EYNTKA Class Field Theory

Nathanael Chwojko-Srawley

November 28, 2024

Contents

Consider a field extension L/K. There are many ways in which we may want to understand this extension. We may look at all the automorphisms $\mathrm{Aut}_K(L)$, which by galois theory tells us that if L/K is finite this corresponds to permutations of roots of polynomials and hence it makes sense to consider the normal closure and separable polynomials, leading us to focus on Galois extensions. The galois group characterizes a lot of information about galois extensions (and consequently, for polynomials and information about their solutions). There are still some open questions that an early exploration of Galois theory hasn't answered, for example:

1. What are the possible extensions given a base field K?
2. Can we use solution mod primes to piece together more information about polynomials? How does this relate to the information about primes given by the galois group?
3. Can we also use this exploration to reveal more information about primes and how they relate (ex. are the more laws like quadratic reciprocity?)

Class Field Theory (CFT) provides the groundwork for answering exactly these questions. The exploration of these results hinges on the fact that we may relate the primes of a Dedekind domain to galois groups via the Frobenius element in the case where L/K is an abelian extension. The nonabelian case is the generalization of these results and would be considered the beginning of Langland's program. By the end of this book, we shall fully classify all abelian extensions given a (global or local) base field K, which we shall see shall is directly related to (rational) primes in these fields linking these two concepts via the *Artin Reciprocity Law*, which shall be the ultimate result of this book.

Generalizing Quadratic Reciprocity

Recall that p is a quadratic residue mod q if and only if $\left(\frac{p}{q}\right) = 1$ where $\left(\frac{p}{q}\right)$ is the Legendre symbol. This symbol had satisfied the following equation:

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

Notice that we can consider the image of the Legendre symbol to be isomorphic to $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))$. As $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ holds information about equations of the form $x^2 - p \mod q$, it would be interesting if there is a function from the primes of $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ to the galois group that commutes with the Legendre symbol:

$$\begin{tikzcd}
\{\text{primes of } \mathbb{Q}(\sqrt{q})/\mathbb{Q}\} \arrow[r, "\left(\frac{p}{q}\right)"] \arrow[d, "="] & \{-1, 1\} \arrow[d, "\cong"] \\
\{\text{primes of } \mathbb{Q}(\sqrt{q})/\mathbb{Q}\} \arrow[r, "?"] & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))
\end{tikzcd}$$

It would then be not too much a stretch to ask if we can replace the domain of these functions with the collection of all ideals of $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$:

$$\begin{tikzcd}
\mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} \arrow[r, "\prod_p\left(\frac{p}{q}\right)"] \arrow[d, "="] & \{-1, 1\} \arrow[d, "\cong"] \\
\mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} \arrow[r, "?"] & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))
\end{tikzcd}$$

In fact, there is a connection: as $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))$ is abelian, then the Frobenius automorphism defined in [ChwNAc, chapter 22.4][1] and is exactly the map we can place at position "?", where the original condition of $\left(\frac{p}{q}\right) = 1$ if and only if there is a quadratic residue becomes "if and only if p splits completely":

$$\begin{tikzcd}
\mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} \arrow[r, "\prod_p\left(\frac{p}{q}\right)"] \arrow[d, "="] & \{-1,1\} \arrow[d, "\cong"] \\
\mathcal{I}_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}} \arrow[r, "\mathrm{Frob}_{\mathfrak{p}}"] & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{q}))
\end{tikzcd}$$

As nice as an observation this is, the question becomes whether this is an accident or a pattern; can $\mathrm{Gal}_{\mathbb{Q}}(K)$ (or even $\mathrm{Gal}_K(L)$) be replaced with another abelian galois group, where the abelian condition is necessary for the Frobenius automorphism to be well-defined, and we can find a corresponding "Legendre symbol" that and a group in the codomain that would make the above diagram commute? Does this generalize when looking at cubic reciprocity, biquadratic reciprocity, and so forth (with the appropriate replacement of the Legendre symbol and its image)? This was a major endeavour in the 20th century: Hilbert's 23rd problem was:

Find a proof of the most general reciprocity law for an arbitrary number field

As it turns out, such a law exists! The group that replaces $\{-1,1\}$ will be the *ideal class group* Cl_K, and the Legendre symbol shall be generalized to the Artin symbol! The result is called *Artin Reciprocity.*

However, it turns out that most groups will not be isomorphic to the class group, but the *quotient* of the class group. The reader may rightfully wonder if there then possibly a maximal extension L/K where $\mathrm{Gal}_K(L)$ is isomorphic to the class group. As it will again turn out, the answer is yes and results from a generalization of Kronecker Weber's theorem! Thus, we shall spent a substantial amount of time showing there are maps that make this diagram commute:

$$\begin{tikzcd}
\{\text{primes of } K\} \arrow[r] \arrow[d, dash, "="] & \mathrm{Gal}_K(L) \arrow[d, dash, "\cong"] \\
\{\text{primes of } K\} \arrow[r] & \mathrm{Cl}(K)/T_K
\end{tikzcd}$$

and if $L = K_H$ is an appropriate "maximal" field, then:

$$\mathrm{Cl}(K) \cong \mathrm{Gal}_K(K_H)$$

This incredible unification of the properties of primes and the polynomial relationships that can be put to associate them can be thought of as a crowning achievement of number theory in the 20th century (where the polynomials relations are represented by the galois group, and the degree in which a prime ideal is away from being a prime element is represented in the class group). In the process of developing this theory, it will come out that there are two approaches to the problem: one done by focusing on primes and their generalizations (i.e. places), and the other focusing on *local fields* and putting together the information of local fields to find global results. This latter approach will be the beginnings of much research into finding a nonabelian version of *Artin Reciprocity* and is a very active area of research as of writing this book[2]

[1] It shall be recalled in section 4.1

[2] See *Langland's Program* for more details

Material Overview

(really cool database for number theory! `https://www.lmfdb.org/`)

(This blog is really good here)

(also take a look at this link)

(and also Milne's book provides some very interesting intuitions!)

(huge amount of inspiration from these notes: MIT notes)

This book is a graduate textbook in number theory. The textbook [ChwNAc] is considered a prerequisite, in particular the chapter on *algebraic number theory* is a good litmus test on verifying the necessary background material.

I want to lay out some really interesting consequences:

1. After proving the Chebotarev Density Theorem, we shall see that a galois extensions of number fields is uniquely determined by the primes of K that split completely in L. A fascinating consequence is that if a.e. primes of K split completely in L, then $L = K$.
2. We shall see something called the *Artin Reciprocity.* This is the step-1 of Langland's program.

Class field theory is about the study of finite galois extensions C_K of a field K with certain properties on their galois group:

1. It must be abelian
2. the primes must be unramified
3. all principal ideals split completely

The reader may be taking away from this that all the objects of interest will lay in the maximal abelian extensions of a field K, and this is correct. What will be the key object of study in class field theory will be the relations between these groups and the yet-to-be-defined generalized class group.

It will eventually be said that a *class field* over K is a field whose galois group is the quotient of the [generalized] class group of K, which will be an abelian group and whose quotient will always be finite. There will be multiple ways of describing the class group. From [ChwNAc] it was defined for Dedekind domain to find how far away a Dedekind domain is from being principal. We shall see a way to describe them way *rays* and with *ideles.* The rays class groups are more algebraic in their definition, while the idele class is more topological in their definition. The ray class groups will be associated to fields which can be thought of as the generalization of the Kronecker-Weber Theorem.

The idelic language is useful, as it shall be shown in section ref:HERE that *any* finite abelian extension L of K will have galois group isomorphic to a quotient of the idele class group of K, namely if I_K is the idele class group, then:

$$\mathrm{Gal}(L/K) \cong \frac{\mathbb{I}_K}{N}$$

If furthermore N has the property of being an open subgroup of finite index, then L will be a *class field.* In the case of number fields, for any finite field $K/\mathbb{Q}$, there will exist an extension of K known as the *Hilbert class field* of K where

$$\mathrm{Gal}_K(K_H) \cong \mathrm{Cl}(K)$$

where $\mathrm{Cl}(K)$ is the class group of K, namely the group representing how how far away the ring $\overline{\mathbb{Z}}^K = \mathcal{O}_K$ is from being principal. This shows that there is a deep connection between the primes of the ring of integers and the symmetries of polynomials over fields! On of the main results that will be shown is that:

$$\begin{tikzcd}
\{\text{primes of } K\} \arrow[r] \arrow[d, dash, "="] & \mathrm{Gal}_K(K_H) \arrow[d, dash, "\cong"] \\
\{\text{primes of } K\} \arrow[r] & \mathrm{Cl}(K)
\end{tikzcd}$$

Note that the horizontal maps need not be isomorphism at all, however the right-vertical map will be an isomorphism!

A glimpse into motivation for why such maps can be interesting is by looking into the simpler case of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (where $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$). In this case, every unramified prime $p \subseteq \mathbb{Z}$ corresponds to the Frobenius automorphism in $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$. The need for the prime to be unramified comes from the need for the inertia group to be trivial for the prime p to be uniquely associated to the Frobenius automorphism. Then recall that p is unramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ if and only if $p \nmid n$. Thus, there is a natural map:

$$\{p \nmid n\} \to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \qquad p \mapsto \mathrm{Frob}_p(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\zeta_n \mapsto \zeta_n^p)$$

Or equivalently as the galois group is isomorphic to the $(\mathbb{Z}/n\mathbb{Z})^*$, it can be thought of the map sending $p \mapsto p \mod n$.

As it shall turn out, an abelian extension is fully characterized by slitting primes!

p.54 of the MIT notes provide an interesting link between the ideal norm and algebraic geometry. Idk where to put this yet, so putting reminder here.

1

Local Fields

In this chapter, we shall explore special fields which focus into a single prime of a number field. For a prime *pin*$\mathbb{Z}$, the fundamental object corresponding to this prime is the p-adic integers $\mathbb{Z}_p$. Intuitively, solving an equation over $\mathbb{Z}_p$ corresponds to solving an equation over $\mathbb{Z}$ mod p^n for each n (which can be thought of as solving the equation over all multiplicities). Each $\mathbb{Z}_p$ shall correspond to a field $\mathbb{Q}_p$, and finite extensions of $\mathbb{Q}_p$, $K_\mathfrak{p}/\mathbb{Q}_p$, shall only contain primes that are over p. The galois group of these extensions shall then be isomorphic to the decomposition group. The field extensions $K_\mathfrak{p}$ shall be called *local number fields.* Finite extensions $K/\mathbb{Q}$ will be called *global number fields.* A large part of the early sections is dedicated to building up the theory of local fields. This culminates with proving the Local-to-Global Correspondence in section 1.8 which readily translates over many results between global fields and local fields.

In the process of developing the generalization, we shall see that the local fields $\mathbb{Q}_p$ correspond very naturally to all possible distinct absolute values that can be defined on $\mathbb{Q}$. In fact, the collection of all possible absolute absolute values that can be defined on $\mathbb{Q}$ shall create the following completions:

$$\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, .., \mathbb{Q}_\infty = \mathbb{R}$$

where there is one distinct completion for each prime, as well as one completion that can in fact be naturally interpreted as the completion at the "prime at infinity". We shall make this idea precise in chapter 2. The idea of places being an extension of primes shall become important when developing class field theory, as well as linking it to the development of extensions of $\mathbb{F}_p(t)$.

Near the end of this chapter, we shall prove the *Kronecker-Weber Theorem* which shows that all abelian extensions are naturally interpreted as being sub-extensions of a cyclic extension. This result shall show a deep connection between galois groups and primes, and shall to great effect be generalized: in chapter 4 we shall develop this completely and show that for every field K,there always exists a field K_H such that the galois group $\mathrm{Gal}_K(K_H)$ is isomorphic to a class group!

1.1 p-adic Integers and p-adic Numbers

Let us start with giving a detailed description of the "new integers" where we only focus on a single prime. Let R be a commutative ring, $\mathfrak{p} \subseteq R$ a prime. Then $R_{\mathfrak{p}}$ will represent the localization of R at $\mathfrak{p}$ (i.e. at the set $R \setminus \mathfrak{p}$). Recall that the completion of R at a prime P is:

$$\varprojlim_n R/\mathfrak{p}^n R = \widehat{R}$$

where the $\mathfrak{p}$ is usually understood from context on the right hand side. For number theory, we are interested in the case where $R = \mathbb{Z}$. This gives us the localizations $\mathbb{Z}_{(p)}$ and the completions $\widehat{\mathbb{Z}}_p$ which we shall denote $\mathbb{Z}_p$. Elements in the completion can be represented as the formal power series:

$$\sum_i^{\infty} a_i p^i = a_0 + a_1 p + a_2 p^2 + \cdots$$

where $a_i \in \{0, ..., p-1\}$. More succidnetly, as $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, as a sequence

$$(a_0 \mod p, a_1 \mod p^2, ...)$$

It is not immediately clear that these two are the same: in the first we have multiplication via convolution, while in the second we have point-wise multiplication. The equivalence in these two representation can be given by the following: any element can be found by seeing that when we are given:

$$s = \sum_i^{\infty} a_i p^i$$

it has to satisfy:

$$s_n = \sum_i^{n-1} a_i p^i$$

hence, for any $[r] \in \mathbb{Z}/p^n\mathbb{Z}$, there exists a representative of the form:

$$[r] = [a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}]$$

Such an expansion can be written down for any $r \in \mathbb{Z}_{(p)}$, that is for any a/b where $p \nmid b$. From this, if we consider $\mathbb{Z}_p$ to be the formal power series with addition/multiplication extending naturally. From this:

Proposition 1.1.1: Representation Of p-addic

Let $\mathbb{Z}_p$ represent the formal p-adic integers and $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ the completion definition. Then:

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

***Proof* :**
Put together all the above assertions.

A motivation for defining the p-adic integers is in the following "universal property": the solutions to Diophantine equations (elements of $\mathbb{Z}[x_1, ..., x_n]$) $\mod p^n$ for all $n \in \mathbb{N}_{>0}$ equivalent to finding solution to diophantine equations over the p-adics. Note that if we ask for solutions over some collection $\mod m$, by the CRT we may reduce the case to solution over powers of primes.

Theorem 1.1.2: Diophantine Equations in p-adic

Let $f \in \mathbb{Z}[x_1, ..., x_n]$. Then the congruence:

$$f \equiv 0 \mod p^n$$

for all $n \geq 1$ is solvable if and only if f is has solutions in the p-adics.

***Proof* :**

Let's first say f has a solution in the p-adics, meaning we make a choice of elements $(x_1, .., x_n)$:

$$(x_1, ..., x_n) = (x_1^{(\nu)}, ..., x_n^{(\nu)})_{\nu \in \mathbb{N}} \in \mathbb{Z}_p^n$$

such that $f(x_1, ..., x_n) = 0$. Then by construction we get:

$$f(x_1^{(\nu)}, ..., x_n^{(\nu)}) = 0 \mod p^\nu$$

Conversely, assume for each $\nu \in \mathbb{N}$ there is a solution

$$f(x_1^{(\nu)}, ..., x_n^{(\nu)}) = 0 \mod p^\nu$$

If by chance we have that the collection $(x_i^{(\nu)})_{\nu \in \mathbb{N}} \in \prod_\nu^\infty \mathbb{Z}/p^\nu\mathbb{Z}$ is already in $\varprojlim_\nu \mathbb{Z}/p^\nu\mathbb{Z}$, we're done. However, having solutions to moduli equaiton doesn't immediately guarantee the regularity needed for the limit. Instead, a p-adic number will be constructed using these numbers.

We shall construct the construction for the case of $n = 1$, the general case follows. Let $x_\nu = x_1^{(\nu)}$. Then this defines a sequence (x_ν) in $\mathbb{Z}$. As $\mathbb{Z}/p\mathbb{Z}$ has finitely many elements, there are infinitely many elements of the sequence that are congruent to the same element $y_1 \mod p$. Then if $(x_\nu^{(1)})$ is the subsequence:

$$(x_\nu^{(1)}) \equiv y_1 \mod p \qquad \text{hence} \qquad F(x_\nu^{(1)}) \equiv 0 \mod p$$

From this, another subsequence $(x_\nu^{(2)}) \subseteq (x_\nu^{(1)})$ can be extracted st

$$(x_\nu^{(2)}) \equiv y_2 \mod p \qquad \text{hence} \qquad F(x_\nu^{(2)}) \equiv 0 \mod p^2$$

Continuing on, we get y_i where

$$y_k \equiv y_{k-1} \mod p^{k-1}$$

Hence, we can define $y = (y_k)_{k \in \mathbb{N}} \in \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, which is our desired p-addic integer:

$$F(y_k) = 0 \mod p^k \qquad \text{if and only if} \qquad F(y) = 0$$

as we sought to show.

Example 1.1: *p*-adic Integers

1. Let $n = 10$. Then $10 = 20_5 = 1010_2 = 101_3 = 10_n$ for $n \geq 10$. For non-prime p, we can still do the n-adic completion $\mathbb{Z}_n$, however we will get zero divisors. For example:
$$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$$
which comes from the direct commuting with completion (see [ChwNAc]).

2. Let $p = 3$ and considier -1_3. I claim that -1_3 exists. We need to find $[\cdots a_3 a_2 a_1]_3$ such that
$$0001_3 + -1_3 = 0$$
Then $\cdots 222_3$ will give the answer. since:
$$\cdots 222_3 + \cdots 0001_3 = \cdots 000_3$$
Repeat this for any negative number

3. Let $p = 3$ and consider $1/2$. I claim that $(1/2)_3$ exists. We need to find $[\cdots a_3 a_2 a_1]_3$
$$(1/2)_3 \cdot 2_3 = \cdots 0001_3$$
To construct such a number, first:
$$a_1 \cdot 2 \equiv 1 \mod 3$$
hence $a_1 = 2$. We then need:
$$2 \cdot a_2 + 1 \equiv 0 \mod 3$$
which gives $a_2 = 1$. Continuing we get:
$$(\cdots 1112_3) \cdot (\cdots 0002)_3 = (\cdots 0001)_3$$
This can be done for any prime $p \neq 2$.

4. Let $a/b \in \mathbb{Q}$. Then if $p \mid b$ there is no p-adic representation. For example, $1/5$ does not have a 5-adic representaiton (you would need to mulitply $1/5$ by 5, but $0005_5 = 0_5$).

5. Using the second example, find the p-adic representation of $\frac{1}{1-p}$.

By the above example, we see that the elements of $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ can be represented as by the p-adic's $\mathbb{Z}_p$ and hence there is a natural map:
$$\mathbb{Z}_{(p)} \to \mathbb{Z}_p$$
This map is not surjective (the right hand side is uncountable, or more concretely the right hand side will have $\sqrt{2}$ when $p \neq 2$). This also comes form the more general result that if R is a ring and $\widehat{R}$ is the completion at $\mathfrak{p}$, then if $u \in R/\mathfrak{p}^n$ is a unit, $u \in R/\mathfrak{p}^{2n}$ is a unit. In particular, if $\mathfrak{p} = \mathfrak{m}$ is a maximal ideal, $\widehat{R}_{\mathfrak{m}}$ is a local ring, and hence $\mathbb{Z}_p$ is a local ring (see [ChwNAc])

Then as $\mathbb{Z}_p$ has a unique maximal ideal, label it $\mathfrak{m}_{\mathfrak{p}}$, let us now consider the localization of $\mathbb{Z}_p$ at $\mathfrak{m}_{\mathfrak{p}}$. Let's denote it $\mathbb{Q}_p$. The completion will consist of all "Laurent series", that is all elements of the form:

$$\sum_{-m}^{\infty} a_i p^i$$

for all $m \in \mathbb{Z}$, $0 \leq a_i < p$. This allows us to represent *any* rational number, for example if $a/b \in \mathbb{Q}$, then represent it as:

$$\frac{a}{b} = \frac{g}{h} p^{-m} \qquad g, h \in \mathbb{Z} \qquad \gcd(gh, p) = 1$$

We can then do the p-adic expantion of $g/h = p^m f$:

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

we then shift everything down by m to get the p-adic expansion of f:

$$a_0 p^{-m} + a_1 p^{-m+1} \cdots + a_{m-1} p^{-1} + a_m + a_{m+1} p + a_{m+2} p^2 + \cdots$$

this is called a p-addic number. Notice the similarity to meromorphic functions in complex analysis (this was where the theory of p-adic integers and numbers where inspired). Hence, we have the more general embedding:

$$\mathbb{Q} \to \mathbb{Q}_p = (\mathbb{Z}_p)_{\mathfrak{m}_\mathfrak{p}}$$

where $\mathbb{Z}$ injects into $\mathbb{Z}_p$ (if a, b have the same p-addic expansion, $a - b$ is divisible by p^n for every n, hence $a = b$ in $\mathbb{Z}$). Given this, idnetify $\mathbb{Q} \subseteq \mathbb{Q}_p$ and $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Let us now take another perspective on $\mathbb{Q}_p$ that is more analytic. Recall that in [ChwNAc, chatper 19] we classified all absolute values on $\mathbb{Q}$, namely the p-valuations and the usual absolute value. Recall the p-valuation is defined on $\mathbb{Q}$ as:

$$|a|_p = \left|\frac{b}{c}\right|_p = \left|p^m \frac{b'}{c'}\right|_p = p^{-m} \qquad \gcd(b'c', p) = 1$$

Where in the p-adic representation of a, we may think of ν_p as counting how many 0's there are before hitting the first non-zero digit, for example in $625 = 1000_5$ we have:

$$|625|_5 = \frac{1}{5^4}$$

Hence, the larger the larger the order of the prime p in a/b, the smaller the valuation. This is perhaps intuitive if we compare p-adic expansion to decimal expansion, in which we have:

$$a_0 + a_1 \left(\frac{1}{10}\right) + a_2 \left(\frac{1}{10}\right)^2 + \cdots$$

with $1 \leq a_0 < 10$. Then the more a_i's that are zero, the smaller the valuation. The above representation of a number in decimal-expansion is good for visualizing a valuation called the ∞-valuation, $|-|_\infty$ which is the unique Archimedean valuation on $\mathbb{Q}$ up to equivalence (as all p-valuations induce an ultra-metric, they are all non-Archimedean). In this construction, what is important is the exponent, and not the p. The intuition from this comes from the induced p-adic topology, namely from $|-|_p$ we can define the [ultra]-metric

$$d(x, y) = |x - y|_p$$

from which we can construct $\mathbb{Q}_p$ from $\mathbb{Q}$ by taking it's completion using the above metric. Then choosing another constant c will produce equivalent topologies; what matter's for the definition is the factoring of the p and not the "concrete representation".

To continue creating intuition's, let us motivate the $|-|_\infty$ symbol. This comes from considering $k(t)$ over a finite field k, where the analog of $\mathbb{Z}$ is $k[x]$. In $k[x]$, there are monic irreducible polynomials which are in one-to-one correspondence with the primes $\mathfrak{p}$ of $k[t]$ (recall $k[t]$ is a PID). Hence, define $|-|_\mathfrak{p} : k(t) \to \mathbb{R}$ as:

$$f(t) = \frac{g(t)}{h(t)} = p(t)^m \frac{g'(t)}{h'(t)} \qquad (g'h', p) = 1$$

Then define $\nu_\mathfrak{p}(f) = m$. Then topologically the choice of what to exponentiate doesn't matter, however an informed choice will give us more information, namely let $q_\mathfrak{p} = q^{d_\mathfrak{p}}$ where q is any real number > 1 and d_p is the degree of the residue class field of $\mathfrak{p}$ over k (i.e. of $\kappa(f)$). Then:

$$\nu_\mathfrak{p}(f) = m \qquad |f|_p = q_\mathfrak{p}^{-\nu_\mathfrak{p}(f)}$$

Notice that $\nu_\mathfrak{p}(0) = \infty$ and $|0|_\mathfrak{p} = 0$, giving us that these are indeed the discrete valuations. When $\mathfrak{p} = (t-a)$, the valuation $\nu_\mathfrak{p}(f)$ gives the order of the zero/poles of the function $f(t)$ at $t = a$. Then for the infinite case, we have:

$$\nu_\infty : k(t) \to \mathbb{Z} \cup \{\infty\} \qquad \nu_\infty(f) = \deg(h) - \deg(g)$$

for $f = g/h \neq 0$ and $g, h \in k[t]$. This can be thought of describing the zero and poles at the point at infinity, i.e. the zeros and pole of the function $f(1/t)$ at the point 0. It is in fact associated to a prime ideal, namely $\mathfrak{p} = (1/t)$ in $k[1/t] \subseteq k(t)$. Hence, when considering the absolute value $|-|$ on $\mathbb{Q}$, we may think of this as being the evaluation at the point at infinity, and hence the $|-|_\infty$ symbol. Notice too how this motivates that the size of $|-|_\infty$ diminishes the more zeros' there are in the decimal expansion and taking the reciprocal of integers. As the concrete value of "t" doesn't matter, we can consider any integer and get an expansion that mimics the properties of $|-|_\infty \to 0$, for example

$$a_0 + a_1\left(\frac{1}{2}\right) + a_2\left(\frac{1}{2}\right)^2 + \cdots$$

Finally, for $k(t)$, there is also a 0-valuation given by:

$$|f/g|_0 = \mathrm{ord} g - \mathrm{ord} f$$

where the order represents the first degree of the smallest non-trivial monomial, for example $\mathrm{ord}(ax^3 + bx) = 1$. Then in $\mathbb{Q}$, $|-|_0$ is the trivial valuation.

Coming back to absolute values over $\mathbb{Q}$, as what is important is the exponent and not the choice of constant to be exponentiated, it is often better to define a new functional, namely a discrete valuation, which only captures the exponent information. The reader should recall from [ChwNAc, chatper 20] the following the function $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ where $x + \infty = \infty + x = \infty + \infty = \infty$:

1. $\nu_p(a) = \infty$ if and only if $a = 0$ (this mirror's the idea that p divides 0 infinitely many times
2. $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
3. $\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b))$

The last condition can be thought of as the ultra-metric condition[1]. From this, we may define p-valuations as

$$| - |_p : \mathbb{Q} \to \mathbb{R} \qquad a \mapsto |a|_p = p^{\nu_p(a)}$$

and we may choose to change p to any other constant $c > 1$.

Now, with the p-adic metric properly defined on $\mathbb{Q}$, we may take the completion of $\mathbb{Q}$ under this metric by taking all Cauchy-sequences of $\mathbb{Q}$ and taking the quotient of all null-sequences (sequences that approach 0). Note that null-sequences form a maximal ideal in the ring of Cauchy-sequences. If R is the ring of Cauchy-sequences and $\mathfrak{m}$, then:

$$\mathbb{Q}_p \cong R/\mathfrak{m}$$

and hence, is an equivalent definition. The reader may see that $\mathbb{Q}_p$ is complete, and that $\mathbb{Q}_\infty = \mathbb{R}$. $\mathbb{Q}$ is naturally embedded in $\mathbb{Q}$ via the constant sequence, and as $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ the p-adic valuation naturally extends, namely:

$$|x|_p := \lim_{n\to\infty} |x_n|_p \in \mathbb{R}$$

where x_n are the elements in the sequence[2]. To show that the $\nu_p(x)$ still represents the exponent (i.e. is an integer), if $x \in \mathbb{Q}_p$ is taken as the class of Cauchy-sequences (where $x_n \neq 0$) then:

$$\nu_p(x_n) = -\log_p |x|_p$$

either diverges or converges is a Cauchy-sequence in $\mathbb{Z}$ which eventually must be constant for large enough n. Then:

$$\nu_p(x) = \lim_{n\to\infty} \nu_p(x_n) = \nu_p(x_n) \qquad \text{for } n \geq n_0$$

Thus, we come full circle and have:

$$|x|_p - p^{-\nu_p(x)}$$

We now have a collection of complete fields with different absolute values:

$$\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, ..., \mathbb{Q}_\infty = \mathbb{R}$$

From each of these, we may extract $\mathbb{Z}_p$ in the following way:

Proposition 1.1.3: Characterizing p-adic Integers

Considering $\mathbb{Q}_p$ as the completion as given above, show that:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ |x|_p \leq 1\}$$

is a well-defined ring. Then $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ with respect to $| - |_p$

***Proof* :**
exercise.

[1] And indeed, we can define discrete valuations to be a generalization of non-Archimedean valuations, see [ChwNAc, chapter 19]

[2] Technically, this is mod $\mathfrak{m}$; the reader may want to do some practice by checking this is indeed well-defined

Using the p-adic valuation, we may characterize the units of $\mathbb{Z}_p$ as:

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \ : \ |x|_p = 1\}$$

Using this, we may represent every $x \in \mathbb{Q}_p^*$ as :

$$x = p^m u \qquad m \in \mathbb{Z}, \ u \in \mathbb{Z}_p^*$$

that is, every element of $\mathbb{Q}_p^*$ is some unit times some power of prime. For if:

$$\nu_p(x) = m \in \mathbb{Z} \quad \Rightarrow \quad \nu_p(xp^m) = 0 \quad \Rightarrow \quad |xp^{-m}|_p = 1$$

thus $u = xp^{-m} \in \mathbb{Z}_p^*$. Going back to the localization definition of $\mathbb{Z}_p$, this can be seen by remembering that all other primes are localized, and hence any prime factorization $\mathbb{Z}_p$ will now only have a single prime left (and the above argument shows this holds in the completion). From this, we can characterize the ideals of $\mathbb{Z}_p$:

Proposition 1.1.4: Classifying Ideals Of p-adic Integers

Let $\mathbb{Z}_p$ be the p-adic integers. Then set set of nonzero ideals of $\mathbb{Z}_p$ are the principal ideals:

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \ : \ \nu_p(x) \geq n\}$$

with $n \geq 0$. Furthermore:

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

***Proof* :**

The first part is a result of the theory of valuations, and is left as an exercise (or check[ChwNAc])

To show the isomorphism, we'll show that the map $\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ where $n \mapsto n \mod p^n\mathbb{Z}_p$ is surjective. To see this, as $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|-|_p$, for any $x \in \mathbb{Z}_p$ there exists an $a \in \mathbb{Z}$ such that

$$|x-a|_p \leq \frac{1}{p^n}$$

Thus, $x - a \in p^n\mathbb{Z}_p$ (since $n \in \mathbb{Q}$ is in $\mathbb{Z}_p$ if and only if $|n|_p \leq 1$), i.e. $x \equiv a \mod p^n\mathbb{Z}_p$. Hence, the map is surjective, the kernel consists of all elements where $a \in \mathbb{Z}$ where $a \in p^n\mathbb{Z}_p$, which is exactly the elements of the form $a = p^n x$ for $x \in \mathbb{Z}$, that is the elements $p^n\mathbb{Z}$, hence:

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

as we sought to show.

Using this, we have that:

Proposition 1.1.5: Next Equivalence Of p-adic Integers

Show that with $\mathbb{Z}_p$ as defined from above we have:

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

***Proof* :**
As $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, we get a surjective homomorphism:

$$\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$$

This gives a family of homomorphisms which can be used to construct a homomorphism:

$$\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

show this is an isomorphism

Finally, let us characterize p-adic integers in one more way and quickly address a possible miss-conception of the fields $\mathbb{Q}_p$ with respect to $\mathbb{R}$. For the new characterization:

Proposition 1.1.6: Equivalence Of p-adic Via Power-series Quotient

$$\mathbb{Z}_p \cong \mathbb{Z}[[x]]/(x-p)$$

***Proof* :**
exercise.

A common mistake a reader may do is think that $\mathbb{Q}_p \cong \mathbb{R}$ algebraically. We proved this is not the case in [ChwNAc], however a concrete example should help.

Example 1.2: Cautions for p-adic Numbers

1. Recall that $1/p \notin \mathbb{Z}_p$ (review why if this is fuzzy). As $1/p \in \mathbb{Q}_p$, we cannot use it to construct our counter-example. Instead, we shall show that $\sqrt{p} \notin \mathbb{Q}_p$. To see this, notice that $\sqrt{p}$ by definition satisfies the equation $x^2 - p$. Then certainly it would have to satisfy the equation modulo p^n for every n. Then if $\sqrt{p} \in \mathbb{Q}_p$, it must be the case that $\sqrt{p} \in \mathbb{Z}_p$ by theorem 1.1.2. However, $x^2 \equiv p \mod p^2$ has no solutions, and hence $\sqrt{p} \notin \mathbb{Q}_p$.

   On the other hand, $\sqrt{1-p^3} \in \mathbb{Q}_p$, as the equations $x^2 - 1 + p^3$ have a solution mod each p^n (use quadratic reciprocity). However, $\sqrt{1-p^3} \notin \mathbb{R}$ as this would require a negative square-root, a number we know that $\mathbb{R}$ does not contain.

2. By field theory, we know that $\mathbb{Q}_p$ embeds into $\mathbb{C}$. This is an example where we really require the axiom of choice. The embeddings is far away from preserving the topological structure of $\mathbb{Q}_p$ or being represented in $\mathbb{C}$. To see this, first notice that $\pm\sqrt{-1} = \pm i \in \mathbb{Q}_5$. It may seem like we should map i to either $\pm i$. However, note that i is closer to 2 while $-i$ is closer to 3. In fact, i is even closer to 57 while the other is much closer to 68. In fact, without the axiom of choice, this embedding would not be possible. Algebraically, you may also try to check that $\mathbb{Q}_5$ has no automorphisms that swap i and $-i$ (in fact it has *no* non-trivial automorphisms, mirroring how $\mathbb{R}$ has no non-trivial automorphisms[a].

3. Another interesting distinction between $\mathbb{Q}_p$ and $\mathbb{R}$ the degree of $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ vs $\overline{\mathbb{R}}/\mathbb{R}$. In the latter, we have $\overline{\mathbb{R}} \cong \mathbb{C}$, and we have a degree two extension. After covering Hensel's lemma, we

shall see that $x^n - p$ is irreducible for each n in $\mathbb{Q}_p$. It can be shown that there are finitely many extensions for each degree n, and so $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ is a countable extension.

[a] see exercise ref:HERE in [ChwNAc]

1.1.1 Generalization: DVR

We now need to have a way to generalize this notion for rings of integers more generally. Recall that Dedekind domains are locally DVRs. The intuition is that the localization of a Dedekind domain to the DVR gives information of the multiplicity of a prime. Topologically, we may take advantage of the fact that ideals in $\mathbb{Z}_p$ form a chain:

$$\mathbb{Z}_p \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq ...$$

More generally, as any discrete valuation ring $\mathcal{O}$ has a chain of ideals, we have:

$$\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq ...$$

Then these ideals form a neighborhood-basis. Indeed, if ν is a normalized exponential valuation (see [ChwNAc, section 20.7]) and $|-| = q^{-\nu}$ for $q > 1$, we have:

$$\mathfrak{p}^n = \left\{ x \in K \ : \ |x| < \frac{1}{q^{n-1}} \right\}$$

and we can define a topology on K^* through the sets:

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K^* \ : \ |1 - x| < \frac{1}{q^{n-1}} \right\} \qquad n > 0$$

so that we have the descending chain:

$$\mathcal{O}^* = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots$$

Notice these are all subgroups under multiplication (use that the valuation is a homomorphism and that $1 + \mathfrak{p}^n = \left\{ x \in K^* \ : \ |1 - x|_p < \frac{1}{q^{n-1}} \right\}$ for some choice of q to define the p-absolute value). These subgroups are called the *higher unit groups* and $U^{(1)}$ is called the group of *principal units*. These groups have the following property:

Proposition 1.1.7: Higher Unit Group

For $n \geq 1$,

$$\mathcal{O}^*/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^* \qquad \text{and} \qquad U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$$

***Proof* :**

Take the surjection $\mathcal{O}^* \to (\mathcal{O}/\mathfrak{p}^n)^*$. The kernel then is certainly $U^{(n)}$. Similarly for the 2nd isomorphism, where $U^{(n)} = 1 + \pi^n \mathcal{O}$ which maps $1 + \pi^n a \mapsto a \mod \mathfrak{p}$.

Proposition 1.1.8: Characterizing DVR Via Completion

Let $\mathcal{O}$ be a DVR. Then:

$$\mathcal{O} \cong \varinjlim_{n} \mathcal{O}/\mathfrak{p}^n \qquad \mathcal{O}^* \cong \varinjlim_{n} \mathcal{O}^*/U^{(n)}$$

showing that each valuation ring is naturally characterized as a colimit given by its unique maximal ideal.

> ***Proof*** **:**
> exercise (Neukirch p.128 if you're stuck)

Completion of Discrete Valuation Ring

Let k be a field with a discrete valuation defined on it. This discrete valuation can be extended to $\widehat{k}$ and denoted $\widehat{\nu}$, the completion of k by setting:

$$\widehat{\nu}(a) = \lim_{n\to\infty} \nu(a_n)$$

Now, for any arbitrarily small ϵ, there exists an a_n such that $|a - a_n| < \epsilon$. Letting $\epsilon = p^{-N}$ for some large n ,we see that at some point it must be that:

$$\widehat{\nu}(a - a_n) \geq \widehat{\nu}(a)$$

and so

$$\nu(a_n) = \widehat{\nu}(a_n - a + a) = \min\{\widehat{\nu}(a_n - a), \widehat{\nu}(a)\} = \widehat{\nu}(a)$$

showing that the valuation extends to the completion:

$$\nu(k^*) = \widehat{\nu}(\widehat{k}^*)$$

Proposition 1.1.9: Valuation Ring Quotient And Completion

Let K be a field with valuation ν. Let $\mathcal{O} \subseteq K$ be the valuation ring of K and $\widehat{\mathcal{O}} \subseteq \widehat{K}$ with completed valuation $\widehat{\nu}$. Then:

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$$

If ν is discrete, then:

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n$$

> ***Proof*** **:**
> generalize proposition 1.1.4

Using this, the p-adic expansion extends to the completion of any discrete discrete valuation of K (see Neukirch p.127 for more details). The main advantage of this generalization is to show that the power-series expansion also works for function fields and we get fields of formal power series $K((x))$ with the infinite expansion representation.

Exercise 1.1.1

1. Show that $\sqrt{2} \in \mathbb{Q}_p$ if and only if $x^2 - 2$ factor into linear factors $\mod p$.

1.2 Extension of Valuation

In this whole section, we shall be consider the following scenario all the time:

Let A be an integral domain, K the field of fractions of A, L a finite extension of K, and B the integral closure of A in L. This setup shall be called the *AKLB setup.*

We shall put some different conditions on A depending on what we need. In number theory, we usually have A be an integral domain.

Recall that each prime $\mathfrak{p} \subseteq A$ where A is a Dedekind domain determines a discrete valuation $\nu_{\mathfrak{p}} : \mathcal{I}_A \to \mathbb{Z}$ by giving the exponent $n_{\mathfrak{p}}$ form the unique factorization (i.e. $\nu_{\mathfrak{p}}(I) = n$ if and only if $IA_{\mathfrak{p}} = \mathfrak{p}^n A_{\mathfrak{p}}$). Thus for each prime $\mathfrak{p} \subseteq A$, we have the discrete valuation:

$$\nu_{\mathfrak{p}} : K \to \mathbb{Z} \qquad \nu_{\mathfrak{p}}(x) = \nu_{\mathfrak{p}}(xA)$$

and hence an absolute value $|x|_{\mathfrak{p}} := c^{\nu_{\mathfrak{p}}(x)}$ for $0 < c < 1$. If we have $AKLB$, primes $\mathfrak{B}/\mathfrak{p}$ also give rise to a discrete valuation $\nu_{\mathfrak{B}}$ on L, each restricts to a valuation on K, but the valuation need not be equal to $\nu_{\mathfrak{p}}$. Let us start by understanding the relation

Definition 1.2.1: Extending Valuations

Let L/K be a finite separable extension, and let ν, w be discrete valuation on K, L respectively. Then if $w|_K = e\nu$ for some $e \in \mathbb{N}_{>0}$, then w is said to *extend ν with index e*

Theorem 1.2.2: Extension of Valuation

Let $AKLB$, $\mathfrak{p} \subseteq A$ a prime, and $\mathfrak{B}/\mathfrak{p}$ a prime in B lying over $\mathfrak{p}$. Then there is a discrete valuation $\nu_{\mathfrak{B}}$ which extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{B}}$, and every discrete valuation on L that extends $\nu_{\mathfrak{p}}$ arises in this way. Thus, we have a bijection $\mathfrak{B} \to \nu_{\mathfrak{B}}$ from $\mathfrak{B}/\mathfrak{p}$ to the set of discrete valuation on L that extend $\nu_{\mathfrak{p}}$.

***Proof* :**

Let $\mathfrak{B}/\mathfrak{p}$ so that $\nu_{\mathfrak{B}}(\mathfrak{p}B) = e_{\mathfrak{B}}$ by definition, and if $\mathfrak{p} \neq \mathfrak{p}'$ then $\nu_{\mathfrak{B}}(\mathfrak{p}'B) = 0$ as $\mathfrak{B}$ lies above only one prime. Now if $I = \prod_{\mathfrak{p}'}(\mathfrak{p}')_{n_{\mathfrak{p}'}}$ is a nonzero fractional ideal then:

$$\nu_{\mathfrak{B}}(IB) = \nu_{\mathfrak{B}}\left(\prod_{\mathfrak{p}'}(\mathfrak{p}')_{n_{\mathfrak{p}'}}B\right) = \nu_{\mathfrak{B}}(\mathfrak{p}^{n_{\mathfrak{p}}}B) = \nu_{\mathfrak{B}}(\mathfrak{p}B)n_{\mathfrak{p}} = e_{\mathfrak{B}}n_{\mathfrak{B}} = e_{\mathfrak{B}}\nu_{\mathfrak{p}}(I)$$

Thus, $\nu_{\mathfrak{B}}$ extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{B}}$.

Furthermore, if $\mathfrak{B}, \mathfrak{B}$ are two distinct primes lying over $\mathfrak{p}$, then neither contains each other, and any $x \in \mathfrak{B} - \mathfrak{B}'$ we have

$$\nu_{\mathfrak{B}}(x) > 0 \geq \nu_{\mathfrak{B}'}(x)$$

and so $\nu_{\mathfrak{B}} \neq \nu_{FB'}$, and so $\mathfrak{B} \mapsto \nu_{\mathfrak{B}}$ is injective.

To show that every extension of valuation arises in this way, let w be a discrete valuation on L that extends $\nu_{\mathfrak{b}}$ with index e. Let

$$W = \{x \in L \ : \ w(x) \geq 0\}$$

be the associated DVR and let $\mathfrak{m}$ be the associated maximal ideal. Since $w|_K = e\nu_{\mathfrak{p}}$ by definition of w, the discrete valuation on w is nonzero on A, and hence $A \subseteq W$. The elements of A with nonzero valuation are exactly the elements of $\mathfrak{p}$, and hence

$$\mathfrak{p} = \mathfrak{m} \cap A$$

Furthermore, the DVR W is integrally closed in its fraction field L (see [ChwNAc]), and so $B \subseteq W$ by minimality for B. Now, $\mathfrak{B}$ is prime (since $\mathfrak{m}$ is) and $\mathfrak{p} = \mathfrak{m} \cap A = \mathfrak{B} \cap A$, and so $\mathfrak{B}$ lies over $\mathfrak{p}$. The ring W contains $B_{\mathfrak{B}}$ and is contained in Frac$B_{\mathfrak{B}} = L$. But now, there is no intermediate rings between DVR and fraction fields (see [ChwNAc]), and so $W = FB_{\mathfrak{B}}$, and $w = \nu_{\mathfrak{B}}$ with $e = e_{\mathfrak{B}}$, completing the proof.

1.3 Local Fields

Definition 1.3.1: Global And Local Fields

1. A *global field* if a finite extension of either $\mathbb{Q}$ or $\mathbb{F}_p(t)$.
2. A *local field* is a field which is complete with respect to a discrete valuation ν and its residue field, k, is finite.

Note that the valuation on the completion of global fields is discrete and has a finite residue class field. If we don't specify the finite residue field, we shall get some constructions we are not looking for. We should immediately re-characterize local fields to make them easier to work with:

Proposition 1.3.2: Characterizing Local Fields

Let K be a local field. Then either:

1. K is a finite extension of $\mathbb{Q}_p$
2. K is a finite extension of $\mathbb{F}_p((t))$

Some authors will define local fields to be completion of fields with respect to an absolute value to allow for $\mathbb{R}$ to be a local field, but this will not be done here In particular, Varma does this.

Proof **:**
Neukirch p.135

I will for now take this as granted, for in my head local fields can be seen as being these by definition. The point of the abstraction is to unify them and not need to keep taking cases, but I will be okay with that for now.

Hence, the local fields of characteristic $p \neq 0$ are of the form $\mathbb{F}_q((t))$ where $q = p^n$, and local fields of characteristic 0 are finite extensions of $K/\mathbb{Q}_p$. The former will be called *power series fields*, and the latter will be called *p-adic number fields*.

Proposition 1.3.3: Compactness Of Local Fields

Let K be a local field. Then K is locally compact, and its valuation ring $\mathcal{O}$ is compact

***Proof* :**
By ref:HERE, $\mathcal{O} \cong \varprojlim \mathcal{O}/\mathfrak{p}^n$ algebraically and topologically. By ref:HERE, $\mathfrak{p}^\nu/\mathfrak{p}^{\nu+1} \cong \mathcal{O}/\mathfrak{p}$, and since $\mathcal{O}/\mathfrak{p}^n$ are finite, they are finite. As $\mathcal{O}$ is a closed subset of the compact product $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^n$, we have that the limit is compact, and hence $\mathcal{O}$ is. Next, for every $a \in K$, $a + \mathcal{O}$ is open and a compact neighborhood, so K is locally compact.

For the topologically minded, here is an interesting result: if K is a locally compact field with respect to a nondiscrete topology, it is isomorphic to euclidean $\mathbb{R}$ or $\mathbb{C}$, or to a local field with the valuation topology. Hence, we can say that we are studying locally compact fields.

Definition 1.3.4: Local Number Field

Let $K_\mathfrak{p}/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. Then $K_\mathfrak{p}$ is called a *local number field*

Notice that the extension has a sub-script $\mathfrak{p}$ attached to it. Each local number field shall be associated to a prime, as theorem 1.2.2 suggests (but we shall prove it in the proceeding sections).

Proposition 1.3.5: Units Of Local Field

Let K be a local field. Then:

$$K^* = (\pi) \times \mu_{q-1} \times U^{(1)}$$

where π is a prime element, $q = \#(\kappa(\mathfrak{p}) = \#(\mathcal{O}/\mathfrak{p})$, and $U^{(1)} = 1 + \mathfrak{p}$ is the group of principal units

***Proof* :**
For any $x \in K^*$, we have that $k = \pi^n u$ for a appropriate prime π, $n \in \mathbb{Z}$, and $u \in \mathcal{O}^*$. As $\mathcal{O}$ contains the $q-1$ roots of unity μ_{q-1} (by Hensel's lemma, $x^{q-1}-1$ splits in $\mathcal{O}$). The homomorphism $\mathcal{O}^* \to \kappa^*$ mapping $u \mapsto u \mod \mathfrak{p}$ has $U^{(1)}$ as a kernel and the group of unity maps bijectively onto κ^*, hence $\mathcal{O}^* = \mu_{q-1} \times U^{(1)}$, as we sought to show.

Proposition 1.3.6: Log For p-adic Number Fields

Let K be a p-adic number field. Then there exists a unique continuous homomorphism:

$$\log : K^* \to K$$

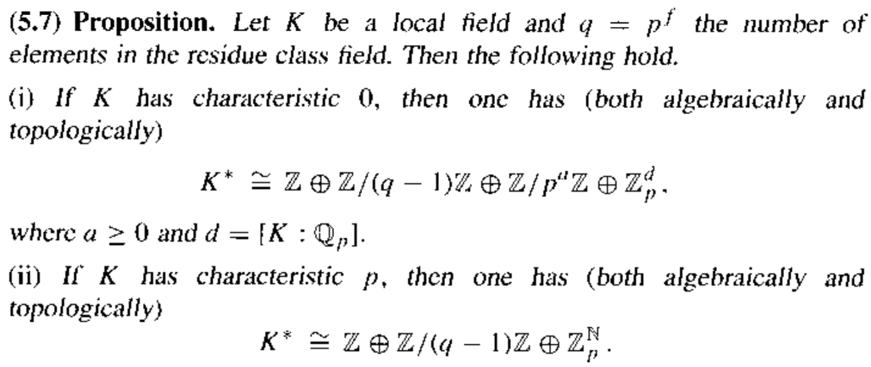
where $\log p = 0$ and on principal ideals $(1+x) \in U^{(1)}$ is given by:

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

Proof **:**
Neukirch p.137 if you want the proof.

(there is one more lemma on p.137 of Neukrich that gives maps $\mathfrak{p}^n \rightleftarrows \exp_{\log} U^{(n)}$)

(using these results, we get a more specific decomposition of the group)



(5.7) Proposition. *Let K be a local field and $q = p^f$ the number of elements in the residue class field. Then the following hold.*

(i) *If K has characteristic 0, then one has (both algebraically and topologically)*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

where $a \geq 0$ and $d = [K : \mathbb{Q}_p]$.

(ii) *If K has characteristic p, then one has (both algebraically and topologically)*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$

(Neukrich at this point takes awhile to develop Henselian fields, as it turns out that most of the theory only requires Hensel's lemma, which applies to fields that are more general than Complete fields and local fields. I will avoid this, it is not necessary at this stage. So, wherever he talks about Henselian fields, just use local fields

If R is a DVR, it's henselization is $\widehat{R} \cap K^{\text{sep}}$, where $K = \text{Frac}(R)$. The idea is that Cauchy sequences that converge (in the completion) to the root of a polynomial are *required* to converge, but not every Cauchy sequence needs to converge!)

1.4 Hensel's Lemma

Recall that given a polynomial $f(x) \in \mathbb{Z}[x]$, it is possible that $f(x)$ has a root a root mod each prime, but f need not have a root. For example recall that $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible (use the fact that $\sqrt{2}$ is irrational in the proof). However, this polynomial is reducible mod every prime (see [ChwNAc, chapter 11.3]). When working over local fields, roots can be lifted! In particular, Hensel's lemma give a way of lifting roots. Let K be a complete field with respect to to some nonarchemedian absolute value $|-|$, and hence has a corresponding valuation. Let $\mathcal{O} \subseteq K$ be the valuation ring with corresponding unique maximal ideal $\mathfrak{p}$ and residue field $\kappa(\mathfrak{p}) = \mathcal{O}/\mathfrak{p}$. For example, $K = \mathbb{Q}_p$ and $\mathcal{O} = \mathbb{Z}_p$ with ideal (p) and $\kappa((p)) = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. Define a *primitive polynomial* $f(x) \in \mathcal{O}[x]$ if

$$f(x) \not\equiv 0 \mod \mathfrak{p}$$

which similarly means

$$|f| = \max\{|a_0|, ..., |a_n|\} = 1$$

Note that it need not be monic. Then factorization mod $\mathfrak{p}$ gives factorization when lifted!

Theorem 1.4.1: Hensel's Lemma

Let K be a complete field with respect to a nonarchemedian absolute value $|-|$, and let $\mathcal{O}$ be the corresponding discrete valuation ring. Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial. Then if it admits a factorization modulo $\mathfrak{p}$:

$$f(x) \equiv \overline{g}(x)\overline{h}(x) \mod \mathfrak{p}$$

into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$, then $f(x)$ admits a factorization

$$f(x) = g(x)h(x)$$

for polynomials $g, h \in \mathcal{O}[x]$ such that the degree of at least g matches, and:

$$g(x) \equiv \overline{g}(x) \mod \mathfrak{p} \qquad \text{and} \qquad h(x) \equiv \overline{h}(x) \mod \mathfrak{p}$$

***Proof* :**

We shall inductively construct g, h. First, let $d = \deg(f)$, $\deg(\overline{g}) = m$, and hence $\deg(\overline{h}) \leq d - m$. Let $g_0, h_0 \in \mathcal{O}[x]$ be polynomial representing $\overline{g}$ and $\overline{h}$ respectively where $\deg(g_0) = \deg(\overline{g})$ and $\deg(h_0) \leq d - m$. As $(\overline{g}, \overline{h}) = 1$ are co-prime, there exits $a, b \in \mathcal{O}[x]$ such that $ag_0 + bh_0 = 1$, hence $ag_0 + bh_0 \equiv 1 \mod \mathfrak{p}$. Now, the trick is to pick among the coefficients of $f - g_0h_0, ag_0bh_0 - 1 \in \mathfrak{p}[x]$ the one with minimum value with respect to $|-|$ (convince yourself this polynomials are in $\mathfrak{p}[x]$). Call this element π.

Using this element, we shall construct g, h that will be the factorizations through the following form:

$$\begin{aligned} g &= g_0 + p_1\pi + p_2\pi^2 + \cdots \\ h &= h_0 + q_1\pi + q_2\pi^2 + \cdots \end{aligned}$$

where $p_i, q_i \in \mathcal{O}[x]$ are polynomials of degree $< m$ and $\leq d - m$ respectively. These are indeed elements of $\mathcal{O}[x]$ when constructed as the limit:

$$\begin{aligned} g_{n-1} &= g_0 + p_1\pi + p_2\pi^2 + \cdots + p_{n-1}\pi^{n-1} \\ h_{n-1} &= h_0 + q_1\pi + q_2\pi^2 + \cdots + p_{n-1}\pi^{n-1} \end{aligned}$$

where

$$f \equiv g_{n-1}h_{n-1} \mod \pi^n \tag{1.1}$$

as the term will always group up to form a polynomial of appropriate degree. What's to do is to show that we can find polynomials g_{n-1}, h_{n-1} that satisfy equation (1.1) which by a small generalization of theorem 1.1.2 shall give the desired polynomial.

For $n = 1$, the solution is immediately given by choice of π. Let us now inductively assume that it works for some $n - 1$, and consider:

$$g_n = g_{n-1} + p_n\pi^n \qquad h_n = h_{n-1} + q_n\pi^n$$

Then:

$$f - g_{n-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \mod \pi^{n+1}$$

As we are in an integral domain, inverses are well-defined and hence we may divide by π^n. This gives:

$$g_{n-1}q_n + h_{n-1}p_n \equiv (g_0q_n + h_0p_n) \equiv \pi^{-n}(f - g_{n-1}h_{n-1}) \equiv f_n \mod \pi$$

where $f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[x]$. Next, since $g_0a + h_0b \equiv 1 \mod \pi$, we have:

$$g_0af_n + h_0bf_n \equiv f_n \mod \pi$$

If we can take $q_n = af_n$ and $p_n = bf_n$, we'd be done, however the degree's may be too big. Hence, write:

$$b(x)f_n(x) = q(x)g_0(x) + p_n(x)$$

where $\deg(p_n) < \deg(g_0) = m$. Since $g_0 \equiv \overline{g} \mod \mathfrak{p}$ and $\deg(g_0) = \deg(\overline{g})$, the highest coefficient of g_0 i a unit, and so $q(z) \in \mathcal{O}[x]$. Thus, we get:

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi$$

Finally, omitting the coefficient divisible by π in the polynomial af_nh_0q, we get q_n such that $g_0q_n + h_0p_n \equiv f_n \mod \pi$, where $\deg(f_n) \leq d$, $\deg(g_0) = m$, and $\deg(h_0p_n) < (d - m) + m = d$, meaning it has degree less than or to $d - m$, giving the induction step, and completing the proof.

Example 1.3: $\mathbb{Q}_p$ contains roots of unity

Consider $x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Over $\mathbb{F}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$, this polynomials splits completely into linear factors. Hence through repeated use of Hensel's lemma it splits in $\mathbb{Z}_p$. As such, the field $\mathbb{Q}_p$ of p-adic number contains the $(p - 1)$ roots of unity!

These along with 0 can even from a system of representatives for the residue class field (the usual representatives are $0, 1, ..., p - 1$).

Corollary 1.4.2: Hensel's Lemma 2

Let R be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field $k = R/\mathfrak{p}$. Then if f is a monic polynomial whose reduction to $k[x]$ has a root $\overline{a} \in k$, then $\overline{a}$ can be lifted to a root of f in R.

Proof **:**
If $\overline{a} \in k = R/\mathfrak{p}$ is a root, then by Hensel's lemma it lifts to a root in R.

Corollary 1.4.3: Hensel's Lemma Giving Newtons Method

Let R be a complete DVR, $f \in R[x]$, and $a_0 \in R$ satisfies:

$$|f(a_0)| < |f'(a_0)|^2$$

implying $f'(a_0)$ divides $f(a_0)$. For any $n \geq 0$ define

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

Then the sequence (a_n) is well-defined and converges to a unique root $a \in R$ for which

$$|a - a_0| \leq \epsilon := \frac{|f(a_0)|}{|f'(a_0)|^2}$$

Furthermore, $|f(a_n)| < \epsilon^{2n}|f'(a_0)|^2$ for all $n \geq 0$

Proof **:**
look at Newton's method.

Corollary 1.4.4: Hensel-Kürchák Lemma

Let K be a complete field with respect to a non-Archimedean valuation $|-|$. Then for every irreducible polynomial $f(x) = a_0 + \cdots a_n x^n \in K[x]$ such that $a_0 a_n \neq 0$, we have:

$$|f| = \max\{|a_0|, |a_n|\}$$

In particular, if $a_n = 1$ and $a_0 \in \mathcal{O}$, then $f \in \mathcal{O}[x]$

This is a rather powerful result, as it limits the possible irreducible polynomials over such fields!

Proof **:**
By multiplying by an appropriate element of K, assume that $f \in \mathcal{O}[x]$ and $|f| = 1$. Let a_r be the first coefficient where $|a_r| = 1$ so that:

$$f(x) \equiv x^r(a_r + a_{r+1}x + \cdots + a - nx^{n-r}) \mod \mathfrak{p}$$

Then $\max\{|a_0|, |a_n|\} < 1$, $0 < r < n$, but then the congruence contradicts Hensel's lemma, as we sought to show.

1.5 Extending Complete DVR's

With this, we return to upgrading our AKLB setup to local fields. We have that that the extension of complete DVR's is "closed". We shall next upgrade the following:

Lemma 1.5.1: Detecting Integral Elements, Complete DVR

Let A be a complete DVR with fraction field K, and L/K be a finite extension of degree n. Then $\alpha \in L$ is integral over A if and only if $N_{L/K}(\alpha) \in A$

Recall that in the case for number fields, this was *not* a sufficient condition [ChwNAc, chapter 22.1].

***Proof* :**
Let $f = \sum_i^d a_i x^i \in K[x]$ be the minimal polynomial of α. If α is integral over A, then $f \in A[x]$, meaning all it's coefficients are in A including the constant, which is equal to $N_{L/K}(\alpha)^e$ ($e = [L : K(\alpha)]$). Conversely, if $N_{L/K}(\alpha) = (-1)^n f(0)^e \in A$, then $f(0) \in A$ since $f(0) \in K$ is the roots of $x^e - (-1)^n N_{L/K}(\alpha) \in A[x]$ and A is integrally closed. Thus, the constant coefficien of f lies in A, and as it is monic, so does f, and so by corollary 1.4.4 $f \in A[x]$, showing that α is integral, completing the proof.

Theorem 1.5.2: Extension of DVR's

Assume $AKLB$ and let A be a complete DVR with maximal ideal $\mathfrak{p}$. Then B is a DVR whose maximal ideal $\mathfrak{B}$ is necessarily the unique prime ideal above $\mathfrak{p}$.

***Proof* :**
Let's first show that the number of primes lying over $\mathfrak{p}$ is 1. There is at least one $\mathfrak{B} \subseteq B$ lying over $\mathfrak{p}$ as the factorization of $\mathfrak{p}B \not\subseteq B$ is non-trivial by theorem 1.2.2. Now, for the sake of contradiction say that there were $\mathfrak{B}, \mathfrak{B}'$ lying over $\mathfrak{p}$ where $\mathfrak{B} \neq \mathfrak{B}'$. Then choose $b \in \mathfrak{B} - \mathfrak{B}'$ and consider $A[b] \subseteq B$. The ideals $\mathfrak{B} \cap A[b]$ and $\mathfrak{B}' \cap A[b]$ are distinct primes ideals of $A[b]$ containing $\mathfrak{p}A[b]$. Furthermore, both are maximal since they are nonzero and $\dim A[b] = \dim(A) = 1$ (as $A[b]$ is integral over$A$, and therefore has the same dimension). The quotient ring $A[b]/\mathfrak{p}A[b]$ thus has *at least* two maximal ideals. Now let $f \in A[x]$ be the minimal polynomial of b over K and let $\overline{f} \in (A/\mathfrak{p})[x]$ be its reduction to the residue field $A/\mathfrak{p}$. Then we have:

$$\frac{(A/\mathfrak{p})[x]}{(\overline{f})} \cong \frac{A[x]}{(\mathfrak{p}, f)} \cong \frac{A[b]}{\mathfrak{p}A[b]}$$

Hence, the ring $(A/\mathfrak{p})[x]/(\overline{f})$ also has at least two maximal ideals, implying that $\overline{f}$ is divisible by two distinct irreducible polynomials (as $(A/\mathfrak{p})[x]$ is a PID). Thus, we get that $\overline{f} = \overline{g}\overline{h}$. Finally, by Hensel's lemma, these can be lifted to a non-trivial factorization $f = gh$ for $f \in A[x]$, contradicting the irreducibility of f.

To close the argument, recall that every maximal ideal of B lies above a maximal ideal of A, but A has only one maximal ideal $\mathfrak{p}$, so B has a unique (nonzero) maximal ideal $\mathfrak{B}$. Thus B is a local Dedekind domain, hence a local PID, and not a field, which is an equivalent definition to a DVR, completing the proof.

Note that completion is necessary for this lemma to work:

Example 1.4: Failure Without Completion

Take $A = \mathbb{Z}_{(5)}$ which is a DVR with maximal ideal (5) but is not complete. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$. Then $\mathcal{O}_L = \mathbb{Z}_{(5)}[i]$, which is a PID, but is *not* a DVR, as the ideals $(1+2i)$ and $(1-2i)$ are both maximal and not equal. However, if we take $A = \mathbb{Z}_5$ and $K = \mathbb{Q}_5$ with $L = \mathbb{Q}_5(i) = \mathbb{Q}_5$, and $B = \mathbb{Z}_5[i] = \mathbb{Z}_5 = \mathbb{A}$, it is a DVR, since x^2+1 has roots in $\mathbb{F}_5$ and we can lift roots in $\mathbb{Z}_5$ via Hensel's lemma.

Notice that the factorization $5 = (1+2i)(1-2i)$ in $\mathbb{Z}_{(5)}[i]$ when replaced with $\mathbb{Z}_5$ we will get that (5) is the product of the maximal ideal and a unit. In fact, not matter what prime we localize at we get this result!

This immediately gives the following

Corollary 1.5.3: The Fundamental Identity For Local Fields

Let K be a local field and L/K a finite extension. Let $\mathfrak{B}$ be the maximal prime of $\mathcal{O}_L$ and $\mathfrak{p}$ the maximal prime of K. Then:

$$[L : K] = n = ef$$

where e and f are the ramification index and inertia degree respectfully.

***Proof* :**

As there is only one prime lying above, the result follow from the global fundamental identity.

Finally, we show that completion is preserved too. First, recall that we may define a norm on a vector-space over k $\|-\| : V \to \mathbb{R}_{\geq 0}$, and that if k is complete then all norms on a finite dimensional k-vector-space are equivalent, including the maximal and euclidean norm. Now:

Theorem 1.5.4: Extension of DVR's, Completion

Let A be a complete DVR with maximal ideal $\mathfrak{p}$, $K = \text{Frac}(A)$, and $\nu_\mathfrak{p}$ a discrete valuation which gives the absolute value $|x|_\mathfrak{p} := c^{\nu_\mathfrak{p}(x)}$ where $0 < c < 1$. Let L/K be a finite extension of degree n. Then the following are equivalent:

1. There is a unique absolute value $|x| := |N_{L/K}(x)|_\mathfrak{p}^{1/n}$ on L that extends $|-|_\mathfrak{p}$
2. The field L is complete with respect to $|-|$, and it's valuation ring $\{x \in L \ : \ |x| \leq 1\}$ is equal to the integral closure B of A in L

Furthermore, if L/K is separable, then B is a complete DVR whose maximal ideal $\mathfrak{B}$ induces:

$$|x| = |x|_\mathfrak{B} := c^{\frac{1}{e_\mathfrak{B}}\nu_\mathfrak{B}(x)}$$

where $e_\mathfrak{B}$ is the ramification index of $\mathfrak{B}$ (recall that $\mathfrak{p}B = \mathfrak{B}^{e_\mathfrak{B}}$).

Proof **:**
Let's first show that $|-|$ is an absolute value. Certainly $|x| = 0$ if and only if $x = 0$, and $|-|$ is multiplicative as the norm is. To show the triangle inequality, it suffices to show that :

$$|x| \leq 1 \Rightarrow |x+1| \leq |x| + 1$$

since in general we always have:

$$|y+z| = |z||y/z+1| \qquad |y| + |z| = |z|(|y/z| + 1)$$

Without loss of generality, we may assume that $|y| \leq |z|$. THen we can even show that $|x| \leq 1 \Rightarrow |x+1| \leq 1$ via;

$$\begin{aligned} &|x| \leq 1 \\ &\Leftrightarrow |N_{L/K}(x)|_{\mathfrak{p}} \leq 1 \\ &\Leftrightarrow N_{L/K}(x) \in A \\ &\Leftrightarrow x \in B \\ &\Leftrightarrow x + 1 \in B \\ &\Leftrightarrow |x+1| \leq 1 \end{aligned}$$

The first bi-conditional is from the definition of $|-|$, the second from the definition of $|-|_{\mathfrak{p}}$, the third from lemma 1.5.1, the fourth is since it is a ring, and the fith is from the first three by replacing x with $x+1$. This

Now, let $x \in K$. Then:

$$|x| = |N_{L/K}(x)|_{\mathfrak{p}}^{1/n} = |x^n|_{\mathfrak{p}}^{1/n} = |x|_{\mathfrak{p}}$$

showing it is indeed an extension. If $|-|_{\mathfrak{p}}$ is non-trivial, then $|x|_{\mathfrak{p}} \neq 1$ for some $x \in K^*$, and if $|x|^a = |x|_{\mathfrak{p}} = |x|$, then $a = 1$, showing that $|-|$ is the unique absolute value in its equivalence class extending $|-|_{\mathfrak{p}}$. As every norm on L induces the same topology, $|-|$ is the only absolute value on L that extends $|-|_{\mathfrak{p}}$.

This covers the equivalences, so now assume L/K is separable. Then B is a DVR by theorem 1.5.2. It is complete since it the valuation ring of L. Next, let $\mathfrak{B}$ be the unique maximal ideal of $\mathfrak{B}$. The valuation $\nu_{\mathfrak{B}}$ extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{B}}$, and so

$$\nu_{\mathfrak{B}}(x) = e_{\mathfrak{B}}\nu_{\mathfrak{p}}(x)$$

Then as $0 < c^{1/e_{\mathfrak{B}}} < 1$, we have the absolute value on L induced by $\nu_{\mathfrak{B}}$ to be:

$$|x|_{\mathfrak{B}} := (c^{1/e_{\mathfrak{B}}})^{\nu_{\mathfrak{B}}(x)}$$

This is indeed equal to $|-|$, for it extends $|-|_{\mathfrak{p}}$ which is know has a unique extension. Computing:

$$y|x|_{\mathfrak{B}} = c^{\frac{1}{e_{\mathfrak{B}}}\nu_{\mathfrak{B}}(x)} = c^{\frac{1}{e_{\mathfrak{B}}}\nu_{\mathfrak{B}}(x)} = c^{\nu_{\mathfrak{p}}(x)} = |x|_{\mathfrak{p}}$$

completing the proof.

By transitivity of the norm in towers, we can uniquely extend the absolute value on the fraction field K of a complete DVR to an algebraic closure $\overline{K}$.

Corollary 1.5.5: DVR Completion And Number Rings

Assume $AKLB$ and let A be a complete DVR with maximal ideal $\mathfrak{p}$. Let $\mathfrak{B}/\mathfrak{p}$. Then

$$\nu_{\mathfrak{B}}(x) = \frac{1}{f_{\mathfrak{B}}}\nu_{\mathfrak{p}}(N_{L/K}(x))$$

for all $x \in L$

***Proof* :**

$$\nu_{\mathfrak{p}}(N_{L/K}(x)) = \nu_{\mathfrak{p}}(N_{L/K}((x))) = \nu_{\mathfrak{p}}(N_{L/K}(\mathfrak{B}^{\nu_{\mathfrak{B}}(x)})) = \nu_{\mathfrak{p}}(\mathfrak{p}^{f_{\mathfrak{B}}\nu_{\mathfrak{B}}(x)}) = f_{\mathfrak{B}}\nu_{\mathfrak{B}}(x)$$

1.6 Dedekind-Kummer for local rings

Recall the Dedekind-Kummer Theorem ([ChwNAc, chapter 22.4]) where a prime $\mathfrak{B}/\mathfrak{p}$ factors like the minimal polynomial of the finite separable extension L/K (i.e. $AKLB$) if the ring of integers of L is monogenic or the prime doesn't contain the conductor. In the case where the ring of integers of K is a DVR and the residue of the extension is finite, we get that B is always monogenic. This require Nakayama's lemma which we remind the reader of:

Lemma 1.6.1: Nakayama's Lemma

Let A be a local rign with maximal ideal $\mathfrak{p}$ and let M b e a finitely generated A-module. If the image of $x_1, ..., x_n \in M$ generate $M/\mathfrak{p}M$ as an $(A/\mathfrak{p})$-vector space, then $x_1, ..., x_n$ generate M as an A-module.

***Proof* :**

see [ChwNAc, section 20.5.5]

This gives a local version of the Dedekind-Kummer theorem that doesn't even need that A, B be Dedekind domain

Corollary 1.6.2: Local Ring Maximal Ideal Extension

Let A be a local Noetherian ring with maximal ideal $\mathfrak{p}$, $g \in A[x]$ be a polynomial with quotient $\overline{g} \in (A/\mathfrak{p})[x]$, and let α be the image of x in the ring $B := A[x]/(g(x))$. Then the maximal ideals of B are $(\mathfrak{p}, g_i(\alpha))$ where $g_1, ..., g_m \in A[x]$ are lifts of the distinct irreducible polynomials $\overline{g}_i \in (A/\mathfrak{p}))[x]$ that divide $\overline{g}$.

Nakayama will give the correspondence, and the fact that A has only a single maximal ideal will force that the extension have only so many possible maximal ideals:

***Proof* :**
By Nakayama's lemma, the quotient map $B \to B/\mathfrak{p}B$ gives a one-to-one correspondence between the maximal ideals of B and the maximal ideals of $B/\mathfrak{p}B$, and hence:

$$B/\mathfrak{p}B \cong A[x]/(\mathfrak{p}, g(x)) \cong (A/\mathfrak{p})[x]/(\overline{g}(x))$$

Now, each maximal ideal of the right hand side is the quotient of an irreducible divisor of $\overline{g}$ (you can use the Chinese remainder theorem if you're unconvinced) and hence as $(A/\mathfrak{p})[x]$ is a PID it is one of the $\overline{g_i}$, as we sought to show.

Theorem 1.6.3: Local Dedekind-Kummer Theorem

Take $AKLB$, where A, B are DVR's, and let $\kappa = A/\mathfrak{p}, \lambda = B/\mathfrak{B}$ be the residue fields given a prime $\mathfrak{B}$ over $\mathfrak{p}$. Then if λ/κ is separable,

$$B = A[\alpha]$$

for appropriate $\alpha \in B$. If L/K is unramified, this then holds for every lift α for any generator $\overline{\alpha}$ for $\lambda = \kappa(\alpha)$.

Hence, by [ChwNAc, Corollary 22.4.8], every ring of integers extension $\mathcal{O}_L/\mathcal{O}_K$ is monogenic, and the [global] Dedekind-Kummer Theorem applies.

***Proof* :**
Let $\mathfrak{p}B = \mathfrak{B}^e$ be the factorization of $\mathfrak{B}/\mathfrak{p}$ and let $f = [\lambda : \kappa$ be the inertia degree so that $ef = n := [L : K]$. As the extension λ/κ is separable, there exists a primitive element

$$\lambda = \kappa(\overline{\alpha}_0)$$

for some $\overline{\alpha}_0 \in \lambda$ whose minimal polynomial $\overline{g}$ is separable of degree f. Let $g \in A[x]$ be the monic lift of $\overline{g}$ and let α_0 be any lift of $\overline{\alpha}_0$ to B. If $\nu_{\mathfrak{B}}(g(\alpha_0)) = 1$, let $\alpha := \alpha_0$. Otherwise, let π_+0 be any uniformizer for B and let $\alpha := \alpha_0 + \pi_0 \in B$. Then $\alpha \equiv \alpha_0 \mod \mathfrak{B}$. Decomposing

$$g(x + \pi_0) = g(x) + \pi_0 g'(x) + \pi_0^2 h(x)$$

for appropriate $h \in A[x]$, we get:

$$\nu_{\mathfrak{B}}(g(\alpha)) = \nu_{\mathfrak{B}}(g(\alpha_0 + \pi_0)) = \nu_F B(g(x + \pi_0) = g(x) + \pi_0 g'(x) + \pi_0^2 h(x)) = 1$$

and hence $\pi := g(\alpha)$ is the uniformizer of B.

Now, we claim that $B = A[\alpha]$. This is the same as $1, \alpha, ..., \alpha^{n-1}$ generates B as an A-module. By Nakayama's lemma, this is equivalent to asking if $1, \alpha, ..., \alpha^{n-1}$ span $B/\mathfrak{p}B$ as a κ-vector space. As $\mathfrak{p} = \mathfrak{B}^e$, $\mathfrak{p}B = (\pi^e)$. This means we can represent each element of $B/\mathfrak{p}B$ as cosets:

$$b + \mathfrak{p}B = b_0 + b_1\pi + b_2\pi + \cdots + b_{e-1}\pi^{e-1} + \mathfrak{p}B$$

where $b_0, ..., b_{e-1}$ are given up to equivalence modulo πB. Now the field theory $1, \overline{\alpha}, ..., \overline{\alpha}^{f-1}$ forms a basis for $B/\pi B = B/\mathfrak{B}$ as a κ-vector space, so we can write this as:

$$\begin{aligned}b + \mathfrak{p}B = (a_0 + a_1\alpha + \cdots + a_{f-1}\alpha^{f-1}) \\ + (a_f + a_{f+1}\alpha + \cdots + a_{2f-1}\alpha^{f-1})g(\alpha) \\ + \cdots \\ + (a_{ef-f+1} + a_{ef-f+2}\alpha + \cdots + a_{ef-1}\alpha^{f-1})g(\alpha)^{e-1} + \mathfrak{p}B\end{aligned}$$

As $\deg g = f$ and $n = ef$, this expresses $b + \mathfrak{p}B$ in the form $b' + \mathfrak{p}B$ with b' in the A-span of $1, ..., \alpha^{n-1}$. Thus:

$$B = A[\alpha]$$

Finally, if L/K is unramified ,then λ/κ is separable, and $e = 1$, $f = n$, and so there there is no need to check if $g(\alpha)$ is a uniformizer which immediately gives $\alpha = \alpha_0$, as we sought to show.

1.7 Ramification in Local Fields

Definition 1.7.1: Ramification Index And Inertia Degree Of Local Fields

Let K be a local field and L/K a finite extension. Let ν be the discrete valuation associated to K and w be extension of ν given by ref:HERE. Then as $\nu(K^*) \subseteq w(L^*)$ define the *ramification index* of L with respect to K to be:

$$e(L : K) = [w(L^*) : \nu(K^*)]$$

and the *inertia degree* of L with respect to K to be

$$f(L : K) = [\lambda : \kappa]$$

where λ, κ are the residue fields of L and K respectively.

Notice that $w = \frac{1}{n}\nu \circ N_{L/K}$, and hence is discrete. If $\mathfrak{o}, \mathfrak{p}, \pi$ and $\mathcal{O}, \mathfrak{B}, \Pi$ are the valuation-ring/maximal-ideal/prime-element of K and L respectively, then:

$$e(L : K) = [w(\Pi)\mathbb{Z} : \nu(\pi)\mathbb{Z}]$$

Hence $\nu(\pi) = ew(\Pi)$ which gives:

$$\pi = u\Pi^e$$

for some unit $u \in \mathcal{O}^*$, which mirrors the result for the definition of ramification index in the case of global fields.

1.7.1 Unramified Extensions

With the fundamental identity property re-defined, let us upgrade the definition of unramified extensions from [ChwNAc, chapter 22.4]:

Definition 1.7.2: Unramified Extension for local field

Let A be a complete DVR with finite residue field, K it's field of fractions, and L a finite extension. Then if:

$$[L : K] = [\kappa(\mathfrak{B}) : \kappa(\mathfrak{p})] = f$$

Then L/K is said to be an *unramified extension.*

Hence, when L/K is finite and unramified, the degree n of L/K has the same degree as the finite separable extension λ/κ

$$[L : K] = [\lambda : \kappa]$$

We may thus ask what is the relation of L/K and λ/κ. In particular, if we fix K with residue field κ, what is the relationship between the finite unramified extensions L/K of degree n and the finite separable extensions λ/κ of degree n. We already know that each L/K uniquely determined a corresponding λ/κ, but is the converse true too? In fact, is is almost as nice as it gets:

Theorem 1.7.3: Unramified Extension And Residue Field Category Equivalence

Let A be a complete DVR with $K = \text{Frac}(A)$ its residue field. Then the category $\mathcal{C}_K^{nr}$ and $\mathcal{C}_\kappa^{\text{sep}}$ are equivalent; the functor $\mathcal{F} : \mathcal{C}_K^{nr} \to \mathcal{C}_\kappa^{\text{sep}}$ sends each unramified extension L/K to its residue field λ, and each K-algebra homomorphism $\varphi : L_1 \to L_2$ to the κ-algebra homomorphism $\overline{\varphi} : \lambda_1 \to \lambda_2$ given by $\overline{\varphi}(\overline{\alpha}) := \overline{\varphi(\alpha)}$ where α is any lift of $\overline{\alpha} \in \lambda_1 = B_1/\mathfrak{B}_1$ to B_1 and $\overline{\varphi}$ is the reduction of $\varphi(\alpha) \in B_2$ to $\lambda_2 := B_2/\mathfrak{B}_2$.

This means that $\mathcal{F}$ gives a bijection between the isomorphism classes in $\mathcal{C}_K^{nr}$, and $\mathcal{C}_\kappa^{\text{sep}}$ and if L_1, L_2 have residue fields λ_1, λ_2, then $\mathcal{F}$ induces a bijection of finite sets:

$$\text{Hom}_K(L_1, L_2) \xrightarrow{\sim} \text{Hom}_\kappa(\lambda_1, \lambda_2)$$

The most interesting part of the proof is $\text{Hom}_K(L_1, L_2) \xrightarrow{\sim} \text{Hom}_\kappa(\lambda_1, \lambda_2)$, which will ultimately come down to Hensel's lemma after all the appropriate build-up.

Proof **:**
Let us start with showing that $\mathcal{F}$ is well-defined. The object certainly map to the object, so we need to show that the morphism map is independent of lifts. Let $\varphi : L_1 \to L_2$ be a K-algebra homomorphism, and for $\overline{\alpha} \in \lambda_1$, let α, α' be two lifts to B_1. Then $\alpha - \alpha' \in \mathfrak{B}_1$, implying $\varphi(\alpha - \alpha') \in \varphi(FB_1) \overset{!}{=} \varphi(B_1) \cap \mathfrak{B}_2 \subseteq \mathfrak{B}_2$, and hence $\overline{\varphi(\alpha)} = \overline{\varphi(\alpha')}$, showing it is well-defined. The $\overset{!}{=}$ equality comes from φ restricts to the ring homomorphism $B_1 \to B_2$ and $B_2/\varphi(B_1)$ is a finite extension of DVRs in which $\mathfrak{B}_2$ lies over the prime $\varphi(\mathfrak{B}_1)$ of $\varphi(B_1)$. Checking that the identity is set to the identity and composition is well-defined now follows quickly.

Let us now show that $\mathcal{F}$ gives an equivalence of categories. Recall from [ChwNAc, Part 8] that this means that:

1. $\mathcal{F}$ is essentially surjective: each separable extension λ/κ is isomorphic to the residue field of some unramified L/K
2. $\mathcal{F}$ is full and faithful, i.e. the hom-map is a bijection.

Starting with essential surjectivity, given a finite separable extension λ/κ, we may apply the primitive element theorem and get:

$$\lambda \cong k(\overline{\alpha}) \cong \frac{\kappa[x]}{(\overline{g}(x)}$$

For appropriate $\overline{\alpha} \in \lambda$ whose minimal polynomial $\overline{g}$ is necessarily monic, irreducible, separable, and of degree $n := [\lambda : \kappa]$. Take any monic lift $g \in A[x]$. Then g is also irreducible, separable, and of degree n¿ Now let :

$$L := \frac{K[x]}{(g(x))} = K(\alpha)$$

Then L/K is a finite separable extensions. By corollary 1.6.2 $(\mathfrak{p}, g(\alpha))$ is the unique maximal ideal of $A[\alpha]$, and :

$$B/\mathfrak{B} \cong \frac{A[\alpha]}{(\mathfrak{p}, g(\alpha))} \cong \frac{A[x]}{(\mathfrak{p}, g(x))} \cong \frac{(A/\mathfrak{p})[x]}{(\overline{g}(x))} \cong \lambda$$

and hence:

$$[L : K] = \deg g = [\lambda : \kappa] = n \ [= f]$$

showing that L/K is unramified, namely by the fundamental identify the ramification index of $\mathfrak{B}$ is necessarily 1.

Next, to show that $\mathcal{F}$ is full and faithful, let us start with the induced maps:

$$\mathrm{Hom}_K(L_1, L_2) \xrightarrow{\sim} \mathrm{Hom}_A(B_1, B_2) \to \mathrm{Hom}_\kappa(\lambda_1, \lambda_2)$$

The first map was shown in [ChwNAc, Chapter 22.1]. It must be shown that the same applies for the second map.

First, notice that:

$$\mathrm{Hom}_A(B_1, B_2) = \mathrm{Hom}_A\left(\frac{A[x]}{(g(x))}, B_2\right) = \mathrm{Hom}_A(A(\alpha), B_2)$$

which comes from B_1 always being a monogenic extension of A (Theorem 1.6.3) and that each A-module homomorphism is uniquely determined by the image of x in B_2. This gives a bijection between $\mathrm{Hom}_A(B_1, B_2)$ and the roots of g in B_2. Now, with the right choice of α, we can give the map. By the primitive root theorem, $\lambda_1 = \kappa(\overline{\alpha})$. Lift $\overline{\alpha}$ to $\alpha \in B_1$. Then $L_1 = K(\alpha)$ since $[L_1 : K] = [\lambda_1 : \kappa]$, and these two quantities equal to the degree of the minimal polynomial of $\overline{g}$ of $\overline{\alpha}$ which cannot be less han the degree of the minimal polynomial g of α (both are monic, so no issues will come from characteristics). THen we saw in theorem 1.6.3 that $B)_1 = A[\alpha]$. Now, consider:

$$\mathrm{Hom}_\kappa(\lambda_1, \lambda_2) = \mathrm{Hom}_\kappa\left(\frac{\kappa[x]}{(\overline{g}(x))}, \lambda_2\right) = \mathrm{Hom}_\kappa(\kappa(\overline{\alpha}), \lambda_2)$$

where the equality again comes from the uniquely determined image of x in λ_2, and there is a bijection between $\mathrm{Hom}_\kappa(\lambda_1, \lambda_2)$ and the roots of $\overline{g}$ in λ_2. Now, $\overline{g}$ is separable, so by Hensel's lemma every root of $\overline{g}$ in $\lambda_2 = B_2/\mathfrak{B}_2$ lifts to unique roots of g in B_2. But then the map is a bijection, as we sought to show.

Note that for the bijection it was only necessary that L_1/K be unramified, so at least the bijection holds if L_2/K is unramified. Furthermore, using this bijection we can compute the galois group of automorphisms of a field by looking at the automorphisms of the residue field.

Corollary 1.7.4: Characterizing Unramified Extensions through residue field

Assume $AKLB$ where A is a complete DVR with residue field κ. Then L/K is unramified if and only if $B = A[\alpha]$ for some $\alpha \in L$ whose minimal polynomial has separable image in $\kappa[x]$.

***Proof* :**
The "if" was given by theorem 1.7.3. for the reverse, note that if g is the minimal polynomial, $\overline{g}$ must be irreducible, otherwise Hensel's lemma would give a lift to a non-trivial factorization of $\overline{g}$, so the residue field extension is separable and has the same degree as L/K, and hence L/K is unramified as $[L : K] = f$, completing the proof.

We shall now build-up to show that all unramified extensions where the residue field κ is finite will be isomorphic to a Cyclotomic extension. Starting with the following:

Lemma 1.7.5: Unramified Cyclotomic Extensions

Let A be a complete DVR with fraction field K and residue field κ, and let ζ_n be the primitive nth roots of unity in some algebraic closure of K with $(n, p) = 1$ where $\operatorname{char} \kappa = p$. Then $K(\zeta_n)/K$ is unramified

***Proof* :**
By the relation's of the root of $f(x) = x^n - 1$, The field $K(\zeta_n)$ is splitting filed of this polynomial over K, The image $\overline{f}$ is separable when $\nmid n$ as $\gcd(\overline{f}, \overline{f}') \neq 1$ if and only if $\overline{f}' = nx^{n-1}$ is zero, or equivalently when $p \mid n$. When $\overline{f}$ is separable, so are all of its divisors, iclusing the reduction of the minimal polynomial of ζ_n (which is a factor of f after dividing by $x - 1$), and it must be irreducible since otherwise we would contain a non-trivial factorization by Hensel's lemma. THus ,the residue field $\kappa(\zeta_n)$ is a separable extension of κ, and so by corollary 1.7.4 $K(\zeta_n)/K$ is unramified, as we sought to show.

Adding on the extra condition that the residue field is finite (which is always the case for local fields), we get to characterize unramified extnesions:

Proposition 1.7.6: Characterizing Unramified Extension Of Local Fields

Let A be a complete DVR with fraction field K and finite residue field $\mathbb{F}_q$. Let L/K be a degree n extension. Then L/K is unramified iff

$$L \cong K(\zeta_{q^n - 1})$$

Furthermore, $A[\zeta_{q^n-1}]$ is the integral closure of A in L, and L/K is a galois extension with

$$\operatorname{Gal}_K(L) \cong \mathbb{Z}/n\mathbb{Z}$$

***Proof* :**
The above corollary showed the "only if" direction, so let us show the "if direction" by assuming L/K is unramified. Then $[\lambda : \kappa] = [L : K] = n$ where by the finiteness of the residue field $\lambda = \mathbb{F}_{q^n}$. By field theory, $\mathbb{F}_{q^n}$ has the multiplicative group of order $q^n - 1$ generated by some $\overline{\alpha}$, say $\overline{g}$ is its minimal polynomial. Then $\overline{g}$ divides $x^{q^n-1} - 1$, and sine $\overline{g}$ is irreducible, $(\overline{g})$ is coprime to $(x^{q^n-1} - 1)/\overline{g}$. By Hensel's lemma, we can lift this all to $A[\zeta_{q^n-1}]$ and show that g divides $x^{q^n-1} - 1 \in A[x]$, and again by Hensel's lemma we can lift $\overline{\alpha}$ to a root α of g which shows that α is a root of $x^{q^n-1} - 1$. Thus, it is a primitive $(q^n - 1)$-root of unity as the reduction is, which implies that

$$L \cong K(\zeta_{q^n-1})$$

Finally, by theorem 1.6.3 we have $B \cong A[\zeta_{q^n} - 1]$ and L is the splitting field of $x^{q^n-1} - 1$ (we can lift the factorization of this polynomial from $\mathbb{F}_{q^n}$ to L via Hensel's lemma). Hence L/K is galois, and the bijection between the $(q^n - 1)$-roots of unity in L and $\mathbb{F}_{q^n}$ induces $\mathrm{Gal}_K(L) \cong \mathbb{Z}/n\mathbb{Z}$, as we sought to show.

The fact that an extension is unramified if and only if $L \cong K(\zeta_{q^n-1})$ implies that we can also deduce when a cyclic extension *is* ramified:

Corollary 1.7.7: Ramification Of Cyclic Extension

Let A be a complete DVR with field of fraction K and finite residue field of characteristic p. Suppose that K does not contain a primitive pth root of unity. Then the extension $K(\zeta_m)/K$ is ramified if and only if $p \mid m$.

***Proof* :**
If $p \nmid m$, by lemma 1.7.5 $K(\zeta_m)/K$ is unramified. if $p \mid m$, then $K(\zeta_m)$ must contain $K(\zeta_p)$ which by proposition 1.7.6 is unramified if and only if $K(\zeta_p) \cong K(\zeta_{p^n-1})$ with $n = [K(\zeta_p) : K]$, which occurs if $p \mid p^n - 1$ (since $\zeta_p \notin K$ by assumption), which certainly is not the case. Hence, $K(\zeta_p)$ is ramified, implying $K(\zeta_m)$ is ramified, as we sought to show.

Now with a choice of complete DVR, we can fully understand the unramified extensions

Example 1.5: Local Number Fields
Let $A = \mathbb{Z}_p$ so that $K = \mathbb{Q}_p$ and $\kappa = \mathbb{F}_p$. Then for each n, the galois field $\mathbb{F}_{p^n}$ is the unique extension of degree n. Thus, by the above results, there is a unique unramified extension of degree n, $L/\mathbb{Q}_p$. This can be explicitly constructed by adjoining a primitive root of unity ζ_{p^n-1} to $\mathbb{Q}_p$.

Maximal Unramified Extension

Let us build-up to the notion of maximal unramified extension, which is an important object for the Artin map. First, the "3rd isomorphism theorem" property applies for unramified extensions

Proposition 1.7.8: Unramified Square

Let L/K and M/K be two extensions, with $\mathfrak{p} \subseteq K$, $\mathfrak{B} \subseteq L$, $\mathfrak{B}' \subseteq M$, $\mathfrak{B} \cap K = \mathfrak{B}' \cap K = \mathfrak{p}$. Then if L/K is unramified for $\mathfrak{B}$ over $\mathfrak{p}$ if LM/M is unramified for $\mathfrak{B}'$ over $\mathfrak{p}$.

Visually,

$$\begin{tikzcd}
& LM & \\
L \arrow[ur] & \Nearrow & M \arrow[ul, "\text{unramified}"'] \\
& K \arrow[ul, "\text{unramified}"] \arrow[ur] &
\end{tikzcd}$$

***Proof* :**
Define:

$$\mathfrak{o}, \mathfrak{p}, \kappa' \qquad \mathcal{O}, \mathfrak{B}, \lambda, \qquad \mathfrak{o}', \mathfrak{p}', \kappa \qquad \mathcal{O}', \mathfrak{B}', \lambda'$$

to the ring of integers, prime, and residue field of K, L, M, LM respectively, and assume L/K is finite. Then λ/κ is also finite and separable, and hence generated by a primitive element $\overline{\alpha}$, $\lambda = \kappa(\overline{\alpha})$. Without loss of generality, we may have $\alpha \in \mathcal{O}$ by multiplying out the denominator, and hence there is a minimal polynomial for α, $f(x) \in \mathfrak{o}[k]$. Let $\overline{f} \in \kappa[x]$ be $\overline{f}(x) = f(x) \mod \mathfrak{p}$. By minimality, the minimal polynomial of α in λ divides $\overline{f}$, hence:

$$[\lambda : \kappa] \leq \deg(\overline{f}) = \deg(f) = [K(\alpha) : K] \leq [L : K] = [\lambda : \kappa]$$

hence $[\lambda : \kappa] \leq [K(\alpha) : K] \leq [\lambda : \kappa]$, and so $L = K(\alpha)$, which also shows that $\overline{f}$ is the minimal polynomial of $\overline{\alpha}$ over κ.

Thus, $LM = M(\alpha)$. To show this extension is unramified, let $g(x) \in \mathcal{O}'[x]$ be the minimal polynomial of α over k', and let $\overline{g}(x) \equiv g(x) \mod \mathfrak{p}' \in \kappa'[x]$. Then as a factor of $\overline{f}$, it is separable, hence irreducible over κ' (or else $g(x)$ is reducible by Hensel's lemma!). Thus we get:

$$[\lambda' : \kappa'] \leq [LM : M] = \deg(g) = \deg(\overline{g}) = [\kappa'(\overline{\alpha}) : \kappa'] \leq [\lambda' : \kappa']$$

Giving that LM/M is unramified.

Finally, if L/K is a extension of the unramified extension LM/K , then it follows that LM/L is unramified, and thus so is L/K by the degree formula, as we sought to show.

Corollary 1.7.9: Composite Of Unramified Extensions

The composite of two unramified extensions of L is again unramified

***Proof* :**
It suffices to show that if L/K, M/K, namely as L/K is unramified by proposition 1.7.8 LM/M is unramified, and hence LM/K is unramified as separability is transitive and the degrees are multiplicative.

Hence, the following is well-defined:

Definition 1.7.10: Maximally Unramified Extension (Hilbert Class Field)

Let L/K be an algebraic extensions. Then the composite of all unramified extensions M/K is called the *maximally unramified extension* of L/K.
If $\overline{K}$ is the algebraic closure of K,then K_{nr}/K is the maximal unramified extension of K.

The term K_{nr} is given by the french "non-ramifiée".

Example 1.6: Maximal Unramified Extension For Local Fields
Take $K = \mathbb{Q}_p$. Then $\mathbb{Q}_p^{nr}$ will be an finite extension with galois group:

$$\mathrm{Gal}_{\mathbb{Q}_p}(\mathbb{Q}_p^{nr}) \cong \mathrm{Gal}_{\mathbb{F}_p}(\overline{\mathbb{F}}_f) = \varprojlim_n \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$$

where the last ring is called the *profinite completion* of $\mathbb{Z}$. The field has value group $\mathbb{Z}$ (it's image under valuation) and residue field $\overline{\mathbb{F}}_p$.

Corollary 1.7.11: Root Of Unity In Maximally Unramified Extension

Let K_{nr}/K be the maximally unramified extension. Then K_{nr} contains all the roots of unity of order M not divisible by the characteristic κ

If κ is a finite field, then the extension K_{nr}/K is generated by the roots of unity.

Proof **:**
This is putting together the results we saw earlier. The polynomial $x^m - 1$ splits over $\overline{\kappa}_s$, and hence over K_{nr} by Hensel's lemma. Similarly, as the roots of unity generate $\overline{\kappa}_s/\kappa$, by Hensel's they also generate K_{nr}

This also shows then that K_{nr} is a Cyclotomic extension of K.

Proposition 1.7.12: Residue Field Of Maximally Unramified Extension

Let M/K be the maximal unramified extension of K. Then the residue class field of M is the separable closure of λ_s of κ.

Proof **:**
This follows from the equivalence of categories presented earlier.

To wrap up this section, let us now look at decomposing an extension L/K into the ramified and unramified portion, and in the case where L/K is galois to find what it is:

Theorem 1.7.13: Tower Extension And Galois Group

Assume $AKLB$ with A a complete DVR and separable residue field extension λ/κ. Let e, f be the ramification index and residue field degree, and let $\mathfrak{B}$ be the unique prime of B. Then:

1. There is a unique intermediate field extension E/K that contains every unramified extension of K in L and has degree $[E : K] = f$
2. The extension L/E is totally ramified and has degree $[L : E] = e$
3. If L/K is galois, then $\mathrm{Gal}_K(L)$ is the decomposition group of $D_{\mathfrak{B}}$. $\mathrm{Gal}_E(L)$ is the inertia subgroup of $I_{\mathfrak{B}}$, and E/K is galois with $\mathrm{Gal}_K(E) \cong D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \mathrm{Gal}_\kappa(\lambda)$

***Proof* :**

1. exercise
2. tower argument
3. Take $D_{\mathfrak{B}} \subseteq \mathrm{Gal}_K(L)$. Then as there is only one prime, the entire group must be the stabilizer, and so $D_{\mathfrak{B}} = \mathrm{Gal}_K(L)$. Take now $\mathfrak{B}_E = \mathfrak{B} \cap E$. Then recall that we get:
$$I_{\mathfrak{B}_E} = \mathrm{Gal}_E(L) \cap I_{\mathfrak{B}}$$
then these thee groups all have order e, and will then have to be equal by their proprieties. As $I_{\mathfrak{B}}$ is a normal subgroup of $D_{\mathfrak{B}}$, E/K is normal, and as it is separable it is Galois. It follows then that:
$$\mathrm{Gal}_K(E) \cong D_{\mathfrak{B}}/I_{\mathfrak{B}} \cong \mathrm{Gal}_\kappa(\lambda)$$
completing the proof.

This gives the following "simplified" tower as compared to the global case:

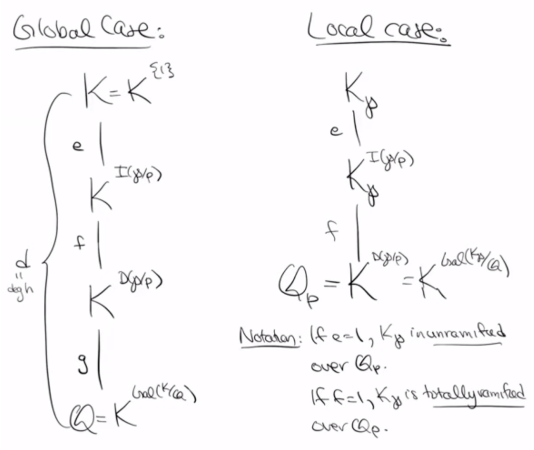

Global Case:
$K = K^{\{1\}}$
e
$K^{I(\wp/p)}$
f
$K^{D(\wp/p)}$
g
$\mathbb{Q} = K^{Gal(K/\mathbb{Q})}$
d = deg h
Local case:
$K_\wp$
e
$K_\wp^{I(\wp/p)}$
f
$\mathbb{Q}_p = K^{D(\wp/p)} = K^{Gal(K_\wp/\mathbb{Q})}$
Notation: If e=1, $K_\wp$ in unramified over $\mathbb{Q}_p$.
If f=1, $K_\wp$ is totally ramified over $\mathbb{Q}_p$.

Figure 1.1: global-local field comparison

Exercise 1.7.1

1. Assume $AKLB$, with A a complete DVR with finite residue field. Then L/K is unramified if and only if $N_{L/K}(B^*) = A^*$. Is this the case for global fields?

1.7.2 Ramified Extensions

We are now in a position where if we have any finite separable extension L/K where A is a complete DVR, then we have a tower $L/E/K$ where E/K is unramified and L/E is totally ramified. We just classified the unramified extensions (or in particular the unramified extensions of field of fractions of complete DVRs), so let us now focus on the ramified case.

Totally ramified extensions of complete DVR

Recall that a polynomial is *Eisenstein* if for some prime $\mathfrak{p} \subseteq R$, the polynomial $f(x) \in R[x]$ has coefficients $a_i \in \mathfrak{p}$ but $a_i^2 \notin \mathfrak{p}$. In the case where the ring is a DVR, this implies that a_0 is a uniformizer, as $\nu_\mathfrak{p}(a_0) = 1$. As the ring is a DVR, it is a PID and hence a UFD, meaning we can apply Gauss's lemma and get that it is irreducible over the field of fractions.

Lemma 1.7.14: DVR Extension Using Eisenstein Polynomial

Let A be a DVR and let $f \in A[x]$ be an Eisenstein polynomial. Then $B = A[\pi] = A[x]/(f)$ is a DVR with uniformizer π, where π is the image of x in $A[x]/(f)$.

***Proof* :**
Let $\mathfrak{p}$ be the maximal ideal of A. Then $f \equiv x^n \mod \mathfrak{p}$, and so by corollary 1.6.2 the ideal $\mathfrak{B}(\mathfrak{p}, x) = (\mathfrak{p}\pi)$ is the only maximal ideal of B. Let $f = \sum_i a_i x^i$. Then as f is Eisenstein, $\mathfrak{p} = (a_0)$, $\mathfrak{B} = (a_0, \pi)$ and $a_0 = -a_1\pi - f_2\pi^2 - \cdots - \pi^n \in (\pi)$, hence $\mathfrak{B} = (\pi)$. As the unique maximal ideal is principal, B is a DVR as we sought to show.

Theorem 1.7.15: Characterizing Totally Ramified Extensions

Assume $AKLB$ with A a complete DVR and π a uniformizer for B. Then the extension L/K is totally ramified if and only if $B = A[\pi]$ and the minimal polynomial of π is Eisenstein

***Proof* :**
By proposition theorem 1.6.3, $B = A[\pi]$. Let f be the minimal polynomial of π. If f is Eisenstein then by lemma 1.7.14 we have $\mathfrak{B} = \mathfrak{p}^n$, hence $\nu_\mathfrak{B}$ extends $\nu_\mathfrak{p}$ with index $e_\mathfrak{B} = n$ and L/K is totally ramified.

Conversely, if L/K is totally ramified, then $\nu_\mathfrak{B}$ extends $\nu_\mathfrak{p}$ with index n, implying

$$\nu_\mathfrak{B}(K) = n\mathbb{Z}$$

Let's first find a K-basis for L. Take the set $\{1, \pi, \pi^2, ..., \pi^{n-1}\}$ where $\pi \in K$ is a uniformizer given by $\nu_\mathfrak{p}$. This set is linearly independent as their valuations are distinct modulo $\nu_\mathfrak{B}(K)$, namely if $\sum_{i=0}^{n-1} a_0\pi^i = 0$ then it must be the case that for some nonzero a_i, a_j $\nu_{\mathfrak{B}}(a_i\pi^i) = \nu_F B(a_j\pi^j)$ which is impossible. As this also spans L, we have that

$$L = K(\pi)$$

Let $f = \sum_{i=0}^{n} a - ix^i \in A[x]$ be the minimal polynomial of π. We must show it is Eisenstein. First note that $\nu_{\mathfrak{B}}(f(\pi)) = 0$ and $\nu_{\mathfrak{B}}(a_i\pi^i) = i \mod n$ for $0 \leq i \leq n$. This is possible only if

$$\nu_{\mathfrak{B}}(a_0) = \nu_{\mathfrak{B}}(a_i\pi^0) = \nu_{\mathfrak{B}}(a_n\pi^n) = \nu_{\mathfrak{B}}(\pi^n) = n$$

and $\nu_{\mathfrak{B}}(a_i) \geq n$ for $0 \leq i < n$. But then this implies $\nu_{\mathfrak{p}}(a_0) = 1$ as $\nu_{\mathfrak{B}}$ extends $\nu_{\mathfrak{p}}$ with index n, and $\nu_{\mathfrak{p}}(a_i) \geq 1$ for $0 \leq i < n$. But then f is Eisenstein. Then lemma 1.7.14 implies $A[\pi] \subseteq B$ is a DVR, and by maximality we get $B = A[\pi]$, completing the proof.

Example 1.7: Environment Title

I'd like to add example 11.6. I want to put in the exercise fomr the HW somewhere because it is actually a really cool exercise.

Definition 1.7.16: Tamely Ramified And Wildly Ramified

Assume $AKLB$ with A a complete DVR and a separable field extension of characteristic $p \geq 0$. Then:

1. The extension L/K is *tamely ramified* if $p \nmid e_{L/K}$ (which is always true if $p = 0$)
2. The extension L/K is *wildly ramified* if $p \mid e_{L/K}$

All unramified extensions are tamely ramified. A totally ramified extension L/K is totally tamely ramified if $p \nmid e_{L/K}$ and is *totally wildly ramified* if $e_{L/K}$ is a power of p. Note that a totally ramified extension that is wildly ramified need not be totally wildly ramified.

Proposition 1.7.17: Tower of Ramified Extensions

The tower of extensions of fields of fractions of complete DVR's with separable residue field extensions of all types of ramified extensions are transitive

***Proof* :**

exercise

The same is not the case for compositum's, for example the compositum of totally ramified extensions need not be totally ramified (see example 1.7).

Theorem 1.7.18: Characterizing Totally Tamely Ramified Extensions

Assume $AKLB$ with A a complete DVR and separable residue field extension of characteristic $p \geq 0$ not dividing $n := [L : K]$. Then the extension L/K is *totally tamely ramified* if and only if $L = K(\pi_A^{1/n})$ for some uniformizer π_A of A.

The main place the tame assumption shall come is when we need to use Hensel's lemma to lift a certain solution. The equivalent of this result in the global case required that the extension be a *Kummer Extension*, which is an extension with enough roots of unity and that there are certain properties satisfied by the galois group of K.

Proof **:**

If $L = K(\pi_A^{1/n})$, then $\pi = \pi_A^{1/n}$ has minimal polynomial $x^n - \pi_A$, which his Eisenstein and so $A[\pi]$ is a DVR by lemma 1.7.14. By maximality of DVR's, $B = A[\pi]$, and by theorem 1.7.15 L/K is totally tamely ramified, as $p \nmid n$.

Conversely, assume L/K is totally tamely ramified and $\mathfrak{p}, \mathfrak{B}$ are the maximal ideals of A, B with uniformizer π_A, π_B respectfully. Then $\nu_{\mathfrak{B}}$ extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{B}} = n$ and $\nu_{\mathfrak{B}}(\pi_B^n) = n = \nu_{\mathfrak{B}}(\pi_A)$. Then $\pi_B^n = u\pi_A$ for some unit $u \in B^*$. As we are totally ramified, $f_{\mathfrak{B}} = 1$, so B and A have the *same* residue field, and so if we lift the image of $u \in B/\mathfrak{B} \cong A/\mathfrak{p}$, to a unit $u_A \in A$, and replace π_A with $u_A^{-1}\pi_A$, we can assume $u \equiv 1 \mod \mathfrak{B}$ (i.e. it is a unit also in $B/\mathfrak{B}$. From this ,define

$$g(x) = x^n - u \in B[x] \qquad \Rightarrow \qquad \overline{g}(x) = x^n - 1 \in (B/\mathfrak{B})[x]$$

Then $\overline{g}'(1) = n \neq 0$ as $p \nmid n$, showing it is a primitive polynomial and so by Hensel's lemma we can lift the root of 1 to r for $g(x)$ in B. Say $\pi = \pi_B/r$. Then π is a uniformizer for B, hence by theorem 1.7.15 $B = A[\pi]$, so $L = K(\pi)$. As $\pi^n = \pi_B^n/r = \pi_B^n/u = \pi_A$, we have:

$$L = K(\pi_A^{1/n})$$

we completed the other direction, as we sought to show.

Proposition 1.7.19: Tower of Ramification

Let K be the field of fractions of a complete DVR and L/K a totally ramified extension. Then there is a unique intermediate field E/K that is totally tamely ramified and L/E is totally wildly ramified

Proof **:**

See MIT notes p.101

Corollary 1.7.20: Tower of Ramification in Separable Case

Let K be the field of fractions of a complete DVR with separable residue field and L/K be a finite separable extension with separable residue field extensions. Then there is a unique intermediate field E such that E/K is tamely ramified and L/E is totally wildly ramified.

> ***Proof*** **:**
> See MIT notes p.101

Krasner's Lemma

This seems to deal with closeness of roots. It is pretty cool, but I will omit it for now. MIT p.102

One result of this shall be used in two chapters, so I'd like to write it down

Exercise 1.7.2

1. Let L/K be a finite extension. Then L/K is a tamely ramified extension (not necessarily totally tamely ramified) if and only if $L = K(\sqrt[m_1]{a_1}, ..., \sqrt[m_r]{a_r})$ where $\gcd(m_i, p) = 1$ (generalize theorem 1.7.18).
2. Generalize proposition 1.7.19 to tamely ramified extensions. Use this to show there exists a maximally tamely ramified extension.

1.8 Local/Global Correspondences

Let $\hat{L}$ be a local field. Then either by definition or by proposition 1.3.2 we know that $\hat{L}$ is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$ for some $p \leq \infty$ or some q. Furthermore, any completion of a global field with any nontrivial absolute value is a local field. It is thus reasonable to ask if we can complete the square; where $\hat{L}$ is the completion of a corresponding global field L that is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$. In the local number field case:

$$\begin{tikzcd}
\mathbb{Q}_p \arrow[r, "\text{finite ext.}"] & \hat{L} \\
\mathbb{Q} \arrow[u, "|-|_p \text{ compl.}"] \arrow[r, dashed, "\text{finite ext.}"] & L \arrow[u, "|-|_{\mathfrak{p}} \text{ compl.}"']
\end{tikzcd}$$

Generalizing the question, given a fixed global field K and a local field $\hat{K}$ that is the completion of K with respect to a nontrivial absolute value $|-|$, if it the case that every finite extension of local field $\hat{L}/\hat{K}$ corresponds to an extension of global field L/K where $\hat{L}$ is the completion of L with respect to to an absolute value whose restriction to K must be equivalent to $|-|$. This is indeed the case! We shall show this for the separable case as it is what we need and the inseparable case offers more complication

Theorem 1.8.1: Local to Global Correspondence

Let K be a global with with a non-trivial absolute value $|-|$ and $\hat{K}$ the completion of K with respect to $|-|$. Then every finite separable extension $\hat{L}/\hat{K}$ is the completion of a finite separable extension of L of K with respect to an absolute avlue that restricts to $|-|$. Furthermore, L can be chosen so that

$$[L : K] = [\hat{L} : \hat{K}]$$

in which case $\hat{L} = \hat{K} \cdot L$.

Proof **:**

Let $\hat{L}/\hat{K}$ be a separable extension of degree n. Let K have an absolute value. If $|-|$ is Archimedean, then K is a number field and $\hat{K} \underset{\sim}{\in} \{\mathbb{R}, \mathbb{C}\}$, in which case these cases are left to the reader.

So assume $|-|$ is nonarchimedean so that the valuation ring of $\hat{K}$ is a complete DVR and $|-|$ is induced by its discrete valuation. As the extension is separable, by the primitive element theorem, we have a monic irreducible and separable polynomial $f \in \hat{K}[x]$ such that

$$\hat{L} = \frac{\hat{K}[x]}{f}$$

Let us now find an appropriate $g \in K[x]$. As k is dense in its completion $\hat{K}$, we can find a monic $g \in K[x]$ such that $\|g - f\|_1 < \delta$ for any $\delta > 0$. Then by theorem ref:HERE[a], g is separable and

$$\hat{L} = \frac{\hat{K}[x]}{g}$$

Then $\hat{L}$ is a finite separable extension of the field of fraction of a complete DVR, and so it is a field of fraction of a complete DVR and has a unique absolute value that extends the absolute value $|-|$ on $\hat{K}$.

Now, consider $L := K[x]/(g)$. The polynomial is irreducible in $\hat{K}[x]$, and hence in $K[x]$, and so

$$[L : K] = \deg g = [\hat{L} : \hat{K}]$$

Note the field $\hat{L}$ contains both $\hat{K}$ and L, and by construction is the smallest field that does this (note that g is irreducible in $\hat{K}[x]$), and so

$$\hat{L} = \hat{K}L$$

Finally, the absolute value on $\hat{L}$ restricts to an absolute value on L extending the absolute value $|-|$ on K , and hence $\hat{L}$ is complete and hence contains the completion of L with respect to $|-|$. On the other hand, the completion of L with respect to $|-|$ contains L and $\overline{H}$, and so must be HHL, as we sought to show.

[a] This theorem was not proven yet in these notes as it is in the Krasner's lemma section!

Let us now assume that $\hat{L}/\hat{K}$ is galois. Then is the corresponding global extension L/K galois, and are their galois groups isomorphic? As it turns out, it need not even be galois:

Example 1.8: Corresponding Global Extension Not Galois

Let $K = \mathbb{Q}$ and $\hat{K} = \mathbb{Q}_7$. Take $\hat{L} = \hat{K}[x]/(x^3 - 2)$. This extension is galois. The extension by definition contains the cube-root of 2, $\sqrt[3]{2}$. The other roots are this root times ζ_3, which is contains in $\mathbb{Q}_7$. This is true as $x^2 + x + 1 \in \mathbb{F}_7[x]$ has two roots which by Hensel's lemma both lift to roots in $\mathbb{Q}_7[x]$. However, $L = K[x]/(x^3 - 2)$ is *not* a galois extension, containing only one root.

However, if we replace K with $\mathbb{Q}(\zeta_3)$, this doesn't change the completion to $\hat{K}$ (take the completion of K with respect to the absolute value induced by a prime above 7), and certainly doesn't change $\hat{L}$, but now $L = K[x]/(x^3 - 2)$ *is* a galois extension.

Is it always possible to give a nice enough adjustment in the base global field K to get a correspondence of galois groups? This turns out to be the case.

Corollary 1.8.2: Local To Global Correspondence, Galois Groups

Let $\hat{L}/\hat{K}$ be a finite galois extension of local fields. Then there exists a finite galois extension of global fields L/K and an absolute value $|-|$ on L such that $\hat{L}$ is the completion of L with respect to $|-|$, $\hat{K}$ is the completion of K with respect to to the restriction of $|-|$ to K, and

$$\mathrm{Gal}_K(L) \cong \mathrm{Gal}_{\hat{K}}(\hat{L})$$

***Proof* :**

The Archimedean case is immediate so assume $|-|$ is nonarchimedean on $\hat{L}$ and it restricts to an absolute value on $\hat{K}$. By theorem 1.8.1 we may assume that this field is the completion of a global field K with respect to the restriction of $|-|$. As in the proof of that theorem, take a monic separable irreducible polynomial $g \in K[x]$ that has all those properties in $\hat{K}[x]$ such that $\hat{L} = \hat{K}[x]/(g)$ and define again $L = K[x]/(g)$ so that $\hat{L} = \hat{K}L$.

This time, let M/K be the splitting field of g. As $\hat{L}/\hat{K}$ is galois, $\hat{L}$ contains the roots too, and so by the universal property of splitting fields $\hat{L}$ contains a subextension in of K isomorphic to M; we may identify this extension with M.

Now, note that $\hat{L}$ is equal to the completion of M with respect to to the restriction of $|-|$ to M. From this we have a group homomorphism induce by restriction:

$$\varphi : \mathrm{Gal}_{\hat{K}}(\hat{L}) \to \mathrm{Gal}_K(M)$$

This map is injective, as each $\sigma \in \mathrm{Gal}_{\hat{K}}(\hat{L})$ is determined by its action on the roots of g in M. Now, replace K by a fixed field of the image of φ, and replace L with M. The completion of K with respect to to the restriction of $|-|$ is still $\hat{K}$, and similarity for L and $\hat{L}$, and so:

$$\mathrm{Gal}_{\hat{K}}(\hat{L}) \cong \mathrm{Gal}_K(L)$$

as we sought to show.

Let us now put this all together and consider the $AKLB$ case and look a primes $\mathfrak{B}$ lying over $\mathfrak{p}$:

Theorem 1.8.3: Global To Local Correspondence

Assume AKLB[a], $\mathfrak{p} \subseteq A$, $\mathfrak{p}B = \prod_{\mathfrak{B}/\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}}}$. Let $K_{\mathfrak{p}}$ be the completion of K with respect to $|-|_{\mathfrak{p}}$ which has maximal ideal $\hat{\mathfrak{p}}$ in its valuation ring. Similarly, for each $\mathfrak{B}/\mathfrak{p}$, let $L_{\mathfrak{B}}$ denote the completion of L with respect to $|-|_{\mathfrak{B}}$ and let $\hat{\mathfrak{B}}$ denote the maximal ideal of the corresponding maximal ideal of the valuation ring. Then:

1. Each $L_{\mathfrak{B}}$ is a finite separable extension of $K_{\mathfrak{p}}$ with $[L_{\mathfrak{B}} : K_{\mathfrak{p}}] \leq [L : K]$.
2. Each $\hat{\mathfrak{B}}$ is the unique prime of $L_{\mathfrak{B}}$ lying over $\hat{\mathfrak{p}}$.
3. Each $\hat{\mathfrak{B}}$ has ramification index $e_{\hat{\mathfrak{B}}} = e_{\mathfrak{B}}$ and residue field degree $f_{\hat{\mathfrak{B}}} = f_{\mathfrak{B}}$.
4. $[L_{\mathfrak{B}} : K_{\mathfrak{p}}] = e_{\mathfrak{B}} f_{\mathfrak{B}}$
5. The map $L \otimes_K K_{\mathfrak{p}} \to \prod_{\mathfrak{B}/\mathfrak{p}} L_{\mathfrak{B}}$ given by $\ell \otimes x \mapsto (\ell x, ..., \ell x)$ is an isomorphism of finite étale $K_{\mathfrak{p}}$ algebras
6. If L/K is galois, then each $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ is galois and we have isomorphisms of decomposition groups and inertia groups:

$$D_{\mathfrak{B}} \cong D_{\hat{\mathfrak{B}}} = \mathrm{Gal}_{K_{\mathfrak{p}}}(L_{\mathfrak{B}}) \qquad I_{\mathfrak{B}} \cong I_{\hat{\mathfrak{B}}}$$

[a] Recall L/K is finite and separable

***Proof* :**
(2) follows from theorem 1.5.2, (3) from simple computations, (4) from (2) and (3) and the fundamental identity. We'll show 1, 5, and 6

1. For each $\mathfrak{B}/\mathfrak{p}$, the embedding $K \hookrightarrow L$ induces an embedding $K_{\mathfrak{p}} \to L_{\mathfrak{B}}$ by mapping the equivalence classes, which is well-defined as a sequence which is Cauchy in K with respect to $|-|_{\mathfrak{p}}$ is also Cauchy in L with respect to $|-|_{\mathfrak{B}}$ (the valuation is extended). Thus $K_{\mathfrak{p}}$ can be viewed as a topological subfield of $L_{\mathfrak{B}}$. To show $[L_{\mathfrak{B}} : K_{\mathfrak{p}}] \leq [L : K]$, first any K-basis $b_1, ..., b_m$ for $L \subseteq L_{\mathfrak{B}}$ spans $L_{\mathfrak{B}}$ as a $K_{\mathfrak{p}}$-vector space. To see this, if $y = (y_n)$ is a cauchy sequence of elements in L, then we can write for each y_n position:

$$y_n = x_{1,n} b_1 + \cdots + x_{m,n} b_m \qquad x_{i,n} \in K$$

   these all will give Cauchy-sequences, as linear maps of finite dimensional normed space are uniformly continuous, and thus preserve Cauchy sequences.

   Next, L is a finite étale K-algebra as L/K is separable. Thus the change of basis $L \otimes_K K_{\mathfrak{p}}$ to $K_{\mathfrak{p}}$ is a finite étale $K_{\mathfrak{p}}$-algebra (see [ChwNAc]). Now, consider the $K_{\mathfrak{p}}$-algebra homomorphism:

$$\varphi_{\mathfrak{B}} : L \otimes_K K_{\mathfrak{p}} \to L_{\mathfrak{B}} \qquad \ell \otimes x \mapsto \ell x$$

   We have that $\varphi_{\mathfrak{B}}(b_i \otimes 1) = b_i$ for each K-basis element $b_i \in L$, and as $b_1, ..., b_m$ span $L_{\mathfrak{B}}$ as a $K_{\mathfrak{p}}$-vector space, this map is surjective. Next, $L \otimes_K K_| fp$ is by definition of finite étale algebraic, it is isomorphic to a finite product of finite separable extensions of $K_{\mathfrak{p}}$.But then $L_{\mathfrak{B}}$ is isomorphic to a subproduct, and thus is also a finite étale $K_{\mathfrak{p}}$ algebra, implying $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ is separable and finite.

5. (uses the weak approximation theorem from Neukrich, I'll get back to it)

6. Assume L/K is galois. Then each $\sigma \in D_{\mathfrak{B}}$ that acts on L respect $v_{\mathfrak{B}}$ as it fixes $\mathfrak{B}$, and so σ preserves Cauchy-sequences, showing that σ is an automorphism of $L_{\mathfrak{B}}$ and fixes $K_{\mathfrak{B}}$. We thus get a well-defined map:
$$\varphi : D_{\mathfrak{B}} \to \mathrm{Aut}_{K_{\mathfrak{p}}}(L\mathfrak{B})$$
This map is injective, for if σ acts trivially on $L_{\mathfrak{B}}$, certainly acts trivially on L. For surjectivity, note that :
$$e_{\mathfrak{B}} f_{\mathfrak{B}} = |D_{\mathfrak{B}}| \leq \#\mathrm{Aut}_{K_{\mathfrak{p}}}(L\mathfrak{B}) \leq [L_{\mathfrak{B}} : K_{\mathfrak{p}}] = e_{\mathfrak{B}} f_{\mathfrak{B}}$$
and so $\#\mathrm{Aut}_{K_{\mathfrak{p}}}(L\mathfrak{B}) \leq [L_{\mathfrak{B}} : K_{\mathfrak{p}}]$ showing that $L_{\mathfrak{B}}/K_{\mathfrak{p}}$ is galois and that φ is surjective, and hence an automorphism. Next, as $\hat{\mathfrak{B}}$ is the only prime of $L_{\mathfrak{B}}$, it must be fixed by every $\sigma \in \mathrm{Gal}_{K_{\mathfrak{p}}}(L_{\mathfrak{B}})$ and so
$$D_{\mathfrak{B}} \cong D_{\hat{\mathfrak{B}}} = \mathrm{Gal}_{K_{\mathfrak{p}}}(L_{\mathfrak{B}})$$
Finally, the inertia groups $I_{\mathfrak{B}}$ and $\hat{I}_{\mathfrak{B}}$ both have the same order and φ restricts to an (injective) homomorphism between these groups, and hence they are isomorphic.

Corollary 1.8.4: Global To Local Correspondence, Norm and Trace

Assume AKLB and let $\mathfrak{p}$ be a prime of A. Then for every $\alpha \in L$, we have:
$$N_{L/K}(\alpha) = \prod_{\mathfrak{B}/\mathfrak{p}} N_{L_{\mathfrak{B}}/K_{\mathfrak{p}}}(\alpha) \qquad \mathrm{tr}_{L/K}(\alpha) = \sum_{\mathfrak{B}/\mathfrak{p}} \mathrm{tr}_{L_{\mathfrak{B}}/K_{\mathfrak{p}}}(\alpha)$$

***Proof* :**
The norm and trace defined by the determinant and trace of the K-linear map $L \xrightarrow{\times\alpha} L$ is unchained when tensoring with $K_{\mathfrak{p}}$, hence by the isomorphism in part (5) of the above theorem we get the desired result.

Corollary 1.8.5: Global To Local Correspondence, Decomposition

Assume AKLB,$\mathfrak{p}$ a prime of A, $\mathfrak{p}B = \prod_{\mathfrak{B}/\mathfrak{p}} \mathfrak{B}^{e_{\mathfrak{B}}}$, $\hat{A}_{\mathfrak{p}}$ the completion of A with respect to $|-|_{\mathfrak{p}}$ and for each $\mathfrak{B}/\mathfrak{p}$ let $\hat{B}_{\mathfrak{B}}$ denote the completion of B with respect to $|-|_{\mathfrak{B}}$. Then
$$B \otimes_A \hat{A}_{\mathfrak{p}} \cong_{\hat{A}_{\mathfrak{p}}} \prod_{\mathfrak{B}/\mathfrak{p}} \hat{B}_{\mathfrak{B}}$$

***Proof* :**
exercise (see p.108 of MIT notes if you're stuck!)

1.9 Different and Discriminant

1.10 Kronecker-Weber Theorem

We are now in a position to prove the famous Kronecker-Weber Theorem using local fields.

Theorem 1.10.1: Global Kronecker-Weber Theorem

Every finite abelian extension of $\mathbb{Q}$ lies in a Cyclotomic field $\mathbb{Q}(\zeta_m)$

Proof **:**
soon

This result can be readily deduced from the local result:

Theorem 1.10.2: Local Kronecker-Weber Theorem

Every finite abelian extension of $\mathbb{Q}_p$ lies in a Cyclotomic field $\mathbb{Q}_p(\zeta_m)$

Proof **:**
soon

Proposition 1.10.3: Local Implies Global Kronecker-Weber

The Local Kronecker-Weber Theorem implies the Global Kronecker-Weber Theorem

Proof **:**
Let $K/\mathbb{Q}$ be a finite abelian extension. Then for each ramified prime p of $\mathbb{Q}$, pick a prime $\mathfrak{p}/p$ and let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. As $K/\mathbb{Q}$ is galois, it makes no difference which $\mathfrak{p}$ is picked. Then we know by theorem 1.8.3 that:

$$\mathrm{Gal}_{\mathbb{Q}_p}(K_\mathfrak{p}) \cong D_\mathfrak{p} \subseteq \mathrm{Gal}_\mathbb{Q}(K)$$

Hence $K_\mathfrak{p}$ i san abelian extension of $\mathbb{Q}_p$. By the local Kronecker-Weber Theorem we have that $K_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{m_p})$ for some $m_p \in N_{>0}$. Now, let $n_p = \nu_p(m_p)$, and define:

$$m = \prod_p p^{n_p}$$

which is finite as there are only finitely many ramified primes. Define $L = K(\zeta_m)$. Then we will show that $L = \mathbb{Q}(\zeta_m)$, showing that $K \subseteq \mathbb{Q}(\zeta_m)$.

First, the field $L = K \cdot \mathbb{Q}(\zeta_m)$ is the compositum of galois extensions of $\mathbb{Q}$, and hence is galois over $\mathbb{Q}$ with galois group isomorphic to a subgroup of $\mathrm{Gal}_\mathbb{Q}(K) \times \mathrm{Gal}_\mathbb{Q}(\mathbb{Q}(\zeta_m))$, and so is abelian. Let $\mathfrak{B}$ be a prime of L lying above the ramified prime $\mathfrak{p}/p$. Then the completion $L_\mathfrak{B}$ is a finite abliean extension of $\mathbb{Q}_p$ as $L/\mathbb{Q}$ is finite abelian. By minimality, $L_\mathfrak{B} = K_\mathfrak{p} \cdot \mathbb{Q}_p(\zeta_m)$. Now, let $F_\mathfrak{B}$ be the maximal unramified extension of $\mathbb{Q}_p$ in $L_\mathfrak{B}$. Then $L_\mathfrak{B}/F_\mathfrak{B}$ is totally ramified, giving $\mathrm{Gal}_{F_{\mathfrak{B}}}(L_{\mathfrak{B}}) \cong I_{\mathfrak{B}} = I_p$ (by theorem 1.8.3). Now, since $K_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\zeta_{m_p})$ and $\mathbb{Q}_p(\zeta_{m_p/p^{n_p}})$ is unramified by lemma 1.7.5, we have $L_{\mathfrak{B}} = F_{\mathfrak{B}}(\zeta_{p^{n_p}})$ (since $\mathbb{Q}_p(\zeta_{p^{n_p}})$ is unramified). Hence $K_{\mathfrak{p}} \subseteq F_{\mathfrak{B}}(\zeta_{p^{n_p}})$. There are a lot of terms going around, so we may visualize them in the following diagram:

$$\begin{tikzcd}
 & & L_{\mathfrak{B}} = K_{\mathfrak{p}} \cdot \mathbb{Q}_p(\zeta_m) = F_{\mathfrak{B}}(\zeta_{p^{n_p}}) & & \\
K_{\mathfrak{p}} \arrow[urr] \arrow[drrr, "\overset{\text{K.W.}}{\subseteq}"] & & F_{\mathfrak{B}} \arrow[u, "\text{totally ramified}"] & & \mathbb{Q}_p(\zeta_m) \arrow[ull] \\
 & & & \mathbb{Q}_p(\zeta_{m_p}) \arrow[ur] & \mathbb{Q}_p(\zeta_{m_p/p^{n_p}}) \arrow[u] \arrow[ull, "\text{by maximality}"'] \\
 & & \mathbb{Q}_p \arrow[uull, "\text{ramifies}"] \arrow[uu, "\text{max unramified}"] \arrow[ur] \arrow[urr, "\text{unramified}"'] & &
\end{tikzcd}$$

Furthermore, $F_{\mathfrak{B}} \cap \mathbb{Q}_p(\zeta_{p^{n_p}}) = \mathbb{Q}_p$ as $\mathbb{Q}_p(\zeta_{p^{n_p}})$ is totally ramified, hence:

$$I_p \cong \mathrm{Gal}_{F_{\mathfrak{B}}}(L_{\mathfrak{B}}) \cong \mathrm{Gal}_{\mathbb{Q}_p}(\mathbb{Q}_p(\zeta_{p^{n_p}}) \cong (\mathbb{Z}/p^{n_p}\mathbb{Z})^*$$

Now, let I be the group generated by the union of the groups $I_p \subseteq \mathrm{Gal}_{\mathbb{Q}}(L)$ for $p \mid m$. Then since $\mathrm{Gal}_{\mathbb{Q}}(L)$ is abelian, $I \subseteq \prod_p I_p$, and so:

$$\#I \leq \prod_{p \mid m} \#I_p = \prod_{p \mid m} \#(\mathbb{Z}/p^{n_p}\mathbb{Z}) = \prod_{p \mid m} \varphi(p^{n_p}) = \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$$

Now, recall that each inertia field L^{I_p} is unramified at p, and $L^I \subseteq L^{I_p}$, and so $L^I/\mathbb{Q}$ is unramified, but then by definition of L^i, $L^I = \mathbb{Q}$. Then:

$$[L : \mathbb{Q}] = [L : L^I] = \#I \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$$

giving $\mathbb{Q}(\zeta_m) \subseteq L$, which must mean that $L = \mathbb{Q}(\zeta_m)$, but hen $K \subseteq L = \mathbb{Q}(\zeta_m)$, as we sought to show.

Before proving the main result, we shall prove a quick important lemma:

Lemma 1.10.4: Kronecker Weber Theorem, Lemma

For any prime p,

$$\mathbb{Q}_p\left((-p)^{1/(p-1)}\right) = \mathbb{Q}_p(\zeta_p)$$

Proof **:**

Let $\alpha = (-p)^{1/(p-1)}$. Then α is the root of the Eisenstein polynomial $x^{p-1} + p$, and hence the extension $\mathbb{Q}_p(\alpha)$ is totally ramified of degree $p-1$ and α is a uniformizer. Let $\pi = \zeta_p - 1$. The minimal polynomial of π is:

$$f(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + p$$

which his Eisenstein, so $\mathbb{Q}_p(\pi) = \mathbb{Q}_p(\zeta_p)$ and is totally ramified of degree $p-1$ with π as a uniformizer. Then we have $u = -\pi^{p-1}/p \equiv 1 \mod \pi$ so u is a unit in the ring of integers of $\mathbb{Q}_p(\zeta_p)$. Setting $g(x) = x^{p-1} - u$ then $g(1) \equiv 0 \mod \pi$ and $g'(1) = p - 1 \not\equiv 0 \mod \pi$, and so by Hensel's lemma we can lift 1 to a root β of $g(x)$ in $\mathbb{Q}_p(\zeta_p)$.

We now have $p\beta^{p-1} = pu = -\pi^{-1}$, hence $(\pi/\beta)^{p-1} + p = 0$, and so $\pi/\beta \in \mathbb{Q}_p(\zeta_p)$ is a root of the minimal polynomial of α. As $\mathbb{Q}_p(\zeta_p)$ is galois, $\alpha \in \mathbb{Q}_p(\zeta_p)$. And since both $\mathbb{Q}_p(\alpha)$ and $\mathbb{Q}_p(\zeta_p)$ both have degree $p-1$, the fields are equal, as we sought to show.

***Proof* :**
of the local Kronecker Weber Theorem

Let us first reduce the proof to cyclic extensions of prime-power degree. This comes down to the correspondence between galois groups and compositum's. Namely, if $L_1/K, L_2/K$ are extensions where $L_1 \cap L_2 = K$, then their galois group is the product of the two galois groups. Then by the classification of finite abelian groups, we may decompose the abelian extension L/K into a compositum $L = L_1 \cdots L_n$ of linearly disjoint cyclic extensions L_i/K of prime-power degree. Then if each L_i lies in a Cyclotomic extension $K(\zeta_{m_i})$, so does L since

$$L \subseteq K(\zeta_{m_1}) \cdots K(\zeta_{m_n}) = K(\zeta_m) \qquad m = m_1 \cdots m_n$$

Hence, we shall focus on cyclic extensions $K/\mathbb{Q}_p$ of prime power l^r. This breaks up into two cass: $\ell = p$ and $\ell \neq p$.

The $\ell \neq p$ case

Let F be the maximal unramified extension of $\mathbb{Q}_p$ in K. Then by proposition 1.7.6 we have $F = \mathbb{Q}_p(\zeta_n)$. Then K/F is totally ramified, and as $\ell \neq p$ it must be tamely ramified. Then by theorem 1.7.18 we have

$$K = F(\pi^{1/e})$$

for some uniformizer π with $e = [K : F]$. Take $\pi = -pu$ for some $u \in \mathcal{O}_F^\times$, as $F/\mathbb{Q}_p$ is unramified[a]. Then the field $K = F(\pi^{1/e}) \subseteq F((-p)^{1/e}) \cdot F(u^{1/e})$. We shall show both lie in a Cyclotomic extension of $\mathbb{Q}_p$.

Now, since $\nu_{\mathfrak{B}}(\mathrm{disc}(x^e - u)) = 0$ for $p \nmid e$, $F(u^{1/e})/F$ is unramified, so $F(u^{1/e})/\mathbb{Q}_p$ is unramified, hence $F(u^{1/e}) = \mathbb{Q}_p(\zeta_k)$ for some $k \in \mathbb{N}_{>0}$. Take the compositum $K(u^{1/e}) = K\dot{\mathbb{Q}}_p(\zeta_k)$, which is abelian and contains the subextension $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ which is galois as it lies in an abelian extension. It is totally ramified since it is an Eisenstein extension. Next, the field $\mathbb{Q}_p((-p)^{1/e})$ containd ζ_e by taking the ratios of roots of $x^e + p$, but $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified as $p \nmid e$, so it must be that

$$\mathbb{Q}_p(\zeta_e) = \mathbb{Q}_p$$

Thus, $e \mid (p-1)$. By lemma 1.10.4:

$$\mathbb{Q}_p((-p)^{2/r}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$$

Then $F((-p)^{1/e}) = F \cdot \mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n)\mathbb{Q}_p(\zeta_p) \subseteq \mathbb{Q}_p(\zeta_{np})$. Hence:

$$K \subseteq F(u^{1/e}) \cdot F((-p)^{1/e}) \subseteq \mathbb{Q}(\zeta_k) \cdot \mathbb{Q}(\zeta_{np}) \subseteq \mathbb{Q}(\zeta_{knp})$$

completing the $\ell \neq p$ case.

The $\ell = p > 2$ case

Let us start with a cyclic extension $K/\mathbb{Q}_p$ of odd degree p^r. Then there are two candidates:

1. $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$, which is unramified of degree p^r
2. the index $p-1$ subfield of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ which is a totally ramifed extension of degree p^r

If K is contained in the compositum of these two fields, we are done. Otherwise, the field $K(\zeta_m($ is a galois extension of $\mathbb{Q}_p$ with:

$$\mathrm{Gal}_{\mathbb{Q}_p}(K(\zeta_m)) \cong \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}$$

for some $s > 0$, in particular the first factor is form the galois group of $\mathbb{Q}_p(\zeta_{p^{p^r}-1})$, the second two from the factors from the galois group of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ (note that $\mathbb{Q}_p(\zeta_{p^{p^r}-1}) \cap \mathbb{Q}_p(\zeta_{p^{r+1}}) = \mathbb{Q}_p$) and the last factor comes from the fact that by assumption $K \not\subseteq \mathbb{Q}_p(\zeta_m)$ so $\mathrm{Gal}_{\mathbb{Q}_p(\zeta_m)}(K(\zeta_m))$ is nontrivial and must have order p^s for some $1 \leq s \leq r$.

Now, the abelian group $\mathrm{Gal}_{\mathbb{Q}_p}(K(\zeta_m))$ has a quotient isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$, and the subfield of $K(\zeta_m)$ corresponding to this quotient is an abelian extension of $\mathbb{Q}_p$ with galois group $(\mathbb{Z}/p\mathbb{Z})^3$. I claim there is no such fields.

First, show that every totally wildly ramified galois extension of $\mathbb{Q}_p$ is cyclic for every odd p. Now, if $G = \mathrm{Gal}_{\mathbb{Q}_p}(K) \cong (\mathbb{Z}/p\mathbb{Z})^3$, then write G as an internal direct sum of the inertia subgroup $I \leqslant G$ and a cyclic subgroup $H \leqslant G$ (as L^i is unramified), and hence a cyclic extension of $\mathbb{Q}_p$ with galois group isomorphic to $G/I \cong H$. But then L^H is totally wildly ramified abelian extension of $\mathbb{Q}_p$ whose galois group G/H is *not* cyclic, which completes the proof for the $\ell = p > 2$ case.

The $\ell = p = 2$ case

We must isolate the $p = 2$ case as there is an extension of $\mathbb{Q}_2$ with galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, namely the Cyclotomic field $\mathbb{Q}_2(\zeta_{24}) = \mathbb{Q}_2(\zeta_3) \cdot \mathbb{Q}_2(\zeta_8)$. We apply the following analogous argument

First, the unramified Cyclotomic field $\mathbb{Q}_2(\zeta_{2^{2^r}-1})$ has galois group $\mathbb{Z}/2^r\mathbb{Z}$ and the totally ramified Cyclotomic field $\mathbb{Q}_2(\zeta_{2^r+2})$ has galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$ (up to isomorphic). Let $m = (2^{2^r} - 1)(2^{r+2})$. Now, if $K \not\subseteq \mathbb{Q}_2(\zeta_m)$, we must have:

$$\mathrm{Gal}_{\mathbb{Q}_2}(K(\zeta_m) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r)^2 \times \mathbb{Z}/2^s\mathbb{Z} & 1 \leq s \leq r \\ (\mathbb{Z}/2^r)^2 \times \mathbb{Z}/2^s\mathbb{Z} & 2 \leq s \leq r \end{cases}$$

and thus must admit a quotient isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$. We shall show no extension of $\mathbb{Q}_2$ has either of these galois groups, showing that K lies in $\mathbb{Q}_2(\zeta_m)$ which will complete the proof.

To do this, first show that there are exactly 7 quadratic extensions of $\mathbb{Q}_2$, and so there is no extension of $\mathbb{Q}_2$ that has galois group $(\mathbb{Z}/2\mathbb{Z})^4$ since this groups has 15 subgroups of index 2 whose fixed fields yields 15 distinct quadratic extensions of $\mathbb{Q}_2$.

Next, there are only finitely many extensions of $\mathbb{Q}_2$ for of degree d for a fixed d, and these can be enumerated by the Eisenstein polynomials in $\mathbb{Q}_2[x]$ of degree d divign the relation given by Krasner's lemma. Then there are 59 quartic extensions of $\mathbb{Q}_2$ of which 12 are cyclic. This would be very tedious to show directly, and can be verified given this link: LMFDB, 2-adic cyclic quadratic fields. Thus there is no extension of $\mathbb{Q}_2$ which has galois group $(\mathbb{Z}/4\mathbb{Z})^3$, as this group has 28 subgroups whose fixed fields gives 28 distinct cyclic quartic extensions of $\mathbb{Q}_2$, but then we have exhausted all possibilities, completing the proof.

[a] namely if $\mathfrak{B}/p$ is the maximal ideal of $\mathcal{O}_F$, then the valuation $\nu_{\mathfrak{B}}$ extends ν_p with index 1 so $\nu_{\mathfrak{B}}(-pu) = \nu_p(-p) = 1$

2

Places: Generalizing Primes

As we saw, primes uniquely correspond to discrete valuations (or equivalence classes of absolute values). Form this perspective, the Archimedean prime could be thought of as the "prime at infinity". This can in fact be made very precise, an shall even need to be taken properly into account when working looking at *ray fields* in chapter 4. We thus dive deeper into this connection

2.1 Generalizing Primes

Definition 2.1.1: Places

Let K be a field. Then a *place* of K is an equivalence class of nontrivial absolute values on K. The set of places of K shall be denoted M_K

Recall that the completions of K are in correspondence with absolute values and are invariant under equivalent absolute values, and hence completions of K are in correspondence with places. If $|-|_\nu$ is some representative absolute value of a place, then K_ν shall denote its completion. If a place is Archimedean, the field K_ν shall be called Archimedean, and nonarchimedean otherwise. If K is a global field, then the completion at a place gives a local field, which if ν is Archimedean we know that $K_\nu \cong \mathbb{R}$ or $K_\nu \cong \mathbb{C}$, and it is nonarchimedean then the absolute value of K_ν is induced by a discrete valuation, which we shall denote ν (this motivated the symbol for general fields, as the discrete valuation is independent of the choice of absolute value representative). When $K = \mathbb{Q}$, this gives the familiar places given by the primes as well as ∞.

Definition 2.1.2: Types of Places

Let K be a global field and ν a place. Then:

1. $K_\nu \cong \mathbb{R}$, ν is said to be a *real place*
2. $K_\nu \cong \mathbb{C}$, ν is said to be a *complex place*
3. If $|-|_\nu$ is induced by a discrete valuation $\nu_\mathfrak{p}$ for a prime $\mathfrak{p} \subseteq K$, then ν is a *finite place*. Otherwise it is an *infinite place*.

Every finite place must be nonarchimedean, every infinite place is Archimedean in characteristic 0 and nonarchimedean otherwise, every Archimedean place is an infinite place, but nonarchimedean may be finite or infinite (depending if the characteristic is positive).

Definition 2.1.3: Extending Places

Lt L/K be an extension of global fields. Then for every ω of L, any absolute value $|{-}|_w$ that represents the equivalence class w restricts to an absolute value on K that represents a place ν of K independent of choice of $|-|_w$. Then we write $w|\nu$ and say that w *extends* ν or that w *lies above* ν

Here now comes the most important results about places that generalize the Archimedean embedding and theorem 1.8.3(5):

Theorem 2.1.4: Extending Global Ring Tensoring Local Ring

let L/K be a finite separable extension of global fields and let ν be a place of K. Then:

$$L \otimes_K K_\nu \cong \prod_{w|\nu} L_w$$

given by

$$\ell \otimes x \mapsto (\ell x, ..., \ell x)$$

Proof **:**
If we restricted to only nonarchimedean places, theorem 1.8.3 would prove it. We generalize to places more generally

This seems not too important to prove rn. ATM, it is MIT theorem 13.5

Corollary 2.1.5: Places and Irreducible Factors

Let L/K be a finite separable extension of global fields, ν a place of K, and $f \in K[x]$ an irreducible polynomial such that $L \cong K[x]/(f(x))$. Then there is a One-to-one correspondence between the irreducible factors of f in $K_\nu[x]$ and the places of L lying above ν. In particular, if $f = f_i \cdots f_r$ are the factors of f in $K_\nu[x]$, then:

$$L_{w_i} \cong \frac{K_\nu[x]}{(f_i(x))} \qquad 1 \leq i \leq r$$

for appropriate w_i's.

***Proof* :**
exercise.

Corollary 2.1.6: Classifying Ebmeddings

Let L/K be a finite separable extension of global fields and ν a place of K. Then given a fixed algebraic closure $\overline{K}_\nu$, there is a bijection

$$\frac{\mathrm{Hom}_K(L, \overline{K}_\nu)}{\mathrm{Gal}_{K_\nu}(\overline{K}_\nu)} \leftrightarrow \{w|\nu\}$$

where the left hand side is the $\mathrm{Gal}_{K_\nu}(\overline{K}_\nu)$-orbits of K-embeddings of L into $\overline{K}_\nu$, and the right hand side is the places of L above ν.

***Proof* :**
Let $L \cong K(\alpha) = k[x]/(f)$ for some $\alpha \in L$ with minimal polynomial $f \in K[x]$. Then from field theory, there is a bijection between $\mathrm{Hom}_K(L, \overline{K}_\nu)$ and the roots of α_i of f in $\overline{K}_\nu$ that is compatible with the action of $\mathrm{Gal}_{K_\nu}(\overline{K}_\nu)$ on both sets.

Now, if $f = f_1 \cdots f_r$ is the factorization of f in $K_\nu[x]$, each f_i corresponds to an orbit of the galois action on the roots of f, which by corollary corollary 2.1.5 we get a one-to-one correspondence with the places of L above ν, as we sought to show.

In the special case of $K = \mathbb{Q}$ and $v = \infty$, we have that

$$\frac{\mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})}{\mathrm{Gal}_{\mathbb{R}}(\mathbb{C})} \leftrightarrow \{w|\infty\}$$

which gives the Archimedean embedding theorem from [ChwNAc, chapter 22]

Definition 2.1.7: Real and Complex Place

Let K be a number field. Then the elements of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$ are the *real embeddings* and the elements of $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ whose image does not lie strictly in $\mathbb{R}$ are called the *complex embeddings*

Corollary 2.1.8: Index Given Real and Complex Embeddings

Let K be a number field with r real places and s complex places. Then:

$$[K : \mathbb{Q}] = r + 2s$$

***Proof* :**
This is computation: take $K \cong \mathbb{Q}[x]/(f)$ for some irreducible separable $f \in \mathbb{Q}[x]$ so that:

$$[K : \mathbb{Q}] = \deg f = \#\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$$

Then the action of $\mathrm{Gal}_{\mathbb{R}}(\mathbb{C})$ on $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ as r orbits of size 1 and 2 orbits of size 2, and the rest follows.

Example 2.1: Real and Complex Places in Non-trivial Field

Take $K = \mathbb{Q}[x]/(x^3 - 2)$. Then there are three embeddigns $K \hookrightarrow \mathbb{C}$ for each root given by:

$$x \mapsto \sqrt[3]{2} \qquad x \mapsto \zeta_3 \sqrt[3]{2} \qquad x \mapsto \zeta_3^2 \sqrt[3]{2}$$

The first is a real embedding, the other two complex and conjugate to each other. Thus, K has a real place and a complex place, and we get that $[K : \mathbb{Q}] = 1 \cdot 1 + 2 \cdot 1 = 3$.

where should I put this result?

Proposition 2.1.9: p-valuation Property

Let $0 \neq r \in \mathbb{Q}$. Then

$$\prod_{p,\infty} |r|_p = 1$$

where p varies over all primes number and ∞

***Proof* :**
Any $r \in \mathbb{Q}$ can be factored as :

$$r = \pm \prod_{p \neq \infty} p^{\nu_p(r)}$$

and the $\pm$ is equal to $a/|a|_\infty$, giving us the result.

Note that this result work in for the elements of $k(t)$, namely

$$\prod_{\mathfrak{p},\infty} |f|_{\mathfrak{p}} = 1$$

2.2 Haar Measure

I want to add this because it came up in my num theory research

2.3 Extending Prime Factorization to Places

In this section, we shall continue the analogy between primes and places by showing that they respect many of the similar identities and properties that prime ideals do. We want to show an analogy for residue field, norm, inertia degree and ramification index, the fundamental identity, picard group, and divisors. In this section, we shall use the words prime and place interchangeably, distinguishing them as finite and infinite primes.

Let us first define the residue field for infinite primes. We shall see that

$$\kappa(\mathfrak{p}) = K_{\mathfrak{p}} \qquad \mathfrak{p} \mid \infty$$

will be the right notion. Now, for each prime $\mathfrak{p}$ we define the (canonical) homomorphism:

$$\nu_{\mathfrak{p}} : K^{\times} \to \mathbb{R}$$

where if $\mathfrak{p}$ is finite, it is the usual $\mathfrak{p}$-adic exponential valuation and $\nu_{\mathfrak{p}}(K^{\times}) = \mathbb{Z}$, and if $\mathfrak{p}$ is infinite then:

$$\nu_{\mathfrak{p}}(a) = -\log(|\tau a|)$$

where $\tau : K \to \mathbb{C}$ is the embedding which defined $\mathfrak{p}$. Now, for any $\mathfrak{p}/p$ (whether p is finite or infinite, define:

$$f_{\mathfrak{p}} = [\kappa(\mathfrak{p}) : \kappa(p)]$$

Where if $\mathfrak{p} \mid \infty$ we have $f_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{R}]$ and

$$\mathfrak{N}(\mathfrak{p}) = \begin{cases} p^{f_{\mathfrak{p}}} & \mathfrak{p} \nmid \infty \\ e^{f_{\mathfrak{p}}} & \mathfrak{p} \mid \infty \end{cases}$$

where e here is Euler's number, not the ramification. In fact, we may consider e as an infinite prime number, and the extension $\mathbb{C}/\mathbb{R}$ can be thought of as an unramified extension with inertia degree 2. Next, define the absolute value $| - |_{\mathfrak{p}} : K \to \mathbb{R}$ via:

$$|a|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-\nu_{\mathfrak{p}}(a)}$$

and $|0|_{\mathfrak{p}} = 0$. If $\mathfrak{p}$ is an infinite prime with associated embedding $\tau : K \to \mathbb{C}$, notice that:

$$|a|_{\mathfrak{p}} = |\tau a| \qquad |a|_{\mathfrak{p}} = |\tau a|^2$$

where $\mathfrak{p}$ is real and complex respectively.

Next, if L/K is a finite extension of K, denote the primes $\mathfrak{B}/\mathfrak{p}$ of L the valuations in the class $\mathfrak{B}$ which, when restricted to K, give $\mathfrak{p}$. In the case of an infinite prime $\mathfrak{B}$, we get the inertia degree and ramification index to be:

$$f_{\mathfrak{B}/\mathfrak{p}} = [L_{\mathfrak{B}} : K_{\mathfrak{p}}] \qquad e_{\mathfrak{B}/\mathfrak{p}} = 1$$

Thus, we may general the fundamental identity and many other results

Proposition 2.3.1: Fundamental Identity For Places

Let $\mathfrak{B}/\mathfrak{p}$ be an extension of primes (finite or infinite). Then:

1. $\sum_{\mathfrak{B}/\mathfrak{p}} e_{\mathfrak{B}/\mathfrak{p}} f_{\mathfrak{B}/\mathfrak{p}} = \sum_{\mathfrak{B}/\mathfrak{p}} [L_{\mathfrak{B}} : K_{\mathfrak{p}}] = [L : K]$
2. $\mathfrak{N}(\mathfrak{B}) = \mathfrak{N}(\mathfrak{p})^{f_{\mathfrak{B}/\mathfrak{p}}}$
3. $\nu_{\mathfrak{B}}(a) = e_{\mathfrak{B}/\mathfrak{p}} \nu_{\mathfrak{p}}(a)$ (for $a \in K^{\times}$)
4. $\nu_{\mathfrak{p}}(N_{L_{\mathfrak{B}}/K_{\mathfrak{p}}}(a)) = f_{\mathfrak{B}/\mathfrak{p}} \nu_{\mathfrak{B}}(a)$ (for $a \in L^{\times}$)
5. $|a|_{\mathfrak{B}} = |N_{L_{\mathfrak{B}}/K_{\mathfrak{p}}}|_{\mathfrak{p}}$ (for $a \in L$)

***Proof* :**
exercise

2.3.1 Galois Theory of Global Fields

Next, let us take a moment to extend the theory of places when L/K is a galois extension of global field. Then we have a galois group $\mathrm{Gal}_K(L)$ acting on the set of places ω of L via $\omega \mapsto \sigma(w)$ where $\sigma(w)$ is the equivalence classes of absolute valued given by

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

This generalizes the case from the finite prime case. We can generalize the decomposition group:

Definition 2.3.2: Decomposition Group For Places

Let L/K be a galois extension of global fields and let w be a place of L. Then the *decomposition group* of w is the stabilizer:

$$D_w = \{\sigma \in \mathrm{Gal}_K(L) \ : \ \sigma(w) = w\}$$

We shall see that in this case we can get infinite primes that ramify. By letting $L \cong \mathbb{Q}[x]/(f)$, we get a one-to-one correspondence between the embeddings of L into $\mathbb{C}$ with the root of $f \in \mathbb{C}$. Then each embedding of L into $\mathbb{C}$ restricts to an embedding of K into $\mathbb{C}$. This map induces a map that sends each infinite place w of L to an infinite place v of K that extends to w. Now, this map may send a complex place to a real place, which happens when a pair of distinct complex conjugate embeddings of L restrict to the same embedding of K (implying it must be a real embedding). In this case, we say that v (and w) is *ramified* in the extension L/K, and the ramification index is $e_\nu = 2$ (and $e_\nu = 1$ otherwise). In this case, we shall also have $f_\nu = 1$ for $\nu \mid \infty$, and $g_\nu = \#\{w|\nu\}$. With all of this, we may generalize the fundamental identity to:

$$e_\nu f_\nu g_\nu = [L : K]$$

and more generally:

Definition 2.3.3: Ramification Index For Global Infinite Primes

Let L/K be a galois extension of number fields L/K. Then:

$$e_0(L/K) = \prod_{\nu \nmid \infty} e_\nu \qquad e_\infty(L/K) = \prod_{\nu \mid \infty} e_\nu$$

$$e(L/K) = e_0(L/K)e_\infty(L/K)$$

Now as L/K is galois, it induces a transitive action on the embeddings and their corresponding places. As $L \cong k[x]/(g)$, each embedding of K into $\mathbb{C}$ gives rise to $[L : K]$ distinct embeddings of L into $\mathbb{C}$ that extend it, one for each root of g in $\mathbb{C}$. Thus ,for each infinite place ν of K, the galois group acts transitively on $\{w \mid \nu\}$, and so either all of the places $w|\nu$ are ramified or none are, which is determined by the decomposition group for places (namely, whether the decomposition group is order 1 or 2).

Let us conclude by generalizing Dirichlet's unit theorem, which is named after *Herband* as it shall have important results linking to Herband's Quotient we reach section 4.3:

Theorem 2.3.4: Herband Unit Theorem

Let L/K be a galois extension of number field. Let $w_1, ..., w_r$ be the real places of L and $w_{r+1}, ..., w_{r+s}$ be the complex places of L. Then there exists $\epsilon_1, ..., \epsilon_{r+s} \in \mathcal{O}_L^\times$ such that

1. $\sigma(\epsilon_i) = \epsilon_j$ if and only if $\sigma(w_i) = w_j$ for all $\sigma \in \mathrm{Gal}_K(L)$
2. $\epsilon_1, ..., \epsilon_{r+s}$ generate a finite index subgroup of $\mathcal{O}_L^\times$
3. $\epsilon_1\epsilon_2 \cdots \epsilon_{r+1} = 1$ and every relation among the ϵ_i is generated by this one.

Proof **:**
This proof is straight from Sutherland's notes. I need some more time to internalize it before typing it out myself. It is here for ease of reference

1. Pick $\epsilon_1, \ldots, \epsilon_{r+s} \in \mathcal{O}_L^\times$ such that $\|\epsilon_i\|_{w_j} < 1$ for $i \neq j$; the existence of such ϵ_i follows from the strong approximation theorem that we will prove in the next lecture; the product formula then implies $\|\epsilon_i\|_{w_i} > 1$. Now let $\alpha_i := \prod_{\sigma \in D_{w_i}} \sigma(\epsilon_i) \in \mathcal{O}_L^\times$. We have $\|\alpha_i\|_{w_i} = \prod_{\sigma \in D_{w_i}} \|\epsilon_i\|_{w_i} > 1$ and $\|\alpha_i\|_{w_j} = \prod_{\sigma \in D_{w_i}} \|\epsilon_i\|_{\sigma(w_j)} < 1$, since $\sigma \in D_{w_i}$ fixes w_i and permutes the w_j with $j \neq i$. Each α_i is fixed by D_{w_i}.

   Let $G := \mathrm{Gal}(L/K)$. For $i = 1, \ldots, r+s$, let $r(i) := \min\{j : \sigma(w_j) = w_j \text{ for some } \sigma \in G\}$, so that $w_{r(i)}$ is a distinguished representative of the G-orbit of w_i. For $i = 1, \ldots, r+s$ let $\beta_i := \sigma(\alpha_{r(i)})$, where σ is any element of G such that $\sigma(w_{r(i)}) = w_i$. The value of $\sigma(\alpha_{r(i)})$ does not depend on the choice of σ because $\sigma_1(w_{r(i)}) = \sigma_2(w_{r(i)})$ if and only if $\sigma_2^{-1}\sigma_1 \in D_{w_{r(i)}}$ and $\alpha_{r(i)}$ is fixed by $D_{w_{r(i)}}$. The β_i then satisfy (i).

2. The β_i also satisfy (2): a product $\gamma_j := \prod_{i \neq j} \beta_i^{n_i}$ cannot be trivial because $\|\gamma_j\|_{w_j} < 1$; in particular, $\beta_1, \ldots, \beta_{r+s-1}$ generate a subgroup of $\mathcal{O}_L^\times$ isomorphic to $\mathbb{Z}^{r+s-1}$ which necessarily has finite index in $\mathcal{O}_L^\times \simeq \mathbb{Z}^{r+s-1} \times \mu_L$ (see Theorem 15.12). But we must have $\prod_i \beta_i^{n_i} = 1$ for some tuple $(n_1, \ldots, n_{r+s}) \in \mathbb{Z}^{r+s}$ (with $n_i = n_j$ whenever w_i and w_j lie in the same

G-orbit, since every $\sigma \in G$ fixes 1). The set of such tuples spans a rank-1 submodule of $\mathbb{Z}^{r+s}$ from which we choose a generator $(n_1, \dots, n_{r+s})$ (by inverting some β_i if necessary, we can make all the n_i positive if we wish). Then $\varepsilon_i := \beta_i^{n_i}$ satisfy (1), (2), (3) as desired.

2.3.2 Picard Group for Places

Let us extend fractional ideals of K by taking into account infinite primes

Definition 2.3.5: Replete Ideal

Let K be a field. Then a *replete ideal* of K is an element of the group:

$$J(\overline{\mathcal{O}}) = J(\mathcal{O}) \times \prod_{\mathfrak{p}\infty} \mathbb{R}_+^\times$$

For notational consistency, for any infinite prime $\mathfrak{p}$ and any real number $\nu \in \mathbb{R}$, let:

$$\mathfrak{p}^\nu := e^\nu \in \mathbb{R}_+^\times$$

Next, given a ysstem of real numbers $\nu_\mathfrak{p}, \mathfrak{p} \mid \infty$, let $\prod_{\mathfrak{p}|\infty} \mathfrak{p}^{\nu_\mathfrak{p}}$ denote the vector:

$$\prod_{\mathfrak{p}|\infty} \mathfrak{p}^{\nu_\mathfrak{p}} = (..., e^{\nu_\mathfrak{p}}, ...) \in \prod_{\mathfrak{p}|\infty} \mathbb{R}_+^\infty$$

and *not* the product of the quantities $e^{\nu_\mathfrak{p}} \in \mathbb{R}$. Then every replete ideal $\mathfrak{a} \in J(\overline{\mathcal{O}})$ admits a unique factorization:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\nu_\mathfrak{p}} \times \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{\nu_\mathfrak{p}}$$

we shall denote the finite portion $\mathfrak{a}_f$ and the infinite portion $\mathfrak{a}_\infty$ so that

$$\mathfrak{a} = \mathfrak{a}_f \times \mathfrak{a}_\infty$$

Then $\mathfrak{a}_f$ is a fractional ideal and $\mathfrak{a}_\infty$ is an element of $\prod_{\mathfrak{p}|\infty} \mathbb{R}_+^\times$. Viewing $\mathfrak{a}_f$ and $\mathfrak{a}_\infty$ as elementst of

$$\mathfrak{a}_f \times \prod_{\mathfrak{p}|\infty} 1 \qquad (1) \times \mathfrak{a}_\infty$$

we can think of all the elements of $J(\overline{\mathcal{O}})$ as

$$\mathfrak{a} = \mathfrak{a}_f \cdot \mathfrak{a}_\infty$$

Now, to each $a \in K^\times$, we can associated to it a *replete principal ideal*:

$$|a| = \prod_{\mathfrak{p}} \mathfrak{p}^{nu_\mathfrak{p}(a)}$$

This forms a subgroup $P(\overline{\mathcal{O}}) \subseteq J(\overline{\mathcal{O}})$ and hence we can define the *replete picard group* or *replete class group*:

Definition 2.3.6: Replete Picard Group

$$\mathrm{Pic}(\overline{\mathcal{O}}) = \frac{J(\overline{\mathcal{O}})}{P(\overline{\mathcal{O}})}$$

Next,

Definition 2.3.7: Absolute Norm For Replete Ideals

The *absolute norm* of a replete ideal $\mathfrak{a}$ is defined to be the positive real number:

$$\mathfrak{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{\nu_{\mathfrak{p}}}$$

The absolute norm is multiplicative and induces a surjective homomorphism:

$$\mathfrak{N} : J(\overline{\mathcal{O}}) \to \mathbb{R}_{+}^{\times}$$

By using a generalization of proposition 2.1.9, the replete norm of a principal ideal a is equal to 1

$$\mathfrak{N}(a) = 1$$

Hence, we in fact get a surjective homomorphism on the replete Picard group

$$\mathfrak{N} : \mathrm{Pic}(\overline{\mathcal{O}}) \to \mathbb{R}_{+}^{\times}$$

There is still a bit more in Neukirch, p.187. I gotta leave it alone for now to finish other work, but must come back

3

Analytic Number Theory

Throughout the readers mathematical career, they will certainly hear that complex analysis and number theory are deeply intertwined together. Any such exploration in length requires some complex analysis, at least the knowledge of factoring holomorphic functions, which is covered [ChwNAd]. We shall show that every global number field shall have a Riemann-zeta function associated to it that gives information about the distribution of primes.

3.1 Riemann-Zeta Function

Definition 3.1.1: Riemann Zeta Function

The *Riemann-zeta function* is a complex function given by the series

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

and is defined on $\mathrm{Re}(s) > 1$.

Using the integral test, we see that this function converges for $\mathrm{Re} s > 1$ (recall the complex part only adds rotation information). Let us prove the second equality of this definition:

Proposition 3.1.2: Euler's Product

For $\mathrm{Re}(s) > 1$, we have:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}$$

which is absolutely convergent and $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$

Proof **:**
We may use the layer-cake representation (see [ChwNAb]), however for clarity we shall prove it more directly. We need the following chain of equalities:

$$\sum_{n=1}^{\infty} n^{-s} \overset{\text{decomp.}}{=} \sum_{n=1}^{\infty} \prod_p p^{-\nu_p(n)s} \overset{!}{=} \prod_p \left(\sum_{e \geq 0} p^{-es} \right) \overset{\text{geo. series}}{=} \prod_p \frac{1}{1-p^{-s}}$$

The key equality to show is the 2nd, which will follow by showing that the domain of convergence will be the same for all these series. Consider $\zeta_m(s)$ to be the function $\zeta(s)$ restricted to the set S_m of all integers m such that there are no prime factors $m < p$. Then there is at most $p_1, ..., p_k$ possible factors. As ζ converges absolutely on $\mathrm{Re}s > 1$, so does ζ_m, and so:

$$\zeta_m(s) = \sum_{m \in S_m} n^{-s} = \sum_{e_1, \ldots, e_k \geq 0} (p_1^{e_1} \cdots p_k^{e_k})^{-s} = \prod_{1 \leq i \leq k} \sum_{e_i \geq 0} (p_i^{-s})^{e_i} = \prod_{p \leq m} \frac{1}{1-p^{-s}}$$

Now, on any $\mathrm{Re}(s) > 1 + \delta$ for any delta, the sequence converges uniformly to $\zeta(s)$. Indeed, for any $\epsilon > 0$ and any s, pick appropriately small δ so that for sufficiently large m:

$$|\sigma(s) - \sigma_m(s)| \leq \left| \sum_{n \geq m} n^{-s} \right| \leq \sum_{n \geq m} |n^{-s} = \sum_{n \geq m} n^{-\mathrm{Re}(s)} \leq \int_m^{\infty} x^{-1-\delta} \leq \frac{1}{\delta} m^{-\delta} < \epsilon$$

Hence, this sequence converges locally uniformly to $\zeta(s)$ in $\mathrm{Re}(s) > 1$. By a similar argument, the sequence $P_m(s) = \prod_{p \leq m} \frac{1}{1-p^{-s}}$ converges to $\prod_p \frac{1}{1-p^s}$. To show it converges on all $\mathrm{Re}(s) > 1$, recall that a $\prod_n p_n$ converges uniformly (and absolutely) if and only if $\sum_n \log(p_n)$ converge uniformly (and absolutely). The sumation of the log converges if it's absolute value converges, hence:

$$\sum_p \left| \log\left(\frac{1}{1-p^{-s}} \right) \right| \overset{\text{Taylor Series}}{=} \sum_p \left| \sum_{e \geq 1} \frac{1}{e} |p^{-se}| \right| \leq \sum_p \sum_{e \geq 1} |p^{-s}|^e = \sum_p \frac{1}{(|p|^s - 1)} < \infty$$

this convergence is valid for $|z| < 1$ as the Taylor series of log converges on this domain. Then $\prod_p \frac{1}{1-p^{-s}}$ is absolutely convergent and nonzero on $\mathrm{Re}(s) > 1$, showing the equality and completing the proof.

Theorem 3.1.3: Meromorphic Extension Of Zeta Function (Analytic continuation)

$\zeta(s)$ extends meromorphically to $\mathrm{Re}(s) > 0$ with a pole at $s = 1$, namely to:

$$\zeta(s) = \frac{1}{s-1} + \varphi(s)$$

where $\varphi(s)$ is a holomorphic function on $\mathrm{Re}(s) > 0$.

***Proof* :**
let us start by showing we can write:

$$\zeta(s) = \frac{1}{s-1} + \varphi(s)$$

for a holomorphic function $\varphi(s)$ on $\mathrm{Re}(s) > 0$. To see this, take:

$$\begin{aligned} \zeta(s) - \frac{1}{s-1} &= \sum_{n\geq 1} n^{-s} - \int_1^\infty x^{-s}dx \\ &= \sum_{n\geq 1}\left(n^{-s} - \int_n^{n+1} x^{-s}dx\right) && \text{abs. convergence} \\ &= \sum_{n\geq 1}\int_n^{n+1}(n^{-s} - x^{-s})dx \end{aligned}$$

Define $\varphi_n(s) = \int_n^{n+1}(n^{-s} - x^{-s})dx$. Then these functions are holomorphic on $\mathrm{Re}(s) > 0$. To show $\varphi(s)$ is holomorphic, for any fixed s_0 such that $\mathrm{Re}(s_0) > 0$, and $x \in [n, n+1]$, we get:

$$\begin{aligned} |n^{-s_0} - x^{-s_0}| &= \left|\int_n^x s_0 t^{-s_0-1}dt\right| \\ &\leq \int_n^x \frac{|s_0|}{t^{s_0+1}}dt \\ &= \int_n^x \frac{|s_0|}{t^{1+\mathrm{Re}(s_0)}}dt \\ &\leq \frac{|s_0|}{n^{1+\mathrm{Re}(s_0)}} \end{aligned}$$

Hence,

$$|\varphi_n(s_0)| \leq \int_n^{n+1} | \leq \frac{|s_0|}{n^{1+\mathrm{Re}(s_0)}}$$

From this bound, we have that for $\epsilon = \mathrm{Re}(s_0)/2$, on $U = B_\epsilon(s_0)$ and each $n \geq 1$:

$$\sup_{s\in U}|\varphi_n(s)| \leq \frac{|s| + \epsilon}{n^{1+\epsilon}} =: M_n$$

Then we get:

$$\sum_n M_n = (|s_0| + \epsilon)\zeta(1+\epsilon)$$

which converges. Thus, the series $\sum_n \varphi_n$ converges absolutely on $\mathrm{Re}(s) > 0$. By the Weiestrass M-test and uniqueness of analytic extension, $\sum_n \varphi_n$ converges to a function

$$\varphi(s) = \zeta(s) - \frac{1}{s-1} \qquad \mathrm{Re}(s) > 0$$

as we sought to show.

Corollary 3.1.4: Residue Of Riemann-Zeta Function

$$\mathrm{Res}_{s=1}\zeta(s) = 1$$

By proposition 3.1.2, we see that $\zeta(s)$ has no roots for $\mathrm{Re}(s) > 1$. This result can be extended to $\mathrm{Re}(s) \geq 1$, which will be important for the prime number theorem. We require the following lemma

Lemma 3.1.5: Mertens Lemma

For any $x, y \in \mathbb{R}$ with $x > 1$

$$|\zeta(x)^3(\zeta(x+iy)^4(1z(x+2iy)| \geq 1$$

This is a “trick” that was found by Merten. For a longer proof but one with more intuition, MIT notes gives a proof by Hadamard (p.149).

***Proof* :**
As $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ for $\mathrm{Re}(s) > 1$:

$$\log|\zeta(s)| = -\sum_p \log|1-p^{-s}| = -\sum_p \mathrm{Re}\log(1-p^{-s}) = \sum_p \left(\sum_{n\geq 1} \frac{\mathrm{Re}(p^{-ns}}{n}\right)$$

Pluging in $s = x + iy$, we get:

$$\log|\zeta(x+iy)| = \sum_p \left(\sum_{n\geq 1} \frac{\cos(ny\log p)}{np^{nx}}\right)$$

And so:

$$\log|\zeta(x)^3(\zeta(x+iy)^4(1z(x+2iy)| = \sum_p \sum_{n\geq 1} \frac{3 + 4\cos(ny\log p) + \cos(2ny\log p)}{np^{nx}}$$

noting that $\cos(2\theta) = 2\cos^2(\theta) - 1$, we get:

$$3 + 4\cos(\theta) + \cos(2\theta) = 2(1+\cos(\theta))^2 \geq 0$$

Taking $\theta = ny\log p$, we get:

$$\log|\zeta(x)^3(\zeta(x+iy)^4(1z(x+2iy)| \geq 0 \Rightarrow |\zeta(x)^3(\zeta(x+iy)^4(1z(x+2iy)| \geq 1$$

completing the proof.

Theorem 3.1.6: Riemann-zeta No Zeros On $x = 1$ Line

The Riemann-zeta function $\zeta(s)$ has no zeros on $\text{Re}(s) \geq 1$

***Proof* :**
By proposition 3.1.2, $\zeta(s)$ on $\text{Re}(s) > 0$ has no zeros. Now, suppose that $\zeta(1 + iy) = 0$ for some $y \in \mathbb{R}$. Then it must be that $y \neq 0$ as $\zeta(s)$ has a pole at $s = 1$, and $\zeta(s0$ does not have a pole at $1 + 2iy \neq 1$ by theorem 3.1.3. It follows that we must have:

$$\lim_{x \to 1} |\zeta(x^3)\zeta(x + iy)^4\zeta(x + 2iy)| = 0$$

As $\zeta(s)$ has a simple pole at $s = 1$, a zero at $1 + iy$, and no pole at $1 + 2iy$. But this contradicts lemma 3.1.5, completing the proof.

In section 3.3 we shall extend this to the entire complex plane, and have explain the common undergraduate "prank" of $1 + 2 + 3 + \cdots = -1/12$, which we shall see is the answer to $\zeta(-1)$. For now, let us continue on to using the zeta function for some truly incredible results.

3.2 Prime Number Theorem

Definition 3.2.1: Prime Counting Function

The *prime counting function* is:

$$\pi(x) = \sum_{p \leq x} 1$$

We shall show that:

$$\pi(x) \sim \frac{x}{\log(x)}$$

meaning that $\lim_{x\to\infty} \pi(x)/\left(\frac{x}{\log(x)}\right) = 1$. Gauss had a better approximation (meaning one whose different grows more slowly) that is asymptotically equivalent that is written down for the reader to know:

$$\pi(x) \sim \text{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

We shall use the Riemann-zeta function to prove this result. This is one of the cases where there is an "elementary" way of proving this, meaning without the use of complex analysis, however the proof is much more difficult and was found around 100 years later By Erdös and Selberg in the 1940s (note that this PNT was hypothesized to be true by Gauss in the 19th century, and proven in 1896). To prove it, take the asymptotically equivalent

$$\vartheta(x) = \sum_{p \leq x} \log p$$

Lemma 3.2.2: Chebyshev's Lemma

$$\pi(x) \sim \frac{x}{\log(x)} \qquad \text{if and only if} \qquad \vartheta(x) \sim x$$

***Proof* :**
Certainly

$$0 \leq \vartheta(x) \leq \pi(x)\log(x) \qquad \Rightarrow \qquad \frac{\vartheta(x)}{x} \leq \frac{\pi(x)\log(x)}{x}$$

To bound the other side, let $\epsilon \in (0,1)$, and notice that:

$$\begin{aligned} \vartheta(x) &\geq \sum_{x^{1-\epsilon}<x\leq p} \log(p) \\ &\geq (1-\epsilon)\log(x)\left(\pi(x) - \pi(x)^{1-\epsilon}\right) \\ &\geq (1-\epsilon)\log(x)\left(\pi(x) - x^{1-\epsilon}\right) \end{aligned}$$

Thus for all ϵ,

$$\pi(x) \leq \left(\frac{1}{1-\epsilon}\right)\frac{\vartheta(x)}{\log(x)} + x^{1-\epsilon}$$

Dividing by x, we can combine the two equations to get:

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)\log(x)}{x} \leq \left(\frac{1}{1-\epsilon}\right)\frac{\vartheta(x)}{x} + \frac{\log(x)}{x^{\epsilon}}$$

Now, the 2nd term on the right hand side tends to 0 as $x \to \infty$, and hence we can make the ratio arbitrarily close (if one tends to one, so does the other), completing the proof.

Let us start by showing that $\vartheta(x)/x$ is bounded, namely it is in $O(x)$ (finding the particular coefficient is much harder)

Lemma 3.2.3: Bounding Prime Counting Quotient

For $x \geq 1$,

$$\vartheta(x) \leq (4\log 2)(x)$$

Hence, $\vartheta(x) \in O(x)$

***Proof* :**
Take first the following:

$$2^{2n} = (1+1)^{2n} = \sum_{m=0}^{2n}\binom{2n}{m} = \frac{(2n)!}{n!n!} \overset{!}{\geq} \prod_{n<p\leq 2n} p = \exp(\vartheta(2n) - \vartheta(n))$$

where the $\overset{!}{\geq}$ inequality came from noticing $(2n)!$ is divisible for every $p \in (n, 2n]$, but $n!$ is not divisible by these p's. Taking the log of both sides, we get:

$$\vartheta(2n) - \vartheta(n) \leq 2n\log(2)$$

which is true for all $n \geq 1$. Now for any natural number $m \geq 1$,

$$\vartheta(2^m) = \sum_{n=1}^{m} \big(\vartheta(2^n) - \vartheta(2^{n-1})\big) \leq \sum_{n=1}^{m} 2^n \log(2) \leq 2^{m+1}\log(2)$$

Finally, for any real $x \geq 1$, choose an m such that $2^{m-1} \leq x < 2^m$ so that:

$$\vartheta(x) \leq \vartheta(2^m) \leq 2^{m+1}\log(2) = (4\log(2))2^{m-1} \leq (4\log(2))x$$

completing the proof.

We must now show the ratio between $\vartheta(x)$ and x is 1 asymptotically. We shall use the following elementary real analysis result to find a good criterion

Lemma 3.2.4: Integral Condition For Linear Asymptotic Equivalence

Let $f : \mathbb{R}_{\geq 1} \to \mathbb{R}$ be a non-deceasing function. Then if

$$\int_1^\infty \frac{f(t) - t}{t^2}$$

Then

$$f(x) \sim x$$

Proof **:**

Define $F(x) = \int_1^x \frac{f(t)-t}{t^2}$. By our hypothesis $\lim_{x\to\infty} F(x)$ exists. Then for any $\epsilon > 0$, for large enough x, all the points are ϵ-close to each other. This implies that for all $\lambda > 1$ and $\epsilon > 0$:

$$|F(\lambda(x) - F(x)| < \epsilon$$

now, fix some $\lambda > 1$. Let's say that $f(x) \sim \lambda x$. Then there is an unbounded sequence λx_n such that $f(x_n) \geq \lambda x_n$ for sufficiently large n. Then:

$$F(\lambda x_n) - F(x_n) = \int_{x_n}^{\lambda x_n} \frac{f(t) - t}{t^2} \overset{!}{\geq} \int_{x_n}^{\lambda x_n} \frac{\lambda x_n - t}{t^2} dt \overset{\text{u sub.}}{=} \int_1^\lambda \frac{\lambda - t}{t^2} dt = c$$

for some constant $c > 0$, where the $\overset{!}{\geq}$ inequality comes from f being non-decreasing. Hence for large enough n,

$$|F(\lambda x_n) - F(x_n)| = c > \epsilon$$

a contradiction. It must then be that $f(x) < \lambda x$ for large enough x. A similar argument can be done to show that for sufficiently large x, $f(x) > \frac{1}{\lambda}x$, As these equality holds for all $\lambda > 1$, we get that:

$$\lim_{x\to\infty} \frac{f(x)}{x} = 1 \qquad \text{i.e.} \qquad f(x) \sim x$$

completing the proof.

To show that $\vartheta(x)$ satisfies the hypothesis of lemma 3.2.4, we shall bring in yet another real analysis tool: Take $H(t) = \vartheta(e^t)e^{-t} - 1$. Doing a change of variable argument, we see that:

$$\int_1^\infty \frac{\vartheta(t) - t}{t^2} dt < \infty \qquad \text{if and only if} \qquad \int_0^\infty H(u)du < \infty$$

The advantage of this change is that we may now use the Laplace transform to find the convergent properties. For completeness, let us box the definition of the Laplace transform:

Definition 3.2.5: Laplace Transform

Let $h : \mathbb{R}_{>0} \to \mathbb{R}$ be a piece-wise continuous function. Then the *Laplace Transform* of h, denoted $\mathcal{L}h$, is the function

$$\mathcal{L}h(s) = \int_0^\infty e^{st}h(t)dt$$

which is holomorphic for $\text{Re}(s) > c$ for any $c \in \mathbb{R}$ where $h(t) = O(ce^{ct})$.

The following properties of Laplace functions should be recalled (see [ChwNAa])

- linearity: $\mathcal{L}(f + ag) = \mathcal{L}(f) + a\mathcal{L}(g)$
- $g_c(x) = c$ is a constant function, then $\mathcal{L}g_c(s) = \frac{c}{s}$
- $\mathcal{L}(e^{at}h(t))(s) = \mathcal{L}(h)(s - a)$, for all $a \in \mathbb{R}$

Let us start understanding $H(u)$ after the application of the Laplace transform:

Lemma 3.2.6: Laplace Transform of Prime Counting Function

$$\mathcal{L}(\vartheta(e^t))(s) = \frac{\Phi(s)}{s}$$

is Holomorphic on $\text{Re}(s) > 1$ where

$$\Phi(s) = \sum_p p^{-s} \log p$$

Proof **:**
By lemma 3.2.3, $\vartheta(e^t) = O(e^t)$, hence $\mathcal{L}(\vartheta(e^t))$ is Holomorphic on $\text{Re}(s) > 1$. Let p_n be the nth prime, and $p_0 = 0$. Then as $\vartheta(e^t)$ is constant on $t \in (\log p_n, \log p_{n+1})$, we have:

$$\int_{\log p_n}^{\log p_{n+1}} e^{st}\vartheta(e^t)dt = \vartheta(p_n) \int_{\log p_n}^{\log p_{n+1}} e^{-st}dt = \frac{1}{s}\vartheta(p_n)\left(p_n^{-s} - p_{n+1}^{-s}\right)$$

Thus:

$$\begin{aligned}(\mathcal{L}\vartheta(et))(s) &= \int_0^\infty e^{-st}\vartheta(e^t)dt \\ &= \frac{1}{s}\sum_{n=1}^\infty \vartheta(p_n)\left(p_n^{-s} - p_{n+1}^{-s}\right) \\ &= \frac{1}{s}\sum_{n=1}^\infty \vartheta(p_n)p_n^{-s} - \frac{1}{s}\sum_{n=1}^\infty \vartheta(p_{n-2})p_n^{-s} \\ &= \frac{1}{s}\sum_{n=1}^\infty \left(\vartheta(p_n) - \vartheta(p_{n-1})\right)p_n^{-s} \\ &= \frac{1}{s}\sum_{n=1}^\infty p_n^{-s}\log p_n \\ &= \frac{\Phi(s)}{s}\end{aligned}$$

as we sought to show.

Using this result, we get that:

$$\mathcal{L}H(s) = \mathcal{L}(\vartheta(e^t)e^{-t})(s) - (\mathcal{L}1)(s) = \mathcal{L}(\vartheta(e^t))(s+1) - \frac{1}{s} = \frac{\Phi(s+1)}{s+1} - \frac{1}{s}$$

We will show this function extends to a meromorphic function on $\mathrm{Re}(s) > 1/2$, and is holomorphic on $\mathrm{Re}(s) \geq 0$ if we eliminate the right denominators. We first require the following which finally uses the Riemann-zeta function:

Lemma 3.2.7: Meromorphic Extension of Laplace Transform

The function $\Phi(s) - \frac{1}{s-1}$ extends to a meromorphic function on $\mathrm{Re}(s) > \frac{1}{2}$ that is holomorphic on $\mathrm{Re}(s) \geq 1$

***Proof* :**

By theorem 3.1.3, $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$, denote this extension by the same $\zeta(s)$. This function has a pole at $s = 1$ and no zeros on $\mathrm{Re}(s) \geq 1$. Thus, the logarithmic derivative $\frac{\zeta'(s)}{\zeta(s)}$ of $\zeta(s)$ is meromorphic on $\mathrm{Re}(s) > 0$ with no zeros on $\mathrm{Re}(s) \geq 1$ and a single simple pole at $s = 1$ with residue -1. Then by looking at the Euler product, for $\mathrm{Re}(s) > 1$ we get:

$$\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= (-\log(\zeta(s)))' \\
&= \left(-\log \prod_p \frac{1}{(1-p^{-s})}\right)' \\
&= \left(\sum_p \log(1-p^{-s})\right)' \\
&= \sum_p \frac{p^{-s}\log p}{1-p^{-s}} \\
&= \sum_p \frac{\log p}{p^s - 1} \\
&= \sum_p \left(\frac{1}{p^s} + \frac{1}{p^s(p^s-1)}\right) \\
&= \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}
\end{aligned}$$

The sum on the right hand side will converge absolutely and locally uniformly to a holomorphic function on $\mathrm{Re}(s) > 1/2$, and the left hand side is meromorphic on $\mathrm{Re}(s) > 0$ and on $\mathrm{Re}(s) \geq 1$ it has only a simple pole at $s = 1$ with residue 1. Thus, by properties of analytic functions we get that

$$\Phi(s) - \frac{1}{s-1}$$

extends to a meromorphic function on $\mathrm{Re}(s) > \frac{1}{2}$ that is holomorphic on $\mathrm{Re}(s) \geq 1$, as we sought to show.

Corollary 3.2.8: Meromorphic Extension of $(\mathcal{L}H)(s)$

The functions $\Phi(s+1) - \frac{1}{s}$ and $(\mathcal{L}H)(s) = \frac{\Phi(s+1)}{s+1} - \frac{1}{s}$ extend to meromorphic functions on $\mathrm{Re}(s) > -\frac{1}{2}$ that are holomorphic on $\mathrm{Re}(s) \geq 0$

Proof **:**
The first is an immediate result of the above lemma. For the econ function, note that

$$\frac{\Phi(s+1)}{s+1} - \frac{1}{s} = \frac{2}{s+1}\left(\Phi(s+1) - \frac{1}{s}\right) - \frac{1}{s+1}$$

is meromorphic on $\mathrm{Re}(s) > -\frac{1}{2}$ and holomorphic on $\mathrm{Re}(s) \geq 0$, as it is the sum of products of such functions, completing the proof.

Theorem 3.2.9: Criterion for Laplace Transform giving Bounded Integral

Let $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ be a bounded piecewise continuous function, and suppose its Laplace transform extends to a holomorphic function $g(s)$ on $\text{Re}(s) \geq 0$. Then the integral $\int_0^\infty f(t)dt$ converges and is equal to $g(0)$

***Proof* :**
Without loss of generality, assume $f(t) \leq 1$ for all $t \geq 0$. Then for $\tau \in \mathbb{R}_{>0}$, define

$$g_\tau(s) = \int_0^\tau f(t)e^{-st}dt$$

By definition

$$\int_0^\infty f(t)dt = \lim_{\tau\to\infty} g_\tau(0)$$

Hence, it suffices to show hat

$$\lim_{\tau\to\infty} g_\tau(0) = g(0)$$

To this end, pick $r > 0$, and let γ_r be the boundary of $\{s : |s| \leq r \text{ and } \text{Re}(s) \geq -\delta_r\}$ for some chosen $\delta_r > 0$ so that g is holomorphic on γ_r (δ_r exists as g is holomorphic on $\text{Re}(s) \geq 0$, and hence on some open ball $B_{\leq 2\delta(y)}(iy)$ for each $y \in [-r, r]$; take $\delta_r = \inf_{y\in[-r,r]}(\delta(y))$). Next, as each γ_r is a simple clsoed curve, and as for each $\tau > 0$ the function $h(s) = (g(s) - g_\tau(s))e^{s\tau}(1 + \frac{s^2}{r^2})$ is holomorphic on a regions containing γ_r, by Cauchy's integral formula (see [ChwNAd]) we can evaluate $h(0)$ to get:

$$g(0) - g_\tau(0) = h(0) = \frac{1}{2\pi i}\int_{\gamma_r} (g(s) - g_\tau(s))\, e^{s\tau}\left(\frac{1}{s} + \frac{s}{r^2}\right) ds \tag{3.1}$$

If we can show that the left hand side tends to 0 as $\tau \to \infty$, we shall get our desired result, namely that for any $\epsilon > 0$ w shall set $r = \frac{3}{\epsilon}$.

Splice $\gamma - r$ into the positive and negative semi-cirlce. Let γ_r^+ denote the positive semi-circle of radius r, i.e. restrict γ_r to $\text{Re}(s) > 0$. Then as the integrand is absolutely bounded by $1/r$ on γ_r^+, for $|s| = r$ and $\text{Re}(s) > 0$ we have:

$$\begin{aligned}
|g(s) - g_\tau(s)| \cdot \left|e^{s\tau}\left(\frac{1}{s} + \frac{s}{r^2}\right)\right| &= \left|\int_\tau^\infty f(t)e^{-st}dt\right| \cdot \frac{e^{\text{Re}(s)\tau}}{r} \cdot \left|\frac{r}{s} + \frac{s}{r}\right| \\
&\leq \int_\gamma^\infty e^{-\text{Re}(s)t}dt \cdot \frac{e^{\text{Re}(s)\tau}}{r} \cdot \frac{2\text{Re}(s)}{r} \\
&= \frac{e^{-\text{Re}(s)\tau}}{\text{Re}(s)} \cdot \frac{e^{\text{Re}(s)\tau}}{r} \cdot \frac{2\text{Re}(s)}{r} \\
&= \frac{2}{r^2}
\end{aligned}$$

Hence:

$$\left|\frac{1}{2\pi i}\int_{\gamma_r^+} (g(s) - g_\tau(s))\, e^{s\tau}\left(\frac{1}{s} + \frac{s}{r^2}ds\right)\right| \leq \frac{1}{2\pi} \cdot \pi r \cdot \frac{2}{r^2} = \frac{1}{r}$$

Now take γ_r^-, i.e. γ_r where $\mathrm{Re}(s) < 0$. Then for any fixed r, the first term $g(s)e^{s\tau}(s^{-1}sr^{-2})$ in equation (3.1) tends to 0 as $\tau \to \infty$ for $\mathrm{Re}(s) < 0$ and $|s| \leq r$. For the second term, note that as $g_\tau(s)$ is holomorphic on $\mathbb{C}$, we may instead integrate over the semicircle of radius r in $\mathrm{Re}(s) < 0$. For $|s| = r$ and $\mathrm{Re}(s) < 0$, we have:

$$\begin{aligned}
\left|g_\tau(s)e^{s\tau}\left(\frac{1}{s}+\frac{s}{r^2}\right)\right| &= \left|\int_\tau^\infty f(t)e^{-st}dt\right| \cdot \frac{e^{\mathrm{Re}(s)\tau}}{r} \cdot \left|\frac{r}{s}+\frac{s}{r}\right| \\
&\leq \int_0^\tau e^{-\mathrm{Re}(s)t}dt \cdot \frac{e^{\mathrm{Re}(s)\tau}}{r} \cdot \frac{-2\mathrm{Re}(s)}{r} \\
&= \left(1-\frac{e^{-\mathrm{Re}(s)\tau}}{\mathrm{Re}(s)}\right) \cdot \frac{e^{\mathrm{Re}(s)\tau}}{r} \cdot \frac{-2\mathrm{Re}(s)}{r} \\
&= \frac{2}{r^2} \cdot (1 - e^{\mathrm{Re}(s)\tau}\mathrm{Re}(s))
\end{aligned}$$

The 2nd factor on the right hand side tends to 1 as $\tau \to \infty$ as $\mathrm{Re}(s) < 0$. We thus get:

$$\left|\frac{1}{2\pi i}\int_{\gamma_r^-}(g(s)-g_\tau(s))\,e^{s\tau}\left(\frac{1}{s}+\frac{s}{r^2}ds\right)\right| \leq \frac{1}{2\pi}\cdot\pi r\cdot\frac{2}{r^2} \overset{\tau\to\infty}{=} \frac{1}{r}+o(1)$$

and the right hand side of equation (3.1) is bounded by $2/r + o(1)$ as $\tau \to \infty$. Hence, setting $r = 3/\epsilon$, we get for sufficiently large τ:

$$|g(0) - g_\tau(0)| < \frac{3}{r} = \epsilon$$

Hence:

$$\lim_{\tau\to\infty} g_\tau(0) = g(0)$$

as we sought to show.

Theorem 3.2.10: Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log(x)}$$

***Proof* :**

Take $H(t) = \vartheta(e^t)e^{-y} - 1$. This is a piecewise continuous functions that is bounded (by lemma 3.2.2) whose Laplace transform extends to a holomorphic function on $\mathrm{Re}(s) \geq 0$ by lemma 3.2.7. By theorem 3.2.9, the integral

$$\int_0^\infty H(t)dt = \int_0^\infty \left(\vartheta(e^t)e^{-t}-1\right)dt$$

converges. Replacing t with $\log(x)$, we get:

$$\int_1^\infty \left(\vartheta(x)\frac{1}{x}-1\right)\frac{dx}{x} = \int_1^\infty \frac{\vartheta(x)-x}{x^2}dx$$

converges. But then by lemma 3.2.4 $\vartheta(x) \sim x$, which by lemma 3.2.2 we get that

$$\pi(x) \sim \frac{x}{\log(x)}$$

as we sought to show.

This gives some Asymptotic behavior of the prime-counting function. Unfortunately, this does not give an error term; this is much harder to find. A proof discovered by Korobov and Vinagradov and independently has shown that this can be refined to:

$$\pi(x) = \mathrm{Li}(x) + O\left(\frac{x}{\exp\left((\log x)^{3/5+o(1)}\right)}\right)$$

with an error term $O\left(\frac{x}{(\log x)^n}\right)$ for all n, with the added restriction that the error term is not in $O(x^{1-\epsilon})$ for any $\epsilon > 0$. If we further assume the Riemann Hypothesis, which states that the zeros for $\zeta(s)$ in the critical strip $0 < \mathrm{Re}(s) < 1$ all lie on the line $\mathrm{Re}(s) = \frac{1}{2}$, then we can show that:

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2} + o(1))$$

If this could be found, then we would know a lot about the distribution of prime numbers, motivating the $1 million bounty for solving the Riemann Hypothesis.

3.3 Functional Equation

We know show how to extend $\zeta(s)$ to a meromorphic function on $\mathbb{C}$ that is holomorphic everywhere except for a simple pole at $s = 1$

MIT notes chapter 17. Skipping for now, noting that

$$\zeta(s) = 2^s \pi^{2-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s)$$

3.4 Dirichlet L-functions: Primes in Arithmetic Progressions

In this section, we shall build-up another important probabilistic fact about primes, namely that they in fact very often distribute very nicely. We build-up to the following result:

Theorem 3.4.1: Dirichlet Coprime Theorem

For all coprime integers a, m, there are infinitely many primes p such that

$$p \equiv a \mod m$$

Furthermore, for appropriate choice of m (called the modulus), the primes shall be equidistributed among them.

Dirichlet proved this back in 1837. However it was Riemann who showed how to establish this result using the Riemann-zeta function, and it will be a modernization of this proof that we shall present.

I may put this intuition for the proof of infinitely many primes once I get why its useful

3.4.1 Dirichlet Characters

Definition 3.4.2: Arithmetic Function

A function $f : \mathbb{Z} \to \mathbb{C}$ is called an *arithmetic function*. The function f is *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all coprime $m, n \in \mathbb{Z}$. It is totally multiplicative if $f(1) = 1$ and $f(mn) = f(m)f(n)$. For $m \in \mathbb{N}_{>0}$, we say that f is *m-periodic* if

$$f(n+m) = f(n) \qquad n \in \mathbb{Z}$$

and m is called the period of f if it is the least $m > 0$ for which this is satisfied .

Definition 3.4.3: Dirichlet Character

A *Dirichlet character* is a periodic totally multiplicative arithmetic function, and is usually denoted $\chi : \mathbb{Z} \to \mathbb{C}$.

As a Dirichlet character is periodic, it must be a finite multiplicatively closed subset of $\mathbb{C}$, and hence is a union of a finite subgroup $U(1)$ and $\{0\}$. The constant $\mathbb{1}(n) = 1$ is the *trivial Dirichlet character*, and is the unique Dirichlet character with period 1. Naturally, each Dirichlet character restricts to a group character χ on $(\mathbb{Z}/m\mathbb{Z})^\times$, and every group character on $(\mathbb{Z}/m\mathbb{Z})^\times$ extends to a Dirichlet character by letting $\chi(n) = 0$ whenever n is not within the period of m.

Definition 3.4.4: Dirichlet Character of Modulus m

Let χ be Dirichlet character. Then it is said to be *of modulus m* if it is an m-periodic Dirichlet character that is the extension of a group character on $(\mathbb{Z}/m\mathbb{Z})^\times$.

Notice that being m-periodic isn't sufficient to have a unique extension, for example a 2-periodic Dirichlet character can have modulus 2^k character. In general, we have the following

Lemma 3.4.5: Inducing same Dirichlet Character

Let χ be a Dirichlet character with period m. Then χ is a Dirichlet character of modulus m' if and only if $m | m' | m^k$ for some k.

Proof **:**
Let us show that $\chi(n) \neq 0$ if and only if $m \perp n$. To that end, suppose $\chi(n) \neq 0$ but $m \not\perp n$. Let p be a common divisor f m and n. Then $\chi(p) \neq 0$. As $\chi(p)\chi(n/p) = \chi(n) \neq 0$ we have that for any $r \in \mathbb{Z}$:

$$\chi(r)\chi(p) = \chi(rp) = \chi(rp + m) = \chi(r + m/p)\chi(p)$$

hence $\chi(r) = \chi(r + m/p)$ (as $\chi(p) \neq 0$. And so this implies χ is (m/p)-periodic, which contradicts the minimality of m. Hence $\chi(n) \neq 0 \Rightarrow m \perp n$.

Next, for any $n \perp m$, pick $a = ne \equiv 1 \mod m$, giving

$$\chi(1) = \chi(a) = \chi(n^e) = \chi(n)^e \neq 0$$

so $\chi(n) \neq 0$, and so $n \perp m \Rightarrow \chi(n) \neq 0$, so χ is a Dirichlet character of modulus m,

Finally, if $m|m'|mk$, then the prime divisors of m' coincide with those of m, and so :

$$n \perp m' \Leftrightarrow n \perp m \Leftrightarrow \chi(n) \neq 0$$

Certainly χ is m'-periodic (as $m|m'$ so χ is a Dirichlet character of modulus m', Conversely, if χ is a Dirichlet character of modulus m' ,then χ is a m'-periodic, and thus $m|m'$, (since m is he period of χ). As χ is a Dirichlet character of modulus m and of modulus m', for each prime p we have:

$$p|m \Leftrightarrow \chi(p) = 0 \Leftrightarrow p|m'$$

and so the prime divisors of m and m' coincide, and so m' divide some power of m for the right k, completing the proof.

This motivates the idea of a minimal or primitive Dirichlet character

Definition 3.4.6: Primitive Dirichlet Character

Let χ_1, χ_2 be Dirichlet character of modulus m_1, m_2 respectively where $m_1 \mid m_2$. Then if $\chi_2(n) = \chi_1(n)$ for $n \in (\mathbb{Z}/m_2\mathbb{Z})^\times$, we say χ_2 is *induced* by χ_1. If a Dirichlet character is induced by no other character, it is said to be *primitive.*

Lemma 3.4.7: Induced Dirichlet Characters

A Dirichlet character χ_2 of modulus m_2 is induced by a Dirichlet character of modulus $m_1 \mid m_2$ if and only if χ_2 is constant on residue classes in $(\mathbb{Z}/m_2\mathbb{Z})^\times$ that are congruent modulo m_1. If this is the case, the Dirichlet character $\chi - 1$ of modulus m_1 that induces χ_2 is uniquely determined

Proof **:**
exercise (very doable, but if stuck look at MIT Chap 18 page 4)

Definition 3.4.8: Principal Dirichlet Character

Let χ be a Dirichlet character. Then χ is called *principal* if it is induced by $\nVdash$. Let $\nVdash_m$ denote the principal Dirichlet character of moduli m corresponding toe the trivial character on $(\mathbb{Z}/m\mathbb{Z})^\times$

Lemma 3.4.9: Characterizing Principal Characters

Let χ be a Dirichlet character of modulus m. Then:

$$\sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0 \qquad \Leftrightarrow \qquad \chi = \nVdash_m$$

Proof **:**
This is a Representation Theory argument. We have that $\chi(n) = 0$ for $n \notin (\mathbb{Z}/m\mathbb{Z})^\times$ if and only if χ restricts to the trivial character on $(\mathbb{Z}/m\mathbb{Z})^\times$. (see [ChwNAc, chapter 24.2]).

Theorem 3.4.10: Characterizing Dirichlet Characters

Every Dirichlet character χ is induced by a primitive Dirichlet character $\tilde{\chi}$ that is uniquely determined by χ

Proof **:**
exercise (also very doable, but more book keeping. If you're stuck see MIT notes Chapter 18 p.4)

Definition 3.4.11: Conductor of Dirichlet Character

The *conductor* of a Dirichlet character χ is the period of the unique primitive Dirichlet character $\tilde{\chi}$ that induces χ

Corollary 3.4.12: Characterizing conductor 1 Character

For any Dirichlet character χ of modulus m we have

$$\sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0 \qquad \text{if and only if} \qquad \chi \text{ has conductor } 1$$

Proof **:**
follow directly from lemma 3.4.9

Corollary 3.4.13: Relating Dirichlet Character to all Concepts

Let $M(m)$ denote the set of Dirichlet characters of modulus m, and $X(m)$ denote the set of primitive Dirichlet characters of conductor dividing m, and $\widehat{G}(m)$ denote the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$. hen we have canonical bijections:

$$M(m) \to X(m) \to\to \widehat{G}(m) \qquad \chi \mapsto \widehat{\chi} \mapsto (n \mapsto \widehat{\chi}(n))$$

Proof **:**
exercise (if stuck MIT chap 18 p 5, but really should be something to do on your own)

We can now make $X(m)$ into a group via $\tilde{\chi_1}\tilde{\chi_2} = \widetilde{\chi_1\chi_2}$. The result is not given by pointwise multiplication of the two separate characters, but the unique primitive character that induces the pointwise product.

Example 3.1: 12-periodic Dirichlet Character
In the following, the period is m and the conductor is c.

m	c	0	1	2	3	4	5	6	7	8	9	10	11	mod-12	principal	primitive
1	1	1	1	1	1	1	1	1	1	1	1	1	1	no	yes	yes
2	1	0	1	0	1	0	1	0	1	0	1	0	1	no	yes	no
3	1	0	1	1	0	1	1	0	1	1	0	1	1	no	yes	no
3	3	0	1	-1	0	1	-1	0	1	-1	0	1	-1	no	no	yes
4	4	0	1	0	-1	0	1	0	-1	0	1	0	-1	no	no	yes
6	1	0	1	0	0	0	1	0	1	0	0	0	1	yes	yes	no
6	3	0	1	0	0	0	-1	0	1	0	0	0	-1	yes	no	no
12	4	0	1	0	0	0	1	0	-1	0	0	0	-1	yes	no	no
12	12	0	1	0	0	0	-1	0	-1	0	0	0	1	yes	no	yes

Note that the exponent of $(\mathbb{Z}/m\mathbb{Z})^\times$ is 2, and so $\chi(n) \in \{0, -1, 1\}$ as $(\text{im}\chi) \cap U(1) \subseteq \mu_2 = \{\pm 1\}$.

3.4.2 Dirichlet L-function

We shall now look at the distributions of primes using the following modified Riemann-Zeta function:

Definition 3.4.14: Dirichlet L-function

Let χ be a Dirichlet Character. Then the *Dirichlet L-function* associated to χ is:

$$L(s,\chi) = \prod_p (1 - \chi(p)p^{-s})^{-1} = \sum_{n\geq 1} \chi(n)n^{-s}$$

Naturally, the product converges absolutely for Re$s > 1$ (as $|\chi(n)| \leq 1$, and hence $L(s,\chi)$ is holomorphic on $\text{Re}(s) > 1$. If $\chi = \mathbb{1}$, Then $L(s,\mathbb{1}) = \zeta(s)$. For each principle character $\mathbb{1}_m$ of modulus m we have:

$$\zeta(s) = L(s, \mathbb{1}_m) \prod_{p|m} (1 - p^{-s})^{-1}$$

continue from p.181 from your pdf of MIT notes.

Theorem 3.4.15: Dirichlet Coprime Theorem

For all coprime integers a, m, there are infinitely many primes p such that

$$p \equiv a \mod m$$

***Proof* :**
MIT notes, chapter 18

3.5 Dedekind-Zeta Functions

In the above section, it (will be) claimed that the L-function $L(s,\chi)$ is holomorphic and nonvanishing at $s=1$ for all non-principal Dirichlet characters χ. To establish this claim, a more general version of the Riemann-zeta function will be required:

Definition 3.5.1: Dedekind Zeta Functions

Let K be a number field. Then

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathrm{Nm}(\mathfrak{a})^{-s} = \sum_{I} \mathfrak{N}(\mathfrak{a})^{-s} = \prod_{p\neq 0} (1-\mathfrak{N}(\mathfrak{p})^{-s})^{-1}$$

Lemma 3.5.2: Relating Zeta Functions

For $\sigma \in \mathbb{R}_{>1}$, $d=[K:\mathbb{Q}]$, $\zeta_K(\sigma)$ converges absolutely and is $\leq \zeta(\sigma)^d$

***Proof* :**
For each prime number p, factor $p\mathcal{O}_K = \prod_{i=1}^g p_i^{e_i}$, $\mathrm{Nm}(P_i) = p_i^{f_i}$, $\sum_i^g e_i f_i = d$. Then the "p-factor of $\zeta_K(\sigma)$" is

$$\prod_i^g (1+p^{-f_i\sigma}+p^{-2f_i\sigma}+\cdots) \leq (1+p^{-\sigma}+p^{-2\sigma}+\cdots)^d$$

with equality if p splits completely

Theorem 3.5.3: Extending Dedekind Zeta Function

$\zeta_k(s)$ extends meromorphically to $s>1-\frac{1}{d}$ with a unique pole (which is simple) at $s=1$ with residue

$$\mathrm{Res}_{s=1}\zeta_k(s) = \frac{2^{\pi}(2\pi^{r_2}|Cl(K)|\,\mathrm{Reg}_k}{w_k|\,\mathrm{disc}_k\,|D^{1/2}}$$

where $w_k = |\mathcal{O}_K^\times[Tor]|$, the number of roots of unity in K

Note this proof has nothing to do with the zeta function. We shall show another theorem and show it implies this one

Theorem 3.5.4: Equivalent Theorem

Define $N_K(x) = \#\{I \subseteq \mathcal{O}_K \ : \ \mathrm{Nm}(I) \leq x\}$ (notice that $N_{\mathbb{Q}}(x) = \lfloor x \rfloor$), and let A_k be the residue of ζ_k at 1. hen: Then

$$N_K(x) = A_K x + O(x^{1-\frac{1}{d}})$$

where O is big-O notation.

***Proof* :**
Thm 2 imply Thm 1

$$\zeta_k(s) = \sum N(I)^{-s}$$

$$\sum n^{-s}(N_K(n) - N_K(n-1))$$

$$= \sum N_k(n)(n^{-s} - (n_1)^{-s})$$

$$= \sum (A_k n + O(x^{1-1/d}))(n^{-s} - (n+1)^{-s})$$

$$= \sum O(n^{-1/d - \mathrm{Re}(s)})$$

where for the last line not that $O(n^{-\mathrm{Re}(s)-2}) = n^{-s} - (n+1)^{-s}$. This converges absolutely for $\mathrm{Re}(s) > 1 - \frac{1}{d}$. So

$$\sum A_k n(n^{-s}(n+1)^{-s}) = A_k \zeta(s)$$

as we sought to show.

Example 3.2: Application

1. Let $K = \mathbb{Q}(i)$. Then $\mathcal{O}_K \setminus \{0\} \xrightarrow{4-1} \{\text{non-zero ideals}\}$ given by $\alpha \mapsto (\alpha)$. Then

$$\begin{aligned} N_K(x) &= \frac{1}{4}\#\{\alpha \in \mathcal{O}_K \ : \ N(\alpha) \leq x\} \\ &= \frac{-1}{4} + \frac{1}{3}\#\{(a,b) \in \mathbb{Z}^2 \ : \ a^2 + b^2 \leq x\} \\ &= \frac{1}{3}\pi x + O(x^{1/2}) \end{aligned}$$

   where we get the πx estimate by counting lattice points within a circle or radius $\sqrt{x}$, giving us $\sim \pi x$.

2. Let $K = \mathbb{Q}(\sqrt{2})$. Then

$$\mathcal{O}_K \setminus \{0\} \xrightarrow{\infty - 1} \{\text{non-zero ideals}\}$$

   For simplicity, we may quotient by $\mathcal{O}_K$ to get an isomorphism.

Lemma 3.5.5: Counting Points In Manifold

Let S be a manifold with boundary. Then for $t \in \mathbb{R}_{>0}$, then

$$\#(t \cdot S \cap \mathbb{Z}^n) = t^n \mathrm{vol}(S) + O(t^{n-1})$$

***Proof* :**
Consider boxes of the form $\vec{v} + [-, 1]^n$,for $\in \mathbb{Z}^n$. Then

$$\mathrm{vol}(tS) =^n \mathrm{vol}(S) = \sum_{\vec{v}} \mathrm{vol}(tS \cap \vec{v} + [0,1]^n) = \#(tS \cap \mathbb{Z}^n) + O(B_1(t\partial S \cap \mathbb{Z}^n))$$

so $\#(B_1(\partial S) \cap \mathbb{Z}^n) \leq \mathrm{vol} \prod_{\mathbb{R}^{n-1}} (t\partial S)$

Exercise 3.5.1

1.

4

Class Field Theory: Places Approach

The Kronecker-Weber Theorem showed us that every abelian extension $L/\mathbb{Q}$ is contained in a Cyclotomic extension. Thus, we may view every galois group $\mathrm{Gal}_{\mathbb{Q}}(L)$ as the quotient of $(\mathbb{Z}/m\mathbb{Z})^*$. Can we do the same if we replace $\mathbb{Q}$ with an arbitrary number field K? In general, these are no longer Cyclotomic extensions of K, but there is still an analogue. They are the *ray class fields*, and their galois groups are isomorphic to *ray class groups.*

To define this group, we shall start with some a generalization of quadratic reciprocity which will be very important for the generalization we are endeavoring on

4.1 Artin Map

Recall that if L/K is a finite abelian galois extension of global fields, and $\mathfrak{B}/\mathfrak{p}$, then there exists an element $\sigma \in \mathrm{Gal}_K(L)$ called he Frobenius element, which is the pre-image given by the map $D_{\mathfrak{p}}(\mathfrak{B}) \to \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$, or (as was proven to be equivalent) the element σ_p such that $\sigma_p(x) = x^{\mathfrak{N}(\mathfrak{p})}$ mod $\mathfrak{p}$. This element is often denoted Frob_p, and if L/K where not abelian this would represent the conjugacy classes of σ_p. This can be represented another way.

Definition 4.1.1: Artin Symbol

Assume $AKLBG$ with the usual setup with residue fields. Then for each prime $\mathfrak{B}$ over L, define the *Artin symbol* to be:

$$\left(\frac{L/K}{\mathfrak{B}}\right) := \sigma_{\mathfrak{B}}$$

If L/K is abelian, then it is unambiguous to write:

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma_{\mathfrak{p}}$$

The simplest case for the Artin symbol if when $\mathfrak{p}$ splits completely, since then $D_{\mathfrak{p}}(\mathfrak{B}) = \{e\}$ and so

$$\left(\frac{L/K}{\mathfrak{B}}\right) = 1$$

Though this definition may seem a little strange with the notation, it shall turn out that an extension L/K of global fields can be completely determined by the set of primes $\mathfrak{p}$ that split completely in L!

A simple immediate thing we shall prove is:

Proposition 4.1.2: Artin Symbol Under Intermediate Fields

Le $AKLBG$ with finite residue field and $\mathfrak{B}/\mathfrak{p}$ unramified. Let E be an intermediate field extension of L and L, and let $\mathfrak{B}_E = \mathfrak{B} \cap E$. Then:

$$\left(\frac{L/E}{\mathfrak{B}}\right) = \left(\frac{L/K}{\mathfrak{B}}\right)^{[\mathbb{F}_{\mathfrak{B}_E}:\mathbb{F}_{\mathfrak{p}}]}$$

Furthermore, if E/K is galois, then $\left(\frac{E/K}{\mathfrak{B}_E}\right)$ is he restriction of $\left(\frac{E/K}{\mathfrak{B}_E}\right)$ to E.

***Proof* :**
The first comes from field theory, namely use $\#\mathbb{F}_{\mathfrak{B}_E} = (\#\mathbb{F}_{\mathfrak{p}})^{[\mathbb{F}_{\mathfrak{B}_E}:\mathbb{F}_{\mathfrak{p}}]}$. The second result come from the factorization in intermediary fields of of primes in galois extensions, see [ChwNAc].

With this setup, we may define the following map. Let S be the set of ramified primes in L/K for global fields. We then know that S is finite. If $\mathcal{I}_A$ is the free abelian group generated by the primes of a Dedekind domain A, let $\mathcal{I}_A^S$ be the free abelian group generated by all primes not in S. Then:

Definition 4.1.3: Artin Map

Let A be a Dedekind domain with finite residue fields. Let L/K be a finite abelian extension where $K = \text{Frac}(A)$, and let S be the set of primes of A that ramify in L. Then there is the homomorphism:

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_A^S \to \text{Gal}_K(L) \qquad \prod_i^m \mathfrak{p}_i^{e_i} \mapsto \prod_i^m \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$$

called the *Artin map*.

A fascinating result we shall prove later is that this map is *surjective*, meaning all the elements of the galois group have a fiber of Frobenius elements. By the earlier discussion we have that

$$\ker\left(\frac{L/K}{\cdot}\right) = \text{all primes that split completely}$$

Example 4.1: Artin Map Practice

As practice, determine this for quadratic extensions, which are certainly abelian. It is in general harder to find the map, and so we shall build-up some machinery.

For notational convenience, let us change about the notation. Let $\mathfrak{m} \subseteq \mathcal{O}_K$ be the minimal ideal divisible by every ramified prime of K, and let $\mathcal{I}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K$ be the sub of the ideal class group where $\nu_{\mathfrak{p}}(I) = 0$ for all $\mathfrak{p} \mid \mathfrak{m}$. Then we can re-write the morphism as :

$$\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \to \text{Gal}_K(L)$$
$$\prod_{\mathfrak{p} \nmid \mathfrak{m}} \mathfrak{p}_i^{n_{\mathfrak{p}}} \mapsto \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(\frac{L/K}{\mathfrak{p}}\right)^{n_{\mathfrak{p}}}$$

For a moment, let's say that $\psi_{L/K}^{\mathfrak{m}}$ is surjective. Then the kernel would be all unramified elements for which the Frobenius element is trivial, namely it will contain all primes that *split completely*. An important result that we shall need later is the following:

Proposition 4.1.4: Tower For Artin Map

Let $K \subseteq L \subseteq M$ be a tower of finite abelian extensions of global field and let $\mathfrak{m} \subseteq \mathcal{O}_K$ be an ideal divisible by all primes $\mathfrak{p} \subseteq \mathcal{O}_K$ that ramify in M. Then the following diagram commutes:

$$\begin{tikzcd}
\mathcal{I}_K^{\mathfrak{m}} \arrow[r, "\psi_{M/K}^{\mathfrak{m}}"] \arrow[dr, "\psi_{L/K}^{\mathfrak{m}}"'] & \text{Gal}_K(M) \arrow[d, "\sigma \mapsto \sigma|_L"] \\
& \text{Gal}_K(L)
\end{tikzcd}$$

> ***Proof*** **:**
> It follows from proposition 4.1.2.

Special case: $\mathbb{Q}$

Let us focus on the case where $K = \mathbb{Q}$ and a finite abelian extension $L/\mathbb{Q}$. In this case, the Kronecker-Weber Theorem tells us that every abelian extension $L/\mathbb{Q}$ lies in a Cyclotomic extension $\mathbb{Q}(\zeta_m)$. By field theory we get a canonical map:

$$\omega : \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \overset{\cong}{\to} (\mathbb{Z}/m\mathbb{Z})^*$$

which can be characterized by $\sigma(\zeta_m) = \zeta_m^{\omega(\sigma)}$. In cyclic extensions, the primes that ramify are those where $p \mid m$. By definition, $(\mathbb{Z}/m\mathbb{Z})^*$ contains all elements that are coprime to m. Furthermore, for each prime $p \nmid m$, σ_p is the unique automorphism where $\sigma(x) \equiv x^p \mod \mathfrak{p}$ for all $\mathfrak{p}/p$ (well-defined as the galois group is abelian). In particular, for each prime p, for all $\mathfrak{p}/p$, the Decomposition group surjects onto the galois group of finite extensions, giving us a Frobenius element, and as we are abelian it in fact gives *the* Frobenius element for p. As we have characterized the galois group automorphisms who's power is coprime to m, we can explicitly write out ω as a map from Frobenius elements:

$$\omega(\sigma_p) = p \mod m$$

As a consequence, we can define an inverse map sending every integer a coprime to m to:

$$\begin{aligned} \omega^{-1} : (\mathbb{Z}/m\mathbb{Z})^* &\to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \\ \omega^{-1}(\overline{a}) &= \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{(a)}\right) \qquad\qquad (a) \in \mathcal{I}_{\mathbb{Q}}^m \end{aligned}$$

As there are enough coprimes elements, the map can be extended to all elements $(a) \in \mathcal{I}_{\mathbb{Q}}^m$ so that the map

$$\psi^m_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : \mathcal{I}_{\mathbb{Q}}^m \to \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$$

is surjective. Finally, by Kronecker-Weber we have that $L \subseteq \mathbb{Q}(\zeta_m)$. The galois group of L is a quotient of $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m))$, and for any prime that ramifies in L certainly ramifies in $\mathbb{Q}(\zeta_m)$ and so we can keep the same m for the group $\mathcal{I}_{\mathbb{Q}}^L$. By proposition 4.1.4 we get the following surjective map:

$$\psi^m_{L/\mathbb{Q}} : \mathcal{I}_{\mathbb{Q}}^m \to \mathrm{Gal}_{\mathbb{Q}}(L)$$

completing the proof in the simplest case. To keep track of everything, here is a diagram:

$$\begin{tikzcd}
\mathcal{I}_{\mathbb{Q}}^m \arrow[r, shift left, "\mathcal{A}:(a)\mapsto\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{a}\right)"] \arrow[dr, "\mathrm{res}\circ\mathcal{A}"'] & \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \arrow[l, shift left, "\omega"] \arrow[d, "\sigma\mapsto\sigma_L"] \\
 & \mathrm{Gal}_{\mathbb{Q}}(L)
\end{tikzcd}$$

Let us now introduce the key ideas and vocabulary that will be necessary to generalize this result to replace $\mathbb{Q}$ with an arbitrary global number field K. These terms shall be made more precise after we the need arises:

- **Existence**: For each integer m, we have a *ray class field* $\mathbb{Q}(\zeta_m)$ which is an abelian extension that unramified only at $p \mid m$ (or equivalently a maximally unramified extension up to the primes $p \mid m$) with galois group isomorphic to the *ray class group* $(\mathbb{Z}/m\mathbb{Z})^*$
- **Completeness**: Every abelian extension of $\mathbb{Q}$ lies in a ray class field
- **Reciprocity**: If $L/\mathbb{Q}$ is abelian and contains in a ray class field $\mathbb{Q}(\zeta_m)$, the Artin map $\mathcal{I}_{\mathbb{Q}}^m \to \mathrm{Gal}_{\mathbb{Q}}(L)$ induces a surjective homomorphism from the ray class group to the galois group $\mathrm{Gal}_{\mathbb{Q}}(L)$, letting us view $\mathrm{Gal}_{\mathbb{Q}}(L)$ as a quotient of the ray class group, in this case $(\mathbb{Z}/m\mathbb{Z})^*$.

4.1.1 Moduli and Ray class Groups

Let us first generalize the role of m, which kept track of the primes that ramify. These primes are all associated to a valuation, which themselves are associated to absolute values. Recall that there are two absolute value not associated to any prime: the trivial and the Archimedean. We ignore the trivial and consider the equivalence classes of absolute values, in other words we are going to be considering *places*.

Definition 4.1.5: Modulus

Let K be a number field. Then a *modulus* or *cycle* $\mathfrak{m}$ for K is a function $M_K \to \mathbb{N}$ with finite support such that if $\nu|\infty$ we have $\mathfrak{m}(\nu) \leq 1$ with $\mathfrak{m}(\nu) = 0$ unless ν is a real place. The modulus is often seen as a formal product $\prod \nu^{\mathfrak{m}(\nu)}$ over M_k which can factor as:

$$\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty \qquad \mathfrak{m}_0 = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})} \qquad \mathfrak{m}_\infty = \prod_{\nu|\infty} \nu^{\mathfrak{m}(\nu)}$$

The modulus $\mathfrak{m}_0$ can be interpreted as an $\mathcal{O}_K$ ideal, and $\mathfrak{m}_\infty$ represents the real places of K. We often write $\#\mathfrak{m}_\infty$ to denote the number of real places in the support of $\mathfrak{m}$. If $\mathfrak{m}, \mathfrak{n}$ are moduli for K, we say that $\mathfrak{m}$ *divides* $\mathfrak{n}$ if $\mathfrak{m}(\nu) \leq \mathfrak{n}(\nu)$ for all $\nu \in M_K$. Similarly, the product is:

$$\mathfrak{mn}(\nu) = \mathfrak{m}(\nu) + \mathfrak{n}(\nu) \qquad \mathfrak{mn}(\nu) = \max(\mathfrak{m}(\nu) + \mathfrak{n}(\nu), 1)$$

where the first is for $\nu \nmid \infty$ and the second for $\nu \mid \infty$. Define also:

$$\gcd(\mathfrak{m}, \mathfrak{n})(\nu) = \min(\mathfrak{m}(\nu), \mathfrak{n}(\nu)) \qquad \gcd(\mathfrak{m}, \mathfrak{n})(\nu) = \max(\mathfrak{m}(\nu), \mathfrak{n}(\nu))$$

The trivial modulus is the modulus whose $\mathcal{O}_K$ ideal is (1), i.e. $\mathfrak{m}_0 = (1)$,and $\#\mathfrak{m}_\infty = 0$.

This leads up to the definition of the ray group. We need a series of definitions:

Definition 4.1.6: Coprime Fractional Ideal and modulus

Let $I \in \mathcal{I}_K$ be a fractional ideal. Then $\mathcal{I}$ is said to be *coprime* if

$$\nu_{\mathfrak{p}}(I) = 0 \qquad \forall \mathfrak{p} \mid \mathfrak{m}_0$$

Definition 4.1.7: Ray Group and Ray Class Group

Let $K/\mathbb{Q}$ be a number field. Then:

1. $\mathcal{I}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K$ is the subgroup of fractional ideals coprime to $\mathfrak{m}$
2. $K^{\mathfrak{m}} \subseteq K^\times$ is the subgroup of elements $\alpha \in K^\times$ where $(a) \in \mathcal{I}_K^{\mathfrak{m}}$
3. $K^{\mathfrak{m},1} \subseteq K^{\mathfrak{m}}$ is the subgroup of elements $\alpha \in K^{\mathfrak{m}}$ where

$$\nu_{\mathfrak{p}}(\alpha - 1) \geq \nu_{\mathfrak{p}}(\mathfrak{m}_0)$$

   for all $\mathfrak{p} \mid \mathfrak{m}_0$ and $\alpha_\nu > 0$ for $\nu \mid \mathfrak{m}_\infty$ (where α_ν is the image of $K \hookrightarrow K_\nu \cong \mathbb{R}$)

4. $\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ is the subgroup of principal fractional ideals $(\alpha) \in \mathcal{I}_K^{\mathfrak{m}}$ with $\alpha \in K^{\mathfrak{m},1}$

The group $\mathcal{R}_K^{\mathfrak{m}}$ is called the *ray group* with modulus $\mathfrak{m}$. The *ray class group* of modulus $\mathfrak{m}$ is the quotient:

$$\mathrm{Cl}_K^{\mathfrak{m}} = \frac{\mathcal{I}_K^{\mathfrak{m}}}{\mathcal{R}_K^{\mathfrak{m}}}$$

Definition 4.1.8: Wide and Narrow Ray Class Group

Let $\mathcal{L}_K^{\mathfrak{m}}$ be a ray class group. Then if $\mathfrak{m}(\nu) = 1$ for every real place, then $\mathrm{Cl}_K^{\mathfrak{m}}$ is called a *narrow ray class group*. A narrow ray class group where $\mathfrak{m}_0 = (1)$ is calle a *narrow class group*.

In this context, the usual class group is sometimes called the *wide class group*.

Definition 4.1.9: Ray Class Field

Let $\mathfrak{m}$ be a modulus. Then a finite abelian extension L/K that is unramified at all places not in $\mathfrak{m}$ for which the kernel of the Artin map:

$$\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}_K(L)$$

is equal to the ray group $\mathcal{R}_K^{\mathfrak{m}}$ is called the *ray class field* for modulus $\mathfrak{m}$.

If $\mathfrak{m}$ is trivial, namely $\mathfrak{m}_0 = (1)$ and $\mathfrak{m}_\infty = 0$ the ray class group is the class group. In the definition, we say "the" ray class field, though we have not yet proved there is a unique modulus $\mathfrak{m}$ associated to each such field. This will be given soon. The $K^{\mathfrak{m},1}$ group given by $\nu_{\mathfrak{p}}(\alpha - 1) \geq \nu_{\mathfrak{p}}(\mathfrak{m}_0)$ (for each prime) translates to in the case where we are only working with finite primes with the condition on representative:

$$(\alpha - 1) = \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha-1)}\mathfrak{q} \qquad \Rightarrow \qquad \alpha \equiv 1 \mod \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{m}_0)}$$

In the case with fractional ideals, we require the generalization. We also require that if there is any real places that α be positive with respect to to the embedding. In the concrete case where $K = \mathbb{Q}$ and $\mathfrak{m}_0$ contests of all ramified primes, are are asking that for each $\mathfrak{p} \in S$, we take the $\alpha \in K^{\mathfrak{m}}$ such that

$$\alpha \equiv 1 \mod \mathfrak{p} \qquad \forall \mathfrak{p} \in S$$

that is we are taking all the elements that map to 1 mod $\mathfrak{p}$. This can be thought of as taking the "units" of the ring of integers, and in fact $\mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$ injects into $\mathcal{O}_K^\times$[1]. This group shall end up being the kernel of the Artin map.

Example 4.2: Ray Class Groups

Let $K = \mathbb{Q}$ and $\mathfrak{m} = (5)$. Then $K^{\mathfrak{m}}$ contains all elements $a/b \in \mathbb{Q}$ (with representative where $\gcd(a, b) = 1$) such that there is no factor of 5. That gives

$$\mathbb{Q}^{\mathfrak{m}} = \left\{\frac{a}{b} \ : \ a, b \not\equiv 0 \mod 5\right\}$$

For $\mathbb{Q}^{\mathfrak{m},1}$, we need need to include all elements such that $a/b \equiv 1 \mod 5$, or $a \equiv b \mod 5$. Coupled with the above condition, that gives:

$$\mathbb{Q}^{\mathfrak{m},1} = \left\{\frac{a}{b} \ : \ a \equiv b \not\equiv 0 \mod 5\right\}$$

Then:

$$\begin{aligned}
\mathcal{I}_K^{\mathfrak{m}} &= \{(1), (2), (3), (4), (1/2), (1/3), (2/3), (3/2), (1/4), (3/4), (4/3), (1/6), (6), ...\} \\
\mathcal{R}_K^{\mathfrak{m}} &= \{(1), (4), (2/3), (3/2), (1/4), (6), (2/7), (7/2), ...\}
\end{aligned}$$

Note that $(2/3) \in \mathcal{R}_K^{\mathfrak{m}}$ even though $2/3 \notin K^{\mathfrak{m},1}$ since $-2/3 \in K^{\mathfrak{m},1}$ and $(-2/3) = (2/3)$. Similarly, $4 \in \mathcal{R}_K^{\mathfrak{m}}$ as $-4 = -4/1$ satisfies the congruence. This shall add all elements that are "positive conjugate". Hence:

$$\text{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}} = \{[(1)], [(2)]\} \cong (\mathbb{Z}/5\mathbb{Z})^\times/\{\pm 1\}$$

This group is isomorphic to the galois group of the totally real subfield $\mathbb{Q}(\zeta_5)^+ \subseteq \mathbb{Q}(\zeta_5)$, which is the ray class for this modulus (as you can verify). If we let $\mathfrak{m} = (5)\infty$, then all the ideals whose congruence was achieved by going into the negatives disappear $(-2/3, -4/1, ...)$ and so we change $\mathcal{R}_K^{\mathfrak{m}}$ to:

$$\mathcal{R}_K^{\mathfrak{m}} = \{(1), (6), (1/6), (2/7), (7/2), ...\}$$

and $\text{Cl}_K^{\mathfrak{m}} \cong (\mathbb{Z}/5\mathbb{Z})^\times$ and the ray class field becomes $\mathbb{Q}(\zeta_5)$. This motivates keeping the real places, as without them we shall get many instances where we have real subfields. Furthermore, notice the resemblance of the ray class group and the modular condition on $K^{\mathfrak{m}}$, namely they are strongly related.

As we see in the example, there is often a difference between $K^{\mathfrak{m},1}$ and $K^{\mathfrak{m}}$. We can quantify exactly how they are different through an appropriate exact sequence. To define it, we first require the following lemma

Lemma 4.1.10: Coprime Ideals in Class Group

Let A be a Dedekind domain and let $\mathfrak{a} \subseteq A$ be an ideal. Then every ideal class in $\text{Cl}(A)$ contains an A-ideal coprime to $\mathfrak{a}$.

[1] More on shall be made precise in theorem 4.1.11

***Proof* :**
Let I be a nonzero fractional ideal of A. Then for each $\mathfrak{p}|\mathfrak{a}$, pick $\pi_\mathfrak{p} \in \mathfrak{p}$ such that

$$\nu_\mathfrak{q}(\pi_\mathfrak{p}) = \nu_\mathfrak{q}(\mathfrak{p}) \qquad \forall\ \mathfrak{q}|\mathfrak{a}$$

Then by some number theory we can put $\alpha = \prod_{\mathfrak{p}|\mathfrak{a}} {\pi_\mathfrak{p}}^{-\nu_\mathfrak{p}(I)}$, so that

$$\nu_\mathfrak{p}(\alpha I) = 0 \qquad \forall\ \mathfrak{p}|\mathfrak{a}$$

thus αI is coprime to $\mathfrak{a}$ and $[\alpha I] = [I]$. Now ,let S be the (finite) set of primes $\mathfrak{p}$ where $\nu_\mathfrak{p}(\alpha I) < 0$. Pick $\pi_\mathfrak{p} \in \mathfrak{p}$ such that $\nu_\mathfrak{q}(\pi_p) = \nu_\mathfrak{q}(\mathfrak{p})$ for all $fq \in S$ and $\mathfrak{q}|\mathfrak{a}$ (which can be done again by number theory, see [ChwNAc, chapter 22]). Now, set

$$a = \prod_{\mathfrak{p}\in S} {\pi_\mathfrak{p}}^{-\nu_\mathfrak{p}(\alpha I)} \in A$$

Then $\nu_\mathfrak{p}(a\alpha I) \geq 0$ for all $\mathfrak{p}$, and $\nu_\mathfrak{p}(a\alpha I) = 0$ for all $\mathfrak{p}|\mathfrak{a}$. Then $a\alpha I$ is an A-ideal coprime to $\mathfrak{a}$, and $[a\alpha I] = [I]$, showing they are in the same equivalence class in the class group, as we sought to show.

Theorem 4.1.11: Canonical Exact Sequence for Modulus

Let $\mathfrak{m}$ be a modulus for a number field K. Then the following is an exact sequence:

$$1 \to \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \to \mathcal{O}_K^\times \to K^\mathfrak{m}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^\mathfrak{m} \to \mathrm{Cl}_K \to 1$$

where $K^\mathfrak{m}/K^{\mathfrak{m},1}$ is canonically isomorphic to:

$$K^\mathfrak{m}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$$

***Proof* :**
Consider

$$K^{\mathfrak{m},1} \overset{f}{\hookrightarrow} K^\mathfrak{m} \xrightarrow{g:\alpha\mapsto(\alpha)} \mathcal{I}_K^\mathfrak{m}$$

This gives us some immediate results:

1. $\ker(f) = 0$ and $\ker g \circ f = \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}$ (as $(\alpha) = (1)$ if and only if $\alpha \in \mathcal{O}_K^\times$),
2. $\ker g = \mathcal{O}_K^\times$, $\mathrm{coker} f = K^\mathfrak{m}/K^{\mathfrak{m},1}$,
3. $\mathrm{coker} g \circ f = \mathrm{Cl}_K^\mathfrak{m} = \mathcal{I}_K^\mathfrak{m}/\mathcal{R}_K^\mathfrak{m}$ and $\mathrm{coker} g = \mathrm{Cl}_K$ (by lemma 4.1.10).

Thus, by the snake lemma, the following commutative diagram with exact arrows:

$$\begin{tikzcd}
1 \arrow[r] & K^{\mathfrak{m},1} \arrow[r, hook, "f"] \arrow[d, "g\circ f"] & K^\mathfrak{m} \arrow[r] \arrow[d, "g"] & K^\mathfrak{m}/K^{\mathfrak{m},1} \arrow[r] \arrow[d, "\pi"] & 1 \\
1 \arrow[r] & \mathcal{I}_K^\mathfrak{m} \arrow[r, "\cong"] & CI_K^\mathfrak{m} \arrow[r] & 1 \arrow[r] & 1
\end{tikzcd}$$

gives a long exact sequence:

$$1 \to \mathcal{O}_K^\times \cap K^{\mathfrak{m},1} \to \mathcal{O}_K^\times \to K^{\mathfrak{m}}/K^{\mathfrak{m},1} \to \mathrm{Cl}_K^{\mathfrak{m}} \to \mathrm{Cl}_K \to 1$$

For the isomorphism, each $\alpha \in K^{\mathfrak{m}}$ can be written as a/b, $a, b \in \mathcal{O}_K$. Hence, by definition of $K^{\mathfrak{m}}$, choose $(a), (b)$ coprime to $\mathfrak{m}_0$. Define the homomorphism:

$$\begin{aligned} \varphi : K^{\mathfrak{m}} &\to \left(\prod_{\nu | \mathfrak{m}_\infty} \{\pm 1\} \right) \times (\mathcal{O}_K/\mathfrak{m}_0)^\times \\ \alpha &\mapsto \left(\prod_{\nu | \mathfrak{m}_\infty} \mathrm{sgn}(\alpha_\nu) \right) \times (\overline{\alpha}) \end{aligned}$$

where the map is well-defined since $\overline{\alpha} = \overline{a}\overline{b}^{-1} \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$ is well-defined. Now, by the Chinese Remainder Theorem:

$$(\mathcal{O}_K/\mathfrak{m}_0)^\times \cong \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times$$

and by theorem ref:HERE[a] φ is surjective. Then the kernel is $K^{\mathfrak{m},1}$, thus φ induces the isomorphism:

$$K^{\mathfrak{m}}/K^{\mathfrak{m},1} \cong \{\pm 1\}^{\#\mathfrak{m}_\infty} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$$

as we sought to show.

[a] (WEAK APPROXIMATION THEOREM, HAVEN'T PUT IT DOWN YET)

Corollary 4.1.12: Size of Ray Class Group

Let K be a number field and let $\mathfrak{m}$ be a modulus for K. The ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$ is a finite abelian group whose cardinality $h_K^{\mathfrak{m}} := \#\mathrm{Cl}_K^{\mathfrak{m}}$ is given by:

$$h_k^{\mathfrak{m}} = \frac{\varphi(\mathfrak{m}) h_K}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}]}$$

where $h_K = \#\mathrm{Cl}_K$, $\varphi(\mathfrak{m}) = \#(K^{\mathfrak{m}}/K^{\mathfrak{m},1}) = \varphi(\mathfrak{m}_\infty)\varphi(\mathfrak{m}_0)$ with:

$$\varphi(\mathfrak{m}_\infty) = 2^{\#\mathfrak{m}_\infty} \qquad \varphi(\mathfrak{m}_n) = \#(\mathcal{O}_K/\mathfrak{m}_0)^\times = N(\mathfrak{m}_0) \prod_{\mathfrak{p}|\mathfrak{m}_0} (1 - N(\mathfrak{p})^{-1})$$

In particular, h_K divides $h_K^{\mathfrak{m}}$ and $h_K^{\mathfrak{m}}$ divides $h_K \varphi(\mathfrak{m})$. The number h_K is called the *ray class number.*

***Proof* :**
The exact sequence in theorem 4.1.11 implies:

$$\frac{\varphi(\mathfrak{m})}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap K^{\mathfrak{m},1}]} = \frac{h_K^{\mathfrak{m}}}{h_K}$$

Computing the ray class number is not easy in general, however there are some algorithms for doing so (MIT notes quote Henri Cohen, Advanced topics in computational number theory)

4.1.2 Polar Density

We shall now build up to proving surjectivity of the Artin map for finite abelian extensions L/K of number fields (namely for any number field K, not just $K = \mathbb{Q}$). The key result needed will be a density result about primes. In this section, all numbers fields shall lie in some fixed algebraic clsorue of $\mathbb{Q}$

Definition 4.1.13: Partial Dedekind Zeta Function

Let K be a number field and let S be a set of primes of K. Then the *partial Dedekind zeta function* associated to S is the holomorphic function on $\mathrm{Re}(s) > 1$[a].

$$\zeta_{K,S}(s) = \prod_{\mathfrak{p}\in S} \frac{1}{(1 - \mathfrak{N}(\mathfrak{p})^{-s})}$$

[a] For the same reason as the Dedekind-zeta function

If S is finite, Then $\zeta_{K,S}(s)$ is certainly holomorphic and nonzero on a neighborhood of 1. If S is cofinite, then it will differ from $\zeta_K(s)$ by a holomorphic factor, and hence extends to a meromorphic function with a simple pole at $s = 1$. If S an infinite collection that is not co-finite, then the situation is in general more complicated; $\zeta_{K,S}(s)$ may or may not extend to a function that is meromorphic on a neighborhood of 1. If it does (or if some power of it does), then we can use the order of the pole at 1 to measure the density of S:

Definition 4.1.14: Polar Density

Let $\zeta_{K,S}$ be the partial Dedekind-zeta function. Then if for some integer $n \geq 1$ the function $\zeta_{K,S}^n$ extends to a meromorphic function on a neighborhood of 1, then the *polar density* of S is defined to be:

$$\rho(S) = \frac{m}{n} \qquad m = -\mathrm{ord}_{s=1}\zeta_{K,S}^n(s)$$

Note that m is the order of the pole if there is a pole at 1. If $\zeta_{K,S}^{n_1}$ and $\zeta_{K,S}^{n_2}$ both extend to a meromorphic function on a neighborhood of 1, then necessarily:

$$n_2\mathrm{ord}_{s=1}\zeta_{K,S}^{n_1}(s) = \mathrm{ord}_{s=1}\zeta_{K,S}^{n_1 n_2} = n_1\mathrm{ord}_{s=1}\zeta_{K,S}^{n_2}(s)$$

hence, $\rho(S)$ does not depend on the choice of n. We shall soon show that $\rho(S) \in [0,1]$, motivating the name *density*. Recall that we have seen something very similar before when we talked about natural density and Dirichlet density. These two are in fact related:

Proposition 4.1.15: Polar and Dirichlet Density

Let S be a set of primes of a number field K. Then if S has a polar density, it has a Dirichlet density, and the two are equal. As a consequence, $\rho(S) \in [0,1]$ whenever it is defined

***Proof* :**
Suppose S has a polar density $\rho(S) = \frac{m}{n}$. Taking the Laurent series expansion of $\zeta^n_{K,S}(s)$ at $s = 1$, and factoring out the leading nonzero term we get:

$$\zeta_{K,S}(s)^n = \frac{a}{(s-1)^m}\left(1 + \sum_{r\geq 1} a_r(s-1)^r\right)$$

for some constant $a \in \mathbb{C}^\times$. In fact, as $\zeta_{K,S}(s) \in \mathbb{R}_{>0}$ for $s \in \mathbb{R}_{>1}$, we must have $a \in \mathbb{R}_{>0}$, and hence $\lim_{s\to 1^+}(s-1)^m\zeta_{K,S}(s)^n \in \mathbb{R}_{>0}$. Taking the log of both sides, we get:

$$n\sum_{\mathfrak{p}\in S}\mathfrak{N}(\mathfrak{p})^{-s} \sim m\log\frac{1}{s-1} \qquad (\text{as } s \to 1^+)$$

Then as $\log(a) = O(1)$, it has no effect since $-m\log(s_1) \to \infty$ as $s \to 1^+$. It then follow that S has Dirichlet density

$$d(S) = \frac{m}{n}$$

Corollary 4.1.16: Polar Density and Natural Density

Let S be a set of primes of a number field K. Then if S has both has polar and natural density, the two coincide

***Proof* :**
As the polar and Dirichlet density coincide, and if the Dirichlet density exists it must coincide with the natural density, all these densities are equal

Note that not all set of primes with a natural density has a polar density (the later is always a rational number, the former need not be, see example ref:HERE).

Polar density is pretty well-behaved. For the following list of properties, we shall need the notion of a degree-1 prime, which is a prime in a number field K such that the degree of its residue field is 1 over $\mathbb{Q}$, i.e. $\mathfrak{N}(\mathfrak{p}) = [\mathcal{O}_K : \mathfrak{p}] = \#\mathbb{F}_{\mathfrak{p}}$.

Proposition 4.1.17: Properties of Polar Density

Let S, T dentoe sets of primes in a number field K, and let $\mathcal{P}$ denote the set of all primes of K, and let $\mathcal{P}_1$ be the set of all degree-1 primes of K. Then:

1. If S is finite, $\rho(S) = 0$. If $\mathcal{P} - S$ is finite, then $\rho(S) = 1$
2. If $S \subseteq T$, and both have polar densities, then $\rho(S) \leq \rho(T)$
3. If two set s S, T have finite intersection and if any two of $S, T, S \cup T$ have polar density, so does the third, and
$$\rho(S \cup T) = \rho(S) + \rho(T)$$
4. $\rho(\mathcal{P}_1) = 1$ and $\rho(S \cap \mathcal{P}_1) = \rho(S)$ whenever S has a polar density

Proof **:**
First, if S is a finite set , $\zeta_{K,S}(s)$ is a finite product of nonvanishing entire functions, and hence is entire (including at $s = 1$!). If the symmetric different between S and T is finite,

$$\zeta_{K,S}(s) f(s) = \zeta_{K,T}(s) g(s)$$

where f, g are non vanishing entire functions. Hence, if S, T differ by a finite set

$$\rho(S) = \rho(T)$$

whenever either have polar density. Then:

1. If $\rho(\emptyset) = 0$, and $\rho(\mathcal{P}) = 1$ (This will follow from the analytic class number formula, which I have will certainly put down as soon as possible!
2. Follows from results of Dirichlet Density
3. If the sets have finite intersection, by the argument made at the beginning of the proof we may take them to be disjoint. Then
$$\zeta_{K,S\cup T}(s)^n = \zeta_{K,S}(s)^n \zeta_{K,T}(s)^n$$
for all $n \geq 1$, which gives the result
4. Take $\mathcal{P}_2 = \mathcal{P} \setminus \mathcal{P}_1$ so that $\mathcal{P} = \mathcal{P}_1 \sqcup \mathcal{P}_2$. The for each rational prime p, we have at most $[K; \mathbb{Q}] = n$ primes $\mathfrak{p}/p$ in $\mathcal{P}_2$ (in particular $n/2$), wheer each have absolute norm $\mathrm{Nm}(\mathfrak{p}) \geq p^2$. Now, following by a comparison with $\zeta(2s)^n$, the product $\zeta_{K,\mathcal{P}_2}(s)$ converges absolutely to a holomorphic function on $\mathrm{Re}(s) > 1/2$, and hence is holomorphic and nonvanishing on a neighborhood of 1 (where it is nonvanishing by the Euler product). Then by definition,
$$\rho(S \cap \mathcal{P}_2) = 0$$
Which then by part (c), when $\rho(S)$ exists, $\rho(S) = \rho(S \cap \mathcal{P}_1)$, completing the proof.

Let us now take a particular S. We will require the following important subset of primes that twill come up again and again:

Definition 4.1.18: Splitting Primes Set

Let L/K be a galois extension, and let $\mathrm{Spl}_K(L)$ denote the set of all primes in K that split completely in L; if K is clear the set will be written $\mathrm{Spl}(L)$

The polar density of this set always exists, and is strongly related to the degree of the extension:

Theorem 4.1.19: Density of Completely Split Prime in Galois Extension

Let L/K be a galois extension of number fields of degree n. Then:

$$\rho(\mathrm{Spl}(L)) = \frac{1}{n}$$

***Proof* :**

By proposition 4.1.17, it suffices to define the set S to be set of degree-1 prime ideal of K that split completely in L and show that:

$$\rho(S) = 1/n$$

Let T be the set of all primes $\mathfrak{q} \subseteq L$ that lie above some $\mathfrak{p} \in S$. As $\mathfrak{p}$ splits completely if and only if $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$. Then for each $\mathfrak{q} \in T$,

$$N_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}} = \mathfrak{p} \qquad \Rightarrow \qquad \mathfrak{N}(\mathbb{N}_{L/K}(\mathfrak{q})) = \mathfrak{N}(\mathfrak{p})$$

and hence $\mathfrak{q}$ is a degree-1 polynomial. Furthermore, if $\mathfrak{q}$ is any unramified degree-1 prime of L and $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$, then:

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

and hence $f_{\mathfrak{p}} = e_{\mathfrak{p}} = 1$, implying that $\mathfrak{p}$ would be a degree-1 prime that splits completely in L and hence is an element of S. As only finitely many primes ramify, all but finitely many of the degree-1 primes in L lie in T, and hence

$$\rho(T) = 1$$

Finally, using proposition 4.1.17, each $\mathfrak{p} \in S$ has exactly n primes $\mathfrak{q} \in T$ lying above it (as $\mathfrak{p}$ splits completely). Thus:

$$\zeta_{L,T}(s) = \prod_{\mathfrak{q} \in T}(1 - \mathfrak{N}(\mathfrak{q})^{-s})^{-1} = \prod_{\mathfrak{p} \in S}(1 - \mathfrak{N}(\mathfrak{p})^{-s})^{-n} = \zeta_{K,S}(s)^n$$

which wrapping up gives:

$$\rho(S) = \frac{1}{n}\rho(T) = \frac{1}{n}$$

as we sought to show.

Corollary 4.1.20: Density of Completely Split Prime in Finite Extension

Let L/K be a finite extension of number fields, M/K it's galois closure of degree n. Then:

$$\rho(\mathrm{Spl}(L)) = \rho(\mathrm{Spl}(M)) = \frac{1}{n}$$

Proof **:**
A prime $\mathfrak{p} \subseteq K$ splits completely in L if and only if it splits completely in all conjugates of L in M. The galois closure of M is the compositum of all conjugates of L, so $\mathfrak{p}$ splits completely in L if and only if it splits completely in M, completing the proof.

Corollary 4.1.21: Polar Density in Sub-extensions

Let L/K be a finite galois extension of number fields with galois group $G = \mathrm{Gal}_K(L)$ and let $H \trianglelefteq G$. Then the set S of primes for which $\mathrm{Frob}_{\mathfrak{p}} \subseteq H$ has polar density

$$\rho(S) = \frac{\#H}{\#G}$$

Proof **:**
Let $F = L^H$. Then F/K is galois (as H is normal) and $\mathrm{Gal}_K(F \cong G/H$ by galois theory. Then for each unramified prime $\mathfrak{p}$ of K, the Frobenius class $\mathrm{Frob}_{\mathfrak{p}}$ lies in H if and only if every $\sigma_{\mathfrak{B}} \in \mathrm{Frob}_{\mathfrak{p}}$ acts trivially on $L^H = F$. This occurs if and only if $\mathfrak{p}$ splits completely in F¿ Then by theorem 4.1.19, the density of this set of primes is:

$$\frac{1}{[F:K]} = \frac{\#H}{\#G}$$

as we sought to show.

We shall now show that given a fixed field K, we may characterize tow number extensions L/K and M/K by only looking at the split primes! To that end, let S, T be sets of primes whose symmetric difference is finite[2]. Then either $\rho(S) = \rho(T)$ or neither sets have a polar density. This forms an equivalence class $S \sim T$. Partially orders the sets of primes via:

$$S \preceq T \qquad \text{if and only if} \qquad S \sim S \cap T$$

that is, $S - T$ is finite. If S, T have polar densities, then by proposition 4.1.17 $S \preceq T$ implies $\rho(S) \leq \rho(T)$. The reason for the direction of the $\preceq$ is clear in the following theorem:

[2] The symmetric distance is $(A \setminus B) \cup (B \setminus A)$

Theorem 4.1.22: Characterizing Galois Extensions Using Polar Density

Let L/K, M/K be two finite galois extensions of number fields. Then:

$$L \subseteq M \Leftrightarrow \mathrm{Spl}(M) \preceq \mathrm{Spl}(L) \Leftrightarrow \mathrm{Spl}(M) \subseteq \mathrm{Spl}(L)$$
$$L = M \Leftrightarrow \mathrm{Spl}(M) \sim \mathrm{Spl}(L) \Leftrightarrow \mathrm{Spl}(M) = \mathrm{Spl}(L)$$

and the map $L \mapsto \mathrm{Spl}(L)$ is an injection from the set of finite galois extension of K (in some fixed algebraic closure) to the sets of primes of K that have a positive polar density

Recall too that the kernel of the Artin map is all primes that split completely. This should give an idea behind why the Artin map is naturally connected to galois group.

***Proof* :**
Certainly:

$$L \subseteq M \Rightarrow \mathrm{Spl}(M) \subseteq \mathrm{Spl}(L) \Rightarrow \mathrm{Spl}(M) \preceq \mathrm{Spl}(L)$$

Thus, it suffices to show $\mathrm{Spl}(M) \preceq \mathrm{Spl}(L) \Rightarrow L \subseteq M$. Recall that $\mathfrak{p} \subseteq K$ splits completely in LM if and only if it splits in both L and M (this is some galois theory and algebraic number theory, see exercise ref:HERE). Then:

$$\mathrm{Spl}(M) \preceq \mathrm{Spl}(L) \Rightarrow \mathrm{Spl}(LM) \sim \mathrm{Spl}(M)$$

Then as we have the following by theorem 4.1.19,

$$\rho(\mathrm{Spl}(M)) = \frac{1}{[M:K]} \qquad \rho(\mathrm{Spl}(LM)) = \frac{1}{[LM:K]}$$

we get that

$$[LM:K] = \rho(\mathrm{Spl}(LM))^{-1} = \rho(\mathrm{Spl}(M))^{-1} = [M:K]$$

which shows that $LM = M$, and so $L \subseteq M$, giving the desired result. This also implies the equality immediately.

Finally, the map is certainly now an injection if it is well defined, which since $\mathrm{Spl}(L)$ always has positive density by theorem 4.1.19, this completes the proof.

4.1.3 Surjectivity of Artin Map

Theorem 4.1.23: Artin Map is Surjective

Let L/K be an abelian extension of number fields and $\mathfrak{m}$ a modulus divisible by all ramified primes. Then the Artin map

$$\psi^{\mathfrak{m}}_{L/K} : \mathcal{I}^{\mathfrak{m}}_K \twoheadrightarrow \mathrm{Gal}_K(L)$$

is surjective

Proof **:**
Take $\text{im}(\psi^{\mathfrak{m}}_{L/K}) = H \subseteq \text{Gal}_K(L)$. Let $F = L^H$. As L/K is abelian, F/K is a galois extension. For each prime $\mathfrak{p} \in \mathcal{I}^{\mathfrak{m}}_K$, the automorphism $\psi^{\mathfrak{m}}_{L/K}(\mathfrak{p}) \in H$ acts trivially on $F = L^H$, therefore $\mathfrak{p}$ splits completely in F. The group $\mathcal{I}^{\mathfrak{m}}_K$ contains all but finitely many primes $\mathfrak{p}$ of K, so the polar density of the primes in K that split completely is 1. But then $[F : K] = 1$, and $H = \text{Gal}_K(L)$, showing surjectivity

Theorem 4.1.24: Kernel of Artin Map

Let $\mathfrak{m}$ be a modulus for a number field K and let L, M be finite abelian extension of K which are unramified at all primes not in the support of $\mathfrak{m}$. If

$$\ker \psi^{\mathfrak{m}}_{L/K} = \ker \psi^{\mathfrak{m}}_{M/K}$$

Then

$$L = M$$

Hence, the ray class field is unique when it exists

Proof **:**
Let S be the set of primes of K that do not divide $\mathfrak{m}$, The each prime $\mathfrak{p}$ in S is unramified in both L and M, and split completely in L (resp. M) if and only if it lies in the kernel of $\psi^{\mathfrak{m}}_{L/K}$ (look back at the definition of Artin map if this is unclear). If $\ker \psi^{\mathfrak{m}}_{L/K} = \ker \psi^{\mathfrak{m}}_{M/K}$, then:

$$\text{Spl}(L) \sim (S \cap \ker \psi^{\mathfrak{m}}_{L/K}) = (S \cap \ker^{\mathfrak{m}}_{M/K}) \sim \text{Spl}(M)$$

Hence, by theorem 4.1.22, $L = M$, as we sought to show.

4.2 Global Class Field Theory

By theorem 4.1.23, we have an exact sequence:

$$1 \to \ker \psi^{\mathfrak{m}}_{L/K} \to \mathcal{I}^{\mathfrak{m}}_K \to \text{Gal}_K(L) \to 1$$

We may then ask if for a suitable choice of modulus $\mathfrak{m}$,

$$\mathcal{R}^{\mathfrak{m}}_K \subseteq \ker \psi^{\mathfrak{m}}_{L/K}$$

this would imply that the Artin map induces an isomorphism between $\text{Gal}_K(L)$ and a quotient of the ray class group $\text{Cl}^{\mathfrak{m}}_K = \mathcal{I}^{\mathfrak{m}}_K / \mathcal{R}^{\mathfrak{m}}_K$. When L is the ray class field for the modulus $\mathfrak{m}$, the Artin map will relate the subfield of L to the quotient of the ray class group. In the maximal case:

$$\text{Cl}^{\mathfrak{m}}_K \cong \text{Gal}_K(M)$$

This will be known as *Artin Reciprocity*. The field M which allows the above isomorphism shall be maximal in some appropriate sense, which shall let us conclude that we shall always have the ray group a subgroup of the kernel $\mathcal{R}^{\mathfrak{m}}_K \subseteq \ker \psi^{\mathfrak{m}}_{L/K}$ with equality in the maximal case.

4.2.1 Ray Class Field And congruence subgroup

Theorem 4.1.24 let us conclude that there is at most 1 ray class field. Let us show that on always exists. As this field is dependent on the modulus, let us label this field $K(\mathfrak{m})$ when/if it exists. Then if it exists, we have that:

$$\mathrm{Gal}_K(K(\mathfrak{m})) \cong \mathrm{Cl}_K^{\mathfrak{m}} \cong \frac{\mathcal{I}_K^{\mathfrak{m}}}{\mathcal{R}_K^{\mathfrak{m}}}$$

From this, we can find an appropriate group associated to If $K \subseteq L \subseteq K(\mathfrak{m})$, an intermediate field, namely the kernel of the Artin map would be a subgroup such that

$$\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{C} \subseteq \mathcal{I}_K^{\mathfrak{m}}$$

which gives the isomorphism:

$$\mathcal{I}_K^{\mathfrak{m}}/\mathcal{C} \cong \mathrm{Cl}_K^{\mathfrak{m}}/\overline{\mathcal{C}} \cong \mathrm{Gal}_K(L)$$

With this setup, we can now phrase the question of the proof of an abelian extension L/K lying in a ray class field as the existence of a modulus $\mathfrak{m}$ for K such that $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$, namely since by proposition 4.1.17 $\mathrm{Spl}(K(\mathfrak{m})) \preceq \mathrm{Spl}(L)$ and $L \subseteq K(\mathfrak{m})$. To that end, we endeavour to better understand congruence subgroups, and also to see if we can specify a minimal modulus $\mathfrak{m}$ for which we should be able to say that any given finite abelian extension L/K lie in a subfield of $K(\mathfrak{m})$. Note that when we proved Kronecker-Weber theorem, there was no question on finding a minimal $\mathfrak{m}$ for which all finite abelian extensions $L/\mathbb{Q}$ embed in $\mathbb{Q}(\zeta_m)$, and so this is a new exploration.

Definition 4.2.1: Congruence Subgroup

Let K be a number field and let $\mathfrak{m}$ be a modulus for K. Then a *congruence subgroup* for the modulus $\mathfrak{m}$ is a subgroup $\mathcal{C} \leqslant \mathcal{I}_K^{\mathfrak{m}}$ such that $\mathcal{R}_K^{\mathfrak{m}} \leqslant \mathcal{C}$. The image of this group in $\mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ will be denoted $\overline{\mathcal{C}}$.

We would like to say that the congruence subgroups will be kernels of Artin maps $\psi_{L/K}^{\mathfrak{m}}$ given a choice of $\mathfrak{m}$. However, the choice of $\mathfrak{m}$ is critical

Example 4.3: Wrong Choice of Modulus

Take $L/\mathbb{Q}$ where $L = \mathbb{Q}[x]/(x^3 - 3x - 1)$. Then you can check that only 3 ramifies. We can thus define the Artin map with modulus $\mathfrak{m} = (3)$. Then check that the ray class field is:

$$\mathbb{Q}(\zeta_3)^+ = \mathbb{Q}$$

and for $\mathfrak{m} = (3)\infty$ it is:

$$\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$$

Then note that neither contain L (they are both degree 2 extensions!), and so $\ker \psi_{L/K}^{(3)}$ and $\ker \psi_{L/K}^{(3)\infty}$ does *not* contain $\mathcal{R}_K^{\mathfrak{m}}$. If we choose $\mathfrak{m} = (9)$, then the corresponding field is $\mathbb{Q}(\zeta_9)^+$, and in fact $L \cong \mathbb{Q}(\zeta_9)^+$, and so $\ker \psi_{L/K}^{(9)}$ is a congruence subgroup for the modulus $\mathfrak{m} = (9)$.

Let us look at the relations between Moduli and ray groups. If $\ker \psi_{L/K}^{\mathfrak{m}}$ is a congruence subgroup for a modulus $\mathfrak{m}$, then for each $\mathfrak{m} \mid \mathfrak{n}$, $\ker \psi_{L/K}^{\mathfrak{n}}$ is a congruence subgroup. If $\mathfrak{m} \mid \mathfrak{n}$, $\mathcal{R}_K^{\mathfrak{n}} \subseteq \mathcal{R}_K^{\mathfrak{m}}$ and $\psi_{L/K}^{\mathfrak{n}}$

is the restriction of $\psi^{\mathfrak{m}}_{L/K}$ to $\mathcal{I}_K^{\mathfrak{n}}$ which contains $\mathcal{R}_K^{\mathfrak{n}}$, and so $\ker \psi^{\mathfrak{n}}_{L/K}$ is a congruence subgroup for the modulus $\mathfrak{n}$. If the support of $\mathfrak{m}$ and $\mathfrak{n}$ are the same, then

$$\mathcal{I}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{n}} \qquad \psi^{\mathfrak{m}}_{L/K} = \psi^{\mathfrak{n}}_{L/K}$$

however, the ray groups $\mathcal{R}_K^{\mathfrak{m}}$ and $\mathcal{R}_K^{\mathfrak{n}}$ may differ.

more intuition; it seems it differs due to multiplicity and real places

Definition 4.2.2: Equivalence Congruence Subgroups

Let K be a number field with moduli $\mathfrak{m}_1, \mathfrak{m}_2$. If $\mathcal{C}_1$ is a congruence subgroup for $\mathfrak{m}_1$ and $\mathcal{C}_2$ is a congruence subgroup for $\mathfrak{m}_2$, then we say that $(\mathcal{C}_1, \mathfrak{m}_1)$ and $(\mathcal{C}_2, \mathfrak{m}_2)$ are *equivalent* if

$$\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1$$

If $\mathfrak{m}_1 = \mathfrak{m}_2$, then this becomes $\mathcal{C}_1 = \mathcal{C}_2$

Proposition 4.2.3: Equivalence relation of congruence subgroups

Let K be a number field. Then the relation in definition 4.2.2 is an equivalence relation. If $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$, then

$$\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \cong \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$$

via canonical isomorphism that preserves cosets of fractional ideals prime to both $\mathfrak{m}_1$ and $\mathfrak{m}_2$

***Proof* :**
Let *sim* be the relationship defined above. Certainly $\sim$ is symmetric and reflexive. For transitivity, take $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ with $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3$ and assume:

$$(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2) \qquad (\mathcal{C}_2, \mathfrak{m}_2) \sim (\mathcal{C}_3, \mathfrak{m}_3)$$

Let $I \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_1$. Then by lemma 4.1.10 and the weak approximation theorem, pick $\alpha \in K^{\mathfrak{m}_1\mathfrak{m}_3,1}$ such that $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3}$. Then $(\alpha) \in \mathcal{R}_K^{\mathfrak{m}_1\mathfrak{m}_3} \subseteq \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{C}_1$, and $I \subseteq \mathcal{C}_1$, hence $\alpha I \in \mathcal{C}_1$ and $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$. Therefore, as $\mathcal{C}_1 \sim \mathcal{C}_2$:

$$\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 \subseteq \mathcal{C}_2$$

Next, $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_1\mathfrak{m}_2\mathfrak{m}_3} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$, and as $\mathcal{C}_2 \sim \mathcal{C}_3$:

$$\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_3 \subseteq \mathcal{C}_3$$

Now, as $(\alpha) \in \mathcal{R}_K^{\mathfrak{m}_1\mathfrak{m}_3} \subseteq \mathcal{R}_K^{\mathfrak{m}_3}$, $(\alpha) \in \mathcal{C}_3$, and so $(\alpha)^{-1} \in \mathcal{C}_3$, and so $\alpha^{-1}\alpha I = I \in \mathcal{C}_3$. Then as we have $I \in \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1}$, $I \in \mathcal{I}_K^{\mathfrak{m}_1} ca[\mathcal{C}_3$. As $I \in \mathcal{I}_K^{\mathfrak{m}_3} \cap \mathcal{C}_1$ was arbitrary,we ahve:

$$I_K^{\mathfrak{m}_3} \cap \mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_3$$

Then by symmetry we get the reverse, and hence

$$(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_3, \mathfrak{m}_3)$$

For the isomorphism, let us define the homomorphism, and then show it is an isomorphism. Take $I \in \mathcal{I}_K^{\mathfrak{m}_1}$ and again pick $\alpha \in K^{\mathfrak{m}_1,1}$ so that $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2}$. Then the image of αI in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$ is independent of choice of α, as for any other $\alpha' \in K^{\mathfrak{m}_1,1}$ where $\alpha' I \in \mathcal{I}_K^{\mathfrak{m}_2}$, $(\alpha I)/(\alpha' I) = (\alpha/\alpha') \in \mathcal{I}_K^{\mathfrak{m}_2}$ and $(\alpha/\alpha' \in \mathcal{R}_K^{\mathfrak{m}_1}$, and so $(\alpha/\alpha') \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{R}_K^{\mathfrak{m}_1} = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{R}_K^{\mathfrak{m}_2}$. We thus have a group homomorphism $\varphi : \mathcal{I}_K^{\mathfrak{m}_1} \to \mathcal{I}_K^{z\mathfrak{m}_2}/\mathcal{C}_2$.

Now, for $I \in \mathcal{C}_1$, $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 \subseteq \mathcal{C}_2$. As $I \in \mathcal{I}_K^{\mathfrak{m}_1} \setminus \mathcal{C}_1$, $\alpha I \in \mathcal{I}_K^{\mathfrak{m}_2} \setminus \mathcal{C}_1$, and so $\alpha I \notin \mathcal{C}_2$, s o

$$\ker \varphi = \mathcal{C}_1$$

and so φ is an injective homomorphism:

$$\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \to \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$$

Then by symmetry we have an injective homomorphism going the other way as well and so

$$\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1 \cong \mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$$

Note that the isomorphism is independent of choice of α, making it canonical, and for any fractional ideal I coprime to $\mathfrak{m}_1$ and $\mathfrak{m}_2$, we may as well choose $\alpha = 1$, in which use the coset of I in $\mathcal{I}_K^{\mathfrak{m}_1}/\mathcal{C}_1$ will be identified with the coset of I in $\mathcal{I}_K^{\mathfrak{m}_2}/\mathcal{C}_2$, completing the proof.

Corollary 4.2.4: Congruence Subgroup For Different Moduli

Let $\mathcal{C}$ be a congruence subgroup for two moduli $\mathfrak{m}_1, \mathfrak{m}_2$. Then

$$(\mathcal{C}, \mathfrak{m}_1) \cong (\mathcal{C}, \mathfrak{m}_2)$$

Proof **:**
exercise, follow from above proposition.

As a consequence, notice that each subgroup $\mathcal{I}_K$ lies in at most one equivalence class of congruence subgroup, and so we can view the equivalence relation $(\mathcal{C}_1, \mathfrak{m}_1) \sim (\mathcal{C}_2, \mathfrak{m}_2)$ as an equivalence relation on the congruence subgroups of $\mathcal{I}_K$, and write $\mathcal{C}_1 \sim \mathcal{C}_2$ unambiguously. Then each equivalence class of congruence subgroups uniquely determines a finite abelian group that is the quotient of a ray class group.

Now, we have that there can b at most one congruence subgroup for each modulus (as $\mathcal{C}_1 \sim \mathcal{C}_2 \Leftrightarrow \mathcal{C}_1 = \mathcal{C}_2$ when $\mathcal{C}_1, \mathcal{C}_2$ are congruence subgroups for the same modulus). Let us now find when there exists a congruence subgroup of a given modulus within an equivalence class

Lemma 4.2.5: Existence of Congruence subgroup

Let $\mathcal{C}_1$ be a congruence subgroup of modulus $\mathfrak{m}_1$ for a number field K¿ Then there exits a congruence subgroup $\mathcal{C}_2$ of modulus $\mathfrak{m}_2 \mid \mathfrak{m}_1$ equivalent to $\mathcal{C}_1$ if and only if

$$\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_1$$

in which case:

$$\mathcal{C}_2 = \mathcal{C}_1 \mathcal{R}_K^{\mathfrak{m}_2}$$

Proof **:**
As $\mathfrak{m}_2 \mid \mathfrak{m}_1$, $\mathcal{I}_K^{\mathfrak{m}_1} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$, so $\mathcal{C}_1 \subseteq \mathcal{I}_K^{\mathfrak{m}_1} \subseteq \mathcal{I}_K^{\mathfrak{m}_2}$. Now suppose $\mathcal{C}_1 \sim \mathcal{C}_1$ has modulus $\mathfrak{m}_2$. Then $|CI_K^{\mathfrak{m}_1} \cap \mathcal{C}_2 = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{C}_1$ and $\mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{C}_2$, so

$$\mathcal{I}_K^{\mathfrak{m}-1} \cap \mathcal{R}_K^{\mathfrak{m}-2} \subseteq \mathcal{C}_1$$

Giving the first claim. Now given the above subset, let $\mathcal{C}_2 := \mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2}$. Then $\mathcal{C}_2$ is a congruence subgroup of modulus $\mathfrak{m}_2$. Then:

$$\mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{C}_1(\mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2}) = \mathcal{I}_K^{\mathfrak{m}_1}\mathcal{C}_1\mathcal{R}_K^{\mathfrak{m}_2} = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$$

Hence $\mathcal{C}_1 \sim \mathcal{C}_2$. Then as the equivalence class of $\mathcal{C}_1$ contains *at most one* congruence subgroup of modulus $\mathfrak{m}_2$, if one exists it in fact *has* to be $\mathcal{C}_1 = \mathcal{C}_1\mathcal{R}^{\mathfrak{m}_2}$, as we sought to show.

Lemma 4.2.6: Congruence Subgroup and GCD

Let $\mathcal{C}_1 \sim \mathcal{C}_2$ be congruence subgroups of modulus $\mathfrak{m}_1, \mathfrak{m}_2$ respectively. Then there exists a congruence subgroup $\mathcal{C} \sim \mathcal{C}_1 \sim \mathcal{C}_2$ with $\mathfrak{n} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$

Proof **:**
Let $\mathfrak{m} = \operatorname{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ and take $\mathcal{D} = \mathcal{I}_K^{\mathfrak{m}_2} \cap \mathcal{C}_1 = \mathcal{I}_K^{\mathfrak{m}_1} \cap \mathcal{C}_2$. Then:

$$\mathcal{R}_K^{\mathfrak{m}} = CR_K^{\mathfrak{m}_1} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{D} \subseteq \mathcal{I}_K^{\mathfrak{m}}$$

Hence $\mathcal{D}$ is a congruence subgroup of modulus $\mathfrak{m}$. As:

$$\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{D} \qquad \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_2} \subseteq \mathcal{D}$$

by lemma 4.2.5 we have

$$\mathcal{D} \sim \mathcal{C}_1 \sim \mathcal{C}_2$$

Now, letting $\mathfrak{n} = \gcd(\mathfrak{m} - 1, \mathfrak{m}_2)$, if we show $\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}^{|}_K fn \subseteq \mathcal{D}$, by lemma 4.2.5 we are done.

Let $\mathfrak{a} = (\alpha) \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{n}}$. Choose $\beta \in K^{\mathfrak{m}} \cap K^{\mathfrak{m}_2,1}$ such that $\alpha\beta \in K^{\mathfrak{m}_1,1}$. Then $(\beta) \in \mathcal{D}$ and $\beta\mathfrak{a} \in \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{m}_1} \subseteq \mathcal{D}$, and so $\beta^{-1}\beta\mathfrak{a} = \mathfrak{a} \in \mathcal{D}$. Thus,

$$\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{n}} \subseteq \mathcal{D}$$

Thus $\mathcal{C} = \mathcal{D}\mathcal{R}_K^{\mathfrak{n}}$ is a congruence subgroup with modulus $\mathfrak{n}$, as we sought to show.

Corollary 4.2.7: Conductor Congruence Subgroup

Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K. Then here exists a unique congruence subgroup in the equivalence class of $\mathcal{C}$ whose modulus $\mathfrak{c}$ divides the modulus of every congruence subgroup equivalent to $\mathcal{C}$

***Proof* :**
Direct application of the above lemma

The $\mathfrak{c}$ is given a name:

Definition 4.2.8: Conductor of Congruence Subgroup

Let $\mathcal{C}$ be a congruence subgroup of a number field K. Then the unique $\mathfrak{c} = \mathfrak{c}(\mathcal{C})$ is called the *conductor* of $\mathcal{C}$. We say that $\mathcal{C}$ is *primitive* if $\mathcal{C} = \mathcal{C}\mathcal{R}_K^{\mathfrak{c}}$.

Proposition 4.2.9: Conductor of Subgroup of Congruence Subgroup

Let $\mathcal{C}$ be a primitive congruence subgroup for a modulus $\mathfrak{m}$ for a number field K. Then $\mathfrak{m}$ is the conductor for every congruence subgroup of $\mathfrak{m}$ contained in $\mathcal{C}$, in particular, $\mathfrak{m}$ is the conductor of $\mathcal{R}_K^{\mathfrak{m}}$

***Proof* :**
Let $\mathcal{C}_0 \subseteq \mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ and let $\mathfrak{c}$ be its conductor. THen $\mathfrak{c} \mid \mathfrak{m}$ and

$$\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{R}_K^{\mathfrak{c}} \subseteq \mathcal{C}_0 \subseteq \mathcal{C}$$

Then by lemma 4.2.5 there is a congruence subgroup of modulus $\mathfrak{c}$ equivalent to $\mathcal{C}$, hence $\mathfrak{m} \mid \mathfrak{c}$, but then $\mathfrak{c} = \mathfrak{m}$, completing the proof.

Note that the modulus $\mathfrak{m}$ occurs as a conductor if and only if $\mathcal{R}_K^{\mathfrak{m}}$ is primitive. This need not hold in general

Example 4.4: Counter Example

Take $K = \mathbb{Q}$, $\mathfrak{m} = (2)$. Then the conductor of $\mathcal{R}_{\mathbb{Q}}^{(2)} = \mathcal{I}_{\mathbb{Q}}^{(2)}$ is (1) as

$$\mathcal{R}_{\mathbb{Q}}^{(2)} \cap \mathcal{I}_{\mathbb{Q}}^{(1)} = \mathcal{I}_{\mathbb{Q}}^{(1)} \cap \mathcal{I}_{\mathbb{Q}}^{(2)} \qquad \Rightarrow \qquad \mathcal{R}_{\mathbb{Q}}^{(2)} \sim \mathcal{I}_{\mathbb{Q}}^{(1)}$$

Thus, (2) is *not* the conductor of any congruence subgroup of $\mathbb{Q}$.

4.2.2 Ray Class Character

We shall now look at the generalized distribution of primes. Recall the Dirichlet density gave us a way of measuring the density of certain sets of primes. Given a congruence of subgroups $\mathcal{C}$ for a modulus $\mathfrak{m}$, when it exists, we will compute a new Dirichlet density $d(\mathcal{C})$ of the set of primes ideals in $\mathfrak{p} \in \mathcal{I}_K^{\mathfrak{m}}$ that lie in $\mathcal{C}$. To that end:

Definition 4.2.10: Ray Class Character

Let K be a number fields, $\chi : \mathcal{I}_K \to \mathbb{C}$ a totally multiplicative function with finite image (so $\mathrm{ch}(\mathcal{O}_K) = 1$). If $\mathfrak{m}$ is a modulus for K such that $\chi^{-1}(U(1)) = \mathcal{I}_K^{\mathfrak{m}}$ and $\mathcal{R}_K^{\mathfrak{m}} \subseteq \ker\chi$, we say that χ is a *ray class character* of modulus $\mathfrak{m}$, and its kernel is the congruence subgroup of modulus $\mathfrak{m}$. The extension by zero f a character is then the finite abelian group $\mathrm{Cl}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}}/\mathcal{R}_K^{\mathfrak{m}}$ die fiend by setting $\chi(I) = 0$ for $I \notin \mathcal{I}_K^{\mathfrak{m}}$.

This entire proof's really cool and generalizes the result about splitting primes, this is a must to write down properly.

Put all the build-up here!

Theorem 4.2.11: Dirichlet Density For Number Fields

Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K and let $n = [\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$. Then the set of primes $\{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density:

$$d(\mathcal{C}) = \begin{cases} \frac{1}{n} & L(1,\chi) \neq 0 \text{ forall } \chi \neq \nVdash \text{ in } X(\mathbb{C}) \\ 0 & \text{otherwise} \end{cases}$$

Corollary 4.2.13 shall show that in fact $d(\mathcal{C}) = 1/n$ always, which shall be easier to show after this result is proven.

Proof **:**
MIT Lec 22 p.7

Corollary 4.2.12: Dirichlet Density when Multiplying by Ideal

Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K and let $n = [\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$. For every ideal $I \in \mathcal{I}_K^{\mathfrak{m}}$, the set $\{\mathfrak{p} \in I\mathcal{C}\}$ has Dirichlet density:

$$d(I\mathcal{C}) = \begin{cases} \frac{1}{n} & L(1,\chi) \neq 0 \text{ forall } \chi \neq \nVdash \text{ in } X(\mathbb{C}) \\ 0 & \text{otherwise} \end{cases}$$

Proof **:**
(The proof will be very similar, an indicator function for I is used, namely $\chi(I)^{-1}$, see the MIT notes if needed)

Corollary 4.2.13: Dirichlet Density For Number Fields Always Exists

Let $\mathcal{C}$ be a congruence subgroup of modulus $\mathfrak{m}$ for a number field K and let $n[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$. Then for every ideal, $I \in \mathcal{I}_K^{\mathfrak{m}}$, the set $\{\mathfrak{p} \in I\mathcal{C}\}$ has Dirichelt density $\frac{1}{n}$, and for every $\chi \neq \nVdash$ in $X(\mathcal{C})$, $L(1,\chi) \neq 0$

Proof **:**
MIT notes chap 22 p.8

Corollary 4.2.14: Comparing Dirichlet Density With Split Primes

Let L/K be an abelian extension of number fields and let $\mathcal{C}$ be a congruence subgroup for a modulus $\mathfrak{m}$ of K. Then if $\operatorname{Spl}(L) \preceq \{\mathfrak{p} \in \mathcal{C}\}$, then:

$$[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}] \leq [L : K]$$

and $[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}] = [L : K]$ if $\operatorname{Spl}(L) \sim \{\mathfrak{p} \in \mathcal{C}\}$

Proof **:**
Recall that $\operatorname{Spl}(L)$ has polar density $1/[L : K]$, which is also the Dirichlet density. We just showed the set $\{\mathfrak{p} \in \mathcal{C}\}$ has Dirichlet density $1/[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]$, and by assumption $\operatorname{Spl}(L) \preceq \{\mathfrak{p} \in \mathcal{C}\}$ hence:

$$\frac{1}{[L : K]} = d(\operatorname{Spl}(L)) \leq d(\mathcal{C}) = \frac{1}{[\mathcal{I}_K^{\mathfrak{m}} : \mathcal{C}]}$$

completing the proof.

4.2.3 Build-up to Artin Reciprocity

We shall now show how to reduce the proof of the Artin reciprocity. The idea is that there is a way of characterizing the appropriate group by means of the norm (i.e. the norm group) which shall have the right properties to satisfy the Artin map kernel condition. We start by boxing the following:

Definition 4.2.15: Conductor of Abelian Extension

Let L/K be a finite abelian extension of local fields. THen the *conductor* of L/K, denoted $\mathfrak{c}(L/K)$ is given as follows:

1. If K is Archimedean, then if $K \cong \mathbb{R}$ we have $\mathfrak{c}(L/K) = 1$, and if $K \cong \mathbb{C}$ we have $\mathfrak{c}(L/K) = 0$

2. If K is nonarchimedean, and $\mathfrak{p}$ is a maximal ideal of its valuation ring $\mathcal{O}_K$, then:

$$\mathfrak{c}(L/K) = \min\left\{n \ : \ 1 + \mathfrak{p}^n \subseteq \operatorname{Nm}_{L/K}(L^\times)\right\}$$

where we set $1 + \mathfrak{p}^0 = \mathcal{O}_K^\times$. If L/K is a finite abelian extension of global fields, then its conductor is the modulus:

$$\mathfrak{c}(L/K) : M_K \to \mathbb{Z} \qquad \nu \mapsto \mathfrak{c}(L_w/K_\nu)$$

Like before, we may view the finite part of $\mathfrak{c}(L/K)$ as an $\mathcal{O}_K$-ideal, and the infinite part as the subset of ramified infinite places. Note too that conductors are defined even when the extension L/K is *not* abelian, which becomes important went looking at galois representation theory.

Proposition 4.2.16: Valuation of Conductor

Let L/K be a finite abelian extension of local or global fields. Then for each prime $\mathfrak{p} \subseteq K$,

$$\nu_{\mathfrak{p}}(\mathfrak{c}(L/K)) = \begin{cases} 0 & \text{iff } \mathfrak{p} \text{ is unramified} \\ 1 & \text{iff } \mathfrak{p} \text{ ramifies tamely} \\ \geq 2 & \text{iff } \mathfrak{p} \text{ is ramifies wildly} \end{cases}$$

Proof **:**
exercise worth doing! Sketch: Archimedean is naturally trivial. For local case recall that $K^\times = \mathbb{Z} \times \mathcal{O}_K^\times = \mathbb{Z} \times (1 + \mathfrak{p}^0)$, $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)^\times$ is surjective with kernel $1 + \mathfrak{p}^1$, and recall proposition 1.1.7

Now, when L/K is totally unramified and local that $K^\times/\mathrm{Nm}_{L/K}(L^\times) \cong \mathrm{Gal}_K(L)$ and if L/K is totally ramified that $K^\times/\mathrm{Nm}_{L/K}(L^\times) \cong \mathcal{O}_K^\times/(\mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$.

Finally, if L/K is tame, $\mathrm{Nm}_{L/K}(1 + \mathfrak{q}) = 1 + \mathfrak{p}$, and is not equal in the wild case.

Note that the finite part of the conductor of an abelian extension divides the discriminant ideal and is divisible by the same set of prime ideals! However, the valuation of the conductor at these primes is usually smaller than the discriminant

Example 4.5: Comparing Size of Conductor Vs Discriminant
Take $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. It's discriminant is $(p)^{p-2}$, but it's conductor is $(p)\infty$.

Lemma 4.2.17: Conductor and Subfields

Let L_1/K and L_2/K be two finite abelian extensions of a local or global field K. Then if $L_1 \subseteq L_2$, $\mathfrak{c}(L_1/K) \mid \mathfrak{c}(L_2/K)$

Proof **:**
If $K \cong \mathbb{R}, \mathbb{C}$, the result is immediate. In the non-Archimedean case recall:

$$\mathrm{Nm}_{L_2/K}(L_2^\times) = \mathrm{Nm}_{L_2/K}(\mathrm{Nm}_{L_2/L_1}(L_2^\times)) \subseteq N_{L_1/K}(L_1^\times)$$

We shall now find a good representation of the kernel of the Artin map $\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}_K(L)$. First, recall from [ChwNAc] that we can define the norm map $\mathrm{Nm}_{L/K} : \mathcal{I}_L \to \mathcal{I}_K$ via:

$$\prod_i \mathfrak{q}_i^{n_1} \mapsto \prod_i \mathfrak{p}_i^{n_i f_i}$$

Define from this the following:

Definition 4.2.18: Norm Group

Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by the conductor of L/K. Then the *norm group* or *Takagi group* associated to $\mathfrak{m}$ is the congruence subgroup:

$$T_{L/K}^{\mathfrak{m}} = \mathcal{R}_K^{\mathfrak{m}} \mathrm{Nm}_{L/K}(\mathcal{I}_L^{\mathfrak{m}})$$

Proposition 4.2.19: Relating Norm Group and Kernel of Artin Map

Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by the conductor of L/K. Then

$$(\mathcal{R}_K^{\mathfrak{m}} \subseteq) \ker \psi_{L/K}^{\mathfrak{m}} \subseteq T_{L/K}^{\mathfrak{m}}$$

Proof **:**
Take $\mathfrak{p} \subseteq K$ that is in $\ker \psi_{L/K}^{\mathfrak{m}}$. Then $\mathfrak{p}$ is coprime to $\mathfrak{m}$, and splits completely in L, so $e_{\mathfrak{p}} = f_{\mathfrak{p}} = 1$. Certainly there is at least one prime $\mathfrak{q} \subseteq L$ above $\mathfrak{p}$, and we know

$$\mathrm{Nm}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}} = \mathfrak{p}$$

But then:

$$\mathfrak{p} \in \mathrm{Nm}_{L/K}(\mathcal{I}_L^{\mathfrak{m}}) \subseteq T_{L/K}^{\mathfrak{m}}$$

completing the proof.

We next have the following very important result relating the sizes of field extensions and the index of the norm group in the ideal group:

Theorem 4.2.20: Fundamental Inequality I

Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus for K divisible by the conductor of L/K. Then:‘

$$[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}] \leq [L : K]$$

Proof **:**
As $T_{L/K}^{\mathfrak{m}}$ is a congruence subgroup that contains all primes of K that split completely in L by the above proposition, this follows by corollary 4.2.14.

From this, we reduced the proof of Artin reciprocity to showing $T_{L/K}^{\mathfrak{m}} \subseteq \ker \psi_{L/K}^{\mathfrak{m}}$ for any modulus $\mathfrak{m}$ divisible by the conductor L/K (so that with proposition 4.2.19 we would get $T_{L/K}^{\mathfrak{m}} = \ker \psi_{L/K}^{\mathfrak{m}}$). Let us formulate what we're proving with this new insight:

Theorem 4.2.21: Fundamental Theorem of Class Field Theory (Ideal-Theoretic)

1. **Existence**: The ray class field $K(\mathfrak{m})$ exists
2. **Completeness**: If L/K i as finite abelian extension, then $L \subseteq K(\mathfrak{m})$ if and only if $\mathfrak{c}(L/K) \mid \mathfrak{m}$. In particular, every finite abelian L/K lies in a ray class field.
3. **Artin Reciprocity**: For each subextension L/K of $K(\mathfrak{m})$, $\ker \psi^{\mathfrak{m}}_{L/K} = T^{\mathfrak{m}}_{L/K}$ with conductor $\mathfrak{c}(L/K) \mid \mathfrak{m}$ and a canonical isomorphism:

$$\mathcal{I}^{\mathfrak{m}}_K / T_{L/K} \cong \mathrm{Gal}_K(L)$$

We thus get a commutative diagram of canonical bijections:

$$\begin{tikzcd}
\{\text{Abelian } L/K \text{ with } \mathfrak{c}(L/K \mid \mathfrak{m}\} \arrow[r, "L \mapsto T^{\mathfrak{m}}_{L/K}"] \arrow[d, "L \mapsto \mathrm{Gal}_K(L)"'] & \{\text{congruence subgroups } \mathcal{C} \subseteq \mathcal{I}^{\mathfrak{m}}_K\} \arrow[d, "\mathcal{C} \mapsto \mathcal{I}^{\mathfrak{m}}_K/\mathcal{C}"] \\
\{\text{quotients of } \mathrm{Gal}_K(K(\mathfrak{m}))\} & \{\text{quotients of } \mathrm{Cl}^{\mathfrak{m}}_K\} \arrow[l, "\psi^{\mathfrak{m}}_{L/K}"]
\end{tikzcd}$$

These are some cool facts, but they seem out of place here. I'll write them down now, but be sure to put them in the right spot

1. For the case for the trivial modulus, we shall see that the *Hilbert Class Field* (definition 1.7.10) will be the ray class field.
2. It shall be shown that in this case the Hilbert class field will be a finite extension of K. Note that infinite unramified extensions exist (and are necessarily then nonabelian (recall infinite galois groups)
3. Such a construction would ceom from a tower of Hilbert class fields. We would start with $K_0 = K$ and then construct the Hilbert class field K_{n+1} of K_n. This would give a tower of finite abelian extensions:
$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$$
Taking $L = \cup_n K_n$, either get that some K_n will have class number one and so $K_N = K_n$ for all $N \geq n$, stabilizing the tower, or this does not happen. In 1964, Golod and Shafarevich showed there are infinite towers of Hilbert class fields, an example being
$$K_0 = \mathbb{Q}(\sqrt{-30030}) = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 11 \cdot 13})$$
4. It was shown that imaginary quadratic field with discriminant $|D| \leq 420$ all have finite Hilbert class field towers that stabilize at either K_2 or K_3.
5. Extensions arising from Hilbert class fields are necessarily solvable, however there are infinite nonsolvable unramified extensions, it was shown that the bi-quadratic extension:
$$\mathbb{Q}(\sqrt{17601097}, \sqrt{17380678572169893})$$
has class number one and its maximal unramified extension is an infinite extension.

4.2.4 Build-up: some Tate Cohomology

Recall from [ChwNAc, chapter 28.1] that we defined group cohomology and found how to compute in the case of finite groups. We defined the *standard resolution*, found ways to compute it, and showed that the cohomology and homology share many properties. We saw there was an isomorphism between $H_0(G, B)$ and $H^0(G, B)$ for the right choice of B (namely either the induced or coinduced representation of A). There is in fact another natural map:

$$A \cong H_0(G, A) \to H^0(G, A) \cong A$$
$$a \mapsto \sum_{g \in G} ga$$

where a is a representative. This map shall let us naturally link the cohomology and homology of group Cohomologies with minimal modification to insure the induced and coinduced G-modules have trivial homologies and Cohomologies in all degrees. Let us characterize this map further:

Definition 4.2.22: Norm Element

The element $N_g = \sum_{g \in G} \in \mathbb{Z}[G]$ is called the *Norm Element*.

Lemma 4.2.23: Norm Map Endomorphism

Let A be a G-module and $N_G : A \to A$ a G-module endomorphism given by $a \mapsto N_G a$. Then:

$$I_G A \subsetneq \ker N_G \qquad \mathrm{im} N_G \subsetneq A^G$$

Hence, N_G induces a morphisms:

$$\hat{N}_G : A_G \to A^G$$

of trivial G-modules .

Proof **:**
As $gN_G = N_G$ for all $g \in G$, $N_G \subsetneq A^G$, and furthermore $N_g(g-1) = 0$ for all $g \in G$, so N_g annihilates the augmentation ideal I_G so $I_G A \subsetneq] ker N_G$, completing the proof.

We thus define the following new cohomology:

Definition 4.2.24: Tate Cohomology

Let A be a G-module for a finite group G. Then for $n \geq 0$, the *Tate cohomology* and *Tate Homology* groups are:

$$\hat{H}^n(G, A) = \begin{cases} \mathrm{coker} \hat{N}_G & n = 0 \\ H^n(G, A) & n > 0 \end{cases} \qquad \hat{H}_n(G, A) = \begin{cases} \ker \hat{N}_G & n = 0 \\ H_n(G, A) & n > 0 \end{cases}$$

And:

$$\hat{H}^{-n}(G, A) = \hat{H}_{n-1}(G, A) \qquad \hat{H}_{-n}(G, A) = \hat{H}^{n-1}(G, A)$$

Note that $\hat{H}^0(G,A)$ is the quotient of A^G with the norm map (particularly, the largest trivial G-module in A), and $\hat{H}_0(G,A)$ is a submodule of A_G (particularly, the largest trivial G-module quotient of A). Hence, any G-module homomorphism induces natural morphism of Tate Cohomologies and homologies in degree $n=0$ (Note that the rest of the degree remains the same as what we've covered in the usual group cohomology). Thus, $\hat{H}^n(G,-)$ and $\hat{H}_n(G,-)$ are both [additive[3]]functors to the abelian category. By the symmetry, we have that Tate cohomology and homology are linked, and so we shall just stick to looking at Tate cohomology.

Let us first show that this linking does indeed give a cohomological functor:

Theorem 4.2.25: Tate Cohomology Functor

Let G be a finite group. Then every short exact sequence of G-module

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

induces a long exact sequence of Tate cohomology groups:

$$\cdots \to \hat{H}^n(G,A) \xrightarrow{\hat{\alpha}^n} \hat{H}^n(G,B) \xrightarrow{\hat{\beta}^n} \hat{H}^n(G,C) \xrightarrow{\hat{\delta}^n} \hat{H}^{n+1}(G,A) \to \cdots$$

and, equivalently, a long exact sequence of Tate homology groups:

$$\cdots \to \hat{H}_n(G,A) \xrightarrow{\hat{\alpha}_n} \hat{H}_n(G,B) \xrightarrow{\hat{\beta}_n} \hat{H}_n(G,C) \xrightarrow{\hat{\delta}_n} \hat{H}_{n-1}(G,A) \to \cdots$$

Furthermore, commutative diagrams of short exact sequence of G-modules induce a commutative diagram of long exact sequences of Tate (co)homology groups

***Proof* :**
All has been proven except the new connection in the middle, namely at the places

$$\hat{H}^0(G,0) = \hat{H}_{-1}(G,-) \qquad \hat{H}_0(G,-) = \hat{H}^{-1}(G,-)$$

This shall be skipped as it is pretty standard diagram chasing proof. If you would like to see the details look at MIT notes p.238.

Corollary 4.2.26: Tate (co)homology On (co)induced Groups

Let G be a finite group and A a free $\mathbb{Z}[G]$-module. Then

$$\hat{H}_n(G,A) = \hat{H}^n(G,A) = 0 \qquad \forall n \in \mathbb{Z}$$

***Proof* :**
exercise

Let us now look at the Tate cohomology of cyclic groups, as it will be important for the Artin Reciprocity proof. Let $G = \langle g \rangle$ be a finite cyclic group. Then $I_G = \langle g-1 \rangle$ (as an ideal of $\mathbb{Z}[G]$).

[3] see lemma ref:HERE

Then for any G-module A, we may create the free resolution:

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_g} \mathbb{Z}[g] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

As I_G is principal, $\text{im}_G = \ker(g-1)$, and so this sequence is exact. Next, as G is abelian, $\mathbb{Z}[G]$ is commutative, and so there is no difference between a left and right $\mathbb{Z}[G]$-module. In particular, we can view any G-module A the following as G-modules: $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$ and $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$ with the G-module action being:

$$g(h \otimes a) = gh \otimes a = h \otimes ga \qquad (g\varphi)(h) = \varphi(gh)$$

Note the importance of working with a commutative group G for these to be well-defined.

Theorem 4.2.27: Characterizing Tate Cohomology Groups with Cyclic Group

Let $G = \langle g \rangle$ be a finite cyclic group and A a G-module. THen for all $n \in \mathbb{Z}$,

$$\hat{H}^{2n}(G, A) \cong \hat{H}_{2n-1}(G, A) \cong \hat{H}^0(G, A)$$
$$\hat{H}_{2n}(G, A) \cong \hat{H}^{2n-1}(G, A) \cong \hat{H}_0(G, A)$$

***Proof* :**
First, recall that:

$$\text{Hom}_{\mathbb{Z}[G]}(G, A) \cong A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A$$

via $\varphi \mapsto \varphi(1)$ and $a \mapsto 1 \otimes a$ which are isomorphisms which preserve "g-multiplication" give endomorphisms:

$$(g\varphi)(1) = g\varphi(1) \qquad 1 \otimes ga = g(1 \otimes a)$$

Now, take the free resolution

$$\cdots \to \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{N_g} \mathbb{Z}[g] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

Then compute $H^n(G, A)$ using the cochain complex:

$$0 \to A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \xrightarrow{N_G} A \to \cdots$$

and the chain complex:

$$\cdots \to A \xrightarrow{N_G} A \xrightarrow{g-1} A \xrightarrow{N_G} A \xrightarrow{g-1} A \to 0$$

Next, recall that $A^G = \ker(g-1)$ for all $n \geq 1$, hence:

$$H^{2n}(G, A) = H_{2n-1}(G, A) = \ker(g-1)/\text{im}(N_G) = \text{coker}\hat{N}_G = \hat{H}^0(G, A)$$

Hence, $\hat{H}^{2n}(G, A) = \hat{H}_{2n-1}(G, A) = \hat{H}^0(G, A)$ for all $n \in \mathbb{Z}$. As $\hat{H}^{-2n}(G, A) = \hat{H}_{2n-1}(G, A)$. Thus, $\hat{H}_{-2n+1} = \hat{H}^{2n}$ for all $n \geq 0$.

Similarly, we have $\text{im}(g-1) = I_G$ for all $n \geq 1$, and so:

$$H_{2n}(G, A) = H^{2n-1}(G, A) = \ker(N_G)/\text{im}(g-1) = \ker \hat{N}_G = \hat{H}_0(G, A)$$

Hence, $\hat{H}_{2n}(G, A) = \hat{H}^{2n-1}(G, A) = \hat{H}_0(G, A)$ for all $n \in \mathbb{Z}$. As $\hat{H}_{-2n}(G, A) = \hat{H}^{2n-1}(G, A)$. Thus, $\hat{H}^{-2n+1} = \hat{H}_{2n}$ for all $n \geq 0$, completing the proof.

Thus, given G is a finite cyclic group, all the Tate (co)homology groups are determined by $\hat{H}^0(G, A)$ and $\hat{H}_0(G, A)$! This complete determination by two groups motivates the following definition:

Definition 4.2.28: Herband Quotient

Let G be a finite cyclic group and let A be a G-module. Then define:

$$h^n(A) = h^n(G, A) = \#\hat{H}^n(G, A)$$
$$h_n(A) = h_n(G, A) = \#\hat{H}_n(G, A)$$

When $h^0(A), h_0(A) < \infty$ are both finite, Then the *Herband quotient* is:

$$h(A) = \frac{h^0(A)}{h_0(A)} \in \mathbb{Q}$$

For a future proof, we put down the following corollary:

Corollary 4.2.29: Exact Hexagon

Let G be a finite cycle group. Then given an exact sequence of G-modules:

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

There is a corresponding exact hexagon:

$$\begin{tikzcd}
 & \hat{H}^0(G, A) \arrow[r, "\hat{\alpha}^0"] & \hat{H}^0(G, B) \arrow[dr, "\hat{\beta}^0"] & \\
\hat{H}_0(G, C) \arrow[ur, "\hat{\delta}_0"] & & & \hat{H}^0(G, C) \arrow[dl, "\hat{\delta}_0"] \\
 & \hat{H}_0(G, B) \arrow[ul, "\hat{\beta}_0"] & \hat{H}_0(G, A) \arrow[l, "\hat{\alpha}_0"'] &
\end{tikzcd}$$

***Proof* :**
put together the above results.

Corollary 4.2.30: Herband Quotient Additive Function

Let G be a finite cycle group. Then given an exact sequence of G-modules:

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

If any two $h(A), h(B), h(C)$ are defined, so is the third, and

$$h(B) = h(A)h(C)$$

***Proof* :**
By using the exact hexagon, we can compute:

$$h^0(A) = \#\hat{H}^0(G,A) = \#\ker\hat{\alpha}^0 \#\hat{\alpha}^0 = \#\ker\alpha^{\#}\ker\beta^0$$

And, repeating the same for $h^0(B)$ and $\hat{H}^1(G,B)$, we get:

$$h^0(A)h^0(C)h_0(B) = \#\ker\hat{\alpha}^0\#\ker\hat{\delta}^0\#\ker\hat{\alpha}_0\#\ker\hat{\beta}_0\#\ker\hat{\delta}_0\#\ker\hat{\alpha}^0 = h^0(A)h^0(C)h_0(B)$$

Similarly for $\hat{H}^0(G,B)$, $\hat{H}_0(G,A)$, $\hat{H}_0(G,C)$, we get:

$$h^0(B)h_0(A)h_0(C) = \#\ker\hat{\beta}^0\#\ker\hat{\delta}^0\#\ker\hat{\alpha}_0\#\ker\hat{\beta}_0\#\ker\hat{\delta}_0\#\ker\hat{\alpha}^0 = h^0(A)h^0(C)h_0(B).$$

Now, if any two $h(A), h(B), h(C)$ are defined, then we see that *at least 4* of the groups in the exact hexagon are finite, and the remaining two (non-adjacent) are forced to be finite. Then re-arranging, we get:

$$h(B) = h(A)h(C)$$

as we sought to show.

Corollary 4.2.31: Special Case of Herband Quotient Additive Function

Let G be a finite cyclic group and let A, B be G-modules. Then if $h(A)$ and $h(B)$ are defined,

$$h(A \oplus B) = h(A)h(B)$$

***Proof* :**
Take the short exact sequence

$$0 \to A \to A \oplus B \to B \to 0$$

and apply corollary 4.2.30.

Corollary 4.2.32: Herband Quotient for Finite and induced Groups

Let G be a finite cyclic group. Then if A is an induced or finite G-module, then

$$h(A) = 1$$

***Proof* :**
Start with A being an induced G-module. Then by corollary 4.2.26 we get $h_0(A) = h^0(A) = h(A) = 1$. Next, if A is finite, then we get the exact sequence:

$$0 \to AG \to A \xrightarrow{g-1} A \to A_G \to 0$$

Which give s$\#A^G = \#\ker(g-1) = \#\text{coker}(g-1) = \#A_G$. Hence:

$$h_0(A) = \#\ker\hat{N}_G = \#\text{coker}\hat{N}_G = h^0(A)$$

giving $h(A) = 1$, completing the proof.

Corollary 4.2.33: Herband Quotient For Finitely Generated Groups

Let G be a finite cyclic group. Then if A is a G-module that is also a finitely generated abelian group, then:

$$h(A) = h(A/A_{\text{tor}})$$

if either is defined.

***Proof* :**
Take the short exact sequence:

$$0 \to A_{\text{tor}} \to A \to A/A_{\text{tor}} \to 0$$

Corollary 4.2.34: Herband Quotient For Trivial G-module With f.g. Group

Let G be a finite cyclic group. Then if A is a trivial G-module that is also a finitely generated abelian group, then:

$$h(A) = (\#G)^r$$

where r is the rank of A

***Proof* :**
As A is finitely generated, $A/A_{\text{tor}} \cong \mathbb{Z}^r$ for appropriate r where we take $\mathbb{Z}$ with the trivial G-module structure. Then $\mathbb{Z}_G = \mathbb{Z} = \mathbb{Z}^G$, and so $\hat{N}_G : \mathbb{Z}_G \to \mathbb{Z}^G$ is multiplication by $\#G$. Thus,

$$h(Z) = \#\text{coker}\hat{N}_G / \# \ker \hat{N}_G = \#G$$

Now use induction on corollary 4.2.31.

Corollary 4.2.35: Herband Quotient and G-module Morphism

Let G be a finite cyclic group and let $\alpha : A \to B$ be a morphism of G-modules with finite kernel and cokernel. Then if either $h(A)$ or $h(B)$ is defined,

$$h(A) = h(B)$$

***Proof* :**
Apply the additive function property to the exact seuqences:

$$0 \to \ker\alpha \to A \to \text{im}\alpha \to 0$$
$$0 \to \text{im}\alpha \to B \to \text{coker}\alpha \to 0$$

which, by using the finiteness so that $h(\ker\alpha) = h(\text{coker}\alpha) = 1$ we get:

$$h(A) = h(\ker\alpha)h(\text{im}\alpha) = h(\text{im}\alpha) = h(\text{im}\alpha)h(\text{coker}\alpha) = h(B)$$

completing the proof.

Corollary 4.2.36: Herband Quotient and Finite-index Submodules

Let G be a finite cyclic group and let $A \subseteq B$ be a sub G-modules with finite index. Then if either $h(A)$ or $h(B)$ is defined,

$$h(A) = h(B)$$

Proof **:**
Use corollary 4.2.35 on the inclusion $A \to B$.

4.3 Artin Reciprocity: Unramified Case

We now return to proving Artin reciprocity. Recall that it was proven in theorem 4.2.20 that:

$$[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}] \leq [L : K] = \mathcal{I}_K^{\mathfrak{m}} : \ker \psi_{L/K}^{\mathfrak{m}}]$$

We must now prove that:

$$[\mathcal{I}_K^{\mathfrak{m}} : T_{L/K}^{\mathfrak{m}}] \geq [L : K]$$

which would given the isomorphism:

$$\mathcal{I}_K^{\mathfrak{m}} / T_{L/K}^{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}_K(L)$$

We shall first prove it in the special case of a cyclic extension L/K when $\mathfrak{m}$ is trivial (so that L/K is unramified), and then generalize for all unramified abelian extensions.

4.3.1 Cyclic Case

Let L/G be a finite cyclic extension with galois group G. Then note that $L, L^\times, \mathcal{O}_L, \mathcal{O}_L^\times, \mathcal{I}_L, \mathcal{P}_L$ are all G-modules as we may define a natural G-action on them.Let us compute the Tate cohomology of these G-modules and the Herband quotients $h(A)$. The Herband quotient (if the quantities are finite) is given by:

$$\hat{H}^0(A) = \hat{H}^0(G, A) = \mathrm{coker}\hat{N}_G = A^G / \mathrm{im}\hat{N}_G = \frac{A[\sigma - 1]}{N_G(A)}$$

$$\hat{H}_0(A) = \hat{H}_0(G, A) = \ker \hat{N}_G = A_G[\hat{N}_G] = \frac{A[N_G}{(\sigma - 1)A}$$

Let us find the norm element. For the multiplicative groups $\mathcal{O}_L^\times$, $L^\times$, $\mathcal{I}_L$, $\mathcal{P}_L$, the norm element $N_G = \sum_i^n \sigma^i$ will correspond to the action of the field norm $N_{L/K}$ and ideal norm $N_{L/K}$ that we've defined previously, given we identify the codomain of the norm map with a subgroup of its domain (i.e. Identifying $L^\times$ and $\mathcal{O}_L^\times$ with $K^\times$ and $\mathcal{O}_K^\times$ via inclusion, and identifying $\mathcal{I}_K$ to $\mathcal{I}_L$ via the inclusion $\mathcal{I}_K \hookrightarrow \mathcal{I}_L$, which restricts to a map $\mathcal{P}_K \hookrightarrow \mathcal{P}_L$, as when extending ideals we may get more principal ideals[4]). We may thus think of the norm map on $\mathcal{I}_L$ as taking the field norm which takes an element of $\mathcal{I}_L$ and gives an element $\mathcal{I}_K$ which corresponds to the map $I \mapsto I^{\#G}$, in which case $\mathcal{I}_K$ is a subgroup of the G-invariants $\mathcal{I}_L^G$ (namely, as L/K is unramified!).

[4] Review the number theory notes in [ChwNAc] if this is unfamiliar

To un-clutter notation, we shall use N to denote both the (relative) field norm $N_{L/K}$ and the ideal norm $N_{L/K}$. Let us recall the following from field theory

Lemma 4.3.1: Character Independence

Let L/K be a finite extension of fields. THen the set $\mathrm{Aut}_K(L)$ is a linearly independent susbset of the set of L-vector space functions $L \to L$

Proof **:**
see [ChwNAc, chapter 18]

Theorem 4.3.2: Trivial Tate Cohomology for L/K

Let L/K be a finite galois extension with $G = \mathrm{Gal}_K(L)$, and for any G-module A, let $\hat{H}^n(A) = \hat{H}^n(G, A)$. Then:

1. $\hat{H}^0(L)$ and $\hat{H}^1(L)$ are trivial
2. $\hat{H}^0(L^\times) \cong K^\times N(L^\times)$ and $\hat{H}^1(L^\times)$ are trivial

Proof **:**

1. First, by definition $L^G = K$, the trace map $T : L \to K$ is not identically zero as L/K is separable and is furthermore surjective, and $N_G(L) = T(L) = K$. So $\hat{H}^0(L) = K/K = 0$

   For $\hat{H}^1(L)$, take $\alpha \in L$. Then $T(\alpha) = \sum_{\tau \in G} \tau(\alpha) = 1$. Consider a 1-cocycle $f : G \to L$ so that $f(\sigma\tau) = f(\sigma) + \sigma(f(\tau))$. Let $\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha)$. Then for all $\sigma \in G$:

   $$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} (f(\sigma\tau) - f(\sigma))(\sigma\tau)(\alpha) = \sum_{\tau \in G} (f(\tau) - f(\sigma))\tau(\alpha) = \beta - f(\sigma),$$

2. For the multiplicative group, first note that $(L^\times)^G = K^\times$, and so $\hat{H}^0(L^\times) = K^\times / N_G L^\times = K^\times / N(L^\times)$. For $\hat{H}^1(L^\times)$, take $f : G \to L^\times$, in particular $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$. Then by the linear independence of characters (lemma 4.3.1), $\alpha \mapsto \sum_{\tau \in G} f(\tau)\tau(\alpha)$ is not the zero map. Now, let $\beta = \sum_{\tau \in G} f(\tau)\tau(\alpha) \in L^\times$ be a nonzero element in its image. Then for all $\sigma \in G$:

   $$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) = \sum_{\tau \in G} f(\sigma\tau)f(\sigma)^{-1}(\sigma\tau)(x) = f(\sigma)^{-1} \sum_{\tau \in G} f(\tau)\tau(\alpha) = f(\sigma)^{-1}\beta,$$

   so $f(\sigma) = \beta/\sigma(\beta)$, and so f is a coboundary, so $\hat{H}^1(L^\times) = H^1(L^\times)$ is trivial. Thus, $f(\sigma) = \beta - \sigma(\beta)$, implying f is a 1-coboundary, letting us conclude that $\hat{H}^1(L) = H^1(L)$ is trivial, as we sought to show.

This gives the famous Hilbert Theorem 90 in cohomological form

Theorem 4.3.3: Hilbert Theorem 90

Let L/K be a finite cyclic extension with Galois group $\mathrm{Gal}_K(L) = \langle\sigma\rangle$. Then $N(\alpha) = 1$ if and only if $\alpha = \beta/\sigma(\beta)$ for some $\beta \in L^\times$

Proof **:**
By theorem 4.2.27

$$\hat{H}^1(L^\times) \cong \hat{H}^{-1}(L^\times) = \hat{H}_0(L^\times) = L^\times[N_G]/(\sigma - 1)(L^\times)$$

And so by theorem 4.3.2

$$L^\times[N_G] = (\sigma - 1)L^\times$$

giving us the result, as we sought to show.

Let us now compute the Herband quotient for $\mathcal{O}_L^\times$ in the case that L/K is a finite cyclic extension of number fields. For the following, recall the discussion in section 2.3 about infinite primes in number fields. We shall use the notation from that section for the following:

Theorem 4.3.4: Herband Quotient For Units of Ring of Integers

Let L/K be a cyclic extension of number fields with cyclic galois group $G = \langle\sigma\rangle$. Then the Herband quotient of the G-module $\mathcal{O}_L^\times$ is:

$$h(\mathcal{O}_L^\times) = \frac{e_\infty(L/K)}{[L : K]}$$

Proof **:**
By using theorem 2.3.4, we can simply the proof by taking elements $\epsilon_1, ..., \epsilon_{r+s} \in \mathcal{O}_L^\times$ and taking the subgroup A generated by these elements and noting that by corollary 4.2.36:

$$h(A) = h(\mathcal{O}_L^\times)$$

For each filed embedding $\phi : K \hookrightarrow \mathbb{C}$, let E_φ be the free $\mathbb{Z}$-module with basis given by $\{\varphi|\phi\}$ consisting of the $[L : K] = n$ embeddings $\varphi : L \hookrightarrow \mathbb{C}$ with G-action

$$\sigma(\varphi) = \varphi \circ \sigma$$

Let ν be the infinite place of K corresponding to ϕ, and let A_ν be the free $\mathbb{Z}$-module with basis $\{w|\nu\}$ consisting of the places of L that extend ν also equipped withthe G-action given by the G action on $\{w \mid \nu\}$. Next, let $\pi : E_\phi \to A_\nu$ be the G-module homomorphism sending each embedding $\varphi \mid \phi$ to the corresponding $w \mid \nu$. Let $m := \#\{w|v\}$ and define $\tau := \sigma^m$; then τ is either trivial or has order 2, and in either case generates the decomposition group D_w for all $w|v$ (since G is abelian). We have an exact sequence

$$0 \to \ker\, \pi \longrightarrow E_\phi \xrightarrow{\pi} A_v \to 0$$

where $\ker\, \pi = (\tau - 1)E_\phi$. If v is unramified, then $\ker\, \pi = 0$ and $h(A_v) = h(E_\phi) = 1$, since $E_\phi \simeq \mathbb{Z}[G] \simeq \mathrm{Ind}^G(\mathbb{Z})$.

Otherwise, order $\{w|v\} = \{w_0, \ldots, w_{m-1}\}$ so

$$\text{ker } \pi = (\tau - 1)E_\phi = \left\{ \sum_{0 \leq i < m} a_i(w_i - w_{m+i}) : a_i \in \mathbb{Z} \right\}$$

and observe that $(\text{ker } \pi)^G = 0$, since τ acts on π as negation, and $(\text{ker } \pi)_G \simeq \mathbb{Z}/2\mathbb{Z}$, since $(\sigma - 1)\text{ker } \pi = \{\sum a_i(w_i - w_{m+i}) : a_i \in \mathbb{Z} \text{ with } \sum a_i \equiv 0 \mod 2\}$ (which is killed by N_G). So in this case $h(\text{ker } \pi) = 1/2$, and therefore $h(A_v) = h(E_\phi)/h(\text{ker } \pi) = 2$, As the Herband quotient is an additive function (corollary 4.2.30), and in every case we have $h(A_v) = e_v$, where $e_v \in \{1, 2\}$ is the ramification index of v.

Now consider the exact sequence of G-modules

$$0 \to \mathbb{Z} \to \bigoplus_{v|\infty} A_v \xrightarrow{\psi} A \to 1$$

where ψ sends each infinite place $w_1, \ldots, w_{r+s}$ of L to the corresponding $\varepsilon_1, \ldots, \varepsilon_{r+s} \in A$ given by Theorem 24.7 (each A_v contains either n or $n/2$ of the w_i in its $\mathbb{Z}$-basis). The kernel of ψ is the trivial G-module $(\sum_i w_i)\mathbb{Z} \simeq \mathbb{Z}$, since we have $\psi(\sum_i w_i) = \prod_i \varepsilon_i = 1$ and no other relations among the ε_i, by Herband's Unit Theorem (theorem 2.3.4), by corollary 4.2.34 $h(\mathbb{Z}) = \#G = [L : K]$, and by corollary 4.2.31, $h(\bigoplus A_v) = \prod h(A_v) = \prod e_v$, so

$$h(A) = \frac{e_\infty(L/K)}{[L : K]}$$

which from our initial observation in the proof implies that

$$h(\mathcal{O}_L^\times) = \frac{e_\infty(L/K)}{[L : K]}$$

as we sought to show.

Lemma 4.3.5: Herband Quotient For Ideal Group is Trivial

Let L/K be a cyclic extension of number fields with galois group G. Then for the G-module $\mathcal{I}_L$,

$$h_0(\mathcal{I}_L) = 1 \qquad h^0(\mathcal{I}_L) = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$$

***Proof* :**

This is essentially a lot of computation. It is clear that $I \in \mathcal{I}_L^G \Leftrightarrow v_{\sigma(\mathfrak{q})}(I) = v_\mathfrak{q}(I)$ for all primes $\mathfrak{q} \in \mathcal{I}_L$. If we put $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_K$, then for $I \in \mathcal{I}_L^G$ the value of $v_\mathfrak{q}(I)$ is constant on $\{\mathfrak{q}|\mathfrak{p}\}$, since G acts transitively on this set. It follows that $\mathcal{I}_L^G$ consists of all products of ideals of the form $(\mathfrak{p}\mathcal{O}_L)^{1/e_\mathfrak{p}}$. Therefore $[\mathcal{I}_L^G : \mathcal{I}_K] = e_0(L/K)$ and $h^0(\mathcal{I}_L) = [\mathcal{I}_L^G : N(\mathcal{I}_L)] = e_0(L/K)[\mathcal{I}_K : N(\mathcal{I}_L)]$ as claimed.

Next, for each prime $\mathfrak{q}|\mathfrak{p}$ recall that $N(\mathfrak{q}) = \mathfrak{p}^{f_\mathfrak{p}}$. Thus if $N(I) = \mathcal{O}_K$ then $N(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{v_\mathfrak{q}(I)}) = \mathfrak{p}^{f_\mathfrak{p} \sum_{\mathfrak{q}|\mathfrak{p}} v_\mathfrak{q}(I)} = \mathcal{O}_K$, equivalently, $\sum_{\mathfrak{q}|\mathfrak{p}} v_\mathfrak{q}(I) = 0$, for every prime $\mathfrak{p}$ of K. Order $\{\mathfrak{q}|\mathfrak{p}\}$ as $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$

so that $\mathfrak{q}_{i+1} = \sigma(\mathfrak{q}_i)$ and $\mathfrak{q}_1 = \sigma(\mathfrak{q}_r)$, let $n_i := v_{\mathfrak{q}_i}(I)$, and define

$$J_{\mathfrak{p}} := \mathfrak{q}_1^{n_1}\mathfrak{q}_2^{n_1-n_2}\mathfrak{q}_3^{n_1-n_2-n_3}\cdots\mathfrak{q}_r^{n_1-n_2-\cdots-n_r}.$$

Then

$$\begin{aligned}\sigma(J_{\mathfrak{p}})/J_{\mathfrak{p}} &= \mathfrak{q}_2^{n_1-(n_1-n_2)}\mathfrak{q}_3^{n_1-n_2-(n_1-n_2-n_3)}\cdots\mathfrak{q}_r^{n_1-\cdots-n_{r-1}-(n_1-\cdots-n_r)}\mathfrak{q}_1^{n_1-\cdots-n_r-n_1}\\ &= \mathfrak{q}_2^{n_2}\mathfrak{q}_3^{n_3}\cdots\mathfrak{q}_r^{n_r}\mathfrak{q}_1^{-n_2-\cdots-n_r} = \mathfrak{q}_2^{n_2}\mathfrak{q}_3^{n_3}\cdots\mathfrak{q}_r^{n_r}\mathfrak{q}_1^{n_1} = \prod_{\mathfrak{q}\mid\mathfrak{p}}\mathfrak{q}^{v_{\mathfrak{q}}(I)},\end{aligned}$$

since $n_1+\cdots+n_r = 0$ implies $n_1 = -n_2-\cdots-n_r$. It follows that $I = \sigma(J)/J$ where $J := \prod_{\mathfrak{p}\mid\mathfrak{m}} J_{\mathfrak{p}}$, thus $I_L[N_G] = (\sigma-1)(I_L)$ and $h_0(\mathcal{I}_L) = 1$.

Theorem 4.3.6: Ambiguous Class Number Formula

Let L/K be a cyclic extension of number fields with galois group G. Then the G-invariant subgroup of the G-module Cl_L has cardinality:

$$\#\mathrm{Cl}_L^G = \frac{e(L/K)\#\mathrm{Cl}_K}{n(L/K)[L:K]}$$

where $n(L/K) = [\mathcal{O}_K^\times : N(L^\times)\cap\mathcal{O}_K^\times] \in \mathbb{N}_{>0}$

Proof **:**
The ideal class group Cl_L is the quotient of $\mathcal{I}_L$ by its subgroup $\mathcal{P}_L$ of principal fractional ideals. We thus have a short exact sequence of G-modules

$$1 \to \mathcal{P}_L \to \mathcal{I}_L \to \mathrm{Cl}_L \to 1.$$

The corresponding exact sequence in (standard) cohomology begins

$$1 \to \mathcal{P}_L^G \to \mathcal{I}_L^G \to \mathrm{Cl}_L^G \to H^1(\mathcal{P}_L) \to 1,$$

By lemma 4.3.5, $H^1(\mathcal{I}_L) \simeq \hat{H}_0(\mathcal{I}_L)$ is trivial. Therefore

$$\#\mathrm{Cl}_L^G = [\mathcal{I}_L^G : \mathcal{P}_L^G]h^1(\mathcal{P}_L). \tag{4.1}$$

Using the inclusions $\mathcal{P}_K \subseteq \mathcal{P}_L^G \subseteq \mathcal{I}_L^G$ we can rewrite the first factor on the right hand side as

$$[\mathcal{I}_L^G : \mathcal{P}_L^G] = \frac{[\mathcal{I}_L^G : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{[\mathcal{I}_L^G : \mathcal{I}_K][\mathcal{I}_K : \mathcal{P}_K]}{[\mathcal{P}_L^G : \mathcal{P}_K]} = \frac{e_0(L/K)\#\mathrm{Cl}_K}{[\mathcal{P}_L^G : \mathcal{P}_K]}, \tag{4.2}$$

where $[\mathcal{I}_L^G : \mathcal{I}_K] = e_0(L/K)$ follows from the proof of lemma 4.3.5. Now, consider the short exact sequence

$$1 \to \mathcal{O}_L^\times \to L^\times \overset{\alpha\mapsto(\alpha)}{\to} \mathcal{P}_L \to 1.$$

The corresponding long exact sequence in cohomology begins

$$1 \to \mathcal{O}_K^\times \to K^\times \to \mathcal{P}_L^G \to H^1(\mathcal{O}_L^\times) \to 1 \to H^1(\mathcal{P}_L) \to H^2(\mathcal{O}_L^\times) \to H^2(L^\times), \tag{4.3}$$

where by Hilbert's 90th Theorem $H^1(L^\times)$ is trivial. We have $K^\times/\mathcal{O}_K^\times \simeq \mathcal{P}_K$, thus

$$[\mathcal{P}_L^G : \mathcal{P}_K] = h^1(\mathcal{O}_L^\times) = \frac{h^0(\mathcal{O}_L^\times)}{h(\mathcal{O}_L^\times)} = \frac{h^0(\mathcal{O}_L^\times)[L:K]}{e_\infty(L/K)},$$

by theorem 4.3.4. Combining this identity with (4.1) and (4.2) gives

$$\#\mathrm{Cl}_L^G = \frac{e(L/K)\#\mathrm{Cl}_K}{[L:K]} \cdot \frac{h^1(\mathcal{P}_L)}{h^0(\mathcal{O}_L^\times)}. \tag{4.4}$$

We can write the second factor on the right hand side using the second part of the long exact sequence in (4.3). Next, by theorem 4.2.27 we have $H^2(-) = \hat{H}^2(-) = \hat{H}^0(-)$. Thus

$$H^1(\mathcal{P}_L) \simeq \ker(\hat{H}^0(\mathcal{O}_L^\times) \to \hat{H}^0(L^\times)) \simeq \ker(\mathcal{O}_K^\times/N(\mathcal{O}_L^\times) \to K^\times/N(L^\times)),$$

so $h^1(\mathcal{P}_L) = [\mathcal{O}_K^\times \cap N(L^\times) : N(\mathcal{O}_L^\times)]$. We have $h^0(\mathcal{O}_L^\times) = [\mathcal{O}_K^\times : N(\mathcal{O}_L^\times)]$, thus

$$\frac{h^0(\mathcal{O}_L^\times)}{h^1(\mathcal{P}_L)} = [\mathcal{O}_K^\times : N(L^\times) \cap \mathcal{O}_K^\times] = n(L/K),$$

and plugging this into (4.4) yields the desired formula, completing the proof.

Artin Reciprocity: Unramified Cyclic Case Proof

Let us now prove the Artin Reciprocity. (don't need to state MIT notes elemetnary theorem, they use snake lemma, you can use 3rd iso).

Theorem 4.3.7: Fundamental Inequality II

Let L/K be a totally unramified cyclic extension of number fields. Then:

$$[\mathcal{I}_K : N(\mathcal{I}_L)\mathcal{P}_K] \geq [L:K]$$

Note that the totally unramified condition applies to infinite primes as well.

Proof **:**
First,

$$[\mathcal{I}_K : N(\mathcal{I}_K(\mathcal{P}_K)] = \frac{[\mathcal{I}_K : \mathcal{P}_K]}{[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K]} = \frac{\#\mathrm{Cl}_K}{[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K]}$$

Re-writing the denominator on the right hand side, we get:

$$\begin{aligned}
[N(\mathcal{I}_L)\mathcal{P}_K : \mathcal{P}_K] &= [N(\mathcal{I}_L) : N(\mathcal{I}_L(\cap\mathcal{P}_K] && \text{2nd iso. thm} \\
&= [\mathcal{I}_L : N^{-1}(\mathcal{P}_K)] && \text{Snake Lem.} \\
&= [\mathcal{I}_L/\mathcal{P}_L : N^{-1}(\mathcal{P}_K)/\mathcal{P}_L] && \text{3rd iso. thm} \\
&= [\mathrm{Cl}_L : \mathrm{Cl}_L[N_G] \\
&= \#N_G(\mathrm{Cl}_L)
\end{aligned}$$

Now, as $h^0(\mathrm{Cl}_L(= [\mathrm{Cl}_L^G : N_G(\mathrm{Cl}_L)]$, by theorem 4.3.6 we get:

$$[\mathcal{I}_K : N(\mathcal{I}_K(\mathcal{P}_K)] = \frac{\#\mathrm{Cl}_K h^0(\mathrm{Cl}_L)}{\#\mathrm{Cl}_L^G} = \frac{h^0(\mathrm{Cl}_L)n(L/K)[L:K]}{e(L/K)} \overset{!}{\geq} [L:K]$$

where the $\overset{!}{\geq}$ comes from the fact that the extension is totally unramified, so $e(L/K) = 1$, and that $h^0(\mathrm{Cl}_L), n(L/K) \geq 1$, which gives the desired inequality as we sought to show.

This gives a special case of the Artin reciprocity

Theorem 4.3.8: Artin Reciprocity Law: Unramified Cyclic Case

Let L/K be a totally unramified cyclic extension of number fields. Then:

$$[\mathcal{I}_K : T_{L/K}] = [L:K]$$

which implies the Artin map induces an isomorphism:

$$\mathcal{I}_K / T_{L/K} \cong \mathrm{Gal}_K(L)$$

***Proof* :**
We combine the inequalities from theorem 4.2.20 and theorem 4.3.7 to get $[\mathcal{I}_K : T_{L/K}] = [L:K]$. For the isomorphism, as $\ker \psi_{L/K} \subseteq T_{L/K}$ and $\psi_{L/K}$ is surjective, we get by counting the index that $\ker \psi_{L/K} = T_{L/K}$, implying $\mathcal{I}_K/T_{L/K} \cong \mathrm{Gal}_K(L)$, as we sought to show.

Corollary 4.3.9: Class Number Away From Galois Group

Let L/K be a totally unramified cyclic extension of number field.s Then

$$\#\mathrm{Cl}_L^G = \frac{\#\mathrm{Cl}_K}{[L:K]}$$

and the Tate cohomology groups of Cl_L are all trivial

***Proof* :**
By the Artin Reciprocity Law in the unramified case and the Fundamental Inequality II, we get

$$n(L/K) = 1 \qquad h^0(\mathrm{Cl}_K) = 1 \qquad e(L/K) = 1$$

and so by the Ambiguous Class Number Formula:

$$\#\mathrm{Cl}_L^G = \frac{\#\mathrm{Cl}_L}{[L:K]}$$

Furthermore as Cl_L is finite by corollary 4.2.32 and

$$h(\mathrm{Cl}_K) = \frac{h^-(\mathrm{Cl}_L)}{h_0(\mathrm{Cl}_L)} = 1 \qquad \Rightarrow \qquad h_0(\mathrm{Cl}_L) = 1$$

And so $\hat{H}^{-1}(\mathrm{Cl}_L)$ and $\hat{H}^0(\mathrm{Cl}_L)$ are trivial, which by theorem 4.2.27 implies all the Tate cohomology groups are trivial, as we sought to show.

Corollary 4.3.10: Norm map is Surjective

Let L/K be a totally unramified cyclic extension of number fields. Then every unit in $\mathcal{O}_K^\times$ is the norm of an element of L, i.e. There is a surjection $\mathrm{Nm}_{L/K} : L^\times \to \mathcal{O}_K^\times$

***Proof* :**

$$n(L/K) = [\mathcal{O}_K^\times : N(L^\times) \cap \mathcal{O}_K^\times] = 1 \qquad \Rightarrow \qquad \mathcal{O}_K^\times = N(L^\times) \cap \mathcal{O}_K^\times$$

Artin Reciprocity: Abelian Case Proof

Let us now generalize for non-trivial modulus. We are in a position where we can have the existence of the class field:

Definition 4.3.11: Class Field For Modulus

Let $\mathfrak{m}$ be a modulus for a number field K and let L/K be a finite abelian extension ramified only at primes $\mathfrak{p} \mid \mathfrak{m}$. Then we say that L is a *class field* for $\mathfrak{m}$ is

$$\ker \psi_{L/K}^{\mathfrak{m}} = T_{L/K}^{\mathfrak{m}}$$

where $\psi_{L/K}^{\mathfrak{m}} : \mathcal{I}_K^{\mathfrak{m}} \to \mathrm{Gal}_K(L)$ is the Artin map

Note that we can make this definition stronger than some books due to our build-up, namely we have proven the surjectivity of the Artin map which we factor into the definition.

Lemma 4.3.12: Compositum of Class Fields

Let $\mathfrak{m}$ be a modulus for a number field K. Then if L_1, L_2 are class fields for $\mathfrak{m}$, then so is their compositum

$$L = L_1 L_2$$

***Proof* :**

Certainly, $L = L_1 L_2$ is ramified only at primes ramified in either L_1, L_2, so L is ramified only at primes $\mathfrak{p} \mid \mathfrak{m}$. Then similarly to theorem 4.1.22 a prime $\mathfrak{p} \nmid fm$ splits completely in L if it splits completely in L_1 and L_2, implying

$$\ker \psi_{L/K}^{\mathfrak{m}} = \ker \psi_{L_1/K}^{\mathfrak{m}} \cap \ker_{L_2/K}^{\mathfrak{m}}$$

As the norm map is transitive on towers, if $I = N_{L?K}(J)$, then $I = N_{L_1/K}(N_{L/L_1}(J))$ and $I = N_{L_2/K}(N_{L/L_2}(J))$, and so:

$$N(\mathcal{I}_L^{\mathfrak{m}}) \subseteq N(\mathcal{I}_{L_1}^{\mathfrak{m}}) \cap N(\mathcal{I}_{L_2}^{\mathfrak{m}}) \qquad \Rightarrow \qquad T_{L/K}^{\mathfrak{m}} \subseteq T_{L_1/K}^{\mathfrak{m}} \cap T_{L_2/K}^{\mathfrak{m}}$$

Finally, if L_1 and L_2 are class fields for $\mathfrak{m}$, then

$$T^{\mathfrak{m}}_{L/K} \subseteq T^{\mathfrak{m}}_{L_1/K} \cap T^{\mathfrak{m}}_{L_2/K} = \ker \psi^{\mathfrak{m}}_{L_1/K} \cap \ker^{\mathfrak{m}}_{L_2/K} = \ker \psi^{\mathfrak{m}}_{L/K}$$

Then as $\ker^{\mathfrak{m}}_{L/K} \subseteq T_{L/K}\mathfrak{m}$, we have equality $T_{L/K} = \ker \psi^{\mathfrak{m}}_{L/K}$, completing the proof.

Corollary 4.3.13: Extending to Abelian Case

Let $\mathfrak{m}$ be a modulus for a number field K. Then if every finite cyclic extension of K with conductor dividing $\mathfrak{m}$ is a class field for $\mathfrak{m}$, then so is every abelian extension of K with conductor dividing $\mathfrak{m}$

***Proof* :**
Let L/K be a finite abelian extension with conductor $\mathfrak{c} \mid \mathfrak{m}$. Then the conductor of any subextension of L divides $\mathfrak{c}$ by lemma 4.2.17, and hence $\mathfrak{m}$.

Now, write $G = \mathrm{Gal}_K(L) \cong H_1 \times \cdots \times H_r$ as a product of cyclic groups, and take

$$L_i = L^{\overline{H}_i} \qquad \overline{H}_i = \prod_{j \neq i} H_J \subseteq G$$

Then the galois groups for these fields are cyclic

$$\mathrm{Gal}_K(L_i) = G/\overline{H_i} \cong H_i$$

Noting that $L = L_1 \cdots L_r$, which is a compositum of linearly disjoint cyclic extensions of K, we have by lemma 4.3.12 that if each L_i are class fields for $\mathfrak{m}$, so is L, completing the proof.

We now have the material to proof the special case the Fundamental Theorem of Class Field Theory

Theorem 4.3.14: Fundamental Theorem of C.F.T. (Ideal-theoretic): Unramified

Let K be a number field with Hilbert class field H. Then:

1. H/K is a finite extension with $\mathrm{Gal}_K(L)$ isomorphic to a quotient of Cl_K
2. *Partial Existence*: $K(1)$ exists if and only if $\mathrm{Gal}_K(H) \cong \mathrm{Cl}_K$ in which case $K(1) = H$
3. **Completeness** Every unramified abelian extension of K is a subfield of H
4. **Artin Reciprocity**: For every unramified abelian extension of K, we have $\ker \psi_{L/K} = T_{L/K}$ along with a canonical isomorphism:

$$\mathcal{I}_K/T_{L/K} \cong \mathrm{Gal}_K(L)$$

***Proof* :**
Theorem 4.3.8 and corollary 4.3.13 give Artin Reciprocity for every unramified abelian extension of K. Furthermore, the distinct unramified abelian extension of L/K correspond to distinct quotients of Cl_K, as all primes that split completely in K are precisely those that lie in the kernel of the

Artin map, and there is a unique correspondence between the splitting primes and fields.

4.4 Local Class Field Theory

The goal of this section is to classify all finite abelian extensions of a given local field K. Instead of doing this for each individual finite abelian extension L/K, we shall instead to it all together with our developed theory of Adele rings by using infinite galois theory (see [ChwNAc, chapter 18.4]).

Definition 4.4.1: Maximal Abelian Extension

Let K be a field with separable closure K^{sep}. Then the field:

$$K^{\text{ab}} = \bigcup_{\substack{L \subseteq K^{\text{sep}} \\ L/K \text{ finite Ab.}}} L$$

is the *maximal abelian extension* of K.

As the categories of separable over residue fields correspond to unramified extensions (theorem 1.7.3) $K^{nr} \subseteq K^{\text{ab}}$ (recall that in the Archimedean case $K = K^{nr}$ and $K^{\text{ab}} = K^{\text{sep}} = \mathbb{C}$, as $\mathbb{C}/\mathbb{R}$ is ramified). We thus ahve:

$$K \subseteq K^{nr} \subseteq K^{\text{ab}} \subseteq K^{\text{sep}}$$

By infinite galois theory, we have that:

$$\text{Gal}_K(K^{\text{ab}}) \cong \varprojlim_L \text{Gal}_K(L)$$

where L ranges over all finite extensions of K in Y^{ab} ordered by inclusion. We then have the galois correspondence:

$$\left\{\begin{matrix} \text{Finite Extension } E/K \\ K \subseteq E \subseteq K^{\text{ab}} \end{matrix}\right\} \underset{(K^{\text{ab}})^H}{\overset{\text{Gal}_E(K^{\text{ab}})}{\rightleftarrows}} \left\{\begin{matrix} \text{closed subgroups } H \\ H \subseteq \text{Aut}_K(K^{\text{ab}}) \end{matrix}\right\}$$

Then finite abelian extensions L/K correspond to pen subgroups of $\text{Gal}_K(K^{\text{ab}})$ (which have finite index as $\text{Gal}_K(K^{\text{ab}})$ is compact). If K is Archimedean so that $K \in \{\mathbb{R}, \mathbb{C}\}$, then this correspondence is immediate: $\mathbb{R}^{\text{ab}} = \mathbb{C}$, $\mathbb{C}^{\text{ab}} = \mathbb{C}$. So let's look at the nonarchimedean case.

Let K is a nonarchimedean local field with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{p}$, and residue field $\mathbb{F}_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. Then if L/K is finite unramified with residue field $\mathbb{F}_{\mathfrak{q}} = \mathcal{O}_L/\mathfrak{q}$. By theorem 1.7.3, we have the natural isomorphism:

$$\langle \text{Frob}_{L/K} \rangle = \text{Gal}_K(L) \cong \text{Gal}_{\mathbb{F}_{\mathfrak{p}}}(\mathbb{F}_{\mathfrak{q}}) = \langle x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}} \rangle$$

where $\text{Frob}_{L/K} \in \text{Gal}_K(L)$ generates it. Then as shown in 4.1, we can naturally define the Artin map:

$$\psi_{L/K} : \mathcal{I}_K \to \text{Gal}_K(L) \qquad \mathfrak{p} \mapsto \text{Frob}_{L/K}$$

which corresponds to the quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $n = [L : K]$. Now, notice that each $I \in \mathcal{I}_K$ is principal when working over a local field as $\mathcal{O}_K$ is a DVR (and hence a PID), and so every I is of the form (x) for $x \in K^\times$. We may thus naturally extend the Artin map to $K^\times$ via:

$$\psi_{L/K}(x) := \psi_{L/K}\left((x)\right)$$

which sends every uniformizer π to the Frobenius element.

We would like to extend this map to $\theta_K : K^\times \to \mathrm{Gal}_K(K^{\mathrm{ab}})$, which is known as the *local Artin homomorphism.*

Theorem 4.4.2: Local Artin Reciprocity

Let K be a local field. Then there is a unique continuous homomorphism

$$\theta_K : K^\times \to \mathrm{Gal}_K(K^{\mathrm{ab}})$$

such that for each finite intermediary extension $K \subseteq L \subseteq K^{\mathrm{ab}}$ the homomorphism:

$$\theta_{L/K} : K^\times \to \mathrm{Gal}_K(L)$$

which is given by $\varphi_{L/K}\mathrm{Res}_{L/K} \circ \theta_K$ (where Res is the natural restriction map $\mathrm{Res}_{L/K} : \mathrm{Gal}_K(K^{\mathrm{ab}}) \twoheadrightarrow \mathrm{Gal}_K(L)$) has the properties that:

1. if K is nonarchimedean, L/K unramified, then $\theta_{L/K}(\pi) = \mathrm{Frob} - L/K$ for every uniformizer π of $\mathcal{O}_K$
2. $\theta_{L/K}$ is surjective with kernel $N_{L/K}(L^\times)$, which induces:

$$\frac{K^\times}{N_{L/K}(L^\times)} \cong \mathrm{Gal}_K(L)$$

The restriction map can be defined, and hence interpreted, in many different ways:

- the map $\sigma \mapsto \sigma|_L$
- the quotient map $\mathrm{Gal}_K(K^{\mathrm{ab}}) \twoheadrightarrow \frac{\mathrm{Gal}_K(K^{\mathrm{ab}})}{\mathrm{Gal}_L(K^{\mathrm{ab}})}$
- The projection from $\mathrm{Gal}_K(K^{\mathrm{ab}}) = \varprojlim_L \mathrm{Gal}(L/K) \subseteq \prod_L \mathrm{Gal}_K(L)$

By the last point, these are exactly the maps that appear in the inverse system defining $\mathrm{Gal}_K(K^{\mathrm{ab}})$.

> ***Proof*** **:**
> not given

There are some interesting contrasts between the local case using Adeles and the global cases using places. Notice that :

1. There is no modulus! K^{ab} contains all abelian extension of K, with non being omitted
2. The ray class group $\mathrm{Cl}_K^{\mathfrak{m}}$ is now replaced by the quotient $K^\times$
3. The Takagi group $N_{L/K}(\mathcal{I}_L^{\mathfrak{m}})\mathcal{R}_K^{\mathfrak{m}} \subseteq \mathcal{I}_K^{\mathfrak{m}}$ is replaced by the (simpler!) $N_{L/K}(L^\times) \subseteq K^\times$

One thing we don't have is that $K^\times \to \mathrm{Gal}_K(K^{\mathrm{ab}})$ is an isomorphism. We shall need to take the profinite completion of $K^\times$. To build up to this, let us better understand the group that shows up in this reciprocity:

Definition 4.4.3: Local Norm Group

Let K be a local field. Then the *local norm group* with respect to L, or just *norm group*, is the subgroup of the form:

$$N_{L/K}(L^\times)$$

Write down further intuition here. Remark 27.4 from the MIT notes can also be helpful

Holding theorem 4.4.2 to be true, it suffices to study norm groups! The following shows how the results translate:

Theorem 4.4.4: Galois Correspondence Via Norm Groups

The map $L \mapsto N_{L/K}(L^\times)$ define an inclusion reversing bijection between the finite abelian extensions L/K in K^{ab} and the norm groups in $K^\times$ where:

1. $N_{L/K}(L_1L_2)^\times = N(L_1^\times) \cap N(L_2^\times)$
2. $N((L_1 \cap L_2)^\times) = N(L_1^\times)N(L_2^\times)$

Furthermore, every norm group of K has finite index in $K^\times$, and every subgroup of $K^\times$ that contains a norm group is a norm group

This proof is from the MIT notes, with references updated.

Proof **:**
First, if $L_1 \subseteq L_2$ are two extensions of K then by transitivity of the field norm:

$$\mathrm{N}_{L_2/K} = \mathrm{N}_{L_1/K} \circ \mathrm{N}_{L_2/L_1},$$

and therefore $\mathrm{N}(L_2^\times) \subseteq \mathrm{N}(L_1^\times)$; the map $L \mapsto \mathrm{N}(L^\times)$ thus reverses inclusions.

This immediately implies $\mathrm{N}((L_1L_2)^\times) \subseteq \mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times)$, since $L_1, L_2 \subseteq L_1L_2$. For the reverse inclusion, let us consider the commutative diagram

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_{L_1L_2/K}"] \arrow[dr, "\theta_{L_1/K}\times\theta_{L_2/K}"'] & \mathrm{Gal}(L_1L_2/K) \arrow[d, "\mathrm{res}\times\mathrm{res}"] \\
 & \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)
\end{tikzcd}$$

By Local Artin Reciprocity (theorem 4.4.2), each $x \in \mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times) \subseteq K^\times$ lies in the kernel of $\theta_{L_1/K}$ and $\theta_{L_2/K}$, hence in the kernel of $\theta_{L_1L_2/K}$ (by the diagram), and therefore in $\mathrm{N}((L_1L_2)^\times)$, again by theorem 4.4.2. This proves (1).

We now show that $L \mapsto \mathrm{N}(L^\times)$ is a bijection; it is surjective by definition, so we just need to show it is injective. If $\mathrm{N}(L_2^\times) = \mathrm{N}(L_1^\times)$ then by (1) we have

$$\mathrm{N}((L_1L_2)^\times) = \mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times) = \mathrm{N}(L_1^\times) = \mathrm{N}(L_2^\times),$$

and theorem 4.4.2 implies $\mathrm{Gal}(L_1L_2/K) \cong \mathrm{Gal}(L_1/K) \cong \mathrm{Gal}(L_2/K)$, which forces $L_1 = L_2$; thus $L \mapsto \mathrm{N}(L^\times)$ is injective.

We now prove (2). The field $L_1 \cap L_2$ is the largest extension of K that lies in both L_1 and L_2, while $\mathrm{N}(L_1^\times)\mathrm{N}(L_2^\times)$ is the smallest subgroup of $K^\times$ containing both $\mathrm{N}(L_1^\times)$ and $\mathrm{N}(L_2^\times)$; they therefore correspond under the inclusion reversing bijection $L \mapsto \mathrm{N}(L^\times)$ and we have $\mathrm{N}((L_1 \cap L_2)^\times) = \mathrm{N}(L_1^\times)\mathrm{N}(L_2^\times)$ as desired.

The fact that every norm group has finite index in $K^\times$ follows immediately from the isomorphism $\mathrm{Gal}(L/K) \cong K^\times/\mathrm{N}_{L/K}(L^\times)$ given by theorem 4.4.2, since $\mathrm{Gal}(L/K)$ is finite.

Finally, let us prove that every subgroup of $K^\times$ that contains a norm group is a norm group. Suppose $\mathrm{N}(L^\times) \subseteq H \subseteq K^\times$, for some finite abelian L/K, and subgroup H of $K^\times$, and put $F := L^{\theta_{L/K}(H)}$. We have a commutative diagram

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_{L/K}"] \arrow[dr, "\theta_{F/K}"'] & \mathrm{Gal}(L/K) \arrow[d, "\mathrm{res}"] \\
 & \mathrm{Gal}(F/K)
\end{tikzcd}$$

in which $\mathrm{Gal}(L/F) = \theta_{L/K}(H)$ is precisely the kernel of the map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$ induced by restriction. It follows from theorem 4.4.2 that

$$H = \ker \theta_{F/K} = \mathrm{N}(F^\times)$$

is a norm group, as we sought to show.

Lemma 4.4.5: Norm Groups Finite Index Subgroup of Units

Let L/K be any extension of local fields. Then if $N(L^\times)$ has finite index in $K^\times$, it is open

Proof **:**

Proof. The lemma is clear if K is Archimedean (either $L = K$ and $\mathrm{N}(L^\times) = K^\times$, or $L \cong \mathbb{C}$, $K \cong \mathbb{R}$, and $[K^\times : \mathrm{N}(L^\times)] = [\mathbb{R}^\times : \mathbb{R}_{>0}] = 2$), so assume K is nonarchimedean. Suppose $[K^\times : \mathrm{N}(L^\times)] < \infty$. The unit group $\mathcal{O}_L^\times$ is compact, so $\mathrm{N}(\mathcal{O}_L^\times)$ is compact (since $\mathrm{N} : L^\times \to K^\times$ is continuous), thus closed in the Hausdorff space $K^\times$. For any $\alpha \in L$,

$$\alpha \in \mathcal{O}_L^\times \iff |\alpha| = 1 \iff |\mathrm{N}_{L/K}(\alpha)| = 1 \iff \mathrm{N}_{L/K}(\alpha) \in \mathcal{O}_K^\times,$$

and therefore

$$\mathrm{N}(\mathcal{O}_L^\times) = \mathrm{N}(L^\times) \cap \mathcal{O}_K^\times.$$

It follows that $\mathrm{N}(\mathcal{O}_L^\times)$ is the kernel of the homomorphism $\mathcal{O}_K^\times \hookrightarrow K^\times \to K^\times/\mathrm{N}(L^\times)$ and therefore $[\mathcal{O}_K^\times : \mathrm{N}(\mathcal{O}_L^\times)] \leq [K^\times : \mathrm{N}(L^\times)] < \infty$. Thus $\mathrm{N}(\mathcal{O}_L^\times)$ is a closed subgroup of finite index in $\mathcal{O}_K^\times$, hence open (its complement is a finite union of closed cosets, hence closed), and $\mathcal{O}_K^\times$ is open[1] in $K^\times$, so $\mathrm{N}(\mathcal{O}_L^\times)$ is open in $K^\times$, and therefore $\mathrm{N}(L^\times)$ is open in $K^\times$, since $\mathrm{N}(L^\times)$ is a union of cosets of the open subgroup $\mathrm{N}(\mathcal{O}_L^\times)$.

The existence part of the Local Artin Reciprocity shows the converse holds. For reference purposes, we shall box this result:

Theorem 4.4.6: Local Artin Reciprocity Norm Group

K is a local field and H is a finite index open subgroup of $K^\times$, then there is a unique extension L/K in $K^{\text{ab}}4$ where $N_{L/K}(L^\times) = H$.

Now, let us focus back on $\theta_K : K^\times \to \text{Gal}_K(K^{\text{ab}})$. This cannot be an isomorphism as $\text{Gal}_K(K^{\text{ab}})$ is compact, while $K^\times$ is not. However, the local existence portion of Local Artin Reciprocity that after taking the profinite completion, the local Artin homomorphism becomes an isomorphism

Theorem 4.4.7: Main Theorem of Local Class Field Theory

Let K be a lcoal field. THen the local Artin homomorphism induces a natural isomorphism:

$$\widehat{\theta}_K : \widehat{K^\times} \xrightarrow{\cong} \text{Gal}_K(K^{\text{ab}})$$

of profinite groups

***Proof* :**
By infinite galois theory, the Galois group $\text{Gal}(K^{\text{ab}}/K)$ is a profinite group, isomorphic to the inverse limit

$$\text{Gal}(K^{\text{ab}}/K) \cong \varprojlim_L \text{Gal}(L/K), \tag{4.5}$$

where L ranges over the finite extensions of K in K^{ab} ordered by inclusion.

It follows from lemma 4.4.5, the comment under it, and the definition of the profinite completion, that

$$\widehat{K^\times} \cong \varprojlim_L K^\times/\text{N}(L^\times), \tag{4.6}$$

where L ranges over finite abelian extensions of K (in K^{sep}). By local Artin reciprocity, for each finite abelian extension L/K we have an isomorphism

$$\theta_{L/K} : K^\times/\text{N}(L^\times) \xrightarrow{\sim} \text{Gal}(L/K),$$

and these isomorphisms commute with inclusion maps between finite abelian extensions of K. We thus have an isomorphism of the inverse systems appearing in (4.5) and (4.6). The isomorphism is canonical because the Artin homomorphism θ_K is unique and the isomorphisms in (4.5) and (4.6) are both canonical, completing the proof.

Proposition 4.4.8: Local Artin Homomorphism is Unique

Let K be a local field and assume every finite index open subgroup of $K^\times$ is a norm group. Then there is at most one homomorphism $\theta : K^\times \to \text{Gal}(K^{\text{ab}}/K)$ of topological groups that has the properties given in Local Artin Reciprocity Law.

***Proof* :**
The proposition is clear when K is Archimedean, so assume it is nonarchimedean. Let $\mathfrak{p} = (\pi)$ be the maximal ideal of $\mathcal{O}_K$, and for each integer $n \geq 0$ let $K_{\pi,n}/K$ be the finite abelian extension given by theorem 4.4.6 corresponding to the finite index subgroup $(1+\mathfrak{p}^n)\langle\pi\rangle$ of $K^\times$; here $1+\mathfrak{p}^n$ and $\langle\pi\rangle$ denote subgroups of $K^\times$, with $1+\mathfrak{p}^0 := \mathcal{O}_K^\times$, and we note that $K^\times \cong \mathcal{O}_K^\times\langle\pi\rangle$.

Suppose $\theta : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is a continuous homomorphism as given by Local Artin Reciprocity. Then $\theta(\pi)$ fixes $K_\pi := \bigcup_n K_{\pi,n}$, since $\pi \in \mathrm{N}(K_{\pi,n}) = \ker\theta_{K_{\pi,n}/K}$. We also know that $\theta_{L/K}(\pi) = \mathrm{Frob}_{L/K}$ for all finite unramified extensions L/K, which uniquely determines the action of $\theta(\pi)$ on K^{nr}, and hence on $K^{\mathrm{ab}} = K_\pi K^{nr}$.

Now suppose $\theta' : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is another continuous homomorphism as given by Local Artin Reciprocity. By the argument above we must have $\theta'(\pi) = \theta(\pi)$ for every uniformizer π of $\mathcal{O}_K$, and $K^\times$ is generated by its subset of uniformizers: if we fix one uniformizer π, every $x \in K^\times$ can be written as $u\pi^n = (u\pi)\pi^{n-1}$ for some $u \in \mathcal{O}_K^\times$ and $n \in \mathbb{Z}$, and $u\pi$ is another uniformizer). It follows that $\theta(x) = \theta'(x)$ for all $x \in K^\times$ and therefore $\theta = \theta'$ is unique, as we sought to show.

Hence, it is worth-while understanding the group $\widehat{K}$. IF K is Archimedean $\widehat{K^\times}$ is trivial or cyclic of order 2. If K is nonarchimedean, let us first pick a uniformizer π for the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then each $x \in K^\times$ can be uniquely represented as $u\pi^{\nu(x)}$ where $u \in \mathcal{O}_K^\times$ and $\nu(x) \in \mathbb{Z}$. Then we get:

$$K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z} \qquad x \mapsto \left(\frac{x}{\pi^{\nu(x)}}, \nu(x)\right)$$

Taking now the profinite completion we get:

$$\widehat{K^\times} \cong \mathcal{O}_K^\times \times \widehat{Z}$$

recalling that $\mathcal{O}_K$ is already a profinite completion (recall section 1.1.1):

$$\mathcal{O}_K^\times \cong \mathbb{F}_\mathfrak{p}^\times \times (1+\mathfrak{p}) \cong \mathbb{F}_\mathfrak{p}^\times \times \varprojlim_n \mathcal{O}_K(1+\mathfrak{p}^n)$$

This isomorphism is dependent on the choice of π (of which are uncountably many), and hence is not a canonical isomorphism. Overall, we now get the commutative diagram of exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\cong"] & K^\times \arrow[r, "\nu"] \arrow[d, "\theta_K"] & \mathbb{Z} \arrow[r] \arrow[d, hook, "\phi"] & 0 \\
1 \arrow[r] & \mathrm{Gal}_{K^{nr}}(K^{\mathrm{ab}}) \arrow[r] & \mathrm{Gal}_K(K^{\mathrm{ab}}) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}_K(K^{nr}) \arrow[r] & 1
\end{tikzcd}$$

where the bottom row is the profinite completion of the top row! The right-most map is given by:

$$\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} \cong \mathrm{Gal}_{\mathbb{F}_\mathfrak{p}}(\overline{\mathbb{F}}_\mathfrak{p}) \cong \mathrm{Gal}_K(K^{nr})$$

sending 1 to the sequence of Frobenius elements. The Frobenius $\varphi(1)$ is a topological generator, making a dense subset. Note that $\varphi(-1)$ is also a generator; sometimes $\varphi(1)$ is called the arithmetic generator while $\varphi(-1)$ is called the geometric generators for reason beyond this book.

The group $\mathrm{Gal}_{K^{nr}}(K^{\mathrm{ab}}) \cong \mathcal{O}_K^\times$ corresponds to the inertia subgroup of $\mathrm{Gal}_K(K^{\mathrm{ab}})$. As the top sequence splits, so does the bottom so that for each choice of uniformizer:

$$\mathrm{Gal}_K(K^{\mathrm{ab}}) \cong \mathrm{Gal}_{K^{nr}}(K^{\mathrm{ab}}) \times \mathrm{Gal}_K(K^{nr}) \cong \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$$

Furthermore, for each choice of uniformizer $\pi \in \mathcal{O}_K$, we get

$$K^{\mathrm{ab}} = K_\pi K^{nr}$$

which corresponds to $K^\times = \mathcal{O}_K^\times \pi^{\mathbb{Z}}$, where the field $K_\pi \subseteq K^{\mathrm{ab}}$ is the subfield fixed by $\theta_K(\pi) \in \mathrm{Gal}_K(K^{\mathrm{ab}})$. Equivalently, K_π si the compositum of all totally ramified finite extensions L/K in K^{ab} where $\pi \in N(L^\times)$.

The simplest such decomposition is given by taking $K = \mathbb{Q}_p$ and $\pi = p$ in which case $K^{\mathrm{ab}} = K_\pi K^{nr}$ is

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_n \mathbb{Q}_p(\zeta_{p^n}) \cdot \bigcup_{m \perp p} \mathbb{Q}_p(\zeta_m)$$

where the first union is fixed by $\theta_K(p)$ and the second union is fixed by $\theta_K(\mathcal{O}_K^\times)$.

Summary

Overall we get a bijection between these three sets:

1. finite-index open subgroups of $K^\times$
2. open subgroups of $\mathrm{Gal}_K(K^{\mathrm{ab}})$
3. finite extensions of K in K^{ab}

which fully classifies abelian extension using *only* information about $K^\times$!

5

Class Field Theory: Adèle Approach

In this chapter, we shall study all completions of a number ring at once. Recall that each $\mathbb{Q}_p$ is locally compact. The product topology $X = \prod_{p \leq \infty} \mathbb{Q}_p$ is *not* necessarily locally compact: if $x \in X$ has a compact neighborhood $C \subseteq X$, then as each open subset must be $\mathbb{Q}_p$ for all but finitely many positions, we see that $\pi_i(C)$ only compact iff almost all $\mathbb{Q}_p$ are compact, which we know is not the case.

5.1 Ring of Adeles and Strong Approximation

Recall that local fields are locally compact (proposition 1.3.3). Many of the results we have shown use the property of locally compact fields. We require local compactness "in the limit"; that is when considering all local fields. We thus take the following particular topology express invented for solving this problem:

Definition 5.1.1: Restricted Product

Let $(X_i)_{i\in I}$ be a family of topological spaces indexed by I, and let $U_i \subseteq X_i$ be a family of open subsets. Then the *restricted product* is the set:

$$\prod_{i\in I}{}' (X_i, U_i) = \{(x_i)_{i\in I} \ : \ x_i \in U_i \text{ for a.e. } i \in I\} \subseteq \prod X_i$$

with topology given by the basis:

$$\mathcal{B} = \left\{ \prod_{i\in I} V_i \ : \ V_i \subseteq X_i \text{ is open for all } i \in I \text{ and } V_i = U_i \text{ for a.e. } i \in I \right\}$$

where almost all means all but finitely many.

Essentially, instead of having X_i at a.e. position, we shall have U_i. Note that this does not mean that that the sets X_i for a specific index i does not exist: the set

$$X_i \times \prod_{i\neq j\in I} U_j$$

is within the restricted product for each index i. This shows that in the finite product cases, the two topologies and sets are identical. Notice that each projection map is still continuous, As $\prod X_i$ is supposed to be the coarsest space with these maps being continuous, we may expect more open sets in the restricted product, and indeed we do: $\prod_i U_i$ is open in the restricted product but not the product (unless, of course, $U_i = X_i$ for a.e. indexes). This also shows that the restricted product is not in the subspace topology, as there are no open sets of $\prod_i X_i$ that can be intersected to get $\prod_i U_i$.

Note that the topology and set of the restricted product does not depend on any particular U_i. Indeed, if $U_i = U_i'$ for a.e. indices, then:

$$\prod_{i\in I}{}' (X_i, U_i) = \prod_{i\in I}{}' (X_i, U_i')$$

Let us show that this topology is the colimit of appropriate subspaces of the product space. Given any $x \in X \prod_{i\in I}' (X_i, U_i)$ define the (possibly empty) finite set:

$$S(x) = \{i \in I \ : \ x_i \notin U_i\}$$

From this, define:

$$X_s = \{x \in X \ : \ S(x) \subseteq S\} = \prod_{i\in S} X_i \times \prod_{i\notin S} U_i$$

Notice that each X_s is an open subset and can be viewed as a subspace of X or as a direct product of appropriate X_i and U_i (the basis $\mathcal{B}$ can be restricted to a basis $\mathcal{B}_S$ that generated both topologies). Notice that if $S \subseteq T$ then $X_S \subseteq X_T$, and hence we may partially order the family of topological space X_S via the inclusion and consider the colimit:

$$\varinjlim_S X_S = \bigsqcup X_S / \sim$$

with the equivalence being given by $x \sim \iota_{ST}(x)$ where $\iota_{ST} : X_S \to X_T$ is the inclusion map. Then it is a good exercise in topology to show that the following are homeomorphic:

$$X \cong_{\mathbf{Top}} \varinjlim X_S$$

Due to this characterization, we can conclude that the restricted product of locally compact spaces is locally compact when the family $(U_i)_{i\in I}$ are a.e. compact (can you see why this fixes the problem of the continuous image of compact sets is compact?)

Let us now work with topological spaces that are relevant to number theory. Let K be a global field, M_K denote the set of places of K, K_ν the corresponding local field, and $\mathcal{O}_\nu$ the valuation ring of K_ν where if ν is Archimedean then $\mathcal{O}_\nu = K_\nu$. Then

Definition 5.1.2: Adèle Ring

Let K be a global field. Then the *adèle ring* or *adele ring* is the restricted product:

$$\mathbb{A}_K = \prod_{\nu\in M_K}' (K_\nu, \mathcal{O}_\nu)$$

which is a subset (not subspace) of $\prod_\nu K_\nu$. Define addition and multiplication component-wise.

Recall that each $\mathcal{O}_\nu$ is compact when ν is non-Archimedean, and that there are only finitely many Archimedean valuations, hence $\mathbb{A}_K$ is locally compact. As K_ν is Hausdroff and the restricted topology is finer, $\mathbb{A}_K$ is also Hausdroff. For each $a \in \mathbb{A}_K$, denote by a_ν the projection into K_ν. For each finite set of place S, we can define the subring of S-adeles:

$$\mathbb{A}_{K,S} = \prod_{\nu\in S} K_\nu \times \prod_{\nu\notin S} \mathcal{O}_\nu$$

so that $\mathbb{A}_K \cong \varinjlim_S \mathbb{A}_{K,S}$, showing that $\mathbb{A}_K$ is also a topological ring. A simple example would be when $K = \mathbb{Q}$, in which case $\mathbb{A}_\mathbb{Q}$ is the union of the rings:

$$\mathbb{R} \times \prod_{p\in S} \mathbb{Q}_p \times \prod_{p\notin S} \mathbb{Z}_p$$

where S varies over all finite sets of primes. Taking the canonical embeddings $K \hookrightarrow K_\nu$, we may induce a canonical embedding:

$$K \hookrightarrow \mathbb{A}_K \qquad x \mapsto (x, x, ...)$$

which is well-defined as $x \in \mathcal{O}_\nu$ for a.e. ν. For reasons that should be illuminating to the reader to ponder, the image K in $\mathbb{A}_K$ is called the *principal adele* subring (which is also a field).

The normalized absoltue value $\| - \|_\nu$ of K_ν can naturally be extended to $\mathbb{A}_K$ for each ν via:

$$\|(a)\|_\nu = \|a_\nu\|_\nu$$

And by proposition 2.1.9 we may define the *adelic absolute value* (or *adelic norm*) to be:

$$\|(a)\| = \prod_{\nu\in M_K} \|a\|_\nu \in \mathbb{R}_{\geq 0}$$

Note that unless $\|a\|_\nu = 1$ for all but finitely many ν, this product will naturally converge to 0. If$\|a\| \neq 0$, this is equal to the *Arakelov divisor*. For any nonzero principal adele a, we may consider it as $a \in K^\times$, and by the product formula $\|a\| = 1$ (showing they form the group of units).

This next section covers the Haar measure on the ring, however as I have yet to fully cover the Haar measure I will omit this for now.

Next, let's consider a base change. Let us see that the embedding $K \hookrightarrow \mathbb{A}_K$ makes $\mathbb{A}_K$ into a K-vector space. IF L/K is any finite separable extension of K, we can take:

$$\mathbb{A}_K \otimes_K L$$

giving an L-vector space. As a topological K-vector space, $\mathbb{A}_K \otimes_K L$ is the product of $[L : K]$ copies of $\mathbb{A}_K$. This product does indeed act how we may expect it to:

Lemma 5.1.3: Adele Ring Change of Basis

Let L/K be a finite separable extension of a global field K. Then there is a natural isomorphism of topological rings:

$$\mathbb{A}_L \cong \mathbb{A}_K \otimes L$$

such that the following diagram commutes:

$$\begin{tikzcd}
L \arrow[r, "\cong"] \arrow[d, hook] & K \otimes_K L \arrow[d] \\
\mathbb{A}_L \arrow[r, "\cong"] & \mathbb{A}_L \otimes_K L
\end{tikzcd}$$

Proof **:**
exercise (good practice for restricted product and for change of basis. At some point, you will need to commute the tensor with the restricted product, which is possible as you are working with the restricted product and not the product)

Lemma 5.1.4: Adele Ring Change of Basis As Vector Space

Let L/K be a degree n separable extension of a global field K. Then there is a natural isomorphism of topological K-vector spaces and local compact groups:

$$\mathbb{A}_L \cong \mathbb{A}_K \oplus \cdots \oplus \mathbb{A}_K$$

which restricts to an isomorphism $L \cong K \oplus \cdots \oplus K$ of the principal adeles of $\mathbb{A}_L$

Proof **:**
immediate from lemma 5.1.3.

More importantly, we can understand the topology of L within $\mathbb{A}_L$. Recall that a group $H \leqslant G$ is *cocompact* if G/H is compact.

Theorem 5.1.5: Principal Adeles Cocompact

Let L be a global field considered as the principal adele ring $L \subseteq \mathbb{A}_L$. Then it is a discrete cocompact subgroup of $\mathbb{A}_L$ seen as an additive group.

Proof **:**
If $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$ (i.e. K is a rational subfield), then it follows from lemma 5.1.4, that if we show it for K, then it follows for L, so assume K is a rational subfield, and identify it with its image in $\mathbb{A}_K$. To show it's discrete, we can show 0 is an isolated point. Take:

$$U = \{a \in \mathbb{A}_K \ : \ \|a\|_\infty < 1, \ \|a\|_\nu \le 1, \ \forall \nu < \infty\}$$

where ∞ denotes the unique infinite place of K. By the product formula, $\|a\| = 1$ for all $a \in K^\times \subseteq \mathbb{A}_K$, and so

$$U \cap K = \{0\}$$

showing it is discrete.

To show K is cocompact, i.e. $\mathbb{A}_K/K$ is compact, take the sets

$$U_\infty = \{x \in K_\infty \ : \ \|x\|_\infty \le 1\} \qquad W = \{a \in \mathbb{A}_K \ : \ \|a\|_\nu \le 1, \ \forall \nu\}$$

Then we may decompose W as:

$$W = U_\infty \times \prod_{\nu<\infty} \mathcal{O}_\nu \subseteq \mathbb{A}_{K,\{\infty\}} \subseteq \mathbb{A}_K$$

which is a product of compact sets, hence compact. If we show that W contains a set of coset representatives for K in $\mathbb{A}_K$, we're done, as then $\mathbb{A}_K/K$ is the image of the comapct set W under the continuous quotient $\mathbb{A}_K \to \mathbb{A}_K/K$.

Let $a = (a_\nu)$ be any element of $\mathbb{A}_K$. To show it has a representative in W, we need that $a = b + c$ for some $b \in W$ and $c \in K$, which we will do by constructing $c \in K$ so that $b = a - c \in W$.

For each $\nu < \infty$ define $x_\nu \in K$ as follows: put $x_\nu := 0$ if $\|a_\nu\|_\nu \le 1$ (almost all ν), and otherwise choose $x_\nu \in K$ so that $\|a_\nu - x_\nu\|_\nu \le 1$ and $\|x_\nu\|_w \le 1$ for $w \ne \nu$. To show that such an x_ν exists, let us first suppose $a_\nu = r/s \in K$ with $r, s \in \mathcal{O}_K$ coprime (note that $\mathcal{O}_K$ is a PID), and let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_\nu$. The ideals $\mathfrak{p}^{\nu(s)}$ and $\mathfrak{p}^{-\nu(s)}(s)$ are coprime, so we can write $r = r_1 + r_2$ with $r_1 \in \mathfrak{p}^{\nu(s)}$ and $r_2 \in \mathfrak{p}^{-\nu(s)}(s) \subseteq \mathcal{O}_K$, so that $a_\nu = r_1/s + r_2/s$ with $\nu(r_1/s) \ge 0$ and $w(r_2/s) \ge 0$ for all $w \ne \nu$. If we now put $x_\nu := r_2/s$, then $\|a_\nu - x_\nu\|_\nu = \|r_1/s\|_\nu \le 1$ and $\|x_\nu\|_w = \|r_2/s\|_w \le 1$ for all $w \ne \nu$ as desired. We can approximate any $a'_\nu \in K_\nu$ by such an $a_\nu \in K$ with $\|a'_\nu - a_\nu\|_\nu < \epsilon$ and construct x_ν as above so that $\|a_\nu - x_\nu\|_\nu \le 1$ and $\|a'_\nu - x_\nu\|_\nu \le 1 + \epsilon$; but for sufficiently small ϵ this implies $\|a'_\nu - x_\nu\|_\nu \le 1$, since the nonarchimedean absolute value $\| - \|_\nu$ is discrete.

Finally, let $x := \sum_{\nu<\infty} x_\nu \in K$ and choose $x_\infty \in \mathcal{O}_K$ so that

$$\|a_\infty - x - x_\infty\|_\infty \le 1.$$

For $a_\infty - x \in \mathbb{Q}_\infty \cong \mathbb{R}$, we can take $x_\infty \in \mathbb{Z}$ in the real interval $[a_\infty - x - 1, a_\infty - x + 1)$. For $a_\infty - x \in \mathbb{F}_q(t)_\infty \cong \mathbb{F}_q((t^{-1}))$ we can take $x_\infty \in \mathbb{F}_q[t]$ to be the polynomial of least degree for which $a_\infty - x - x_\infty \in \mathbb{F}_q[[t^{-1}]]$.

Now let $c := \sum_{\nu \leq \infty} x_\nu \in K \subseteq \mathbb{A}_K$, and let $b := a - c$. Then $a = b + c$, with $c \in K$, and we claim that $b \in W$. For each $\nu < \infty$ we have $x_w \in \mathcal{O}_\nu$ for all $w \neq \nu$ and

$$\|b\|_\nu = \|a - c\|_\nu = \left\| a_\nu - \sum_{w \leq \infty} x_w \right\|_\nu \leq \max(\|a_\nu - x_\nu\|_\nu, \max(\{\|x_w\|_\nu : w \neq \nu\})) \leq 1,$$

by the nonarchimedean triangle inequality. For $\nu = \infty$ we have $\|b\|_\infty = \|a_\infty - c\|_\infty \leq 1$ by our choice of x_∞, and $\|b\|_\nu \leq 1$ for all ν, so $b \in W$ as claimed and the theorem follows.

Let us put this result to good use by showing the strong approximation Theorem for Adele rings. To show this result, let us generalize the Minkowski Lattice Point Theorem to bound the size a prime via a principal prime:

Theorem 5.1.6: Adelic Blichfeldt-Minkowski Lemma

Let K be a global field. Then there exists a positive constant B_K such that for any $a \in \mathbb{A}_K$ with $\|a\| > B_K$, there exists a nonzero principal adele $x \in K \subseteq \mathbb{A}_K$ such that

$$\|x\|_\nu \leq \|a\|_\nu \qquad \forall \nu \in M_K$$

This proof is directly from the MIT notes.

Proof **:**

Let $b_0 := \operatorname{covol}(K)$ be the measure of a fundamental region for K in $\mathbb{A}_K$ under our normalized Haar measure μ on $\mathbb{A}_K$ (as K is cocompact, b_0 is finite). Now define

$$b_1 := \mu(\{z \in \mathbb{A}_K : \|z\|_\nu \leq 1 \text{ for all } \nu \text{ and } \|z\|_\nu \leq \frac{1}{4} \text{ if } \nu \text{ is Archimedean}\}).$$

Then $b_1 \neq 0$, since K has only finitely many Archimedean places. Now let $B_K := b_0/b_1$.

Suppose $a \in \mathbb{A}_K$ satisfies $\|a\| > B_K$. We know that $\|a\|_\nu \leq 1$ for all almost all ν, so $\|a\| \neq 0$ implies that $\|a\|_\nu = 1$ for almost all ν. Let us now consider the set

$$T := \{t \in \mathbb{A}_K : \|t\|_\nu \leq \|a\|_\nu \text{ for all } \nu \text{ and } \|t\|_\nu \leq \frac{1}{4}\|a\|_\nu \text{ if } \nu \text{ is Archimedean}\}.$$

From the definition of b_1 we have

$$\mu(T) = b_1\|a\| > b_1 B_K = b_0;$$

this follows from the fact that the Haar measure on $\mathbb{A}_K$ is the product of the normalized Haar measures μ_ν on each of the K_ν. Since $\mu(T) > b_0$, the set T is not contained in any fundamental region for K, so there must be distinct $t_1, t_2 \in T$ with the same image in $\mathbb{A}_K/K$, equivalently, whose difference $x = t_1 - t_2$ is a nonzero element of $K \subseteq \mathbb{A}_K$. We have

$$\|t_1 - t_2\|_\nu \leq \begin{cases} \max(\|t_1\|_\nu, \|t_2\|_\nu) \leq \|a\|_\nu & \text{finite place} \\ \|t_1\|_\nu + \|t_2\|_\nu \leq 2 \cdot \frac{1}{4}\|a\|_\nu \leq \|a\|_\nu & \text{real place} \\ (\|t_1 - t_2\|_\nu^{1/2})^2 \leq (\|t_1\|_\nu^{1/2} + \|t_2\|_\nu^{1/2})^2 \leq (2 \cdot \frac{1}{2}\|a\|_\nu^{1/2})^2 \leq \|a\|_\nu & \text{complex place} \end{cases}$$

Here we have used the fact that the normalized absolute value $\| - |_\nu$ satisfies the nonarchimedean triangle inequality when ν is nonarchimedean, $\| - \|_\nu$ satisfies the Archimedean triangle inequality when ν is real, and $\| - \|_\nu^{1/2}$ satisfies the Archimedean triangle inequality when ν is complex. Thus $\|x\|_\nu = \|t_1 - t_2\|_\nu \leq \|a\|_\nu$ for all places $\nu \in M_K$ as desired.

Theorem 5.1.7: Strong Approximations For Places

Let $M_K = S \sqcup T \sqcup \{w\}$ be a partition of the places of a global field K, where S is finite. Then fixing a $a_\nu \in K$ and $\epsilon_\nu \in \mathbb{R}_{>0}$ for each S, there exists a $x \in K$ such that

$$\begin{aligned} \|x - a_\nu\|_\nu \leq \epsilon_\nu, \, \forall \nu \in S \\ \|x_\nu\|_\nu \leq 1, \, \forall \nu \in T \end{aligned}$$

with no constraint on $\|x\|_w$

This proof is again straight from the MIT notes with references updated

***Proof* :**
Let $W = \{z \in \mathbb{A}_K : \|z\|_v \leq 1 \text{ for all } v \in M_K\}$ as in the proof of theorem 5.1.5. Then W contains a complete set of coset representatives for $K \subseteq \mathbb{A}_K$, so $\mathbb{A}_K = K + W$. For any nonzero $u \in K \subseteq \mathbb{A}_K$ we also have $\mathbb{A}_K = K + uW$: given $c \in \mathbb{A}_K$ write $u^{-1}c \in \mathbb{A}_K$ as $u^{-1}c = a + b$ with $a \in K$ and $b \in W$ and then $c = ua + ub$ with $ua \in K$ and $ub \in uW$. Now choose $z \in \mathbb{A}_K$ such that

$$0 < \|z\|_v \leq \epsilon_v \text{ for } v \in S, \quad 0 < \|z\|_v \leq 1 \text{ for } v \in T, \quad \|z\|_w > B \prod_{v \neq w} \|z\|_v^{-1},$$

where B is the constant in the Blichfeldt-Minkowski Lemma (this is clearly possible: every $z = (z_v)$ with $\|z_v\|_v \leq 1$ is an element of $\mathbb{A}_K$). We have $\|z\| > B$, so there is a nonzero $u \in K \subseteq \mathbb{A}_K$ with $\|u\|_v \leq \|z\|_v$ for all $v \in M_K$.

Now let $a = (a_v) \in \mathbb{A}_K$ be the adele with a_v given by the hypothesis of the theorem for $v \in S$ and $a_v = 0$ for $v \notin S$. We have $\mathbb{A}_K = K + uW$, so $a = x + y$ for some $x \in K$ and $y \in uW$. Therefore

$$\|x - a_v\|_v = \|y\|_v \leq \|u\|_v \leq \|z\|_v \leq \begin{cases} \epsilon_v & \text{for } v \in S, \\ 1 & \text{for } v \in T, \end{cases}$$

as we sought to show.

As a direct consequence

Corollary 5.1.8: Density of Principal Adeles

Let K be a glboal field and let w be any place of K. Then K is dense in the restricted product $\prod'_{\nu \neq w}(K_\nu, \mathcal{O}_\nu)$.

***Proof* :**
immediate consequence.

It was remarked that these results can be extended for algebraic groups (algebraic variety with compatible group structure), showing there is something deeper going on in this approximation.

5.1.1 Units of Adèle Ring

Let us now try to find:

$$\mathbb{A}_K^\times = \left\{(a) \in \mathbb{A}_K \ : \ a_\nu \in K_\nu^\times, \ \forall \nu \in M_k \text{ and } a_\nu \in \mathcal{O}_\nu^\times \text{ for a.e. } \nu \in M_K\right\}$$

where if ν is Archimedean then $\mathcal{O}_K^\times$ is either $\mathbb{R}^\times$ or $\mathbb{C}^\times$. Unfortunately, $\mathbb{A}_K^\times$ is not a topological subgroup of $\mathbb{A}_K$, as the inversion map $a \mapsto a^{-1}$ is not continuous. To see this, take the case where $K = \mathbb{Q}$. Then for each prime p, consider $a(p) = (1, ..., 1, p, 1, ...) \in \mathbb{A}_\mathbb{Q}$ so that $a(p)_p = p$ and $a(p)_q = 1$ for $q \neq p$. Ten every basic open set $U \subseteq \mathbb{A}_\mathbb{Q}$ around 1 must have the form (for some finite $S \subseteq M_\mathbb{Q}$):

$$\prod_{\nu \in S} U_\nu \times \prod_{\nu \notin S} \mathcal{O}_\nu$$

where $1_\nu \in U_\nu$. Then certainly U contains $a(p)$ for sufficiently large p. Thus, we get that in $\mathbb{A}_\mathbb{Q}$ the following limit is:

$$\lim_{p \to \infty} a(p) = 1$$

However, U does not contain $a(p)^{-1}$ for any sufficiently large p, hence we also have:

$$\lim_{p \to \infty} a(p)^{-1} \neq 1^{-1} = 1$$

Thus $a \mapsto a^{-1}$ is *not* a continuous map in the subspace $\mathbb{A}_K^\times$. The problem is more general than our number-theoretic context, as a topological ring has no continuous inverse condition, there is no good reason that $R^\times \subseteq R$ be a topological group in the subspace topology (unless, of course, R is a subring of a topological field which explains why this problem did not occur for $\mathcal{O}_K^\times$ and why this cannot happen for the ring of adeles as it is not an integral domain).

To resolve this, we impose the weakest topology that will make $R^\times$ a topological group, namely, we take the embedding:

$$\varphi : R^\times \to R \times R \qquad r \mapsto (r, r^{-1})$$

and put the weakest topology on $R^\times$ that makes this map $\varphi : R^\times \to \varphi(R^\times)$ a homeomorphism. This is the subspace topology of $\varphi(R^\times) \subseteq R \times R$. The map $r \mapsto r^{-1}$ is naturally continuous as it is the composition of φ with the projection onto the second component.

With this in mind, let us return to $\mathbb{A}_K^\times$. Then we have $\varphi : \mathbb{A}_K^\times \to \mathbb{A}_K \times \mathbb{A}_K$, and each $\varphi(a) = (a, a^{-1})$ lies in a product $U \times V$ of basic open sets $U, V \subseteq \mathbb{A}_K$, which forces both a, a^{-1} to lie in $\mathcal{O}_\nu$, and hence in $\mathcal{O}_\nu^\times$ for almost all ν. From this, we see that the induced topology on $\mathbb{A}_K^\times$ is the restricted product with open sets that we would have hopped to have:

Definition 5.1.9: Idele Group

Let K be a global field. Then the *idele group* of K is the topological group:

$$\mathbb{I}_K = \prod_{\nu}{}' (K_\nu^\times, \mathcal{O}_\nu^\times)$$

with multiplication defined pointwise. Then $\mathbb{I}_K$ is the set $\mathbb{A}_K^\times$ with the restricted product topology instead of the subspace topology. The canonical embedding $K \hookrightarrow \mathbb{A}_K$ restricts to a canonical embedding $K^\times \hookrightarrow \mathbb{I}_K$. The *idele class group* is the topological group:

$$C_K = \frac{\mathbb{I}_K}{K^\times}$$

From here on out, we may use $\mathbb{A}_K^\times$ and $\mathbb{I}_K$ interchangeably, understanding that $\mathbb{A}_K^\times$ has the restricted product topology instead of the subspace topology. Furthermore, $\mathbb{I}_K$ is a locally compact group (it is certainly Hausdroff as it is finer than $\mathbb{A}_K^\times$ with the subspace topology which is Hausdroff, and each $\mathcal{O}_K^\times$ is compact with $K_\nu^\times$ being locally compact). Next, $K^\times$ is a discrete subgroup of $\mathbb{I}_K$: as K is a discrete subset of $\mathbb{A}_K$ (by theorem 5.1.5, $K \times K$ is a discrete subset of $\mathbb{A}_K \times \mathbb{A}_K$, and as $K^\times$ lies in the image of $\mathbb{A}_K^\times \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ and $K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$, $K^\times$ is discrete in $\mathbb{A}_K^\times$, and hence in $\mathbb{I}_K$ (as the topology is finer). We shall return to cocompactness shortly.

Let us see how this new topology fixes the counter-example presented earlier for the lack of continuity. Take again the sequence $(a(p))_p$. Then this sequence no longer converges to 1 in $\mathbb{I}_\mathbb{Q}$. Notice that for the basic open neighborhood of 1:

$$\prod_\nu \mathcal{O}_\nu^\times = \prod_p \mathbb{Z}_p^\times \times \mathbb{R}^\times \subseteq \mathbb{I}_\mathbb{Q}$$

none of the $a(p)$ lie in this set, and hence this sequence cannot converge to 1. In fact, this implies it cannot converge at all for if it converges to some $1 \neq x \in \mathbb{I}_\mathbb{Q}$, then it would converge to $1 \neq x \in \mathbb{A}_\mathbb{Q}^\times \subseteq \mathbb{A}_\mathbb{Q}$ which we know is not the case. The high-level idea is that we added more open sets to this topology, increasing the requirement for sequences to converge (and at the same time, make it easier for the inverse map to be continuous).

With this, we may now associate the elements of $\mathbb{I}_K$ to the ideals in $\mathcal{I}_K$. Consider the surjective homomorphism:

$$\mathbb{I}_K \to \mathcal{I}_K \qquad a \mapsto \prod \mathfrak{p}^{\nu_\mathfrak{p}(a)}$$

Then the image of the composition

$$K^\times \hookrightarrow \mathbb{I}_K \twoheadrightarrow \mathcal{I}_K$$

is $\mathcal{P}_K$, and so we have a surjective homomorphism from $\mathbb{I}_K$ to $C_K = \mathbb{I}_K/K^\times$ onto $\mathrm{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$ which makes the following diagram of exact sequences commute:

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r] \arrow[d, two heads] & \mathbb{I}_K \arrow[r] \arrow[d, two heads] & C_K \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & \mathcal{P}_K \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

When working with K and $\mathbb{A}_K$, it was also shown that K is cocompact, however $K^\times$ is not cocompact, and so the idele class group C_K is locally compact but not compact. This can be seen more evidently if we recall that the group of units $\mathcal{O}_K^\times$ is not a cocompact subgroup of $K_\mathbb{R}^\times$ as $\log(\mathcal{O}_K^\times)$ is not a (full) sub-lattice in $\mathbb{R}^{r+s} \cong \log(K_\mathbb{R}^\times)$ (recall it lies in the trace-zero hyperplane, see [ChwNAc]). We must thus get the corresponding trace zero hyperplane for $\mathbb{I}_K$. Take the continuous homomorphism between topological groups:

$$\| - \| : \mathbb{I}_K \to \mathbb{R}_{>0}^\times \qquad a \mapsto \|a\| = \prod_\nu \|a\|_\nu$$

where $\| - \|$ is the adelic norm. Then $\|a\| > 0$ for $a \in \mathbb{I}_K$ as $a_\nu \in \mathcal{O}_\nu^\times$ for a.e. ν, which implies $\|a\|_\nu = 1$ for a.e. ν, making the product effectively a finite product, and it is nonzero as $a_\nu \in K_\nu^\times$ is nonzero for all $\nu \in M_K$. This motivates the following natural topological group:

Definition 5.1.10: 1-Ideles Group

Let K be a global field. Then the group if *1-ideles* is the topological group

$$\mathbb{I}_K^1 = \ker \| - \| = \{a \in \mathbb{I}_K \ : \ \|a\| = 1\}$$

An important result that we shall need is that the topology of $\mathbb{I}_K^1$ is the same as the subspace topology induced by $\mathbb{A}_K$

Lemma 5.1.11: Topology of 1-Idele Group

Let group of 1-ideles $\mathbb{I}_K^1$ is a closed usbset of $\mathbb{A}_K$ and $\mathbb{I}_K$, and the two induced subspace topologies on $\mathbb{I}_K^1$ coincide.

This proof is from the MIT notes (it is pretty well-outlined, I wouldn't of written it much differently)

Proof **:**
We first show that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, and therefore also in $\mathbb{I}_K$, since it has a finer topology. Consider any $x \in \mathbb{A}_K - \mathbb{I}_K^1$. We will construct an open neighborhood U_x of x that is disjoint from $\mathbb{I}_K^1$. The union of the U_x is then the open complement of the closed set $\mathbb{I}_K^1$. For each $\epsilon > 0$, finite $S \subseteq M_K$, and $x \in \mathbb{A}_K$ we define

$$U_\epsilon(x, S) := \{u \in \mathbb{A}_K : \|u - x\|_v < \epsilon \text{ for } v \in S \text{ and } \|u\|_v \leq 1 \text{ for } v \notin S\},$$

which is a basic open set of $\mathbb{A}_K$ (a product of open sets U_v for $v \in S$ and $\mathcal{O}_v$ for $v \notin S$).

The case $\|x\| < 1$. Let S be a finite set containing the Archimedean places $v \in M_K$ and all v for which $\|x\|_v > 1$, such that $\prod_{v \in S} \|x\|_v < 1$: such an S exists since $\|x\| < 1$ and $\|x\|_v \leq 1$ for almost all v. For all sufficiently small $\epsilon > 0$ the set $U_x := U_\epsilon(x, S)$ is an open neighborhood of x disjoint from $\mathbb{I}_K^1$ because every $y \in U_x$ must satisfy $\|y\| < 1$.

The case $\|x\| > 1$. Let B be twice the product of all the $\|x\|_v$ greater than 1. Let S be the finite set containing the Archimedean places $v \in M_K$, all nonarchimedean v with residue field cardinality less than $2B$, and all v for which $\|x\|_v > 1$. For all sufficiently small $\epsilon > 0$ the set $U_x := U_\epsilon(x, S)$ is an open neighborhood of x disjoint from $\mathbb{I}_K^1$ because for every $y \in U_x$, either $\|y\|_v = 1$ for all $v \notin S$, in which case $\|y\| > 1$, or $\|y\|_v < 1$ for some $v \notin S$, in which case $\|y\|_v < 1/(2B)$ and $\|y\| < 1$.

This proves that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$, and therefore also in $\mathbb{I}_K$. To prove that the subspace topologies coincide, it suffices to show that for every $x \in \mathbb{I}_K^1$ and open $U \subseteq \mathbb{I}_K$ containing x there exists open sets $V \subseteq \mathbb{I}_K$ and $W \subseteq \mathbb{A}_K$ such that $x \in V \subseteq U$ and $V \cap \mathbb{I}_K^1 = W \cap \mathbb{I}_K^1$; this implies that every neighborhood basis in the subspace topology of $\mathbb{I}_K^1 \subseteq \mathbb{I}_K$ is a neighborhood basis in the subspace topology of $\mathbb{I}_K^1 \subseteq \mathbb{A}_K$ (the latter is a priori coarser than the former).

So consider any $x \in \mathbb{I}_K^1$ and open neighborhood $U \subseteq \mathbb{I}_K$ of x. Then U contains a basic open set

$$V = \{u \in \mathbb{A}_K : \|u - x\|_v < \epsilon \text{ for } v \in S \text{ and } \|u\|_v \leq 1 \text{ for } v \notin S\},$$

for some $\epsilon > 0$ and finite $S \subseteq M_K$ (take $S = \{v \in M_K : \|x\| \neq 1 \text{ or } \pi_v(U) \neq \mathcal{O}_v\}$ and $\epsilon > 0$ small enough). If we now put $W := U_\epsilon(x, S)$ then $x \in V \subseteq U$ and $V \cap \mathbb{I}_K^1 = W \cap \mathbb{I}_K^1$ as desired.

Theorem 5.1.12: Fujisaki's Lemma

Let K be any global field. Then the principal ideles $K^\times \subseteq \mathbb{I}_K$ are a discrete cocompact subgroup of the group of 1-ideles $\mathbb{I}_K^1$.

Proof **:**

As $K^\times$ is discrete in $\mathbb{I}_K$, it is discrete in the subspace $\mathbb{I}_K^1$. As in the proof of theorem 5.1.5, to prove that $K^\times$ is cocompact in $\mathbb{I}_K^1$ it suffices to exhibit a compact set $W \subseteq \mathbb{A}_K$ for which $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$ under the quotient map (here we are using Lemma 26.8: $\mathbb{I}_K^1$ is closed so $W \cap \mathbb{I}_K^1$ is compact).

To construct W we first choose $a \in \mathbb{A}_K$ such that $\|a\| > B_K$, where B_K is the Blichfeldt-Minkowski constant in theorem 5.1.6, and let

$$W := L(a) = \{x \in \mathbb{A}_K : \|x\|_v \leq \|a\|_v \text{ for all } v \in M_K\}.$$

Now consider any $u \in \mathbb{I}_K^1$. We have $\|u\| = 1$, so $\|\frac{a}{u}\| = \|a\| > B_K$, and by theorem 5.1.6 there is a $z \in K^\times$ for which $\|z\|_v \leq \|\frac{a}{u}\|_v$ for all $v \in M_K$. Therefore $zu \in W$. Thus every $u \in \mathbb{I}_K^1$ can be written as $u = z^{-1} \cdot zu$ with $z^{-1} \in K^\times$ and $zu \in W \cap \mathbb{I}_K^1$. Thus $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$ under the quotient map $\mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$, which is continuous, and it follows that $\mathbb{I}_K^1/K^\times$ is compact.

Fujisaki's lemma is a generalization of many previous results, and can be used to prove many of the finiteness or bounding results seen in [ChwNAc], including the proof of Dirichlet's Unit Theorem.

Definition 5.1.13: Norm-1 Idele Class Group

Let K be a global field. Then the [compact] group

$$C_K^1 = \mathbb{I}_K^1/K^\times$$

is the *norm-1 idele class group.*

Let us now generalize the idele norm to map to idele groups:

Definition 5.1.14: Idele Norm

Let L/K be a finite separable extension of global field.s Then the *idele norm* $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ is given by $N_{L/K}(b_w) = (a_\nu)$ for each

$$a_\nu = \prod_{w|\nu} N_{L_w/K_\nu}(b_w)$$

with $N_{L_w/K_\nu} : L_w \to K_\nu$ is the field norm.

By the above exact sequence, the Idele norm extends the field norm on the subgroup of principal ideles $L^\times \subseteq \mathbb{I}_L$, and we have the commutative diagram relating the three norms:

$$\begin{tikzcd}
L^\times \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathbb{I}_L \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathcal{I}_L \arrow[d, "\mathrm{N}_{L/K}"] \\
K^\times \arrow[r] & \mathbb{I}_K \arrow[r] & \mathcal{I}_K
\end{tikzcd}$$

which gives:

$$\begin{tikzcd}
C_L \arrow[r, two heads] \arrow[d, "\mathrm{N}_{L/K}"] & \mathrm{Cl}_L \arrow[d, "\mathrm{N}_{L/K}"] \\
C_K \arrow[r, two heads] & \mathrm{Cl}_K
\end{tikzcd}$$

5.2 Artin Homomorphism

Let us now combine the local Artin homomorphisms to define a global Artin homomorphism. To setup, let K be a global field, choose a separable closure K^{sep}, for each ν of K choose a separable closure K_ν^{sep}, and let $K^{\mathrm{ab}}, K_\nu^{\mathrm{ab}}$ denote the maximal abelian extensions within these separable closures. All abelian extension for the remainder of this chapter shall be within these maximal abelian extensions. Then recall that for each K_ν we have:

$$\theta_{K_\nu} : K_\nu^\times \to \mathrm{Gal}_{K_\nu}(K_\nu^{\mathrm{ab}})$$

where for each finite abelian extension L/K and each place $w|\nu$ of L, composing θ_{K_ν} with the natural map $\mathrm{Gal}_{K_\nu}(K^{\mathrm{ab}}) \twoheadrightarrow \mathrm{Gal}_{K_\nu}(L_w)$ gives the surjective homomorphism:

$$\theta_{L_w/K_\nu} : K_\nu^\times \to \mathrm{Gal}_{K_\nu}(L_w)$$

which has kernel $N_{L_w/K_\nu}(L_w^\times)$. In the case where K_ν is nonarchimedean and L_w/K_ν is unramified, for all uniformizers π_ν of K_ν:

$$\theta_{L_w/K_\nu}(\pi_\nu) = \mathrm{Frob}_{L_w/K_\nu}$$

Next, define:

$$\varphi_w : \mathrm{Gal}_{K_\nu}(L_w) \to \mathrm{Gal}_K(L)$$
$$\sigma \mapsto \sigma|_L$$

which is certainly well-defined and injective (recall each $y \in L_w$ can be written as lx, $l \in L$ and $x \in K_\nu$). In particular, if ν is Archimedean, $\varphi_w(\mathrm{Gal}_{K_\nu}(L_w))$ is trivial or generated by the involution given by complex conjugation in $L_w \cong \mathbb{C}$, and if ν is finite and $\mathfrak{q}$ is the prime of L corresponding go $w|\nu$, then $\varphi_w(\mathrm{Gal}_{K_\nu}(L_w))$ is the familiar decomposition group $D_\mathfrak{q} \subseteq \mathrm{Gal}_K(L)$. The image is the stabalizer of w under the action of $\mathrm{Gal}_K(L)$ on $\{w|\nu\}$. The composition $\varphi_w \circ \theta_{L_w/K_\nu} : K_\nu^\times \to \mathrm{Gal}_K(L)$ gives a map independence of choice of $w|\nu$ (namely since $\varphi_w(\theta_{L_w/K_\nu}(\pi_\nu) = \mathrm{Frob}_\nu$.

Let us now bring in $\mathbb{I}_K$. For each place ν of K, we can embed $K_\nu^\times$ into the idele group $\mathbb{I}_K$ via:

$$\begin{aligned} \iota_\nu : K_\nu^\times &\hookrightarrow \mathbb{I}_K \\ \alpha &\mapsto (1, 1, ..., 1, \alpha, 1, ...) \end{aligned}$$

Note that the image intersects $K^\times \subseteq \mathbb{I}_K$ trivially. The embedding is compatible with the idele norm in that if L/K is any finite separable extension and w is a place of L that extends the place ν of K, then the diagram commutes

$$\begin{tikzcd} L_w^\times \arrow[r, "N_{L_w/K_\nu}"] \arrow[d, hook, "\iota_w"] & K_\nu^\times \arrow[d, hook, "\iota_\nu"] \\ \mathbb{I}_L \arrow[r, "N_{L/K}"] & \mathbb{I}_K \end{tikzcd}$$

Finally, we define a system of compatible homomorphisms to take the limit of. For each finite abelian extension L/K, for each place ν of K, we can pick a place w of L st $w|\nu$ and define

$$\begin{aligned} \varphi_{L/K} : \mathbb{I}_K &\to \mathrm{Gal}_K(L) \\ (a_\nu) &\mapsto \prod_\nu \varphi_w(\theta_{L_w/K_\nu}(a_\nu)) \end{aligned}$$

This product is well-defined as $a_\nu \in \mathcal{O}_\nu^\times$ and ν is unramified in L for a.e. ν, which implies:

$$\varphi_w(\theta_{L_w/K_\nu}(a_\nu)) = \mathrm{Frob}_\nu^{\nu(a_\nu)} = 1 \qquad \text{a.e.}$$

It is furthermore a continuous homomorphism, with kernel being the union of open sets of the form

$$U_a = U_S \times \prod_{\nu \notin S} \mathcal{O}_\nu^\times \subseteq \ker \theta_{L/K}$$

where $a = (a_\nu) \in \ker \theta_{L/K}$, S contains all ramified ν and all ν such that $a_\nu \notin \mathcal{O}_\nu^\times$, and U_S is the kernel of $(a_\nu)_{\nu \in S} \mapsto \prod_{\nu \in S} \varphi_w(\theta_{L_w/K_\nu}))$.

These maps work well with finite abelian extensions: if $L_1 \subseteq L_2$ is a finite abelian extension of K then

$$\theta_{L_1/K}(a) = \theta_{L_2/K}(a)|_{L_1} \qquad \forall a \in \mathbb{I}_K$$

Thus, the collection $\theta_{L/K}$ where L ranges over finite abelian exensions of K in K^{ab} ordered by inclusion form a compatible system of homomorphism from $\mathbb{I}_K$ to $\varprojlim_L \mathrm{Gal}_K(L) \cong \mathrm{Gal}_K(K^{\mathrm{ab}})$. By the universal property of profinite completion, they uniquely determine a continuous homomorphism. From this, we have built-up to the map:

Definition 5.2.1: Global Artin Homomorphism

Let K be a global field. Then the *global Artin homomorphism* is the continuous homomorphism:

$$\theta_K : \mathbb{I}_K \to \mathrm{Gal}_K(K^{\mathrm{ab}}) \cong \varprojlim_{L} \mathrm{Gal}_K(L)$$

given by $\theta_{L/K} : \mathbb{I}_K \to \mathrm{Gal}_K(L)$ where L ranges over all finite abelian extension of K in K^{ab}.

This map is the natural map that holds all the local artin homomorphism

Proposition 5.2.2: Universal Property Global Artin Map

Let K be a global field. Then the global Artin homomorphism θ_K is the unique continuous homomorphism $\mathbb{I}_K \to \mathrm{Gal}_K(K^{\mathrm{ab}})$ with the property that for every finite abelian extension L/K in K^{ab} and every place w of L lying over a place ν of K, the following diagram commutes:

$$\begin{tikzcd}
K_v^\times \arrow[r, "\theta_{L_w/K_v}"] \arrow[d, hook, "\iota_v"] & \mathrm{Gal}(L_w/K_v) \arrow[d, hook, "\phi_w"] \\
\mathbb{I}_K \arrow[r, "\theta_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

where the homomorphism $\theta_{L/K}$ is defined by $\theta_{L/K}(a) = \theta_K(a)|_L$.

***Proof* :**
We just showed that θ_K satisfies the property, what's left to show is uniqueness.

For the sake of contradiction, assume that there is another continuous homomorphism $\theta'_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the same property. We may view elements of $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim \mathrm{Gal}(L/K)$ as elements of $\prod_{L/K} \mathrm{Gal}(L/K)$, where L varies over finite abelian extensions of K in K^{ab}. If θ_K and θ'_K are not identical, then there must be an $a \in \mathbb{I}_K$ and a finite abelian extension L/K for which $\theta_{L/K}(a) \neq \theta'_{L/K}(a)$.

Let S be a finite set of places of K that includes all places v for which $a_v \notin \mathcal{O}_v^\times$ and all ramified places of L/K. Define $b \in \mathbb{I}_K$ by $b_v := 1$ for $v \in S$ and $b_v := a_v$ for $v \notin S$, so that $a = b\prod_{v\in S} \iota_v(a_v)$. Then $\theta_{L_w/K_v}(b_v) = 1$ for all places v, so we must have $\theta_{L/K}(b) = 1 = \theta'_{L/K}(b)$, and for $v \in S$ we have

$$\theta_{L/K}(\iota_v(a_v)) = \phi_w(\theta_{L_w/K_v}(a_v)) = \theta'_{L/K}(\iota_v(a_v)),$$

by the commutativity of the diagram in the proposition. But then

$$\theta_{L/K}(a) = \theta_{L/K}(b) \prod_{v\in S} \theta_{L/K}(\iota_v(a_v)) = \theta'_{L/K}(b) \prod_{v\in S} \theta'_{L/K}(\iota_v(a_v)) = \theta'_{L/K}(a),$$

forcing $\theta'_K = \theta_K$, as we sought to show.

With this build-up, we can now state the global Artin reciprocity law

Theorem 5.2.3: Global Artin Reciprocity

Let K be a global field. Then the kernel of the global Artin homomorphism θ_K contains $K^\times$, and we get a continuous homomorphism:

$$\theta_K : C_K \to \text{Gal}_K(K^{\text{ab}})$$

where $C_K = \mathbb{I}_K/K^\times$, where every finite abelian extension $K \subseteq L \subseteq K^{\text{ab}}$ we get the homomorphism

$$\theta_{L/K} : C_K \to \text{Gal}_K(L)$$

by composing θ_K with the natural surjection $\text{Gal}_K(K^{\text{ab}}) \twoheadrightarrow \text{Gal}_K(L)$ which has kernel $N_{L/K}(C_L)$, hence:

$$\frac{C_K}{N_{L/K}(C_L)} \cong \text{Gal}_K(L)$$

Proof **:**
This is just taking the quotient of the above map and following through the consequences, with the well-definedness needing to be the only non-immediate result to check.

Theorem 5.2.4: Global Existence Theorem

Let K be a global field. Then for every finite index open subgroup H of C_K, there exists a finite abelian extension $K \subseteq L \subseteq K^{\text{ab}}$ where

$$N_{L/K}(C_L) = H$$

Proof **:**
not presented

Note that we have not specified whether θ_K is injective or surjective. It may in fact be one or the other:

1. When K is a number field, θ_K is surjective but not injective
2. When K is a global function field, θ_K is injective but not surjective, the image consisting on automorphisms $\sigma \in \text{Gal}_K(K^{\text{ab}})$ corresponding to integer powers of the Frobenius automorphism of $\text{Gal}_k(k^{\text{sep}})$ where k is the constant field of K

If we take the profinite completion will give an isomorphism:

Theorem 5.2.5: Main Theorem of Global Class Field Theory

Let K be a global field. Then the global Artin homomorphism θ_K induces a natural isomorphism

$$\widehat{\theta}_K : \widehat{C_K} \xrightarrow{\cong} \mathrm{Gal}_K(K^{\mathrm{ab}})$$

of profinite groups

Proof **:**
not presented

We thus get the corerspondence

$$\left\{\begin{matrix}\text{Finite Extension } E/K \\ K \subseteq E \subseteq K^{\mathrm{ab}}\end{matrix}\right\} \underset{(K^{\mathrm{ab}})^{\theta_K(H)}}{\overset{N_{E/K}(C_E)}{\rightleftarrows}} \left\{\begin{matrix}\text{closed subgroups } H \\ H \subseteq \mathrm{Aut}_K(K^{\mathrm{ab}})\end{matrix}\right\}$$

with a corresponding isomorphism $C_K/H \cong \mathrm{Gal}_K(E)$ where $H = N_{E/K}(C_E)$. The global Artin homomorphism also has the following functorial property that can be thought of as the first part of Langland's program

Theorem 5.2.6: Functoriality of Artin Homomorphism

Let K be a global field and L/K a finite separable extension (not necessarily abelian!). Then the following diagram commutes

Proof **:**
exercise

5.2.1 Relating to Ideal-Theoretic Version

In the ideal-theoretic case (the places approach), we directly worked with global fields, and hence needed to use a modulus to isolate the ramifying primes. This shall could be "resolved" instead with the right choice of open subgroup to mod C_K. Let K be a number field and let $\mathfrak{m} : M_K \to \mathbb{Z}_{\geq 0}$ be a modulus for K, which we view as a formal product $\mathfrak{m} = \prod_v v^{e_v}$ over the places v of K with $e_v \leq 1$ when v is Archimedean and $e_v = 0$ when v is complex. For each place v we define the open subgroup

$$U_K^{\mathfrak{m}}(v) := \begin{cases} \mathcal{O}_v^\times & \text{if } v \nmid \mathfrak{m}, \text{ where } \mathcal{O}_v^\times := K_v^\times \text{ when } v \text{ is infinite}), \\ \mathbb{R}_{>0} & \text{if } v|\mathfrak{m} \text{ is real, where } \mathbb{R}_{>0} \subseteq \mathbb{R}^\times \cong \mathcal{O}_v^\times := K_v^\times, \\ 1+\mathfrak{p}^{e_v} & \text{if } v|\mathfrak{m} \text{ is finite, where } \mathfrak{p} = \{x \in \mathcal{O}_v : |x|_v < 1\}, \end{cases}$$

and let $U_K^{\mathfrak{m}} := \prod_v U_K^{\mathfrak{m}}(v) \subseteq \mathbb{I}_K$ denote the corresponding open subgroup of $\mathbb{I}_K$. The image $\overline{U}_K^{\mathfrak{m}}$ of $U_K^{\mathfrak{m}}$ in the idele class group $C_K = \mathbb{I}_K/K^\times$ is a finite index open subgroup. The idelic version of a ray class group is the quotient

$$C_K^{\mathfrak{m}} := \mathbb{I}_K/(U_K^{\mathfrak{m}}K^\times) = C_K/\overline{U}_K^{\mathfrak{m}},$$

and we have isomorphisms

$$C_K^{\mathfrak{m}} \cong \mathrm{Cl}_K^{\mathfrak{m}} \cong \mathrm{Gal}(K(\mathfrak{m})/K),$$

where $\mathrm{Cl}_K^{\mathfrak{m}}$ is the ray class group for the modulus $\mathfrak{m}$, and $K(\mathfrak{m})$ is the corresponding ray class field, which we can now define as the finite abelian extension L/K for which

$$\mathrm{N}_{L/K}(C_L) = \overline{U}_K^{\mathfrak{m}}$$

which we know exists by the Global Existence Theorem.

If L/K is any finite abelian extension, then $\mathrm{N}_{L/K}(C_L)$ contains $\overline{U}_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$; this follows from the fact that the groups $\overline{U}_K^{\mathfrak{m}}$ form a fundamental system of open neighborhoods of the identity. Indeed, the conductor of the extension L/K is precisely the minimal modulus $\mathfrak{m}$ for which this is true. It follows that every finite abelian extension L/K lies in a ray class field $K(\mathfrak{m})$, with $\mathrm{Gal}(L/K)$ isomorphic to a quotient of a ray class group $C_K^{\mathfrak{m}}$.

5.3 Application: Chebotarev Density Theorem

Look at Lenstra-Chebotarev PDF, it has an excellent intuition on the densities!

We need some build-up

Proposition 5.3.1: Dirichlet Density to Ray Class Element

Let $\mathfrak{m}$ be a modulus for a number field K, and let $\mathrm{Cl}_K^{\mathfrak{m}}$ be the corresponding ray class group. Then for every ray class $c \in \mathrm{Cl}_K^{\mathfrak{m}}$, the Dirichlet density of the set of primes $\mathfrak{p}$ of K lie in c is

$$\frac{1}{\#\mathrm{Cl}_K^{\mathfrak{m}}}$$

Proof **:**
Apply corollary 4.2.13 to $\mathcal{C} = \mathcal{R}_K^{\mathfrak{m}}$

As the ray class fields exists (theorem 4.2.21), we get the abelian case. We next require one more result for the main theorem:

Corollary 5.3.2: Dirichlet Density singleton Conjugacy

Let L/K be a finite abelian extension of number fields with galois group G. THen for every $\sigma \in G$, the Dirichlet density of the set S of primes $\mathfrak{p}$ of K unramified in L for which $\mathrm{Frob}_{\mathfrak{p}} = \{\sigma\}$ is

$$\frac{1}{\#G}$$

Proof **:**
Let $\mathfrak{m} = \mathrm{cond}(L/K)$ be the conductor of the extension L/K; then L is a subfield of the ray class field $K(\mathfrak{m})$ and $\mathrm{Gal}(L/K) \cong \mathrm{Cl}_K^{\mathfrak{m}}/H$ for some subgroup H of the ray class group. For each unramified prime $\mathfrak{p}$ of K we have $\mathrm{Frob}_{\mathfrak{p}} = \{\sigma\}$ if and only if $\mathfrak{p}$ lies in one of the ray classes contained in the coset of H in $\mathrm{Cl}_K^{\mathfrak{m}}/H$ corresponding to σ. The Dirichlet density of the set of primes in each ray class is $1/\#\,\mathrm{Cl}_K^{\mathfrak{m}}$, by Proposition 28.10, and there are $\#H$ ray classes in each

coset of H; thus $d(S) = \#H/\# \operatorname{Cl}_K^{\mathfrak{m}} = 1/\#G$ as we sought to show.

Theorem 5.3.3: Chebotarev Density Theorem

Let L/K be a finite galois extension of number fields with galois group $G = \operatorname{Gal}_K(L)$. Let $C \subseteq G$ be a union of conjugacy classes, and let S be the set of primes$\mathfrak{p}$ of K unramified in L with $\operatorname{Frob}_{\mathfrak{p}} \subseteq C$. Then:

$$d(S) = \frac{\#C}{\#G}$$

Note that G is not assumed to be abelian, hence in this case $\operatorname{Frob}_{\mathfrak{p}}$ is a conjugacy class

***Proof* :**

It suffices to consider the case where C is a single conjugacy class, which we now assume; we can reduce to this case by partitioning C into conjugacy classes and summing Dirichlet densities (as proved on Problem Set 9). Let S be the set of primes $\mathfrak{p}$ of K unramified in L for which $\operatorname{Frob}_{\mathfrak{p}}$ is the conjugacy class C.

Let $\sigma \in G$ be a representative of the conjugacy class C, let $H_\sigma := \langle \sigma \rangle \subseteq G$ be the subgroup it generates, and let $F_\sigma := L^{H_\sigma}$ be the corresponding fixed field. Let T_σ be the set of primes $\mathfrak{q}$ of F_σ unramified in L for which $\operatorname{Frob}_{\mathfrak{q}} = \{\sigma\} \subseteq \operatorname{Gal}(L/F_\sigma) \subseteq \operatorname{Gal}(L/K)$ (note that the Frobenius class $\operatorname{Frob}_{\mathfrak{q}}$ is a singleton because $\operatorname{Gal}(L/F_\sigma) = H_\sigma$ is abelian). We have $d(T_\sigma) = 1/\#H_\sigma$, since L/F_σ is abelian, by Corollary 28.11.[2]

As you proved on Problem Set 9, restricting to degree-1 primes (primes whose residue field has prime order) does not change Dirichlet densities, so let us replace S and T_σ by their subsets of degree-1 primes, and define $T_\sigma(\mathfrak{p}) := \{\mathfrak{q} \in T_\sigma : \mathfrak{q}|\mathfrak{p}\}$ for each $\mathfrak{p} \in S$.

Claim: For each prime $\mathfrak{p} \in S$ we have $\#T_\sigma(\mathfrak{p}) = [G : H_\sigma]$.

Proof of claim: Let $\mathfrak{r}$ be a prime of L lying above $\mathfrak{q} \in T_\sigma(\mathfrak{p})$. Such an $\mathfrak{r}$ is unramified, since $\mathfrak{p}$ is, and we have $\operatorname{Frob}_{\mathfrak{r}} = \sigma$, since $\operatorname{Frob}_{\mathfrak{q}} = \{\sigma\}$. It follows that $\operatorname{Gal}(\mathbb{F}_{\mathfrak{r}}/\mathbb{F}_{\mathfrak{q}}) = \langle \overline{\sigma} \rangle \simeq H_\sigma$.

Therefore $f_{\mathfrak{r}/\mathfrak{q}} = \#H_\sigma$ and $\#\{\mathfrak{r}|\mathfrak{q}\} = 1$, since $\#H_\sigma = [L : F_\sigma] = \sum_{\mathfrak{r}|\mathfrak{q}} e_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{r}/\mathfrak{q}}$. We have $f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} = \#H_\sigma$, since $f_{\mathfrak{q}/\mathfrak{p}} = 1$ for degree-1 primes $\mathfrak{q}|\mathfrak{p}$, and $e_{\mathfrak{r}/\mathfrak{p}} = 1$, thus

$$\#G = [L : K] = \sum_{\mathfrak{r}|\mathfrak{p}} e_{\mathfrak{r}/\mathfrak{p}} f_{\mathfrak{r}/\mathfrak{p}} = \#\{\mathfrak{r}|\mathfrak{p}\}\#H_\sigma = \#T_\sigma(\mathfrak{p})\#H_\sigma,$$

We now observe that

$$\sum_{\mathfrak{p} \in S} \operatorname{N}(\mathfrak{p})^{-s} = \sum_{\sigma \in C} \sum_{\mathfrak{p} \in S} \frac{1}{[G : H_\sigma]} \sum_{\mathfrak{q} \in T_\sigma(\mathfrak{p})} \operatorname{N}(\mathfrak{q})^{-s} = \frac{\#C}{[G : H_\sigma]} \sum_{\mathfrak{q} \in T_\sigma} \operatorname{N}(\mathfrak{q})^{-s}$$

since $\operatorname{N}(\mathfrak{q}) = \operatorname{N}(\mathfrak{p})$ for each degree-1 prime $\mathfrak{q}$ lying above a degree-1 prime $\mathfrak{p}$, and therefore

$$d(S) = \frac{\#C}{[G : H_\sigma]} d(T_\sigma) = \frac{\#C\#H_\sigma}{[G : H_\sigma]} = \frac{\#C}{\#G}.$$

completing the proof

Index

Bibliography

Chwojko-Srawley, Nathanael. *Everything You Need To Know About Partial Differential Equations.* 1st ed. NA. URL: `https://nathanaelsrawley.com/assets/pdfs/notes/EYNTKA_PDEs.pdf`.

– *Everything You Need To Know About Real Analysis.* 1st ed. Vol. 1. NA. URL: `https://nathanaelsrawley.com/assets/pdfs/notes/EYNTKA_real_analysis.pdf`.

– *Everything You Need To Know About Undergraduate Algebra.* 1st ed. NA. URL: `https://nathanaelsrawley.com/assets/pdfs/notes/EYNTKA_algebra.pdf`.

– *Everything You Need To Know About Complex Analysis.* 1st ed. NA. URL: `https://nathanaelsrawley.com/assets/pdfs/notes/EYNTKA_complex_analysis.pdf`.