeed, suppose $\{b_i\}_{i\in I} \subset B/\mathfrak{p}B$ is linearly independent over $A/\mathfrak{p}$. Lift each b_i arbitrarily to $\beta_i \in B$. Then $\{\beta_i\}_{i\in I}$ is linearly independent over A (take any linearly combination that gives 0, divide by a power of a uniformizer π of A until some coefficients are units, reduce mod $\mathfrak{p}$). Then I is finite since L/K is finite. Now let $\beta_1, \dots, \beta_m$ for some $m \le n$ be in B such that their images in $B/\mathfrak{p}B$ form a basis over $A/\mathfrak{p}$. We claim that they generate B as an A-module. Take any $b \in B$. Then there exists $a_{ij} \in A$ such that

$$\begin{aligned} b &= \sum_{i=1}^m a_{0i}\beta_i + \pi \sum_{i=1}^m a_{1i}\beta_i + \pi^2 \sum_{i=1}^m a_{2i}\beta_i + \cdots \\ &= \lim_n \sum_{i=1}^m \left(\sum_{j=0}^n a_{ji}\pi^j \right) \beta_i \end{aligned}$$

belongs to $A\beta_1 + \cdots + A\beta_m$ since A is complete. □

Suppose now K is a complete discrete valued field with valuation ring A, maximal ideal $\mathfrak{p}$, and residue field k. Let L be an algebraic extension of K. Then the absolute value $|.|$ on K extends uniquely to an absolute value $|.|$ on L, with valuation ring B, maximal ideal $\mathfrak{q}$, and residue field ℓ. We say L/K is **unramified** if ℓ/k is separable and $\mathfrak{q} = \mathfrak{p}B$. In other words, the ramification degree $e = 1$. We say L/K is **totally ramified** if $\ell = k$. In other words, the residue degree $f = 1$.

§2.3 Totally ramified extensions

Theorem 2.3.1

Totally ramified extensions of a complete discrete valued field K of finite degrees are all of the form $K[x]/(f(x))$ for some Eisenstein polynomial $f(x)$. Moreover, for any uniformizer β of B, we have $B = A[\beta] \cong A[x]/(f(x))$.

Proof. Suppose L/K is totally ramified of degree n. Let β be a generator of the maximal ideal of L. Then $\mu(\beta) = 1/n$. The minimal polynomial $f(x)$ of β is then of degree n and its Newton polygon has a segment of length n and slope $-1/n$. This implies that $f(x)$ is Eisenstein: $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $\mu(a_i) \ge 1$ and $\mu(a_0) = 1$; and $L = K(\beta) \cong K[x]/(f(x))$. Conversely, if $f(x)$ is Eisenstein, then $f(x)$ is irreducible (by the usual proof of Eisenstein's criterion or by Newton polygon) and any root β of $f(x)$ satisfies $\mu(\beta) = 1/n$. Hence $K(\beta)$ is totally ramified of degree n.

Consider now the ring $A[\beta] \cong A[x]/(f(x))$. It suffices to prove that it has a unique maximal ideal and that it is principal, which would imply that $A[\beta]$ is a DVR and so integrally closed. Since $A[\beta]$ is finite over A, by Nakayama's lemma, any maximal ideal $\mathfrak{m}$ of $A[\beta]$ must contain $\mathfrak{p}A[\beta]$ (as $\mathfrak{m} + \mathfrak{p}A[\beta] = A[\beta]$ would imply $\mathfrak{m} = A[\beta]$). Now $A[\beta]/\mathfrak{p}A[\beta] \cong k[x]/(x^n)$ has the unique maximal ideal (x). Hence $\mathfrak{m} = (\mathfrak{p}, \beta) = (\beta)$ is principal. □

For any $f = \sum a_m x^m$ and $g = \sum b_m x^m \in K[x]$ of degree n, we say that f and g are close if $|a_m - b_m|$ is small for every $m = 0, \ldots, n$. Our next main result is that $K[x]/(f(x))$ and $K[x]/(g(x))$ are isomorphic over K if f and g are close enough.

Proposition 2.3.2

(Krasner's Lemma) Suppose K is a non-archimedean complete valued field. Suppose β is algebraic over K and α is separable over $K(\beta)$. Suppose α is closer to β than to any conjugate of α. Then $\alpha \in K[\beta]$.

Proof. Any conjugate of α over $K(\beta)$ is of the form $\sigma(\alpha)$ for some $\alpha : K(\alpha, \beta) \to \bar{K}$ fixing $K(\beta)$. Then

$$|\sigma(\alpha) - \beta| = |\sigma(\alpha - \beta)| = |\alpha - \beta|$$

and so

$$|\sigma(\alpha) - \alpha| = |(\sigma(\alpha) - \beta) - (\alpha - \beta)| \leq |\alpha - \beta|$$

which is only possible if $\sigma(\alpha) = \alpha$. □

Corollary 2.3.3

Suppose K is a non-archimedean complete valued field. Let $f(x)$ be a separable irreducible polynomial in $K[x]$ of degree n. Then for any polynomial $g(x) \in K[x]$ of degree n that is close enough to $f(x)$, g is irreducible and $K[x]/(g(x)) \cong K[x]/(f(x))$.

Proof. We may assume $f(x)$ is monic and factors as $(x - \alpha_1) \cdots (x - \alpha_n)$ over some separable extension of K. Let β be a root of $g(x)$. Then for g close enough to f, $|f(\beta)| = |(f - g)(\beta)|$ is small enough. Hence, one of the $|\beta - \alpha_i|$ can be made smaller than all $|\alpha_j - \alpha_i|$. Krasner's Lemma then implies that $K(\alpha_i) \subset K(\beta)$. Comparing degrees we find that g is irreducible and $K(\alpha_i) = K(\beta)$. □

We can use this result to prove that $\mathbb{C}_p$ is algebraically closed. Fix any irreducible polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{C}_p$. Since $\bar{\mathbb{Q}}_p$ is dense in $\mathbb{C}_p$, there exist $b_i \in \bar{\mathbb{Q}}_p$ close enough to a_i such that $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ is irreducible in $\mathbb{C}_p[x]$. Since $g \in \bar{\mathbb{Q}}_p[x]$ already splits in $\bar{\mathbb{Q}}_p$, we have $n = 1$.

Corollary 2.3.4

Suppose K is a complete discrete valued field of characteristic 0 and finite residue field (i.e. finite extension of $\mathbb{Q}_p$). Then for any positive integer n, there are only finitely many totally ramified extensions of K of degree n up to isomorphism.

Proof. View each Eisenstein polynomial as an element in the compact set $\mathfrak{p} \times \cdots \mathfrak{p} \times (\mathfrak{p} \backslash \mathfrak{p}^2)$. Two elements that are sufficiently close give isomorphic field extensions. Done by compactness. □

In characteristic p, there could be infinitely many totally ramified extensions of degree p. Consider $K = \mathbb{F}_p((t))$ with $\mu(t) = 1$ and Artin-Schreier extensions of the form $K_n = K[x]/(x^p - x - t^{-n})$ for any positive integer n not divisible by p. Then K_n/K is Galois with Galois group $\mathbb{Z}/p\mathbb{Z}$. The conjugate of any root α of $x^p - x - t^{-n}$ are $\alpha, \alpha+1, \ldots, \alpha+(p-1)$ which all have the same valuation and multiply to t^{-n}. Hence $\mu(\alpha) = -n/p$. Since $p \nmid n$, we see that K_n/K is totally ramified. Now given any positive n, m with $p \nmid nm$, it follows from general facts about Artin-Schreier extensions (or bash-able) that if there do not exist $a, a' \in \mathbb{F}_p^\times$ and $b \in K$ such that $at^{-n} - a't^{-m} = b^p - b$, then the extensions K_n/K and K_m/K are not isomorphic. Indeed, any such b must have negative valuation, but then $\mu(b^p) < \mu(b)$ so $\mu(b^p - b) = \mu(b^p) = p\mu(b)$ but $\mu(at^{-n} - a't^{-m}) = \min\{-n, -m\}$ is not divisible by p.

§2.4 Totally tamely ramified extensions

A finite extension L/K of discrete valued fields with separable residue field extension is: **tamely ramified** if $\operatorname{char}(k) \nmid e$; **wildly ramified** if $\operatorname{char}(k) \mid e$. We have a very nice description for the totally tamely ramified extensions.

Theorem 2.4.1

Totally and tamely ramified extensions of a complete discrete valued field K of degree e with $\operatorname{char}(k) \nmid e$ are all of the form $K[x]/(x^e - \pi)$ for some uniformizer π of K.

Proof. It is clear that any extension of the form $K(\sqrt[e]{\pi})$ is totally and tamely ramified since $\sqrt[e]{\pi}$ is a root of $x^e - \pi$ which is Eisenstein. Suppose now L/K is totally and tamely ramified of degree e. By (the proof of) Theorem **??**, we know that $L = K(\beta)$ for some uniformizer β for L. The minimal polynomial of β is of the form $x^e + a_{e-1}x^{e-1} + \cdots + a_1x + a_0$ where $\mu(a_i) \geq 1$ and a_0 is a uniformizer. Then

$$\beta^e = -a_0 - a_1\beta - \cdots - a_{e-1}\beta^{e-1}.$$

Let $\pi = -a_0$. We see that

$$|\beta^e - \pi| < |\pi| = |\beta|^e.$$

Consider $f(x) = x^e - \pi$. We will use Krasner's Lemma to prove that $f(x)$ has a root in $K(\beta) = L$, which would imply that $L = K[x]/(x^e - \pi)$ since L is generated by any uniformizer. Let $\alpha_1, \ldots, \alpha_e$ denote the roots of $f(x)$. Then they all have the same valuation as β and

$$|\beta|^e > |\beta^e - \pi| = |\beta - \alpha_1| \cdots |\beta - \alpha_e|.$$

By renaming, suppose $|\beta - \alpha_1| < |\beta| = |\alpha_1|$. Now since $|e| = 1$, we have

$$|f'(\alpha_1)| = |\alpha_1|^{e-1} = |\alpha_2 - \alpha_1| \cdots |\alpha_e - \alpha_1|.$$

Hence all $|\alpha_i - \alpha_1| = |\alpha_1| > |\beta - \alpha_1|$. Hence $\alpha_1 \in K(\beta)$ by Krasner's Lemma. □

Corollary 2.4.2

Suppose L/K is a totally ramified extension of a complete discrete valued field of degree e. Let $p = \operatorname{char}(k)$ and let $e' = e/\gcd(e, p^\infty)$. Then there exists a tamely ramified extension T/K contained in L of degree e'.

Proof. This follows from the above proof. Let $d = \gcd(e, p^\infty)$. After getting $|\beta^e - \pi| < |\beta|^e$, we let $\beta' = \beta^d$ and consider $f(x) = x^{e'} - \pi$. Let $L' = K(\beta')$ and the same proof above implies that L' contains a subfield T isomorphic to $K[x]/(x^{e'} - \pi)$, which is tamely ramified of degree e'. □

Example: Consider $L = \mathbb{Q}_p(\zeta_{p^m})$ and $K = \mathbb{Q}_p$. The minimal polynomial of ζ_{p^m} is

$$\Phi_{p^m}(x) = \frac{x^{p^m} - 1}{x^{p^{m-1}} - 1} = x^{(p-1)p^{m-1}} + x^{(p-2)p^{m-1}} + \cdots + x^{p^{m-1}} + 1 \equiv (x-1)^{(p-1)p^{m-1}} \bmod p.$$

Then $\Phi_{p^m}(x+1) \equiv x^{(p-1)p^{m-1}} \pmod p$ and $\Phi_{p^m}(1) = p$. Hence $\Phi_{p^m}(x+1)$ is an Eisenstein polynomial and so $L = \mathbb{Q}_p(\zeta_{p^m} - 1)$ is totally ramified of degree $(p-1)p^{m-1}$ with uniformizer $\beta = \zeta_{p^m} - 1$. We have

$$|(\zeta_{p^m} - 1)^{(p-1)p^{m-1}} - (-p)| < |p|.$$

When $m = 1$, the extension is tamely ramified and we have $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p((-p)^{1/(p-1)})$. Note since $\mathbb{Q}_p$ contains all the $(p-1)$-th roots of unities, $\mathbb{Q}_p((-p)^{1/(p-1)})$ is Galois over $\mathbb{Q}_p$. In general, for $m > 1$, $\mathbb{Q}_p(\zeta_p)$ is the tame part of $\mathbb{Q}_p(\zeta_{p^m})$. We note that it is very important that p is a uniformizer in K for this example.
Exercise: Find a finite extension K of $\mathbb{Q}_3$ such that $K(\zeta_3)/K$ is not totally ramified.

Corollary 2.4.3

Suppose $\mathrm{char}(k) \nmid e$. For any $a \in K$ with $\gcd(e, \mu(a)) = 1$, the polynomial $x^e - a \in K[x]$ is irreducible and the extension $K[x]/(x^e - a)$ is totally and tamely ramified of degree e.

Proof. From the Newton polygon, we see that the roots of $x^e - a$ in $\bar{K}$ all have valuation $\mu(a)/e$. No product of any nonempty proper subset of them can have integer valuation. Hence $x^e - a$ is irreducible. Let $L = K[x]/(x^e - a)$. Then $\mu(a)/e$ is some integer divided by the ramification degree of L. Again from $\gcd(\mu(a), e) = 1$, we see that L/K is totally ramified of degree e, and tame because $\mathrm{char}(k) \nmid e$. □

Corollary 2.4.4

Suppose K is a complete discrete valued field containing all e-th roots of unities where $\mathrm{char}(k) \nmid e$. For any positive integer t, the field $K(\alpha)$ where $\alpha^e = \pi^t$ is tamely ramified over K of degree $e/\gcd(e, t)$, where π is some uniformizer of K.

Proof. Let $d = \gcd(e, t)$. Then $\alpha^{e/d} = \zeta \pi^{t/d}$ for some ζ with $\zeta^d = 1$. Since K contains all e-th roots of unities, there exists some $\zeta_e \in K$ such that $\zeta_e^{e/d} = \zeta$. Then $K(\alpha) = K(\alpha/\zeta_e)$ where $(\alpha/\zeta_e)^{e/d} = \pi^{t/d}$. Since now $\gcd(e/d, t/d) = 1$, we are done by Corollary **??**. □

Remark: Let $p = \mathrm{char}(k)$. Then the subgroup $U_1 = 1 + \pi\mathcal{O}$ has no prime-to-p torsion. Suppose $p \nmid e$. Then the condition $\zeta_e \in K$ is equivalent to $\zeta_e \in k$, which in the case k is finite is equivalent to $e \mid |k| - 1$. Indeed, if $d \mid e$ such that $\zeta_e^d \equiv 1 \pmod \pi$, then $\zeta_e^d \in U_1$ is e/d-torsion, which is impossible. Hence, if $\zeta_e \in K$, then its reduction mod π in k also has order e. Conversely, if $\zeta_e \in k$, then we apply Hensel's lemma to $x^e - 1$ to lift it to K. Note also that in order for $L = K[x]/(x^e - \pi)$ to be Galois, we must have $\zeta_e \in L$, which is equivalent to $\zeta_e \in k$ since L/K is totally ramified and so has the same residue field.

Exercise: Suppose $L/\mathbb{Q}_p$ is a Galois totally and tamely ramified extension of degree e. Prove that $e \mid p-1$ and $\mathrm{Gal}(L/\mathbb{Q}_p) \cong C_e$ is cyclic.
Exercise: Let K be a local field and let n be a positive not divisible by $\mathrm{char}(k)$. How "many" totally ramified extensions of K are there of degree n?

§2.5 Unramified extensions

In Theorem **??**, we saw that in the totally ramified case, where $f(x)$ reduces to $\bar{x}^n$, the ring $A[x]/(f(x))$ is maximal in $K[x]/(f(x))$. This is also true in the other extreme where $f(x)$ reduces to an irreducible polynomial. In other words, when the extension is unramified.

Theorem 2.5.1

Unramified extensions of a complete discrete valued field K of finite degrees are all of the form $K[x]/(f(x))$ for some monic $f(x) \in A[x]$ with $\bar{f}(x) \in k[x]$ irreducible and separable. Moreover, the integral closure of A is $B = A_f = A[x]/(f(x))$.

Proof. Suppose first that L/K is an unramified extension of degree n. Its residue field extension ℓ/k is separable of degree n. By the primitive element theorem, there exists $\alpha \in B$ such that $\ell = k(\bar{\alpha})$ where $\bar{\alpha}$ denotes the image of α in ℓ. Let $f(x) \in A[x]$ denote the minimal polynomial of α. Then $\bar{f}(\bar{\alpha}) = 0$. Hence $f(x)$ has degree n and $L = K[x]/(f(x))$.

Conversely, suppose $f(x) \in A[x]$ is monic with $\bar{f}(x) \in k[x]$ irreducible and separable. Then $f(x)$ is irreducible. Let $L = K[x]/(f(x))$ with residue field ℓ. Let π be a uniformizer of A. Then similar to the totally ramified case, every maximal ideal of A_f contains (π) but $A_f/(\pi) \cong A[x]/(\pi, f(x)) \cong k[x]/(\bar{f}(x))$ which is a field. Hence the unique maximal ideal of A_f is (π) and A_f is a DVR. So $B = A_f$ with maximal ideal $\mathfrak{p}A_f$. Hence L/K is unramified. □

Corollary 2.5.2

Suppose K is a complete discrete valued field. Then a finite unramified extension L/K is Galois if and only if the residue extension is Galois.

Proof. With the above notation, L/K is Galois if and only if L contains all the conjugates of α, which happens if and only if $f(x)$ splits in B if and only if $\bar{f}(x)$ splits in ℓ by Hensel's lemma, if and only if ℓ/k is Galois. □

Suppose now L/K is finite unramified and suppose L'/K is any algebraic extension of K. Denote the corresponding rings and maximal ideals and residue fields by $B, \mathfrak{q}, \ell, B', \mathfrak{q}', \ell'$. Let $\sigma \in \mathrm{Hom}_K(L, L')$ be a field homomorphism $L \to L'$ fixing K. Since $|\sigma(\alpha)| = |\alpha|$ for any $\alpha \in L$ (by the uniqueness of extensions of absolute values), we see that $\sigma(B) \subset B'$ and $\sigma(\mathfrak{q}) \subset \mathfrak{q}'$. Then σ descends to a map on the quotient $\sigma : \ell \to \ell'$ fixing k.

Proposition 2.5.3

Suppose L/K is finite unramified where K is a complete discrete valued field. Suppose L'/K is any algebraic extension of K. The maps $\mathrm{Hom}_K(L, L') \longrightarrow \mathrm{Hom}_A(B, B') \longrightarrow \mathrm{Hom}_k(\ell, \ell')$ defined above are bijections.

Proof. The first map is clearly a bijection. The bijectivity of the second map follows from Theorem **??** and Hensel's lemma. Indeed, let $f(x) \in A[x]$ monic with $\bar{f}(x) \in k[x]$ irreducible and separable such that $B = A[x]/(f(x))$ and $\ell = k[x]/(\bar{f}(x))$. Then $\mathrm{Hom}_A(B, B')$ is in bijection with the set of roots of $f(x)$ in B'. By replacing L' by its intersection with the splitting field of $f(x)$, we may assume it is finite of K. Similarly $\mathrm{Hom}_k(\ell, \ell')$ is in bijection with the set of roots of $\bar{f}(x)$ in ℓ' with the map given by reduction. Since $\bar{f}$ is separable and B' is a complete DVR, every root of $\bar{f}$ in ℓ' lifts uniquely to a root of f in B'. □

Theorem 2.5.4

There is an equivalence of categories between unramified extensions of K and separable extensions of k. Moreover, given any algebraic extension L/K with separable residue field extension ℓ/k, there is a unique intermediate unramified field extension E/K that contains all unramified extensions of K in L. The extension L/E is totally ramified.

Proof. Proposition **??** implies the desired equivalence for finite extensions. The infinite case follows by viewing any infinite algebraic extension as a direct limit of finite extensions. More precisely, suppose ℓ/k is infinite separable. Then we express

$$\ell = \varinjlim_{\ell'/k \text{ finite}} \ell'.$$

For each finite ℓ'/k, we have the associated finite unramified extension L'/K. For any $\ell'_1 \to \ell'_2$ in the direct system, we have the corresponding $L'_1 \to L'_2$. We can now take L as the direct limit of the L'.

For the second statement, let E be the unramified extension of K with residue field ℓ. Identify E as a subfield of L via the identity map $\ell \to \ell$. For any unramified extension K' of K in L, the inclusion map $k' \hookrightarrow \ell$ induces an injection $K' \to E$ that when composed with the inclusion $E \hookrightarrow L$ is the inclusion $K' \hookrightarrow L$. Hence $K' \subset E$. Finally, L/E is totally ramified since their residue fields are equal. □

The maximal unramified extension of K is denoted K^{un}. Its residue field is the separable closure of k with Galois group

$$\mathrm{Gal}(K^{\mathrm{un}}/K) \cong \mathrm{Gal}(k^{\mathrm{sep}}/k).$$

When the residue field $k = \mathbb{F}_q$ is finite (in other words when K is a local field), we can be a lot more precise about their unramified extensions. Since finite extensions of $\mathbb{F}_q$ are all Galois, all finite unramified extensions of K are Galois.

Theorem 2.5.5

Let K be a complete discrete valued field with residue field $k = \mathbb{F}_q$ and characteristic p.

1. For any positive integer n, K has a unique unramified extension L of degree n, given by $K(\zeta_{q^n-1})$. It is Galois with Galois group $\mathbb{Z}/n\mathbb{Z}$, generated by the automorphism σ defined by $\sigma(x) \equiv x^q \pmod{\mathfrak{q}}$ for every $x \in B$. The map σ is called the **Frobenius** element of L/K, denoted $\mathrm{Frob}_{L/K}$.
2. Let m be a positive integer such that $p \nmid m$. Then for any unit $u \in A^\times$, the extension $K(\sqrt[m]{u})/K$ is unramified. When $u = 1$, the extension $K(\zeta_m)/K$ has degree d where d is the smallest positive integer such that $q^d \equiv 1 \pmod{m}$.

Proof. Let L/K be unramified of degree n. Suppose $\bar{\alpha} \in \mathbb{F}_{q^n}$ generates $\mathbb{F}_{q^n}^\times$. Let $\bar{f}$ be the minimal polynomial of $\bar{\alpha}$ over $\mathbb{F}_q$. Then $\deg \bar{f} = n$ and $\bar{f} \mid x^{q^n-1} - 1$. Since $x^{q^n-1} - 1$ is separable, Hensel's lemma implies that $\bar{f}$ lifts to some irreducible $f(x) \in A[x]$ that divides $x^{q^n-1} - 1$ and $\bar{\alpha}$ lifts to some root $\alpha \in B$ of $f(x)$. Then α is a $(q^n - 1)$-th root of unity, primitive because $\bar{\alpha}$ is. Comparing degrees gives $L = K(\alpha) = K(\zeta_{q^n-1})$. It is clearly Galois because all the conjugates of ζ_{q^n-1} are powers of it.

Suppose $p \nmid m$. Let $f(x) \in A[x]$ denote the minimal polynomial of $\sqrt[m]{u}$ over K. Since $f(x)$ is irreducible in $K[x]$, we see that $\bar{f}(x) = g(x)^e$ for some irreducible $g \in k[x]$ and $e \geq 1$. From $f(x) \mid x^m - u$ in $A[x]$, we get $\bar{f}(x) \mid x^m - \bar{u}$ in $k[x]$, which has no repeated factors over $\mathbb{F}_q$ when $p \nmid m$. Hence $e = 1$ and $\bar{f}(x)$ is irreducible. Hence $K(\sqrt[m]{u})/K$ is unramified.

When $u = 1$, we have the better division $f(x) \mid \Phi_m(x)$ where $\Phi_m(x)$ is the m-th cyclotomic polynomial since any element of order m is a root of $\Phi_m(x)$ from the factorization formula $x^m - 1 = \prod_{d \mid m} \Phi_d(x)$. We then have $\bar{f}(x) \mid \Phi_m(x)$ in $k[x]$. In a field of characteristic not dividing m, any root of $\Phi_m(x)$ has multiplicative order m. Indeed, if $\ell \mid m$ is a proper divisor, then we have the factorization

$$x^m - 1 = \Phi_m(x)(x^\ell - 1)G(x)$$

for some $G(x) \in \mathbb{Z}[x]$. Since $x^m - 1$ has no repeated root, we see that $\Phi_m(x)$ and $x^\ell - 1$ can't have a common root. Therefore, the residue field extension is $\mathbb{F}_q(\zeta_m)/\mathbb{F}_q$. Finally, we note that $\mathbb{F}_q(\zeta_m) = \mathbb{F}_{q^d}$ where d is the smallest positive integer such that $\mathbb{F}_{q^d}^\times$ contains a cyclic group of order m. □

Adjoining p-power roots of unities will result in a totally ramified extension if the base field is unramified over $\mathbb{Q}_p$, similar to what we did previously for $\mathbb{Q}_p$ where the important ingredient is that p is a uniformizer so that $\Phi_{p^m}(x + 1)$ is Eisenstein.

Proposition 2.5.6

Let p be a prime and m be any positive integer. Let $K/\mathbb{Q}_p$ be an unramified extension. Then $K(\zeta_{p^m})/K$ is totally ramified of degree $(p - 1)p^{m-1}$ and Galois group $(\mathbb{Z}/p^m\mathbb{Z})^\times$. When $m = 1$, $K(\zeta_p)/K$ is totally and tamely ramified and in fact $K(\zeta_p) = K((-p)^{1/(p-1)})$.

Proof. For each $n \in (\mathbb{Z}/p^m\mathbb{Z})^\times$, the map $\zeta_{p^m} \mapsto \zeta_{p^m}^n$ is a K-autmorphism of $K(\zeta_{p^m})$ and by comparing sizes, we have $\mathrm{Gal}(K(\zeta_{p^m})/K) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$. □

Remark: It is possible for $K(\zeta_p)/K$ to be a nontrivial unramified extension. As an example, consider $p = 3$ and $K = \mathbb{Q}_3(\sqrt{3})$, which is a quadratic totally ramified extension of $\mathbb{Q}_3$. The polynomial x^2+1 is irreducible (and separable) over $\mathbb{F}_3$ and so $L = K[x]/(x^2+\sqrt{3}x+1)$ is unramified over K of degree 2. Let $\beta \in L$ be the image of x. Then

$$(\sqrt{3}\beta+1)^3 = 3\sqrt{3}\beta^3 + 9\beta^2 + 3\sqrt{3}\beta + 1 = 3\sqrt{3}\beta(\beta^2+\sqrt{3}\beta+1)+1 = 1.$$

Hence $\sqrt{3}\beta+1 = \zeta_3$ and $L = K(\zeta_3)$ is unramified over K. Note that since ζ_3 is secretly $\sqrt{-3}$, we have $K(\zeta_3) = K(\sqrt{-1}) = K(\zeta_4)$ is unramified over K.

We now have a fairly nice decomposition of a finite extension L/K of a complete discrete valued field with separable residue field extension into

$$K \subset E \subset T \subset L$$

where

1. E/K is unramified of degree f with residue field ℓ/k, generated by ζ_{q^f-1} if $k = \mathbb{F}_q$;
2. T/E is totally and tamely ramified of degree $e' = e/\gcd(e, p^\infty)$, generated by some $\beta \in T$ where $\beta^{e'}$ is some uniformizer of E;
3. L/T is totally and wildly ramified of degree e/e'.

When L/K is infinite, we have the same tower where E is the maximal unramified extension of K in L from Theorem **??**. The maximal tamely ramified extension T of K exists by the following result.

Proposition 2.5.7

Let E be a finite extension of a complete discrete valued field K.

1. If $E \supset F \supset K$, then E/K is unramified/tamely ramified/totally ramified if and only if E/F and F/K are.
2. If E/K is unramified/tamely ramified and L is a finite extension of K, then EL/L is unramified/tamely ramified.
3. If E_1/K and E_2/K are both unramified/tamely ramified, then so is E_1E_2/K.

Proof. The first statement follows from the obvious multiplicative property of e (and f):

$$e_{E/K} = e_{E/F}e_{F/K}, \qquad f_{E/K} = f_{E/F}f_{F/K}.$$

The third statement follows from the first two. We prove the second statement first when E/K is unramified. In this case, we have $E = K(\alpha)$ where the minimal polynomial $f(x) \in A[x]$ of α satisfy $\bar{f}(x) \in k[x]$ irreducible. Let ℓ_E denote the residue field of E. Then $\ell_E = k(\bar{\alpha})$. Let ℓ denote the residue field of L and let $\bar{g}(x)$ be the minimal polynomial of $\bar{\alpha}$ over ℓ. We have the factorization $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$ of coprime polynomials, which lifts to a factorization $f(x) = g(x)h(x)$ in $B[x]$ where B is the integral closure of A in L. Since $\bar{h}(\bar{\alpha}) \neq 0$, we have $h(\alpha) \neq 0$. Hence $g(\alpha) = 0$. Since $\bar{g}(x)$ is irreducible, we see that $g(x) \in L[x]$ is irreducible and $EL = L(\alpha)$ is unramified over L.

It remains to consider the case where E/K is tamely ramified. Since we have proved the result for unramified extensions, we may assume E/K is totally and tamely ramified of degree e. By Theorem **??**, we know $E = K(\alpha)$ where $\alpha^e = \pi$ is some uniformizer of K. Let ω be a uniformizer of L and write $\pi = u\omega^t$ for some unit u in B. Now $EL = L(\alpha)$ where $\alpha^e = u\omega^t$. Let $L' = L(\sqrt[e]{u}, \zeta_e)$, which is unramified by Theorem **??** and the earlier result about unramified extensions. It suffices to prove that $L'(\alpha)/L'$ is tame, for then $L'(\alpha)/L$ is tame and so $L(\alpha)/L$ is tame. Now $L'(\alpha) = L'(\alpha/\sqrt[e]{u})$ where $(\alpha/\sqrt[e]{u})^e = \omega^t$ and L' contains all e-th roots of unities. We are done by Corollary **??**. □

The Remark right after Theorem **??** implies that these properties do not hold for totally ramified extensions. Recall that $K = \mathbb{Q}_3(\sqrt{3})$ is totally ramified over $\mathbb{Q}_3$. The field $K' = \mathbb{Q}_3(\zeta_3)$ is also totally ramified over $\mathbb{Q}_3$. However, $KK' = K(\zeta_3)$ is unramified over K.

We saw that finite totally ramified and unramified extensions are monogenic, in the sense that $B = A[\beta]$ for some $\beta \in B$. In fact, the same is true for all finite extensions of complete discrete valued fields with separable residue extensions.

Proposition 2.5.8

Let L/K be a finite extension of a complete discrete valued field K with separable residue extension ℓ/k. Then the integral closure of A in L is monogenic.

Proof. Let $\beta \in B$ such that its reduction $\bar{\beta}$ in ℓ generates ℓ over k. Let $f(x) \in A[x]$ be a monic polynomial such that $\bar{f}(x) \in k[x]$ is the minimal polynomial of $\bar{\beta}$. Since ℓ/k is separable, we know that $f'(\beta) \in B^\times$ is a unit. Let ω be a uniformizer for B. If $\mu_L(f(\beta)) \geq 2$, then $f(\beta + \omega) \equiv \omega f'(\beta) \pmod{\omega^2}$ has valuation 1. By replacing β by $\beta + \omega$ if necessary, we may assume $f(\beta)$ is a uniformizer of B. It is now easy to see that $B = A[\beta]$ (by Nakayama for example). □

We can now be explicit about the maximal unramified E. Suppose $B = A[\beta]$ for some $\beta \in L$. Let $f(x) \in A[x]$ be the minimal polynomial of β over K. Since $f(x)$ is irreducible, we see that $\bar{f} = \bar{g}^e$ for some irreducible $\bar{g}(x) \in k[x]$. Now

$$B/\pi B \cong A[x]/(f(x), \pi) \cong k[x]/(\bar{g}^e).$$

Hence the residue field ℓ for L is then isomorphic to $k[x]/(\bar{g})$. Lift $\bar{g}$ arbitrarily to a monic polynomial $g \in A[x]$ and Hensel lift some root of $\bar{g}$ in ℓ to $\beta' \in B$. We then have an embedding from the unramified extension $E = K[x]/(g(x))$ to L sending x to β'. The extension L/E is totally ramified of degree e.

Exercise: Find an example of an irreducible $f(x) \in \mathbb{Z}_p[x]$ such that $\bar{f} = \bar{g}^e$ for some irreducible $\bar{g} \in \mathbb{F}_p[x]$ but the ramification degree of $\mathbb{Q}_p[x]/(f(x))$ over $\mathbb{Q}_p$ is not e.

§2.6 Local Kronecker-Weber

We can now prove the local Kronecker-Weber theorem.

Theorem 2.6.1

Every finite abelian extension of $\mathbb{Q}_p$ lies in a cyclotomic field $\mathbb{Q}_p(\zeta_n)$.

Proof. Firstly, we easily reduce to the case of cyclic extensions of prime powers degree since every abelian extension is a compositum of linearly disjoint cyclic extensions of prime powers degree. We consider the tame case first. Suppose $K/\mathbb{Q}_p$ is finite abelian and tamely ramified. Let E be the maximal unramified subextension. Then $K = E(\pi^{1/e})$ for some uniformizer π of E. Write $\pi = (-p)u$ for some unit u in E, which is possible since p is a uniformizer of E. Then $K(u^{1/e}) = E(u^{1/e}, (-p)^{1/e})$. Now $E(u^{1/e})$ is unramified over E and so also over $\mathbb{Q}_p$. Since unramified extensions are cyclotomic, we have

$$E(u^{1/e}, (-p)^{1/(p-1)}) = E(u^{1/e}, \zeta_p) = \mathbb{Q}_p(\zeta_m, \zeta_p)$$

for some m of the form $p^f - 1$. It thus remains to prove that $e \mid p-1$. The extension $K(u^{1/e})/\mathbb{Q}_p$ is abelian, as the compositum of the abelian extensions K and $E(u^{1/e})$. The subextension $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is then Galois, implying that $\zeta_e \in \mathbb{Q}_p$ and so $e \mid p-1$.

It remains to consider the case where $K/\mathbb{Q}_p$ is cyclic of degree p^r for some positive integer r. Suppose first that $p > 2$. Let $K_1 = \mathbb{Q}_p(\zeta_{p^{p^r}-1})$ and $K_2 = \mathbb{Q}_p(\zeta_{p^{r+1}})$. Then K_1 is unramified with Galois group $\mathbb{Z}/p^r\mathbb{Z}$ and K_2 is totally ramified with Galois group $\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$, and we expect $K \subseteq K_1K_2$. Suppose for contradiction that K is not contained in K_1K_2. Then

$$\mathrm{Gal}(KK_1K_2/\mathbb{Q}_p) \hookrightarrow (\mathbb{Z}/p^r\mathbb{Z}) \times (\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/p^r\mathbb{Z})$$

with order more than $p^r \cdot p^r(p-1)$. This means that $\mathbb{Q}_p$ has an abelian extension with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$.

If $p = 2$, we need to take $K_2 = \mathbb{Q}_2(\zeta_{2^{r+2}})$ so that $\mathrm{Gal}(K_2/\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$. Then if K is not contained in K_1K_2, we have

$$\mathrm{Gal}(KK_1K_2/\mathbb{Q}_2) \hookrightarrow (\mathbb{Z}/2^r\mathbb{Z}) \times (\mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^r\mathbb{Z})$$

with order more than $2^r \cdot 2^{r+1}$. This means that $\mathbb{Q}_2$ has an abelian extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$.

You will prove in HW3, with the help of some Kummer theory, that these extensions of $\mathbb{Q}_p$ and $\mathbb{Q}_2$ do not exist. □

Local class field theory gives a correspondence between open subgroups N of $K^\times$ of finite index and finite abelian extensions L of K. Under this correspondence, $N = N_{L/K}(L^\times)$ and $\mathrm{Gal}(L/K) \cong K^\times/N_{L/K}(L^\times)$. From the decompositions

$$\begin{aligned} \mathbb{Q}_p^\times &\cong \mathbb{Z} \times \langle \zeta_{p-1} \rangle \times \mathbb{Z}_p, \quad \text{for } p > 2, \\ \mathbb{Q}_2^\times &\cong \mathbb{Z} \times \langle -1 \rangle \times \mathbb{Z}_2, \end{aligned}$$

we see that

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times p} \cong (\mathbb{Z}/p\mathbb{Z})^2, \qquad \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^3, \qquad \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 4} \cong (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z}).$$

Hence $\mathbb{Q}_p^\times$ and $\mathbb{Q}_2^\times$ do not contain finite index subgroups with the desired quotients.

As a consequence of the local Kronecker-Weber, we see that the maximal abelian extension of $\mathbb{Q}_p$ has the form

$$\mathbb{Q}_p^{\mathrm{ab}} = \varinjlim_f \mathbb{Q}_p(\zeta_{p^f-1}) \cdot \varinjlim_n \mathbb{Q}_p(\zeta_{p^n}).$$

The first direct limit is the maximal unramified extension $\mathbb{Q}_p^{\mathrm{un}}$ of $\mathbb{Q}_p$. Taking Galois groups gives

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \cong \varprojlim_f \mathbb{Z}/f\mathbb{Z} \times \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \hat{\mathbb{Z}} \times \mathbb{Z}_p^\times,$$

which is the profinite completion of $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$. There is a natural reciprocity map

$$\phi : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$$

sending $p^m u$, where u is a unit, to the automorphism that acts as Frob^m on $\mathbb{Q}_p^{\mathrm{un}}$ and sends ζ_{p^n} to $\zeta_{p^n}^u$ on $(\mathbb{Q}_p)_p = \varinjlim \mathbb{Q}_p(\zeta_{p^n})$. Computing the image of the norm map gives

$$\begin{aligned} N(\mathbb{Q}_p(\zeta_{p^f-1})^\times) &= p^{f\mathbb{Z}} \times \mathbb{Z}_p^\times, \\ N(\mathbb{Q}_p(\zeta_{p^n})^\times) &= p^{\mathbb{Z}} \times (1 + p^n\mathbb{Z}_p). \end{aligned}$$

The first equality is a general fact about finite unramified extensions, which follows from the fact that the norm and trace are surjective on finite fields. The second equality actually follows from a general construction in the proof of local class field theory! If we compare these norm groups to the action of $\phi(p^m u)$, we see that there is some norm compatibility result:

$$\phi(a)|_L = \mathrm{id}_L \quad \Longleftrightarrow \quad a \in N_{L/\mathbb{Q}_p}(L^\times).$$

The construction of the totally ramified component $(\mathbb{Q}_p)_p$ for a general local field of characteristic 0 is the meat of Lubin-Tate theory, recalling that we can no longer naively adjoin p-power roots of unities.

The maximal tamely ramified extension $\mathbb{Q}_p^{\mathrm{tr}}$ is obtained from $\mathbb{Q}_p^{\mathrm{un}}$ by adjoining e-th roots of p for positive integers e not divisible by p. These are Kummer extensions with Galois group $\mathbb{Z}/e\mathbb{Z}$ as $\mathbb{Q}_p^{\mathrm{un}}$ contains all e-th roots of unities for $p \nmid e$. So we have

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{tr}}/\mathbb{Q}_p^{\mathrm{un}}) \cong \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z} = \prod_{q \neq p} \mathbb{Z}_q.$$

The wild ramification is more complicated. Iwasawa (On Galois Groups of Local Fields 1955) proved that $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{tr}})$ is the pro-p completion of the free group on countably many generators. Here the pro-p completion of any group G is the inverse limit of G/N over normal subgroups N where G/N is a finite p-group. All of the above are true for any finite extension of $\mathbb{Q}_p$, namely for any local field with mixed characteristic. In general, it is known to be topologically finitely presented with known generators and relations.

§2.7 Ramification groups

Suppose K is a complete discrete valued field and L be a finite Galois extension of K with Galois group G. Suppose the residue extension ℓ/k is separable. Let E be the maximal unramified extension in L/K. Let A, B, A_E be the valuation rings of K, L and E.

Recall that we have the natural maps

$$\mathrm{Hom}_K(L, L) \longrightarrow \mathrm{Hom}_A(B, B) \longrightarrow \mathrm{Hom}_k(\ell, \ell).$$

We also know that $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(\ell/k)$. By extending any K-automorphism of E to a K-automorphism of L, we have the surjection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$. Its kernel is the **inertia group**, $I_{L/K}$:

$$I_{L/K} = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(b) \equiv b \pmod{\mathfrak{q}}, \forall b \in B\} \cong \mathrm{Gal}(L/E).$$

Proposition 2.7.1

There is a short exact sequence

$$1 \to I_{L/K} \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k) \to 1.$$

The maximal unramified extension E is the fixed field of the inertia group $I_{L/K}$.

If $\mathrm{char}(k) = 0$, then $T = L$. If $\mathrm{char}(k) = p$, then T is the maximal extension of E in L with $[L : T]$ equal to the largest p-power divisor of $[L : E]$. In other words, $\mathrm{Gal}(L/T)$ is the Sylow p-subgroup of $I_{L/K}$.

To understand the inertia group $I_{L/K}$ better, we fix a uniformizer π of L, which automatically generates B as an A_E-algebra. Then we have the map $\theta_0 : I_{L/K} \to B^\times$ via $\theta_0(\sigma) = \sigma(\pi)/\pi$. The group of units $B^\times$ has a filtration

$$B^\times = U_0 \supset U_1 \supset U_2 \supset \cdots$$

where $U_i = 1 + \mathfrak{q}^i$ for $n \geq 1$, with

$$B^\times/U_1 \cong \ell^\times \qquad \text{and} \qquad U_i/U_{i+1} \cong \mathfrak{q}^i/\mathfrak{q}^{i+1} \cong \ell.$$

The **ramification** group $R_{L/K}$ is defined to be $\theta_0^{-1}(U_1)$. More generally, we define all the **higher ramification** groups: for any integer $i \geq 0$,

$$\begin{aligned} G_i &= \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(b) \equiv b \pmod{\mathfrak{q}^{i+1}}, \forall b \in B\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma \text{ acts trivially on } B/\mathfrak{q}^{i+1}\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(\beta) \equiv \beta \pmod{\mathfrak{q}^{i+1}}\} \end{aligned}$$

where $\beta \in B$ is any element with $B = A[\beta]$, which exists by Proposition **??**. Then by definition, we have

$$I_{L/K} = G_0.$$

It is easy to see that each G_i is a normal subgroup of G: for any $\sigma, \tau \in \mathrm{Gal}(L/K)$, we have

$$\sigma(\beta) \equiv \beta \pmod{\mathfrak{q}^{i+1}} \implies \tau\sigma\tau^{-1}(\tau(\beta)) \equiv \tau(\beta) \pmod{\mathfrak{q}^{i+1}}.$$

Now for any $\sigma \in G_0$, since σ fixes A_E the integral closure of A in E, and $B = A_E[\pi]$, we have for any $i \geq 1$,

$$\begin{aligned} G_i &= \{\sigma \in G_0 \colon \sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{i+1}}\} \\ &= \{\sigma \in G_0 \colon \sigma(\pi)/\pi \equiv 1 \pmod{\mathfrak{q}^{i}}\} \\ &= \theta_0^{-1}(U_i). \end{aligned}$$

Note that if $\sigma \in G_i$ and $u \in B^\times$, then from $\sigma(u) \equiv u \pmod{\mathfrak{q}^{i+1}}$, we have $\sigma(u)/u \in U_{i+1}$. Hence, θ_0 induces a map

$$\theta_i : G_i/G_{i+1} \to U_i/U_{i+1}$$

which does not depend on the choice of π. It then follows that θ_i is an injective group homomorphism. As a consequence, we have

$$G_0/G_1 \hookrightarrow \ell^\times \qquad \text{and} \qquad G_i/G_{i+1} \hookrightarrow \ell.$$

Proposition 2.7.2

The group G_0/G_1 is cyclic, mapped isomorphically by θ_0 to a subgroup of the group of roots of unities in $\ell^\times$ of order prime to $\mathrm{char}(k)$. Moreover:

1. If $\mathrm{char}(k) = 0$, then $G_1 = \{1\}$;
2. If $\mathrm{char}(k) = p$, then G_1 is the Sylow p-subgroup of G_0 and has a filtration where the quotients are $\mathbb{Z}/p\mathbb{Z}$.

In particular, the maximal tamely ramified extension T is the fixed field of $G_1 = R_{L/K}$.

Proof. In the characteristic 0 case, ℓ has no nontrivial finite subgroup. In the characteristic p case, ℓ is an $\mathbb{F}_p$-vector space and so all of its (additive) subgroups are products of $\mathbb{Z}/p\mathbb{Z}$. □

Corollary 2.7.3

All finite Galois extensions of K are solvable.

Remark: The fact that a totally and tamely ramified Galois extension is cyclic (as G_0/G_1 is cyclic) also follows from Kummer theory. If $L = K[x]/(x^e - \pi)$ is Galois over K, then $\zeta_e \in L$. Since $p \nmid e$, we know $K(\zeta_e)/K$ is unramified and so $\zeta_e \in K$ since L/K is totally ramified. Hence by Kummer theory, $K(\sqrt[e]{\pi})/K$ is cyclic. Note since ζ_e is a unit, it also follows that the residue field k contains ζ_e and so $e \mid |k| - 1$.

As another application of the filtration on the units, we have the following result.

Proposition 2.7.4

Suppose the residue field k is finite. Then there are finitely many totally and tamely ramified extensions of K of degree e. When the residue field k is separably closed, the totally and tamely ramified extension of K of degree e is unique.

Proof. We know that totally and tamely ramified extensions of K of degree e are all of the form $K[x]/(x^e - \pi)$ for some uniformizer π of K. If two uniformizers π_1, π_2 in K satisfy $\pi_1/\pi_2 \in A^{\times e}$, then $K[x]/(x^e - \pi_1)$ and $K[x]/(x^e - \pi_2)$ are isomorphic. Since $p \nmid e$, we have $A^\times/A^{\times e} \cong k^\times/k^{\times e}$ is finite. When k is separably closed, this set is trivial. □

Example 1: Let's compute the ramification groups in the example of $L = K[x]/(x^p - x - t^{-n})$ where $K = \mathbb{F}_p((t))$ and $p \nmid n$. Since L/K is a degree p extension, there is an integer $s \geq 1$ such that $G_s = \mathbb{Z}/p\mathbb{Z}$ and $G_{s+1} = \{1\}$. We prove that $s = n$. Let α denote the image of x. Then $\mu_K(\alpha) = -n/p$ and so $\mu_L(\alpha) = -n$. Let π denote a uniformizer of L. Now G is generated by σ where $\sigma(\alpha) = \alpha + 1$ and

$$\frac{\sigma(\alpha^{-1})}{\alpha^{-1}} = \frac{\alpha}{\alpha+1} = 1 - \frac{1}{\alpha+1} \in U_n \backslash U_{n+1}.$$

On the other hand $\alpha^{-1} = \pi^n u$ for some unit $u \in B^\times$. We have $\sigma(u)/u \in U_{s+1}$ and $\sigma(\pi)/\pi \in U_s \backslash U_{s+1}$. Since $p \nmid n$, we see that $(\sigma(\pi)/\pi)^n \in U_s \backslash U_{s+1}$. Therefore,

$$\frac{\sigma(\alpha^{-1})}{\alpha^{-1}} = \left(\frac{\sigma(\pi)}{\pi}\right)^n \frac{\sigma(u)}{u} \in U_s \backslash U_{s+1}.$$

Thus, $s = n$. This gives another proof that the fields L for different n are non-isomorphic.
Example 2: As another example, consider the ramification groups of $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$. We saw before that $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ is totally ramified of degree $(p-1)p^{n-1}$ and Galois group $G = G_0 = (\mathbb{Z}/p^n\mathbb{Z})^\times$. For any $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, we write σ_a for the Galois element sending ζ_{p^n} to $\zeta_{p^n}^a$. For any $m \le n$, we have the subfield $\mathbb{Q}_p(\zeta_{p^m}))$ with Galois group

$$G(m) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^m})) = \{\sigma_a \in G\colon a \equiv 1 \pmod{p^m}\}.$$

Let μ_m denote the normalized valuation on $\mathbb{Q}_p(\zeta_{p^m}))$ so that $\mu_m(\zeta_{p^m} - 1) = 1$ for $m = 1, \ldots, n$. Fix any $\sigma_a \neq 1$ in G. We compute

$$\mu_n(\sigma_a(\zeta_{p^n} - 1) - (\zeta_{p^n} - 1)) = \mu_n(\zeta_{p^n}^a - \zeta_{p^n}) = \mu_n(\zeta_{p^n}^{a-1} - 1).$$

Let $v \ge 0$ be the largest integer such that $a \equiv 1 \pmod{p^v}$. In other words, $a \in G(v)\backslash G(v+1)$. Then $\zeta_{p^n}^{a-1}$ is a primitive p^{m-v}-th root of unity. Hence

$$\mu_n(\zeta_{p^n}^{a-1} - 1) = p^v \mu_{n-v}(\zeta_{p^{n-v}} - 1) = p^v.$$

In other words, we have, for any integer $v = 0, \ldots, n-1$,

$$G_{p^{v-1}} = G_{p^{v-1}+1} = \cdots = G_{p^v - 1} = G(v), \qquad \text{and} \qquad G_{\ge p^{n-1}} = 1.$$

We remark that all of the above remain true if $\mathbb{Q}_p$ is replaced by an unramified extension of $\mathbb{Q}_p$ by Proposition **??**, recalling that the key is that p is a uniformizer so $\Phi_{p^n}(x+1)$ is Eisenstein.

Note that $(p-1)p^{v-1}$ of the ramification groups G_u equal $G(v)$ and $G/G(v) \cong (\mathbb{Z}/p^v\mathbb{Z})^\times$ has size $(p-1)p^{v-1}$. One is then lead to the conjecture that the number of ramification groups that equal some fixed nontrivial (normal) subgroup H of G is divisible by $[G : H]$. This is true for abelian extensions, known as the Hasse-Arf theorem! In HW 3, you will explore a Q_8-extension (not a typo!) where

$$G_0 = G_1 = Q_8 \qquad \text{and} \qquad G_2 = G_3 = \{\pm 1\} \qquad \text{and} \qquad G_4 = \{1\}.$$

Here there are only 2 ramification groups with index 4.

§2.8 Upper numbering ramification groups

Let K be complete discrete valued field and let L/K be a finite Galois extension with separable residue extension. Let A and B denote the valuation rings of K and L respectively. We know that $B = A[\beta]$ for some $\beta \in B$. We let $i_G(\sigma) = \mu_L(\sigma(\beta) - \beta)$ for any $\sigma \in G = \mathrm{Gal}(L/K)$ so that the ramification groups G_i have the property that

$$i_G(\sigma) = i + 1 \Longleftrightarrow \sigma \in G_i \backslash G_{i+1}.$$

Now if H is a subgroup of G, then H is the Galois group of some L/K' and $i_G(\sigma) = i_H(\sigma)$. Hence we have

$$H_i = H \cap G_i.$$

In other words, the lower numbering ramification groups behave well with subgroups. However, they are not convenient when it comes to quotients.

Proposition 2.8.1

Suppose H is normal. Let $M = L^H$ be the fixed field of H. Then for any $\sigma \in G$,

$$i_{G/H}(\sigma H) = \frac{1}{e_{L/M}} \sum_{\tau \in H} i_G(\sigma\tau) = \frac{1}{\# H_0} \sum_{\tau \in H} i_G(\sigma\tau).$$

Proof. Let C denote the integral closure of A in M. Let $\gamma \in C$ be such that $C = A[\gamma]$. We see that it suffices to prove that

$$\mu_L(\sigma(\gamma) - \gamma) = \mu_L\left(\prod_{\tau \in H} (\sigma\tau(\beta) - \beta)\right),$$

since then dividing by $e_{L/M} = \# H_0$ gives the desired result. Let $f(x) \in C[x]$ be the minimal polynomial of β over C. Then

$$f(x) = \prod_{\tau \in H} (x - \tau(\beta)).$$

For any $f(x) = c_d x^d + \cdots c_0 \in C[x]$, we write

$$f^\sigma(x) = \sigma(c_d)x^d + \cdots + \sigma(c_0).$$

Note that every coefficient of $f^\sigma - f$ is of the form $\sigma(c) - c$ for some $c \in C$. Since $C = A[\gamma]$, we see that every coefficient of $f^\sigma - f$ is divisible by $\sigma(\gamma) - \gamma$ in C. Hence $\sigma(\gamma) - \gamma$ divides $f^\sigma(\beta) - f(\beta)$ in B where

$$f^\sigma(\beta) - f(\beta) = f^\sigma(\beta) = \prod_{\tau \in H} (\beta - \sigma\tau(\beta)).$$

For the other division, let $g(x) \in A[x]$ such that $\gamma = g(\beta)$. Then $g(x) - \gamma \in C[x]$ vanishes at β and so

$$g(x) - \gamma = f(x)h(x)$$

for some $h(x) \in C[x]$. Note that $g^\sigma = g$ since $g \in A[x]$. Apply σ and then set $x = \beta$ gives

$$\gamma - \sigma(\gamma) = f^\sigma(\beta) \cdot h^\sigma(\beta)$$

which gives the division in B in the other direction. □

There is a family of subgroups of G where the ramification groups behave well with quotients.

Corollary 2.8.2

Suppose $H = G_j$ for some $j \geq 0$. Then $(G/H)_i = G_i/H$ for all $i \leq j$ and $(G/H)_i = \{1\}$ for all $i > j$.

Proof. Take any $\sigma \in G \backslash H$. Then $i_G(\sigma) < i_G(\tau)$ for any $\tau \in H$ since $H = G_j$, and so

$$i_G(\sigma\tau) = \mu_L(\sigma\tau\beta - \beta) = \mu_L(\sigma(\tau\beta - \beta) + \sigma\beta - \beta) = i_G(\sigma)$$

since

$$\mu_L(\sigma(\tau\beta - \beta)) = \mu_L(\tau\beta - \beta) = i_G(\tau) > i_G(\sigma).$$

Since $H \subset G_0$, we have $H_0 = H$. Then by Proposition **??**, we have $i_{G/H}(\sigma H) = i_G(\sigma)$. Hence $(G/H)_i = G_i/H$ for all $i \leq j$; and for $i > j$, $(G/H)_i \subset (G/H)_j = \{1\}$. □

Note that we proved that:

$$i_G(\sigma\tau) \geq \min\{i_G(\sigma), i_G(\tau)\}, \text{ with equality if } i_G(\sigma) \neq i_G(\tau).$$

Suppose now H is a general normal subgroup of G, it is still reasonable to expect that for any integer $v \geq 0$, $(G/H)_v = G_uH/H$ for some integer $u \geq 0$. For example, when $v = 0$, $(G/H)_0$ corresponds to the maximal unramified extension of K in M, which is the same as M intersecting with the maximal unramified extension of K in L. So $(G/H)_0 = G_0H/H$. For any $\sigma \in G\backslash H$, let

$$j(\sigma) = \max_{\tau\in H} i_G(\sigma\tau).$$

Then

$$\begin{aligned} \sigma H \in G_uH/H &\iff j(\sigma) - 1 \geq u \\ \sigma H \in (G/H)_v &\iff i_{G/H}(\sigma H) - 1 \geq v. \end{aligned}$$

Suppose $i_G(\sigma) = j(\sigma)$. Then for any $\tau \in H$, if $i_G(\tau) < i_G(\sigma)$, then $i_G(\sigma\tau) = i_G(\tau)$; if $i_G(\tau) \geq i_G(\sigma)$, then $j(\sigma) \geq i_G(\sigma\tau) \geq i_G(\sigma) = j(\sigma)$. In both cases, we have

$$i_G(\sigma\tau) = \min\{i_G(\tau), j(\sigma)\}.$$

Hence, we have

$$i_{G/H}(\sigma H) = \frac{1}{\#H_0}\sum_{\tau\in H} \min\{i_G(\tau), j(\sigma)\}.$$

Note this formula implies that $i_{G/H}(\sigma H)$ can be expressed as an increasing function in $j(\sigma)$. We define for any real number $u \geq -1$, and any finite Galois extension L/K,

$$\varphi_{L/K}(u) = \frac{1}{\#G_0}\left(\sum_{\sigma\in G} \min\{i_G(\sigma), u+1\}\right) - 1 = \frac{1}{\#G_0}\sum_{\sigma\in G_0} \min\{i_G(\sigma) - 1, u\}.$$

Then $\varphi_{L/K}$ is a piece-wise linear non-decreasing function and for any integer $u \geq -1$,

$$G_uH/H = (G/H)_{\varphi_{L/M}(u)}.$$

Proposition 2.8.3

Let $u \geq -1$ be any real number. Let m be an integer such that $m \leq u < m+1$. Prove that

$$\varphi_{L/K}(u) = \frac{1}{\#G_0}(\#G_1 + \cdots + \#G_m + (u-m)\#G_{m+1}).$$

In other words, $\varphi_{L/K}(-1) = -1$, is piece-wise linear, with slopes $\#G_{m+1}/\#G_0$ in $[m, m+1]$.

Proof. (Proof by staring.) Since $\varphi_{L/K}(-1) = -1$ is clear and $\varphi_{L/K}$ is piece-wise linear, it suffice to prove the slope statement. Let $u \in (m, m+1)$ be a non-integer. Then $\min\{i_G(\sigma) - 1, u\} = u$ if and only if $i_G(\sigma) - 1 \geq m+1$ if and only if $\sigma \in G_{m+1}$. □

Example: Consider the extension $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$. We computed earlier that $G_0 = (\mathbb{Z}/p^n\mathbb{Z})^\times$ and

$$G_{p^{v-1}} = G_{p^{v-1}+1} = \cdots = G_{p^v-1} = G(v) = 1 + p^v\mathbb{Z}/p^n\mathbb{Z}$$

with index $(p-1)p^{v-1}$ in G_0 for $v \geq 1$. Working out φ, we find that $\varphi(p^v - 1) = v$ for $v = 0, 1, 2, \ldots$ and is piecewise linear joining them. In the case of the Q_8-extension with $G_0 = G_1 = Q_8$ and $G_2 = G_3 = \{\pm 1\}$ and $G_4 = 1$, we have $\varphi(1) = 1$ and $\varphi(3) = 3/2$.

Lemma 2.8.4

If $\varphi_{L/K}(u) \in \mathbb{Z}$, then $u \in \mathbb{Z}$.

Proof. If $v = \varphi_{L/K}(u) \in \mathbb{Z}$, then

$$(u-m)\#G_{m+1} = v\#G_0 - (\#G_1 + \cdots + \#G_m)$$

but every term on the right hand side is divisible by $\#G_{m+1}$. □

The Hasse-Arf theorem states that the points where the slopes change are all lattice points (points with both coordinates integers). This is equivalent to our conjecture earlier that the number of ramification groups equal to H is divisible by the index $[G:H]$.

Theorem 2.8.5

(Hasse-Arf) If G is abelian and $G_u \neq G_{u+1}$, then $\varphi_{L/K}(u) \in \mathbb{Z}$.

It is common to define G_u for any real number $u \geq -1$ by $G_u = G_{\lceil u \rceil}$ and $G_{-1} = G$. We define the **upper numbering** ramification groups by

$$G^v = G_u \qquad \text{where} \qquad v = \varphi_{L/K}(u).$$

Note that Lemma **??** implies that if $v \in \mathbb{Z}$, then $u \in \mathbb{Z}$. The Hasse-Arf theorem implies that if G is abelian, then G^v and G^{v+1} (when $v \in \mathbb{Z}$) are either equal, or are two consecutive ramification groups and so G^v/G^{v+1} is a subgroup of $\{1\}$, $\ell^\times$ or ℓ.

The advantage of the upper numbering is that

$$G^{\varphi_{L/K}(u)}H/H = G_uH/H = (G/H)_{\varphi_{L/M}(u)} = (G/H)^{\varphi_{M/K}(\varphi_{L/M}(u))}$$

Proposition 2.8.6

For any $u \geq -1$,

$$\varphi_{L/K}(u) = \varphi_{M/K}(\varphi_{L/M}(u)).$$

Therefore (Herbrand's Theorem) for any $v \geq -1$,

$$(G/H)^v = G^vH/H.$$

Proof. Since both sides are piecewise linear and start at $(-1,-1)$. It suffices to prove the two sides have the same slopes at non-integer points. Suppose $u \notin \mathbb{Z}$ and $v = \varphi_{L/M}(u)$. Note that $v \notin \mathbb{Z}$. Then the derivative of the right hand side is

$$\frac{\#(G/H)_v}{e_{M/K}} \cdot \frac{\#H_u}{e_{L/M}} = \frac{\#(G_uH/H)\cdot\#(G_u \cap H)}{e_{L/K}} = \frac{\#G_u}{e_{L/K}}$$

which equals the derivative of the left hand side. □

The fact that the upper numbering ramification groups behave well with quotients means that we can define them for infinite Galois extensions. Let L/K be an infinite

Galois extension. Let $\Sigma(L/K)$ denote the set of intermediate fields F such that F/K is finite Galois. We have

$$\begin{aligned}\mathrm{Gal}(L/K) &= \varprojlim_{F\in\Sigma(L/K)} \mathrm{Gal}(F/K) \\ &= \{(\sigma_F) \in \prod_{F\in\Sigma(L/K)} \mathrm{Gal}(F/K) \colon \sigma_{F_1}|_{F_1\cap F_2} = \sigma_{F_2}|_{F_1\cap F_2}\}.\end{aligned}$$

If we give each $\mathrm{Gal}(F/K)$ the discrete topology and the product the product topology, then the image of $\mathrm{Gal}(L/K)$ is closed and so is compact by Tychonoff's Theorem. Pulling back this topology gives the Krull topology on $\mathrm{Gal}(L/K)$, where a basis of open neighborhood is given by $\sigma\,\mathrm{Gal}(L/F)$ for any $\sigma \in \mathrm{Gal}(L/K)$ and any finite extension F/K. Infinite Galois theory gives a correspondence between the closed subgroups of $\mathrm{Gal}(L/K)$ and intermediate fields E/K. We can then define

$$\begin{aligned}\mathrm{Gal}(L/K)^v &= \varprojlim_{F\in\Sigma(L/K)} \mathrm{Gal}(F/K)^v \\ &= \bigcap_{F\in\Sigma(L/K)} \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma|_F \in \mathrm{Gal}(F/K)^v\}.\end{aligned}$$

Note that they are all closed in $\mathrm{Gal}(L/K)$.
Example: Consider $(\mathbb{Q}_p)_p = \varinjlim \mathbb{Q}_p(\zeta_{p^n})$. We have for $v \geq 1$,

$$\begin{aligned}\mathrm{Gal}((\mathbb{Q}_p)_p/\mathbb{Q}_p) &\cong \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times, \\ \mathrm{Gal}((\mathbb{Q}_p)_p/\mathbb{Q}_p)^v &\cong \varprojlim(1+p^v\mathbb{Z}/p^n\mathbb{Z}) \cong 1+p^v\mathbb{Z}_p.\end{aligned}$$

We can give another proof of the local Kronecker-Weber theorem using Hasse-Arf!

Proposition 2.8.7

Suppose that $L/\mathbb{Q}_p$ is abelian, totally ramified and contains $(\mathbb{Q}_p)_p$. Then $L = (\mathbb{Q}_p)_p$.

Proof. It suffices to assume $L/(\mathbb{Q}_p)_p$ is finite. Let $G = \mathrm{Gal}(L/\mathbb{Q}_p)$ and $H = \mathrm{Gal}(L/(\mathbb{Q}_p)_p)$. Then we have for any integers $v \geq 0$

$$1+p^v\mathbb{Z}_p \cong (G/H)^v = G^vH/H \cong G^v/(G^v\cap H).$$

From the following commuting diagram with exact rows and injective vertical maps

$$\begin{tikzcd} 1 \arrow[r] & G^{v+1}\cap H \arrow[r] \arrow[d] & G^{v+1} \arrow[r] \arrow[d] & 1+p^{v+1}\mathbb{Z}_p \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & G^v\cap H \arrow[r] & G^v \arrow[r] & 1+p^v\mathbb{Z}_p \arrow[r] & 1 \end{tikzcd}$$

we have

$$\#(G^v/G^{v+1}) = \#(G^v\cap H/G^{v+1}\cap H)\cdot\begin{cases} p-1 & \text{if } v=0, \\ p & \text{if } v\geq 1.\end{cases}$$

In particular, the groups G^v have finite index in G. Hence their fixed field is some finite extension E_v/K with $\mathrm{Gal}(E_v/K)^v = \{1\}$. Moreover,

$$\begin{aligned}G^v/G^{v+1} &= \bigcap_{F\in\Sigma(L/\mathbb{Q}_p)} \{\sigma\in\mathrm{Gal}(E_{v+1}/\mathbb{Q}_p) \colon \sigma|_F \in \mathrm{Gal}(F/\mathbb{Q}_p)^v\} \\ &\hookrightarrow \mathrm{Gal}(E_{v+1}/\mathbb{Q}_p)^v/\,\mathrm{Gal}(E_{v+1}/\mathbb{Q}_p)^{v+1} \\ &\hookrightarrow \begin{cases} \mathbb{F}_p^\times & \text{if } v=0, \\ \mathbb{F}_p & \text{if } v\geq 1,\end{cases}\end{aligned}$$

where the last inclusion uses Hasse-Arf. Hence, we see that for all $v \geq 0$,

$$G^v \cap H = G^{v+1} \cap H.$$

However, $H \subset G_0 = G^0$ and so $H \subset G^v$ for all $v \geq 0$. Therefore, $H = 1$ since $\bigcap_v G^v = 1$ as any $\sigma \in \bigcap_v G^v$ is trivial on any finite F/K. □

Corollary 2.8.8

(Local Kronecker-Weber) We have $\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p^{\text{un}} \cdot (\mathbb{Q}_p)_p$.

Proof. Extend the automorphism that acts as Frobenius on $\mathbb{Q}_p^{\text{un}}$ and identity on $(\mathbb{Q}_p)_p$ to an automorphism τ on $\mathbb{Q}_p^{\text{ab}}$. Then for any finite abelian extension $M/(\mathbb{Q}_p)_p$, the fixed field of $\tau|_M$ is a totally ramified extension of $\mathbb{Q}_p$ that contains $(\mathbb{Q}_p)_p$, and so is $(\mathbb{Q}_p)_p$ itself by Proposition **??**. In other words, $\text{Gal}(M/(\mathbb{Q}_p)_p) = \langle \tau|_M \rangle$ is cyclic. Now if M_1 and M_2 are two degree n extensions of $(\mathbb{Q}_p)_p$ in $\mathbb{Q}_p^{\text{ab}}$, then since $\text{Gal}(M_1M_2/(\mathbb{Q}_p)_p)$ is cyclic and has a unique subgroup of index n, we see that $M_1 = M_2$. Now the compositum $\mathbb{Q}_p(\zeta_{p^n-1}) \cdot (\mathbb{Q}_p)_p$ is degree n over $(\mathbb{Q}_p)_p$. We conclude that any finite abelian extension $M/\mathbb{Q}_p$ is contained in $\mathbb{Q}_p^{\text{un}} \cdot (\mathbb{Q}_p)_p$ □

§2.9 Discriminant

Suppose L/K is a finite separable extension of a complete discrete valued field K with separable residue extension ℓ/k. Then we know that the valuation ring B is monogenic: there exists $\beta \in B$ such that $B = A[\beta]$. Let $f(x) \in A[x]$ be the minimal polynomial of β. We define the **discriminant** of L/K as the principal ideal

$$\text{Disc}(L/K) = (N_{L/K}(f'(\beta)))$$

We will define the discriminant more generally later and show that they coincide in this case.

To see the independence with β, we let $\sigma_1, \ldots, \sigma_n$ denote the n embeddings of $L = K(\beta)$ into K^{sep}. In other words, they are determined by $\sigma_i(\beta) = \beta_i$ where the polynomial $f(x)$ factors as $\prod_{i=1}^n (x - \beta_i)$ in K^{sep}. The embeddings together define an isomorphism

$$L \otimes_K K^{\text{sep}} \cong (K^{\text{sep}})^n$$

of K^{sep}-vector spaces. The determinant of multiplication by $f'(\beta)$ on L as a K-vector space equals the determinant of multiplication by $(f'(\beta_1), \ldots, f'(\beta_n))$ in $(K^{\text{sep}})^n$. Hence, we have the familiar

$$N_{L/K}(f'(\beta)) = \prod_{i=1}^n f'(\beta_i) = (-1)^{n(n-1)/2} \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} \Delta(f).$$

we can write the discriminant $\Delta(f)$ as the square of the Vandermonde determinant of the $n \times n$ matrix M whose (i,j)-entry is $\sigma_i(\beta^{j-1})$. Now if $\{\alpha_1, \ldots, \alpha_n\}$ is another A-basis for B, and M' is the matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$, then $\det M$ and $\det M'$ differ by a unit in $A^\times$. Then, we also have the usual

$$\text{Disc}(L/K) = (\det(\sigma_i(\alpha_j))^2) = (\det(\text{Tr}_{L/K}(\alpha_i \alpha_j))).$$

If M/L is another finite separable extension with separable residue extension, then

$$\operatorname{Disc}(M/K) = \operatorname{Disc}(L/K)^{[M:L]} N_{L/K}(\operatorname{Disc}(M/L)).$$

This can be checked by bashing out the matrices. We will give a more intrinsic proof when we define discriminants in general later. Note that for any uniformizer ω of L, we have

$$e_{L/K} \cdot \mu_K(N_{L/K}(\omega)) = \mu_L(N_{L/K}(\omega)) = [L:K].$$

Hence, we have

$$N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{L/K}}.$$

Recall that when A is a Dedekind domain with field of fraction K and L/K a finite separable extension, we have the inverse different of the integral closure B over A:

$$\mathcal{D}_{B/A}^{-1} = \{a \in L \colon \operatorname{Tr}_{L/K}(ab) \in A, \forall b \in B\}$$

and the discriminant

$$\operatorname{Disc}(L/K) = \operatorname{Disc}(B/A) = N_{L/K}(\mathcal{D}_{B/A}).$$

When B is monogenic, that is, $B = A[\beta]$ for some $\beta \in B$, from the proof of Theorem **??**, we can compute the inverse different using the basis $\{1, \beta, \dots, \beta^{n-1}\}$ to find

$$\mathcal{D}_{B/A} = (f'(\beta)).$$

Taking norm gives the usual

$$\operatorname{Disc}(L/K) = (\Delta(f)) = (\prod_{i<j}(\beta_i - \beta_j)^2)$$

where $\beta_1, \dots, \beta_n$ denote the conjugates of β, and $\Delta(f)$ is the (polynomial) discriminant of $f(x)$. Let $\sigma_1, \dots, \sigma_n$ denote all the embeddings of L in K^{sep} so that $\beta_i = \sigma_i(\beta)$. Then we can write $\Delta(f)$ as the square of the Vandermonde determinant of the matrix M whose (i,j)-entry is $\sigma_i(\beta^j)$. Now if $\{\alpha_1, \dots, \alpha_n\}$ is another A-basis for B, and M' is the matrix whose (i,j)-entry is $\sigma_i(\alpha_j)$, then $\det M$ and $\det M'$ differ by a unit in $A^\times$. Then, we also have the usual

$$\operatorname{Disc}(L/K) = (\det(\sigma_i(\alpha_j))^2) = (\det(\operatorname{Tr}_{L/K}(\alpha_i\alpha_j))).$$

Proposition 2.9.1

Let M/L be a finite separable extension and let C be the integral closure of A in M. Then

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}, \qquad \operatorname{Disc}(M/K) = \operatorname{Disc}(L/K)^{[M:L]} N_{L/K}(\operatorname{Disc}(M/L)).$$

Proof. Let I be any fractional ideal of C (in M). Then

$$\begin{aligned} I \subset \mathcal{D}_{C/B}^{-1} &\iff \operatorname{Tr}_{M/L}(IC) \subset B \\ &\iff \mathcal{D}_{B/A}^{-1} \operatorname{Tr}_{M/L}(I) \subset \mathcal{D}_{B/A}^{-1} \\ &\iff \operatorname{Tr}_{L/K}(\mathcal{D}_{B/A}^{-1} I) \subset A \\ &\iff \mathcal{D}_{B/A}^{-1} I \subset \mathcal{D}_{C/A}^{-1} \\ &\iff I \subset \mathcal{D}_{B/A}\mathcal{D}_{C/A}^{-1}. \end{aligned}$$

The statement about the discriminants follow from $N_{M/K} = N_{L/K} \circ N_{M/L}$, which follows from the same statement for elements and by localization. □

We will focus on the case K is a complete discrete valued field and when the residue extension ℓ/k is separable. We will see later that the inverse different and the discriminant behave well with respect to localization and completion.

Proposition 2.9.2

Let M/L be a finite separable extension and let C be the integral closure of A in M. Then

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}, \qquad \mathrm{Disc}(M/K) = \mathrm{Disc}(L/K)^{[M:L]} N_{L/K}(\mathrm{Disc}(M/L)).$$

By Proposition **??**, we know that there exists $\beta \in B$ such that $B = A[\beta]$ with minimal polynomial $f(x)$. Then we have:

Lemma 2.9.3

Suppose L/K is unramified. Then $\mathrm{Disc}(L/K) = (1)$.

Proof. In this case, β is a simple root of $f(x)$ and so $f'(\beta)$ is a unit. □

Corollary 2.9.4

Suppose E/K is the maximal unramified extension in L/K. Then

$$\mathrm{Disc}(L/K) = N_{E/K}(\mathrm{Disc}(L/E)).$$

More explicitly, recall that any finite L/K is of the form $L = K[x]/(f(x))$ where $\bar{f} = \bar{g}^e$ for some irreducible $\bar{g}(x) \in k[x]$. Let $E = K[x]/(g(x))$. Then L/E is totally ramified of degree e and E/K is unramified of degree $\deg(\bar{g})$. Suppose $\mathrm{char}(k) \nmid e$ so that the extension is tame. Then we have from the next calculation that $\mathrm{Disc}(L/E) = \mathfrak{p}^{e-1}$ and $\mathrm{Disc}(E/K) = (1)$. Hence we have

$$\mathrm{Disc}(L/K) = N_{E/K}(\mathrm{Disc}(L/E)) = \mathfrak{p}^{\deg(\bar{g})(e-1)}.$$

As an immediate consequence, we see that if $\mathrm{Disc}(L/K)$ is squarefree and $e \geq 2$, then $\deg(\bar{g}) = 1$ and $e = 2$.

Proposition 2.9.5

(Ore's condition) Suppose L/K is totally ramified of degree e. Then $\mathrm{Disc}(L/K) = \mathfrak{p}^m$ with

$$e - 1 + \mu_L((m \bmod e) + 1) \leq m \leq e - 1 + \mu_L(e).$$

We have equality $m = e-1$ if and only if L/K is tamely ramified. Moreover, any m satisfying the above inequality can happen.

Proof. In this case, β is a uniformizer and $f(x)$ is an Eisenstein polynomial $f(x) = x^e + a_{e-1}x^{e-1} + \cdots + a_0$ with $a_i \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. Then

$$f'(\beta) = e\beta^{e-1} + (e-1)a_{e-1}\beta^{e-2} + \cdots + a_1.$$

Note that $\mu_L(ia_i\beta^{i-1}) \geq e$ for all $i = 1, \ldots, e-1$ since each $a_i \in \mathfrak{p} = \mathfrak{q}^e$ and $\mu_L(e\beta^{e-1}) = \mu_L(e) + e - 1$. Hence $\mu_L(f'(\beta)) \geq e - 1$ with equality if and only if $\mu_L(e) = 0$ if and only if $\operatorname{char}(k) \nmid e$.

For the more precise bound, note that $e \mid \mu_L(ia_i)$ and so each $\mu_L(ia_i\beta^{i-1}) \equiv i - 1 \pmod{e}$. In other words, they all have distinct valuations. Hence $\mu_L(f'(\beta)) \leq \mu_L(e\beta^{e-1}) = e - 1 + \mu_L(e)$. For the lower bound, suppose $m \equiv s - 1 \pmod{e}$ for some $s = 1, \ldots, e$. This means that

$$m = \mu_L(f'(\beta)) = \mu_L(sa_s\beta^{s-1}) = \mu_L(s) + \mu_L(a_s) + s - 1.$$

If $s = e$, then this is exactly $e - 1 + \mu_L(s)$. If $s < e$, then $\mu_L(a_s) \geq e$ and we have $m \geq e - 1 + \mu_L(s)$.

The last statement is obvious by choosing a_s to have the correct valuation and all other a_i's to have huge valuations. □

The extension $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ is totally and tamely ramified of degree $p-1$. Hence

$$\operatorname{Disc}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) = (p^{p-2}).$$

What about $\operatorname{Disc}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$? We can use ramification groups!

Corollary 2.9.6

Suppose K is a complete discrete valued field with finite residue field. Then for any integers $e, m \geq 1$, there are only finitely many extensions L of K of degree e and $\mu(\operatorname{Disc}(L/K)) \leq m$.

Proof. From the uniqueness of unramified extensions of any degree, we may consider only the totally ramified case. □

Suppose now L/K is Galois with Galois group G. Then

$$f'(\beta) = \prod_{\sigma \in G, \sigma \neq 1} (\beta - \sigma(\beta)).$$

Recall that $i_G(\sigma) = \mu_L(\sigma(\beta) - \beta)$. Hence, we have

$$\begin{aligned}
\mu_L(f'(\beta)) &= \sum_{\sigma \neq 1} i_G(\sigma) \\
&= 1(|G_0| - |G_1|) + 2(|G_1| - |G_2|) + 3(|G_2| - |G_3|) + \cdots \\
&= |G_0| + |G_1| + \cdots + |G_{m-1}| - m,
\end{aligned}$$

where G_m is the first trivial ramification group.

We apply this to $\operatorname{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Recall that for any $v = 1, \ldots, n-1$, there are $(p-1)p^{v-1}$ ramification groups with index $(p-1)p^{v-1}$. The group G_0 has order $(p-1)p^{n-1}$ and the first trivial ramification group is $G_{p^{n-1}}$. Hence, we have

$$\operatorname{Disc}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = (p^{\phi(p^n)(n - \frac{1}{p-1})}) = (p^{np^n - (n+1)p^{n-1}}).$$

For the funny Q_8 example with $G_0 = G_1 = Q_8$, $G_2 = G_3 = \{\pm 1\}$, $G_4 = 1$, we have

$$\operatorname{Disc}(L/K) = \mathfrak{p}^{16}.$$

Finally consider the example $K_n = K[x]/(x^p - x - t^{-n})$ where $K = \mathbb{F}_p((t))$ and $p \nmid n$. We saw that $G_s = \mathbb{Z}/p\mathbb{Z}$ for $s = 0, \ldots, n$ and $G_{n+1} = \{1\}$. Hence we have

$$\operatorname{Disc}(K_n/K) = (t^{(p-1)(n+1)}).$$

Note that in this case $e = p = 0$ in L so the term $\mu_L(e) = \infty$ in Ore's condition. Note also that since $p \nmid n$, we have $(p-1)(n+1) \not\equiv p - 1 \pmod{p}$, so that $(p-1)(n+1) \bmod p + 1 \neq p$.

Corollary 2.9.7

Suppose K is a complete discrete valued field and L/K is a finite extension with separable residue extension. Let L'/K be the Galois closure. Then

$$\mu_L(\mathcal{D}_{B/A}) = \frac{1}{e_{L'/L}} \sum_{\sigma \in \mathrm{Gal}(L'/K) \setminus \mathrm{Gal}(L'/L)} i_{\mathrm{Gal}(L'/K)}(\sigma).$$

Theorem 2.9.8

Suppose K is a complete discrete valued field. Let $s \geq 0$ be any integer. Then for any positive integer n, there are only finitely many Galois extensions L/K of degree n and $G_s = \{1\}$.

Proof. The condition $G_s = \{1\}$ implies $\mu_L(\mathcal{D}_{B/A}) \leq (n-1)s$ by Proposition **??**. □

§2.10 The mass formula of Serre and Bhargava

In this section, we discuss Serre's beautiful mass formula about the number of totally ramified extensions of a local field K of fixed degree n. Let $\Sigma_n(K)$ denote the set of degree n totally ramified extensions of K contained in (some fixed) K^{sep}. Let $\Sigma_n(K)/\sim$ denote the set of these fields up to K-isomorphisms.

We consider the tame case $p \nmid n$ first, where $p = \mathrm{char}(k)$ and k is finite. We know they are all isomorphic to $K(\sqrt[n]{\pi})$ for some uniformizer π of K. Kummer theory implies that $K(\sqrt[n]{\pi_1})$ and $K(\sqrt[n]{\pi_2})$ are isomorphic over K if and only if $\pi_2/\pi_1 \in K^{\times n}$, provided that K contains all n-th roots of unities. Since adjoining the n-th root of a unit is an unramified extension, the same holds without the assumption of $\zeta_n \in K$. More precisely, suppose $K(\sqrt[n]{\pi_1})$ and $K(\sqrt[n]{\pi_2})$ are isomorphic over K. Then $\sqrt[n]{u} \in K(\sqrt[n]{\pi_1})$ where $u = \pi_2/\pi_1 \in A^\times$. Since $K(\sqrt[n]{u})/K$ is unramified and $K(\sqrt[n]{\pi_1})/K$ is totally ramified, we see that $\sqrt[n]{u} \in K$. In other words, there is a bijection

$$\Sigma_n(K)/\sim \quad \longleftrightarrow \quad A^\times/A^{\times n} \quad \longleftrightarrow \quad k^\times/k^{\times n}.$$

On the other hand, we have the bijection

$$\mathrm{Aut}_K(K(\sqrt[n]{\pi})) \quad \longleftrightarrow \quad A^\times[n] \quad \longleftrightarrow \quad k^\times[n] \quad \longleftrightarrow \quad k^\times/k^{\times n}.$$

In other words, we find that

$$\sum_{L \in \Sigma_n(K)/\sim} \frac{1}{\#\,\mathrm{Aut}_K(L)} = 1.$$

In the general case, we also need to weight by the discriminant. Suppose that $k \cong \mathbb{F}_q$. We write

$$\mathrm{Disc}_q(L/K) = q^{\mu(\mathrm{Disc}(L/K))} = \#(A/\mathrm{Disc}(L/K)).$$

Recall that in the tame case, $\mathrm{Disc}_q(L/K) = q^{n-1}$.

Theorem 2.10.1

Let K be a local field with residue field $\mathbb{F}_q$. Let $n \geq 1$ be a positive integer. Then

$$\sum_{L \in \Sigma_n(K)/\sim} \frac{1}{\# \operatorname{Aut}_K(L)} \frac{1}{\operatorname{Disc}_q(L/K)} = \frac{1}{q^{n-1}},$$

where $\operatorname{Aut}_K(L)$ denote the group of K-automophisms of L.

Remark 1: When counting isomorphism classes, it is standard to weight by the inverse of the size of the stabilizers. We note that every $L \in \Sigma_n(K)$ is isomorphic to $n/\# \operatorname{Aut}_K(L)$ many distinct field extensions of K contained within a fixed separable closure K^{sep}. Hence, we also have

$$\sum_{L \in \Sigma_n(K)} \frac{1}{\operatorname{Disc}_q(L/K)} = \frac{n}{q^{n-1}}.$$

Remark 2: When K has characteristic p, this is an infinite sum. Serre's mass formula then predicts that this sum converges. When K has characteristic 0, we already know this is a finite sum.

Let m_K and m_L denote the normalized Haar measures on K and L. In other words, they are translation invariant normalized so that $m_K(A) = m_L(B) = 1$ and so $m_K(\mathfrak{p}) = q^{-1}$. Let

$$P_n = \mathfrak{p} \times \cdots \times \mathfrak{p} \times (\mathfrak{p} \backslash \mathfrak{p}^2) \subset \mathfrak{p}^n$$

parameterize Eisenstein polynomials over K. Extend m_K to m_K^n on K^n via the product measure. We have

$$m_K^n(P_n) = q^{-n}(1 - q^{-1}).$$

For any $L \in \Sigma_n$, let P_n^L denote the subset of P_n consisting of polynomials f such that $L \cong K[x]/(f(x))$. Then

$$m_K^n(P_n) = q^{-n}(1 - q^{-1}) = \sum_{L \in \Sigma_n(K)/\sim} m_K^n(P_n^L).$$

Note in the case K has positive characteristic, we need to remove the subset of P_n consisting of the inseparable irreducible polynomials, but it is easy to prove that this subset has measure 0. It now suffices to prove that

$$m_K^n(P_n^L) = \frac{1}{\# \operatorname{Aut}_K(L)} \frac{1}{\operatorname{Disc}_q(L/K)} q^{-1}(1 - q^{-1}).$$

We now fix L with valuation ring B and maximal ideal $\mathfrak{q}$. Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of L in K^{sep}. Consider the map

$$\varphi_L : \mathfrak{q} \backslash \mathfrak{q}^2 \to P_n^L$$

defined by

$$\varphi_L(\pi) = N_{L/K}(x + \pi) = \prod_{i=1}^{n} (x + \sigma_i(\pi)).$$

The map φ_L is an $\# \operatorname{Aut}_K(L)$-to-1 surjective map. Indeed, given any $f \in P_n^L$, fix an isomorphism $K[x]/(f(x)) \to L$ and let π denote the image of $-x$. Then $\varphi_L(\pi) = f$. Moreover, two elements $\pi_1, \pi_2 \in \mathfrak{q} \backslash \mathfrak{q}^2$ have the same image if and only if they are conjugate.

Since $m_L(\mathfrak{q}\backslash\mathfrak{q}^2) = q^{-1}(1-q^{-1})$, it remains to compute the Jacobian of φ_L and prove that for any $\pi \in \mathfrak{q}\backslash\mathfrak{q}^2$,

$$\mu(\mathrm{Jac}(\varphi_L)(\pi)) = \mu(\mathrm{Disc}(L/K)).$$

We fix an A-basis $\{e_1, \dots, e_n\}$ for B. This identified L as K^n, B as A^n, and Haar measure m_L as the product measure $m_K \times \cdots \times m_K$. We can extend φ_L to a map $K^n \to K^n$ as the composite of

$$\varphi_1 : (b_1, \dots, b_n) \mapsto (\sigma_1(b_1e_1 + \cdots + b_ne_n), \dots, \sigma_n(b_1e_1 + \cdots + b_ne_n))$$

and

$$\varphi_2 : (x_1, \dots, x_n) \mapsto (x_1 + \cdots + x_n, \dots, x_1 \cdots x_n).$$

We note that

$$\mathrm{Jac}(\varphi_1)(b_1, \dots, b_n) = \det(\sigma_i(e_j))$$

and

$$\mathrm{Jac}(\varphi_2)(x_1, \dots, x_n) = \prod_{i<j}(x_i - x_j).$$

To see the latter formula, note that $\mathrm{Jac}(\varphi_L)(x_1, \dots, x_n)$ is homogeneous of degree $n(n-1)/2$ and vanishes when $x_i = x_j$ for any $i < j$. To find the leading constant, set $x_n = 0$ and apply induction. Suppose now $\pi \in \mathfrak{q}\backslash\mathfrak{q}^2$ corresponds to some $(b_1, \dots, b_n) \in A^n$. Then

$$\mathrm{Jac}(\varphi_L)(\pi) = \det(\sigma_i(e_j)) \cdot \prod_{i<j}(\sigma_i(\pi) - \sigma_j(\pi)).$$

Since $B = A[\pi]$, we know that the square of each factor above generates $\mathrm{Disc}(L/K)$. The proof of Serre's mass formula is now complete.

The map φ_L sending $\alpha \in \mathcal{O}_L$ to the coefficients of $f_\alpha = N_{L/K}(x+\alpha)$ is also of interest when L is a degree n étale K-algebra or when $B \neq A[\alpha]$. That is, when $L \cong K[x]/(f(x))$ for some polynomial $f(x) \in K[x]$ of degree n and nonzero discriminant. In this case, we have

$$\begin{aligned}|\mathrm{Jac}(\varphi_L)(\alpha)| &= |\det(\sigma_i(e_j))| \cdot |\prod_{i<j}(\sigma_i(\alpha) - \sigma_j(\alpha)| \\ &= \frac{1}{\mathrm{Disc}_q(L/K)^{1/2}} \cdot |\Delta(f_\alpha)|^{1/2}.\end{aligned}$$

Let $A_n \cong A^n$ denote the space of monic degree n polynomials in $A[x]$ equipped with the measure m_K^n and let ψ be a measurable function on A_n. For example, ψ could be the characteristic function of the set of polynomial with squarefree discriminant. Then we have

$$\int_{A_n} \psi(f)\, df = \sum_{\substack{[L:K]=n \\ \text{étale}/\sim}} \frac{1}{\#\,\mathrm{Aut}_K(L)} \frac{1}{\mathrm{Disc}_q(L/K)^{1/2}} \int_{\mathcal{O}_L} \psi(f_\alpha) \cdot |\Delta(f_\alpha)|^{1/2} d\alpha.$$

Let's now consider generalizations of Serre's mass formula due to Bhargava. First let's consider all field extensions. Fix positive integers e, f. We write the splitting type $(L/K) = (f^e)$ if $e_{L/K} = e$ and $f_{L/K} = f$. The totally ramified case corresponds to the splitting type (1^n). Let E be the unique unramified extension of degree f over K in K^{sep}. Recall that by Corollary **??** that $\mathrm{Disc}(L/K) = N_{E/K}(\mathrm{Disc}(L/E))$. Since $N_{E/K}(\mathfrak{q}_E) = \mathfrak{p}^f$, we see that

$$\mathrm{Disc}_{q_E}(L/E) = (q^f)^{\mu_E(\mathrm{Disc}(L/E))} = q^{\mu_E(N_{E/K}(\mathrm{Disc}(L/E)))} = \mathrm{Disc}_q(L/K).$$

Since E/K is Galois, any L/K with splitting type (f^e) contains E. Therefore, by Serre's mass formula,

$$\sum_{(L/K)=(f^e)} \frac{1}{\operatorname{Disc}_q(L/K)} = \sum_{(L/E)=(1^e)} \frac{1}{\operatorname{Disc}_{q_E}(L/K)} = \frac{e}{q^{f(e-1)}}.$$

In other words, we have proved:

Proposition 2.10.2

Let K be a local field with residue field $\mathbb{F}_q$. Let e, f be positive integers. Then

$$\sum_{(L/K)=(f^e)/\sim} \frac{1}{\#\operatorname{Aut}(L/K)} \frac{1}{\operatorname{Disc}_q(L/K)} = \frac{1}{f} \frac{1}{q^{f(e-1)}}.$$

An **étale** algebra L over K is a K-algebra that is isomorphic to a finite product of finite separable field extensions of K. If $L \cong K_1 \times \cdots \times K_r$ where each K_i is a finite separable field extension of K with spliting type $f_i^{e_i}$, then we write the splitting type of L/K as $(L/K) = (f_1^{e_1} \cdots f_r^{e_r})$. The discriminant of L/K is the product of the discriminants of K_i/K, since both can be defined using the trace form. Counting isomorphism classes of such L weighted by $\frac{1}{\#\operatorname{Aut}(L/K)}$ is the same as counting ordered products $K_1 \times \cdots \times K_r$ weighted by

$$\frac{1}{\#\operatorname{Aut}(K_1/K)} \cdots \frac{1}{\#\operatorname{Aut}(K_r/K)} \cdot \frac{1}{N},$$

where N denotes the number of permutations of the factors $f_i^{e_i}$ preserving $(f_1^{e_1} \cdots f_r^{e_r})$. For any splitting type $\sigma = (f_1^{e_1} \cdots f_r^{e_r})$, we define

$$\operatorname{Disc}_q(\sigma) = q^{f_1(e_1-1)+\cdots+f_r(e_r-1)}, \qquad \#\operatorname{Aut}(\sigma) = N f_1 \cdots f_r.$$

For example, for $\sigma = (111^2 23333^4)$, $\operatorname{Disc}_q(\sigma) = q^{10}$ and $\#\operatorname{Aut}(\sigma) = 1{\cdot}1{\cdot}1{\cdot}2{\cdot}3{\cdot}3{\cdot}3{\cdot}3{\cdot}2!{\cdot}3! = 1944$. We therefore have:

Proposition 2.10.3

Let K be a local field with residue field $\mathbb{F}_q$. Let σ be a splitting type for a degree n étale algebra of K. Then

$$\sum_{(L/K)=\sigma/\sim} \frac{1}{\#\operatorname{Aut}(L/K)} \frac{1}{\operatorname{Disc}_q(L/K)} = \frac{1}{\#\operatorname{Aut}(\sigma)} \frac{1}{\operatorname{Disc}_q(\sigma)}.$$

We can now prove Bhargava's mass formula using some combinatorics.

Theorem 2.10.4

Let K be a local field with residue field $\mathbb{F}_q$. Then

$$\sum_{[L:K]=n \text{ étale}/\sim} \frac{1}{\#\operatorname{Aut}(L/K)} \frac{1}{\operatorname{Disc}_q(L/K)} = \sum_{k=0}^{n-1} \frac{p(k, n-k)}{q^k},$$

where $p(k, n-k)$ is the number of partitions of k into at most $n-k$ parts.

Proof. Fix any splitting type σ with

$$k = f_1(e_1 - 1) + \cdots + f_r(e_r - 1) \geq 0.$$

The number $\#\operatorname{Aut}(\sigma)$ should look familiar in terms of centralizers of conjugacy classes in symmetric groups. For any $t \geq 0$, let n_t denote the sum of f_i with $e_i - 1 = t$. Note that $n_{k+1} = 0$. Let $\chi_\sigma = (\chi_0, \ldots, \chi_k)$ denote the conjugacy class in $G = S_{n_0} \times \cdots \times S_{n_k}$ where χ_t corresponds to the cycle structure $(f_{i_1}, \ldots, f_{i_s})$ where these are all the f_i with $e_i = t$. Then

$$\#\operatorname{Aut}(\sigma) = \#C_G(\chi_\sigma),$$

where $C_G(\chi_\sigma)$ denotes the centralizer of χ_σ. We write $\pi(\sigma) = (n_0, \ldots, n_k)$. Note that

$$k = n_1 + 2n_2 + \cdots + kn_k$$

is a partition of k into $n_1 + \cdots + n_k \leq n - k$ parts, since

$$k + n_0 + n_1 + \cdots + n_k = \sum_i e_i f_i = n.$$

Conversely, given any partition of k into at most $n - k$ parts, we let n_t be the number of parts equal to t for $t \geq 1$ and let $n_0 = n - k - n_1 - \cdots - n_k \geq 0$. Hence there are $p(k, n-k)$ different $(k+1)$-tuples $(n_0, \ldots, n_k)$ for which there exists a splitting type σ with $\pi(\sigma) = (n_0, \ldots, n_k)$ and $\operatorname{Disc}_q(\sigma) = q^k$. Therefore, by Proposition **??**, it remains to prove that

$$\sum_{\pi(\sigma)=(n_0,\ldots,n_k)} \frac{1}{\#\operatorname{Aut}(\sigma)} = 1.$$

This follows from the above interpretation of $\#\operatorname{Aut}(\sigma)$ as $\#C_G(\chi_\sigma)$. Indeed, as σ vary over all possible splitting types with $\pi(\sigma) = (n_0, \ldots, n_k)$, the conjugacy class χ_σ recovers all conjugacy classes in G. Hence

$$\sum_{\pi(\sigma)=(n_0,\ldots,n_k)} \frac{\#G}{\#\operatorname{Aut}(\sigma)} = \sum_{\chi \subset G \text{ conjugacy class}} \#\chi = \#G.$$

Canceling the $\#G$ completes the proof. □

Corollary 2.10.5

Let K be a local field with residue field $\mathbb{F}_q$. Then

$$\sum_{[L:K]=n \text{ unramified}/\sim} \frac{1}{\#\operatorname{Aut}(L/K)} \frac{1}{\operatorname{Disc}_q(L/K)} = 1.$$

Proof. Unramified étale extensions correspond to splitting types σ with $k = 0$ and $\pi(\sigma) = (n)$. □

We also have similar mass formula for étale extensions of $\mathbb{R}$. Degree n étale extensions of $\mathbb{R}$ are of the form $L \cong \mathbb{R}^{n-2k} \times \mathbb{C}^k$ for some integer $0 \leq k \leq n/2$. For such L, we have $\#\operatorname{Aut}(L/\mathbb{R}) = (n-2k)! \cdot k! \cdot 2^k$. We associate to it the conjugacy class $\chi_{n,k} \subset S_n$ whose cycle structure consists of k 2's so that

$$\#\operatorname{Aut}(L/\mathbb{R}) = \#C_{S_n}(\chi_{n,k}).$$

The union of these $\chi_{n,k}$ over $0 \leq k \leq n/2$ is exactly the set $S_n[2]$ of 2-torsion elements of S_n.

Proposition 2.10.6

We have

$$\sum_{[L:\mathbb{R}]=n \text{ étale}/\sim} \frac{1}{\#\operatorname{Aut}(L/\mathbb{R})} = \frac{\#S_n[2]}{n!}.$$

Using these mass formula, Bhargava gave a conjectured formula for the number $N(S_n, X)$ of S_n-number fields of degree n and absolute discriminant bounded by X:

$$\lim_{X\to\infty} \frac{N(S_n, X)}{X} = \frac{1}{2}\left(\frac{\#S_n[2]}{n!}\right) \cdot \prod_p \left(\frac{p-1}{p} \sum_{k=0}^{n-1} \frac{p(k, n-k)}{p^k}\right).$$

A similar heuristic formula can be written down for extensions of global fields. These have been proven for $n = 2, 3, 4, 5$. The extra factor of $1/2$ can be viewed as coming from that $|\Delta(f_\alpha)|^{1/2}$ in the formula for $|\operatorname{Jac}(\varphi_L)(\alpha)|$ when $K = \mathbb{R}$!

3 Absolute values over Global fields

A **global field** is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$ for some prime p. We began this semester classifying absolute values on $\mathbb{Q}$ and on $\mathbb{F}_p(t)$. What about their extensions? We begin with a lemma that reduces to the case of finite separable extensions.

Lemma 3.0.1

Suppose L is a finite extension of $\mathbb{F}_p(t)$ for some prime p. Then there exists $u \in L$ such that L is finite separable over $\mathbb{F}_p(u)$.

Proof. (Sketch) Let K be a subfield of L that is separable over $\mathbb{F}_p(u)$ for some $u \in L$ and such that $[L : K]$ is minimal. Suppose $K \neq L$. Then let $w \in L \backslash K$ with $w^p \in K$. Prove that u is separable over $\mathbb{F}_p(w)$ and so $K(w)$ is separable over $\mathbb{F}_p(w)$ with $[L : K(w)] < [L : K]$. □

Theorem 3.0.2

Let K be a field with an absolute value $|.|$ and completion $\hat{K}$. Let L/K be a finite separable extension. Then there are finitely many extensions $|.|_1, \dots, |.|_r$ of $|.|$ to L. They correspond to the decomposition

$$L \otimes_K \hat{K} \cong \prod_{i=1}^{r} L_i$$

where each L_i is a finite separable extension of $\hat{K}$ and is the completion of L with respect to $|.|_i$.

Proof. Write $L = K[\beta]$ for some $\beta \in L$. Let $f(x) \in K[x]$ be its minimal polynomial and suppose it factors as $f(x) = g_1(x) \cdots g_r(x)$ into irreducible polynomials in $\hat{K}[x]$. Let $L_i = \hat{K}[x]/(g_i(x))$ for any $i = 1, \dots, r$. Then since L/K is separable,

$$L \otimes_K \hat{K} \cong \hat{K}[x]/(f(x)) \cong \prod_{i=1}^{r} L_i.$$

Suppose $|.|'$ is an absolute value on L extending $|.|$. Let L' denote its completion and let $\iota : L \hookrightarrow L'$ denote the natural embedding. Then $L' = \hat{K}[\iota(\beta)] = \hat{K}(\iota(\beta))$ because $\hat{K}[\iota(\beta)]$ is complete and contains $\iota(L)$ as a dense subset. Let $g(x) \in \hat{K}[x]$ denote the minimal polynomial of $\iota(\beta)$. Then since $f(\iota(\beta)) = 0$, we see that $g = g_i$ for some $i = 1, \dots, r$ and so $L' \cong L_i$.

Conversely, fix some $i = 1, \dots, r$. The absolute value $|.|$ on $\hat{K}$ extends uniquely to $|.|_i$ on $L_i = \hat{K}[x]/(g_i(x))$. We then have an embedding $L \hookrightarrow L_i$ sending β to x. Restricting $|.|_i$ to L then gives an absolute value on L. □

We consider the archimedean absolute values, which only exist for number fields (finite extension of $\mathbb{Q}$). In this case, we have $K = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(f(x))$ for some monic irreducible $f(x) \in \mathbb{Q}[x]$. We factor $f(x)$ in $\mathbb{R}[x]$ into a product of r_1 linear factors and r_2 quadratic factors. Then $r_1 + 2r_2 = n = [K : \mathbb{Q}]$. We have

$$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

There are r_1 real embeddings $\sigma_1, \dots, \sigma_{r_1}$ sending β to a real root of $f(x)$; and $2r_2$ complex embeddings, namely $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ and their complex conjugates, sending β to a complex root of $f(x)$. We define the normalized absolute values by

$$\begin{aligned} ||a||_i &= |\sigma_i(a)|, && \text{for} \quad i = 1, \dots, r_1, \\ ||a||_i &= |\sigma_i(a)|^2, && \text{for} \quad i = r_1 + 1, \dots, r_1 + r_2. \end{aligned}$$

The choice of the normalizations is so that

$$|N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r_1+r_2} ||a||_i.$$

As some concrete examples, we have

- $\mathbb{Q}(\zeta_3) \hookrightarrow \mathbb{C} : \zeta_3 \mapsto \zeta_3$,
- $\mathbb{Q}(\zeta_5) \hookrightarrow \mathbb{C} \times \mathbb{C} : \zeta_5 \mapsto (\zeta_5, \zeta_5^2)$,
- $\mathbb{Q}(\sqrt{2}) \hookrightarrow \mathbb{R} \times \mathbb{R} : \sqrt{2} \mapsto (\sqrt{2}, -\sqrt{2})$.

The ring of integers $\mathcal{O}_K$ of K is isomorphic to $\mathbb{Z}^n$ as an abelian group. Its image in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is then a full rank lattice Λ_K, upon identifying $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ as $\mathbb{R}$-vector spaces.

Proposition 3.0.3

We have
$$|\mathrm{Disc}(K/\mathbb{Q})| = 2^{2r_2}\mathrm{Vol}(\mathbb{R}^n/\Lambda_K)^2 = 2^{2r_2}\mathrm{Disc}(\Lambda_K)^2,$$
where Vol is the usual Euclidean volume.

Proof. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Recall that

$$\mathrm{Disc}(K/\mathbb{Q}) = \det(\sigma_i(\alpha_j))^2.$$

For each $\ell = 1, \dots, r_2$, adding the $r_1 + r_2 + \ell$ row to the $r_1 + \ell$ row turns the $r_1 + \ell$ row into $2\mathrm{Re}(\sigma_{r_1+\ell}(\alpha_j))$. Then subtracting $1/2$ of this new $r_1 + \ell$ row from the $r_1 + r_2 + \ell$ row turns it into $-\mathrm{Im}(\sigma_{r_1+\ell}(\alpha_j))i$. In other words, if we write M for the $n \times n$ matrix whose j-th column is the image of α_j in $\mathbb{R}^n$. Then

$$\det(\sigma_i(\alpha_j)) = \pm(-2i)^{r_2} \det M.$$

We are now done because $|\det(M)|$ is exactly the discriminant of Λ_K. □

Remark: One can get rid of the 2^{2r_2} using a different normalization of $\mathbb{C} \cong \mathbb{R}^2$.

Theorem 3.0.4

The images of $\mathcal{O}_K$ in $\mathbb{R}^{r_1-1} \times \mathbb{C}^{r_2}$ and $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2-1}$ are dense.

For example, we have the familiar density result of $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}$ and $\mathbb{Z}[\zeta_5] \hookrightarrow \mathbb{C}$.

Proof. The key idea is Minkowski's convex body theorem. Take a convex region in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ that is tiny in all but one directions and sufficiently large in that last one direction so that its volume is bigger than $2^n \mathrm{Disc}(\Lambda_K)$. Here we consider each $\mathbb{C}$-factor as "one direction" as well. Then a nonzero $\alpha_0 \in \mathcal{O}_K$ can be found inside.

Fix some v in $\mathbb{R}^{r_1-1} \times \mathbb{C}^{r_2}$ or $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2-1}$ to be approximated. Embed it in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ by setting its remaining coordinate 69. Every point in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is not too far from some lattice points in Λ_K. In other words, there exists a constant C depending only on K such that $|v/\alpha_0 - \alpha|_i < C$ for all i for some $\alpha \in \mathcal{O}_K$. Then $|v - \alpha_0\alpha|_i < C|\alpha_0|_i$ for all i. By choosing our convex body in the beginning so that $|\alpha_0|_i < \epsilon/C$ for all but one i, we have $|v - \alpha_0\alpha|_i < \epsilon$ for all but one i. □

When the absolute value $|.|$ is discrete with valuation ring A, we can also describe the extensions in terms of the splitting of prime ideals. Let B be the integral closure of A. Let $\mathfrak{p}$ denote the (nonzero) prime ideal of A corresponding to $|.|$ so that $\mathfrak{p}$ consists of all $\alpha \in A$ such that $\alpha^n \to 0$ under $|.|$. Any extension $|.|'$ to L extending $|.|$ then defines a prime ideal $\mathfrak{q}$ of B that contains $\mathfrak{p}$. To understand the splitting of prime ideals, we recall some results about Dedekind domains.

A **Dedekind domain** is a Noetherian integrally closed integral domain such that every nonzero prime ideal is maximal. Every PID is Dedekind. In particular, $\mathbb{Z}$ and $\mathbb{F}_p[x]$ are Dedekind domains.

Theorem 3.0.5

Suppose A is a Dedekind domain with field of fraction K. Let L/K be a finite separable extension. Then the integral closure B of A in L is a Dedekind domain.

Proof. We first prove that B is finite over A and so is also Noetherian. This is where separability is used. By the primitive element theorem, $L = K(\beta)$ for some $\beta \in B$. Let $f(x) \in K[x]$ be its minimal polynomial of degree n. Let $\beta_1, \dots, \beta_n$ denote the roots of $f(x)$. The trace $\mathrm{Tr}_{L/K}$ of any $g(\beta) \in L$ is defined as

$$\mathrm{Tr}_{L/K}(g(\beta)) = \sum_{i=1}^{n} g(\beta_i).$$

We have the following interesting formula:

$$\mathrm{Tr}_{L/K}(\beta^j/f'(\beta)) = \begin{cases} 0 & \text{if } j = 0, \dots, n-2, \\ 1 & \text{if } j = n-1, \\ \in A & \text{if } j \geq n. \end{cases}$$

Using partial fraction decomposition, we have

$$\frac{1}{f(T)} = \sum_{i=1}^{n} \frac{1}{f'(\beta_i)(T - \beta_i)}.$$

Expanding both sides as power series in $1/T$ gives

$$\frac{1}{T^n} + \text{ higher order terms} = \frac{1}{T} \sum_{j=0}^{\infty} \frac{\mathrm{Tr}_{L/K}(\beta^j/f'(\beta))}{T^j}.$$

Comparing coefficients when give the above formula. The upshot is that $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is a non-degenerate symmetric bilinear form on L. For any A-module $M \subseteq L$, we define its dual

$$M^\vee = \{a \in L \colon \mathrm{Tr}_{L/K}(ab) \in A \colon \forall b \in M\}.$$

If M is free of full rank, so that an A-basis is also a K-basis of L, its dual is also free of full rank by taking a dual basis. If $M \subseteq B$, then since $\mathrm{Tr}_{L/K}(b) \in A$ for every $b \in B$, we see that $B \subseteq M^\vee$. By taking $M = A[\beta] = \mathrm{Span}_A\{1, \beta, \ldots, \beta^{n-1}\}$, we have

$$B \subseteq M^\vee = \frac{1}{f'(\beta)} A[\beta].$$

Hence B is finite over A.

As the integral closure of A, B is integrally closed. It remains to prove that any nonzero prime ideal $\mathfrak{q}$ of B is maximal. Let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{p}$ is clearly a proper prime ideal. We prove that it is nonzero. Take any $\beta \in \mathfrak{q} - \{0\}$. Let $f(x) \in A[x]$ be its minimal polynomial. Then $f(0) \in \mathfrak{q} \cap A - \{0\}$. Now $B/\mathfrak{q}$ is an integral domain that is algebraic over a field $A/\mathfrak{p}$. Hence $B/\mathfrak{q}$ is a field. □

Remark 1: The separable assumption is needed to ensure that B is finitely generated over A. (Note that since B is integral over A, finitely generated and finite are the same.) Without the separability assumption, it is possible that B is not finitely generated over A (Borevich-Shafarevich [Number Theory] Ex.11 p.205). In general, an (integrally closed) integral domain A with field of fraction K is Japanese if its integral closure B in any finite extension L of K is finitely generated over A. Our argument proves that a Dedekind domain whose fraction field is perfect is Japanese. It is not hard to prove that a complete DVR is also Japanese.

Remark 2: For any $\alpha \in L^\times$, we define a pairing $\langle\ ,\ \rangle_\alpha : L \times L \to K$ by

$$\langle x, y\rangle_\alpha = \mathrm{Tr}_{L/K}(\alpha x y / f'(\beta)).$$

The Gram matrix of the pairing $\langle\ ,\ \rangle_1$ when expressed in the basis $\{1, \beta, \ldots, \beta^{n-1}\}$ has 1's on the antidiagonal and 0's above the antidiagonal. In other words, there is an isometry between the quadratic spaces $(L, \langle\ ,\ \rangle_1)$ and the split quadratic space $(K^n, x^t A_0 y)$ where A_0 is the $n \times n$ matrix with 1's on the antidiagonal and 0's everywhere else. Multiplication by β defines a K-linear operator on L that is self-adjoint with respect to $\langle\ ,\ \rangle_1$:

$$\langle \beta x, y\rangle_1 = \langle x, \beta y\rangle_1 = \langle x, y\rangle_\beta.$$

Under the isometry $L \to K^n$, we then have a self-adjoint operator T on K^n with characteristic polynomial $f(x)$. This is very similar to the construction of the companion matrix, but with the extra condition that it is self-adjoint. The splitness condition is very important, as one recalls that for a positive definition quadratic form on $\mathbb{R}^n$, the characteristic polynomial of a self-adjoint operator splits over $\mathbb{R}$.

It is not hard to check that any non-degenerate symmetric pairing on L for which $\cdot\beta$ is self-adjoint is of the form $\langle\ ,\ \rangle_\alpha$ for some $\alpha \in L^\times$. Clearly two such pairings are equivalent over K if the α's differ by a square in $L^\times$. Suppose now n is odd. In order for $\langle\ ,\ \rangle_\alpha$ to be equivalent to the split quadratic form of discriminant 1, we need $N_{L/K}(\alpha) \in K^{\times 2}$. Hence, we have a bijection between $\mathrm{SO}(A_0)(K)$-orbits of self-adjoint operators with characteristic polynomial $f(x)$ and the subset of $(L^\times/L^{\times 2})_{N=1}$ for which $\langle\ ,\ \rangle_\alpha$ is split. The group $(L^\times/L^{\times 2})_{N=1}$ turns out to be isomorphic to $H^1(K, J[2])$ where $J[2]$ is the 2-torsion group scheme of the Jacobian of the hyperelliptic curve $y^2 = f(x)$, assuming that $\Delta(f) \neq 0$. One can then obtain a bijection between the 2-Selmer group of J and "locally soluble" $\mathrm{SO}(A_0)(K)$-orbits. Counting these orbits then give results on the average sizes of the 2-Selmer groups of Jacobians of hyperelliptic curves.

We now collect some important properties of Dedekind domains A.

- For every nonzero prime ideal $\mathfrak{p}$, the localization $A_\mathfrak{p}$ is a DVR.
- If $M_1 \subseteq M_2$ are A-modules such that $M_1 A_\mathfrak{p} = M_2 A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$, then $M_1 = M_2$. (This is true for any ring.)
- Every ideal I of A contains a finite product of nonzero prime ideals. This implies that it is contained in only finitely many prime ideals. (This is true for any Noetherian rings. Let I be maximal among all ideals that do not contain a product of prime ideals. Then I can't be prime. Let $x, y \in A - I$ with $xy \in I$. Then $I \supset (I + (x))(I + (y))$ but both $I + (x)$ and $I + (y)$ contain a product of prime ideals.)

We define $\mu_\mathfrak{p}(I)$ for any ideal I and any nonzero prime ideal $\mathfrak{p}$ as the non-negative integer such that

$$IA_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^{\mu_\mathfrak{p}(I)}.$$

Then we have the factorization

$$I = \prod_\mathfrak{p} \mathfrak{p}^{\mu_\mathfrak{p}(I)}.$$

We define $\mu_\mathfrak{p}(a)$ for an element $a \in A$ as $\mu_\mathfrak{p}((a))$ or equivalently as $\mu_\mathfrak{p}(a)$ inside the DVR $A_\mathfrak{p}$. Applying this to the ideal $\mathfrak{p}B$ and the Dedekind domain B, we get a factorization

$$\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{\mu_\mathfrak{q}(\mathfrak{p})}.$$

We define the ramification degrees $e_{\mathfrak{q}/\mathfrak{p}}$ and the residue degrees $f_{\mathfrak{q}/\mathfrak{p}}$ by

$$e_{\mathfrak{q}/\mathfrak{p}} = \mu_\mathfrak{q}(\mathfrak{p}) \qquad \text{and} \qquad f_{\mathfrak{q}/\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}].$$

Let $\hat{A}_\mathfrak{p}$ and $\hat{B}_\mathfrak{q}$ denote the completions of $A_\mathfrak{p}$ and $B_\mathfrak{q}$, with field of fractions $K_\mathfrak{p}$ and $L_\mathfrak{q}$. From the Chinese Remainder Theorem, we have

$$B/\mathfrak{p}B \cong \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}} \cong \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}\hat{B}_\mathfrak{q} \cong \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}/\mathfrak{p}\hat{B}_\mathfrak{q}.$$

Taking $\dim_{A/\mathfrak{p}}$ gives

$$n = \dim_{A_\mathfrak{p}}(B \otimes_A A_\mathfrak{p}) = \dim_{A/\mathfrak{p}} B/\mathfrak{p}B = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}.$$

Applying Nakayama's lemma to $\hat{A}_\mathfrak{p}$ gives

$$B \otimes_A \hat{A}_\mathfrak{p} \cong \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}.$$

For any Dedekind domain A and nonzero prime ideal $\mathfrak{p}$, we define the normalized absolute value

$$||a||_\mathfrak{p} = (N\mathfrak{p})^{-\mu_\mathfrak{p}(a)} = \#(A_\mathfrak{p}/(a)) \qquad \text{where} \qquad N\mathfrak{p} = \#(A/\mathfrak{p}).$$

Then similar to the archimedean case, we have

$$||N_{L/K}(a)||_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} ||a||_{\mathfrak{q}}.$$

Using the decomposiion $L \otimes_K K_{\mathfrak{p}} \cong \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$, we have

$$N_{L/K}(a) = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(a).$$

One can then check explicitly that

$$||N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(a)||_{\mathfrak{p}} = ||a||_{\mathfrak{q}}.$$

Remark: We can give a more instrinsic proof of the formula $||N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(a)||_{\mathfrak{p}} = ||a||_{\mathfrak{q}}$ using Haar measures $m_{\mathfrak{q}}$ on $L_{\mathfrak{q}}$ and $m_{\mathfrak{p}}$ on $K_{\mathfrak{p}}$. The normalized absolute value is defined so that for any measurable set E,

$$m_{\mathfrak{q}}(aE) = ||a||_{\mathfrak{q}} m_{\mathfrak{q}}(E).$$

Under the identification $L_q \cong K_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}$ as $K_{\mathfrak{p}}$-vector spaces and $m_{\mathfrak{q}} = m_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}$, we also have

$$m_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}(aE) = ||N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(a)||_{\mathfrak{p}} \cdot m_{\mathfrak{p}}^{[L_{\mathfrak{q}}:K_{\mathfrak{p}}]}(E).$$

Let M_K denote the set of equivalence classes of absolute values of K, also known as the set of "places". We have defined the normalized absolute values $||.||_v$ for each place $v \in M_K$. If v corresponds to a real embedding $\sigma : K \hookrightarrow \mathbb{R}$, then

$$||a||_v = |\sigma(a)|.$$

If v corresponds to a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, then

$$||a||_v = |\sigma(a)|^2.$$

For the non-archimedean v, we have the associated DVR $A_v = \{a \in K\colon |a|_v \leq 1\}$ with maximal ideal $\mathfrak{m}_v = \{a \in K\colon |a|_v < 1\}$ and the normalized $\mathfrak{m}_v$-adic valuation μ_v, all of which are independent on the choice of $|.|_v$. We then define

$$||a||_v = (\#A_v/\mathfrak{m}_v)^{-\mu_v(a)} = \#A_v/(a).$$

Example: For $K = \mathbb{Q}$ and $a = \pm p_1^{k_1} \cdots p_m^{k_m}$, we have

$$||a||_\infty = p_1^{k_1} \cdots p_m^{k_m}, \qquad ||a||_{p_i} = p_i^{-k_i}, \qquad ||a||_p = 1 \text{ for } p \neq p_i.$$

For $K = \mathbb{F}_p(t)$ and some $a(t) \in \mathbb{F}_p[t]$, we have

$$||a||_\infty = p^{\deg a}, \qquad ||a||_{\pi(t)} = (p^{\deg \pi})^{-\mu_\pi(a)}.$$

Note that in both cases, we have the product formula:

$$\prod_{v \in M_K} ||a||_v = 1, \qquad \text{for } a \in K^\times.$$

Suppose now L/K is finite separable. For $w \in M_L$ and $v \in M_K$, we write $w \mid v$ if $||.||_w$ extends some absolute value equivalent to $||.||_v$. The normalizations were chosen so that

$$\prod_{w|v} ||a||_w = ||N_{L/K}(a)||_v.$$

Hence, we have the famous product formula for global fields.

Theorem 3.0.6

Let K be a global field. Then for any $a \in K^{\times}$,

$$\prod_{v \in M_K} ||a||_v = 1.$$

Remark: It is a theorem of Artin-Whaples that the global fields are exactly those where the absolute values can be normalized to satisfy the product formula.

§3.1 Dedekind-Kummer and Discriminant

Let A be a Dedekind domain with field of fraction K. Let L/K be a finite separable extension and let B be the integral closure of A. On writing $L = K(\beta) \cong K[x]/(f(x))$ for some monic irreducible $f(x) \in K[x]$, we see that for any prime ideal $\mathfrak{p}$ of A, the factorization $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ can be read off from the factorization of $f(x)$ over $K_{\mathfrak{p}}$ as $f(x) = f_1(x) \cdots f_r(x)$ where each $\bar{f}_i(x) = g_i(x)^{e_i}$ in $(A/\mathfrak{p})[x]$ with $g_i(x)$ irreducible. The theorem of Dedekind-Kummer allows us to read off the factorization of $\mathfrak{p}B$ from $\bar{f}(x) = g_1^{e_1} \cdots g_r^{e_r}$ directly.

Theorem 3.1.1

(Dedekind-Kummer) Suppose that $\mathfrak{p}B$ is coprime to the ideal $\{a \in B \colon aB \subseteq A[\beta]\}$. Suppose $f(x)$ mod $\mathfrak{p}$ factors as $g_1(x)^{e_1} \cdots g_r(x)^{e_r}$ where $g_i \in (A/\mathfrak{p})[x]$ are distinct irreducible polynomials. Then $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ for some prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ of B with residue degree $f_{\mathfrak{q}_i/\mathfrak{p}} = \deg(g_i)$. Moreover, lifting each $g_i(x)$ arbitrarily to some $h_i(x) \in A[x]$, we have $\mathfrak{q}_i = (\mathfrak{p}, h_i(\beta))$.

Proof. The assumption that $\mathfrak{p}B$ is coprime to $\{a \in B \colon aB \subseteq A[\beta]\}$ implies that

$$B/\mathfrak{p}B = A[\beta]/\mathfrak{p}A[\beta] \cong (A/\mathfrak{p})[x]/(g_1(x)^{e_1} \cdots g_r(x)^{e_r}) =: R.$$

The key idea now is that the factorization of $\mathfrak{p}$ in $\mathcal{O}_K$ can be read off from the ring-theoretic properties of R. Namely, r is the number of maximal ideals of R. For any maximal ideal $\mathfrak{m}$ of R, the residue degree f_i is $[R/\mathfrak{m} : A/\mathfrak{p}]$; and the ramification degree e_i is the smallest positive integer d such that $\mathfrak{m}^d = 0$ in the localization $R_{\mathfrak{m}}$. The explicit description of $\mathfrak{q}_i$ follows from the explicit description of the maximal ideals of R. □

Remark: When $K = \mathbb{Q}$, the coprimeness condition is equivalent to $p \nmid [B : \mathbb{Z}[\beta]]$.
Example 1: Consider the example $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$. The ring of integers $B = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ with the ring $\mathbb{Z}[\sqrt{5}]$ having index 2. We can then use the factorization of $x^2 - 5$ mod p to deduce the splitting of pB for $p \neq 2$. Using quadratic reciprocity, we know that for $p \equiv 1, 4 \pmod 5$, the ideal $(p) = \mathfrak{q}_1\mathfrak{q}_2$ splits; for $p \equiv 2, 3 \pmod 5$, the ideal (p) stays prime; for $p = 5$, the ideal pB ramifies as $(\sqrt{5})^2$. For $p = 2$, we need to use the minimal polynomial of $(1 + \sqrt{5})/2$, which is $x^2 - x - 1$. We see that it is irreducible mod 2 and so (2) stays prime.
Example 2: Consider the Dedekind field $K = \mathbb{Q}[x]/(f(x))$ where $f(x) = x^3 - x^2 - 2x - 8$. It is easy to check that $f(x)$ mod 3 is irreducible and so $f(x) \in \mathbb{Q}[x]$ is irreducible. Mod 2, $\bar{f}(x) = x^2(x - 1)$. We see that the simple root 1 lifts to a root in $\mathbb{Q}_2$. From $f(0) = -8$ and $f'(0) = -2$, we see that 0 lifts to a root in $\mathbb{Q}_2$ that is congruent to 0 mod 4. Hence

$f(x)$ splits completely in $\mathbb{Q}_2$. (Note that $f(-2) = -16$ and $f'(-2) = 14$, so -2 lifts to a root in $\mathbb{Q}_2$ that is congruent to $-2 \bmod 8$.) This means that the ideal (2) splits completely as $\mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ in B. However, there does not exist a monic cubic polynomial $g(x)$ whose reduction mod 2 is a factor of 3 distinct linear polynomials in $\mathbb{F}_2[x]$. Hence for any $\beta \in B$, we have $2 \mid [B : \mathbb{Z}[\beta]]$. In other words, B is not monogenic with a local obstruction at 2. We also say the field K is not monogenic as its ring of integer is not monogenic.

It is conjectured that for $n \geq 3$, 100% of number fields of degree n are not monogenic, when ordered by the absolute value of the discriminant. When counting monogenic cubic fields, we are essentially counting monic polynomials $x^3 + Ax + B \in \mathbb{Z}[x]$ with absolute discriminant $|-4A^3 - 27B^2| < X$. We expect the answer to be on the order of $X^{5/6}$, but proving it is equivalent to counting elliptic curves ordered by discriminant, which is unknown. By counting monic polynomials with squarefree discriminant, we produced $X^{1/2+1/n}$ monogenic number fields of degree n and we expect this to be the correct order of magnitude for them. By counting binary n-ic forms with squarefree discriminant, we produced $X^{1/2+1/(n-1)}$ number fields of degree n, which has a higher order of magnitude that $1/2 + 1/n$.

We know give the proper definition of the discriminant of a finite separable extension L/K of global fields. We define first the ideal norm.

Let A be a Dedekind domain with field of fraction K. Let L be a finite dimensional K-vector space and let M and N be two sub-A-lattices. In other words, they are sub-A-modules locally free of rank $\dim_K L$. We first define their ideal index $[M : N]_A$. If they are free over A, then there is some K-linear isomorphism $T : L \to L$ sending M to N and we define $[M : N]_A = (\det T)$. In general, since the localizations $A_\mathfrak{p}$ are all PID, we define $[M : N]_A$ to be the fractional ideal of A such that

$$[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}} = [M : N]_A A_\mathfrak{p}.$$

Now if L/K is a finite separable extension with ring of integer B, we define the ideal norm

$$N_{B/A}(I) = [B : I]_A.$$

It then follows from the definition that for any $\alpha \in L^\times$,

$$N_{B/A}(\alpha B) = N_{L/K}(\alpha)A.$$

It is also easy to see that the ideal norm is multiplicative by checking it locally.

Lemma 3.1.2

If $N \subseteq M$ and $M/N \cong A/I_1 \times \cdots \times A/I_m$ as A-modules, then $[M : N]_A = I_1 \cdots I_m$.

Proof. We work locally over $A_\mathfrak{p}$. Fix bases for $M_\mathfrak{p}$ and $N_\mathfrak{p}$ and let $T \in M_{n\times n}(A_\mathfrak{p})$ sending $M_\mathfrak{p}$ to $N_\mathfrak{p}$. Since $A_\mathfrak{p}$ is a PID, we have (from the Smith normal form) $T = UDV$ where $U, V \in \mathrm{GL}_n(A_\mathfrak{p})$ and D is diagonal with entries $\pi^{d_1}, \ldots, \pi^{d_n}$ where π is some fixed uniformizer of $A_\mathfrak{p}$. Then we have

$$\begin{aligned} M_\mathfrak{p}/N_\mathfrak{p} &\cong A_\mathfrak{p}/\mathfrak{p}^{d_1} \times \cdots \times A_\mathfrak{p}/\mathfrak{p}^{d_n} \\ &\cong A_\mathfrak{p}/\mathfrak{p}^{\mu_\mathfrak{p}(I_1)} \times \cdots \times A_\mathfrak{p}/\mathfrak{p}^{\mu_\mathfrak{p}(I_m)}. \end{aligned}$$

Hence we see that $d_1 + \cdots + d_n = \mu_\mathfrak{p}(I_1) + \cdots + \mu_\mathfrak{p}(I_m)$. In other words, $(\det D) = (I_1 \cdots I_m)A_\mathfrak{p}$. □

Corollary 3.1.3

We have $N_{B/A}(\mathfrak{q}) = [B : \mathfrak{q}]_A = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$. As a consequence $N_{B/A}(\mathfrak{p}B) = \mathfrak{p}^{[L:K]}$. Recall that the same is true for $N_{L_\mathfrak{q}/K_\mathfrak{p}}(\mathfrak{q})$.

Proof. Follows immediately from $B/\mathfrak{q} \cong (A/\mathfrak{p})^{f_{\mathfrak{q}/\mathfrak{p}}}$ as $A/\mathfrak{p}$-vector spaces. □

Recall that we have a non-degenerate symmetric trace pairing on L. Suppose $L = K(\beta)$ for some $\beta \in B$. Let $f(x) \in A[x]$ be the minimal polynomial of β and let $C = A[\beta]$. Then its dual

$$C^\vee = \{a \in L\colon\ \mathrm{Tr}_{L/K}(ab) \in A, \forall b \in C\} = \frac{1}{f'(\beta)}C.$$

Hence we have

$$[C^\vee : C]_A = (N_{L/K})(f'(\beta)).$$

We saw last time that there are examples where $B \neq C$. We define the **different** $\mathcal{D}_{B/A}$ as the (fractional) ideal of B such that

$$\mathcal{D}_{B/A}^{-1} = \{a \in L\colon\ \mathrm{Tr}_{L/K}(ab) \in A, \forall b \in B\} = B^\vee.$$

The (relative) **discriminant** of B over A is defined as the ideal norm of $\mathcal{D}_{B/A}$:

$$\mathrm{Disc}(L/K) = N_{B/A}(\mathcal{D}_{B/A}) = [B^\vee : B]_A.$$

If $B = C = A[\beta]$ is monogenic, then we have

$$\mathcal{D}_{B/A} = (f'(\beta)) \qquad \text{and} \qquad \mathrm{Disc}(L/K) = (N_{L/K}(f'(\beta)).$$

Theorem 3.1.4

We have

$$\mathrm{Disc}(L/K) = \prod_{\mathfrak{q}} \mathrm{Disc}(L_\mathfrak{q}/K_\mathfrak{p}).$$

We need to check that taking dual behaves well with respect to localization and completion. Localization is straightfoward. Let $S \subseteq A$ be multiplicatively closed. Then for any $s \in S$ and any $a \in L$,

$$\mathrm{Tr}_{L/K}(sa) = s\mathrm{Tr}_{L/K}(a).$$

Hence for any sub-A-module M of L, we have

$$(S^{-1}M)^\vee = S^{-1}M^\vee.$$

Note that if $T : M_\mathfrak{p} \to N_\mathfrak{p}$, then its adjoint $T^* : N_\mathfrak{p}^\vee \to M_\mathfrak{p}^\vee$ where the adjoint is defined with respect to the trace pairing:

$$\langle x, Ty\rangle = \mathrm{Tr}_{L/K}(x(Ty)) = \mathrm{Tr}_{L/K}((T^*x)y) = \langle T^*x, y\rangle.$$

In terms of matrices, we have $T^* = A_0^{-1}T^tA_0$, where A_0 is a Gram matrix for the pairing, so it has the same determinant as T. Hence, we see that

$$[M : N]_A = [N^\vee : M^\vee]_A.$$

In particular, when applied to $M = B$ and $N = C = A[\beta]$, we have

$$[C^\vee : C]_A = [B^\vee : B]_A [B : C]_A^2.$$

Hence if $N_{L/K}(f'(\beta))$ is squarefree, we see that $B = A[\beta]$.

Completion also works as expected. Since $A_\mathfrak{p}$ is a PID, we can take an $A_\mathfrak{p}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for $B_\mathfrak{p}$. Let $\{w_1, \ldots, w_n\}$ be its dual basis in $B_\mathfrak{p}^\vee = B^\vee \otimes A_\mathfrak{p}$. Then $\{\alpha_1, \ldots, \alpha_n\}$ is also an $\hat{A}_\mathfrak{p}$-basis for $B \otimes \hat{A}_\mathfrak{p}$. Under the decomposition

$$B \otimes \hat{A}_\mathfrak{p} \cong \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q} \hookrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q} \cong L \otimes_K K_\mathfrak{p},$$

the trace $\mathrm{Tr}_{L/K}$ decomposes as $\oplus \mathrm{Tr}_{L_\mathfrak{q}/K_\mathfrak{p}}$. Hence, we have

$$B^\vee\Big(\prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}\Big) = B^\vee \otimes \hat{A}_\mathfrak{p} = \mathrm{Span}_{\hat{A}_\mathfrak{p}}\{w_1, \ldots, w_n\} = \Big(\prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}\Big)^\vee = \prod_{\mathfrak{q}|\mathfrak{p}} \hat{B}_\mathfrak{q}^\vee.$$

In other words,

$$\mathcal{D}_{B/A} = \prod \mathfrak{q}^{a_\mathfrak{q}} \quad \Longrightarrow \quad \mathfrak{q}^{a_\mathfrak{q}} \hat{B}_\mathfrak{q} = \mathcal{D}_{\hat{B}_\mathfrak{q}/\hat{A}_\mathfrak{p}}.$$

Taking norms and applying Corollary **??** completes the proof of Theorem **??**. □

Corollary 3.1.5

Let K be a field with an absolute value $|.|_v$ and completion K_v. Let K_v^{sep} denote a separable closure of K_v. Let L/K be a finite separable extension. Then the distinct extensions $|.|_w$ of $|.|_v$ to L arise from embeddings $\sigma : L \hookrightarrow K_v^{\mathrm{sep}}$ by pulling back the unique extension of $|.|_v$ to K_v^{sep} via σ. Two embeddings give the same valuations on L if and only if they differ by some element in $\mathrm{Gal}(K_v^{\mathrm{sep}}/K_v)$.

Proof. An embedding $L \hookrightarrow K_v^{\mathrm{sep}}$ is given by sending β to a root of $f(x) = g_1(x) \cdots g_r(x)$. Galois permutes the roots of each g_i. □

Corollary 3.1.6

Let L/K be a finite separable extension of global fields. Then the unramified primes are exactly the ones not dividing the discriminant. In particular, all but finitely many primes are unramified; and L/K is everywhere unramified if and only if $\mathrm{Disc}(L/K) = (1)$.

When $K = \mathbb{Q}$, we can take a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ for B. The determinant of the matrix sending its dual basis to $\{\alpha_1, \ldots, \alpha_n\}$ is then $\det(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))$. Hence, we recover the familiar

$$\mathrm{Disc}(L/\mathbb{Q}) = (\det(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i\alpha_j))) = (\det(\sigma_i(\alpha_j)))^2$$

where $\sigma_1, \ldots, \sigma_n$ are all the embeddings of L into $\mathbb{C}$. You might have seen the following result from 441:

Theorem 3.1.7

Let K be a number field of degree n. Then every ideal class has a representative $I \subset \mathcal{O}_K$ with

$$NI \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\mathrm{Disc}(K/\mathbb{Q})|}.$$

In particular,

$$|\mathrm{Disc}(K/\mathbb{Q})| \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2r_2} \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{n} > 1$$

unless $n = 1$. In other words, every nontrivial extension of $\mathbb{Q}$ is ramified somewhere.

he different behaves well in towers of extensions.

Proposition 3.1.8

Let M/L be a finite separable extension and let C be the integral closure of A in M. Then

$$\mathcal{D}_{C/A} = \mathcal{D}_{C/B}\mathcal{D}_{B/A}, \qquad \mathrm{Disc}(M/K) = \mathrm{Disc}(L/K)^{[M:L]}N_{B/A}(\mathrm{Disc}(M/L)).$$

Proof. Let I be any fractional ideal of C (in M). Then

$$\begin{aligned} I \subset \mathcal{D}_{C/B}^{-1} &\iff \mathrm{Tr}_{M/L}(IC) \subset B \\ &\iff \mathcal{D}_{B/A}^{-1}\,\mathrm{Tr}_{M/L}(I) \subset \mathcal{D}_{B/A}^{-1} \\ &\iff \mathrm{Tr}_{L/K}(\mathcal{D}_{B/A}^{-1}I) \subset A \\ &\iff \mathcal{D}_{B/A}^{-1}I \subset \mathcal{D}_{C/A}^{-1} \\ &\iff I \subset \mathcal{D}_{B/A}\mathcal{D}_{C/A}^{-1}. \end{aligned}$$

The statement about the discriminants follow from $N_{C/A} = N_{B/A} \circ N_{C/B}$, which follows from the same statement for elements, or can be checked on prime ideals. □

Here is an interesting application of this formula. Let $K = \mathbb{Q}$ and let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial with squarefree discriminant. Let $M = \mathbb{Q}[x]/(f(x))$. Since $\Delta(f)$ is squarefree, we have $\mathrm{Disc}(M/\mathbb{Q}) = (\Delta(f))$ is squarefree. Hence if L is an intermediate field with $[M : L] > 1$, then $\mathrm{Disc}(L/\mathbb{Q}) = (1)$ and so $L = \mathbb{Q}$. Alternatively, we will see soon that the splitting field of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ with squarefree discriminant is an S_n-extension. Since S_n has no proper subgroup that strictly contains S_{n-1}, we also see that there are no intermediate fields in $M/\mathbb{Q}$. Moreover, one can prove that the extension $F/\mathbb{Q}(\sqrt{\Delta(f)})$ is an everywhere unramified A_n-extension.
Exercise: Prove that a transitive subgroup of S_n generated by transpositions is S_n.

§3.2 Decomposition groups

Let L be a finite Galois extension of a number field K. We find some natural subgroups of the Galois group $G = \mathrm{Gal}(L/K)$. One way to do this is to find something that G acts on and then take the stabilizer subgroups. Fix some $v \in M_K$ and we consider the action of G on the set $\{w \in M_L : w \mid v\}$ via

$$|\alpha|_{\sigma w} = |\sigma(\alpha)|_w.$$

The **decomposition group** of w is defined as

$$D_w = \{\sigma \in G\colon \sigma w = w\}.$$

Any $\sigma \in G$ defines an isometry from $(L, |.|_{\sigma w})$ to $(L, |.|_w)$ fixing K and thus extends to a continuous isomorphism from $L_{\sigma w}$ to L_w fixing K_v. Since L/K is Galois, we have $L \cong K[x]/(f(x))$ where $f(x)$ is the minimal polynomial of some primitive element. Then $L_w \cong K_v[x]/(g(x))$ for some irreducible factor $g(x)$ of $f(x)$ in $K_v[x]$. Since $f(x)$ splits in L, we see that $g(x)$ splits in L_w. Hence L_w/K_v is Galois, as the splitting field of $g(x)$. The natural map $D_w \longrightarrow \mathrm{Gal}(L_w/K_v)$ is injective as L is a subfield of L_w.

Proposition 3.2.1

The map $D_w \longrightarrow \mathrm{Gal}(L_w/K_v)$ defined above is an isomorphism and G acts transitively on the set $\{w \in M_L\colon w \mid v\}$.

Proof. This follows from a counting argument. Fix any $w_0 \mid v$ and let $S = \{\sigma w_0\colon \sigma \in G\}$. Then $\#S = [G : D_w]$. For any $\tau \in G$, we have $\tau D_w \tau^{-1} = D_{\tau w}$ and so $\#D_w = \#D_{w_0}$ for any $w \in S$. Thus, we have

$$\#G = [G : D_{w_0}]\#D_{w_0} = \sum_{w\in S} \#D_w \leq \sum_{w\in S}[L_w : K_v] \leq \sum_{w|v}[L_w : K_v] = [L : K] = \#G.$$

Hence $S = \{w \in M_L\colon w \mid v\}$ and $\#D_w = [L_w : K_v]$ for all $w \mid v$. □

Corollary 3.2.2

In a finite Galois extension of global fields L/K, for any fixed $v \in M_K$, the ramification behavior of each $w \mid v$ are all the same. That is

$$e_{L_w/K_v} \cdot f_{L_w/K_v} \cdot \#\{w \in M_L\colon w \mid v\} = [L : K].$$

Suppose now v corresponds to the prime ideal $\mathfrak{p}$ and $w \mid v$ corresponds to a prime ideal $\mathfrak{q} \mid \mathfrak{p}$. Let $k_\mathfrak{p}$ and $\ell_\mathfrak{q}$ denote the corresponding residue fields. Then we have the **inertia subgroup** $I_\mathfrak{q}$ and the exact sequence

$$1 \longrightarrow I_\mathfrak{q} \longrightarrow D_\mathfrak{q} \longrightarrow \mathrm{Gal}(\ell_\mathfrak{q}/k_\mathfrak{p}) \longrightarrow 1,$$

where $\#I_\mathfrak{q} = e_{\mathfrak{q}/\mathfrak{p}}$ and $\mathrm{Gal}(\ell_\mathfrak{q}/k_\mathfrak{p})$ is cyclic of order $f_{\mathfrak{q}/\mathfrak{p}}$. In terms of the ideals, we have

$$\begin{aligned} D_\mathfrak{q} &= \{\sigma \in G\colon \sigma(\mathfrak{q}) = \mathfrak{q}\},\\ I_\mathfrak{q} &= \{\sigma \in D_\mathfrak{q}\colon \sigma(b) \equiv b \pmod{\mathfrak{q}},\ \forall b \in B\}. \end{aligned}$$

The main structure theorem for the fixed fields of $I_\mathfrak{q}$ and $D_\mathfrak{q}$ are as follows.

Theorem 3.2.3

Consider the fixed fields

$$K \subseteq L^{D_\mathfrak{q}} \subseteq L^{I_\mathfrak{q}} \subseteq L.$$

Let E be an intermediate field in L/K and let $\mathfrak{q}_E = \mathfrak{q} \cap E$. Then:

(a) $E \subseteq L^{I_\mathfrak{q}}$ if and only if $e_{\mathfrak{q}_E/\mathfrak{p}} = 1$;

(b) $E \subseteq L^{D_\mathfrak{q}}$ if and only if $e_{\mathfrak{q}_E/\mathfrak{p}} = f_{\mathfrak{q}_E/\mathfrak{p}} = 1$.

Theorem 3.2.4

Let $D_{\mathfrak{p}}$ be the subgroup of G generated by all $D_{\mathfrak{q}}$ over $\mathfrak{q} \mid \mathfrak{p}$ and similarly for $I_{\mathfrak{p}}$. Consider the fixed fields

$$K \subseteq L^{D_{\mathfrak{p}}} \subseteq L^{I_{\mathfrak{p}}} \subseteq L.$$

Let E be an intermediate field in L/K. Then:

(a) The decomposition field $L^{D_{\mathfrak{p}}}$ and the inertia field $L^{I_{\mathfrak{p}}}$ are Galois over K;

(b) $E \subseteq L^{I_{\mathfrak{p}}}$ if and only if $\mathfrak{p}$ is unramified in E, i.e. $e_{\mathfrak{q}/\mathfrak{p}} = 1$ for every prime $\mathfrak{q}$ of E above $\mathfrak{p}$;

(c) $E \subseteq L^{D_{\mathfrak{p}}}$ if and only if $\mathfrak{p}$ splits completely in E, i.e. $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$ for every prime $\mathfrak{q}$ of E above $\mathfrak{p}$.

Proof. The normality of $I_{\mathfrak{p}}$ and $D_{\mathfrak{p}}$ follow from the definitions:

$$\tau D_{\mathfrak{q}} \tau^{-1} = D_{\tau\mathfrak{q}} \qquad \text{and} \qquad \tau I_{\mathfrak{q}} \tau^{-1} = I_{\tau\mathfrak{q}}.$$

It is also easy to see that Theorem **??** follows immediately from Theorem **??**.

We write $D_{\mathfrak{q}}(L/E)$ and $I_{\mathfrak{q}}(L/E)$ for the decomposition and inertia group of $\mathfrak{q}$ for the intermediate extension L/E. Then

$$D_{\mathfrak{q}}(L/E) = D_{\mathfrak{q}} \cap \mathrm{Gal}(L/E) \qquad \text{and} \qquad I_{\mathfrak{q}}(L/E) = I_{\mathfrak{q}} \cap \mathrm{Gal}(L/E).$$

Let $F = L^{I_{\mathfrak{q}}}$. Then $I_{\mathfrak{q}}(L/F) = \mathrm{Gal}(L/F) = I_{\mathfrak{q}}$. Now

$$I_{\mathfrak{q}}(L/E) = \mathrm{Gal}(L/E) \cap \mathrm{Gal}(L/F) = \mathrm{Gal}(L/EF) = I_{\mathfrak{q}}(L/EF).$$

Hence we have $e_{\mathfrak{q}/\mathfrak{q}_E} = e_{\mathfrak{q}/\mathfrak{q}_{EF}}$. Now

$$E \subseteq F \iff \mathrm{Gal}(L/EF) = \mathrm{Gal}(L/F) \iff I_{\mathfrak{q}}(L/EF) = I_{\mathfrak{q}}(L/F) \iff e_{\mathfrak{q}/\mathfrak{q}_{EF}} = e_{\mathfrak{q}/\mathfrak{q}_F} \iff e_{\mathfrak{q}/\mathfrak{q}_E} = e_{\mathfrak{q}/\mathfrak{q}_F}$$

which is equivalent to $e_{\mathfrak{q}_E/\mathfrak{p}} = e_{\mathfrak{q}_F/\mathfrak{p}} = 1$. The second follows with the same argument with all the $I_{\mathfrak{q}}$ replaced by $D_{\mathfrak{q}}$ and $e_{\mathfrak{q}/*}$ replaced by $e_{\mathfrak{q}/*} f_{\mathfrak{q}/*}$. □

We consider some consequences of the main structure theorem.

Corollary 3.2.5

Let L/K be a finite Galois extension of global fields. Let H be the subgroup of $\mathrm{Gal}(L/K)$ generated by all the inertia subgrousp $I_{\mathfrak{p}}$. Then L^H/K is everywhere unramified. In particular, if $K = \mathbb{Q}$, then the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is generated by inertia.

Using the decomposition and inertia fields $L^{D_{\mathfrak{p}}}$ and $L^{I_{\mathfrak{p}}}$, we see that:

Corollary 3.2.6

Let L_1/K and L_2/K be finite separable extensions of global fields. Let $\mathfrak{p}$ be a prime of K.

- $\mathfrak{p}$ is unramified in L_1 and L_2 if and only if it is unramified in $L_1 L_2$
- $\mathfrak{p}$ splits completely in L_1 and L_2 if and only if it splits completely in $L_1 L_2$.

Corollary 3.2.7

Let E/K be a finite separable extension of global fields with Galois closure L/K. Let $\mathfrak{p}$ be a prime of K.

- $\mathfrak{p}$ is unramified in E if and only if it is unramified in L.
- $\mathfrak{p}$ splits completely in E if and only if it splits completely in L.

Example: Suppose $f(x) \in \mathbb{Q}[x]$ is irreducible of degree n with squarefree discriminant. For example $f(x) = x^5 - x - 1$ with $\Delta(f) = 19 \cdot 151$. Let L denote the splitting field of $f(x)$. Let p be a prime dividing $\Delta(f)$. Then we can factor $f(x)$ as $g_1(x) \cdots g_{r-1}(x)h(x)$ into irreducibles in $\mathbb{Q}_p[x]$, where each $\bar{g}_i(x) \in \mathbb{F}_p[x]$ is irreducible and $\bar{h}(x) = (x-a)^2$ for some $a \in \mathbb{F}_p$. For any prime $\mathfrak{q} \mid p$, we see that $L_\mathfrak{q} \cong \mathbb{Q}_p(\alpha_1, \ldots, \alpha_{n-2}, \beta, \gamma)$ where $\alpha_1, \ldots, \alpha_{n-2}$ are the roots of $g_1(x) \cdots g_{r-1}(x)$ in $\bar{\mathbb{Q}}_p$ and β and γ are the roots of $h(x)$. Since $\mathbb{Q}_p(\alpha_1, \ldots, \alpha_{n-2})/\mathbb{Q}_p$ is unramified, we see that any element of the inertia subgroup $I_\mathfrak{q}$ acts trivially on $\alpha_1, \ldots, \alpha_{n-2}$ and so can only swap β and γ. In other words, $I_\mathfrak{q}$ is generated by a transposition. Since any transitive subgroup of S_n generated by transpositions is S_n, we see that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$.

We can also compute the discriminant of $L/\mathbb{Q}$. Any prime $p \nmid \Delta(f)$ is unramified in $\mathbb{Q}[x]/(f(x))$ and so also is unramified in its Galois closure and so does not contribute to the discriminant. Suppose $p \mid \Delta(f)$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the primes above it in L. Then we know that they all have ramification degree $e = 2$, and some common residue degree $f_\mathfrak{p}$ with $2rf_\mathfrak{p} = n!$. Recalling that the discriminant is 0 or 1 mod 4, we see that if $\Delta(f)$ is squarefree, then $2 \nmid \Delta(f)$. Hence we may assume $p \neq 2$ and so the ramification is tame. Hence

$$\mathrm{Disc}_p(L/\mathbb{Q}) = \prod_{i=1}^{r} p^{f(e-1)} = p^{rf} = p^{n!/2}.$$

Multiplying over all $p \mid \Delta(f)$ gives

$$(\mathrm{Disc}(L/\mathbb{Q})) = (\Delta(f)^{n!/2}).$$

Consider now the quadratic subextension $F = \mathbb{Q}(\sqrt{\Delta(f)})$. Since $\Delta(f) \equiv 1 \pmod 4$, we see that $(\mathrm{Disc}(F/\mathbb{Q})) = (\Delta(f))$. Using the formula

$$\mathrm{Disc}(L/\mathbb{Q}) = \mathrm{Disc}(F/\mathbb{Q})^{[L:F]} N_{F/\mathbb{Q}}(\mathrm{Disc}(L/F)),$$

we find that $\mathrm{Disc}(L/F) = (1)$. In other words, L/F is an everywhere unramified A_n-extension.

Example: We consider a more explicit example. Let $f(x) = x^3 + x + 1$ with $\Delta(f) = -31$.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[ddr, dash] & \\
E \arrow[ddr, dash, "3"'] & & \\
 & & F \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\begin{aligned} E &= \mathbb{Q}[x]/(x^3+x+1) & \mathcal{O}_E &= \mathbb{Z}[\beta] \\ F &= \mathbb{Q}(\sqrt{-31}) & \mathcal{O}_F &= \mathbb{Z}[\frac{1+\sqrt{-31}}{2}] \end{aligned}$$

There are four different cases for the splitting of p in E: $p = 31$ the only ramified prime; p splits completely; p splits as $\mathfrak{p}_1\mathfrak{p}_2$ where $f_{\mathfrak{p}_1/\mathfrak{p}} = 1$ and $f_{\mathfrak{p}_2/\mathfrak{p}} = 2$; p stays inert. We describe the splitting of p in E, F, L in all these cases.

- The ramified prime $p = 31$. We have $x^3 + x + 1 = (x - 3)(x - 14)^2$ in $\mathbb{F}_{31}[x]$. So we have
$$31\mathcal{O}_E = (31, \beta - 3)(31, \beta - 14)^2 \qquad \text{and} \qquad 31\mathcal{O}_F = (\sqrt{-31})^2.$$
In L, we see that $2 \mid e$ and $r \geq 2$. Hence we must have $e = 2$, $f = 1$ and $r = 3$. So
$$(31, \beta - 3)\mathcal{O}_L = \mathfrak{m}_1^2 \qquad \text{and} \qquad (31, \beta - 14)\mathcal{O}_L = \mathfrak{m}_1'\mathfrak{m}_1'' \qquad \text{and} \qquad \sqrt{-31}\mathcal{O}_L = \mathfrak{m}_1\mathfrak{m}_1'\mathfrak{m}_1''.$$

- Suppose p splits completely in E. Then it splits completely in L and also in F. We have
$$p\mathcal{O}_E = \mathfrak{p}_1\mathfrak{p}_1'\mathfrak{p}_1'' \qquad \text{and} \qquad p\mathcal{O}_F = \mathfrak{q}_1\mathfrak{q}_1'$$
$$\mathfrak{p}_1\mathcal{O}_L = \mathfrak{m}_1^{(1)}\mathfrak{m}_1^{(2)} \qquad \text{and} \qquad \mathfrak{p}_2\mathcal{O}_L = \mathfrak{m}_1^{(3)}\mathfrak{m}_1^{(4)} \qquad \text{and} \qquad \mathfrak{p}_3\mathcal{O}_L = \mathfrak{m}_1^{(5)}\mathfrak{m}_1^{(6)}$$
$$\mathfrak{q}_1\mathcal{O}_L = \mathfrak{m}_1^{(1)}\mathfrak{m}_1^{(3)}\mathfrak{m}_1^{(5)} \qquad \text{and} \qquad \mathfrak{q}_2\mathcal{O}_L = \mathfrak{m}_1^{(2)}\mathfrak{m}_1^{(4)}\mathfrak{m}_1^{(6)}.$$
We note that there exists an element of order 2 in $\mathrm{Gal}(L/\mathbb{Q})$ sending $\mathfrak{m}_1^{(1)}$ to $\mathfrak{m}_1^{(2)}$. Hence they can't both lie over the same prime ideal in $\mathcal{O}_F$, which is fixed by the C_3 subgroup of S_3. Since the prime splits in F, we see that -31 is a square mod p. In fact, Kronecker proved that these are precisely the primes such that $p \neq 31$ and
$$\exists u, v \in \mathbb{Z}, p = u^2 + uv + 8v^2 = \frac{1}{4}((2u + v)^2 + 31v^2).$$
In other words, in this case, there exists an element $\alpha \in \mathcal{O}_F$ with norm p. So the ideals $\mathfrak{q}_1 = (\alpha)$ and $\mathfrak{q}_1' = (\bar{\alpha})$ are principal.

- Suppose p splits as $\mathfrak{p}_1\mathfrak{p}_2$ in E. Then we have $2 \mid f$ and $r \geq 2$. Hence, we must have $e = 1$, $f = 2$, $r = 3$. So
$$p\mathcal{O}_E = \mathfrak{p}_1\mathfrak{p}_2 \qquad \text{and} \qquad \mathfrak{p}_1\mathcal{O}_L = \mathfrak{m}_2 \qquad \text{and} \qquad \mathfrak{p}_2\mathcal{O}_L = \mathfrak{m}_2'\mathfrak{m}_2''$$
$$p\mathcal{O}_F = \mathfrak{q}_2 \qquad \text{and} \qquad \mathfrak{q}_2\mathcal{O}_L = \mathfrak{m}_2\mathfrak{m}_2'\mathfrak{m}_2''.$$
This is the case where p stays inert in $\mathbb{Q}(\sqrt{-31})$. In other words, -31 is not a square mod p.

- Suppose p stays inert in E. Then it can't stay inert in L, because C_6 is not a subgroup of S_3. So
$$p\mathcal{O}_E = \mathfrak{p}_3 \qquad \text{and} \qquad \mathfrak{p}_3\mathcal{O}_L = \mathfrak{m}_3\mathfrak{m}_3'$$
$$p\mathcal{O}_F = \mathfrak{q}_1\mathfrak{q}_1' \qquad \text{and} \qquad \mathfrak{q}_1\mathcal{O}_L = \mathfrak{m}_3 \qquad \text{and} \qquad \mathfrak{q}_2\mathcal{O}_L = \mathfrak{m}_3'.$$
These are all the primes such that
$$\exists u, v \in \mathbb{Z}, p = 2u^2 + uv + 4v^2.$$
For example when $p = 2$, which is too small for there to be element of $\mathcal{O}_F$ of norm 2. So the two prime ideals $\mathfrak{q}_1$ and $\mathfrak{q}_1'$ are non-principal. They are distinct and are inverses of each other in the class group. So they generate a subgroup of order 3. In fact, the class group of $\mathbb{Q}(\sqrt{-31})$ is isomorphic to C_3 with representatives $\{(1), \mathfrak{q}_1, \mathfrak{q}_1'\}$. We note that these are exactly the prime ideals of $\mathcal{O}_F$ that don't split completely in L.

We observe also that the extension L/F is everywhere unramified with Galois group also C_3. It is a consequence of global class field theory that any number field K admist a Hilbert class field $H(K)$, which is the maximal abelian unramified extension of K. There is a canonical isomorphism
$$\mathrm{Cl}(K) \to \mathrm{Gal}(H(K)/K).$$
As explored above, this map should encode information about whether the prime ideal splits completely in $H(K)$...

§3.3 Frobenius and Chebotarev density theorem

Suppose now the prime ideal $\mathfrak{p}$ is unramified. Let $\mathfrak{q} \mid \mathfrak{p}$ be a prime ideal in $\mathcal{O}_L$. Then the inertia subgroup $I_\mathfrak{q}$ is trivial and

$$D_\mathfrak{q} \cong \mathrm{Gal}(\ell_\mathfrak{q}/k_\mathfrak{p}) \cong \mathbb{Z}/[\ell_\mathfrak{q} : k_\mathfrak{p}]\mathbb{Z}.$$

We then have the **Frobenius element** $(\mathfrak{q}, L/K)$ as the element in $D_\mathfrak{q}$ that maps to the map $x \mapsto x^{N\mathfrak{p}}$ in $\mathrm{Gal}(\ell_\mathfrak{q}/k_\mathfrak{p})$. Its order is the residue degree $[\ell_\mathfrak{q} : k_\mathfrak{p}]$ and $D_\mathfrak{q} = \langle (\mathfrak{q}, L/K) \rangle$. For any $\tau \in G$, we have

$$(\tau\mathfrak{q}, L/K) = \tau(\mathfrak{q}, L/K)\tau^{-1}.$$

Indeed, for any $\alpha \in \mathcal{O}_L$,

$$(\mathfrak{q}, L/K)\tau^{-1}(\alpha) \equiv \tau^{-1}(\alpha)^{N\mathfrak{p}} \pmod{\mathfrak{q}}$$

and so

$$\tau(\mathfrak{q}, L/K)\tau^{-1}(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\tau\mathfrak{q}}.$$

We write $(\mathfrak{p}, L/K)$ for the conjugacy class of G containing any $(\mathfrak{q}, L/K)$. When G is abelian, $(\mathfrak{p}, L/K)$ is also written for the element inside this conjugacy class of size 1.

Suppose now L/K is the splitting field of some $f(x) \in A[x]$. Since $\mathfrak{p}$ is unramified, we can factor

$$f(x) \bmod \mathfrak{p} = g_1(x) \cdots g_r(x) \in k_\mathfrak{p}[x]$$

into irreducibles. Since the map $x \mapsto x^{N\mathfrak{p}}$ acts cyclicly on the roots of any irreducible polynomial in $k_\mathfrak{p}[x]$, we see that

$$(\mathfrak{q}, L/K) = (\deg(g_1)\text{-cycle}) \cdots (\deg(g_r)\text{-cycle}) \in S_{\text{roots of } f(x)}.$$

Example: Consider the splitting field L of x^3+x+1 over $\mathbb{Q}$, with $E = \mathbb{Q}[x]/(x^3+x+1)$. Write $S_3 = \{1, b, b^2, a, ab, ab^2\}$.

- If $\mathfrak{p}$ splits completely in $\mathcal{O}_E$, then
$$(\mathfrak{p}, L/\mathbb{Q}) = (1)(1)(1) = \{1\}.$$
- If $\mathfrak{p}\mathcal{O}_E = \mathfrak{p}_1\mathfrak{p}_2$, then
$$(\mathfrak{p}, L/\mathbb{Q}) = (1)(2) = \{a, ab, ab^2\}.$$
- If $\mathfrak{p}\mathcal{O}_E = \mathfrak{p}_3$, then
$$(\mathfrak{p}, L/\mathbb{Q}) = (3) = \{b, b^2\}.$$

Example: Consider $f(x) = x^5 - x - 1$. Then mod 2, we have $f(x) = (x^2+x+1)(x^3+x^2+1)$ and mod 3 it is irreducible. So the Galois group of f contains a 5-cycle and a $(2,3)$-cycle. It then must contain a transposition and so is the entire S_5. (Recall that if p is a prime, then S_p is generated by a p-cycle and any transposition.) Note also that $f(x)$ is irreducible mod 5 since it is of the form $x^p - x + a$.

We now list some nice properties of $(\mathfrak{q}, L/K)$.

- The prime $\mathfrak{p}$ splits completely in L if and only if $f_{\mathfrak{q}/\mathfrak{p}} = 1$ if and only if $(\mathfrak{q}, L/K) = 1$ if and only if $(\mathfrak{p}, L/K) = 1$.

- If E is an intermediate field that is Galois over K, then

$$(\mathfrak{q}_E, E/K) = (\mathfrak{q}, L/K)|_E \qquad \text{and} \qquad (\mathfrak{q}, L/E) = (\mathfrak{q}, L/K)^{f_{\mathfrak{q}_E/\mathfrak{p}}}.$$

  Hence $\mathfrak{p}$ splits completely in E if and only if $(\mathfrak{p}, L/K)|_E = 1$ if and only if $(\mathfrak{p}, L/K) \in \mathrm{Gal}(L/E)$.

- If E is an intermediate field that is not necessarily Galois over K, then we saw before that $f_{\mathfrak{q}_E/\mathfrak{p}} = 1$ if and only if $E \subseteq L^{D_\mathfrak{q}}$. Since $D_\mathfrak{q}$ is generated by $(\mathfrak{q}, L/K)$, we have

$$f_{\mathfrak{q}_E/\mathfrak{p}} = 1 \quad \Longleftrightarrow \quad (\mathfrak{q}, L/K) \in \mathrm{Gal}(L/E).$$

Chebotarev's density theorem states that every possible splitting behavior happen:

Theorem 3.3.1

Let K be a number field and let L/K be a finite Galois extension with Galois group G. Then for any conjugacy class C of G,

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \colon (\mathfrak{p}, L/K) = C, N\mathfrak{p} < X\}}{\#\{\mathfrak{p} \colon N\mathfrak{p} < X\}} = \frac{\#C}{\#G}.$$

Example: Applying to the example of $x^3 + x + 1$, we see that $1/6$ of primes split completely in $\mathcal{O}_E$; $1/2$ of the primes splits into $\mathfrak{p}_1\mathfrak{p}_2$ (we already know this as primes where -31 is a quadratic residue); $1/3$ of the primes stay inert. Note that the average number of roots mod p as p varies is then

$$\frac{1}{6} \cdot 3 + \frac{1}{2} \cdot 1 + \frac{1}{3} \cdot 0 = 1.$$

Kronecker proved in 1880 that for an irreducible polynomial in $\mathbb{Z}[x]$, the average number of roots of $f(x)$ mod p as p varies is 1. In light of the Chebotarev density theorem, this is a consequence of Burnside's fixed point formula: for a group $G = \mathrm{Gal}(f)$ acting transitively on the set of roots of $f(x)$, we have

$$\sum_{\sigma\in G} \#\{\alpha \colon \sigma(\alpha) = \alpha\} = |G|.$$

If we take the polynomial $f(x) = x^3 - 3x + 1$, then things are different. Its discriminant is 81 and so its Galois group is $\mathbb{Z}/3\mathbb{Z}$. It turns out that for $p \neq 3$, $f(x)$ splits completely if $p \equiv \pm 1 \pmod 9$ and has no roots otherwise by relating $f(x + x^{-1})$ with $\Phi_9(x) = x^6 + x^3 + 1$. Kronecker-Weber says that every abelian extension is contained in some cyclotomic extension, and in light of this splitting result, we expect that $K = \mathbb{Q}[x]/(f(x)) \subseteq \mathbb{Q}(\zeta_9)$. In fact, we have the factorization

$$x^3 - 3x + 1 = (x - (\zeta_9 + \zeta_9^{-1}))(x - (\zeta_9^2 + \zeta_9^{-2}))(x - (\zeta_9^4 + \zeta_9^{-4})).$$

The Frobenius element $(p, \mathbb{Q}(\zeta_9)/\mathbb{Q})$ for $p \neq 3$ is given by $\zeta_9 \mapsto \zeta_9^p$. It is then clear that $(p, \mathbb{Q}(\zeta_9)/\mathbb{Q})$ acts trivially on the roots $\zeta_9 + \zeta_9^{-1}, \zeta_9^2 + \zeta_9^{-2}, \zeta_9^4 + \zeta_9^{-4}$ if and only if $p \equiv \pm 1 \pmod 9$.

We note in the above example that for a density $1/6 + 1/2$ primes p, there exists a degree 1 prime $\mathfrak{p} \mid p$ in K (that is, a prime $\mathfrak{p} \mid p$ with $f_{\mathfrak{p}/p} = 1$). We can give a general formula for this density. Given a finite extension L/K of number fields, let $P_1(L/K)$ denote the set of primes $\mathfrak{p}$ of K that is unramified in L and is divisible by some prime $\mathfrak{q}$ in L with $f_{\mathfrak{q}/\mathfrak{p}} = 1$. Let $\mathrm{Spl}(L/K)$ denote the set of unramified primes of K that splits completely in L. When L/K is Galois, $P_1(L/K) = \mathrm{Spl}(L/K)$. When $L = K[x]/(f(x))$ for some irreducible $f(x) \in A[x]$ with roots $\alpha_1, \dots, \alpha_n$ in the Galois closure M/K, we see that

$$\mathfrak{p} \in P_1(L/K) \quad \Longleftrightarrow \quad (\mathfrak{p}, M/K)(\alpha_i) = \alpha_i \text{ for some } i = 1, \dots, n.$$

Let H be the (proper) subgroup of $G = \mathrm{Gal}(M/K)$ consisting of automorphisms fixing α_1. Then

$$\mathfrak{p} \in P_1(L/K) \quad \Longleftrightarrow \quad (\mathfrak{p}, M/K) \subseteq \bigcup_{\tau \in G} \tau H \tau^{-1}.$$

The above union is a union of at most $[G : H]$ conjugates of H all containing 1, and so is a proper subset of G. This proves that the density of $P_1(L/K)$ is strictly between 0 and 1.

Example: Applying this result to the example of $H = \{1, a\}$ and $G = S_3 = \{1, b, b^2, a, ab, ab^2\}$, we find the union of the conjugates of H is $\{1, a, ab, ab^2\}$ which is $2/3 = 1/6 + 1/2$ of the size of G.

Corollary 3.3.2

Suppose $f \in \mathcal{O}_K[x]$ is an irreducible polynomial. Then for a set, of density strictly between 0 and 1, of primes $\mathfrak{p}$, there exist $\alpha \in \mathcal{O}_K$ such that $f(\alpha) \equiv 0 \pmod{\mathfrak{p}}$.

Proof. Let $L = K[x]/(f(x))$. By Theorem **??**, apart from finitely many primes that divide the discriminant of $f(x)$, we know that $\mathfrak{p} \in P_1(L/K)$ if and only if $f(x)$ has a linear factor mod $\mathfrak{p}$. □

Theorem 3.3.3

(Bauer) Suppose E/K and L/K are finite extensions of number fields and that L/K is Galois. Suppose that there exists a set S of primes of density 0 such that $P_1(E/K) \backslash S \subseteq \mathrm{Spl}(L/K) \backslash S$. Then $L \subseteq E$.

Proof. Let M be the Galois closure of LE over K. It suffices to show that $\mathrm{Gal}(M/E) \subseteq \mathrm{Gal}(M/L)$. Take any $\sigma \in \mathrm{Gal}(M/E)$. By the Chebotarev density theorem, there exists an unramified prime $p \notin S$ and a prime $\mathfrak{q} \mid p$ in M such that $(\mathfrak{q}, M/K) = \sigma$. From $(\mathfrak{q}, M/K) \in \mathrm{Gal}(M/E)$, we see that $\mathfrak{p} \in P_1(E/K) \backslash S$. By assumption, we see that $\mathfrak{p}$ splits completely in L. Hence we also have $\sigma = (\mathfrak{q}, E/K) \in \mathrm{Gal}(M/L)$. □

In the case that both M/K and L/K are Galois, we obtain the following result, which also has a simpler proof via the Chebotarev density theorem.

Theorem 3.3.4

Suppose L/K and M/K are finite Galois extensions of number fields. Then

$$L = M \Longleftrightarrow \mathrm{Spl}(L/K) = \mathrm{Spl}(M/K).$$

In other words, Galois extensions are "determined" by the set of primes that split completely.

Proof. Only the backwards direction is nontrivial. Suppose $\mathrm{Spl}(L/K) = \mathrm{Spl}(M/K)$. Consider the Galois extension LM/K. For any $\mathfrak{p} \in \mathrm{Spl}(L/K) = \mathrm{Spl}(M/K)$, we have

$$(\mathfrak{p}, LM/K)|_L = (\mathfrak{p}, L/K) = 1, \qquad (\mathfrak{p}, LM/K)|_M = (\mathfrak{p}, M/K) = 1.$$

Hence $\mathfrak{p}$ splits completely in LM and so $\mathrm{Spl}(LM/K) = \mathrm{Spl}(L/K)$. This implies that $[LM : K] = [L : K]$ and so $LM = L$ and similarly $LM = M$. □

It is a result of global class field theory that for abelian extensions L/K, the splitting behavior of primes is given by congruence conditions. We can be very explicit in the case of $\mathbb{Q}$.

§3.4 Cyclotomic extensions of $\mathbb{Q}$ and applications

We will now run our theory through $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ and prove some interesting applications along the way. The minimal polynomial of ζ_m over $\mathbb{Q}$ is the m-th cyclotomic polynomial

$$\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ \gcd(k,m)=1}} (x - \zeta_m^k).$$

It is irreducible of degree $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$ and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_{p|m} (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times, \qquad \text{where} \qquad m = \prod_{p|m} p^{n_p}.$$

For any positive integer t,

$$\begin{aligned} (\mathbb{Z}/p^t\mathbb{Z})^\times &\cong C_{p^{t-1}(p-1)}, \qquad \text{if } p \text{ is odd} \\ (\mathbb{Z}/2^t\mathbb{Z})^\times &\cong \begin{cases} 1 & \text{if } t = 1 \\ C_2 & \text{if } t = 2 \\ C_2 \times C_{2^{t-2}} & \text{if } t \ge 3. \end{cases} \end{aligned}$$

The local extension $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ is unramified if $p \nmid m$. When $p \mid m$, we write $m = p^{n_p}s$ where $p \nmid s$ and we have

$$\mathbb{Q}_p(\zeta_m) = F_p(\zeta_{p^{n_p}}) \qquad \text{where} \qquad F_p = \mathbb{Q}_p(\zeta_s).$$

The decomposition group $D_p = D_\mathfrak{q}$ and inertia group $I_p = I_\mathfrak{q}$ for any prime $\mathfrak{q} \mid p$ because the extension is abelian, and it factors as

$$D_p \cong I_p \times \mathrm{Gal}(F_p/\mathbb{Q}_p) \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times \times C_{o_s(p)}$$

where $o_s(p)$ denotes the order of p mod s (see Theorem **??**). We note that for any prime $p' \neq p$, the inertia group $I_{p'}$ acts trivially on $\zeta_{p^{n_p}}$ since $\mathbb{Q}_{p'}(\zeta_{p^{n_p}})/\mathbb{Q}_{p'}$ is unramified. Hence the distinct inertia groups intersect trivially and we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \prod_{p|m} I_p.$$

Proposition 3.4.1

Suppose $L/\mathbb{Q}(\zeta_m)$ is a finite extension such that $L/\mathbb{Q}$ is abelian. Suppose for any prime $p \mid m$ and any prime $\mathfrak{q} \mid p$ in L, we have $L_{\mathfrak{q}} \cong E_p(\zeta_m)$ for some unramfied extension $E_p/\mathbb{Q}_p$; and that any prime $p \nmid m$ is unramified in L. Then $L = \mathbb{Q}(\zeta_m)$.

Proof. The inertia groups I_p for L are isomorphic to $\mathrm{Gal}(F_p(\zeta_{p^{n_p}})/F_p) \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^\times$ for $p \mid m$ where $F_p = E_p(\zeta_s)$ is unramified over $\mathbb{Q}_p$; and trivial for $p \nmid m$. Since $\mathrm{Gal}(L/\mathbb{Q})$ is generated by all the I_p, we have

$$[L : \mathbb{Q}] = \#\,\mathrm{Gal}(L/\mathbb{Q}) \leq \prod_{p \mid m} \#(\mathbb{Z}/p^{n_p}\mathbb{Z})^\times = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

Hence $L = \mathbb{Q}(\zeta_m)$ since $\mathbb{Q}(\zeta_m) \subseteq L$. □

We are now ready to prove the global Kronecker-Weber theorem.

Theorem 3.4.2

Suppose $K/\mathbb{Q}$ is a finite abelian extension. Then $K \subseteq \mathbb{Q}(\zeta_m)$ for some positive integer m.

Proof. For any prime p that ramifies in K, the local extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ is abelian for any prime $\mathfrak{p} \mid p$ since its Galois group D_p is a subgroup of the abelian group $\mathrm{Gal}(K/\mathbb{Q})$. By local Kronecker-Weber (Theorem **??**), there exists $m_p \in \mathbb{N}$ such that $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$. Let m be the lcm of all these m_p, so that $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_m)$ for every prime p that ramifies in K. We prove that $K \subseteq \mathbb{Q}(\zeta_m)$.

Let $L = K \cdot \mathbb{Q}(\zeta_m) = K(\zeta_m)$ be the compositum. It is enough to prove that $L = \mathbb{Q}(\zeta_m)$. As a compositum of two abelian extensions of $\mathbb{Q}$, we see that $L/\mathbb{Q}$ is abelian. Let p be a prime dividing m and let $\mathfrak{q} \mid p$ be a prime of L and let $\mathfrak{p} = \mathfrak{q} \cap K$. If p is ramified in K, we have $L_{\mathfrak{q}} = K_{\mathfrak{p}}(\zeta_m) = \mathbb{Q}_p(\zeta_m)$. If p is unramified in K, then $L_{\mathfrak{q}} = K_{\mathfrak{p}}(\zeta_m)$ with $K_{\mathfrak{p}}/\mathbb{Q}_p$ unramified. For any prime $p \mid m$, let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$. Then $L_{\mathfrak{q}} = K_{\mathfrak{p}}(\zeta_m) = \mathbb{Q}_p(\zeta_m)$. For any prime $p \nmid m$, it is unramified in K and $\mathbb{Q}(\zeta_m)$ and so also unramified in L. We are now done by Proposition **??**. □

Remark: It is also easy to see that the global Kronecker-Weber implies the local Kronecker-Weber. Indeed, given any finite abelian $K'/\mathbb{Q}_p$, we have $K' = \mathbb{Q}_p[x]/(f(x))$ for some monic irreducible $f(x) \in \mathbb{Z}_p[x]$. By Krasner's Lemma, there exists $g(x) \in \mathbb{Z}[x]$ close enough to $f(x)$ such that g is irreducible in $\mathbb{Z}_p[x]$ and $\mathbb{Q}_p[x]/(f(x)) = \mathbb{Q}_p[x]/(g(x))$. Let $K = \mathbb{Q}[x]/(g(x))$. Then $K \otimes_{\mathbb{Q}} \mathbb{Q}_p = K'$. Apply global Kronecker-Weber to fit K inside some $\mathbb{Q}(\zeta_n)$. Then $K' \subseteq \mathbb{Q}_p(\zeta_n)$.

Next, we compute the discriminant $\mathrm{Disc}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. It is enough to consider primes $p \mid m$. Recall that $\mathbb{Q}_p(\zeta_m) = F_p(\zeta_{p^{n_p}})$ where $F_p/\mathbb{Q}_p$ is unramified of degree $f = o_s(p)$ where $s = m/p^{n_p}$. We have

$$\mathrm{Disc}_p(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \mathrm{Disc}_p(F_p(\zeta_{p^{n_p}})/F_p)^f = p^{\phi(p^{n_p})(n_p - \frac{1}{p-1})f}.$$

The prime p splits into $r = \phi(m)/(\phi(p^{n_p})f)$ primes $\mathfrak{p}$ in $\mathbb{Q}(\zeta_m)$. Combining them gives

$$\mathrm{Disc}_p(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = p^{\phi(m)(\mu_p(m) - \frac{1}{p-1})}$$

where we have written $\mu_p(m) = n_p$. Multiplying over all $p \mid m$ gives

$$\mathrm{Disc}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \Big(\prod_{p \mid m} p^{\phi(m)(\mu_p(m) - \frac{1}{p-1})}\Big).$$

Proposition 3.4.3

The ring of integers of $\mathbb{Q}(\zeta_m)$ is $\mathbb{Z}[\zeta_m]$. As a result, for $m \geq 3$,

$$\Delta(\Phi_m(x)) = (-1)^{\phi(m)/2} \prod_{p|m} p^{\phi(m)(\mu_p(m)-\frac{1}{p-1})}.$$

Proof. The sign of $\Delta(\Phi_m(x))$ can be obtained from how complex conjugation acts on $\prod(\zeta_m^i - \zeta_m^j)$. More precisely, complex conjugation sends ζ_m^i to ζ_m^{m-i} and so negates every term in the product. There are $\phi(m)(\phi(m)-1)/2$ terms, but $\phi(m)-1$ is always odd.

The conceptual reason for why $\mathbb{Z}[\zeta_m]$ is the ring of integers is that locally, $\mathbb{Z}_p[\zeta_m]$ is the valuation ring of $\mathbb{Q}_p(\zeta_m)$ for every prime. More rigorously, it suffices to prove that for any nonzero prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_m]$, $\mathfrak{p}$ is principal in the localization $\mathbb{Z}[\zeta_m]_{(\mathfrak{p})}$, for this would imply that $\mathbb{Z}[\zeta_m]_{(\mathfrak{p})}$ is a DVR.

Let p be the rational prime that $\mathfrak{p}$ lies over. Then $\mathfrak{p} = (p, g(\zeta_m))$ for some $g(x) \in \mathbb{Z}[x]$ such that $\bar{g} \in \mathbb{F}_p[x]$ is an irreducible factor of $\Phi_m(x)$. Write $m = p^{n_p}s$ with $p \nmid s$. Here we allow $n_p = 0$. The idea now is that in the unramified case, p should generate $\mathfrak{p}$; while in the ramified case, $\zeta_{p^{n_p}} - 1$ should generate $\mathfrak{p}$. Note that

$$\bar{g} \mid \Phi_m(x) \mid x^m - 1 = (x^s - 1)^{p^{n_p}} \qquad \Longrightarrow \qquad \bar{g} \mid x^s - 1.$$

Let $h(x) \in \mathbb{Z}[x]$ such that $\bar{g}\bar{h} = x^s - 1$. Then there exists $j(x) \in \mathbb{Z}[x]$ such that

$$x^s - 1 = g(x)h(x) + pj(x).$$

Setting $x = \zeta_m$ and noting that $m/s = p^{n_p}$, we see that

$$\zeta_{p^{n_p}} - 1 = g(\zeta_m)h(\zeta_m) + pj(\zeta_m) \in \mathfrak{p}.$$

If $n_p \geq 1$, then recalling that $\Phi_{p^{n_p}}(x+1)$ is Eisenstein, we know that $\zeta_{p^{n_p}-1} \mid p$ in $\mathbb{Z}[\zeta_{p^{n_p}}]$. Hence it suffices to prove that $\zeta_{p^{n_p}} - 1 \mid g(\zeta_m)$ in $\mathbb{Z}[\zeta_m]_{(\mathfrak{p})}$. If $n_p = 0$, then it suffices to prove that $p \mid g(\zeta_m)$ in $\mathbb{Z}[\zeta_m]_{(\mathfrak{p})}$. It now suffices to prove that $h(\zeta_m) \in \mathbb{Z}[\zeta_m]_{(\mathfrak{p})}^\times$.

Since $\bar{g}\bar{h} = x^s - 1$ and $x^s - 1$ has no repeated factors mod p, we see that $\bar{g}$ and $\bar{h}$ are coprime in $\mathbb{F}_p[x]$. Hence there exist $a, b, c \in \mathbb{Z}[x]$ such that

$$a(x)g(x) + b(x)h(x) = 1 + pc(x).$$

Setting $x = \zeta_m$ gives $b(\zeta_m)h(\zeta_m) \in 1 + \mathfrak{p}$ and so $h(\zeta_m) \in \mathbb{Z}[\zeta_m]_{(\mathfrak{p})}^\times$. □

We now consider the Frobenius element $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q})$ with $p \nmid m$. Recall the isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ sends a mod m to the automorphism σ_a that sends ζ_m to ζ_m^a. So we have

$$(p, \mathbb{Q}(\zeta_m/\mathbb{Q})) = \sigma_p.$$

Chebotarev density theorem says that for any $\gcd(a, m) = 1$, the density of primes p such that $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q}) = \sigma_a$ is $1/\phi(m)$. The condition $(p, \mathbb{Q}(\zeta_m)/\mathbb{Q}) = \sigma_a$ is equivalent to $p \equiv a \pmod{m}$ and we recover Dirichlet's theorem on primes in arithmetic progressions.

If K is an intermediate extension in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, which by Kronecker-Weber includes all finite abelian extensions of $\mathbb{Q}$, then

$$\begin{aligned} p \text{ splits completely in } K \quad &\Longleftrightarrow \quad \sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K) \\ &\Longleftrightarrow \quad p \equiv a \pmod{m} \text{ for some } \sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K). \end{aligned}$$

In other words, these primes p are defined by congruence conditions. More generally, the splitting behavior of p in K is determined by the cycle structure of $(p, K/\mathbb{Q})$, which is the image of σ_p in the quotient $\mathrm{Gal}(K/\mathbb{Q})$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Hence it is determined by congruence conditions mod m.

The converse is also true. Suppose $K/\mathbb{Q}$ is a finite Galois extension such that there are $a_1, \dots, a_r, m \in \mathbb{N}$ such that for all but a density 0 of primes p, the prime p splits completely in K if and only if $p \equiv a_1, \dots, a_r \pmod{m}$. Then $K \subseteq \mathbb{Q}(\zeta_m)$ and so $K/\mathbb{Q}$ is abelian. To prove this, we show that if p splits completely in $\mathbb{Q}(\zeta_m)$, then it splits completely in K. Let M be the Galois closure of $K.\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$. There is a positive density of primes q of $\mathbb{Q}$ that splits completely in M. These primes are 1 mod m since they split completely in $\mathbb{Q}(\zeta_m)$ and also split completely in K. So one of the $a_i = 1$ mod m.

Suppose p is odd and also $m = q$ is an odd prime. Let $K = \mathbb{Q}(\sqrt{q^*})$ be the discriminant subfield of $\mathbb{Q}(\zeta_q)$ where $q^* = (-1)^{(q-1)/2}q$ differs from $\mathrm{Disc}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ by a square. Then $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/K)$ is the index 2 subgroup of C_{q-1} consisting of squares. Hence

$$p \text{ splits completely in } K \iff \sigma_p \in \{\sigma_a^2 \colon a \in (\mathbb{Z}/q\mathbb{Z})^\times\}.$$

On the one hand, p splits completely in the quadratic field K if and only if q^* is a square mod p. On the other hand, $\sigma_p = \sigma_a^2$ for some a if and only if p is a square mod q. We now have the law of quadratic reciprocity:

$$\lg pq = \lg q^* p = (-1)^{(p-1)(q-1)/4} \lg qp.$$

We now consider another interesting application. We have seen that if $f(x) \in \mathbb{Z}[x]$ is irreducible, then for a positive proporition of primes p, there exists $b \in \mathbb{Z}$ such that $p \mid f(b)$. Applying this to the polynomial $x^2 - a$ for example, we see that if a is a square mod p for all but finitely many primes p, then a is a perfect square. What about other values of n? For example, what about $x^4 - 4$ and $x^6 - 9$? Note that

$$x^8 - 16 = (x^2 - 2)(x^2 + 2)((x-1)^2 + 1)((x+1)^2 + 1).$$

For any prime p, out of -1, 2 and -2, at least one of them is a square mod p. So 16 is an 8-th power mod p for every prime p but it is not a perfect 8-th power. We prove that this is essentially the only exception.

Theorem 3.4.4

Let a be a positive integer such that $x^n - a$ has a root mod p for all sufficiently large prime p. Then either $a = b^n$ for some integer b or $8 \mid n$ and $a = 2^{n/2}b^n$ for some integer b.

The key lemma is:

Lemma 3.4.5

Let a be a positive integer such that $x^n - a$ has a root mod p for all sufficiently large prime p. Then $\mathbb{Q}(\sqrt[n]{a}) \subseteq \mathbb{Q}(\zeta_n)$. In particular, $\mathbb{Q}(\sqrt[n]{a})$ is Galois.

Note since $\mathbb{Q}(\zeta_n)$ is abelian, it doesn't matter which n-th root of a we take. We will henceforth take the positive real n-th root as $\sqrt[n]{a}$ since $a \in \mathbb{N}$.

Proof. Let $K = \mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ be the splitting field of $x^n - a$. Then for all sufficiently large prime p, the assumption that a is an n-th power mod p implies that

$$\text{if } \zeta_n \in \mathbb{F}_p, \text{ then } x^n - a \text{ splits completely in } \mathbb{F}_p[x].$$

The hypothesis $\zeta_n \in \mathbb{F}_p$ is equivalent to $n \mid p - 1$ which is equivalent to p splitting completely in $\mathbb{Q}(\zeta_n)$. The conclusion is equivalent to p splitting completely in K. Therefore, we have $K \subseteq \mathbb{Q}(\zeta_n)$. □

Applying this to $x^4 - 4$, we find that $\sqrt[4]{4} = \sqrt{2}$ does not lie in $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$. Applying this to $x^6 - 9$, we find that $\mathbb{Q}(\sqrt[3]{3})$ is not a subfield of $\mathbb{Q}(\zeta_6)$. Note also that $\mathbb{Q}(\sqrt[3]{3})$ is real and so can't contain ζ_3 and is not Galois over $\mathbb{Q}$. Applying this to $x^8 - 16$, we find that $\mathbb{Q}(\sqrt{2})$ does lie in $\mathbb{Q}(\zeta_8)$. These three examples are essentially the full proof!

Lemma 3.4.6

For $t \geq 3$, every $\mathbb{Q}(\zeta_{2^t})$ contains a unique real quadratic subfield, namely $\mathbb{Q}(\sqrt{2})$. Moreover, $\mathbb{Q}(\zeta_4)$ does not contain a real quadratic subfield

Proof. Suppose $t \geq 3$. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^t})/\mathbb{Q}) \cong C_2 \times C_{2^{t-2}}$ where the first C_2 factor is generated by complex conjugation σ_{-1} and the $C_{2^{t-2}}$ is generated by σ_5. Hence, there is a unique subgroup of index 2 containing σ_{-1}. □

Proof of Theorem ??: Let d be the largest divisor of n such that $a = c^d$ for some positive integer c. In other words, $d = \gcd(\gcd_p \mu_p(a), n)$. Then the real number $c^{d/n}$ is an n-th root of a. So it is an algebraic integer and we have $\mathbb{Q}(c^{d/n}) \subseteq \mathbb{Q}(\zeta_n)$. The minimal polynomial $f(x)$ of $c^{d/n}$ is a divisor of $x^{n/d} - c$. Since all the roots of $x^{n/d} - c$ have absolute value $c^{d/n}$, we see that $|f(0)| = c^{\deg(f)d/n}$. Hence $a = |f(0)|^{n/\deg(f)}$. This implies that $n \mid \deg(f)\mu_p(a)$ for every prime p. Hence $(n/\gcd(n, \deg(f))) \mid d$. Since $\deg(f) \leq n/d$, this is only possible if $\deg(f) = n/d$ and so $x^{n/d} - c$ is irreducible. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is abelian, we see that $\mathbb{Q}(c^{d/n})/\mathbb{Q}$ is Galois and so contains $\zeta_{n/d}$ as the splitting field of the irreducible polynomial $x^{n/d} - c$. Since $\mathbb{Q}(c^{d/n}) \subseteq \mathbb{R}$, we see that $n/d = 1$ or 2. If $n/d = 1$, then we are done.

Suppose now $n/d = 2$. Then $a = c^{n/2}$ and $c \in \mathbb{N}$ is not a square. We already know that a is a square (from for example Chebotarev applied to $x^2 - a$). So $2 \mid d$. Write $d = 2m$ so that $n = 4m$ and $a = c^{2m} = (c^{m/2})^4$. Applying Lemma **??** to the real number $c^{m/2}$ gives $\mathbb{Q}(c^{m/2}) \subseteq \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$. Hence $c^{m/2} \in \mathbb{Z}$. Since c is not a square, we have $2 \mid m$ and so $8 \mid n$. Now write $n = 2^k\ell$ for some $k \geq 3$ and odd integer ℓ. We have

$$a = c^{2^{k-1}\ell} = (c^{\ell/2})^{2^k}.$$

Applying Lemma **??** again to the irrational real number $c^{\ell/2}$ gives $\mathbb{Q}(c^{\ell/2}) \subseteq \mathbb{Q}(\zeta_{2^k})$. Hence, we have $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{2})$. So $c = 2b^2$ for some positive integer b and $a = 2^{n/2}b^n$.

4 (Local) Class Field Theory via Lubin-Tate Theory

§4.1 Main theorems of (Local) Class Field Theory

For the remainder of the semester, we will focus on Local class field theory. In this section, we will discuss the norm groups and give the statement of the main theorems.

Throughout, K is a non-archimedean local field with absolute value $|.|$, valuation ring A, group of units U_K and residue field $k = \mathbb{F}_q$ with characteristic p. We start with the unramified case.

Proposition 4.1.1

Let L/K be a finite unramified extension of K of degree n. Then the norm map $N_{L/K} : U_L \to U_K$ is surjective.

Proof. Let ℓ denote the residue field of L. We have a filtration on U_K and U_L via $U_K^n = 1 + \pi_K^n A$ and $U_K^n = 1 + \pi_L^n \mathcal{O}_L$ where π_K and π_L are uniformizers of K and L. The norm map descends to the quotients $U_L^n / U_L^{n+1} \to U_K^n / U_K^{n+1}$ as follows:

- If $n = 0$, then $N_{L/K}$ is the norm map $N_{\ell/k} : \ell^\times \to k^\times$ for finite fields;
- If $n \geq 1$, then $N_{L/K}$ is the trace map $\mathrm{Tr}_{\ell/k} : \ell \to k$ for finite fields;

via the identification $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$. These maps on the residue fields are all surjective. Hence we are done by completeness. □

Corollary 4.1.2

Let L/K be a finite unramified extension of K of degree n. Then

$$N_{L/K}(L^\times) = U_K \times \pi_K^{n\mathbb{Z}}.$$

Let $\mathrm{Frob}_{L/K} \in \mathrm{Gal}(L/K)$ denote the Frobenius map that reduces to $x \mapsto x^q$ on the residue field. Then there is a group isomorphism

$$K^\times / N_{L/K}(L^\times) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(L/K)$$

sending a uniformizer of K to $\mathrm{Frob}_{L/K}$.

Proof. This follows because $N_{L/K}(U_L) = U_K$ and $\mu(N_{L/K}(\pi_L)) = n$. □

Note that in general, we have $\mu(N_{L/K}(\pi_L)) = f_{L/K}$. So the norm group $N_{L/K}(L^\times)$ contains a uniformizer of K if and only if L/K is totally ramified.

Let K^{ab} denote the maximal abelian extension of K (in some algebraic closure). The main theorem of local class field theory is:

Theorem 4.1.3

There exists a unique homomorphism

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that:

1. for any uniformizer π of K and any finite unramified extension L/K, $\phi_K(\pi)|_L = \mathrm{Frob}_{L/K}$;
2. for any finite abelian extension L/K, ϕ_K induces an isomorphism

$$\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K).$$

In particular,

$$\# K^\times/N_{L/K}(L^\times) = [L : K].$$

The maps $\phi_K, \phi_{L/K}$ are called the **local reciprocity maps** or local Artin maps. Some other common notations are

$$\phi_{L/K}(a) = \mathrm{rec}_{L/K}(a) = (a, L/K) = \lg L/K a.$$

We will write $N(L^\times)$ for $N_{L/K}(L^\times)$. These are the **norm groups** in $K^\times$ (where L/K is a finite abelian extension). Abelian extensions of K are determined by their norm groups.

Corollary 4.1.4

The map $L \mapsto N(L^\times)$ defines an inclusion-reversing bijection between finite abelian extensions of K and norm groups in $K^\times$ with

$$N((L_1L_2)^\times) = N(L_1^\times) \cap N(L_2^\times), \qquad N((L_1 \cap L_2)^\times) = N(L_1^\times) \cdot N(L_2^\times).$$

Moreover, every subgroup of $K^\times$ containing a norm group is a norm group.

Proof. Transitivity of norms implies that the map $L \mapsto N(L^\times)$ is inclusion-reversing (note this does not need Theorem **??**). Now Theorem **??** implies that $a \in N(L^\times)$ if and only if $\phi_K(a)|_L = 1$. This proves the result on $N((L_1L_2)^\times)$. Now if $N(L_2^\times) \supset N(L_1^\times)$, then $N((L_1L_2)^\times) = N(L_1^\times) \cap N(L_2^\times) = N(L_1^\times)$ and so $[L_1L_2 : K] = [L_1 : K]$, which implies that $L_2 \subset L_1$. Therefore, the map $L \mapsto N(L^\times)$ is bijective.

Suppose N is a subgroup of $K^\times$ containing $N(L^\times)$. Then $\phi_{L/K}(N)$ is a subgroup of $\mathrm{Gal}(L/K)$, with fixed field E. Then $a \in N$ if and only if $\phi_{L/K}(a)|_E = 1$. Hence $N = N(E^\times)$. Finally, $L_1 \cap L_2$ is contained in L_1 and L_2 and so $N((L_1 \cap L_2)^\times) \supseteq N(L_1^\times) \cdot N(L_2^\times)$. Conversely, $N(L_1^\times) \cdot N(L_2^\times) = N(E^\times)$ for some E contained in L_1 and L_2. So E is contained in $L_1 \cap L_2$ and $N(E^\times) \supseteq N((L_1 \cap L_2)^\times)$. Therefore, we have equality. □

Proposition 4.1.5

Let L be a finite abelian extension of K. Then $N(L^\times)$ is an open subgroup of $K^\times$.

Proof. Note that a closed subgroup of finite index is open, since its complement is a finite union of cosets, each of which is closed. Note also that the norm map is continuous because it is given by polynomials after choosing a K-basis for L. This is not enough to conclude that $N(L^\times)$ is closed, but it does imply that $N_{L/K}(U_L)$ is closed since U_L is compact. Since $N_{L/K}(U_L) = U_K \cap N(L^\times)$, we see that

$$U_K/N_{L/K}(U_L) \hookrightarrow K^\times/N(L^\times)$$

which is finite. Hence $N_{L/K}(U_L)$ is open in U_K, which is then open in $K^\times$. Finally any subgroup containing an open neighborhood of 1 is automatically open (any $a \in N(L^\times)$ is contained in the open set $aN_{L/K}(U_L) \subset N(L^\times)$). □

Remark: When K is characteristic 0, all finite index subgroups are open. They all contain $K^{\times m}$ for some positive integer m and we saw before that every element sufficiently close to 1 has an m-th root. When K has characteristic p, this is not true. For example consider $K = \mathbb{F}_p((t))$. The first unit group $U_{K,1} = 1 + t\mathbb{F}_p[[t]]$ is a $\mathbb{Z}_p$-module and one observes that $1 + t^m$ for $p \nmid m$ are all $\mathbb{Z}_p$-independent. In fact,

$$U_{K,1} \cong \prod_{\mathbb{N}} \mathbb{Z}_p.$$

Consider the quotient $\prod_{\mathbb{N}} \mathbb{F}_p$, which has a dense subset $\bigoplus_{\mathbb{N}} \mathbb{F}_p$. The maximal ideal I of $\prod_{\mathbb{N}} \mathbb{F}_p$ containing $\bigoplus_{\mathbb{N}} \mathbb{F}_p$ has index p, since its residue field is $\mathbb{F}_p$ as every element satisfies $x^p = x$. Note that I is not closed. Let U be the pre-image of I in $U_{K,1}$. Then $U \times t^{\mathbb{Z}}$ is a subgroup of K of finite index that is not closed.

The second main theorem in LCFT is the local existence theorem:

Theorem 4.1.6

The norm groups in $K^\times$ are exactly the open subgroups of $K^\times$ of finite index.

Remark: We remark that these results hold trivially when $K = \mathbb{R}$ and even more trivially when $K = \mathbb{C}$. The group $\mathbb{R}^\times$ has exactly two subgroups of finite index; $\mathbb{R}^+ = N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times)$ and $\mathbb{R}^\times = N_{\mathbb{R}/\mathbb{R}}(\mathbb{R}^\times)$.

Even though each $\phi_{L/K}$ is an isomorphism, the map ϕ_K is not an isomorphism. We will get an isomorphism if we complete $K^\times$ with respect to the norm topology, where the norm groups (open subgroups of finite index) form a fundamental system of neighborhood of 1. Let $\widehat{K^\times}$ denote this completion. We then have an isomorphism

$$\phi : \widehat{K^\times} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

From the fundamental system of open subgroups of finite index:

$$K^\times \cong U_K \times \pi^{\mathbb{Z}} \cong U_K \times \mathbb{Z} \supset (1 + \mathfrak{p}^n) \times m\mathbb{Z},$$

we see that

$$\widehat{K^\times} \cong U_K \times \hat{\mathbb{Z}}.$$

Now U_K and $\hat{\mathbb{Z}}$ are closed subgroups and so are their images under ϕ. By infinite Galois theory, they correspond to subfields of K^{ab}. Recall that the norm groups from unramified extensions are of the form $U_K \times e\mathbb{Z}$. The subfield of K^{ab} fixed by $\phi(U_K)$ is the maximal unramified extension K^{un}. For each positive integer n, let $K_{\pi,n}$ denote the finite extension of K with norm group $(1+\mathfrak{p}^n)\times\mathbb{Z}$. The union $K_\pi = \bigcup_n K_{\pi,n}$ is the subfield of K^{ab} fixed by $\phi(\pi)$. We have

$$K^{\mathrm{ab}} = K^{\mathrm{un}} K_\pi.$$

Observe that $\phi(\pi)$ is the element acting trivially on K_π and acting via the Frobenius on K^{un}. The same is true for any other possible reciprocity map ϕ'. In other words, any two possible reciprocity maps have the same image on every uniformizer. This proves uniqueness, assuming existence and Theorem **??**. We note also that Theorem **??** follows from Corollary **??** and the following result.

Proposition 4.1.7

For any positive integers n, m. There is a finite abelian extension L/K whose norm group is $(1+\mathfrak{p}^n)\times\pi^{m\mathbb{Z}}$.

When $K=\mathbb{Q}_p$ and $\pi = p$, the field $K_{\pi,n}$ is $\mathbb{Q}_p(\zeta_{p^n})$, assuming LCFT and recalling that we proved that the norm group of $\mathbb{Q}_p(\zeta_{p^n})$ contains $1+p^n\mathbb{Z}_p$ in HW2. Note that $\mathbb{Q}_p(\zeta_p)$ is generated by the roots of

$$f(T) = (1+T)^p - 1 = pT + \cdots + T^p$$

and we can view $\mathbb{Q}_p(\zeta_{p^n})$ as generated by the roots of

$$f^{(n)}(T) := f(f(\cdots f(T)\cdots)) = p^n T + \cdots + T^{p^n} = (1+T)^{p^n} - 1.$$

Now

$$K_\pi = \mathbb{Q}_p(\zeta_{p^\infty}) = \varinjlim_n \mathbb{Q}_p(\zeta_{p^n}).$$

The isomorphism

$$\mathbb{Z}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$$

comes from the compatible system of isomorphisms

$$(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p).$$

When attempting to generalize this to an arbitrary K and π, the key difficulty is the isomorphisms

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z} \cong \langle\zeta_{p^n}\rangle \cong \{\alpha\in\bar{\mathbb{Q}}_p\colon f^{(n)}(\alpha)=0\}$$

where the last map is given by $u\mapsto u-1$. The induced group structure on the set of roots of $f^{(n)}$ can be extended to the set $\Lambda = \{\alpha\in\bar{\mathbb{Q}}_p\colon |\alpha|<1\}$ via $x+_f y = (1+x)(1+y)-1 = x+y+xy$. The action of $\mathbb{Z}_p$ on the set of roots of $f^{(n)}$ can also be extended to Λ via

$$[a](x) = (1+x)^a - 1 = \sum_{m=1}^{\infty}\frac{a(a-1)\cdots(a-m+1)}{m!}x^m.$$

We note that $[p](T) = f(T)$.

To generalize this to an arbitrary K and π, it seems natural to take $f(T) = \pi T + T^q$. Here π is needed to make f/T Eisenstein; and q is needed to have the correct degree. Then we need a group law on $\Lambda = \{\alpha\in\bar{K}\colon |\alpha|<1\}$ and an A-module structure so that $[\pi](T) = f(T)$. To do this, we need the theory of formal group laws.

§4.2 Lubin-Tate formal groups

Let A be a commutative ring. We can add and multiply power series with coefficients in A inside the ring $A[[T]]$. We can also compose two power series f and g if $g \in TA[[T]]$. We write $f \circ g(T) = f(g(T))$. Similarly, if $f \in A[[T_1, \dots, T_m]]$ and $g_1, \dots, g_m \in A[[S_1, \dots, S_n]]$, then we can compose them to get $f(g_1, \dots, g_m)$ if the constant terms in $g_1, \dots, g_m$ are all 0.

A **(one parameter commutative) formal group law** is a power series $F \in A[[X, Y]]$ such that:

(a) $F(Y, X) = F(X, Y)$;

(b) $F(X, 0) = X$;

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

Note that (a) and (b) imply that F is of the form

$$F(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j.$$

It is then easy to prove that there exist $i_F(X) = -X + \sum_{i=2}^{\infty} a_i X^i$ such that $F(X, i_F(X)) = 0$.

Given two formal group laws $F, G \in A[[X, Y]]$, a **homomorphism** $f : F \to G$ is a power series $f \in TA[[T]]$ such that

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

Lemma 4.2.1

Let $f \in TA[[T]]$. Then there exists $g \in TA[[T]]$ with $f \circ g = T$ if and only if $f \in T(A[[T]])^\times$. In this case, g is unique and $g \circ f = T$. We write $g = f^{(-1)}$.

Proof. The first statement and the uniqueness of g follow by writing out the coefficients. To prove $g \circ f = T$, we note the associativity of composition:

$$f \circ (g \circ h) = (f \circ g) \circ h$$

which follows because $f \circ g$ is linear in f and $T^n \circ g = g^n$. Suppose now $f \circ g = T$. Then $g \in T(A[[T]])^\times$ as well and there exists $h \in TA[[T]]$ such that $g \circ h = T$. Associativity then gives $f = h$. □

When $f^{(-1)}$ exists for a homomorphism $f : F \to G$, we see that $f^{(-1)}$ is a homomorphism $G \to F$ and we say f is an **isomorphism**.

The following result will be proved in HW5. We won't use it here, but it is quite useful when studying elliptic curves over local fields.

Theorem 4.2.2

When A has characteristic 0, all formal group laws are isomorphic to the formal additive group $\widehat{\mathbb{G}_a}$ with $F(X, Y) = X + Y$ over $A \otimes_{\mathbb{Z}} \mathbb{Q}$.

When A is complete with respect to a non-archmedean absolute value $|.|$, let $\mathfrak{m} = \{a \in A \colon |a| < 1\}$. Then a formal group law F defines an abelian group structure on $\mathfrak{m}$ via

$$x +_F y = F(x, y), \qquad -_F x = i_F(x).$$

and a homomorphism $h : F \to G$ defines a group homomorphism

$$x \mapsto h(x) : (\mathfrak{m}, +_F) \to (\mathfrak{m}, +_G).$$

The usual group structure on $\mathfrak{m}$ is given by $\widehat{\mathbb{G}_a}$. The pullback of the multiplicative group structure on $1 + \mathfrak{m}$ via the map $x \mapsto 1 + x$ is the group structure on $\mathfrak{m}$ given by the multiplicative formal group $\widehat{\mathbb{G}_m}$ with $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$, which admits the polynomial $f(T) = (1 + T)^p - 1$ as an endomorphism as

$$F(f(T), f(S)) = (1 + T)^p(1 + S)^p - 1 = f(F(T), F(S)).$$

The ring $A[[T]]$ itself is complete with respect to the T-adic absolute value. Hence given $f, g \in TA[[T]]$ and a formal group law G, we can define

$$f +_G g = G(f(T), g(T)), \qquad -_G f = i_G(f).$$

Proposition 4.2.3

For any formal group laws F and G, the set $\mathrm{Hom}(F, G)$ of homomorphisms becomes an abelian group with $+_G$. When $F = G$, the endomorphism group $\mathrm{End}(F) = \mathrm{Hom}(F, F)$ with $+_F$ is a (non-commutative) ring with $f \circ g$.

Proof "by elimination": What else could it be? □

We return to the situation of non-archimedean local field K, valuation ring A, and residue field $\mathbb{F}_q$. Fix a uniformizer π. Let $\mathcal{F}_\pi \subset A[[T]]$ consist of all f such that

$$f(T) \equiv \pi T \pmod{T^2} \qquad \text{and} \qquad f(T) \equiv T^q \pmod{\pi}.$$

For example $\pi T + T^q \in \mathcal{F}_\pi$ in general, and $(1 + T)^p - 1 \in \mathcal{F}_p$ in $\mathbb{Q}_p$.

Theorem 4.2.4

There is a unique formal group law F_f admitting f as an endomorphism.

This is the **Lubin-Tate** formal group of f. To prove its existence, note that we are looking for a power series $F = X + Y + \text{higher order term}$ such that $F(f(X), f(Y)) = f(F(X, Y))$.

But wait! Using the time stone, we foresee a future where we need to work with unramified extensions of K. So let's do it right! Let E/K be a *complete* unramified extension of K with valuation ring A_E. One can take E to be a finite unramified extension of K or the completion of K^{un}. Let σ denote the Frobenius of K extended to E. In other words, σ (topologically if $E = K^{\mathrm{un}}$) generates $\mathrm{Gal}(E/K)$. For any uniformizer ω of E, define $\mathcal{F}_\omega \subseteq A_E[[T]]$ to consist of all f such that

$$f(T) \equiv \omega T \pmod{T^2} \qquad \text{and} \qquad f(T) \equiv T^q \pmod{\omega}.$$

We note that we are still using the size of the residue field of K for q, and not that of E. We aim to find a formal group law $F_f \in A_E[[X, Y]]$ such that $f \in \mathrm{Hom}(F_f, F_f^\sigma)$. We claim that it is enough to prove that for any $m \in \mathbb{N}$, the existence and uniqueness of some $F \in A_E[[X_1, \dots, X_m]]$ such that

$$F(X_1, \dots, X_m) = X_1 + \cdots + X_m + \cdots \qquad \text{and} \qquad F^\sigma(f(X_1), \dots, f(X_m)) = f(F(X_1, \dots, X_m)). \tag{4.1}$$

The existence of (**??**) for $m = 2$ gives F_f.

- Set $G_2(X, Y) = F_f(Y, X) = X + Y + \cdots$. Then

  $$G_2^\sigma(f(X), f(Y)) = F_f^\sigma(f(Y), f(X)) = f(F_f(Y, X)) = f(G_2(X, Y)).$$

  Hence, the uniqueness of (**??**) when $m = 2$ implies that $F_f(X, Y) = F_f(Y, X)$.

- Set $G_1(X) = F_f(X, 0) = X + \cdots$. Then

  $$G_1^\sigma(f(X)) = F_f^\sigma(f(X), f(0)) = f(F_f(X, 0)) = f(G_1(X)).$$

  Since the same is true for X, we have $F_f(X, 0) = X$ using (**??**) with $m = 1$.

- Set $G_3(X, Y, Z) = F_f(X, F_f(Y, Z))$. Then

  $$G_3^\sigma(f(X), f(Y), f(Z)) = F_f^\sigma(f(X), F_f^\sigma(f(Y), f(Z))) = f(F_f(X, F_f(Y, Z)) = f(G(X, Y, Z)).$$

  The same is true for $H_3(X, Y, Z) = F_f(F_f(X, Y), Z)$. Hence (**??**) with $m = 3$ gives $F_f(X, F_f(Y, Z)) = F_f(F_f(X, Y), Z)$.

We now state and prove a more general version of (**??**). It is not important that we have the same f on both sides, or that the linear coefficients of F are all 1. We consider any $f \in \mathcal{F}_\pi$ and any $g \in \mathcal{F}_\omega$. Suppose $F(X_1, \dots, X_m) = a_1X_1 + \cdots + a_mX_m + \cdots$. Then the linear coefficients of $F^\sigma \circ f$ are $a_i^\sigma \cdot \pi$ while the linear coefficients of $g \circ F$ are $\omega \cdot a_i$. Hence we need each a_i to belong to

$$A_{\pi,\omega}^E = \{a \in A_E \colon a^\sigma / a = \omega/\pi\}.$$

Note that when $\pi = \omega$, this is just A.

Proposition 4.2.5

Let E/K be a complete unramified extension with uniformizers π, ω. Let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$ and let $a_1, \dots, a_m \in A_{\pi,\omega}^E$. Then there exists a unique $F(X_1, \dots, X_m) \in A_E[[X_1, \dots, X_m]]$ such that

(a) $F \equiv a_1X_1 + \cdots + a_mX_m \pmod{(X_1, \dots, X_m)^2}$

(b) $g(F(X_1, \dots, X_m)) = F^\sigma(f(X_1), \dots, f(X_m))$

Proof. Just do the only thing possible and it works. We write $g \circ F$ and $F^\sigma \circ f$ to simplify notation. Let $I = (X_1, \dots, X_m)$. We prove by the induction the existence and uniqueness of F_r satisfying (a) and (b) mod I^{r+1}. When $r = 1$, $F_1 = a_1X_1 + \cdots + a_mX_m$ is clearly the unique choice since $a_i^\sigma \pi = \omega a_i$ for all i. Suppose we are now given F_r. We prove the uniqueness and existence of a homogeneous polynomial $h(X_1, \dots, X_m) \in A_E[X_1, \dots, X_m]$ of degree $r + 1$ such that $g \circ (F_r + h) = (F_r + h)^\sigma \circ f$ mod I^{r+2}. We have

$$\begin{aligned} g \circ (F_r + h) &\equiv g \circ F_r + \omega h \pmod{I^{r+2}} \\ (F_r + h)^\sigma \circ f &\equiv F_r^\sigma \circ f + \pi^{r+1} h^\sigma \pmod{I^{r+2}} \end{aligned}$$

since $f, g \equiv \pi T, \omega T \pmod{T^2}$. Since $f, g \equiv T^q \pmod{\pi}$, we have

$$g \circ F_r - F_r^\sigma \circ f \equiv F_r(X_1, \ldots, X_m)^q - F_r^\sigma(X_1^q, \ldots, X_m^q) = 0 \text{ in } (A_E/(\pi))[X_1, \ldots, X_m].$$

Fix any monomial of degree $r+1$. Its coefficient in $g \circ F_r - F_r^\sigma \circ f$ is of the form $\pi\beta$ for some $\beta \in A_E$. Hence its coefficient α in h should satisfy

$$\pi^{r+1}\alpha^\sigma - \omega\alpha = -\pi\beta.$$

Let $v = \pi\beta/\omega \in A_E$ and $z = \pi^{r+1}/\omega \in (\pi)$. Then

$$\alpha = v + z\alpha^\sigma = v + zv^\sigma + zz^\sigma\alpha^{\sigma^2} = \cdots = v + zv^\sigma + zz^\sigma v^{\sigma^2} + zz^\sigma z^{\sigma^2} v^{\sigma^3} + \cdots$$

has a unique limit in A_E since each $z^{\sigma^n} \in (\pi)$. □

As a consequence, we have our desired formal group law F_f.

Theorem 4.2.6

Let E/K be a complete unramified extension with uniformizer π. For any $f \in \mathcal{F}_\pi$, there exists a unique formal group law $F_f \in A_E[[X, Y]]$ such that $f \in \operatorname{Hom}(F_f, F_f^\sigma)$.

Corollary 4.2.7

For any $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_\omega$ and $a \in A_{\pi,\omega}^E$, there is a unique $[a]_{f,g} \in A_E[[T]]$ such that

$$[a]_{f,g}(T) \equiv aT \pmod{T^2}, \qquad g \circ [a]_{f,g} = [a]_{f,g}^\sigma \circ f.$$

Moreover, $[a]_{f,g} \in \operatorname{Hom}(F_f, F_g)$ and $[1]_{f,f}(T) = T$. For any $b \in A_{\pi,\omega}^E$, we have

$$[a+b]_{f,g} = [a]_{f,g} +_{F_g} [b]_{f,g}$$

For any $b \in A_{\omega,\omega'}^E$ and any $h \in \mathcal{F}_{\omega'}$ we have

$$[ab]_{f,h} = [b]_{g,h} \circ [a]_{f,g}.$$

In particular, $F_f \cong F_g$ over A_E if $A_{\pi,\omega}^E \cap A_E^\times$ is nonempty. When $\pi = \omega$, this is always true. In general, this is true over B.

Proof. We need to prove

$$[a]_{f,g} \circ F_f = F_g \circ [a]_{f,g}.$$

Both have linear terms $aX + aY$ and

$$g \circ [a]_{f,g} \circ F_f = [a]_{f,g}^\sigma \circ f \circ F_f = ([a]_{f,g} \circ F_f)^\sigma \circ f,$$

$$g \circ F_g \circ [a]_{f,g} = F_g^\sigma \circ g \circ [a]_{f,g} = (F_g \circ [a]_{f,g})^\sigma \circ f.$$

Therefore, they are equal by Proposition **??**. The rest follows similarly. □

Corollary 4.2.8

For any $f \in \mathcal{F}_\pi$, $g \in \mathcal{F}_\omega$ and $a \in A_{\pi,\omega}^E$ we have

$$F_{f^\sigma} = F_f^\sigma \qquad \text{and} \qquad [a]_{f,g}^\sigma = [a^\sigma]_{f^\sigma, g^\sigma}.$$

Corollary 4.2.9

For any $f \in \mathcal{F}_\pi$, there is an injective ring homomorphism $A \hookrightarrow \mathrm{End}(\mathcal{F}_f)$ sending a to $[a]_f := [a]_{f,f}$.

Example: Suppose $f \in \mathcal{F}_\pi$. Then $f^\sigma \in \mathcal{F}_{\pi^\sigma}$ and by definition $\pi \in A^E_{\pi,\pi^\sigma}$ and we have

$$[\pi]_{f,f^\sigma} : \mathcal{F}_f \to \mathcal{F}_{f^\sigma} = \mathcal{F}_f^\sigma \qquad \text{and} \qquad [\pi]_{f,f^\sigma} \equiv \pi T \pmod{T^2}.$$

Then we see that $[\pi]_{f,f^\sigma} = f$. This suggests that instead of considering $f \circ f$, we should consider

$$f^\sigma \circ f = [\pi^\sigma]_{f^\sigma, f^{\sigma^2}} \circ [\pi]_{f,f^\sigma} = [\pi\pi^\sigma]_{f,f^{\sigma^2}}.$$

In general, we define for any positive integer n,

$$f_n = f^{\sigma^{n-1}} \circ \cdots \circ f^\sigma \circ f = [\pi\pi^\sigma \cdots \pi^{\sigma^{n-1}}]_{f,f^{\sigma^n}}.$$

Recall that when $f(T) = (1+T)^p - 1$ and we are working over $\mathbb{Q}_p$, this $f_n(T)$ is simply $(1+T)^{p^n} - 1$.

§4.3 The Lubin-Tate extension K^{LT}

Let E^s denote a separable closure of E and let $\Lambda = \{\alpha \in E^s \colon |\alpha| < 1\}$. Suppose π is a uniformizer of E and $f \in \mathcal{F}_\pi$. Note that Λ is not complete, but any two $\alpha, \beta \in \Lambda$ belong to some finite extension L/K, so the formal group law $\mathcal{F}_f$ defines a group law $+_f$ on Λ and the injection $A \hookrightarrow \mathrm{End}(\mathcal{F}_f)$ gives Λ an A-module structure. Define

$$\Lambda_n^{(f)} = \Lambda[f_n] = \{\alpha \in \Lambda \colon f_n(\alpha) = 0\}, \qquad E_{\pi,n} = E(\Lambda_n^{(f)}).$$

Proposition 4.3.1

The set $\Lambda_n^{(f)}$ is finite and is an A-submodule of $(\Lambda, +_f)$. If π_0 is a uniformizer of K, then

$$\Lambda_n^{(f)} = \Lambda[\pi_0^n] = \{\alpha \in \Lambda \colon [\pi_0^n](\alpha) = 0\}.$$

The field $E(\Lambda_n^{(f)})$ is a finite extension of E, independent of the choice of $f \in \mathcal{F}_\pi$.

Proof. Since $f_n(T) \equiv T^{q^n} \pmod{\pi}$, we know that f_n has at most q^n roots in Λ by Weierstrass preparation (over the completion of $\bar{E}$): any power series is a product of a unit and a polynomial; and a unit does not have any root in Λ.

Since $f_n \in \mathrm{Hom}(F_f, F_{f^{\sigma^n}})$, we have

$$f_n(\alpha +_f \beta) = f_n(\alpha) +_{f^{\sigma^n}} f_n(\beta) = 0$$

and so $\Lambda_n^{(f)}$ is a subgroup of Λ. For any uniformizer ω of E, and any $g \in \mathcal{F}_\omega$ and $a \in A^E_{\pi,\omega}$, we have

$$g_n \circ [a]_{f,g} = [a\omega\omega^\sigma \cdots \omega^{\sigma^{n-1}}]_{f,g^{\sigma^n}} = [a']_{f^{\sigma^n}, g^{\sigma^n}} \circ [\pi\pi^\sigma \cdots \pi^{\sigma^{n-1}}]_{f,f^{\sigma^n}} = [a']_{f^{\sigma^n}, g^{\sigma^n}} \circ f_n$$

where

$$a' = auu^\sigma \cdots u^{\sigma^{n-1}} \in A^E_{\pi^{\sigma^n}, \omega^{\sigma^n}}, \qquad \text{and} \qquad u = \frac{\omega}{\pi}.$$

So $[a]_{f,g}$ sends the roots of f_n to the roots of g_n. Restricting to $\omega = \pi$ and $g = f$ and $a \in A$, we see that $[a]_{f,f}$ preserves $\Lambda_n^{(f)}$. Hence, $\Lambda_n^{(f)}$ is a sub-A-module of Λ.

Since π_0^n and $\pi\pi^\sigma \cdots \pi^{\sigma^{n-1}}$ have the same valuation, we can write $\pi_0^n = \pi\pi^\sigma \cdots \pi^{\sigma^{n-1}} v_n$ for some unit $v_n \in A_E^\times$. Then $[\pi_0^n]_{f,f} = [v_n]_{f^{\sigma^n},f} \circ [\pi\pi^\sigma \cdots \pi^{\sigma^{n-1}}]_{f,f^{\sigma^n}}$. Since $[v_n]_{f^{\sigma^n},f} \in TA_E[[T]]^\times$ is invertible, we see that $\Lambda = \Lambda[\pi_0^n]$.

Now suppose $\omega = \pi$ and $g \in \mathcal{F}_\pi$. Using $a = 1$, we get a bijection

$$[1]_{f,g} : \Lambda_n^{(f)} \to \Lambda_n^{(g)}$$

defined by a power series in $A_E[[T]]$. To prove that they generate the same extension over E, we need the following lemma.

Lemma 4.3.2

Let L/E be finite Galois and let $\tau \in \mathrm{Gal}(L/E)$. Let $h(T_1, \ldots, T_m) \in A_E[[T_1, \ldots, T_m]]$. Then for any $\alpha_1, \ldots, \alpha_m \in L$ with absolute value less than 1, we have

$$h(\tau(\alpha_1), \ldots, \tau(\alpha_m)) = \tau(h(\alpha_1, \ldots, \alpha_m)).$$

Proof. For any $t \geq 1$, let $h_t(T_1, \ldots, T_m)$ be the polynomial formed from $h(T)$ by keeping only the terms with degree at most t. Write $\alpha = (\alpha_1, \ldots, \alpha_m)$ Hence

$$h(\tau(\alpha)) = \lim_{t\to\infty} h_t(\tau(\alpha)) = \lim_{t\to\infty} \tau(h_t(\alpha)) = \tau(h(\alpha)),$$

where the second equality follows from the conitnuity of τ, as it is metric-preserving. □

We can now complete the proof of Proposition **??**. Let $L = E(\Lambda_n^{(f)}, \Lambda_n^{(g)})$. Then for any $\tau \in \mathrm{Gal}(L/E)$ and any $\alpha \in \Lambda_n$, we have

$$[1]_{f,g}(\tau(\alpha)) = \tau([1]_{f,g}(\alpha)).$$

Hence we see that τ acts trivially on $\Lambda_n^{(f)}$ if and only if it acts trivially on $[1]_{f,g}(\Lambda_n^{(f)}) = \Lambda_n^{(g)}$. Therefore, $E(\Lambda_n^{(f)}) = E(\Lambda_n^{(g)})$. □

Theorem 4.3.3

Let π be a uniformizer of E and let π_0 be a uniformizer of K. The extension $E_{\pi,n}/E$ is Galois and totally ramified of degree $(q-1)q^{n-1}$. Its norm group contains $\pi^{\sigma^{n-1}}$. Moreover, there is a compatible system of isomorphisms

$$(A/(\pi_0^n))^\times \cong \mathrm{Gal}(E_{\pi,n}/E).$$

On passing to the inverse limit, we have an isomorphism

$$U_K = A^\times \cong \mathrm{Gal}(E_\pi/E).$$

Proof. By Proposition **??**, we may fix $f = \pi T + T^q$. We prove first that $E_{\pi,n}/E$ is the splitting field of f_n and so is Galois. (Separability is left as an exercise.) It suffices to prove that any nonzero root of f_n in $\bar{E}$ has absolute value less than 1. Let μ denote the normalized valuation on E so that $\mu(\pi) = 1$. We prove by induction on n that if $\alpha \in E^s$ is either 0 or satisfies $0 < \mu(\alpha) \leq 1$, then any root γ of $f_n - \alpha$ also is either 0 or satisfies $0 < \mu(\gamma) \leq 1$. Define $f_0(T) = T$ so that the base case $n = 0$ is automatic. Suppose $n \geq 1$. If γ is a root of $f_n(T) - \alpha$, then $f_{n-1}(\gamma)$ is a root β of

$$f^{\sigma^{n-1}}(T) - \alpha = T^q + \pi^{\sigma^{n-1}}T - \alpha.$$

If $\alpha = 0$, then either $\beta = 0$ or β is a root of the Eisenstein polynomial $T^{q-1} + \pi^{\sigma^{n-1}}$ which has valuation $1/(q-1) \in (0, 1]$. If $\alpha \neq 0$, then from the Newton polygon, we see that $\mu(\beta) = \mu(\alpha)/q \in (0, 1]$. We are then done by induction applied to $f_{n-1}(\gamma) = \beta$.

Let $\pi_1, \ldots, \pi_n \in \Lambda$ such that

$$\pi_n \xmapsto{f} \pi_{n-1} \xmapsto{f^\sigma} \pi_{n-2} \mapsto \cdots \mapsto \pi_1 \xmapsto{f^{\sigma^{n-1}}/T} 0.$$

Then

- $f_n(\pi_n) = 0$ and so $\pi_n \in \Lambda_n$.
- $E(\pi_1)/E$ is totally ramified of degree $q-1$, as $f^{\sigma^{n-1}}/T = T^{q-1} + \pi^{\sigma^{n-1}}$ is Eisenstein.
- $E(\pi_k)/E(\pi_{k-1})$ is totally ramified of degree q with π_k being a uniformizer for $E(\pi_k)$ for $k \geq 2$, as $f^{\sigma^{n-k}} - \pi_{k-1} = T^q + \pi^{\sigma^{n-k}}T - \pi_{k-1}$ is Eisenstein.

Note that $E(\pi_n)$ is a subfield of $E_{\pi,n}$ of degree $(q-1)q^{n-1}$. (Be a bit careful with the notation here, the π_i here also depend on n. For example, we may have $\pi_{n-1} \notin \Lambda_{n-1}$.)

The A-module $\Lambda_n = \Lambda[\pi_0^n]$ is torsion and π_0-primary. So it decomposes as a product of cyclic A-modules of the form $A/(\pi_0^d)$. Similar to last time, we write $\pi_0^{n-1} = \pi\pi^\sigma \cdots \pi^{\sigma^{n-2}}v_{n-1}$ for some unit $v_{n-1} \in A_E^\times$. Then we have

$$[\pi_0^{n-1}](\pi_n) = [v_{n-1}]_{f^{\sigma^{n-1}},f}(\pi_1) \neq 0.$$

Hence π_n generates a cyclic A-submodule of Λ_n isomorphic to $A/(\pi_0^n)$. Then from

$$q^n = \#A/(\pi_0^n) \leq \#\Lambda_n \leq \deg(f_n) \leq q^n,$$

we conclude that $\Lambda_n \cong A/(\pi_0^n)$ and is generated by π_n. (Note this also proves that the roots of f_n are all distinct and belong to E^s.)

By Lemma **??**, we know that any $\tau \in \mathrm{Gal}(E_{\pi,n}/E)$ commutes with any power series in $A_E[[T_1, \ldots, T_m]]$. Commuting with f_n implies that $\tau : \Lambda_n \to \Lambda_n$. Commuting with $F_f(X, Y)$ implies that it respects the abelian group structure $+_{F_f}$. Commuting with any $[a]_{f,f}$ for $a \in A$ implies that it is an A-module homomorphism on Λ_n. Since $E_{\pi,n}$ is generated by Λ_n, we have an injection

$$\mathrm{Gal}(E_{\pi,n}/E) \hookrightarrow \mathrm{End}_A(\Lambda_n) \cong (A/(\pi_0^n))^\times.$$

Comparing sizes then gives the isomorphism and $E_{\pi,n} = E(\pi_n)$ and $\mathrm{Gal}(E_{\pi,n}/E) \cong (A/(\pi_0^n))^\times$. The isomorphisms are compatible with the restriction map from $\mathrm{Gal}(E_{\pi,n+1}/E)$ to $\mathrm{Gal}(E_{\pi,n}/E)$ since they are all induced by $[a]_{f,f}$ on Λ. Hence on taking inverse limits, we have

$$\mathrm{Gal}(E_\pi/E) \cong A^\times.$$

For any $a \in A^\times$, we will write $[a]_f$ for the element of $\mathrm{Gal}(E_\pi/E)$ that acts via the power series $[a]_{f,f}$ on any Λ_n. It does not act on the entire E_π as the power series $[a]_{f,f}$.

Finally to prove the norm statement, we saw before that the minimal polynomial of π_k over $E(\pi_{k-1})$ is $f^{\sigma^{n-k}}(T) - \pi_{k-1}$ when $k \geq 2$; and the minimal polynomial of π_1 over E is $T^{q-1} + \pi^{\sigma^{n-1}}$. Hence

$$N_{E(\pi_k)/E(\pi_{k-1})}(\pi_k) = (-1)^{q-1}\pi_{k-1},$$

and taking norm down to E gives

$$N_{E(\pi_n)/E}(\pi_n) = N_{E(\pi_1)/E}((-1)^{q-1}\pi_1) = (-1)^{(q-1)^2}(-1)^{q-1}\pi^{\sigma^{n-1}} = \pi^{\sigma^{n-1}}.$$

The proof is now complete. □

Remark 1: When $E = K$, the map σ is trivial. Hence we have

$$N_{K_{\pi,n}/K}(\pi_n) = \pi.$$

Remark 2: When $n = 1$, $E_{\pi,1}$ is the splitting field of $f/T = T^{q-1} + \pi$. Since E contains ζ_{q-1}, we see that $E_{\pi,1} = E((-\pi)^{1/(q-1)})$ is a Kummer extension. Hence for two uniformizers π, ω of E, the two fields $E_{\pi,1}$ and $E_{\omega,1}$ are equal if and only if ω/π is a $(q-1)$-th power in $A_E^\times$. We note that every element in $U_E^1 = 1 + (\pi)$ is a $(q-1)$-th power by Hensel. In other words, if $\omega/\pi \in U_E^1$, then $E_{\pi,1} = E_{\omega,1}$. We will see later that in the case $E = K$, if $\omega/\pi \in U_K^n = 1 + (\pi^n)$, then $K_{\pi,n} = K_{\omega,n}$. Hence both π and ω belong to the norm group. As a consequence, we see that $U_K^n \subseteq N(K_{\pi,n}^\times)$.

To compare K_π and K_ω, we need to pass to the completion of K^{un}. Let B denote its valuation ring and let σ denote the Frobenius map Frob_K extended from K^{un} by continuity. We have the following result whose proof we defer to the next section.

Theorem 4.3.4

Suppose $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$ with $\omega = u\pi$ for some unit $u \in U_K$. Then $\mathcal{F}_f$ and $\mathcal{F}_g$ are A-isomorphic over B. More precisely, there exists $\epsilon \in B^\times$ such that $\sigma(\epsilon)/\epsilon = u$ and a power series $\theta(T) \in B[[T]]$ such that

$$\theta(T) \equiv \epsilon T \pmod{T^2}, \qquad \sigma\theta = \theta \circ [u]_f$$

$$\theta \circ F_f = F_g \circ \theta, \qquad \theta \circ [a]_f = [a]_g \circ \theta \text{ for any } a \in A.$$

We now consider the dependence on π. Note that if $A_{\pi,\omega}^E \neq \emptyset$, then by scaling by π_0, we may find $a \in A_{\pi,\omega}^E \cap A_E^\times$. Then $[a]_{f,g} \in A_E[[T]]$ is an invertible power series sending Λ_n to Λ_n'. By Lemma **??**, we see that the extensions $E_{\pi,n} = E_{\omega,n}$ and so $E_\pi = E_\omega$ over E. When $E = \widehat{K^{\mathrm{un}}}$, this is always non-empty.

Lemma 4.3.5

Let B be the valuation ring of the completion of K^{un}. Then we have exact sequences

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\sigma-1} B \longrightarrow 1, \qquad 1 \longrightarrow A^\times \longrightarrow B^\times \xrightarrow{\sigma/1} B^\times \longrightarrow 1.$$

Proof. Let R be the valuation ring of K^{un} with maximal ideal $\mathfrak{q} = \pi R$. Then B is the $\mathfrak{q}$-adic completion of R. The map $\sigma - 1$ on $R/\mathfrak{q} = \bar{\mathbb{F}}_q$ is $x \mapsto x^q - x$, which is surjective with kernel $\mathbb{F}_q$. Hence we have an exact sequence

$$1 \longrightarrow A/\mathfrak{p} \longrightarrow R/\mathfrak{q} \xrightarrow{\sigma-1} R/\mathfrak{q} \longrightarrow 1.$$

Consider the diagram

$$\begin{tikzcd}
1 \arrow[r] & R/\mathfrak{q} \arrow[r, "\pi^{n-1}"] \arrow[d, "\sigma-1"] & R/\mathfrak{q}^n \arrow[r] \arrow[d, "\sigma-1"] & R/\mathfrak{q}^{n-1} \arrow[r] \arrow[d, "\sigma-1"] & 1 . \\
1 \arrow[r] & R/\mathfrak{q} \arrow[r, "\pi^{n-1}"] & R/\mathfrak{q}^n \arrow[r] & R/\mathfrak{q}^{n-1} \arrow[r] & 1
\end{tikzcd}$$

It follows from induction and the Snake lemma that

$$1 \longrightarrow A/\mathfrak{p}^n \longrightarrow R/\mathfrak{q}^n \xrightarrow{\sigma-1} R/\mathfrak{q}^n \longrightarrow 1$$

is exact. Taking inverse limits gives the first exact sequence. Similar proof applies for the second exact sequence as the map $x \mapsto x^{q-1}$ is surjective on $\bar{\mathbb{F}}_q^\times$ with kernel $\mathbb{F}_q^\times$. □

Lemma 4.3.6

Let B be the valuation ring of the completion of K^{un}. Then the map $\sigma/1 : B^\times \to B^\times$ defined by $b \mapsto b^\sigma/b$ is surjective.

Proof. The proof is essentially the same as the surjectivity of norms on units for unramified extensions. Fix some uniformizer π_0 of K. Then we have a filtration on $B^\times$ by U^n where $U^n = 1 + (\pi_0^n)B$ for $n \geq 1$. The map $\sigma/1$ descends to $U^n/U^{n+1} \to U^n/U^{n+1}$ as follows.

- When $n = 0$, $\sigma/1$ is the map $x \mapsto x^{q-1}$ on $B^\times/U^1 = \bar{\mathbb{F}}_q^\times$.
- When $n \geq 1$, $\sigma/1$ is the map $x \mapsto x^q - x$ on $U^n/U^{n+1} \cong \bar{\mathbb{F}}_q$.

These maps on the algebraic closure $\bar{\mathbb{F}}_q$ are all surjective. We are now done by completeness. □

Remark: Recall that we have the Teichmüller lift $\alpha : \bar{\mathbb{F}}_q \to B$ defined for any complete non-archimedean valuation ring with perfect residue fields (in Lecture 4). This is a multiplicative map and so σ acts as raising to the q-th power on its image. Fix some uniformizer π_0 of K. We can then express every element of B uniquely as the power series

$$a_0 + a_1\pi_0 + a_2\pi_0^2 + \cdots, \qquad \text{where} \qquad a_i \in \alpha(\bar{\mathbb{F}}_q).$$

If E/K is unramified of degree m, then elements of A_E are of the same form as above where each $a_i \in \alpha(\mathbb{F}_{q^m})$.

Corollary 4.3.7

Let E, E' be finite unramified extensions of K. For any uniformizer π of E and uniformizer ω of E', we have

$$E_\pi.K^{\mathrm{un}} = E'_\omega.K^{\mathrm{un}} =: K^{\mathrm{LT}}.$$

Proof. It suffices to prove that for any $n \geq 1$, we have

$$K^{\mathrm{un}}(\Lambda[\pi^n]) = K^{\mathrm{un}}(\Lambda[\omega^n]).$$

We know that this is true when we take completion of K^{un}:

$$\widehat{K^{\mathrm{un}}}(\Lambda[\pi^n]) = \widehat{K^{\mathrm{un}}}(\Lambda[\omega^n]).$$

Let $L_{\pi,n} = K^{\mathrm{un}}(\Lambda[\pi^n])$. We note that $\widehat{K^{\mathrm{un}}}(\Lambda[\pi^n])$ is the completion $\widehat{L_{\pi,n}}$ since it is complete and $L_{\pi,n}$ is dense. The Galois group $\mathrm{Gal}(\bar{K}/L_{\pi,n})$ acts trivially on $L_{\pi,n}$ and so by continuity also acts trivially on its completion. Hence we have $L_{\pi,n} = \widehat{L_{\pi,n}} \cap \bar{K} = \widehat{L_{\omega,n}} \cap \bar{K} = L_{\omega,n}$. □

Fixing a uniformizer π of K and some $f \in \mathcal{F}_\pi$. We have an isomorphism

$$U_K \times \hat{\mathbb{Z}} \cong \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{\mathrm{un}}/K) \cong \mathrm{Gal}(K^{\mathrm{LT}}/K).$$

We define the reciprocity map

$$\phi_\pi : K^\times \to \mathrm{Gal}(K^{\mathrm{LT}}/K)$$

by: for any $u \in U_K$ and $m \in \mathbb{Z}$,

$$\phi_\pi(u\pi^m)|_{K_\pi} = [u^{-1}]_f \qquad \text{and} \qquad \phi_\pi(u\pi^m)|_{K^{\mathrm{un}}} = \sigma^m.$$

It is easy to see that ϕ_π is injective, (continuous) and its image consists of $\tau \in \mathrm{Gal}(K^{\mathrm{LT}}/K)$ such that $\tau|_{K^{\mathrm{un}}} = \sigma^m$ for some integer m.

Theorem 4.3.8

The map $\phi_K = \phi_\pi$ is independent of π.

Proof. Let ω be another uniformizer of K. It suffices to prove that $\phi_\pi(\omega) = \phi_\omega(\omega)$ since then for any uniformizer π', ϕ_π and $\phi_{\pi'}$ are equal on all uniformizers of K, which generate $K^\times$. Both act as Frobenius on K^{un}. Since $\phi_\omega(\omega)$ acts trivially on K_ω, it suffices to show that $\phi_\pi(\omega)$ also acts trivially on K_ω which we prove below in Theorem **??**. □

Remark: For the purpose of defining the Lubin-Tate extension K^{LT}/K and the reciprocity map, there is no need to deal with unramified extensions of K and Frobenius twists. However, according to future Jerry, this will be needed to prove the norm compatibility of the reciprocity maps.

Theorem 4.3.9

Suppose E/K has degree m. Let ω be a uniformizer of E and let $g \in \mathcal{F}_\omega$ be defined over A_E. Let π be a uniformizer of K and let $f \in \mathcal{F}_\pi$ be defined over A. Let $u \in U_K$ with $N_{E/K}(\omega) = u\pi^m$. Let $\epsilon \in B^\times$ such that $\sigma(\epsilon)/\epsilon = \omega/\pi$ and let $\theta = [\epsilon]_{f,g}$. Then

$$\theta^{\sigma^m} = \theta \circ [u]_f.$$

As a consequence, $\phi_\pi(N_{E/K}(\omega))$ acts trivially on E_ω. In particular, if $E = K$, then $\phi_\pi(\omega)|_{K_\omega} = 1$.

Proof. We prove the last statement first by proving that $\tau = \phi_\pi(u\pi^m)$ acts trivially on $E(\Lambda_n^{(g)})$. Note that it acts on K^{un} and $\widehat{K^{\mathrm{un}}}$ by σ^m, so it acts trivially on E. The map θ is a bijection $\Lambda_n^{(f)} \to \Lambda_n^{(g)}$ defined by a power series

$$\theta(T) = \epsilon T + a_2T^2 + a_3T^3 + \cdots, \qquad \text{where} \qquad \epsilon, a_2, a_3, \ldots \in B.$$

Fix any $\alpha \in \Lambda_n^{(f)}$. We know that $\tau(a_i) = a_i^{\sigma^m}$ and $\tau(\alpha) = [u]_{f,f}^{-1}(\alpha)$. Hence by continuity, we have

$$\tau(\theta(\alpha)) = \tau(\epsilon)\tau(\alpha) + \tau(a_2)\tau(\alpha)^2 + \tau(a_3)\tau(\alpha)^3 + \cdots = \theta^{\sigma^m} \circ [u]_f^{-1}(\alpha).$$

Therefore, it suffices to prove that $\theta^{\sigma^m} = \theta \circ [u]_f$. Note that the Galois group $\mathrm{Gal}(E/K)$ is the cyclic group of order m generated by σ. From $\epsilon^\sigma/\epsilon = \omega/\pi$, we have

$$\frac{\epsilon^{\sigma^m}}{\epsilon} = \frac{\epsilon^{\sigma^m}}{\epsilon^{\sigma^{m-1}}} \cdots \frac{\epsilon^{\sigma^2}}{\epsilon^\sigma}\frac{\epsilon^\sigma}{\epsilon} = \frac{\omega\omega^\sigma \cdots \omega^{\sigma^{m-1}}}{\pi^m} = \frac{N_{E/K}(\omega)}{\pi^m} = u.$$

Hence $\epsilon^{\sigma^m} = u\epsilon$. So we have

$$[\epsilon^{\sigma^m}]_{f,g} = [u\epsilon]_{f,g} = [\epsilon]_{f,g} \circ [u]_{f,f} = \theta \circ [u]_f.$$

Finally since σ^m acts trivially on E, we have $\theta^{\sigma^m} = [\epsilon^{\sigma^m}]_{f^{\sigma^m}, g^{\sigma^m}} = [\epsilon^{\sigma^m}]_{f,g} = \theta \circ [u]_f$. □

Corollary 4.3.10

Let $u \in U_K^n = 1 + (\pi^n)$ and $\omega = u\pi \in K$. Then $K_{\pi,n} = K_{\omega,n}$.

Proof. Let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$. Let $\theta(T) \in B[[T]]$ be the power series defining an A-isomorphism $\mathcal{F}_f \to \mathcal{F}_g$. Then we have $\theta^\sigma = \theta \circ [u]_f$. It suffices to prove that $\theta(\alpha) \in K_{\pi,n}$ for any $\alpha \in \Lambda[\pi^n]$. A priori, we have

$$\theta(\alpha) \in \widehat{K^{\text{un}}(\alpha)} \cap \bar{K} = K^{\text{un}}(\alpha) \subseteq K^{\text{un}} K_{\pi,n}.$$

Since $K_{\pi,n}$ and K^{un} are linearly disjoint, it suffices to show that $\theta(\alpha)$ is fixed by the Frobenius map σ. We have

$$(\theta(\alpha))^\sigma = (\theta^\sigma)(\alpha) = \theta([u]_f(\alpha)) = \theta(\alpha)$$

since U_K^n acts trivially on $\Lambda[\pi^n]$. □

While we are still fresh with the explicit construction of K_π, let's first prove local Kronecker-Weber.

Theorem 4.3.11

Let K be a non-archimedean local field. Then $K^{\text{ab}} = K^{\text{LT}} = K^{\text{un}} \cdot K_\pi$.

The proof is essentially identical to the proof for $\mathbb{Q}_p$ given in Section 8 using ramification groups and Hasse-Arf. We recall it in the language of K_π.

- Prove that if L/K is a totally ramified abelian extension containing K_π, then $L = K_\pi$.
- Prove that any finite extension of K_π in K^{ab} is cyclic over K_π.
- Prove that any two finite extensions of K_π in K^{ab} of the same degree are equal.
- The extension $K(\zeta_{q^d-1}) \cdot K_\pi$ is an extension of K_π in K^{LT} of degree d over K_π. Hence any finite abelian extension of K lies in K^{LT}.

To prove the second bullet point, we extend the map $\phi_\pi(\pi)$ from K^{LT} to K^{ab}. Recall that $\phi_\pi(\pi)$ acts trivially on K_π and as the (topological generator) Frobenius σ on K^{un}. Let M/K_π be a finite extension in K^{ab}. Then the fixed field $M^{\langle \tau|_M \rangle}$ is a totally ramified abelian extension of K containing K_π. By the first bullet point, it equals K_π. Hence $\text{Gal}(M/K_\pi) = \langle \tau|_M \rangle$ is cyclic.

To prove the third bullet point, let M_1/K_π and M_2/K_π be two extensions in K^{ab} of degree d. Then $\text{Gal}(M_1M_2/K_\pi)$ is finite cyclic, and so has a unique quotient of size d proving that $\text{Gal}(M_1M_2/M_1) = \text{Gal}(M_1M_2/M_2)$. Hence $M_1 = M_2$.

The first bullet point is where we used ramification groups. Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/K_\pi)$. We prove that $H \subseteq \bigcap G^v = 1$ by proving that $[G^v \cap H : G^{v+1} \cap H] = 1$ for all v. We know that

$$(G/H)^v = G^v H/H \cong G^v/(G^v \cap H)$$

and so by Snake lemma, we have

$$[G^v : G^{v+1}] = [G^v \cap H : G^{v+1} \cap H] \cdot [(G/H)^v : (G/H)^{v+1}].$$

From an explicit description of $(G/H)^v$, we know that G^v is finite index in G. Since it is always closed, its fixed field E_v is some finite abelian extension of K. We then have

$$G^v/G^{v+1} \hookrightarrow \mathrm{Gal}(E_{v+1}/K)^v/\,\mathrm{Gal}(E_{v+1}/K)^{v+1} \hookrightarrow \begin{cases} k^\times & \text{if } v = 0, \\ k & \text{if } v \geq 1. \end{cases}$$

The last inclusion is a consequence of Hasse-Arf, which implies that for finite abelian extensions, consecutive upper numbering ramification groups (with integer indices) are either equal or are consecutive lower numbering ramification groups. It then remains to compute the ramification groups of K_π/K to show that

$$(G/H)^v/(G/H)^{v+1} \cong \begin{cases} k^\times & \text{if } v = 0, \\ k & \text{if } v \geq 1. \end{cases}$$

Theorem 4.3.12

Under the isomorphism $U_K = A^\times \cong \mathrm{Gal}(K_\pi/K)$, We have for any integer $v \geq 1$,

$$\mathrm{Gal}(K_\pi/K)^v = U_K^v = 1 + \pi^v A.$$

Proof. The proof here is also almost identical to the $\mathbb{Q}_p(\zeta_{p^n})$ calculation. We consider $K_{\pi,n}/K$ with Galois group isomorphic to $(A/(\pi^n))^\times$. The isomorphism sends $a \in A$ to $\sigma_a = [a]_f$ where $f(T) = T^q + \pi T$. Suppose now $a = 1 + u\pi^v$ for some integer $v \geq 1$ and unit $u \in A^\times$. Recall the elements $\pi_1, \ldots, \pi_n$ in $K_{\pi,n}$ where $f(\pi_i) = \pi_{i-1}$ for $i \geq 2$ and $(f/T)(\pi_1) = 0$. Then each π_i is an uniformizer for $K(\pi_i)$. Let μ_i denote the normalized valuation on $K(\pi_i)$ so that $\mu_i(\pi_i) = 1$. Then we have,

$$i_G(\sigma_a) = \mu_n([a]_f(\pi_n) - \pi_n) = \mu_n([u]_f[\pi]_f^v \pi_n)) = \mu_n(\pi_{n-v}) = q^v.$$

Hence we see that

$$G_{q^{v-1}} = \cdots = G_{q^v - 1} = 1 + \pi^v (A/(\pi^n))^\times = G^v.$$

Taking inverse limits gives the desired result. □

Proof of Theorem ??: We now prove the desired $\theta^{\sigma^m} = \theta \circ [u]_f$. From the definition of θ, we have that

$$g = \theta^\sigma \circ f \circ \theta^{-1}.$$

Hence, by repeatedly taking σ and composing, we get

$$g_m = \theta^{\sigma^m} \circ f_m \circ \theta^{-1} = \theta^{\sigma^m} \circ f^{(m)} \circ \theta^{-1} = \theta^{\sigma^m} \circ [\pi^m]_f \circ \theta^{-1}.$$

Since $\mathrm{Gal}(E/K)$ is cyclic of order m generated by σ, we see that

$$g_m \equiv N_{E/K}(\omega)T \pmod{T^2}.$$

Moreover, since $g \in A_E[[T]]$ is fixed by σ^m, we have

$$g \circ g_m = g^{\sigma^m} \circ g_m = g_{m+1} = g_m^{\sigma} \circ g.$$

Hence

$$g_m = [u\pi^m]_g = [\epsilon]_{f,g} \circ [u]_f \circ [\pi^m]_f \circ [\epsilon]_{f.g}^{-1} = \theta \circ [u]_f \circ [\pi^m]_f \circ \theta^{-1}.$$

Therefore, we have $\theta^{\sigma^m} \circ [\pi^m]_f = \theta \circ [u]_f \circ [\pi^m]_f$. That is

$$\theta^{\sigma^m} \circ f^{(m)} = \theta \circ [u]_f \circ f^{(m)}.$$

Here $f^{(m)} = f_m$ is f composed with itself m times. We are now done by the next Lemma **??**.

Lemma 4.3.13

Suppose $h \in B[[T]]$ and $f \in \mathcal{F}_\pi$. For any integer $\ell \geq 1$, if $h \circ f \equiv 0 \pmod{\pi^\ell}$, then $h \equiv 0 \pmod{\pi^\ell}$. In particular, $h \circ f = 0$ implies $h = 0$.

Proof. Modulo π, we have $h(T^q) \equiv 0$. Hence $h \equiv 0$. Divide h by π and repeat. □

§4.4 Norm compatibility

Our main theorem this section is the following norm compatibility result of ϕ_K.

Theorem 4.4.1

Let L/K be a finite extension of non-archimedean local fields. Then the following diagram commutes.

$$\begin{tikzcd}
L^\times \arrow[r, "\phi_L"] \arrow[d, "N_{L/K}"] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[d, "\sigma \mapsto \sigma|_{K^{\mathrm{ab}}}"] \\
K^\times \arrow[r, "\phi_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

Remark: We have used Theorem **??** to replace K^{LT} by K^{ab} and similarly for L. Note also that $K^{\mathrm{ab}}L/L$ is abelian and so K^{ab} is a subfield of L^{ab}. We are not assuming that L/K is abelian because the proof won't need it. The proof can also be made to work without proving Theorem **??** first, with L^{LT} in place of L^{ab} and $L^{\mathrm{LT}} \cap K^{\mathrm{LT}}$ in place of K^{ab} in the above diagram.

Corollary 4.4.2

Suppose L/K is a finite abelian extension.Then ϕ_K defines an isomorphism

$$\phi_{L/K} : K^\times/N_{L/K}(L^\times) \cong \mathrm{Gal}(L/K).$$

Proof. Write $\phi_{L/K}$ also for the composite map $K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$. Since the image of ϕ_K is dense and $\mathrm{Gal}(K^{\mathrm{ab}}/L)$ is a closed subgroup of finite index, we see that the image of ϕ_K hits every coset of $\mathrm{Gal}(K^{\mathrm{ab}}/L)$ and so $\phi_{L/K}$ is surjective. The kernel of $\phi_{L/K}$ clearly contains $N_{L/K}(L^\times)$. Suppose now $\phi_{L/K}(a) = 1$. Then $\phi_K(a) \in \mathrm{Gal}(K^{\mathrm{ab}}/L)$. Extend it to $\mathrm{Gal}(K^{\mathrm{ab}}L/L)$ and then to some $\tau \in \mathrm{Gal}(L^{\mathrm{ab}}/L)$. Let $E = K^{\mathrm{un}} \cap L$. Then τ acts on $E^{\mathrm{un}} = K^{\mathrm{un}}$ via $\phi_K(a)$, which is some integer power of Frobenius. Since L/E is totally ramified, L^{un} is formed from L by adjoining the same roots of unities as E^{un} is formed from E. Hence τ acts on L^{un} by some integer power of Frobenius. There then exists $b \in L^\times$ such that $\phi_L(b) = \tau$. Then $\phi_K(a) = \phi_K(N_{L/K}(b))$. By injectivity, we have $a = N_{L/K}(b)$. □

Proof of Theorem ??: We now prove the desired $\theta^{\sigma^m} = \theta \circ [u]_f$ which implies that $\phi_K(N_{E/K}(\omega))$ acts trivially on E_ω, where E/K is unramified of degree m. Note that the Galois group $\mathrm{Gal}(E/K)$ is the cyclic group of order m generated by σ. From $\epsilon^\sigma/\epsilon = \omega/\pi$, we have

$$\frac{\epsilon^{\sigma^m}}{\epsilon} = \frac{\epsilon^{\sigma^m}}{\epsilon^{\sigma^{m-1}}} \cdots \frac{\epsilon^{\sigma^2}}{\epsilon^\sigma}\frac{\epsilon^\sigma}{\epsilon} = \frac{\omega\omega^\sigma \cdots \omega^{\sigma^{m-1}}}{\pi^m} = \frac{N_{E/K}(\omega)}{\pi^m} = u.$$

Hence $\epsilon^{\sigma^m} = u\epsilon$. Note that both sides are in $A_{\pi,\omega}^{\hat{K}^{\mathrm{un}}}$. So we have

$$[\epsilon^{\sigma^m}]_{f,g} = [u\epsilon]_{f,g} = [\epsilon]_{f,g} \circ [u]_{f,f} = \theta \circ [u]_f.$$

Finally since σ^m acts trivially on E, we have

$$\theta^{\sigma^m} = [\epsilon^{\sigma^m}]_{f^{\sigma^m}, g^{\sigma^m}} = [\epsilon^{\sigma^m}]_{f,g} = \theta \circ [u]_f.$$

We work towards proving Theorem **??**. It is easy to see that it suffices to prove it when L/K is unramified; and when L/K is totally ramified. It also suffices to prove that for any uniformizer ω of L,

$$\phi_L(\omega)|_{K^{\mathrm{ab}}} = \phi_K(N_{L/K}(\omega)).$$

On K^{un}, we know that $\phi_L(\omega)$ acts as $\mathrm{Frob}_L = \mathrm{Frob}_K^{f_{L/K}}$. We know also that $\mu_K(N_{L/K}(\omega)) = f_{L/K}$, so we see that $\phi_L(\omega)|_{K^{\mathrm{un}}} = \phi_K(N_{L/K}(\omega))|_{K^{\mathrm{un}}}$.

In the unramified case, Theorem **??** implies that $\phi_K(N_{L/K}(\omega))$ acts trivially on L_ω, and so does $\phi_L(\omega)$. Hence they agree on $K^{\mathrm{un}} \cdot L_\omega = K^{\mathrm{LT}} = K^{\mathrm{ab}}$.

We focus now on the totally ramified case. In this case, $\phi_L(\omega)$ acts as $\mathrm{Frob}_L = \mathrm{Frob}_K$ on K^{un}. So

$$\phi_L(\omega)|_{K^{\mathrm{ab}}} = \phi_K(\pi)$$

for some uniformizer π of K. The goal now is to prove that

$$N_{L/K}(\omega) = \pi.$$

Observe that we have

$$(K^{\mathrm{ab}})^{\phi_K(\pi)} = K_\pi \hookrightarrow L_\omega = (L^{\mathrm{ab}})^{\phi_L(\omega)}.$$

They are all totally ramified over K. The key idea now is to recover π from the norm subgroups, recalling that $\pi \in N(K_{\pi,n}^\times)$.

Suppose now L/K is totally ramified. Consider first that $L = K_{\pi,n}$ for some uniformizer π and integer $n \geq 1$. In this case, $\phi_L(a)|_{K_{\pi,n}}$ is trivial for all $a \in U_L$. Hence if the diagram does commute, then every element of $N_{L/K}(U_L)$ acts trivially on $K_{\pi,n}$. Under the isomorphism $A/(\pi^n)^\times \to \mathrm{Gal}(K_{\pi,n}/L)$, this means that $N_{L/K}(U_L) \subset 1 + \mathfrak{p}^n$ where $\mathfrak{p} = (\pi)$. We claim that conversely, this is enough to prove the diagram commutes for any totally ramified L/K.

Theorem 4.4.3

We have $N(K_{\pi,n}^\times) = (1+\mathfrak{p}^n) \times \pi^{\mathbb{Z}}$.

For any infinite extension F/K, we write

$$N(F^\times) = \bigcap_{L\subset F,\ [L:K]<\infty} N(L^\times).$$

Corollary 4.4.4

We have $N(K_\pi^\times) = \pi^{\mathbb{Z}}$. Moreover, if F/K is a totally ramified extension containing K_π, then $N(F^\times) = \pi^{\mathbb{Z}}$.

Proof. Since F contains K_π, we have $N(F^\times) \subseteq N(K_\pi^\times) \subseteq \pi^{\mathbb{Z}}$. It remains to prove that $N(F^\times)$ contains a uniformizer, which then must be π. We know this is true for finite totally ramified extensions. To prove it for infinite totally ramified extensions, we use a little bit of topology. For any finite L/K contained in F, let $S(L)$ denote the nonempty set of uniformizers of K contained in $N(L^\times)$. Then $S(L) = N_{L/K}(\pi_L U_L)$ is a compact subset of the compact set πU_K such that any finite intersection $S(L_1)\cap\cdots\cap S(L_m)$ contains $S(L_1\cdots L_m)$ which is nonempty. Hence, the intersection of all of the $S(L)$ is nonempty. (Otherwise, their complements is a cover of πU_K that does not admit a finite subcover.) □

Proof of Theorem ??: Suppose L/K is totally ramified. For any finite extension M/K contained in L_ω, we have $N(M^\times)\cap N(L^\times) = N((LM)^\times)$. We write N_K for the norm groups down to K and N_L for the norm groups down to L. Then

$$N_K(L_\omega^\times) = \bigcap_{\substack{M\subseteq L_\omega \\ [M:K]<\infty}} N_K(M^\times) = \bigcap_{\substack{L\subseteq M\subseteq L_\omega \\ [M:K]<\infty}} N_K(M^\times) = N_{L/K}(N_L(L_\omega^\times)) = N_{L/K}(\omega^{\mathbb{Z}}).$$

On the other hand, L_ω is totally ramified over K containing K_π so we have $N_K(L_\omega^\times) = \pi^{\mathbb{Z}}$. Therefore, $N_{L/K}(\omega) = \pi$. □

Corollary 4.4.5

Let n, m be any positive integers. Let π be a uniformizer of K. Let E be the unramified extension of K of degree m. Let $L = K_{\pi,n}E$. Then $N(L^\times) = (1+\mathfrak{p}^n)\times \pi^{m\mathbb{Z}}$.

Proof. Since $K_{\pi,n}$ has norm group $(1+\mathfrak{p}^n)\times\pi^{\mathbb{Z}}$ and E has norm group $U_K\times\pi^{m\mathbb{Z}}$, we see that the norm group of L is contained in $(1+\mathfrak{p}^n)\times\pi^{m\mathbb{Z}}$. Comparing indices gives equality. □

We will have completed the proofs of the main theorems of LCFT once we prove that $K_{\pi,n}$ has the correct norm group.

Proof of Theorem ??: From Corollary **??**, we see that $N(K_{\pi,n}^\times)$ contains $u\pi$ for any $u\in U_K^n$. Hence it remains to prove that the norm of any unit lies in U_K^n. Fix $f = \pi T + T^q$. Since $K_{\pi,n}$ is totally ramified over K with uniformizer π_n, we see that any unit in $K_{\pi,n}$

is of the form $h(\pi_n)$ for some $h \in A[T]$ with $h(0) \in U_K$. So $h \in A[[T]]^\times$. Moreover, the conjugates of π_n over K are exactly the elements of $\Lambda_n \backslash \Lambda_{n-1}$ using the fact that Λ_n is the A-cyclic module generated by π_n and Λ_{n-1} is generated by $[\pi_0](\pi_n) = \pi_{n-1}$. Hence

$$N(h(\pi_n)) = \prod_{\beta \in \Lambda_n \backslash \Lambda_{n-1}} h(\beta) = \left(\prod_{\beta \in \Lambda_n} h(\beta) \right) / \left(\prod_{\beta \in \Lambda_{n-1}} h(\beta) \right).$$

The trick is to consider

$$h_n(T) = \prod_{\beta \in \Lambda_n} h(T +_f \beta) = \prod_{\beta \in \Lambda_n} h(F_f(T, \beta)).$$

Lemma 4.4.6

There exists a unique map $N : A[[T]] \to A[[T]]$ such that for any $h \in A[[T]]$,

$$N(h) \circ f(T) = \prod_{\lambda \in \Lambda_1} h(T +_f \lambda).$$

This is the Coleman norm operator.

Proof. Let $h_1(T)$ denote the right hand side. Since $h_1(T)$ is symmetric in $\lambda \in \Lambda_1$, we see that $h_1(T) \in A[[T]]$. By the associativity of F_f, we have

$$h_1(T +_f \lambda) = h_1(T), \qquad \text{for any } \lambda \in \Lambda_1.$$

Then the power series $h_1(T) - h_1(0) \in TA[[T]]$ vanishes at all $\lambda \in \Lambda_1$. Since $f(T) = \prod_{\lambda \in \Lambda_1}(T - \lambda)$, we have $f(T) \mid h_1(T) - h_1(0)$ in $A[[T]]$ by Lemma **??**. Let $g_1(T) \in A[[T]]$ be their quotient. Then

$$h_1(T) = h_1(0) + g_1(T) f(T).$$

Now for any $\lambda \in \Lambda$, we have $f(T +_f \lambda) = f(T) +_f f(\lambda) = f(T)$. Hence

$$h_1(T +_f \lambda) = h_1(0) + g_1(T +_f \lambda) f(T +_f \lambda) = h_1(0) + g_1(T +_f \lambda) f(T).$$

In other words,

$$g_1(T +_f \lambda) = g_1(T), \qquad \text{for any } \lambda \in \Lambda_1.$$

We can then repeat the above to write

$$g_1(T) = g_1(0) + g_2(T) f(T).$$

We thus have a sequence $a_0, a_1, \ldots$ in A such that

$$h_1(T) = a_0 + a_1 f(T) + a_2 f(T)^2 + \cdots = N(h) \circ f$$

where

$$N(h)(T) := a_0 + a_1 T + a_2 T^2 + \cdots \in A[[T]].$$

It is easy to see that $N(h)$ is unique since $g \circ f = 0$ implies that $g = 0$. (Exercise.) □

Lemma 4.4.7

Suppose $h \in A[[T]]$ with distinct roots $\alpha_1, \ldots, \alpha_n$ in Λ. Then $(T-\alpha_1)\cdots(T-\alpha_n) \mid h$ in $A[[T]]$.

Proof. The same proof for polynomials works here. The condition that $\alpha_i \in \Lambda$ ensures convergence. □

Lemma 4.4.8

Let N^n denote N composed with itself n times. Then for any $h \in A[[T]]$,

$$h_n(T) = \prod_{\beta \in \Lambda_n} h(T +_f \beta) = N^n(h) \circ f^{(n)}(T).$$

Proof. We now prove by induction on n. The case $n = 1$ is the definition of N. Let Ω be a set of representatives for Λ_n/Λ_1. In other words, every element of Λ_n can be written uniquely as $\beta +_f \gamma$ for some $\beta \in \Omega$ and $\gamma \in \Lambda_1$. We also have $f(\Omega) = \Lambda_{n-1}$. Then

$$h_n(T) = \prod_{\beta \in \Omega} \prod_{\lambda \in \Lambda_1} h(T +_f \beta +_f \lambda) = \prod_{\beta \in \Omega} N(h) \circ f(T +_f \beta) = \prod_{\lambda \in \Lambda_{n-1}} N(h)(f(T) +_f \lambda)$$

which by induction equals $N^{n-1}(N(h)) \circ f^{(n-1)}(f(T)) = N^n(h) \circ f^{(n)}(T)$. □

Lemma 4.4.9

The Coleman norm operator N has the following properties:

(a) $N(h_1 h_2) = N(h_1)N(h_2)$;

(b) $N(h) \equiv h \pmod{\pi}$;

(c) If $h \in T^i A[[T]]^\times$ for some $i \geq 0$, then $N(h) \in h(A[[T]])^\times$;

(d) If $h \equiv 1 \pmod{\pi^n}$, then $N(h) \equiv 1 \pmod{\pi^{n+1}}$.

Combining these, we see that if $h \in T^i A[[T]]^\times$ for some $i \geq 0$, then $N^n(h)/N^{n-1}(h) \equiv 1 \pmod{\pi^n}$.

Proof. Statement (a) follows from uniqueness. For (b), we note that $N(h) \circ f(T) \equiv N(h)(T^q) \bmod \pi$. On the other hand, $\Lambda_1 \subset (\pi_1)$ and so $T +_f \lambda \equiv T \bmod \pi_1$ for any $\lambda \in \Lambda_1$. Hence the product

$$\prod_{\lambda \in \Lambda_1} h(T +_f \lambda) \equiv h(T)^q \equiv h(T^q) \pmod{\pi},$$

since they are congruent mod π_1 but have coefficients in A. This proves (b). Statement (c) when $i = 0$ follows from (b) (which is all we need) since $N(h)(0) \equiv h(0) \not\equiv 0 \pmod{\pi}$. Consider $h(T) = T$. It is clear from the construction of N that $N(T) = Tg(T)$ for some $g \in A[[T]]$. It suffices to prove that $g(0) \in A^\times$. By definition, we have

$$(\pi T + T^q)g(\pi T + T^q) = T \prod_{\lambda \in \Lambda_1 \setminus \{0\}} (T +_f \lambda).$$

Divide by T and set $T = 0$. We get $\pi g(0) = N_{K_{\pi,1}/K}(\pi_1) = (-1)^{q-1}\pi$. Hence $g(0) \in A^\times$. The general case follows by multiplicativity (a). For (d), write $h = 1 + \pi^n g$ for some $g \in A[[T]]$. Then

$$N(h) \circ f(T) = \prod_{\lambda \in \Lambda_1} (1 + \pi^n g(T +_f \lambda)) \equiv (1 + \pi^n g(T))^q \equiv 1 \pmod{\pi^{n+1}}.$$

So $(N(h) - 1) \circ f(T) \equiv 0 \pmod{\pi^{n+1}}$. Modulo π, we find $(N(h) - 1)(T^q) \equiv 0$ and so $N(h) - 1 \equiv 0 \pmod{\pi}$. Divide it by π and repeat. We conclude that $N(h) - 1 \equiv 0 \pmod{\pi^{n+1}}$.

Finally, by (b) and (c), we see that $N(h)/h \equiv 1 \pmod{\pi}$. Now apply (d) and (a) $n-1$ times to $N(h)/h$. □

Theorem **??** now follows because

$$N(h(\pi_n)) = \frac{N^n(h)(0)}{N^{n-1}(h)(0)} \in 1 + \mathfrak{p}^n.$$

§4.5 Summary for the proof of Local class field theory

1. Given the data $(E, \pi, f \in \mathcal{F}_\pi)$ of a complete unramified extension E/K, a uniformizer π of E, and some $f = T^q + \pi T + \cdots$:
   - Obtain a formal group law F_f such that $f \in \operatorname{Hom}(F_f, F_f^\sigma)$.
   - Define $E_{\pi,n}$ as the field over E generated by the roots of $f^{\sigma^{n-1}} \circ \cdots \circ f^\sigma \circ f$.
   - Prove that $E_{\pi,n}/E$ is totally ramified with Galois group isomorphic to $(A/(\pi_K)^n)^\times$. Take
   $$E_\pi = \varinjlim E_{\pi,n}.$$
2. Given two such (E, π, f) and (E, ω, g) and some $a \in A^E_{\pi,\omega} \cap A_E^\times$:
   - Obtain an isomorphism $[a]_{f,g} : E_\pi \to E_\omega$.
   - Pass to the completion of K^{un} and then intersect with $\bar{K}$ to show that
   $$K^{\text{LT}} = K^{\text{un}} E_\pi.$$
   is independent on the choice of the data (E, π, f) where E/K is finite.
3. Define the reciprocity map
   $$\phi_\pi : K^\times \to \operatorname{Gal}(K^{\text{LT}}/K)$$
   by having $\phi_\pi(u\pi^m)$ act as $[u]_f^{-1}$ on K_π and as σ^m on K^{un}.
   - Prove that given (E, ω, g) where E/K is finite unramified,
   $$\phi_\pi(N_{E/K}(\omega))|_{E_\omega} = \text{id}.$$
   - Use this to prove that ϕ_π is independent on the choice of π and that it is norm compatible with respect to finite unramified extensions.
   - Compute the ramification groups of K_π/K and use Hasse-Arf to prove the local Kronecker-Weber theorem (exactly as in the $\mathbb{Q}_p$ case):
   $$K^{\text{LT}} = K^{\text{ab}}.$$

4. Prove that $N(K_{\pi,n}^\times) = U_K^n \times \pi^{\mathbb{Z}}$.
   - The containment $N(K_{\pi,n}^\times) \supseteq U_K^n \times \pi^{\mathbb{Z}}$ follows from $K_{\pi,n} = K_{\omega,n}$ when $\omega/\pi \in U_K^n$ and that $\pi \in N(K_{\pi,n})^\times$.
   - The containment $N(K_{\pi,n}^\times) \subseteq U_K^n \times \pi^{\mathbb{Z}}$ uses the Coleman norm operator to prove that the norm of a unit is in U_K^n.
   - The equality is used to prove norm compatibility with respect to finite totally ramified extensions.

§4.6 A little bit of GCFT

We begin with an example. Let q be an odd prime and let $K = \mathbb{Q}(\sqrt{q^*})$, where $q^* = (-1)^{(q-1)/2}$. So K is the discriminant subfield of $\mathbb{Q}(\zeta_q)$. We identify $\operatorname{Gal}(K/\mathbb{Q}) \cong \{1, -1\}$ and consider the reciprocity maps

$$\phi_v : \mathbb{Q}_v^\times \to \operatorname{Gal}(K_w/\mathbb{Q}_v) \hookrightarrow \operatorname{Gal}(K/\mathbb{Q}) = \{1, -1\}.$$

Suppose first that $v = \infty$. If $q \equiv 1 \pmod 4$, then $q^* > 0$ and ϕ_∞ is trivial. If $q \equiv 3 \pmod 4$, then $q^* < 0$ and $\phi_\infty : \mathbb{R}^\times \to \{1, -1\}$ is the sign map. So we have

$$\phi_\infty(p) = 1 \qquad \text{and} \qquad \phi_\infty(-1) = \lg -1q.$$

Suppose now $v \neq q$ is a finite prime. Then $K_w/\mathbb{Q}_v$ is unramified so every unit $\mathbb{Z}_v^\times$ maps to 1. If $p = v$, then $\phi_v(p)$ is Frobenius which equals 1 if and only if p splits completely in K. So we have

$$\text{for } v \neq q : \qquad \phi_v(p) = \begin{cases} \lg q^*p & \text{if } p = v \\ 1 & \text{if } p \neq v \end{cases} \qquad \text{and} \qquad \phi_v(-1) = 1.$$

Finally suppose $v = q$. In this case, $K_w/\mathbb{Q}_q$ is totally ramified of degree 2. So its norm group is an index 2 subgroup of $\mathbb{Q}_q^\times$ containing q as $q = N(\zeta_q - 1)$. The only such subgroup is $q^{\mathbb{Z}} \times \langle \zeta_{q-1}^2 \rangle \times (1 + q\mathbb{Z}_q)$. So we have

$$\phi_q(p) = \begin{cases} \lg pq & \text{if } p \neq q \\ 1 & \text{if } p = q \end{cases} \qquad \text{and} \qquad \phi_q(-1) = \lg -1q.$$

Quadratic reciprocity then implies

$$\prod_{v \in M_{\mathbb{Q}}} \phi_v(a) = 1, \qquad \forall a \in \mathbb{Q}^\times.$$

This suggests a global reciprocity map

$$\phi : \prod_{v \in M_{\mathbb{Q}}} \mathbb{Q}_v^\times \to \operatorname{Gal}(K/\mathbb{Q})$$

having the diagonally embedded $\mathbb{Q}^\times$ in the kernel. Such a map is certainly not well-defined. We need to replace the infinite product with a restricted direct product. For any global field K, we define the group J_K of **idèles** to be

$$J_K = \{(a_v) \in \prod_{v \in M_K} K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v\} = \prod_{v \in M_K}{}' (K_v^\times, \mathcal{O}_v^\times).$$

where $\mathcal{O}_v$ denote the valuation ring of K_v for v finite. For any finite abelian extension L/K and any $(a_v) \in J_K$, we can now multiply the local reciprocity maps $\phi_{L_w/K_v} : K_v^\times \to \mathrm{Gal}(L_w/K_v) \hookrightarrow \mathrm{Gal}(L/K)$ into a global reciprocity map

$$\phi_{L/K} : J_K \to \mathrm{Gal}(L/K).$$

Note since for any $(a_V) \in J_K$, for all but finitely many v, L_w/K_v is unramified and $a_v \in \mathcal{O}_v^\times$, we have $\phi_{L_w/K_v}(a_v) = 1$ so the above map is well-defined.

Theorem 4.6.1

The map $\phi_{L/K}$ is surjective with kernel $K^\times N_{L/K}(J_L)$.

Let $C_K = J_K/K^\times$ denote the **idèle class group**. Then we have an isomorphism

$$\phi_{L/K} : C_K/N_{L/K}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Taking inverse limit over L, we have the norm compatible global reciprocity map

$$\phi_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Example: What is $C_{\mathbb{Q}}$? Elements in $J_{\mathbb{Q}}$ have coordinates $p_1^{a_1}u_1, \ldots, p_m^{a_m}u_m$ for finitely many primes, with the rest all units, and some $r \in \mathbb{R}$. Modding out by $\mathbb{Q}^\times$ gets rid of all the finitely many prime powers, and the sign of r. Hence

$$C_{\mathbb{Q}} \cong (0,\infty) \times \prod_p \mathbb{Z}_p^\times \cong (0,\infty) \times \hat{\mathbb{Z}}^\times \cong (0,\infty) \times \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

When taking norms from $K = \mathbb{Q}(\sqrt{q^*})$, we see that it surjects onto $(0,\infty)$ and each $\mathbb{Z}_p^\times$ for $p \neq q$. The image of the units in $\mathbb{Z}_q^\times$ is the index 2 subgroup $\langle \zeta_{q-1}^2 \rangle \times (1 + q\mathbb{Z}_q)$. We see that the quotient is isomorphic to C_2.

To state the Existence theorem, we need to define topologies on J_K and C_K. There is also the ring of **adeles**

$$\mathbb{A}_K = \{(a_v) \in \prod_{v \in M_K} K_v \colon a_v \in \mathcal{O}_v \text{ for all but finitely many } v\} = \prod_{v \in M_K}{}' (K_v, \mathcal{O}_v)$$

where a basis of open sets is of the form $\prod_v U_v$ where all but finitely many $U_v = \mathcal{O}_v$. It is easy to see that $J_K = \mathbb{A}_K^\times$ and we give it the topology induced from the map $x \mapsto (x, x^{-1}) : J_K \to \mathbb{A}_K \times \mathbb{A}_K$. Note this is not the same as the restricted directed product topology of J_K itself.

Proposition 4.6.2

Embed K diagonally in $\mathbb{A}_K$. Then K is discrete in $\mathbb{A}_K$ and $K^\times$ is discrete in J_K. Let $J_K^1 = \{(a_v) \in J_K \colon \prod_v |a_v|_v = 1\}$. Then $\mathbb{A}_K/K$ and $J_K^1/K^\times$ are compact.

Remark: Suppose K is a number field with r_1 real embeddings and r_2 conjugate pairs of complex embeddings. Then the quotient $\mathbb{A}_K/K$ is the same as $\prod_{v \nmid \infty} \mathcal{O}_v \times (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}/\mathcal{O}_K)$. The compactness of $J_K^1/K^\times$ implies the finiteness of class groups and Dirichlet's unit theorem that $U_K \cong \mathbb{Z}^{r_1+r_2-1} \times \langle \mu_\infty \rangle$ where $\langle \mu_\infty \rangle$ denotes the finite (cyclic) subgroup of roots of unities contained in K.

Theorem 4.6.3

When K is a number field, ϕ_K defines an isomorphism $C_K/C_K^\circ \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)$ where C_K° denote the connected component of the identity of C_K, which also equals the subgroup of infinitely divisible elements of C_K. When K is a function field over $\mathbb{F}_p$, ϕ_K is injective and its image consists of elements in $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ that restricts to some integer power of Frobenius in $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$.

Theorem 4.6.4

(Existence Theorem) There is a one-to-one correspondence between open subgroups of C_K of finite index and finite abelian extensions L/K via the norm group $N_{L/K}(C_L)$.

We end by giving an interpretation of these results in terms of the classical treatment using ideals. Any open subgroup of J_K of finite index contains a subgroup of the form $U_{\mathfrak{m}} = \prod_v U_{\mathfrak{m},v}$ where the **modulus** $\mathfrak{m} = \prod_v v^{e_v}$ is a formal product where $e_v = 0$ for all but finitely many v; $e_v \in \{0,1\}$ if v is real and $e_v = 0$ if v is complex; and

$$U_{\mathfrak{m},v} = \begin{cases} \mathcal{O}_v^\times & \text{if } v \text{ is finite and } e_v = 0 \\ 1 + \mathfrak{p}^{e_v} & \text{if } v = \mathfrak{p} \text{ is finite and } e_v > 0 \\ K_v^\times & \text{if } v \text{ is infinite and } e_v = 0 \\ \mathbb{R}^+ & \text{if } v \text{ is real and } e_v = 1. \end{cases}$$

Let $C_K^{\mathfrak{m}}$ be the image of $U_{\mathfrak{m}}$ in C_K. This is called the **congruence subgroup of C_K of modulus $\mathfrak{m}$**. When all $e_v = 0$, namely $\mathfrak{m} = 1$, the quotient group J_K/U_1 is isomorphic to the ideal group I_K of K. In other words, C_K/C_K^1 is isomorphic to the class group $\mathrm{Cl}(K)$ of K. Since $U_1/U_{\mathfrak{m}}$ is clearly finite, we see that $C_K^{\mathfrak{m}}$ is an open subgroup of C_K of finite index. By the Existence Theorem, it corresponds to a finite abelian extension $K(\mathfrak{m})/K$, called the **ray class field of modulus $\mathfrak{m}$**. The quotient

$$C_K/C_K^{\mathfrak{m}} \cong \mathrm{Gal}(K(\mathfrak{m})/K)$$

is called the **ray class group of modulus $\mathfrak{m}$**. Since $C_K^{\mathfrak{m}}$ is the norm group of $K(\mathfrak{m})$, we see that $K(\mathfrak{m})/K$ is unramified at all places v with $e_v = 0$. When $\mathfrak{m} = 1$, $K(1)$ is the **Hilbert class field** of K, which is the maximal abelian extension of K unramified everywhere.

Proposition 4.6.5

Let m be a positive integer. The ray class field of $\mathbb{Q}$ of modulus $m \cdot \infty$ is $\mathbb{Q}(\zeta_m)$.

Proof by "elimination": What else could it be? For any prime p and positive integer n, we know that the norm group of $\mathbb{Q}_p(\zeta_{p^n})$ contains $1 + p^n\mathbb{Z}_p$. So $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(m \cdot \infty)$. For equality, it is not hard to show that $C_{\mathbb{Q}}/C_{\mathbb{Q}}^{m\cdot\infty} \cong (\mathbb{Z}/m\mathbb{Z})^\times$. □

Remark: The ray class field of $\mathbb{Q}$ of modulus m is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

The ray class group of modulus $\mathfrak{m}$ is traditionally defined as the quotient $I_K^{\mathfrak{m}}/K^{\mathfrak{m}}$ where $I_K^{\mathfrak{m}}$ is the group of fractional ideals generated by prime ideals with $e_v = 0$ and $K^{\mathfrak{m}} = K^\times \cap \prod_{e_v \neq 0} U_{\mathfrak{m},v}$. We have an isomorphism

$$J_K/U_{\mathfrak{m}} \to I_K^{\mathfrak{m}} \times \prod_{e_v \neq 0} K_v^\times/U_{\mathfrak{m},v}$$

and an exact sequence

$$1 \to K^m \to K^\times \to \prod_{e_v \neq 0} K_v^\times / U_{\mathfrak{m},v} \to 1.$$

Therefore, we have an isomorphism

$$C_K / C_K^{\mathfrak{m}} \cong J_K / (U_{\mathfrak{m}} K^\times) \cong I_K^{\mathfrak{m}} / K^{\mathfrak{m}}.$$

Note that $I_K^{\mathfrak{m}}$ is generated by prime ideals unramified in $K(\mathfrak{m})$. We can then extend the Frobenius $(\mathfrak{p}, K(\mathfrak{m})/K)$ by linearity to the Artin symbol $(\mathfrak{a}, K(\mathfrak{m})/K)$ for any $\mathfrak{a} \in I_K^{\mathfrak{m}}$.

Theorem 4.6.6

The isomorphism

$$\mathrm{Cl}_{\mathfrak{m}}(K) = I_K^{\mathfrak{m}} / K^{\mathfrak{m}} \to C_K / C_K^{\mathfrak{m}} \to \mathrm{Gal}(K(\mathfrak{m})/K)$$

is given by the Artin symbol $(\mathfrak{a}, K(\mathfrak{m})/K)$.

We say two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ coprime to $\mathfrak{m}$ are congruent mod $\mathfrak{m}$ if their images in $I_K^{\mathfrak{m}}/K^{\mathfrak{m}}$ are equal. We note that for any finite abelian L/K, the norm group $N_{L/K}(C_L)$ contains some $U_{\mathfrak{m}}$ since it is an open subgroup of finite index. As a consequence, L is a subfield of the ray class field $K(\mathfrak{m})$. Recall in the case of $\mathbb{Q}$ where upon embedding L inside $\mathbb{Q}(\zeta_m)$, primes that split completely in L are defined by congruence conditions mod m. Here, primes $\mathfrak{p}$ of K that split completely in L are defined by congruence conditions mod the modulus $\mathfrak{m}$. The converse is also true!

Proposition 4.6.7

Let L/K be a finite Galois extension of number fields. Suppose there is a modulus $\mathfrak{m}$ such that except for a finite set S of primes, the condition that a prime $\mathfrak{p}$ of K splitting completely in L is defined by congruence conditions mod $\mathfrak{m}$. Then L/K is abelian.

Proof. Let M be the Galois closure of $LK(\mathfrak{m})$ over K. We prove $L \subseteq K(\mathfrak{m})$ by showing that for all but finitely many primes, if $\mathfrak{p}$ splits completely in $K(\mathfrak{m})$, then it splits completely in L. By the Chebotarev density theorem, there exists a prime $\mathfrak{q} \notin S$ of K that split completely in M. Then $\mathfrak{q}$ splits completely in L and $K(\mathfrak{m})$. Let $\mathfrak{p} \notin S$ be a prime that splits completely in $K(\mathfrak{m})$. Then $\mathfrak{p} \equiv \mathfrak{q} \equiv 1 \bmod \mathfrak{m}$ since this is the condition for splitting completely in $K(\mathfrak{m})$. Since $\mathfrak{q}$ splits completely in L, we have $\mathfrak{p}$ splits completely in L since that's also defined by (possibly more) congruence conditions mod $\mathfrak{m}$. □

Corollary 4.6.8

(Furtwängler) For any subgroup H of the class group of K, there is an unramified abelian extension L/K such that the primes that split completely in L are exactly those whose ideal class lies in H.

What's next if one wants to learn more?

There are many directions one can go from here:

1. **Group cohomology**: A proof of global class field theory and another proof of local class field theory.

2. **Complex multiplication**: A construction of the ray class fields for imaginary quadratic fields, using torsion points of elliptic curves.

3. **Drinfeld modules**: A construction of ray class field for function fields.

4. **The Langlands program**: A study of n-dimensional representations of $\mathrm{Gal}(\bar{K}/K)$ with a lot of correcting adjectives! The case $n = 1$ is the group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ and follows from class field theory.