Algebraic Number Theory Summary

SIXUAN LOU

Contents

0. Overview

This document is a recollection of things I have learned from the Part III Michaelmas term lectures given by Professor Jack Thorne. The course has an emphasis on developing basic local (p-adic) tools in algebraic number theory, and using them to understand the global structure. We will not be able to give a proof of global class field theory.

This note is not an accurate representation of the lectures (look up Professor Thorne's website for the official lecture notes). I have omitted a large portion of technical proofs, interested readers are encouraged to work them out. Please send comments and corrections to `tmzl dot sx at gmail dot com`.

1. Dedekind Domains

We are interested in Dedekind domains because they are naturally associated to a number field K as the ring of integers $\mathcal{O}_K$. One goal in algebraic number theory is to understand the field K and extensions L/K through the "internal" arithmetic structures of these fields. These "internal" arithmetic structures often refer to the ideal structure of their rings of integers. One manifestation of this idea is the class field theory, which classify **all** abelian extensions of a number field in terms of some arithmetic object, called the "ray class group" $H(m)$ of the field. In this section we will investigate the basic properties of a Dedekind domain. We will prove the most important property of a Dedekind domain, that is the unique factorization of ideals.

Date: June 13, 2020.

We start our investigation of Dedekind domains by examining what do they look like "locally". These local objects are called "discrete valuation rings", and they are of particular simple structure.

Definition 1.1 (DVR)**.** Let A be a ring, say A is a **discrete valuation ring (DVR)** if (1) A is a PID and (2) A has a unique nonzero prime ideal $\mathfrak{m}$, principally generated by some element π.

Observe a DVR $(A, \mathfrak{m})$ is in particular a local ring, so the elements outside the maximal ideal are units, hence we have decomposition $A = (\pi)A \sqcup A^\times$. We can further decompose $(\pi)A = (\pi^2)A \sqcup (\pi)A^\times$, hence inductively we obtain $A = (\sqcup_{i\geq 0}(\pi^i)A^\times) \sqcup (\cap_{i\geq 0}(\pi^i))$. Where elements in $\cap_{i\geq 0}(\pi^i)$ are "infinitely divisible" by π. Since A is a PID, in particular the ideal $\cap_{i\geq 0}(\pi^i)$ is principally generated. Since by definition $(\pi) \cdot \cap_{i\geq 0}(\pi^i) \subseteq \cap_{i\geq 0}(\pi^i)$, so by NAK, it equals zero. So any nonzero element x in A has unique expression $x = \pi^n u$, where $n \geq 0$ and $u \in A^\times$. Let K denote the fraction field of A, then any nonzero element $x \in K$ has unique expression $\pi^n u$, where $n \in \mathbb{Z}$ and $u \in A^\times$. The element π is called a **uniformizer** of the DVR A. For a nonzero element $x = \pi^n u \in K$, the integer n is independent of the choice of π and called the **(discrete) valuation** of x, denoted $\nu(x)$. The map $\nu : K^\times \to \mathbb{Z}$ satisfies properties

(1) $\nu : K^\times \to \mathbb{Z}$ is a surjective group homomorphism,
(2) $\forall x, y \in K^\times : \nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, and the equality holds if $\nu(x) \neq \nu(y)$.

Conversely, if we are given a field K equipped with a valuation $\nu : K^\times \to \mathbb{Z}$, we can define subring $A_K := \{x \in K^\times : \nu(x) \geq 0\} \cup \{0\}$ and ideal $\mathfrak{m}_K := \{x \in K^\times : \nu(x) > 0\} \cup \{0\}$. Then the resulting pair $(A_K, \mathfrak{m}_K)$ is a DVR. So given field K, there exists bijection

$$\left\{\begin{matrix}\text{subrings } A \subseteq K \text{ s.t. } A \text{ is a DVR} \\ \text{and } \operatorname{Frac} A = K\end{matrix}\right\} \longleftrightarrow \{\text{valuations } \nu : K^\times \to \mathbb{Z}.\}$$

DVRs are characterized as follows:

Lemma 1.2. Let A be a Noetherian domain, then

$$A \text{ is a DVR} \iff A \text{ is normal and has a unique nonzero prime.}$$

In order to see explicitly the meaning of the statement "Dedekind domains are locally DVRs", we take a detour and recall some basic properties of localization. Let A be a ring, $S \subseteq A$ a multiplication subset,

(1) $S^{-1}A$ is a ring, it admits a natural map $\varphi : A \to S^{-1}A$ sending $a \in A$ to $a/1$, with kernel all elements annihilated by S.
(2) If A is a domain, and $0 \notin S$, then $S^{-1}A$ may be identified with the subring $\{a/s : a \in A, s \in S\}$ of of the fraction field.
(3) The localization functor $S^{-1} : Mod(A) \to Mod(A)$ is exact. In particular, if $I \lhd A$, $S^{-1}I$ is an ideal of $S^{-1}A$, identified with $\{x/s : x \in I, s \in S\}$.
(4) We have correspondence of prime ideals

$$\left\{\begin{matrix}\text{prime ideals } \mathfrak{p} \lhd A \\ \text{s.t. } \mathfrak{p} \cap S = \varnothing\end{matrix}\right\} \longleftrightarrow \{\text{prime ideals } \mathfrak{q} \lhd S^{-1}A.\}$$

given by $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ and $\varphi^{-1}(\mathfrak{q}) \hookleftarrow \mathfrak{q}$.

Therefore for any prime ideal $\mathfrak{p} \lhd A$, the localization $A_\mathfrak{p} := (A \setminus \mathfrak{p})^{-1}A$ is a local ring with maximal ideal $\mathfrak{p}A_\mathfrak{p}$. A **Dedekind domain** is a Noetherian domain A satisfying the following equivalent properties

(1) For any nonzero prime $\mathfrak{p} \lhd A$, $A_{\mathfrak{p}}$ is a DVR,
(2) A is normal and of Krull dimension 1.

We now study the ideal structure of DVR and Dedekind domains.

Let A be a domain with fractional field K, a **fractional ideal** of A is a finitely generated A-submodule of K. Let I, J be fractional ideals of A, we may verify the sum $I + J$, product $I \cdot J$ and the **ideal quotient** $(I : J) := \{x \in K : xJ \subseteq I\}$ are again fractional ideals of A. Moreover, these operations play well with localizations. If $S \subseteq A$ is a multiplicative subset, then $S^{-1}I, S^{-1}J$ are fractional ideals of $S^{-1}A$ and $S^{-1}(I + J) = (S^{-1}I) + (S^{-1}J)$, $S^{-1}(I \cdot J) = (S^{-1}I) \cdot (S^{-1}J)$, $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$. Observe if A is a DVR with uniformizer π, then each fractional ideal I of A is principally generated by (π^i) for some $i \in \mathbb{Z}$. So if A is a Dedekind domain, the equality $I \cdot (A : I) = I$ holds when localized at each prime of A, hence it holds globally. This makes the set of fractional ideals of a Dedekind domain A into a group with unit (1), denoted $\operatorname{Div} A$. In particular $\operatorname{Div} A_{\mathfrak{p}} \cong \mathbb{Z}$ for all nonzero prime $\mathfrak{p} \lhd A$.

Let A be a Dedekind domain with fractional field K. For each prime $\mathfrak{p} \lhd A$, localization gives us a homomorphism $\nu_{\mathfrak{p}} : \operatorname{Div} A \to \operatorname{Div} A_{\mathfrak{p}} \cong \mathbb{Z}$. The homomorphism $\nu_{\mathfrak{p}}$ can be described explicitly by $\nu_{\mathfrak{p}}(I) = \nu_{\mathfrak{p}}(x)$, where $x \in IA_{\mathfrak{p}}$ principally generates $IA_{\mathfrak{p}}$ and $\nu_{\mathfrak{p}}$ on the RHS is an abuse of notation which denotes the discrete valuation associated to the DVR $A_{\mathfrak{p}}$. Since $\nu_{\mathfrak{p}}(\mathfrak{p}) = 1$, the homomorphism $\nu_{\mathfrak{p}}$ is surjective. Taking product over all nonzero prime, we get an injective homomorphism

$$\prod_{\mathfrak{p}} \nu_{\mathfrak{p}} : \operatorname{Div} A \to \prod_{\mathfrak{p}} \mathbb{Z}\,.$$

We can show for any $I \in \operatorname{Div} A$, there are only finitely many nonzero primes $\mathfrak{p}$ of A such that $\nu_{\mathfrak{p}}(I) \neq 0$, to the homomorphism lands in $\oplus_{\mathfrak{p}} \mathbb{Z}$. We arrive at the main proposition of the section, the unique factorization of ideals in Dedekind domain:

Proposition 1.3. (1) The map $\prod_{\mathfrak{p}} \nu_{\mathfrak{p}} : \operatorname{Div} A \to \bigoplus_{\mathfrak{p}} \mathbb{Z}$ is an isomorphism.
(2) For any $I \in \operatorname{Div} A$, $I = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(I)}$.

2. Complete DVRs

Let $f \in \mathbb{Z}[x]$ be a polynomial, if $\alpha \in \mathbb{Z}$ is a root of f, then we have a sequence $(\alpha_n)_n$, where $\alpha_n := x \bmod p^n$ is a root of $\overline{f}(x) \in \mathbb{Z}/p^n[x]$. Hence if f has no roots modulo some p^n, f has no roots over $\mathbb{Z}$. Hensel's lemma gives us a partial converse – under certain assumptions, we may lift a root of $\overline{f}(x) \in \mathbb{Z}/p[x]$ to a root of $f(x) \in \mathbb{Z}_{(p)}[x]$ (a local root of f at prime p). We organize these "sequences of elements modulo p^n ($n \in \mathbb{N}$)" using notion of complete DVR. Complete DVRs will also be essential for a local study of the ramification theory of primes under field extensions.

An **inverse system of groups** is a sequence of groups A_i ($i \in \mathbb{Z}_{>0}$) with group homomorphisms $f_i : A_{i+1} \to A_i$ ($i \in \mathbb{Z}_{>0}$). The **inverse limit**, denoted $\varprojlim_i A_i$, of an inverse system (A_i, f_i) is the subgroup of $\prod_{i=1}^{\infty} A_i$ given by

$$\varprojlim_i A_i := \left\{ (a_i) \in \prod_{i=1}^{\infty} A_i : \forall i \geq 1, f_i(a_{i+1}) = a_i \right\}.$$

This is a ring if all A_i are rings and f_i are ring homomorphisms. The main example we are interested in is the case $(A, (\pi))$ is a DVR, then we have an inverse system $A/(\pi) \leftarrow A/(\pi^2) \leftarrow A/(\pi^3) \leftarrow \cdots$, where all the maps are the quotient maps. In this case, we have a natural homomorphism $A \to \varprojlim_i A/(\pi^i)$ whose kernel is $\cap_{i\geq 1} A/(\pi^i) = 0$, hence it is injective.

We say a DVR A is **complete** if the homomorphism $A \to \varprojlim_i A/(\pi^i)$ is an isomorphism. For $x, y \in \operatorname{Frac} A$, define

$$d(x,y) := \begin{cases} 0 & ,(x = y) \\ 2^{-\nu(x-y)} & ,(x \neq y), \end{cases}$$

then d is a ultrametric on A and A is complete if and only if it is complete as a metric space.

Fix a set $X \subseteq A$ of representatives of residue classes in $A/(\pi)$, with $0 \in X$. Then for each $i \geq 0$, the set X is in bijection with the quotient $\pi^i A/\pi^{i+1}A$. So for each $i \geq 1$ and $a \in A/(\pi^i)$, a has a unique representation $a = a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1}$, where $a_i \in X$. Under this representation, the quotient map $A/(\pi^{i+1}) \to A/(\pi^i)$ is given by forgetting the last digit. So every element $x \in \widehat{A} := \varprojlim_i A/(\pi^i)$ has a unique infinite sum representation $\sum_{i \geq 0} a_i \pi^i$, where $a_i \in X$. Suppose $a_0 = \cdots = a_{n-1} = 0$ and $a_n \neq 0$, then then $a_n \in A^\times$ and we may write $x = \pi^n a_n(1 - \pi y)$, where $y = -\sum_{i \geq 0} \frac{a_{n+i}}{a_n}\pi^i$. We note by geometric series expansion, $1 - \pi y$ has inverse $1 + \pi y + \pi^2 y^2 + \cdots$. So every element $x \in \widehat{A}$ has a unique expression $x = \pi^n u$, where $n \in \mathbb{Z}_{\geq 0}$ and $u \in \widehat{A}^\times$, hence $\widehat{A}$ is a DVR with uniformizer π. Furthermore, using the representation above, we see for each $i \geq 1$, the map $A/\pi^i A \to \widehat{A}/\pi^i \widehat{A}$ is a isomorphism. Therefore $\widehat{A}$ is complete DVR.

Definition 2.1 (p-adic integers, p-adic rationals)**.** Let p be a prime, the localization $\mathbb{Z}_{(p)}$ is a DVR, hence the **ring of p-adic integers** $\mathbb{Z}_p := \widehat{\mathbb{Z}}_{(p)}$ is a complete DVR. The **field of p-adic rationals** is the fraction field $\mathbb{Q}_p := \operatorname{Frac} \mathbb{Z}_p$.

Lemma 2.2 (Hensel's Lemma)**.** Let A be a complete DVR, $f(x) \in A[x]$ a monic polynomial. Suppose given $\alpha \in A$ such that $\nu(f(\alpha)) > 2\nu(f'(\alpha))$, then there exists a unique $a \in A$ such that $f(a) = 0$ and $\nu(a - \alpha) > \nu(f'(\alpha))$.

Proof Idea. We use Newton's method, define $a_1 := \alpha, a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)}$. Induct on n show

(1) $a_n \in A$
(2) $\nu(f'(a_n)) = \nu(f'(a_1))$
(3) $\nu(f(a_n)) \geq 2\nu(f'(a_n)) + 2^{n-1}\nu(f(a_1)/f'(a_1)^2)$.

The element $a \in A$ is constructed as the Cauchy sequence $(a_n)_n$. □

Corollary 2.3. Let (A, π) be a DVR, with residue field $k := A/(\pi)$, $f(x) \in A[x]$ a monic polynomial, $\overline{f}(x) := f(x) \bmod (\pi) \in k[x]$. Suppose given $\overline{\alpha} \in k$ a simple root of $\overline{f}(x)$, then there exists a unique $a \in A$ such that $f(a) = 0$ and $\overline{\alpha} \equiv a \bmod (\pi)$.

Proof. Let $\alpha \in A$ be any lift of $\overline{\alpha}$. Then $\nu(f(\alpha)) \geq 1$ and $\nu(f'(\alpha)) = 0$, apply Hensel's Lemma. □

Hensel's Lemma is very important, many results in the following sections will depend on it. Here is one simple application of it.

***Example* 2.4.** Identify the squares in $\mathbb{Q}_p^\times$. Since $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$, it suffices to determine the squares in $\mathbb{Z}_p^\times$. Let $u \in \mathbb{Z}_p^\times$, consider $f(x) := x^2 - u \in \mathbb{Z}_p[x]$, $f'(x) = 2x$. Suppose v is a root of f. Then $\overline{v} \in \mathbb{Z}/p$ is a root of $\overline{f}(x)$. If $p \neq 2$, then $\nu_p(f'(v)) = \nu_p(2v) = \nu_p(2) = 0$. So $\overline{f}'(\overline{v}) \neq 0$, so $\overline{v}$ is a simple root of $\overline{f}$, so f has a root by Hensel's lemma. If $p = 2$, we cannot apply Hensel directly. Since v is a root of f, it is a root of f modulo $2^3 = 8$. We note $(\mathbb{Z}/8)^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ and $\left(\frac{u}{8}\right) = 1$ if and only if $u \equiv 1 \bmod 8$. If $u \equiv v^2 \bmod 8$, then $\nu_2(f(v)) \geq 3$ and $\nu_2(f'(v)) = \nu_2(2v) = 1$, by Hensel's Lemma, u is a square. To conclude, if

$p \neq 2$, squares in $\mathbb{Q}_p^\times$ are $p^{2k}v$, where $k \in \mathbb{Z}$ and $\left(\frac{v}{p}\right) = 1$. And squares in $\mathbb{Q}_2^\times$ are $2^{2k}v$, where $k \in \mathbb{Z}$ and $v \equiv 1 \bmod 8$.

Here is another application of Hensel's lemma: classifying certain cyclic extensions of $\mathbb{Q}_p$. Consider the mod p map $\mathbb{Z}_p^\times \twoheadrightarrow \mathbb{F}_p^\times$. Let $\overline{\alpha} \in \mathbb{F}_p^\times$, then it is a simple root of $x^p - x \in \mathbb{F}_p[x]$, so there is a unique lift $\tau(\overline{\alpha}) \in \mathbb{Z}_p^\times$. By uniqueness of the lift, we obtain a splitting $\tau : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ of tho mod p map. The splitting τ is called the **Teichmuller lift** . Therefore $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times \mathrm{Ker}(\text{mod } p) = \mathbb{F}_p^\times \times (1 + p\,\mathbb{Z}_p^\times)$. And $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\,\mathbb{Z}_p^\times)$.

Suppose p, q are primes such that $q \mid (p-1)$. Then $\mathbb{Q}_p$ contains $\mathbb{F}_p$, which contains all q-th roots of unity. So by Kummer theory, there is a bijection between isomorphism classes of cyclic extensions of $\mathbb{Q}_p$ of degree q and subgroups of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^q$ of order q. Since inverse limit is left exact,

$$1 + p\,\mathbb{Z}_p^\times \cong \varprojlim_i \mathrm{Ker}((\mathbb{Z}/p^i)^\times \to (\mathbb{Z}/p)^\times).$$

Since the mod p map $(\mathbb{Z}/p^i)^\times \to (\mathbb{Z}/p)^\times$ is surjective, the kernel has order $\phi(p^i)/\phi(p) = p^{i-1}$. Since $(\mathbb{Z}/p^i)^\times$ is cyclic of order $\phi(p^i)$, the kernel is cyclic of order p^{i-1}. Since $(p, q) = 1$, then q-th power map from kernel to itself is an isomorphism. So $(1 + p\,\mathbb{Z}_p^\times)^q \cong 1 + p\,\mathbb{Z}_p^\times$. So

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^q \cong \frac{\mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\,\mathbb{Z}_p^\times)}{q\,\mathbb{Z} \times (\mathbb{F}_p^\times)^q \times (1 + p\,\mathbb{Z}_p^\times)} \cong \mathbb{Z}/q \times (\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^q).$$

Let $g \in \mathbb{F}_p^\times$ be a generator, δ be the order of $g^q \in \mathbb{F}_p^\times$, then $\delta \mid (p-1)$, $(p-1) \mid q\delta$. Together with $q \mid (p-1)$, we have $\delta q = (p-1)$, hence the quotient $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^q$ is cyclic of order q. Observe there are $q+1$ subgroups of $\mathbb{Z}/q \times \mathbb{Z}/q$ of order q, so there are precisely $q+1$ isomorphism classes of cyclic extensions of $\mathbb{Q}_p$ of degree q.

3. Extensions of Dedekind Domains

Put everything in a relative context, we want to consider the following setup: let A be a Dedekind domain, $K = \mathrm{Frac}\,A$, E/K is a separable extension, B is the integral closure of A in E. We will show that B is a f.g. A-module and a Dedekind domain as well. We want to study the ideal structure of B using information about A and the extension. If the extension E/K is Galois, we also want to study the Galois group $\mathrm{Gal}(E/K)$. The main technique is to reduce the study to the "local" case, when we are focusing at a prime $\mathfrak{p} \lhd A$ and a prime $\mathfrak{q} \lhd B$ lying above $\mathfrak{p}$.

Since E/K is separable, we can take the Galois closure L/K of E/K, let $\sigma_1, \ldots, \sigma_n : E \to L$ be all K-embeddings of E. Then for all $x \in E$, $\mathrm{Tr}_{E/K}(x) = \sum_{i=1}^n \sigma_i(x) \in K$. Since $\sigma_i : E^\times \to L^\times$ are linearly independents as characters of $E^\times$, there exists $e \in E^\times$ such that $\mathrm{Tr}_{E/K}(e) \neq 0$. Then for any $x \neq 0 \in E$, $\mathrm{Tr}_{E/K}(x(xe^{-1})) \neq 0$. So the K-bilinear form $T : E \times E \to K$, $T(x, y) = \mathrm{Tr}_{E/K}(xy)$ is non-degenerate.

Observe if $S \subseteq A$ is a multiplicative subset, then $S^{-1}A$ is also a Dedekind domain with same fraction field K. And the integral closure of $S^{-1}A$ in E is $S^{-1}B$. So in particular since the integral closure of K in E is E, $(A - \{0\})^{-1}B = E$, so $E = K \cdot B$ is spanned by B. Let $E = K\langle e_1, \ldots, e_n\rangle$, $(e_i \in B)$, then using the non-degenerate form T, we may pick a dual basis $\langle f_1, \ldots, f_n\rangle$. Any element $x \in B$ may be written as a sum $\sum_{i=1}^n \langle x, e_i\rangle f_i \in \sum_{i=1}^n Af_i$. Since A is noetherian, so is $\sum Af_i$, so is B. Let $\mathfrak{q} \lhd B$ be any nonzero prime ideal, then $\mathfrak{p} := \mathfrak{q} \cap A$ is a nonzero prime in A, we have inclusion $A/\mathfrak{p} \hookrightarrow B/\mathfrak{q}$, so $B/\mathfrak{q}$ is a finite dimensional $A/\mathfrak{p}$ vector space and a domain, so $B/\mathfrak{q}$ is a field. This shows B is a noetherian, integrally closed, dimension 1 domain, i.e., a Dedekind domain.

Observe a prime $\mathfrak{q} \lhd B$ lies above $\mathfrak{p} \lhd A$ iff $\mathfrak{q} \cap A = \mathfrak{p}$ iff $\nu_{\mathfrak{q}}(\mathfrak{p}B) > 0$. Let $e_{\mathfrak{q}/\mathfrak{p}} := \nu_{\mathfrak{q}}(\mathfrak{p}B)$ denote the **ramification index of $\mathfrak{p}/\mathfrak{q}$** , let $f_{\mathfrak{q}/\mathfrak{p}} := [k_{\mathfrak{q}} : k_{\mathfrak{p}}] = [B/\mathfrak{q} : A/\mathfrak{p}]$ denote the **residue degree of $\mathfrak{p}/\mathfrak{q}$** . Then for any nonzero prime $p \lhd A$,

$$\sum_{\mathfrak{q}:\nu_{\mathfrak{q}}(\mathfrak{p}B)>0} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} = [E : K].$$

We say $\mathfrak{p}$ is

- **unramified in** E/K if $\forall \mathfrak{q}$ lying above $\mathfrak{p}$, $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is separable and $e_{\mathfrak{q}/\mathfrak{p}} = 1$.
- **split in** E/K if $\forall\, \mathfrak{q}$ lying above $\mathfrak{p}$, $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$.
- **ramified in** E/K if $\exists\, \mathfrak{q}$ lying above $\mathfrak{p}$, $e_{\mathfrak{q}/\mathfrak{p}} > 1$.
- **inert in** E/K if $\exists!\, \mathfrak{q}$ lying above $\mathfrak{p}$ and $e_{\mathfrak{q}/\mathfrak{p}} = 1$.
- **totally ramified in** E/K if $\exists!\, \mathfrak{q}$ lying above $\mathfrak{p}$ and $f_{\mathfrak{q}/\mathfrak{p}} = 1$.

We are particularly interested in the case when E/K is Galois. In this case,

Proposition 3.1. Under the setup with E/K Galois, $G := \mathrm{Gal}(E/K)$. Let $\mathfrak{q} \lhd B$ be a nonzero prime, $\mathfrak{p} := \mathfrak{q} \cap A$.

1. G acts transitively on the set of prime ideals in B lying above $\mathfrak{p}$.
2. $\forall \sigma \in G$: $f_{\sigma(\mathfrak{q})/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}}, e_{\sigma(\mathfrak{q})/\mathfrak{p}} = e_{\mathfrak{q}/\mathfrak{p}}$.
3. $[E : K] = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} g_{\mathfrak{q}/\mathfrak{p}}$.

Proof. Let $\mathfrak{q}_1 = \mathfrak{q}, \dots, \mathfrak{q}_k$ be all primes of B lying above $\mathfrak{p}$. For all $x \in \mathfrak{q}$, we know $N_{E/K}(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{q} \cap A = \mathfrak{p}$, so $N_{E/K}(x) \in \mathfrak{q}_i$ for all i, so for each i there exists $\sigma \in G$ such that $\sigma(x) \in \mathfrak{q}_i$, since $\sigma(\mathfrak{q})$ is a prime ideal, $\sigma(\mathfrak{q}) = \mathfrak{q}_i$, (1) is proved. Since $\sigma \bmod \mathfrak{q}$ defines an isomorphism $k_{\mathfrak{q}} \to k_{\sigma(\mathfrak{q})}$ of extensions of $k_{\mathfrak{p}}$, so $f_{\mathfrak{q}/\mathfrak{p}} = f_{\sigma(\mathfrak{q})/\mathfrak{p}}$. By unique factorization of ideals in B, $e_{\mathfrak{q}/\mathfrak{p}} = e_{\sigma(\mathfrak{q})/\mathfrak{p}}$, so (2) and (3) are proved. □

In this case, the **decomposition group** , denoted $D_{\mathfrak{q}/\mathfrak{p}}$ is the stabilizer of the prime ideal $\mathfrak{q}$. If $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is separable, then $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is also Galois and there is a natural surjective homomorphism $D_{\mathfrak{q}/\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$. The kernel is called the **inertia group** , denoted $I_{\mathfrak{q}/\mathfrak{p}}$. By the orbit-stabilizer formula, $D_{\mathfrak{q}/\mathfrak{p}}$ has size $e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$, hence $I_{\mathfrak{q}/\mathfrak{p}}$ has size $e_{\mathfrak{q}/\mathfrak{p}}$. We have ses

$$0 \longrightarrow I_{\mathfrak{q}/\mathfrak{p}} \longrightarrow D_{\mathfrak{q}/\mathfrak{p}} \longrightarrow \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \longrightarrow 0$$

Consider the case E/K is a Galois extension of number fields, let $p \in \mathbb{Z}$ be a fixed prime, let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime lying above (p). Then $[k_{\mathfrak{p}} : \mathbb{F}_p] \leq [K : \mathbb{Q}] < \infty$, so $k_{\mathfrak{p}}$ is a finite field of characteristic p, hence $k_{\mathfrak{p}}$ is perfect and any finite extension of $k_{\mathfrak{p}}$ is separable. For any prime $\mathfrak{q} \lhd \mathcal{O}_E$ lying above $\mathfrak{p}$, the extension $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is Galois. Suppose $\mathfrak{p}$ is unramified in $\mathcal{O}_L$, i.e., $I_{\mathfrak{q}/\mathfrak{p}} = 1$ and $D_{\mathfrak{q}/\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$. Recall the Galois group $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ has a canonical generator, the Frobenius automorphism $x \mapsto x^{|k_{\mathfrak{p}}|}$. The corresponding element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in D_{\mathfrak{q}/\mathfrak{p}}$ is the unique element such that for all $\alpha \in \mathcal{O}_E$,

$$\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}(\alpha) \equiv \alpha^{|k_{\mathfrak{p}}|} \pmod{\mathfrak{q}}.$$

Observe for $\sigma \in G$, one has commutative diagram

$$\begin{tikzcd}
k_{\mathfrak{q}} \arrow[r, "x \mapsto x^{|k_{\mathfrak{p}}|}"] \arrow[d, "\sigma|_{\mathcal{O}_E} \bmod \mathfrak{q}"'] & k_{\mathfrak{q}} \arrow[d, "\sigma|_{\mathcal{O}_E} \bmod \mathfrak{q}"] \\
k_{\sigma(\mathfrak{q})} \arrow[r, "x \mapsto x^{|k_{\mathfrak{p}}|}"] & k_{\sigma(\mathfrak{q})}
\end{tikzcd}$$

the top arrow is induced by $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ and the bottom path is induced by $\sigma^{-1}\,\mathrm{Frob}_{\sigma(\mathfrak{q})/\mathfrak{p}}\,\sigma$, so $\mathrm{Frob}_{\sigma(\mathfrak{q})/\mathfrak{p}} = \sigma\,\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}\,\sigma^{-1}$. If E/K is an abelian extension, the element $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is independent of $\mathfrak{q}$ and we obtain the **Artin symbol** $\left(\frac{E/K}{\mathfrak{p}}\right) \in G$.

We give an example how the ramification of primes could control the Galois group. Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree n, let K be the splitting field of $f(x)$ over $\mathbb{Q}$, then $K/\mathbb{Q}$ is Galois, we want to obtain information of $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\alpha_1, \dots, \alpha_n \in K$ be the roots of $f(x)$, then the Galois group injects into the symmetric group on these n roots, $\varphi : G \hookrightarrow \mathrm{Sym}(n)$. Let $p \in \mathbb{Z}$ be a prime such that $p \nmid \operatorname{disc} f$, or equivalently, $\overline{f}(x) = f(x) \bmod p$ factors into a product distinct irreducible polynomials $\overline{f}_1(x) \cdots \overline{f}_r(x) \in \mathbb{F}_p[x]$. We claim G contains a permutation of cycle type $(d_1)\cdots(d_r)$, where $d_i := \deg \overline{f}_i(x)$.

Let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime lying above (p), then $k_{\mathfrak{p}} = \mathbb{F}_p(\overline{\alpha}_1, \dots, \overline{\alpha}_n)$. The minimal polynomial of each $\overline{\alpha}_i$ is irreducible and divides $\overline{f}(x)$, hence must equal to some irreducible factor $\overline{f}_j(x)$ of $\overline{f}(x)$, which is separable over $\mathbb{F}_p$, so the residue classes $\overline{\alpha}_1, \dots, \overline{\alpha}_n$ are distinct. Hence the natural map $G \twoheadrightarrow \mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ is injective, hence it is an isomorphism. So the prime $(p) \lhd \mathbb{Z}$ is unramified in $\mathcal{O}_K$. We claim the permutation $\varphi(\mathrm{Frob}_{\mathfrak{p}/p})$ for any prime $\mathfrak{p}$ lying above (p) has cycle type $(d_1)\cdots(d_r)$. This is equivalent to show $\mathrm{Frob}_{\mathfrak{p}/p}$ has r orbits of sizes $d_1, \dots, d_r$. This is again equivalent to show the action of $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ on the set $\{\overline{\alpha}_1, \dots, \overline{\alpha}_n\}$ has r orbits of sizes $d_1, \dots, d_r$. If $\mathcal{O} = \{\beta_1, \dots, \beta_k\}$ is an orbit of the action, we associated to it an irreducible factor $\prod_{i=1}^k (x - \beta_i) \in \mathbb{F}_p[x]$ of $\overline{f}(x)$. Since $\overline{f}(x)$ has r irreducible factors of degrees $d_1, \dots, d_r$, the claim follows.

We conclude this section by proving the essential reduction to the local picture.

Proposition 3.2. Under the general setup given at the beginning of the section,

(1) There is a natural homomorphism $\widehat{A}_{\mathfrak{p}} \to \widehat{B}_{\mathfrak{q}}$ extending the inclusion $A \hookrightarrow B$.
(2) Let $K_{\mathfrak{p}} := \operatorname{Frac} \widehat{A}_{\mathfrak{p}}$, $E_{\mathfrak{q}} := \operatorname{Frac} \widehat{B}_{\mathfrak{q}}$. Then $E_{\mathfrak{q}} = K_{\mathfrak{p}} \cdot E$ is generated over $K_{\mathfrak{p}}$ by E, $E_{\mathfrak{q}}/K_{\mathfrak{p}}$ is finite separable, and $\widehat{B}_{\mathfrak{q}}$ is the integral closure of $\widehat{A}_{\mathfrak{p}}$ in $E_{\mathfrak{q}}$.
(3) $e_{\mathfrak{q}/\mathfrak{p}} = e_{\mathfrak{q}\widehat{B}_{\mathfrak{q}}/\mathfrak{p}\widehat{A}_{\mathfrak{p}}}$, $f_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}\widehat{B}_{\mathfrak{q}}/\mathfrak{p}\widehat{A}_{\mathfrak{p}}}$, $[E_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$.
(4) Suppose E/K is Galois, then so is $E_{\mathfrak{q}}/K_{\mathfrak{p}}$ and we have a natural isomorphism $D_{\mathfrak{q}/\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}(E_{\mathfrak{q}}/K_{\mathfrak{p}})$.

Proof. (1) For all $i \geq 1$, we have natural homomorphism $A/\mathfrak{p}^i \hookrightarrow B/\mathfrak{q}^i$, taking the limit, we get natural homomorphism $\widehat{A}_{\mathfrak{p}} \to \widehat{B}_{\mathfrak{q}}$, which extends $A \hookrightarrow B$.

(2) The question is local in $\mathfrak{p}$, so we may replace A by $A_{\mathfrak{p}}$ and assume A is a DVR. We know B is a Dedekind domain, and finitely generated, torsion free A-module. By the structure theorem, B is a finite free A-module. So for $i \geq 1$,$B/\mathfrak{p}^i B$ is is a finite free $A/\mathfrak{p}^i$-module. Suppose $\mathfrak{p}B = \prod_{j=1}^r \mathfrak{q}_j^{e_{\mathfrak{q}_j/\mathfrak{p}}}$, then by CRT for $i \geq 1$,

$$B/\mathfrak{p}^i B \cong \prod_{j=1}^r B/\mathfrak{q}_j^{i \cdot e_{\mathfrak{q}_j/\mathfrak{p}}}.$$

Since limit commutes with direct product, we have isomorphism of finite free $\widehat{A}_{\mathfrak{p}}$-modules

$$\varprojlim_i B/\mathfrak{p}^i B \cong \prod_{j=1}^r \varprojlim_i B/\mathfrak{q}_j^{i \cdot e_{\mathfrak{q}_j/\mathfrak{p}}} \cong \prod_{j=1}^r \varprojlim_i B/\mathfrak{q}_j^i \cong \prod_{j=1}^r \widehat{B}_{\mathfrak{q}_j}.$$

In particular, a direct summand $\widehat{B}_{\mathfrak{q}}$ is finite free over $\widehat{A}_{\mathfrak{p}}$. Since $\widehat{B}_{\mathfrak{q}}/\mathfrak{p}\widehat{B}_{\mathfrak{q}} \cong B/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$ is generated by B over $A/\mathfrak{p}$, by NAK, $\widehat{B}_{\mathfrak{q}}$ is generated by B over $\widehat{A}_{\mathfrak{p}}$. So $E_{\mathfrak{q}}$ is generated by E over $K_{\mathfrak{p}}$, $E_{\mathfrak{q}} = K_{\mathfrak{p}} \cdot E$. Since every element of E is separable over K, it is also separable over $K_{\mathfrak{p}}$, so $E_{\mathfrak{q}}/K_{\mathfrak{p}}$ is separable. Since $\widehat{B}_{\mathfrak{q}}$ is a complete DVR, it is integrally closed. Since $\widehat{B}_{\mathfrak{q}}$ is generated by B, it is integral over $\widehat{A}_{\mathfrak{p}}$, so it equals the integral closure of $\widehat{A}_{\mathfrak{p}}$ in $E_{\mathfrak{q}}$.

(3) $f_{\mathfrak{q}\widehat{B}_{\mathfrak{q}}/\mathfrak{p}\widehat{A}_{\mathfrak{p}}} = [\widehat{B}_{\mathfrak{q}}/\mathfrak{q}\widehat{B}_{\mathfrak{q}} : \widehat{A}_{\mathfrak{p}}/\mathfrak{p}\widehat{A}_{\mathfrak{p}}] = [B/\mathfrak{q} : A/\mathfrak{p}] = f_{\mathfrak{q}/\mathfrak{p}}$. Observe $\mathfrak{p}\widehat{B}_{\mathfrak{q}} = (\prod_{j=1}^{r} \mathfrak{q}_j^{e_{\mathfrak{q}_j/\mathfrak{p}}})\widehat{B}_{\mathfrak{q}} = \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}\widehat{B}_{\mathfrak{q}}$, by unique factorization, $e_{\mathfrak{q}\widehat{B}_{\mathfrak{q}}/\mathfrak{p}\widehat{A}_{\mathfrak{p}}} = e_{\mathfrak{q}/\mathfrak{p}}$. Since $\mathfrak{q}\widehat{B}_{\mathfrak{q}}$ is the only prime above $\mathfrak{p}\widehat{A}_{\mathfrak{p}}$, $[K_{\mathfrak{q}} : K_{\mathfrak{p}}] = e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$.

(4) Since $E_{\mathfrak{q}} = K_{\mathfrak{p}} \cdot E$, if E is the splitting field of a separable polynomial over K, then $E_{\mathfrak{q}}$ is the splitting field of the same polynomial over $K_{\mathfrak{p}}$, so $E_{\mathfrak{q}}/K_{\mathfrak{p}}$ is Galois as well. Given $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$, then $\sigma(\mathfrak{q}) = \mathfrak{q}$, hence it induces an automorphism of $E_{\mathfrak{q}}/K_{\mathfrak{p}}$, this defines a natural homomorphism $D_{\mathfrak{q}/\mathfrak{p}} \to \mathrm{Gal}(E_{\mathfrak{q}}/K_{\mathfrak{p}})$. Since $D_{\mathfrak{q}/\mathfrak{p}}$ and $\mathrm{Gal}(E_{\mathfrak{q}}/K_{\mathfrak{p}})$ both have size $e_{\mathfrak{q}/\mathfrak{p}} \cdot f_{\mathfrak{q}/\mathfrak{p}}$, it suffices to show this natural homomorphism is injective. Since $E_{\mathfrak{q}} = K_{\mathfrak{p}} \cdot E$, so if an automorphism fixes $E_{\mathfrak{q}}$, it fixes E as well.

□

We now prove the main result of our course, which states a relation between the global ideal structure and local factorizations of polynomial.

Corollary 3.3. Under the general setup given at the beginning of the section. Let $\alpha \in E$ such that $E = K(\alpha)$, let $f(x) \in K[x]$ be the minimal polynomial of α. Then for every nonzero prime $\mathfrak{p} \lhd A$, there is a bijection:

$$\left\{\begin{array}{l}\text{prime ideals } \mathfrak{q} \lhd B\\ \text{lying above } \mathfrak{p}\end{array}\right\} \xrightarrow{\quad\sim\quad} \left\{\begin{array}{l}\text{irreducible factors } g(x)\\ \text{of } f(x) \text{ in } K_{\mathfrak{p}}[x]\end{array}\right\}$$

$$\mathfrak{q} \longmapsto \left(\begin{array}{l}\text{the unique irreducible factor } g(x) \text{ of } f(x)\\ \text{in } K_{\mathfrak{p}}[x] \text{ such that } g(\alpha) = 0 \text{ in } E_{\mathfrak{q}}\end{array}\right)$$

Proof. Let L be the Galois closure of E/K, let $C \subseteq L$ be the integral closure of A in L. Let $G := \mathrm{Gal}(L/K)$, $H := \mathrm{Gal}(L/E)$. We observe

(1) Fix a prime $\mathfrak{r} \lhd C$ lying abover $\mathfrak{p}$, then by orbit-stabilizer the map $\sigma \mapsto \sigma(\mathfrak{r})$ determines a bijection of G-sets (i.e., respects left G-action) $G/D_{\mathfrak{r}/\mathfrak{p}} \xrightarrow{\sim} \{\text{primes of } C \text{ lying above } \mathfrak{p}\}$. Then we have induced bijection $H\backslash G/D_{\mathfrak{r}/\mathfrak{p}} \xrightarrow{\sim} \{\text{primes of } B \text{ lying above } \mathfrak{p}\}$, given by $\sigma \mapsto \sigma(\mathfrak{r}) \cap B$. By definition of H, this is well-defined. Since G acts transitively on primes in C above $\mathfrak{p}$, this map is surjective. Since G acts transitively on primes in C above a fixed prime $\mathfrak{q}$ of B above $\mathfrak{p}$, this map is injective.

(2) Since L/K is Galois, $L_{\mathfrak{r}}/K_{\mathfrak{p}}$ is also Galois, let $\alpha_1 = \alpha, \ldots, \alpha_n \in L$ be the roots of $f(x)$. The map $\sigma \mapsto \sigma(\alpha)$ defines a bijection of G-sets $G/H \xrightarrow{\sim} \{\alpha_1, \ldots, \alpha_n\}$. Then we have induced bijection $D_{\mathfrak{r}/\mathfrak{p}}\backslash G/H \to D_{\mathfrak{r}/\mathfrak{p}}$-orbits of $\{\alpha_1, \ldots, \alpha_n\}$. Since $D_{\mathfrak{r}/\mathfrak{p}} \cong \mathrm{Gal}(L_{\mathfrak{r}}/K_{\mathfrak{p}})$, and each Galois orbit $\{\beta_1, \ldots, \beta_k\}$ is associated to an irreducible factor $g(x) := \prod_{i=1}^{k}(x - \beta_i) \in K_{\mathfrak{p}}[x]$ of $f(x)$. The factor $g(x)$ associated to $\overline{\sigma} \in D_{\mathfrak{r}/\mathfrak{p}}\backslash G/H$ is the unique irreducible factor of $f(x)$ such that $g(\sigma(\alpha)) = 0$ in $L_{\mathfrak{r}}$.

Putting these together, we have a bijection of G-sets

$$\begin{tikzcd}
\left\{\begin{matrix}\text{primes of } B \text{ lying}\\ \text{above } \mathfrak{p}\end{matrix}\right\} \arrow[r, "\sim"] & H\backslash G/D_{\mathfrak{r}/\mathfrak{p}} \arrow[r, "\sim"] & D_{\mathfrak{r}/\mathfrak{p}}\backslash G/H \arrow[r, "\sim"] & \left\{\begin{matrix}\text{irreducible factors } g(x)\\ \text{of } f(x) \text{ in } K_{\mathfrak{p}}[x]\end{matrix}\right\} \\
\mathfrak{q}=\sigma(\mathfrak{r})\cap B \arrow[r, mapsto] & \overline{\sigma} \arrow[r, mapsto] & \overline{\sigma}^{-1} \arrow[r, mapsto] & \left(\begin{matrix}\text{the unique irreducible factor } g(x)\\ \text{of } f(x) \text{ in } K_{\mathfrak{p}}[x] \text{ such that}\\ g(\sigma^{-1}(\alpha))=0 \text{ in } L_{\mathfrak{r}}\end{matrix}\right)
\end{tikzcd}$$

To finish the proof it suffices to show for all $\sigma \in G$ and all irreducible factor $g(x)$ of $f(x)$ in $K_{\mathfrak{p}}[x]$, $g(\sigma^{-1}(\alpha))$ in $L_{\mathfrak{r}}$ iff $g(\alpha)=0$ in $E_{\sigma^{-1}(\mathfrak{r})\cap B}$. Observe for all $i \geq 1$, σ determines an isomorphism $C/\mathfrak{r}^i \xrightarrow{\sim} C/\sigma(\mathfrak{r})^i$, hence an isomorphism $L_{\mathfrak{r}} \xrightarrow{\sim} L_{\sigma(\mathfrak{r})}$. So $g(\sigma^{-1}(\alpha))$ in $L_{\mathfrak{r}}$ iff $\sigma(g(\sigma^{-1}(\alpha)))=0$ in $L_{\sigma^{-1}(\mathfrak{r})}$. Since σ fixes g, the above is true iff $g(\alpha)=0$ in $L_{\sigma^{-1}(\mathfrak{r})}$. Since $E_{\sigma^{-1}(\mathfrak{r})\cap B} \subseteq L_{\sigma^{-1}(\mathfrak{r})}$, the claim follows. □

Here is a simple example of the correspondence. $K=\mathbb{Q}, E=\mathbb{Q}(i)$, $f(x)=x^2+1$. Consider the prime $2 \in \mathbb{Z}$, observe we have factorization $2\,\mathcal{O}_E = 2\,\mathbb{Z}[i] = (1+i)^2$, so there is only one prime lying above (2), so $f(x)$ is irreducible in $\mathbb{Q}_2[x]$. Consider the prime $5 \in \mathbb{Z}$, note $(5)=(2+i)(2-i)$, so $f(x)$ splits in $\mathbb{Q}_5[x]$. Since 2 is a simple root of $f(x)$ modulo (5), by Hensel's lemma, $\exists!\,\theta \in \mathbb{Q}_5$ such thath $f(\theta)=0$ and $\theta \bmod 5 = 2$, so $f(x)$ factors as $(x-\theta)(x+\theta)$ over $\mathbb{Q}_5$. Observe $i-\theta \equiv i-2 \equiv -4 \neq 0 \bmod (2+i)$, so $i-\theta \neq 0$ in $E_{(i+2)}$. So the factor $(x-\theta)$ corresponds to the prime $(2-i)$ and $(x+\theta)$ corresponds to the prime $(2+i)$.

4. Extensions of CDVFs

In this section we consider the local picture we have reduced us into – the extensions of complete discrete valuation fields. Recall we have the following setup: A is a Dedekind domain, $K=\operatorname{Frac} A$, E/K finite separable extension, B is the integral closure of A in E, $\mathfrak{p} \lhd A$, $\mathfrak{q} \lhd B$ primes, $\nu_{\mathfrak{q}}(\mathfrak{p}B) > 0$. We have finite separable extension $E_{\mathfrak{q}}/K_{\mathfrak{p}}$. We have a name for such an extension.

Definition 4.1 (complete discrete valuation field)**.** A **complete discrete valuation field** (CDVF) is a pair (K, ν_K), where K is a field and $\nu_K : K^\times \to \mathbb{Z}$ is a discrete valuation, such that the DVR A_K associated to the valuation is complete. Let π_K denote a choice of uniformizer of A_K.

If (K,ν_K) is a CDVF, E/K is a finite separable extension then $E=K(\alpha)$ for some $\alpha \in E$, let $f(x) \in K[x]$ be the minimal polynomial of α. Let A_E denote the integral closure of A_K in E. Since K is a CDVF, $K_{(\pi_K)} = K$, hence $f(x) \in K_{(\pi_K)}[x]$ is irreducible, so by Corollary 3.3, A_E has precisely one prime lying above (π_K). Since A_K is a DVR, this implies A_E is a DVR as well. Let $\nu_E : E^\times \to \mathbb{Z}$ denote the associated valuation on E. Let π_E be some uniformizer of A_E, recall (proposition 3.2) $E_{(\pi_E)} = K_{(\pi_K)} \cdot E = K \cdot E = E$. So E is a CDVF as well. Such an extension E/K is called an **extension of CDVFs** . Let $k_E := A_E/(\pi_E)$, $k_K := A_K/(\pi_K)$ denote the residue fields, let $f_{E/K}$ denote the residue degree $[k_E : k_K]$ and let $e_{E/K}$ denote the ramification index $e_{(\pi_E)/(\pi_K)}$. Since A_K and A_E are DVRs, E/K can be one of the following

- split iff $E=K$.
- unramified iff k_E/k_K is separable and $e_{E/K}=1$.
- ramified iff $e_{E/K} > 1$.
- totally ramified iff $f_{E/K}=1, e_{E/K}=[E:K]$.

We will later give a characterization of the two extreme cases: unramified and totally ramified extensions of CDVFs. And we will use ramification groups to study all cases in between.

For an extension E/K of CDVFs, there is a simple relation between two valuations ν_K and ν_E. Suppose E/K is Galois, and let $\sigma \in G = \mathrm{Gal}(E/K)$. Observe $\sigma : A_E^\times \to A_E^\times$ and $\nu_E(\sigma(\pi_E)) = \nu_E(\sigma^{-1}(\pi_E)) = 1$. So $\nu_E(\cdot)$ in invariant under the action of G. If $\alpha \in K^\times$, then $\nu_E(\alpha) = \nu_E(\pi_K^{\nu_K(\alpha)}) = e_{E/K}\nu_K(\alpha)$. Then for all $x \in E^\times$,

$$\frac{1}{f_{E/K}}\nu_K(N_{E/K}(x)) = \frac{1}{f_{E/K}e_{E/K}}\nu_E(N_{E/K}(x)) = \frac{[E:K]}{f_{E/K}e_{E/K}}\nu_E(x) = \nu_E(x).$$

We claim this relation also holds for general E/K. Let L be the Galois closure of E/K, then

$$\nu_L(x) = \frac{1}{f_{L/K}}\nu_K(N_{L/K}(x)) = \frac{1}{f_{L/E}}\nu_E(N_{L/E}(x)) \qquad (x \in L^\times).$$

If $x \in E^\times$, then $N_{L/E}(x) = x^{[L:E]}$ and $N_{L/K}(x) = N_{E/K}(x)^{[L:E]}$, so

$$\frac{[L:E]}{f_{L/K}}\nu_K(N_{E/K}(x)) = \frac{[L:E]}{f_{L/E}}\nu_E(x) \implies \nu_E(x) = \frac{f_{L/E}}{f_{L/K}}\nu_K(N_{E/K}(x)) = \frac{1}{f_{E/K}}\nu_K(N_{E/K}(x)).$$

We introduce the technique of Newton polygon that allows us to obtain information of roots and factorizations of a polynomial over CDVF by looking at a simple diagram plotted using the valuations of its coefficients.

Definition 4.2 (Newton polygon)**.** Let A be a DVR, $K = \mathrm{Frac}\, A$, $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ a monic polynomial with $a_n \neq 0$. The **Newton polygon** is the graph of the largest piecewise linear function $N : [0,n] \to \mathbb{R}$ such that (1) $N(0) = 0$, $N(n) = \nu_K(a_n)$, (2) for $j = 1, \ldots, n-1$, $N(j) \leq \nu_K(a_j)$, and (3) N is convex.

When the field K contains all roots of f, the Newton polygon of f is determined by the valuations of the roots of f.

Lemma 4.3. *Let A be a DVR, $K = \mathrm{Frac}\, A$, $\alpha_1, \ldots, \alpha_n \in K^\times$, $f(x) := \prod_{i=1}^n (x - \alpha_i) = x^n + a_1x^{n-1} + \cdots + a_n$. Let $\lambda_i := \nu_K(\alpha_i)$ $(i = 1, \ldots, n)$, then $\lambda_1, \ldots, \lambda_n$ are the slopes of $N_K(f)$ with multiplicity. In particular, the slopes of Newton polygon $N_K(f)$ are integers.*

Proof. Rearrange the roots such that $\lambda_1 \leq \cdots \leq \lambda_n$. Define $L : [0,n] \to \mathbb{R}$ by $L(j) := \lambda_1 + \cdots + \lambda_j$, and linear between any two consecutive points. Then $L(0) = 0, N(n) = \lambda_1 + \cdots + \lambda_n = \nu_{a_n}$, L is convex, and for all $j = 1, \ldots, n-1$, by the ultrametric property of valuation,

$$\nu_K(a_j) = \nu_K(\alpha_1 \cdots \alpha_j + \sum_{(i_1 < \cdots < i_j) \neq (1, \ldots, j)} \alpha_{i_1} \cdots \alpha_{i_j}) \geq \nu_K(\alpha_1 \cdots \alpha_j) = L(j).$$

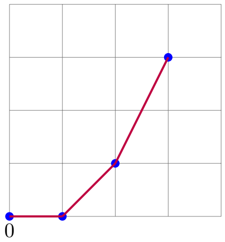
So by maximality, $N_K \geq L$. To show they are equal, it suffices to show if $(j, L(j))$ is a vertex of L, it is also a vertex of N_K. If it is the case, then $\lambda_{j+1} > \lambda_j$, so the inequality above becomes an equality, so $\nu_K(a_j) = L(j)$, so $L(j) \leq N_K(j) \leq \nu_K(a_j) = L(j)$, so $N_k(j) = L(j)$ and $(j, L(j))$ is also a vertex of $N_K(f)$. □

If K is a CDVF, when we can look at the splitting field L of f and use the simple relation between the valuations ν_K and ν_L to determine what the Newton polygon of f over K looks like. Since valuation ν_E is invariant under the Galois action, this determines a factorization of f over K.

Proposition 4.4. Let K be a CDVF, $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in K[x]$, $a_n \neq 0$ a separable polynomial. Let $\lambda_1 < \cdots < \lambda_r$ be the slopes of $N_K(f)$ where the slope λ_i has multiplicity N_i. Then there exists a unique factorization $f(x) = \prod_{i=1}^r g_i(x)$ in $K[x]$, where each $g_i(x) \in K[x]$ is monic and its Newton polygon $N_K(g_i)$ has a single slope λ_i of multiplicity N_i.

Proof. Let E be the splitting field of $f(x)$ over K, let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of $f(x)$. Then E/K is a Galois extension of CDVFs. WLOG we assume $\nu_E(\alpha_1) \leq \cdots \leq \nu_E(\alpha_n)$. By Lemma 4.3, and the fact that $\nu_E|_{K^\times} = e_{E/K}\nu_K$, $N_E(f)$ has slopes $e_{E/K}\lambda_1 < \cdots < e_{E/K}\lambda_r$ with multiplicities $N_1, \ldots, N_r$. Let $g_i(x) := \prod_{\alpha_j : \nu_E(\alpha_j) = \lambda_i e_{E/K}}(x - \alpha_j)$ $(1 \leq i \leq r)$. Since the set $\left\{\alpha_j : \nu_E(\alpha_j) = \lambda_i e_{E/K}\right\}$ is an orbit of the Galois action, each $g_i(x) \in K[x]$ is an irreducible factor of $f(x)$. By construction $N_K(g_i)$ has a single slope λ_i of multiplicity N_i, and this factorization of $f(x)$ is unique by construction. □

***Example* 4.5.** Consider the polynomial $f(x) = x^3 + x^2 + 2x + 8 \in \mathbb{Q}_2[x]$. The Newton polygon $N_{\mathbb{Q}_2}(f)$ is drawn below.



Observe the Newton ploygon has 3 distinct slopes $0, 1, 2$, $f(x)$ splits over $\mathbb{Q}_2$. If $f(x)$ is irreducible over $\mathbb{Q}$, then $E := \mathbb{Q}[x]/(f(x))$ is a degree 3 extension where the prime $(2) \lhd \mathbb{Z}$ splits.

Let A be a DVR, $K = \operatorname{Frac} A$, a monic polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in K[x]$ is **Eisenstein** if $\nu_A(a_i) \geq 1$, $(1 \leq i \leq n-1)$ and $\nu_A(a_n) = 1$. Equivalently, $f(x)$ is Eisenstein if and only if the Newton polygon $N_K(f)$ has a single slope $1/n$ with multiplicity n. We characterize totally ramified and unramified extensions of CDVFs.

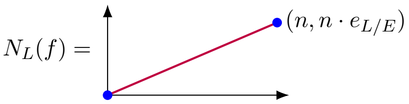
Proposition 4.6.

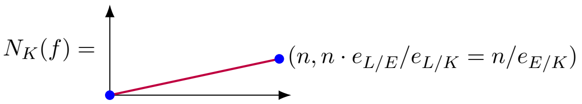
(1) Let E/K be a totally ramified extension of CDVFs, let $f(x) \in K[x]$ be the minimal polynomial of a chosen uniformizer π_E of A_E. Then $f(x)$ is Eisenstein and $E = K(\pi_E)$.

(2) Let K be a CDVF, $f(x) \in K[x]$ be a separable Eisenstein polynomial, $E := K[x]/(f(x))$. Then $f(x)$ is irreducible over K, E/K is totally ramified, and $x \bmod f(x) \in E$ is a uniformizer of A_E.

Proof.

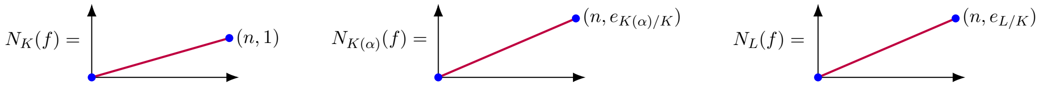
(1) Let $L/E/K$ be the Galois closure of E/K, and $f(x)$ factorizes as $f(x) = (x - \pi_E)(x - \alpha_2)\cdots(x - \alpha_n)$ over L. Since $\nu_L(\cdot)$ is invariant under Galois action, $\nu_L(\pi_E) = \nu_L(\alpha_i) = e_{L/E}$ for all i. So





Since $\nu_K(a_n) \geq 1$ is an integer, we must have $n \geq e_{E/K}$. On the other hand, since E/K is totally ramified, $e_{E/K} = [E : K] \geq [K(\pi_E) : K] \geq n$, so $e_{E/K} = n$, $f(x) \in K[x]$ is Eisenstein and $K(\pi_E) = E$.

(2) Let L be the splitting field of $f(x)$ over K, let $\alpha \in L$ be a root of $f(x)$. We consider the tower $L/K(\alpha)/K$. Since $f(x)$ is Eisenstein over K,



Since $N_L(f)$ has a single slope of $e_{L/K}/n = e_{L/K(\alpha)}\nu_{K(\alpha)}(\alpha)$, so $N_{K(\alpha)}(f)$ has a single slope of $e_{K(\alpha)/K}/n = \nu_{K(\alpha)}(\alpha)$, which is a positive integer. In particular, $e_{K(\alpha)/K} \geq n$. On the other hand, $e_{K(\alpha)/K} \leq [K(\alpha) : K] \leq n$, so $e_{K(\alpha)/K} = n$. Hence $K[x]/(f(x)) \to K(\alpha)$, $\overline{x} \mapsto \alpha$ induces a surjective map between K-vector spaces, hence it is an isomorphism. So $f(x)$ is irreducible and E/K is a totally ramified extension of CDVFs and $\nu_E(x \bmod f(x)) = \nu_{K(\alpha)}(\alpha) = 1$, so $x \bmod f(x) \in E$ is a uniformizer of A_E.

□

Proposition 4.7. Let K be a CDVF, ℓ/k_K a finite separable extension. Then there exists an unramified extension L/K of CDVFs and an isomorphism $i : \ell \to k_L$ satisfying the following universal property: for any extension E/K of CDVFs and k_K-embeddings $j : \ell \hookrightarrow k_E$, there is a unique K-embedding $J : L \to E$ such that the following diagram commutes:

$$\begin{tikzcd}
& k_L \arrow[dr, "J|_{A_L} \bmod \pi_L"] & \\
\ell \arrow[ur, "i", "\sim"'] \arrow[rr, hook, "j"] & & k_E
\end{tikzcd}$$

Proof. Let $\overline{\alpha} \in \ell$ be a primitive element, let $\overline{f}(x) \in k_K[x]$ be the minimal polynomial of $\overline{\alpha}$, let $f(x) \in A_K[x]$ be a monic lift of $\overline{f}(x)$, define $L := K[x]/(f(x))$, let α denote the residue class $x \bmod f(x)$. Since $\overline{f}(x)$ is irreducible and separable, so is $f(x)$, so L/K is a separable extension of CDVFs. There is an inclusion $A_K[x] \hookrightarrow L[x]$, note the image lands in $A_L[x]$ and $f(x)$ is mapped to zero, so we have map $A_K[x]/(f(x)) \to A_L[x]$. Since $(\pi_K) \subseteq (\pi_L)$, this induces map $i : \ell = k_K[x]/(\overline{f}(x)) = A_K[x]/(\pi_K, f(x)) \to A_L[x]/(\pi_L) = k_L$ of k_K-algebras. Since this map is nonzero, it must be an k_K-embedding. Since $f_{L/K} = [k_L : k_K] \leq [L : K] = \deg f(x) = \deg \overline{f}(x) = [\ell : k_K]$, the map $i : \ell \to k_L$ must be an isomorphism.

Let E/K be another extension of CDVFs with a k_K-embedding $j : \ell \hookrightarrow k_E$. Such embedding is determined by a root $\overline{\theta}$ of $\overline{f}(x)$ in k_E. Since $\overline{f}(x)$ is separable, such root is simple, and by Hensel's Lemma, $\exists!\ \theta \in A_E$ such that $f(\theta) = 0$ and $\theta \bmod \pi_E = \overline{\theta}$. So any such embedding is determined by a root of $f(x)$ in E, hence determines a unique embedding $J : L \to E$ such that $\overline{J} \circ i = j : \ell \to k_E$. □

In particular, since any finite field $\mathbb{F}_p$ has a unique degree n separable extension $\mathbb{F}_{p^n} / \mathbb{F}_p$ for all $n \in \mathbb{Z}_{\geq 1}$, the p-adic field $\mathbb{Q}_p$ has a unique unramified extension E_{p^n} together with an isomorphism $\mathbb{F}_{p^n} \xrightarrow{\sim} k_{E_{p^n}}$.

As another consequence of the characterization, for any extension E/K of CDVFs with k_E/k_K separable, there is an unramified extension E_0/K with $k_E \cong k_{E_0}$ and a K-embedding $E_0 \hookrightarrow E$. Identify E_0 with its image in E, we get a tower $E/E_0/K$. For any unramified subextension $E/L/K$, we have a k_K-embedding $k_L \hookrightarrow k_E = k_{E_0}$, hence the embedding lifts to a K-embedding $L \hookrightarrow E_0$. Hence E_0/K is the **maximal unramified subextension** of E/K .

Intuitively, the maximal unramified subextension should be the subfield with "no inertia", i.e., it should be the fixed field of the inertia group. This is indeed the case.

Proposition 4.8. Let E/K be a Galois extension of CDVFs with k_E/k_K separable, then $E_0 \cong E^{I_{E/K}}$, where $I_{E/K} = \left\{\sigma \in \mathrm{Gal}(E/K) : \sigma|_{A_E} \bmod \pi_E = \mathrm{id}_{k_E}\right\}$ is the inertia subgroup.

Proof. We adopt the construction in Proposition 4.7. Since E/K is Galois and k_E/k_K is separable, k_E/k_K is Galois, so k_E contains all roots of $\overline{f}(x)$. Since $\overline{f}(x)$ is separable, by Hensel's Lemma, E contains all roots of $f(x)$, so E_0/K is Galois. By Galois theory, it suffices to show $\mathrm{Gal}(E/E_0) = I_{E/K}$. Since Hensel's Lemma gives us a bijection between roots of $\overline{f}(x)$ in k_E and roots of $f(x)$ in E, for $\sigma \in \mathrm{Gal}(E/K)$, $\sigma \in I_{E/K}$ iff $\overline{\sigma} \in \mathrm{Gal}(k_E/k_K)$ fixes all roots of $\overline{f}(x)$ iff σ fixes E_0. □

This suggests us a way to investigate the question of "how ramified an extension of CDVFs is". If E/K is an Galois extension of CDVFs with k_E/k_K separable, then we have tower $E/E_0 = E^{I_{E/K}}/K$, where E_0/K is unramified and E/E_0 is totally ramified. Then we hope to investigate how ramified E/E_0 is by looking at various subgroups of the inertia group. We introduce the notion of ramification groups to do just that.

Unless otherwise mentioned, all extensions E/K below will be Galois and k_E/k_K separable, let $G := \mathrm{Gal}(E/K)$ denote the Galois group, let π_E, π_K be some uniformizers of A_E, A_K respectively. We first observe A_E could be generated by a single element α, $A_E = A_K[\alpha]$.

Setup: E/K Galois extension of CDVFs, k_E/k_K separable

Proof. Suppose $k_E = k_K(\overline{y})$, let $\overline{p}(x) \in k_K[x]$ be the minimal polynomial of $\overline{y}$, $p(x) \in A_K[x]$ a monic lift of $\overline{f}(x)$. Since $\overline{p}(x)$ is separable, by Hensel's Lemma, $\exists!\ y \in A_E$ such that $p(y) = 0$ and $y \bmod \pi_E = \overline{y}$. Consider the element $\alpha := y + \pi_E \in A_E$. Observe by Taylor expansion, $p(y + \pi_E) = \pi_E p'(y) + \pi_E^2 z$. Since $\overline{p'}(y) \neq 0$, we have $\nu_E(p(y + \pi_E)) = 1$, so $p(y + \pi_E)$ is an uniformizer of A_E. Also observe the map $A_K[y + \pi_E] \to k_E$ sending $y + \pi_E$ to $\overline{y}$ is surjective. Hence every element of A_E can be written as $\sum_{i \geq 0} a_i p(y + \pi_E)^i$, where $a_i \in X$, and $X \subseteq A_K[y + \pi_E]$ a set of representatives of residue classes in k_E.

Since A_E is finite as a A_K module, and by the observation above $A_E/(\pi_K) = A_E/(\pi_E^{e_{E/K}})$ is generated by $y + \pi_E$, it follows by NAK that $A_E = A_K[y + \pi_E]$. □

Define function $i_G : G \to \mathbb{Z}$, $i_G(\sigma) := \nu_E(\sigma(\alpha) - \alpha)$. And define the ***i*-th lower ramification group** G_i to be

$$\begin{aligned} G_i &:= \left\{\sigma \in G : i_G(\sigma) \geq i + 1\right\} \\ &= \left\{\sigma \in G : \nu_E(\sigma(\alpha) - \alpha) \geq i + 1\right\} \\ &= \left\{\sigma \in G : \sigma|_{A_E} \bmod \pi_E^{i+1} = \mathrm{id} \in \mathrm{Aut}(A_E/(\pi_E^{i+1}))\right\}. \end{aligned}$$

Remark: the function i_G may be defined using any uniformizer π_E, we choose α for simplicity

If $\sigma \in G_i$, $\tau \in G$, then $\overline{\tau\sigma\tau^{-1}} = \overline{\tau}\overline{\sigma}\overline{\tau}^{-1} = \overline{\tau}\overline{\tau}^{-1} = \mathrm{id} \in \mathrm{Aut}(A_E/(\pi_E^{i+1}))$. So $G_i \lhd G$ for all $i \geq -1$. Note by definition $\cap_{i \geq -1} G_i = 1$, so we get a filtration of G

$$G = G_{-1} \geq G_0 = I_{E/K} \geq G_1 \geq G_2 \geq \cdots \geq G_N = 1.$$

***Remark* 4.9.** For $\sigma, \tau \in G$, one has $i_G(\sigma\tau) \geq \min\{i_G(\sigma), i_G(\tau)\}$, with equality if and only if $i_G(\sigma) \neq i_G(\tau)$.

Why? suppose $i_G(\sigma) = a$ and $i_G(\tau) = b$, then $\sigma(\pi_E) = \pi_E + \pi_E^a u_1$ and $\tau(\pi_E) = \pi_E + \pi_E^b u_2$, hence $\sigma\tau(\pi_E) = \pi_E + \pi_E^a z_1 + (\pi_E + \pi_E^a u_1)^b \sigma(u_2)$, so $i_G(\sigma\tau) = \min\{a, b \cdot \nu_E(\pi_E + \pi_E^a u_1)\}$. If $a = 0$, it equals 0; otherwise it equals $\min\{a, b\}$ as we wished.

Example **4.10.**

(1) Consider the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$. This is a totally ramified Galois extension of CDVFs since the minimal polynomial of $\sqrt{2}$ is Eisenstein. We have $G = \{1, \tau\} = I_{E/K} = G_0 = G_{-1}$, where $\tau : \sqrt{2} \mapsto -\sqrt{2}$. Since $\sqrt{2}$ is a uniformizer, and $i_G(\tau) = \nu_E(-2\sqrt{2}) = 3$, we have $G_{-1} = G_0 = G_1 = G_2 = \{1, \tau\}$ and $G_3 = \{1\}$.

(2) Consider the extension $\mathbb{Q}_2(i)/\mathbb{Q}_2$, the minimal polynomial of $i+1$ is $(x-1)^2+1 = x^2-2x+2$, which is Eisenstein, so this is a totally ramified Galois extension of CDVFs with uniformizer $i+1$. We have $G = \{1, \tau\} = I_{E/K} = G_0 = G_{-1}$, where $\tau : i \mapsto -i$. Since $i_G(\tau) = \nu_E(-2i) = \nu_E((1+i)^2) = 2$, we have $G_{-1} = G_0 = G_1 = \{1, \tau\}$ and $G_2 = \{1\}$.

Intuitively, $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is more ramified than $\mathbb{Q}_2(i)/\mathbb{Q}_2$.

Observe by definition, if $H \leq G$ is a subgroup, $K' := E^H$, identify H with $\mathrm{Gal}(G/K')$, then $H_i = G_i \cap H$. However it is not generally true that given $H \lhd G$, we have $(G/H)_i = G_iH/H$. In the rest of the section we will

(1) Investigate the structure of the filtration $G = G_{-1} \geq G_0 \geq G_1 \geq G_2 \geq \cdots$.
(2) Fix the problem that ramification groups are incompatible with quotients.

4.1. **Structure of the filtration by lower ramification groups.** Define **unit groups** $U_E^{(0)} = U_E := A_E^\times$ and $U_E^{(i)} := \mathrm{Ker}(A_E^\times \to (A_E/(\pi_E)^i)^\times)$. So we get a filtration of unit groups $U_E^{(0)} \geq U_E^{(1)} \geq U_E^{(2)} \geq \cdots$. Observe we have group isomorphisms $U_E^{(i)}/U_E^{(i+1)} \to \pi_E^i A_E/\pi_E^{i+1}A_E$ induced by the map $\alpha \in U_E^{(i)} \mapsto \alpha - 1 \in \pi_E^i A_E$. Why is this a group map? Let $\alpha, \beta \in U_E^{(i)}$, we want to show $(\alpha\beta - 1) - (\alpha - 1) - (\beta - 1) \in \pi_E^{i+1}A_E$. Note it equals $\alpha(\beta-1) - (\beta-1) = (\alpha-1)(\beta-1)$. Since $\alpha - 1, \beta - 1 \in \pi_E^i$, their product is divisible by π_E^{i+1}.

Why do we care about unit groups? Because we have the following equivalence: for $\sigma \in G$,

$$\sigma \in G_i \iff i_G(\sigma) \geq i+1 \iff \nu_E(\sigma(\pi_E) - \pi_E) \geq i+1$$
$$\iff \nu_E\left(\frac{\sigma(\pi_E)}{\pi_E} - 1\right) \geq i \iff \frac{\sigma(\pi_E)}{\pi_E} \in 1 + \pi_E^i A_E = U_E^{(i)}.$$

So we get an injective group maps $G_i/G_{i+1} \hookrightarrow U_E^{(i)}/U_E^{(i+1)}$. In particular, we have

$$G_0/G_1 \hookrightarrow U_E^{(0)}/U_E^{(1)} \cong k_E^\times, \qquad G_i/G_{i+1} \hookrightarrow \pi^i A_E/\pi^{i+1}A_E \quad (i \geq 1).$$

So G_0/G_1 is cyclic and G_i/G_{i+1} are abelian $(i \geq 1)$. In particular G_0 is solvable. So if the quotient $G/G_0 = G/I_{E/K} \cong \mathrm{Gal}(k_E/k_K)$ is solvable, then the whole Galois group $G = \mathrm{Gal}(E/K)$ is solvable. Recall finite extensions of a finite field are cyclic, so if k_K is a finite field, then for any E/K Galois CDVF extension, k_E/k_K separable, E/K is solvable. In particular, there are no Galois extension of CDVFs E/K, k_E/k_K separable, k_K finite, with $\mathrm{Gal}(E/K) \cong A_5$.

We have a finer description of the quotients. Suppose $\mathrm{char}\, k_E = 0$, then each quotient π_E^i/π_E^{i+1} is a $\mathbb{Q}$-vector space, and hence each quotient G_i/G_{i+1} is a finite subgroup of a $\mathbb{Q}$-vector space, hence must be trivial. Since for $i \gg 0$, $G_i = 0$, all of G_i $(i \geq 1)$ must be trivial. So $G_0 \leq k_E^\times$ is finite cyclic.

Suppose $\mathrm{char}\, k_E = p > 0$, then each π_E^i/π_E^{i+1} $(i \geq 1)$ is a finite dimensional $\mathbb{F}_p$-vector space, so have order some p power. So G_1 is a p-subgroup of G_0. Furthermore, since $G_0/G_1 \leq k_E^\times$ is cyclic of order coprime to p, $G_1 \lhd G_0$ is a p-Sylow subgroup.

Definition 4.11 (tame/wild ramification)**.** Let E/K be a Galois extension of CDVFs with k_E/k_K separable. We say E/K is **tamely ramified** if $G_1 = 1$, otherwise we say it is **wildly ramified** .

Remark **4.12.** E/K is tamely ramified if and only if $\operatorname{char} k_E = 0$, or $\operatorname{char} k_E = p > 0$ and $p \nmid |G_0| = e_{E/K}$.

Remark **4.13.** If E/K is tamely and totally ramified, $|G| = |G_0| = e_{E/K} = [E : K]$ divides $\left|k_E^\times\right|$. So we could get some information of the size of the Galois group using information of the size of $k_E^\times$.

We give a characterization of tamely and totally ramified extensions E/K.

Proposition 4.14. Let E/K be tamely and totally ramified, then there exists uniformizer π_K of A_K such that $A_E = A_K[\sqrt[n]{\pi_K}]$, where $n = [E : K]$.

Proof. Since E/K is totally ramified, $e_{E/K} = n$, $G = G_0 = I_{E/K}$, $f_{E/K} = 1$, $k_E = k_K$. Since E/K is tamely ramified, $G = G_0 \hookrightarrow k_K^\times$, so $G \cong \mathbb{Z}/n$, so k_K contains an element $\overline{\zeta}$ of order n. Let $f(X) := X^n - 1$, note $f'(X) = nX^{n-1}$, so $\overline{f}'(X) = n\overline{\zeta}^{n-1}$. If $n = 0 \in k_K$, then $\operatorname{char} k_K \mid n$, but this is absurd because finite subgroups of a field of characteristic p are cyclic and of order coprime to p. Hence $\overline{\zeta}$ is a primitive root of $\overline{f}(X)$, so by Hensel's lemma, there is a unique lift $\zeta \in A_K$ with $\zeta^n = 1$ and $\zeta \bmod \pi_K = \overline{\zeta}$.

Let $\sigma \in G$ be a generator, consider the element

$$\alpha := \pi_E + \zeta^{-1}\sigma(\pi_E) + \zeta^{-2}\sigma^2(\pi_E) + \cdots + \zeta^{-(n-1)}\sigma^{n-1}(\pi_E) \in A_E.$$

Note

$$\sigma(\alpha) = \sigma(\pi_E) + \zeta^{-1}\sigma^2(\pi_E) + \cdots + \zeta^{-(n-2)}\sigma^{n-1}(\pi_E) + \zeta^{-(n-1)}\pi_E = \zeta\alpha.$$

Hence $\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n$, so α^n is fixed by G, so $\alpha^n \in K \cap A_E = A_K$. Furthermore, since $\zeta \in A_K^\times \subseteq A_E^\times$, $\nu_E(\zeta) = 0$, and $\nu_E(\cdot)$ is preserved by G, so $\nu_E(\alpha) = \nu_E(n\pi_E) = \nu_E(\pi_E) = 1$, so $\alpha \in A_E$ is a uniformizer. So $\nu_K(\alpha^n) = \nu_E(\alpha^n)/n = 1$, and $\alpha^n \in A_K$ is also a uniformizer. Finally, since $k_K = k_E$, every element of A_E may be expressed as $\sum_{i\geq 0} a_i\alpha^i$, where $a_i \in A_K$. So $A_E = A_K[\alpha]$, we are done. □

4.2. **Fixing the indexing of the ramification groups.** We now fix the indexing of the ramification groups so that they are compatible with quotients. Recall the setup: E/K a Galois extension of CDVFs with Galois group G, $H \lhd G$, $K' := E^H$. We first observe some relations between i_G and $i_{G/H}$.

Proposition 4.15. For every $\sigma \in G/H$,

$$i_{G/H}(\sigma) = \frac{1}{e_{E/K'}} \sum_{s\in G:\overline{s}=\sigma\in G/H} i_G(s)$$

Proof (Due to Tate). Pick generators $x \in A_E$ and $y \in A_{K'}$ such that $A_E = A_K[x]$ and $A_{K'} = A_K[x]$. Then for $sH \in G/H$, $i_{G/H}(sH) = \nu_{K'}(sH(y) - y) = \frac{1}{e_{E/K'}}\nu_E(s(y) - y)$. Suffices to show for $s \in G$,

$$\nu_E(s(y) - y) = \sum_{t\in H} \nu_E(st(x) - x) = \nu_E(\prod_{t\in H}(st(x) - x)),$$

we may assume $s \notin H$ because in that case both sides are infinite.

Key observation: from Galois theory, we know the minimal polynomial of x over K' equals $f(X) = \prod_{t\in H}(t(x) - X)$. This is because H fixes the minimal polynomial, hence every H-conjugate of x is a root of the minimal polynomial. For $s \in G$, let $s \cdot f(X)$ denote the polynomial $f(X)$ with each coefficient acted upon by s. So $\prod_{t\in H}(st(x) - x) = (s \cdot f)(x)$.

Let $s \in G - H$ be fixed, let $a := s(y) - y$ and $b := \prod_{t\in H}(st(x) - x)$, we will show $(a) = (b) \lhd A_E$. Expand the minimal polynomial $f(X)$ into $\sum a_i X^i$, for $a_i \in A_E \cap K' = A_{K'}$. Since $A_{K'} = A_K[y]$, we have polynomials $f_i(X) \in A_K[X]$ such that $a_i = f_i(y)$. Observe

$$(s \cdot f)(X) - f(X) = \sum[s(a_i) - a_i]X^i = \sum[f_i(s(y) - y)]X^i.$$

Since $\nu_E(f_i(s(y) - y)) \geq \nu_E(s(y) - y)$ (clear if $\deg f_i \geq 1$, and if $\deg f_i = 0$, then $a_i \in A_K$, so $s(a_i) - a_i = 0$), $\nu_E((s \cdot f)(x)) = \nu_E((s \cdot f)(x) - f(x)) \geq \nu_E(s(y) - y)$, so $a \mid b$.

Conversely, suppose $y = g(x)$ for $g(X) \in A_K[X]$, then $g(X) - y \in A_{K'}[X]$ has x as a root, hence is divisible by $f(X)$, so $g(X) - y = f(X) \cdot h(X)$ in $A_{K'}[X]$. Then $(s \cdot f)(X)$ divides $s \cdot g(X) - s(y) = g(X) - s(y)$, so $b = (s \cdot f)(x)$ divides $g(x) - s(y) = -a$. We win. □

We make our first step toward the case of quotients.

Proposition 4.16. Suppose the normal subgroup $H \lhd G$ equals some G_j $(j \geq 0)$, then $(G/H)_i = G_i/H$ for $(i \leq j)$ and $(G/H)_i = 1$ for $i \geq j$.

Proof. Note $G/H = G_{-1}/H \geq G_0/H \geq G_1/H \cdots \geq G_j/H = 1$ is a filtration of G/H, so for any $\sigma \neq \mathrm{id} \in G/H$, there is some $i \geq -1$ such that $\sigma \in G_i/H$ but $\sigma \notin G_{i+1}/H$. So any representative $s \in G$ of σ is contained in $G_i - G_{i+1}$, so $i_G(s) = i + 1$. So Proposition 4.15 tells us $i_{G/H}(\sigma) = |H|\,(i+1)/e_{E/K'}$.

Furthermore, since $H \leq G_0$, the fixed field $K' = E^H$ is an intermediate field between E and $E_0 = E^{G_0}$, in particular E/K' is totally ramified, and $e_{E/K'} = [E : K'] = |H|$. So $i_{G/H}(\sigma) = i + 1$. So $G_i/H = (G/H)_i$ for $-1 \leq i \leq j$. And for $i \geq j$, $(G/H)_i \leq (G/H)_j = G_j/G_j = 1$, they are all trivial. □

We want to modify the indexing so that the above is true for any normal subgroup $H \lhd G$. We introduce the upper ramification indexing as following.

For any real number $u \geq 0$, let $G_u := G_{\lceil u \rceil}$. Define **ramification function** $\varphi_{E/K} : [0, \infty) \to [0, \infty)$ by

$$\varphi_{E/K}(u) := \int_0^u [G_0 : G_t]^{-1} dt.$$

Note $\varphi_{E/K}$ is continuous, piecewise linear, strictly increasing, and the discontinuities of its derivative occurs only at the integer values of u. Let $\psi_{E/K}$ denote its inverse: $\psi_{E/K}(v) := \varphi^{-1}_{E/K}(v)$ for $v \in [0, \infty)$. So $\psi_{E/K}$ is also a strictly increasing piecewise linear function from $[0, \infty)$ to $[0, \infty)$, with slopes of each linear segment the reciprocals of the slopes of segments of $\varphi_{E/K}$. Define the **upper ramification groups** to be $G^v := G_{\psi_{E/K}(v)}$.

This definition is precisely the one we need to have $(G/H)^v = G^v H/H$ for all v. To see that, we need several numerical identities.

Lemma 4.17.

$$\varphi_{E/K}(u) + 1 = \frac{1}{|G_0|} \sum_{s\in G} \min\{i_G(s), u + 1\}.$$

Proof. Observe both sides are piecewise linear and equals 1 at 0. So it suffices to check their derivatives are the same on each linear piece $[m, m+1]$. Note if $m \leq u \leq m+1$, then the derivative of LHS is $[G_0 : G_u]^{-1}$ and the derivative of RHS is

$$\frac{1}{|G_0|} \sum_{s \in G : i_G(s) \geq u+1} 1 = \frac{1}{|G_0|} \sum_{s \in G_u} 1 = [G_0 : G_u]^{-1},$$

because $i_G(s) \geq u+1 \iff s \in G_u$. We win. □

Lemma 4.18. For $\sigma \in G/H$, let $j(\sigma)$ denote the least upper bound of $i_G(s)$ as s runs through all representatives of σ in G. Then

$$i_{G/H}(\sigma) - 1 = \varphi_{E/K'}(j(\sigma) - 1).$$

Proof. Pick representative s of σ so that $i_G(s) \geq i_G(st)$ for all $t \in H$, hence $j(\sigma) = i_G(s)$. Expand both sides using Lemma 4.17 and Proposition 4.15, we want to show

$$\frac{1}{e_{E/K'}} \sum_{t \in H} i_G(st) = \frac{1}{|H_0|} \sum_{t \in H} \min\{i_H(t), j(\sigma)\}.$$

Recall $e_{E/K'} = \left|I_{E/K'}\right| = |H_0|$. It suffices to show for each $t \in H$, $i_G(st) = \min\{i_H(t), j(\sigma)\}$. Note $i_H(t) = \nu_E(t(\pi_E) - \pi_E) = i_G(t)$, so we want to show $i_G(st) = \min\{i_G(t), i_G(s)\}$. Suppose $i_G(t) < i_G(s)$, then by an earlier remark, $LHS = i_G(t) = RHS$. Suppose $i_G(t) \geq i_G(s)$, then $i_G(s) \leq i_G(st) \leq i_G(s)$, so $LHS = RHS = i_G(s)$. □

Theorem 4.19 (Herbrand's Theorem)**.** If $v = \varphi_{E/K'}(u)$, then $G_u H/H = (G/H)_v$, where $G_u H/H$ denotes the image of G_u in the quotient G/H.

Proof. Let $\sigma = sH \in G/H$, then

$$\begin{aligned} \sigma \in G_u H/H &\iff \exists t \in H, st \in G_u \\ &\iff \exists t \in H, i_G(st) \geq u+1 \\ &\iff j(\sigma) \geq u+1 \\ &\iff \varphi_{E/K'}(j(\sigma) - 1) \geq v && \varphi_{E/K'} \text{ is monotone} \\ &\iff i_{G/H}(\sigma) \geq v+1 && \text{Lemma 4.18} \\ &\iff \sigma \in (G/H)_v && . \end{aligned}$$

□

Corollary 4.20. The functions φ, ψ satisfy the transitivity relations:

$$\varphi_{E/K} = \varphi_{K'/K} \circ \varphi_{E/K'}, \quad \psi_{E/K} = \psi_{E/K'} \circ \psi_{K'/K}.$$

Proof. It suffices to show the case for φ, we will check the derivatives of both sides coincide on non-integer values. Let $u \in (0, \infty)$ be a non-integer, $v := \varphi_{E/K'}(u)$, then

$$(\varphi_{K'/K} \circ \varphi_{E/K'})'(u) = \varphi'_{K'/K}(v) \cdot \varphi'_{E/K'}(u) = [(G/H)_0 : (G/H)_v]^{-1} \cdot [H_0 : H_u]^{-1} = \frac{\left|(G/H)_v\right| |H_u|}{e_{K'/K} e_{E/K'}}.$$

By Theorem 4.19, the numerator equals $\left|G_u H/H\right| |H_u|$. Since we have short exact sequence

$$0 \longrightarrow H_u = G_u \cap H \longrightarrow G_u \longrightarrow G_u H/H \longrightarrow 0$$

so the derivative equals $|G_u| / e_{E/K} = [G_0 : G_u]^{-1} = \varphi'_{E/K}(u)$. We are done. □

Corollary 4.21.

$$(G/H)^v = G^v H/H \qquad (v \geq 0).$$

Proof.

$$(G/H)^v = (G/H)_{\psi_{K'/K}(v)} = G_{\psi_{E/K'} \circ \psi_{K'/K}(v)} H/H = G_{\psi_{E/K}(v)} H/H = G^v H/H.$$

□

4.3. **Generalization and applications.** We are now able to generalize the notion of "maximal unramified subextension" to non Galois extensions of CDVFs with separable residue extensions.

Definition 4.22. Let E/K be any extension of CDVFs with k_E/k_K separable, let $v \geq 0$ be a real number. Define subextension $K \subseteq E^v \subseteq E$ to be $E^v := E \cap L^{G^v}$, where L/E is any extension of CDVFs, k_L/k_E separable, and L/K Galois, and $G := \mathrm{Gal}(L/K)$.

Some immediate observations:

(1) For $v < v'$, $\psi_{L/K}(v) < \psi_{L/K}(v')$, $G^v \geq G^{v'}$, so $E^v \subseteq E^{v'}$.
(2) Since $G^v = 1$ for $v \gg 0$ (recall $\psi_{E/K}$ is strictly increasing), so $\cup_{v \geq 0} E^v = E$.
(3) As v increases from 0, the field E^v will start from the maximal unramified subextension of E/K and become more and more ramified, until become the whole extension E/K.
(4) The definition of E^v is independent of the choice of extension L. Let $L, L'/E$ be two such extensions, the their compositum LL' in $\overline{E}$ is again an extension over E, Galois over K. So it suffices to consider a tower $L'/L/E$, with L'/K and L/K Galois with Galois groups G' and G, respectively. Let $H := \mathrm{Gal}(L'/L)$.

$$\begin{tikzcd}
L' \arrow[d, dash, "H"'] \arrow[dd, dash, bend left, "G'"] \\
L \arrow[d, dash, "G"'] \\
K
\end{tikzcd}$$

Recall from the compatibility of upper indexing with quotients, $G^v = (G'/H)^v = G'^v H/H$, so $E \cap L^{G^v} = E \cap (L')^{G'^v}$.

This definition allow us to study the ramification theory of CDVFs using ramification groups, in the case that the extension is not Galois. In particular we have description of the maximal unramified subextension using ramification groups.

Proposition 4.23. Let E/K be a possibly non-Galois extension of CDVFs with k_E/k_K separable, then

(1) E^0 is the maximal unramified subextension of E/K.
(2) If $E/M/K$ is an intermediate field, then $M^v = E^v \cap M$.
(3) Let $E/M, N/K$ be two intermediate fields, then $M^v \cdot N^v \subseteq (M \cdot N)^v$. In particular, if $M^v = M$ and $N^v = N$, then $M^v \cdot N^v = (M \cdot N)^v$.

Proof. Let L/K be the Galois closure of E/K (we know exists because any extension of CDVFs is assumed to be separable), let $G = \mathrm{Gal}(L/K)$, then $G^0 = G_0 = I_{L/K}$, and $L^{I_{L/K}} = L_0$ is the maximal unramified subextension of L/K. So $E_0 \subseteq L_0 \cap E = E^0$. On the other hand by the multiplicative property of residue degrees in towers, $E^0 = L_0 \cap E$ is unramified over K, so $E^0 = E_0$ is the maximal unramified subextension of E/K.

Part (2) follows from definition of E^v and M^v. For part (3), $M^v \cdot N^v = (M \cap L^{G^v}) \cdot (N \cap L^{G^v}) = (M \cdot N) \cap L^{G^v} = (M \cdot N)^v$. □

Unlike the lower ramification filtration, the upper ramification filtration could jump on rational values. However for most examples we care about, the jumps can only be integers: this is the Hasse-Arf theorem. It is stated below, we will not prove it.

Theorem 4.24 (Hasse-Arf)**.** Let $K/\mathbb{Q}_p$ be a finite extension, E/K an abelian extension, then any jump of the upper ramification filtration of $\mathrm{Gal}(E/K)$ is an integer.

To conclude this section we introduce an important notion that will be used to organize the global class field theory – the conductor ideal. Let $K/\mathbb{Q}_p$ be a finite extension, E/K an abelian extension, the **conductor ideal** $C_{E/K} \lhd A_K$ is (π_K^a), where a is the smallest non-negative integer such that $\mathrm{Gal}(E/K)^a = 1$, or equivalently $E^a = E$.

***Remark* 4.25.** E/K unramified iff $E^0 = E$ iff $C_{E/K} = (\pi_K^0) = (1)$.

Proposition 4.26. Let $K/\mathbb{Q}_p$ be a finite extension, E/K an abelian extension, $E/E_1, E_2/K$ two abelian subextensions. Then $E_1 \cdot E_2/K$ is also abelian, and $C_{E_1 \cdot E_2/K} = \mathrm{lcm}(C_{E_1/K}, C_{E_2/K})$.

Proof. Observe we have inclusion of Galois groups $\mathrm{Gal}(E_1 \cdot E_2/K) \hookrightarrow \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K)$, so $E_1 \cdot E_2/K$ is abelian. We also have in this case, $(E_1 \cdot E_2)^v = E_1 \cdot E_2$ if and only if $(E_1)^v = E_1$ and $(E_2)^v = E_2$. Why? We know one direction from previous discussions. Conversely note since $E_1 \cdot E_2/K$ is abelian, so $(E_i)^v = E_i \cap (E_1 \cdot E_2)^v = E_i \cap E_1 \cdot E_2 = E_i$. □

5. Global Class Field Theory

The goal of this section is to classify all abelian extensions of a fixed number field K. We will not prove the main theorem of global class field theory. Instead we will understand the statement and its implications.

Let E/K be an abelian extension of number fields. We start our discussion by defining a global **conductor ideal** $C_{E/K} \lhd \mathcal{O}_K$. Define $C_{E/K} := \prod_{0 \neq \mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_K} \mathfrak{p}^{a_\mathfrak{p}}$, where $a_\mathfrak{p}$ is the smallest non-negative integer such that for any $\mathfrak{q} \in \mathrm{Spec}\, \mathcal{O}_E$ lying above $\mathfrak{p}$, $E_\mathfrak{q}^{a_\mathfrak{p}} = E_\mathfrak{q}$. Since E/K is Galois, the Galois group acts transitively on the set of primes of $\mathcal{O}_E$ lying above $\mathfrak{p}$, so there is an isomorphism of extensions CDVFs $E_{\mathfrak{q}_1} \xrightarrow{\sim} E_{\mathfrak{q}_2}$ over $K_\mathfrak{p}$ for $\mathfrak{q}_1, \mathfrak{q}_2$ lying above $\mathfrak{p}$. So the exponent $a_\mathfrak{p}$ equals the smallest non-negative integer such that $E_{\mathfrak{q}_i}^{a_\mathfrak{p}} = E_{\mathfrak{q}_i}$ for each $\mathfrak{q}_i$ lying above $\mathfrak{p}$. Therefore $C_{E/K} \cdot \mathcal{O}_{K,\mathfrak{p}} = C_{E_\mathfrak{q}/K_\mathfrak{p}}$ for any $\mathfrak{q}$ lying above $\mathfrak{p}$, where the right hand side is the local conductor ideal we have introduced earlier.

We also note a prime $\mathfrak{p} \in \mathrm{Spec}\, \mathcal{O}_K$ is ramified in E if and only if $\mathfrak{p} \mid C_{E/K}$. So the conductor ideal describes those primes of $\mathcal{O}_K$ that could ramify in E. To see the use of this notion, we consider the special case of classifying abelian extensions of $K = \mathbb{Q}$.

First recall if ζ_N denotes a primitive N-th root of unity, then $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is an abelian extension with Galois group isomorphic to $(\mathbb{Z}/N)^\times$. The isomorphism is given by sending $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \mapsto a \in (\mathbb{Z}/N)^\times$ so that $\sigma(\zeta_N) = \zeta_N^a$. Hence by Galois theory, we have bijection

$$\begin{Bmatrix} \text{subextensions} \\ \mathbb{Q}(\zeta_N)/K/\mathbb{Q} \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} \text{subgroups} \\ H \leq (\mathbb{Z}/N)^\times \end{Bmatrix}.$$

We also have

Theorem 5.1 (Kronecker-Weber)**.** Let $K/\mathbb{Q}$ be an abelian extension, then there exists an integer $N \geq 1$ such that $K \subseteq \mathbb{Q}(\zeta_N)$. More precisely, $K \subseteq \mathbb{Q}(\zeta_N)$ if and only if $C_{K/\mathbb{Q}} \mid (N)$. So for integer $N \geq 1$, we have a bijection

$$\left\{\begin{matrix}\text{abelian extensions } K/\mathbb{Q}\\ \text{with } C_{K/\mathbb{Q}} \mid (N)\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups}\\ H \leq (\mathbb{Z}/N)^{\times}\end{matrix}\right\}$$

We formulate the class field theory for cyclotomic fields.

Theorem 5.2 (Class field theory for cyclotomic fields)**.** Let $N \geq 1$ be an integer, $K/\mathbb{Q}$ an abelian extension such that $C_{K/\mathbb{Q}} \mid N$. So for any prime p not dividing N must be unramified in K, so the Artin symbol $\left(\frac{K/\mathbb{Q}}{(p)}\right) \in \mathrm{Gal}(K/\mathbb{Q})$ is well-defined. Then there exists a unique surjective group homomorphism $\phi_{K/\mathbb{Q}} : (\mathbb{Z}/N)^{\times} \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$ that sends any residue class of prime $p \nmid N$ to the Actin symbol $\left(\frac{K/\mathbb{Q}}{(p)}\right)$. Furthermore, the map $K \mapsto \ker(\phi_{K/\mathbb{Q}})$ defines the bijection above

$$\begin{array}{ccc}\left\{\begin{matrix}\text{abelian extensions } K/\mathbb{Q}\\ \text{with } C_{K/\mathbb{Q}} \mid (N)\end{matrix}\right\} & \longleftrightarrow & \left\{\begin{matrix}\text{subgroups}\\ H \leq (\mathbb{Z}/N)^{\times}\end{matrix}\right\}\\ K & \longmapsto & \ker(\phi_{K/\mathbb{Q}})\end{array}$$

To generalize all of this to the case of an arbitrary number field K, we introduce the following notations.

Let K be a number field, a **modulus** is a pair $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$, where $\mathfrak{m} \lhd \mathcal{O}_K$ is an ideal and $\mathfrak{m}_\infty \subseteq \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$ is some set of $\mathbb{Q}$-homomorphisms from K into $\mathbb{R}$. The **trivial modulus** is the pair $(\mathcal{O}_K, \varnothing)$. For abelian extension E/K of number fields, we have a natural associated modulus $\mathfrak{m}_{E/K} := (C_{E/K}, \{\tau : K \hookrightarrow \mathbb{R} : \nexists\, \overline{\tau} : E \hookrightarrow \mathbb{R}, \overline{\tau}|_K = \tau\})$.

Definition 5.3. Let K be a number field, $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ a modulus,

$$\begin{aligned}
&\mathscr{I} := \{\text{nonzero fractional ideals of } \mathcal{O}_K\}\\
&\mathscr{P} := \{\text{nonzero principal fractional ideals of } \mathcal{O}_K\}\\
&H_K := \mathscr{I}/\mathscr{P} \quad \text{the usual ideal class group}\\
&\mathscr{I}(\mathfrak{m}_0) := \{\text{nonzero fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}_0\}\\
&\qquad = \left\{I \in \mathscr{I} : \forall\, 0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K, \nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0 \implies \nu_{\mathfrak{p}}(I) = 0\right\}\\
&K(\mathfrak{m}_0) := \left\{\alpha \in K^{\times} : \forall\, 0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K, \nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0 \implies \nu_{\mathfrak{p}}(\alpha) = 0\right\}\\
&K_{\mathfrak{m}} := \left\{\alpha \in K^{\times} : \begin{matrix}\forall\, 0 \neq \mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K, \nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0 \implies 1 \equiv \alpha \bmod \mathfrak{m}_0\, \mathcal{O}_{K,\mathfrak{p}}\\ \forall\, \tau \in \mathfrak{m}_\infty, \tau(\alpha) > 0\end{matrix}\right\}\\
&\mathscr{P}(\mathfrak{m}_0) := \left\{(\alpha) : \alpha \in K(\mathfrak{m}_0)\right\}\\
&\mathscr{P}_{\mathfrak{m}} := \left\{(\alpha) : \alpha \in K_{\mathfrak{m}}\right\}\\
&H(\mathfrak{m}) := \mathscr{I}(\mathfrak{m}_0)/\mathscr{P}_{\mathfrak{m}} \quad \text{the } \textbf{ray class group} \text{ of } (K, \mathfrak{m})
\end{aligned}$$

Observe for the trivial modulus, the ray class group coincides the usual ideal class group. Moreover, the ray class group generalizes the notion of usual ideal class group and the group $(\mathbb{Z}/N)^{\times}$ from the case of $K = \mathbb{Q}$.

Proposition 5.4. Let K be a number field, $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ a modulus, then

(1) the ray class group $H(\mathfrak{m})$ is a finite abelian group,
(2) there are short exact sequences of abelian groups

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{P}(\mathfrak{m}_0)/\mathscr{P}_{\mathfrak{m}} \arrow[r] & H(\mathfrak{m}) = \mathscr{I}(\mathfrak{m}_0)/\mathscr{P}_{\mathfrak{m}} \arrow[r] & H_K \arrow[r] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathcal{O}_K^\times}{\mathcal{O}_K^\times \cap K_{\mathfrak{m}}} \arrow[r] & (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \prod_{\tau\in\mathfrak{m}_\infty}\{\pm 1\} \arrow[r] & \frac{\mathscr{P}(\mathfrak{m})}{\mathscr{P}_{\mathfrak{m}}} \arrow[r] & 0
\end{tikzcd}$$

Proof sketch. Assume the result that the usual ideal class group H_K is finite, the first part follows from the second. To show the first sequence is short exact it suffices to show $H_K \cong \mathscr{I}(\mathfrak{m}_0)/\mathscr{P}(\mathfrak{m}_0)$. Note we have injection $\mathscr{I}(\mathfrak{m})/\mathscr{P}(\mathfrak{m}_0) \hookrightarrow H_K$, to show surjectivity it suffices to show for each nonzero fractional ideal I of $\mathcal{O}_K$, there exists $\alpha \in K^\times$ so that $\alpha^{-1}I \in \mathscr{I}(\mathfrak{m}_0)$. Put $\alpha := \prod_{\mathfrak{p}:\nu_{\mathfrak{p}}(\mathfrak{m}_0)>0} \pi_{\mathfrak{p}}^{\nu_{\mathfrak{p}}(I)}$ suffices.

For the second sequence, note we have commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^\times \cap K_{\mathfrak{m}} \arrow[r] \arrow[d, hook] & K_{\mathfrak{m}} \arrow[r] \arrow[d, hook] & \mathscr{P}_{\mathfrak{m}} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & K(\mathfrak{m}_0) \arrow[r] & \mathscr{P}(\mathfrak{m}_0) \arrow[r] & 0
\end{tikzcd}$$

so by snakes lemma, we have short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathcal{O}_K^\times}{\mathcal{O}_K^\times \cap K_{\mathfrak{m}}} \arrow[r] & \frac{K(\mathfrak{m}_0)}{K_{\mathfrak{m}}} \arrow[r] & \frac{\mathscr{P}(\mathfrak{m}_0)}{\mathscr{P}_{\mathfrak{m}}} \arrow[r] & 0.
\end{tikzcd}$$

One can show the map

$$\begin{tikzcd}
\dfrac{K(\mathfrak{m}_0)}{K_{\mathfrak{m}}} \arrow[r] & (\mathcal{O}_K/\mathfrak{m}_0)^\times \times \displaystyle\prod_{\tau\in\mathfrak{m}_\infty}\{\pm 1\} \arrow[r] & \displaystyle\prod_{\mathfrak{p}\text{ s.t.}\nu_{\mathfrak{p}}(\mathfrak{m}_0)>0}\left(\mathcal{O}_{K,\mathfrak{p}}^\times/1+\mathfrak{m}_0\,\mathcal{O}_{K,\mathfrak{p}}\right) \times \displaystyle\prod_{\tau\in\mathfrak{m}_\infty}\mathbb{R}/\mathbb{R}_{>0} \\
\alpha \arrow[rr, mapsto] & & ((\alpha)_{\mathfrak{p}}, \tau(\alpha))
\end{tikzcd}$$

is an isomorphism. Some observations/hints:

(1) If $0 \neq \mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ such that $\nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0$, then the inclusion $K^\times \hookrightarrow K_{\mathfrak{p}}^\times$ restricts to $K(\mathfrak{m}_0) \hookrightarrow \mathcal{O}_{K,\mathfrak{p}}^\times$, because the valuation at $\mathfrak{p}$ is zero.
(2) We have short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & 1+\mathfrak{m}_0\,\mathcal{O}_{K,\mathfrak{p}} \arrow[r] & \mathcal{O}_{K,\mathfrak{p}}^\times \arrow[r] & (\mathcal{O}_K/\mathfrak{m}_0)^\times \arrow[r] & 0
\end{tikzcd}$$

(3) By Chinese remainder theorem, for any $x \in (\mathcal{O}_K/\mathfrak{m}_0)^\times$, there exists $\alpha \in \mathcal{O}_K$ with $\alpha \equiv x \bmod \mathfrak{m}_0$, replacing α with $\alpha + kN$ for some $k \in \mathbb{N}$ and $N \in \mathbb{Z}\cap\mathfrak{m}_0$, we may also assume $\tau(\alpha) > 0$.
(4) For any subset $S \subseteq \mathfrak{m}_\infty$, there exists $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 1 \mod \mathfrak{p}$ for all $\mathfrak{p}$ with $\nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0$, and $\tau(\alpha) = 1$ if $\tau \in S$ and $\tau(\alpha) = -1$ if $\tau \notin S$.
(5) Let $\theta \in K$ be a primitive element, with minimal polynomial $f(X) \in \mathbb{Q}[X]$, then real embeddings of K corresponds to real roots of $f(X)$. Let α_τ be the real root associated to $\tau \in S$, then fix a real polynomial $g(X) \in \mathbb{R}[X]$ such that $g(\alpha_\tau) = 1$ if $\tau \in S$ and $g(\alpha_\tau) = -1$ if $\tau \notin S$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists $h(X) \in \mathbb{Q}[X]$ with $h(\alpha_\tau) > 0$ if $\tau \in S$ and $h(\alpha_\tau) < 0$ if $\tau \notin S$. Clear the denominators we may assume $h(X) \in \mathbb{Z}[X]$. Let $\alpha \in \mathcal{O}_K$ be any element such that $\alpha \equiv 1 \bmod \mathfrak{p}$ for $\nu_{\mathfrak{p}}(\mathfrak{m}_0) > 0$, and replace α by some $\alpha + kNh(\theta)$ for $k \gg 1$ suffices.

□

Here is the statement of global class field theory.

Theorem 5.5 (Global class field theory)**.** Let K be a number field, $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ a modulus of K. Then

(1) If E/K is an abelian extension with $\mathfrak{m}_{E/K} \leq \mathfrak{m}$, then there exists a unique surjection $\phi_{E/K} : H(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(E/K)$ that sends each residue class $[\mathfrak{p}] \in H(\mathfrak{m})$ to the Artin symbol $(\frac{E/K}{\mathfrak{p}})$.

(2) The map $E/K \mapsto \mathrm{Ker}(\phi_{E/K}) \leq H(\mathfrak{m})$ defines an order-reversing bijection

$$\begin{Bmatrix} \text{abelian extensions } E/K \\ \text{with } \mathfrak{m}_{E/K} \leq \mathfrak{m} \end{Bmatrix} \longleftrightarrow \begin{Bmatrix} \text{subgroups of} \\ H(\mathfrak{m}) \end{Bmatrix}$$

In particular there exists a unique abelian extension $L(\mathfrak{m})/K$, maximal among abelian extensions E/K with $\mathfrak{m}_{E/K} \leq \mathfrak{m}$, such that $\phi_{L(\mathfrak{m})/K} : H(\mathfrak{m}) \to \mathrm{Gal}(L(\mathfrak{m})/K)$ is an isomorphism. This extension is called the **ray class field** of K and $\mathfrak{m}$.

In particular, when the modulus $\mathfrak{m} = (\mathcal{O}_K, \varnothing)$ is trivial, we have a unique maximal abelian extension L/K such that every $\mathbb{Q}$ homomorphism $K \to \mathbb{R}$ extends to L. This extension is called the **Hilbert class field of** K .

Let's see the class field theory for cyclotomic fields in this language. Let $N \geq 1$ be an integer, consider the modulus $\mathfrak{m} = ((N), \tau)$, where $\tau : \mathbb{Q} \hookrightarrow \mathbb{R}$ is the inclusion. Recall $H_{\mathbb{Q}} = 1$, so by Proposition 5.4, we compute $H(\mathfrak{m}) = (\mathbb{Z}/N)^\times \times \{\pm 1\}/\{\pm 1\} = (\mathbb{Z}/N)^\times$. So by GCFT, we get the order-reversing bijection as in Theorem 5.2.

5.1. **Binary quadratic form and imaginary quadratic extensions of $\mathbb{Q}$.** Finally we discuss a technique for computing class numbers for imaginary quadratic extensions of $\mathbb{Q}$. There is also a beautiful solution to the classical representation problem of representing a prime using a binary quadratic form.

A **binary quadratic form (BQF)** is a function $f(x,y) = ax^2 + bxy + cy^2$ with integers a, b, c. Such a form may also be represented by the matrix $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in Mat_2(\mathbb{Z})$ in the sense that

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Note $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic forms, by $(\gamma \cdot f)(x,y) := f(\gamma^{-1} \begin{pmatrix} x \\ y \end{pmatrix})$. So $\gamma \cdot f$ has matrix representation

$$\gamma^{-t} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \gamma^{-1}.$$

Define the **discriminant of BQF** $f(x,y)$ to be $b^2 - 4ac$. Note $\mathrm{disc}\, f = (-4) \cdot \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$, so $\mathrm{disc}\, f = \mathrm{disc}(\gamma \cdot f)$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. So the discriminant is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Recall the notion of discriminant of a finite extension $K/\mathbb{Q}$. Suppose $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$. Recall $K/\mathbb{Q}$ is separable, so there are n distinct embeddings $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$, each determined by the image of a fixed primitive element of K. Define the discriminant of extension $K/\mathbb{Q}$ with respect to basis $\alpha_1, \dots, \alpha_n$ to be $\operatorname{disc}(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))$. Observe this definition is independent of the ordering of α_j's and σ_i's. Observe by construction if $\beta_1, \dots, \beta_n$ is another basis of K over $\mathbb{Q}$, with $\beta_i = \sum a_{ij}\alpha_j$, then, $\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(a_{ij})^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n)$.

In particular, if $M \leq K$ is a subgroup, free over $\mathbb{Z}$ of rank n, then any two $\mathbb{Z}$-basis of M are related by an element of $\mathrm{GL}_n(\mathbb{Z})$, which has determinant ± 1, so $\operatorname{disc} M$ is well-defined independent of choice of integral basis. Recall in particular the ring of integers $\mathcal{O}_K$ of a number field $K/\mathbb{Q}$ has an integral basis, so $\operatorname{disc} \mathcal{O}_K$ is well-defined.

Moreover, if $M_2 \leq M_1 \leq K$ are subgroups, where M_i are both free over $\mathbb{Z}$ of rank n, then using Smith normal form, we see there are integral bases $\alpha_1, \dots, \alpha_n$ of M_1 and $\beta_1, \dots, \beta_n$ of M_2 such that $\beta_i = \lambda_i \alpha_i$. So $\operatorname{disc} M_2 = \left(\prod \lambda_i\right) \operatorname{disc} M_1 = [M_1 : M_2] \operatorname{disc} M_1$. So $\operatorname{disc} M_1 = \operatorname{disc} M_2$ if and only if $[M_1 : M_2] = 1$, if and only if $M_1 = M_2$.

We say a binary quadratic form $f(x, y) = ax^2 + bxy + cy^2$ is **positive definite** if for all $(x, y) \neq (0, 0)$, we have $f(x, y) > 0$. If $a \neq 0$, we may rewrite the form as

$$f(x, y) = a(x + \frac{b}{2a}y)^2 + (c - \frac{b^2}{4a})y^2$$

so $f(x, y)$ is positive definite if and only if $a > 0$ and $\operatorname{disc} f < 0$.

Now we are ready to formulate the fundamental relation between the ideal class group of imaginary quadratic fields and binary quadratic forms.

Theorem 5.6. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic extension, let $D = \operatorname{disc} \mathcal{O}_K$, then there is a bijection

$$\left\{\begin{array}{l}\mathrm{SL}_2(\mathbb{Z})\text{-orbits of positive definite bi-}\\ \text{nary quadratic forms } f(x,y) = ax^2 + \\ bxy + cy^2 \text{ with discriminant } D\end{array}\right\} \longleftrightarrow H_K$$

$$f(x, y) = ax^2 + bxy + cy^2 \longmapsto \mathbb{Z} \oplus \mathbb{Z}\beta, \quad \beta = \tfrac{-b+\sqrt{D}}{2a}$$

The theorem follows from the following proposition:

Proposition 5.7. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic extension, let $D = \operatorname{disc} \mathcal{O}_K$, then there is a $\mathrm{SL}_2(\mathbb{Z})$-equivariant bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\left\{\begin{array}{l}\text{positive definitie binary quadratic}\\ \text{forms } f(x,y) = ax^2 + bxy + cy^2 \text{ with}\\ \text{discriminant } D\end{array}\right\} \longleftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\left\{\begin{array}{l}\beta \in K \text{ with positive imagi-}\\ \text{nary part such that } \mathbb{Z} \oplus \mathbb{Z}\beta\\ \text{is a fractional ideal of } \mathcal{O}_K\end{array}\right\}$$

$$f(x, y) = ax^2 + bxy + cy^2 \longmapsto \beta = \tfrac{-b+\sqrt{D}}{2a}$$

where $\mathrm{SL}_2(\mathbb{Z})$ acts on right hand side by Möbius transformations, via $\begin{pmatrix} X & Y \\ Z & W \end{pmatrix} \cdot \beta := (X\beta + Y)/(Z\beta + W)$.

Now notices the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half complex plane $\mathfrak{h} = \{z \in \mathbb{C} : Imz > 0\}$ via Möbius transformations has fundamental domain

$$\mathscr{D} = \left\{z \in \mathfrak{h} : |z| > 1, -\frac{1}{2} \leq Rez \leq \frac{1}{2}\right\} \cup \left\{z \in \mathfrak{h} : |z| = 1, -\frac{1}{2} \leq Rez \leq 0\right\}.$$

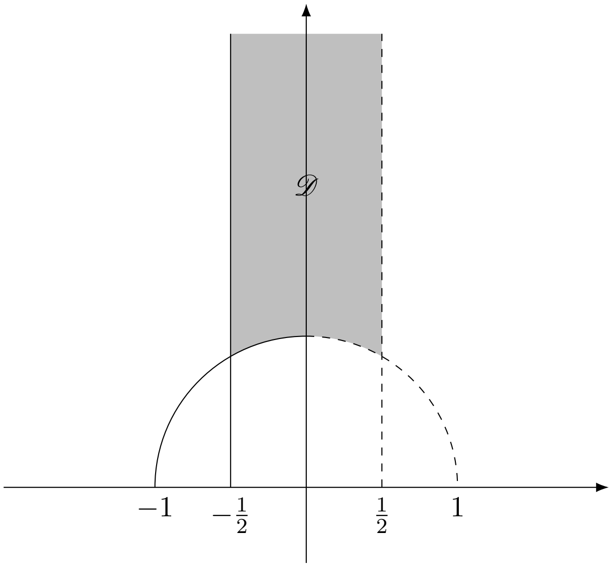


FIGURE 1. Fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathfrak{h}$

Therefore let $D = \operatorname{disc} \mathcal{O}_K$, then each $\mathrm{SL}_2(\mathbb{Z})$-orbit of positive definite binary quadratic form has a unique representative that is **reduced** , in the sense than $c \geq a \geq |b|$ and if either $c = a$ or $a = |b|$, then $b \geq 0$. In particular, we observe if $f(x, y) = ax^2 + bxy + cy^2$ is reduced, then $-D = 4ac - b^2 \geq 3b^2$, so $|b| \leq \sqrt{|D|/3}$, so there are only finitely many such reduced forms with discriminant D. This gives an alternative proof that the ideal class group H_K of an imaginary quadratic field, is finite.

Furthermore, one observes the identity element of H_K corresponds to the reduced form $x^2 - Dy^2/4$ if $D = 4d$ (i.e., when $d \equiv 2, 3 \bmod 4$), and $x^2 + xy + (1 - D)y^2/4$ if $D = d$ (i.e., when $d \equiv 1 \bmod 4$). These are called the **principal binary quadratic forms** of discriminant D .

Moreover if $f(x, y) = ax^2 + bxy + cy^2$ is a reduced form of discriminant D, then it corresponds to an element $[I = \mathbb{Z} + \mathbb{Z}\,\beta] \in H_K$ of order dividing 2 if and only if $[I] = [\sigma(I)]$, where $\sigma : \sqrt{-d} \mapsto -\sqrt{-d}$ generates the Galois group $\mathrm{Gal}(K/\mathbb{Q})$; and by looking at the element β in $\mathfrak{h}$, we see this happens if and only if either $c = a$ or $a = b$ or $b = 0$.

We now have the result.

Corollary 5.8. Let $K/\mathbb{Q}$ be an imaginary quadratic extension, $D = \operatorname{disc} \mathcal{O}_K$, a prime $p \nmid D$ can be represented by the principal binary quadratic form of discriminant D if and only if the ideal (p) splits completely in the Hilbert class field L/K of K.

Proof. Observe we can write the principal form as $f(x, y) = (x + y\beta)(x + y\sigma(\beta))$. Recall by class field theory, a prime $P \subseteq \mathcal{O}_K$ splits in L if and only if $\phi_{L/K}(P) = \left(\frac{L/K}{P}\right) = 1$, if and only if P is principal. Putting these together, we have

$$\begin{aligned}
&(p) \text{ splits in } L \\
\iff\ & (p)\,\mathcal{O}_K = P_1P_2 \text{ and } P_i \text{ splits in } L \\
\iff\ & (p)\,\mathcal{O}_K = P_1P_2 \text{ and } P_1 = (\alpha) \text{ is principal and } P_2 = (\sigma(\alpha)) \\
\iff\ & \exists x, y \in \mathbb{Z}, p = f(x,y) = \underbrace{(x + y\beta)}_{\alpha}\underbrace{(x + y\sigma(\beta))}_{\sigma(\alpha)} \\
\iff\ & p \text{ is represented by } f(x,y).
\end{aligned}$$

□

Index