University of
Cambridge

Mathematics Tripos

Part III

Algebraic Number Theory

Michaelmas, 2019

Lectures by
J. A. Thorne

Notes by
Qiangru Kuang

Contents

0 Introduction

In IID Number Fields, we studied finite extensions of $\mathbb{Q}$ and their rings of integers. We proved two fundamental theorem for $\mathcal{O}_K$:

- finiteness of ideal class group,
- finite generation of $\mathcal{O}_K^\times$.

In this course, we'll study

- completion at a prime,
- Galois theory of local and global fields.

and finally we'll describe class field theory (description only).

1 Dedekind domains

Definition (discrete valuation ring)**.** Let A be a ring. We say A is a *discrete valuation ring* (DVR) if A is a principal ideal domain (PID) and A has a unique non-zero prime ideal.

Let A be a DVR. Then the unique non-zero prime ideal $\mathfrak{m}_A$ of A is also maximal, so A is also a local ring, i.e. A has a unique maximal ideal. Hence $k_A = A/\mathfrak{m}_A$ is a field, the residue field of A.

As A is a PID, $\mathfrak{m}_A = (\pi)$ is principal. Any generator π is called a *uniformiser*. If π, π' are uniformisers then $(\pi) = (\pi')$ so $\pi' = \pi u$ for some $u \in A^\times$.

Since A is a local, A can be written as the disjoint union

$$\begin{aligned} A &= A^\times \cup \mathfrak{m}_A \\ &= A^\times \cup \pi A \\ &= A^\times \cup \pi A^\times \cup \pi^2 A \\ &= \bigcup_{i\geq 0} \pi^i A^\times \cup \bigcap_{i\geq 0} \pi^i A \end{aligned}$$

In fact, the ideal $I = \bigcap_{i\geq 0} \pi^i A$ is zero. This follows from

Lemma 1.1 (Nakayama's lemma)**.** *Let R be a local ring, $P \subseteq R$ the unique maximal ideal, M a finitely generated (fg) R-module. Then*

1. *if $M = PM$ then $M = 0$. This is equivalent to $M/PM = 0$.*
2. *if $N \leq M$ is an R-submodule such that $N + PM = M$ then $N = M$. This is saying there is a surjection $N \twoheadrightarrow M/PM$.*

Proof.

1. Let $a_1, \dots a_g$ be a generating set for M with g as small as possible, $g \geq 1$. Then $a_1 \in M = PM$ so we can write
$$a = \sum_{i=1}^{g} x_i a_i$$
where $x_i \in P$. Hence
$$(1 - x_1)a_1 = \sum_{i=2}^{g} x_i a_i.$$
Since R is local, $1 - x_1 \in R^\times$ so $a_1 \in \langle a_2, \dots, a_g \rangle$, contradicting the minimality of g.
2. Apply first part to M/N.

□

Now back to the statement. Note $\pi I = I$ so Nakayama's lemma implies that $I = 0$. Hence each element of $x \in A, x \neq 0$ admits a unique description

$x = \pi^n u$, $n \geq 0, u \in A^\times$. Each non-zero ideal of A has the form (π^i) for some $i \geq 0$.

Therefore we can define a function $v : K^\times \to \mathbb{Z}$ where $K = \operatorname{Frac} A$ with the following properties:

1. v is a surjective homomorphism,
2. for all $x, y \in K^\times$ such that $x + y \neq 0$, $v(x + y) \geq \min(v(x), v(y))$, with equality if $v(x) \neq v(y)$.

We define $v(x) = n$ when $x = \pi^n u$ for some $n \in \mathbb{Z}, u \in A^\times$.

Proof.

1. $\pi^n u \cdot \pi^m v = \pi^{n+m} uv$.
2. wlog $x = \pi^a u, y = \pi^{a+b} v$ where $a \in \mathbb{Z}, b \geq 0$. Then
$$x + y = \pi^a (u + v\pi^b).$$
If $b > 0$ then $u + v\pi^b \in A^\times$.

□

Definition (valuation)**.** If L is a field, we call a function $w : L^\times \to \mathbb{Z}$ a *valuation* if satisfies 1, 2 above.

Thus if we have a DVR then we have a valuation. The converse also holds: if $w : L^\times \to \mathbb{Z}$ is a valuation, we define

$$A_L = \{x \in L^\times : w(x) \geq 0\} \cup \{0\}$$
$$\mathfrak{m}_L = \{x \in L^\times : w(x) > 0\} \cup \{0\}$$

Lemma 1.2. *If k is a field, then there is a bijection between*

1. *subrings $A \leq K$ such that A is a DVR and* $\operatorname{Frac} A = K$,
2. *valuations $v : K^\times \to \mathbb{Z}$.*

Proof. Exercise. □

Example.

1. Let p be a prime, $v : \mathbb{Q}^\times \to \mathbb{Z}$ defined by
$$v(p^n \frac{r}{s}) = n$$
if $r, s \in \mathbb{Z}$, $(p, rs) = 1$.
2. Let K be the field of meromorphic functions on $\mathbb{C}$, $v : K^\times \to \mathbb{Z}$ defined by
$$v(f) = \operatorname{ord}_{z=0} f(z).$$

We will see via localisation we can reduce problems to DVR. Hence we need a way to recognise DVR. This is the content of the next proposition

Proposition 1.3. *Let A be a Noetherian domain. Then TFAE:*

1. *A is a DVR.*
2. *A is integrally closed in* $\operatorname{Frac} A$ *and A has a unique non-zero prime ideal.*

Recall that A is integrally closed if for all $\gamma \in K, a_1, \dots, a_n \in A$, if there is a relation

$$\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0$$

then $\gamma \in A$. Equivalently, for all $\gamma \in K$, $A[\gamma]$ is fg as an A-module then $\gamma \in A$.

Proof.

- $2 \implies 1$: suppose $\gamma \in K - A$ and there exist $a_1, \dots, a_n \in A$ such that

  $$\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0.$$

  We can write $\gamma = \pi^{-k}u$ for some $k > 0, u \in A^\times$. Hence

  $$-\pi^{-nk}u^n = a_1\pi^{-(n-1)k}u^{n-1} + \cdots + a_n.$$

  The valuation of LHS is $-nk$ and the valuation of RHS is at least

  $$\min_{i=1}^{n} v(a_i\pi^{-(n-i)k}) \geq \min v(\pi^{-(n-i)k}) = \min -(n-i)k \geq -(n-1)k.$$

  These two expressions must be equal, absurd. Thus A is integrally closed in K. A has a unique non-zero prime ideal as A is a DVR.

- $2 \implies 1$: Let $\mathfrak{m} \subseteq A$ be the unique non-zero prime ideal. Claim that for any proper non-zero ideal $I \subseteq A$, there exists $n \geq 1$ such that $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.

  Proof. $I \subseteq \mathfrak{m}$ as $\mathfrak{m}$ is the unique maximal ideal. Suppose for contradiction exists I such that $\mathfrak{m}^n \nsubseteq I$ for all $n \geq 1$. Since A is Noetherian, we can assume that I is maximal with this property. Note I is not prime as otherwise $I = \mathfrak{m}$. This means that there exist $a, b \in A$ such that $a, b \notin I$ but $ab \in I$. Then the inclusions $I \subseteq I + (a), I \subseteq I + (b)$ are proper. By maximality of I, there exists $n_1, n_2 \geq 1$ such that

  $$\mathfrak{m}^{n_1} \subseteq I + (a)$$
  $$\mathfrak{m}^{n_2} \subseteq I + (b)$$

  Then

  $$\begin{aligned}\mathfrak{m}^{n_1+n_2} &\subseteq (I + (a))(I + (b)) \\ &\subseteq I + (ab) \\ &\subseteq I\end{aligned}$$

  as $ab \in I$. Absurd. □

Now we can show $\mathfrak{m}$ is principal. Choose $\alpha \in \mathfrak{m} - \{0\}$. If $\mathfrak{m} = (\alpha)$ then done. Otherwise, choose $n \geq 2$ minimal such that $\mathfrak{m}^n \subseteq (\alpha) \subseteq \mathfrak{m}$. Then $\mathfrak{m}^{n-1} \nsubseteq (\alpha)$ so exists $\beta \in \mathfrak{m}^{n-1} - (\alpha)$ such that

$$\gamma = \frac{\beta}{\alpha} \in \frac{1}{\alpha}\mathfrak{m}^{n-1} - A.$$

Then

$$\gamma\mathfrak{m} = \frac{\beta}{\alpha}\mathfrak{m} \subseteq \frac{1}{\alpha}\mathfrak{m}^{n-1}\mathfrak{m} \subseteq \frac{1}{\alpha}\mathfrak{m}^n \subseteq A.$$

If $\gamma\mathfrak{m} \subseteq \mathfrak{m}$ then $A[\gamma] \hookrightarrow \mathrm{End}_A(\mathfrak{m})$ as A-modules. $\mathrm{End}_A(\mathfrak{m})$ is a fg A-module as A is Noetherian. So A integrally closed in K implies that $\gamma \in A$. So we must have $\gamma\mathfrak{m} = A$. Hence $\mathfrak{m} = \gamma^{-1}A$. So $\pi = \gamma^{-1} \in A$ and π generates $\mathfrak{m}$.

Since A is a local ring, we have

$$\begin{aligned} A &= A^\times \cup \mathfrak{m} \\ &= A^\times \cup \pi A \\ &= \bigcup_{i \geq 0} \pi^i A^\times \cup I \end{aligned}$$

where $I = \bigcap_{i \geq 0} \pi^i A$. $I = 0$ as I is fg (as A is Noetherian) and $\pi I = I$, so we can apply Nakayama's lemma. Hence

$$A = \{0\} \cup \bigcup_{i \geq 0} \pi^i A^\times$$

and A is a DVR.

□

Definition (multiplicative subset)**.** Let A be a ring. A *multiplicative subset* of A is a subset $S \subseteq A$ satisfying

1. $1 \in S$,
2. for all $x, y \in S$, $xy \in S$.

Definition (localisation of ring)**.** Let $S \subseteq A$ be a multiplicative subset. We define $S^{-1}A$ to be the set of equivalence classes of pairs $(a, s) \in A \times S$ under the relation $(a, x) \sim (a', s')$ if there exists $t \in S$ such that $t(s'a - sa') = 0$.

We write $\frac{a}{s} \in S^{-1}A$ for the equivalence class of (a, s).

Lemma 1.4.

1. *$S^{-1}A$ is well-defined and admits a ring structure.*
2. *There is a ring homomorphism*

$$\begin{aligned} A &\to S^{-1}A \\ a &\mapsto \frac{a}{1} \end{aligned}$$

with kernel $\{a \in A : \text{ exists } s \in S, sa = 0\}$.

3. *If* A *is a domain and* $0 \notin S$ *then* $S^{-1}A$ *may be identified with the subring* $\{\frac{a}{s} : a \in A, s \in S\}$ *of* $\operatorname{Frac} A = (A - \{0\})^{-1}A$.

Proof.

1. $\sim$ is an equivalence relation: it is reflexive and symmetric by definition. For transitivity, suppose $(a, s) \sim (a', s') \sim (a'', s'')$, then exist $t, t' \in S$ such that $tas' = ta's, t'a's'' = t'a''s'$. Then

$$tt's'as'' = tt's''a's = tt'a''s's$$

i.e.

$$tt's'(as'' - a''s) = 0.$$

To make $S^{-1}A$ a ring, the zero element is $\frac{0}{1}$, the multiplicative identity is $\frac{1}{1}$, and addition and multiplication are defined as

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$
$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

Check the ring axioms are satisfied.

2. $f : A \to S^{-1}A$ is a ring homomorphism by definition.

$$\ker f = \{a \in A : \frac{a}{1} = \frac{0}{1}\} = \{a \in A : \text{ exists } s \in S \text{ such that } sa = 0\}.$$

3. Now we suppose A is a domain. Recall that

$$\operatorname{Frac} A = \{(a, s) \in A \times (A - \{0\})\}/\bullet$$

where $(a, s) \bullet (a', s')$ if $as' = a's$. We need to check that if $S \subseteq A$ if a multiplicative subset with $0 \notin S$ then $(a, s) \sim (a', s')$ implies $(a, s) \bullet (a', s')$.

□

Definition (localisation of module)**.** Let $S \subseteq A$ to be a multiplicative subset and let M be an A-module. Then we define $S^{-1}M$ to be the set of equivalence classes in $M \times S$ for the relation $(m, s) \sim (m', s')$ if there exists $t \in S$ such that $t(ms - m's) = 0$.

We write $\frac{m}{s}$ for the equivalence class of (m, s).

Exercise.

1. $S^{-1}M$ is an $S^{-1}A$-module via

$$\frac{a}{s} \cdot \frac{m}{s'} = \frac{am}{ss'}$$
$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}$$

2. If $f : M \to N$ is an A-module homomorphism then there is a homomorphism

$$S^{-1}f : S^{-1}M \to S^{-1}N$$
$$\frac{m}{s} \mapsto \frac{f(m)}{s}$$

3. S^{-1} is a functor from the category of A-modules to the category of $S^{-1}A$-modules.

Lemma 1.5. *Let*

$$M' \xrightarrow{f} M \xrightarrow{f'} M''$$

be an exact sequence of A-modules. Then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}f'} S^{-1}M''$$

is also exact.

Proof. $f' \circ f = 0$ so $S^{-1}f' \circ S^{-1}f = 0$. For the other inclusion, let $\frac{m}{s} \in \ker S^{-1}f'$, i.e. $\frac{f'(m)}{s} = 0$, i.e. there exists $s' \in S$ such that $0 = s'f'(m) = f'(s'm)$ so $s'm \in \ker f' = \operatorname{im} f$. Hence there exists $m' \in M'$ such that $f(m') = s'm$. Then

$$S^{-1}f(\frac{m'}{ss'}) = \frac{f(m')}{ss'} = \frac{s'm}{ss'} = \frac{m}{s}.$$

□

Corollary 1.6. *If f is surjective (injective, resp) then so is $S^{-1}f$.*

Let $I \subseteq A$ be an ideal. Then $I \hookrightarrow A$ is an injective homomorphism of A-modules. Hence $S^{-1}I \hookrightarrow S^{-1}A$ is an injective homomorphism of $S^{-1}A$-module. Hence $S^{-1}I$ may be identified with an ideal of $S^{-1}A$. It's the ideal

$$S^{-1}A \cdot I = \{\frac{x}{s} : x \in I, s \in S\} \subseteq S^{-1}A.$$

Proposition 1.7. *Let $S \subseteq A$ be a multiplicative subset. Then there is a bijection between the following two sets:*

1. *prime ideals $P \subseteq A$ such that $P \cap S = \emptyset$,*
2. *prime ideal $Q \subseteq S^{-1}A$,*

given by $P \mapsto S^{-1}P, Q \mapsto f^{-1}(Q)$ where $f : A \to S^{-1}A$ is the localisation map.

Proof. Check the maps are well-defined: if $1 \in S^{-1}P$ then $\frac{1}{s} = \frac{x}{s}$ for some $x \in P, s \in S$ so exists $t \in S$ such that $t(s - x) = 0$. Then $ts = tx \in P$ so $t \in P$ or $s \in P$.

If $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}A$ and $\frac{aa'}{ss'} \in S^{-1}P$ then $\frac{aa'}{ss'} = \frac{x}{t}$. Hence exists $t' \in S$ such that

$$tt'aa' = t'ss'x \in P.$$

Since P is prime, $aa' = P$ so $a \in P$ or $a' \in P$. Hence $\frac{a}{s}$ or $\frac{a'}{s'} \in S^{-1}P$. Thus $S^{-1}P$ is prime.

If $Q \subseteq S^{-1}A$ then $S^{-1}A/Q$ is a non-zero domain. Then $A/f^{-1}(Q) \hookrightarrow S^{-1}A/Q$ so $A/f^{-1}(Q)$ is also a non-zero domain so $f^{-1}(Q)$ is a prime ideal (this in fact follows from the fact that pullback of any prime ideal is prime).

It is left as an exercise to check the maps in the statement of the proposition are mutually inverse bijections. □

Corollary 1.8. *Let A be a ring and $P \subseteq A$ a prime ideal. Then*

1. *$S = A - P$ is a multiplicative subset of A.*
2. *$S^{-1}A$ is a local ring with unique maximal ideal $S^{-1}P$.*

We usually write A_P for $(A - P)^{-1}A$.

For example $\mathbb{Z}_{(p)} = (\mathbb{Z} - p\mathbb{Z})^{-1}\mathbb{Z}$.

Proposition 1.9. *Let A be a Noetherian domain. Then TFAE:*

1. *For every non-zero prime ideal $P \subseteq A$, A_P is a DVR.*
2. *A is integrally closed in $K = \operatorname{Frac} A$ and every non-zero prime ideal is maximal.*

Consequently, for any P there is the valuation $v_P : K^\times \to \mathbb{Z}$ associated to A_P.

Definition (Dedekind domain)**.** Any ring satisfying the conditions is called a *Dedekind domain.*

Proof.

- 1 $\implies$ 2: wlog we can assume A does have non-zero prime ideals. Suppose given a relation
$$a^n + a_1a^{n-1} + \cdots + a_n = 0$$
where $a \in A, a_i \in A$. Then A_P is a DVR implies that A_P is integrally closed in K so $a \in A_P$ for all P. Therefore for all P we can find $x_P \in A, s_P \in A - P$ such that $a = \frac{x_P}{s_P}$ in K. In particular $s_Pa \in A$.
The ideal
$$I = (s_P : P \subseteq A \text{ non-zero prime ideal})$$
is the unit ideal, since it is not contained in any maximal ideal of A. Therefore there exists element $t_P \in A$, with only finitely many non-zero, such that
$$1 = \sum_P t_P s_P.$$

Then
$$a = \sum_P t_P s_P a \in A.$$

Let $P \subseteq Q$ be non-zero prime ideals of A, with Q maximal. Then $PA_Q \subseteq QA_Q$ are non-zero prime ideals of A_Q, a DVR. Hence $PA_Q = QA_Q$ and $P = Q$.

- $2 \implies 1$: Again we can assume that A has a non-zero prime ideal P. We must show A_P is a DVR, or equivalently that A_P is integrally closed in K and has a unique non-zero prime ideal.

  Suppose given a relation
  $$\left(\frac{a}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{a}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$
  where $a, a_1, \ldots, a_n \in A, s_1, \ldots, s_n \in A - P, s \in A - \{0\}$. Multiply through by $(s_1 \cdots s_n)^n$,
  $$\left(\frac{as_1 \cdots s_n}{s}\right)^n + \left(\frac{as_1 \cdots s_n}{s}\right)^{n-1} a_1 s_2 \cdots s_n + \cdots + s_1 s_2 \cdots a_n = 0.$$
  As A is integrally closed, $\frac{as_1 \cdots s_n}{s} \in A$ so
  $$\frac{a}{s} = \frac{as_1 \cdots s_n}{s} \cdot \frac{1}{s_1 \cdots s_n} \in A_P$$
  so A_P is integrally closed.

  Let $Q \subseteq A_P$ be a non-zero prime ideal. Then eixsts $Q' \subseteq P$ such that $Q'A_P = Q$. By assumption we must have $Q' = P$ and hence $Q = PA_P$.

□

Definition (fractional ideal)**.** Let A be a domain, $K = \operatorname{Frac} A$. A *fractional ideal* of A is a fg A-submodule of K.

If $I, J \subseteq K$ are fractional ideals then
$$I + J = \{x + y : x \in I, y \in J\}$$
$$IJ = \{xy : x \in I, y \in J\}$$

are also fractional ideals. On the other hand,
$$(I : J) = \{x \in K : xJ \subseteq I\}$$
is an A-submodule of K but is in general not fg.

Lemma 1.10. *Let A be a Noetherian domain, $S \subseteq A$ a multiplicative subset. Then*

1. *if I, J are fractional ideals then $S^{-1}I$ is a fractional ideal of $S^{-1}A$ and*
   $$S^{-1}(I + J) = S^{-1}I + S^{-1}J$$
   $$S^{-1}(IJ) = S^{-1}I \cdot S^{-1}J$$

2. *if I, J are fractional ideals of A and J is non-zero then $(I : J)$ is a fractional ideal of A and*

$$S^{-1}(I : J) = (S^{-1}I : S^{-1}J).$$

Proof.

1. Exercise.
2. If $a \in A - \{0\}$ then

$$(I : (a)) = \{x \in K : x(a) \subseteq I\} = \{x \in K : xa \in I\} = a^{-1}I.$$

In partuclar $(I : (a))$ is fg and hence a fractional ideal.

In general, write $J = (a_1, \ldots, a_n)$ where $a_i \in K^\times$. Then

$$(I : J) = \{x \in K : \text{for all } i, xa_i \in I\} = \bigcap_{i=1}^{n} a_i^{-1}I.$$

In paricular $(I : (a)) \subseteq (I : (a_1))$. Since A is Noetherian, any submodule of $(I : (a_1))$ is fg and hence $(I : J)$ is a fractional ideal.

To show $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$, we have

$$\text{LHS} = S^{-1} \bigcap_{i=1}^{n} a_i^{-1}I$$

$$\text{RHS} = \bigcap_{i=1}^{n} a_i^{-1}S^{-1}I = \bigcap_{i=1}^{n} S^{-1}(a_i^{-1}I)$$

so in fact it's enough to show that if $I, J \subseteq K$ are fractional ideals of A then

$$S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J).$$

We certainly have $S^{-1}(I \cap J) \subseteq (S^{-1}I) \cap (S^{-1}J)$. Suppose $\frac{x}{s} = \frac{y}{t}$ where $x \in I, y \in J, s, t \in S$ then $xt = sy \in I \cap J$ and

$$\frac{x}{s} = \frac{xt}{st} \in S^{-1}(I \cap J).$$

□

Proposition 1.11. *Let A be a Dedekind domain and let* Div A *be the set of non-zero fractional ideals of A. Then* Div A *forms a group under the multiplication of fractional ideals.*

Proof. $A = (1)$ is a multiplicative identity. Must show that for any non-zero fractional ideal I,

$$I(A : I) = A.$$

Observe that if $P \subseteq A$ is a non-zero prime ideal then $IA_P = (\pi_P^i)$ as A_P is a DVR, so $(A_P : IA_P) = (\pi_P^{-i})$ so

$$\text{LHS}_P = IA_P(A_P : IA_P) = A_P = \text{RHS}_P$$

so it is enough to show that if I, J are fractional ideals of A such that $IA_P = JA_P$ for all P then $I = J$. In fact, we are going to show if $IA_P \subseteq JA_P$ then $I \subseteq J$. Suppose $IA_P \subseteq JA_P$ for any non-zero prime ideal $P \subseteq A$. Let $x \in I$. Then $x \in IA_P \subseteq JA_P$ so we can write $x = \frac{y_P}{s_P}$ where $y_P \in J, s_P \in A - P$. Now we use

$$(s_P : P \subseteq A \text{ non-zero prime ideal}) = (1)$$

to write $1 = \sum_P s_P t_P$ where $t_P \in A$ and only finitely many are non-zero. Then

$$x = \sum_P t_P s_P x \in J.$$

□

Observe that for any non-zero P, there is a homomorphism

$$\begin{aligned} \operatorname{Div} A &\to \operatorname{Div} A_P \\ I &\mapsto IA_P \end{aligned}$$

But $\operatorname{Div} A_P \cong \mathbb{Z}$ canonically as every non-zero fractional ideal of A_P has the form (π^i) for some $i \in \mathbb{Z}$.

We can define a homomorphism $v_P : \operatorname{Div} A \to \mathbb{Z}$ by $v_P(I) = v_P(x)$ where $IA_P = (x)$. In particular, for any $x \in K^\times$, $v_P((x)) = v_P(x)$. Note that v_P is surjective since $PA_P = (\pi)$ as $v_P(P) = 1$ for any P. Taking the product over all non-zero prime ideals, we get a homomorphism

$$\prod_P v_P : \operatorname{Div} A \to \prod_P \mathbb{Z}.$$

This is injective as we showed that for any $I, J \in \operatorname{Div} A$, $I = J$ if and only if for all P, $IA_P = JA_P$. Now we characterise the image.

Lemma 1.12. *For any $I \in \operatorname{Div} A$, the set $\{P : v_P(I) \neq 0\}$ is finite.*

In other words, $\prod_P v_P$ takes values in $\bigoplus_P \mathbb{Z} \subseteq \prod_P \mathbb{Z}$.

Proof. Suppose $I = (\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n})$ where $a_i \in A, b_i \in A - \{0\}$. Let $b = b_1 \cdots b_n$. Then $J = bI$ is an ideal of A and

$$v_P(I) = v_P(J) - v_P((b)).$$

So it's enough to prove the lemma in the case $I \subseteq A$ is an ideal.

Let $\alpha \in I - \{0\}$. Then $(\alpha) \subseteq I$ and for any non-zero prime ideal $P \subseteq A$, $v_P(\alpha) \geq v_P(I) \geq 0$ so in fact we can assume $I = (\alpha)$ is principal.

Now we observe that $v_P(\alpha) > 0$ if and only if $\alpha \in PA_P$ if and only if $\alpha \in P$. So it's enough to show that there are only finitely many P's such that $\alpha \in P$.

Suppose for contradiction there are infinitely many $P_1, P_2, \dots$ such that $\alpha \in P_i$. Define $J_i = P_1 \cap \cdots \cap P_i$. Then

$$J_1 \supseteq J_2 \supseteq \cdots \supseteq (\alpha)$$

so

$$\alpha J_1^{-1} \subseteq \alpha J_2^{-1} \subseteq \cdots \subseteq A.$$

This is an ascending chain of ideals of A so there exists $n \geq 1$ such that $\alpha J_n^{-1} = \alpha J_{n+1}^{-1}$. Hence $J_n = J_{n+1}$, i.e.

$$P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n \cap P_{n+1}.$$

Choose $x_i \in P_i - P_{n+1}$ for $i \leq n$. Then

$$x_1 \cdots x_n \in P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n \cap P_{n+1}.$$

Since P_{n+1} is prime, we have $x_i \in P_{n+1}$ for some $i \leq n$. Absurd. □

Proposition 1.13.

1. *$\prod_P v_P : \operatorname{Div} A \to \bigoplus_P \mathbb{Z}$ is an isomorphism.*
2. *For any $I \in \operatorname{Div} A$,*
$$I = \prod_I P^{v_P(I)}$$
so we have unique factorisation of fractional ideals.

Proof.

1. It's enough to show
$$v_Q(P) = \begin{cases} 1 & P = Q \\ 0 & \text{otherwise} \end{cases}$$
as then $(\delta_{PQ})_Q$ are in the ring and they generate $\bigoplus_P \mathbb{Z}$. $v_P(P) = 1$ by definition as PA_P is the maximal ideal of A_P. If $Q \neq P$ then we must show $PA_Q = A_Q$: if $PA_Q \neq A_Q$ then $PA_Q \subseteq QA_Q$ so $P \subseteq Q$. This is impossible as both P and Q are maximal ideals.

2. $I = \prod_P P^{v_P(I)}$ if and only if for all Q,
$$v_Q(I) = v_Q(\prod_P P^{v_P(I)}).$$
As $v_Q(P) = \delta_{PQ}$, RHS equals to $v_Q(I)$.

□

2 Complete DVRs

Definition (inverse system, inverse limit)**.** Suppose given groups A_i and homomorphisms $f_i : A_{i+1} \to A_i$ for all $i \geq 1$

$$A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \cdots$$

we call such a collection an *inverse system*. Its *inverse limit* is

$$\varprojlim_i A_i = \{(a_i) \in \prod_{i=1}^{\infty} A_i : f_i(a_{i+1}) = a_i \text{ for all } i \geq 1\} \subseteq \prod_{i=1}^{\infty} A_i.$$

This is a group. If the A_i's (f_i's respectively) are abelian groups/rings (homomorphisms/ring homomorphisms) then so is $\varprojlim_i A_i$.

Suppose A is a DVR with uniformiser π. Then we can make an inverse system

$$A/(\pi^1) \longleftarrow A/(\pi^2) \longleftarrow A/(\pi^3) \longleftarrow \cdots$$

with maps the natural quotient maps. There's a homomorphism $A \to A/(\pi^i)$, hence $A \to \prod_{i=1}^{\infty} A/(\pi^i)$ which takes values in $\varprojlim_i A/(\pi^i)$.

Definition (complete)**.** We say A is *complete* if the homomorphism

$$A \to \varprojlim_i A/(\pi^i)$$

is an isomorphism.

The kernel of this homomorphism is $\bigcap_{i\geq 1}(\pi^i) = 0$ so A is complete if and only if the map is surjective.

Lemma 2.1. *TFAE:*

1. *A is complete.*
2. *A is complete as a metric space with respect to the metric*

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

3. *K is complete as a metric space with respect to the metric given by the formula.*

Proof. We first explain why d is a metric. d satisfies the ultrametric triangle inequality

$$d(x,y) \leq \max(d(x,y), d(y,z))$$

for all x, y, z. This is because we can assume x, y, z. Then this is equivalent to

$$v(x-z) \geq \min(v(x-y), v(y-z))$$

but LHS is equal to $v((x-y)+(y-z))$. This is the axiom defining a valuation.

- $1 \implies 2$: Let $(a_n)_{n\geq 1}$ be a Cauchy sequence in A, meaning that for all $\varepsilon > 0$, exists N such that for all $n, m \geq N$, $d(a_n, a_m) < \varepsilon$. Equivalently, for all $M > 0$, exists $N(M)$ such that for all $n, m \geq N(M)$,

$$a_n = a_m \pmod{\pi^M}.$$

We can define $b = (b_i)_{i\geq 1} \in \prod_{i=1}^{\infty} A/(\pi^i)$ by

$$b_n = a_{N(n)} \pmod{\pi^n}$$

By definition of Cauchy sequence, $b \in \varprojlim_i A/(\pi^i)$. Since A is a complete DVR, exists $a \in A$ such that $a = a_{N(n)} \pmod{\pi^n}$ for all $n \geq 1$. Hence $v(a - a_{N(n)}) \geq n$, i.e. $d(a, a_{N(n)}) \leq 2^{-n}$ so $\lim_{n\to\infty} a_n = a$.

- $2 \implies 1$: Suppose given $(a_n)_{n\geq 1} \in \varprojlim_n A/(\pi^n)$. Let $\tilde{a}_n \in A$ be any element such that $\tilde{a}_n \pmod{\pi^n} = a_n$. Then for all $m \geq n$, $\tilde{a}_m = \tilde{a}_n \pmod{\pi^n}$ by definition of inverse limit, i.e. $d(\tilde{a}_m, \tilde{a}_n) \leq 2^{-n}$, so $(\tilde{a}_n)_{n\geq 1}$ is a Cauchy sequence in A. So there exists $a \in A$ such that $\tilde{a}_n \to a$ in A, i.e. for all $M \geq 1$ exists $N(M)$ such that for all $n \geq N(M)$, $\tilde{a}_n = a \pmod{\pi^M}$. Hence a is a preimage of $(a_n)_{n\geq 1}$ under the map $A \to \varprojlim_i A/(\pi^i)$.

- $3 \implies 2$: We must show A is a closed subspace of K. Claim that

$$A = \{x \in K : d(0, x) \leq 1\},$$

as $d(0, x) \leq 1$ if and only if $x = 0$ and $v(x) \geq 0$.

- $2 \implies 3$: For any $x, y \in K$,

$$d(\pi x, \pi y) = \frac{1}{2} d(x, y).$$

Let $(a_n)_{n\geq 1}$ be a Cauchy sequence in K. Then there exists $N \geq 1$ such that $\pi^N a_n \in A$ for all $n \geq 1$: there exists M such that for all $n, m \geq M$, $d(a_n, a_m) \leq 1$. Equivalently, $a_n - a_m \in A$ so it's enough to choose N so that $\pi^N a_n \in A$ for $1 \leq n \leq M$. $(\pi^N a_n)_{n\geq 1}$ is a Cauchy sequence in A so exists $a \in A$ such that $d(\pi^N a_n, a) \to 0$ as $n \to \infty$. Thus $a_n \to \pi^{-N} a$ in K.

□

Exercise. Show that A is also open in K. Show futhermore that K is totally disconnected.

Remark. When we speak of topology on K or convergence in K we always mean with respect to the metric d.

Proposition 2.2. *Let A be a DVR, $\pi \in A$ a uniformiser. Then*

1. *$A \to \hat{A} = \varprojlim_i A/(\pi^i)$ is injective, $\hat{A}$ is a complete DVR and π is a uniformiser of $\hat{A}$.*
2. *For all $i \geq 1$, the map $A/\pi^i A \to \hat{A}/\pi^i \hat{A}$ is an isomorphism.*
3. *Let $X \subseteq A$ be a subset of representatives for the residue classes of*

> *$A/(\pi)$, with $0 \in X$. Then for all $a \in \hat{A}$, there exists a unique expression*
>
> $$a = \sum_{i=0}^{\infty} a_i \pi^i$$
>
> *with $a_i \in X$ for all $i \geq 0$. This is the* π-adic expansion *of a.*

Proof. We first observe that for all $a \in A/(\pi^i)$, there exist unique $a_0, \ldots, a_{i-1} \in X$ such that

$$a = a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} \pmod{\pi^i}.$$

Induction on i: for $i = 1$ this is the definition of X. To show this for $i+1$, let $a \in A/(\pi^{i+1})$. Then $a \pmod{\pi^i} \in A/(\pi^i)$ so by induction there exist unqiue $a_0, \ldots, a_{i-1}$ such that

$$a - (a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1}) \in \pi^i A/\pi^{i+1}A.$$

The map

$$\begin{aligned} X &\to A/(\pi) \to \pi^i A/\pi^{i+1}A \\ x &\mapsto x \pmod{\pi} \\ y \pmod{\pi} &\mapsto \pi^i y \pmod{\pi^{i+1}} \end{aligned}$$

is bijective. Hence there eixsts unique $a_i \in X$ such that

$$a - (a_0 + \cdots + a_i\pi^i) = 0 \pmod{\pi^{i+1}}.$$

Note that we have a commutative diagram

$$\begin{array}{ccc} A/(\pi^{i+1}) & \longleftrightarrow & \{a_0 + a_1\pi + \cdots + a_i\pi^i : a_j \in X\} \\ \downarrow & & \downarrow \\ A/(\pi^i) & \longleftrightarrow & \{a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} : a_j \in X\} \end{array}$$

where the map on the right is to omit the π^i term. Thus there is a bijection between $\hat{A}$ and the set of formal sums $\sum_{i=0}^{\infty} a_i\pi^i$ where $a_i \in X$ for all $i \geq 0$. Note that we can't yet think of it as an infinite sum since we haven't yet shown $\hat{A}$ is complete. For any i, we set

$$x_i = a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} \pmod{\pi^i} \in A/(\pi^i),$$

then $\sum_{i=0}^{\infty} a_i\pi^i$ is simply a short hand for the element $x = (x_i)_{i\geq 1} \in \varprojlim_i A/(\pi^i) = \hat{A}$.

Let's now show $\hat{A}$ is a DVR. We know $A \to \hat{A}$ is injective. We'll show each non-zero element $x \in \hat{A}$ has a unique expression $x = \pi^n u$ where $n \geq 0, u \in \hat{A}^\times$. Let's write $x = a_0 + a_1\pi + \cdots$ and say

$$a_0 = a_1 = \cdots = a_{n-1} = 0, a_n \neq 0.$$

Then $x = \pi^n y$ where $y = a_n + a_{n+1}\pi + \cdots$. Note if $\alpha \in X - \{0\}$ then $\alpha \pmod{\pi}$ is non-zero and hence $\alpha \in A^\times$. Thus $y = a_n(1 - \pi b)$ where

$$b = 1 - \pi a_n^{-1}a_{n+1} - \pi^2 a_n^{-1}a_{n+2} + \cdots \in \hat{A}.$$

It's enough to show $1 - \pi b \in \hat{A}^\times$. An inverse is given by

$$1 + \pi b + \pi^2 b^2 + \cdots \in \hat{A}.$$

This shows $\hat{A}$ is a DVR with uniformiser π.

The map $A/\pi^i A \to \hat{A}/\pi^i \hat{A}$ is bijective as elements of both sides can be uniquely represented by elements of the form

$$a_0 + a_1\pi + \cdots + a_{i-1}\pi^{i-1} \pmod{\pi^i}$$

where $a_i \in X$. It follows that $\hat{A}$ is complete, as the map

$$\hat{A} \to \varprojlim_i \hat{A}/\pi^i \hat{A} \cong \varprojlim_i A/\pi^i A$$

is an isomorphism by the definition of $\hat{A}$. □

Remark. If A is complete then $\hat{A} \cong A$.

Observe that if $K = \operatorname{Frac} A, \hat{K} = \operatorname{Frac} \hat{A}$ then the valuation $v : K^\times \to \mathbb{Z}$ extends to a valuation $v : \hat{K}^\times \to \mathbb{Z}$ such that $\hat{A} = \{x \in \hat{K} : v(x) \geq 0\}$.

$$\begin{array}{ccc} A & \hookrightarrow & K \\ \downarrow & & \downarrow \\ \hat{A} & \hookrightarrow & \hat{K} \end{array}$$

An element of $\hat{A}$ admits a unique π-adic expansion $\sum_{i=0}^{\infty} a_i \pi^i$ where a_i lie in a fixed set representatives in A for $A/(\pi)$, and the series $\sum_{i=0}^{\infty} a_i \pi^i$ is a convergent infinite sum in $\hat{A}$.

Definition (p-adic integer)**.** Let p be a prime. Then we define the *p-adic integers* and *p-adic rational numbers* to be

$$\mathbb{Z}_p = \hat{\mathbb{Z}}_{(p)}$$
$$\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$$

respectively.

$p \in \mathbb{Z}_p$ is a uniformiser and $\mathbb{Z}_p/(p) \cong \mathbb{Z}_{(p)}/(p)$. To compute the residue field of $\mathbb{Z}_{(p)}$, we use the exact sequence

$$0 \longrightarrow p\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

of $\mathbb{Z}$-modules. It remains exact after localisation so

$$0 \longrightarrow p\mathbb{Z}_{(p)} \longrightarrow \mathbb{Z}_{(p)} \longrightarrow (\mathbb{Z} - (p))^{-1}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

is still exact so

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong (\mathbb{Z} - (p))^{-1}\mathbb{Z}/p\mathbb{Z}.$$

In fact $\mathbb{Z}/p\mathbb{Z} \to (\mathbb{Z} - (p))^{-1}\mathbb{Z}/p\mathbb{Z}$ is an isomorphism as every element of $\mathbb{Z} - (p)$ has image in $\mathbb{Z}/p\mathbb{Z}$ contained in $(\mathbb{Z}/p\mathbb{Z})^\times$.

As a consequence, we have $\mathbb{Z}_p/(p) \cong \mathbb{Z}/p\mathbb{Z}$ so we can choose the set of representatives to be $\{0, 1, \ldots, p-1\}$. It follows that each element of $\mathbb{Z}_p$ has a unique expression as $\sum_{i=0}^{\infty} a_i p^i$ and each element of $\mathbb{Q}_p$ has a unique expression $\sum_{i \in \mathbb{Z}} a_i p^i$ where $a_i \in \{0, \ldots, p_1\}$ and the set $\{i < 0 : a_i \neq 0\}$ is finite.

Example. $-1 \in \mathbb{Z} \subseteq \mathbb{Z}_2$ has

$$-1 = \frac{1}{1-2} = 1 + 2 + 2^2 + \cdots$$

What is $\mathbb{Q}_p$ like? It is a mixture of $\mathbb{R}$ and $\mathbb{F}_p$ and has features of both analytic ($\mathbb{R}$) and algebraic (number fields) objects.

Lemma 2.3 (Hensel's lemma)**.** *Let A be a complete DVR. Let $f(x) \in A[x]$ be monic. Suppose given $\alpha \in A$ such that $v(f(\alpha)) > 2v(f'(\alpha))$. Then exists a unique $a \in A$ such that $f(a) = 0$ and $v(a - \alpha) > v(f'(\alpha))$.*

Corollary 2.4. *Let A be a complete DVR and $f(x) \in A[x]$ a monic polnomial. Let $k = A/(\pi)$ and $\overline{f}(x) = f(x) \pmod{\pi} \in k[x]$. Suppose there exists $\overline{\alpha} \in k$ a simple root of $\overline{f}(x)$, then exists a unique $a \in A$ such that $f(a) = 0$ and $a = \overline{\alpha} \pmod{\pi}$.*

Proof. Let $\alpha \in A$ be a lift of $\overline{\alpha}$. Then $\overline{f}'(\overline{\alpha}) \neq 0$ implies that $f'(\alpha) \in A^\times$ so $v(f'(\alpha)) = 0$. Then apply the lemma. □

Proof of Hensel's lemma. We first show existence of a by Newton's method. Define

$$a_1 = \alpha, \quad a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

We show the following claims by induction on $n \geq 1$:

1. $a_n \in A$, or equivalently $v(a_n) \geq 0$.
2. $v(f'(a_n)) = v(f'(a_1))$.
3. $v(f(a_n)) \geq 2v(f'(a_n)) + 2^{n-1}v(f(a_1)/f'(a_1)^2)$.

For $n = 1$,

1. $a_n = \alpha \in A$ by hypothesis.
2. Tautological.
3. $v(f(a_1)) \geq 2v(f'(a_1)) + v(f(a_1)/f'(a_1)^2) = v(f(a_1))$.

Suppose the three statements hold for $1, 2, \ldots, n$. We will show they hold for $n + 1$.

1. By definition $a_{n+1} = a_n - f(a_n)/f'(a_n)$ so $a_{n+1} \in A$ if and only if $v(f(a_n)/f'(a_n)) \geq 0$. But 3 says
$$v(f(a_n)/f'(a_n)) \geq v(f'(a_n)) + 2^{n-1}v(f(a_1)/f'(a_1)^2) \geq 0.$$
2. Enough to show $v(f'(a_{n+1})) = v(f'(a_n))$. Easy to see that $f'(a_{n+1}) - f'(a_n)$ is divisible by $-a_{n+1}+a_n = f(a_n)/f'(a_n)$ so we'll have $v(f'(a_{n+1})) = v(f'(a_n))$ if
$$v(f(a_n)/f'(a_n)) > v(f'(a_n)),$$
i.e. $v(f(a_n)/f'(a_n)^2) > 0$. But
$$v(f(a_n)/f'(a_n)^2) \geq 2^{n-1}v(f(a_1)/f'(a_1)^2) > 0.$$

3. Suppose $f(x) = \sum_{i=0}^{m} a_i x^i$ where $a_i \in A$. Then we use Taylor expansion with a small tweak

$$\begin{aligned} f(X+Y) &= \sum_{i=0}^{m} a_i (X+Y)^i \\ &= \sum_{i=0}^{m} a_i (X^i + iX^{i-1}Y + Y^2 g_i(X,Y)) \quad g_i(X,Y) \in \mathbb{Z}[X,Y] \\ &= f(X) + f'(X)Y + Y^2 g(X,Y) \quad g(X,Y) \in A[X,Y] \end{aligned}$$

hence

$$\begin{aligned} f(a_{n+1}) &= f(a_n - f(a_n)/f'(a_n)) \\ &= f(a_n) - f'(a_n)f(a_n)/f'(a_n) \\ &\quad + (f(a_n)/f'(a_n))^2 \underbrace{g(a_n, f(a_n)/f'(a_n))}_{\in A} \end{aligned}$$

so

$$\begin{aligned} v(f(a_{n+1})) &\geq 2v(f(a_n)) - 2v(f'(a_n)) \\ &\geq 2(2v(f'(a_n)) + 2^{n-1}v(f(a_1)/f'(a_1)^2)) - 2v(f'(a_n)) \\ &= 2v(f'(a_n)) + 2^n v(f(a_1)/f'(a_1)^2) \end{aligned}$$

We've also shown $(a_n)_{n\geq 1}$ is a Cauchy sequence as

$$v(a_{n+1} - a_n) = v(f(a_n)/f'(a_n)) \to \infty$$

as $n \to \infty$ so there is a limit $a \in A$. We have $f(a) = \lim_{n\to\infty} f(a_n) = 0$ so a is a root.

For uniqueness, we need to show if $a + h \in A$ is another root such that $v(a + h - \alpha) > v(f'(\alpha))$ then $h = 0$. Since $v(a - \alpha) > v(f'(\alpha))$, we must have $v(h) > v(f'(\alpha))$. Using Taylor expansion, we find

$$0 = f(a+h) = f(a) + hf'(a) + h^2 g(a,h)$$

and hence $hf'(\alpha) = -h^2 g(a,h)$. If $h \neq 0$ then $f'(\alpha) = -hg(a,h)$. Hence

$$v(f'(\alpha)) \geq v(h) > v(f'(\alpha)),$$

absurd. □

Example. Which elements in $\mathbb{Q}_p^\times$ are squares? Any element of $\mathbb{Q}_p^\times$ admits a unqiue expression $x = p^n u$ where $n \in \mathbb{Z}, u \in \mathbb{Z}_p^\times$. Equivalently, there is an isomorphism

$$\begin{aligned} \mathbb{Q}_p^\times &\cong \mathbb{Z} \times \mathbb{Z}_p^\times \\ x &\mapsto (n, u) \end{aligned}$$

It's enough to determine when $u \in \mathbb{Z}_p^\times$ is a square. Equivalently, when the polynomial $f(x) = x^2 - u$ has a root in $\mathbb{Z}_p$. There is a simple necessary condition from arithmetics: there is a surjective homomorphism $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times, x \mapsto \overline{x}$

$(\mathrm{mod}\ p)$ and if $u \in (\mathbb{Z}_p^\times)^2$ then $\overline{u} \in (\mathbb{F}_p^\times)^2$. Let's check if it is sufficient: if $\overline{u} \in (\mathbb{F}_p^\times)^2$ and let $v \in \mathbb{Z}_p^\times$ satisfy $\overline{v}^2 = \overline{u}$. Then $\overline{f}(\overline{v}) = 0$ so we are in the position to use Hensel's lemma. Note $f'(v) = 2v$ and $v(f'(v)) = v(2)$. If p is odd then $f'(v)$ is a unit, so by the corollary there exists a unique $w \in \mathbb{Z}_p^\times$ such that $w^2 = u$ and $\overline{w} = \overline{v}$.

If $p = 2$ then we have $v(f(v)) \geq 1, v(f'(v)) = 1$ so we can't conclude anything yet. Note for any $n \geq 1$ there is a homomorphism $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ so if u is a square, $u \pmod{p^n}$ is also a square for any $n \geq 1$. For $n = 3$ we have a map

$$\mathbb{Z}_2^\times \to (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

hence if $u \in (\mathbb{Z}_2^\times)^2$ then $u = 1 \pmod 8$. Conversely, if $u = 1 \pmod 8$ then $f(1) = 1 - u = 0 \pmod 8$, i.e. $v(f(1)) \geq 3$, and $f'(1) = 2$ so $v(f'(1)) = 1$. In this case Hensel's lemma does apply and u is indeed a square.

Proposition 2.5.

1. *If p is odd then $u \in \mathbb{Z}_p^\times$ is a square if and only if $u \pmod p \in \mathbb{F}_p^\times$ is a square.*
2. *If $p = 2$ then $u \in \mathbb{Z}_2^\times$ is a square if and only if $u = 1 \pmod 8$, or equivalently $u \pmod 8 \in (\mathbb{Z}/8\mathbb{Z})^\times$ is a square.*

In the example we used the surjective homomorphism

$$\begin{aligned} \mathbb{Z}_p^\times &\to \mathbb{F}_p^\times \\ \sum_{i=0}^{\infty} a_i p^i &\mapsto a_0 \pmod p \end{aligned}$$

In fact, this homomoprhism has a unique splitting, i.e. exists a unique homomorphism $\tau : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ such that for all $\overline{\alpha} \in \mathbb{F}_p^\times$, $\tau(\overline{\alpha}) \pmod p = \overline{\alpha}$. This τ is called the *Teichmüller lift* and is constructed as follow: let $f(x) = x^p - x$. Then for all $\overline{\alpha} \in \mathbb{F}_p, \overline{f}(\overline{\alpha}) = 0$, and $\overline{f}'(x) = px^{p-1} - 1 \pmod p = -1$ so never vanishes. So Hensel's lemma says that for all $\overline{\alpha} \in \mathbb{F}_p$, exists a unique $\alpha \in \mathbb{Z}_p$ such that $\alpha^p = \alpha$ and $\alpha \pmod{p\mathbb{Z}_p} = \overline{\alpha}$. Define $\tau(\overline{\alpha}) = \alpha$.

If $\overline{\alpha}, \overline{\beta} \in \mathbb{F}_p^\times$ then

$$(\tau(\overline{\alpha})\tau(\overline{\beta}))^p = \tau(\overline{\alpha})^p \tau(\overline{\beta})^p = \tau(\overline{\alpha})\tau(\overline{\beta})$$

and $\tau(\overline{\alpha})\tau(\overline{\beta}) \pmod{p\mathbb{Z}_p} = \overline{\alpha}\overline{\beta}$. Uniqueness part of Hansel's lemma thus says that $\tau(\overline{\alpha}\overline{\beta}) = \tau(\overline{\alpha})\tau(\overline{\beta})$, i.e. τ is a homomorphism.

τ is the unique splitting: if $\sigma : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ is another splitting then for all $\overline{\alpha} \in \mathbb{F}_p^\times$,

$$\sigma(\overline{\alpha})^p = \sigma(\overline{\alpha}^p) = \sigma(\overline{\alpha})$$

so $f(\sigma(\overline{\alpha})) = 0$. Uniqueness again says that $\sigma = \tau$.

As a consequence

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times \cong \mathbb{Z} \times (1 + p\mathbb{Z}_p) \times \mathbb{F}_p^\times$$

corresponding to the expression $p^n \cdot u \cdot \tau(\overline{\alpha})$. There is an isomorphism

$$1 + p\mathbb{Z}_p \cong \varprojlim_i \underbrace{\ker((\mathbb{Z}/p^i\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times)}_{p\text{-power order}}$$

so for any $n \in \mathbb{N}, (n,p) = 1$, the map

$$\begin{aligned} 1 + p\mathbb{Z}_p &\to 1 + p\mathbb{Z}_p \\ x &\mapsto x^n \end{aligned}$$

is a bijective group homomorphism. Hence there is an isomorphism

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^n \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^n.$$

Suppose q is a prime such that $p = 1 \pmod q$. Then $\mathbb{Q}_p^\times$ contains a primitive qth root of unit ζ_q. This is because $\zeta_q \in \mathbb{Q}_p^\times$ if and only if $\mathbb{Q}_p^\times$ contains an element of order q. But $\mathbb{F}_p^\times$ is cyclic of order $p-1$ so this is true.

Lemma 2.6. *Under this assumption, $\mathbb{Q}_p$ has exactly $q+1$ isomorphism classes of Galois extensions of degree q.*

Proof. Since $\zeta_q \in \mathbb{Q}_p^\times$, Kummer theory tells us that such extensions correspond to subgroups of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^q$ of order q, where an element z of the subgroup corresponds to the extension $\mathbb{Q}_p(\sqrt[q]{z})$. We've computed $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^q \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, which has $q+1$ subgroups of order q. □

Before the end of the chapter, we briefly indicate where we're heading: we define K_Q to be the fraction field associated to the completion of $\mathcal{O}_K$ localised at Q. Then we are going to consider its "rings of integers" $\mathcal{O}_{K_Q}$ so we have the following picture:

$$\begin{array}{ccccc} K & \mathcal{O}_K & Q & \mathcal{O}_{K_Q} & K_Q \\ | & | & | & | & | \\ \mathbb{Q} & \mathbb{Z} & p\mathbb{Z} & \mathbb{Z}_p & \mathbb{Q}_p \end{array}$$

If $K/\mathbb{Q}$ is Galois then so is $K_Q/\mathbb{Q}_p$ and $\mathrm{Gal}(K_Q/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q})$, and we are going to study $\mathrm{Gal}(K_Q/\mathbb{Q}_p)$ in detail.

3 Extensions of Dedekind domains

Let A be a Dedekind domain and $K = \operatorname{Frac} A$. Let E/K be a finite separable extension.

Definition (integral element)**.** We say $\gamma \in E$ is *integral* over A if exists $n \geq 1$, $a_1, \ldots, a_n \in A$ such that

$$\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0.$$

Lemma 3.1. *TFAE:*

1. *γ is integral over A.*
2. *$A[\gamma]$ is a finitely generated A-module.*
3. *there exists a non-zero $A[\gamma]$-submodule $M \leq E$ which is a finitely generated A-module.*

Proof.

- 1 $\implies$ 2: If $\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0$ then $A[\gamma] = A + A\gamma + \cdots + A\gamma^{n-1}$.
- 2 $\implies$ 1: A is Noetherian and $A[\gamma]$ is a finitely generated A-module so

  $$A \subseteq A + A[\gamma] \subseteq A + A\gamma + A[\gamma^2] \subseteq \cdots$$

  is eventually stationary, so exists $n \geq 1$ such that $\gamma^n \in A + A\gamma + \cdots + A\gamma^{n-1}$.
- 2 $\implies$ 3: $M = A[\gamma]$.
- 3 $\implies$ 2: Since M is finitely generated and A is Noetherian, $\operatorname{End}_A(M)$ is a finitely generated A-module. Since M is non-zero, $A[\gamma] \to \operatorname{End}_A(M), x \mapsto (m \mapsto xm)$ is an injective homomorphism of A-modules. Hence $A[\gamma]$ is a finitely generated A-module.

□

Let $B = \{\gamma \in E : \gamma \text{ integral over } A\}$, the integral closure of A in E.

Lemma 3.2. *B is a subring of E and B is integrally closed in E.*

Proof. Suppose $b_1, \ldots, b_m \in B$. Then $A[b_1, \ldots, b_m]$ is a finitely generated A-module: if we have relations

$$b_i^{n_i} + a_{1,i}b_i^{n_i-1} + \cdots + a_{n_i,i} = 0$$

for all i then $\{\prod_{i=1}^m b_i^{m_i} : 0 \leq m_i < n_i\}$ is a generating set for $A[b_1, \ldots, b_m]$.

This also shows that B is a ring: if $b_1, b_2 \in B$ then $A[b_1, b_2] \subseteq E$ is a fg A-module stable under multiplication by $b_1 + b_2$ and b_1b_2. So part 3 of the lemma implies that $b_1 + b_2, b_1b_2 \in B$.

Now suppose $\gamma \in E$ and exists $n \geq 1$, $b_1, \ldots, b_n \in B$ such that

$$\gamma^n + b_1\gamma^{n-1} + \cdots + b_n = 0.$$

We must show $\gamma \in B$. This relation shows $A[b_1, \ldots, b_n][\gamma] = A[b_1, \ldots, b_n, \gamma]$ is a fg $A[b_1, \ldots, b_n]$-module. But $A[b_1, \cdots, b_n]$ is a fg A-module, so $A[b_1, \ldots, b_m, \gamma]$ is a fg A-module: if $\{x_i\}$ generates $A[b_1, \ldots, b_m, \gamma]$ as an $A[b_1, \ldots, b_m]$-module and $\{y_j\}$ generates $A[b_1, \ldots, b_m]$ as an A-module then $\{x_i y_j\}$ generates $A[b_1, \ldots, b_n, \gamma]$ as an A-module. In particular γ is integral over A so $\gamma \in B$. □

Lemma 3.3. *Let $T : E \times E \to K$ be the symmetric K-bilinear form defined by $T(x, y) = \mathrm{tr}_{E/K}(xy)$. Then T is nondegenerate.*

Proof. This is a consequence of the assumption that E/K is separable. Let L/K be the Galois closure of E/K. Let $\sigma_1, \ldots, \sigma_n : E \to L$ be the distinct K-embeddings, where $n = [E : K]$. Then for all $x \in E$

$$\mathrm{tr}_{E/K}(x) = \sigma_1(x) + \cdots + \sigma_n(x).$$

Recall from Galois theory that $\sigma_1, \ldots, \sigma_n$ are linearly independent (over K) as homomorphisms $\sigma_i : E^\times \to L^\times$, so there exists $x \in E^\times$ such that $\sigma_1(x) + \cdots + \sigma_n(x) \neq 0$ and therefore $\mathrm{tr}_{E/K}(x) \neq 0$. Then for all $y \in E^\times$,

$$T(xy^{-1}, y) = \mathrm{tr}_{E/K}(x) \neq 0,$$

i.e. $\ker T = 0$ and T is nondegenerate. □

Remark. If $x \in B$ then $\mathrm{tr}_{E/K}(x) \in A$: $\sigma_i(x) \in L$ is integral over A and hence $\sigma_1(x) + \cdots + \sigma_n(x)$ is an element of L which is in K and integral over A. A being integrally closed implies that $\mathrm{tr}_{E/K}(x) \in A$.

Observe that if $S \subseteq A$ is multiplicatively closed and $0 \notin S$ then $S^{-1}A$ is a Dedekind domain with field of fractions K. Moreover, the integral closure of $S^{-1}A$ in E is $S^{-1}B$. This is because $S^{-1}B$ is contained in the integral closure of $S^{-1}A$ in E. Conversely, if $\gamma \in E$ satisfies

$$\gamma^n + \frac{a_1}{s_1}\gamma^{n-1} + \cdots + \frac{a_n}{s_n} = 0$$

where $a_i \in A, s_i \in S$ then

$$(\gamma s_1 \cdots s_n)^n + \frac{a_1}{s_1}(s_1 \cdots s_n)^{n-1}(\gamma s_1 \cdots s_n)^{n-1} + \cdots = 0$$

and hence $\gamma s_1 \cdots s_n \in B$ so $\gamma \in S^{-1}B$.

For example $(A - \{0\})^{-1}A = K$ so $(A - \{0\})^{-1}B = E$. In particular B always span E as a K-vector space and $\mathrm{Frac}\, B = E$.

Proposition 3.4. *B is fg as A-module and is a Dedekind domain.*

Proof. Let $e_1, \ldots, e_n$ be basis of E as K-vector space. We assume that in fact $e_1, \ldots, e_n \in B$. Recall that there is a K-bilinear form $T : E \times E \to K, (x, y) \mapsto \mathrm{tr}_{E/K}(xy)$ and is nondegenerate as E/K is separable. Moreover if

$x \in B$ then $\mathrm{tr}_{E/K}(x) \in A$. Let $f_1, \ldots, f_n$ be the dual basis of $e_1, \ldots, e_n$ with respect to T, i.e. for all i, j, $T(e_i, f_j) = \mathrm{tr}_{E/K}(e_i f_j) = \delta_{ij}$. If $x \in B$ we can write $x = \sum_{j=1}^{n} a_j f_j$ where $a_j \in K$, and

$$\mathrm{tr}_{E/K}(xe_i) = T(x, e_i) = \sum_{j=1}^{n} a_j T(f_j, e_i) = a_i \in A.$$

As x is arbitrary, this shows $B \subseteq \sum_{j=1}^{n} Af_j$. As A is Noetherian, B is fg as an A-module. Hence B is fg as an A-algebra, so by Hilbert basis theorem B is Noetherian as a ring.

To show B is a Dedekind domain, it remains to show that every non-zero prime ideal $Q \subseteq B$ is maximal or equivalently, B/Q is a field. To show this let $P = A \cap Q$. Then P is prime. It is also non-zero: if $\gamma \in Q - \{0\}$ then it satisfies an equation

$$\gamma^m + a_1\gamma^{m-1} + \cdots + a_m = 0$$

where $a_i \in A$. We can assume $a_m \neq 0$ (otherwise divide by γ). Then

$$a_m = -(\gamma^m + a_1\gamma^{m-1} + \cdots + a_{m-1}\gamma) \in A \cap Q - \{0\}.$$

$$\begin{array}{ccccc} E & \text{——} & B & \text{——} & Q \\ | & & | & & | \\ K & \text{——} & A & \text{——} & P \end{array}$$

We have an injective ring homomorphism $A/P \to B/Q$ where A/P is a field, B/Q is a domain and B/Q is finite dimensional as an A/P-vector space (as B is fg as A-module). It follows that B/Q is a field: let $\alpha \in B/Q - \{0\}$ and consider the map $M_\alpha : B/Q \to B/Q, \beta \mapsto \beta\alpha$. M_α is a linear map of A/P-vector spaces and is injective because $A \neq 0$ and B/Q is a domain. Since B/Q has finite dimension, M_α must be surjective. Hence exists $\alpha' \in B/Q$ such that $M_\alpha(\alpha') = \alpha\alpha' = 1$. □

We showed in the proof that if $Q \subseteq B$ is a non-zero prime ideal then $P = A \cap Q \subseteq A$ is a non-zero prime ideal. In this case, we say Q *lies above* P. We have Q lies above P if and only if $Q \supseteq PB$ if and only if $v_Q(PB) > 0$ where $v_Q : E^\times \to \mathbb{Z}$ is the valuation corresponding to Q. This is left as an exercise.

Definition (residue degree, ramification index)**.** If Q lies above P, we define the *residue degree* of Q over P to be

$$f_{Q/P} = [B/Q : A/P]$$

and the *ramification index* to be

$$e_{Q/P} = v_Q(PB).$$

Note that they are both integers greater than 0.

Proposition 3.5. *Let $P \subseteq A$ be a non-zero prime ideal. Then*

$$\sum_{v_Q(PB)>0} e_{Q/P} f_{Q/P} = [E : K].$$

Proof. Let $S = A - P$. Then $S^{-1}B$ is the integral closure of $S^{-1}A$. In addition localisation preserves residue degree and ramification index: we have

$$e_{S^{-1}Q/S^{-1}P} = e_{Q/P}, \quad f_{S^{-1}Q/S^{-1}P} = f_{Q/P}.$$

The first is because by unique factorisation,

$$PB = \prod_Q Q^{e_{Q/P}}$$
$$S^{-1}PB = \prod_Q (S^{-1}Q)^{e_{Q/P}}$$

so by prime ideal correspondence for localisation we must have equality. The second is because the maps $A/P \to S^{-1}A/S^{-1}P, B/Q \to S^{-1}B/S^{-1}Q$ are both isomophisms. Therefore we can replace A by $S^{-1}A$ and assume that A is a DVR, in particular a PID. Then B is a fg A-module which is torsion free, so we can use the classification of fg modules over a PID to conclude that as an A-module, $B \cong A^n$ for some $n \in \mathbb{N}$. Then

$$E = (A - \{0\})^{-1}B \cong (A - \{0\})^{-1}A^n \cong K^n$$

and hence $n = [E : K]$.

Reducing modulo P, we have an isomorphism $B/PB \cong (A/P)^n$ of A/P-vector spaces. By Chinese remainder theorem we have an isomorphism

$$B/PB \cong \prod_{Q:v_Q(PB)>0} B/Q^{v_Q(PB)}.$$

Hence

$$[E : K] = n = \sum_{Q:v_Q(PB)>0} \dim_{A/P} B/Q^{v_Q(PB)}.$$

We have a chain of inclusions

$$B \supseteq Q \supseteq Q^2 \supseteq \cdots \supseteq Q^{v_Q(PB)}$$

so

$$\dim_{A/P} B/Q^{v_Q(B)} = \sum_{i=0}^{e_{Q/P}-1} \dim_{A/P} Q^i/Q^{i+1}.$$

For any $i \geq 0$, Q^i/Q^{i+1} has dimension 1 as a B/Q-vector space (as $Q^i/Q^{i+1} \to Q^iB_Q/Q^{i+1}B_Q$ is an isomorphism, so can reduce to the case of B_Q). Therefore

$$\dim_{A/P} Q^i/Q^{i+1} = [B/Q : A/P] \dim_{B/Q} Q^i/Q^{i+1} = f_{Q/P}.$$

We thus get

$$[E : K] = n = \sum_{Q:v_Q(PB)>0} \sum_{i=0}^{e_{Q/P}-1} f_{Q/P} = \sum_Q e_{Q/P} f_{Q/P}.$$

□

$$\begin{array}{ccccc} E & \text{——} & B & \text{——} & \{Q_1, \ldots, Q_r\} \\ | & & | & & | \\ K & \text{——} & A & \text{————} & P \end{array}$$

Let $e_i = e_{Q_i/P}, f_i = f_{Q_i/P}$ and so $\sum_{i=1}^{r} e_i f_i = [E : K]$.

Definition (unramified ideal, split ideal)**.** If for all $1 \leq i \leq r, e_i = 1$, B/Q_i is a separable extension of A/P we say P is *unramified* in B (or E).

If for all $1 \leq i \leq r, e_i = f_i = 1$, we say P *splits completely* in B (or E).

Notation. If P is a prime ideal in a Dedekind domain then we write k_P for the quotient field by P. For example $k_Q = B/Q, k_P = A/P$.

Example. If $E/\mathbb{Q}$ is a number field (i.e. finite extension), we write $\mathcal{O}_E$ for the integral closure of $\mathbb{Z}$ in K. If $E = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}, d \neq 0, 1$ is a squarefree integer, then we can show

$$\mathcal{O}_E = \begin{cases} \mathbb{Z}[\sqrt{d}] & d = 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d = 1 \pmod 4 \end{cases}$$

Note $\sqrt{d}$ satisfies $X^2 - d = 0$ and $\frac{1+\sqrt{d}}{2}$ satisfied $X^2 - X + \frac{1-d}{4}$. This shows the given rings are at least subrings of $\mathcal{O}_E$. To show there's nothing else, let $\alpha \in \mathcal{O}_E$. We can write $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Q}$. Note $\mathrm{Gal}(E/\mathbb{Q})$ acts on E and preserves $\mathcal{O}_E$: if $\alpha \in \mathcal{O}_E$ so

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$$

for $a_i \in \mathbb{Z}$, and $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ then

$$\sigma(\alpha)^n + a_1\sigma(\alpha)^{n-1} + \cdots + a_n = 0$$

so $\sigma(\alpha) \in \mathcal{O}_E$. Hence $\overline{\alpha} = a - b\sqrt{d} \in \mathcal{O}_E$ so

$$\alpha + \overline{\alpha} = 2a \in \mathcal{O}_E \cap \mathbb{Q} = \mathbb{Z}$$
$$\alpha\overline{\alpha} = a^2 - b^2 d \in \mathbb{Z}$$

we can make substitution $a = \frac{u}{2}$ where $u \in \mathbb{Z}$ to get $u^2 - 4b^2 d \in 4\mathbb{Z}$ so $4b^2 d \in \mathbb{Z}$. Let p be an odd prime. Then

$$v_p(4b^2 d) = v_p(d) + 2v_p(b) \geq 0.$$

d is squarefree so $v_p(d) \in \{0, 1\}$. Hence $v_p(b) \geq 0$. Similarly

$$v_2(4b^2 d) = v_2(d) + 2(v_2(b) + 1) \geq 0$$

so $v_2(b) \geq -d$. So we can write $b = \frac{v}{2}$ for some $v \in \mathbb{Z}$. Then

$$4\alpha\overline{\alpha} = u^2 - dv^2 \in 4\mathbb{Z},$$

i.e. $u^2 = dv^2 \pmod 4$. If $d = 2, 3 \pmod 4$ this forces both $u, v \in 2\mathbb{Z}$ so have $a, b \in \mathbb{Z}$, and therefore $\alpha \in \mathbb{Z}[\sqrt{d}]$. If $d = 1 \pmod 4$ we get $u^2 = v^2 \pmod 4$ so $u = v \pmod 2$. This shows $\mathcal{O}_E = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ in this case.

Next we show how to factorise $p\mathcal{O}_E$ when p is a prime number. First suppose p is odd. Then it's enough to factorise $p\mathcal{O}_E[\frac{1}{2}] = p\mathbb{Z}[\frac{1}{2}, \sqrt{d}]$. We compute

$$\frac{\mathcal{O}_E[\frac{1}{2}]}{p\mathcal{O}_E[\frac{1}{2}]} = \frac{\mathbb{Z}[\frac{1}{2}, \sqrt{d}]}{p\mathbb{Z}[\frac{1}{2}, \sqrt{d}]} = \frac{\mathbb{Z}[\frac{1}{2}, X]}{(X^2 - d, p)} = \frac{\mathbb{F}_p[X]}{(X^2 - d)} = \begin{cases} \mathbb{F}_p \times \mathbb{F}_p & \left(\frac{d}{p}\right) = 1 \\ \mathbb{F}_{p^2} & \left(\frac{d}{p}\right) = -1 \\ \mathbb{F}_p[X]/(X^2) & p \mid d \end{cases}$$

Now suppose $p\mathcal{O}_E = \prod_Q Q^{e_{Q/P}}$, then by Chinese remainder theorem

$$\mathcal{O}_E/p\mathcal{O}_E \cong \prod_Q (\mathcal{O}_E/Q^{e_{Q/P}}).$$

There are three possible isomorphism classes of this quotient, corresponding to that for $\mathcal{O}_E[\frac{1}{2}]/p\mathcal{O}_E[\frac{1}{2}]$:

- p splits completely if $\left(\frac{d}{p}\right) = 1$.
- p is unramified (and not split) if $\left(\frac{d}{p}\right) = -1$.
- p is ramified if $p \mid d$.

It remains to treat the case $p = 2$. If $d = 2, 3 \pmod 4$ then

$$\mathcal{O}_E/2\mathcal{O}_E \cong \mathbb{F}_2[X]/(X^2 - d) = \mathbb{F}_2[X]/((X - d)^2)$$

so 2 is ramified in $\mathcal{O}_E$ in this case. If $d = 1 \pmod 4$ then

$$\mathcal{O}_E/2\mathcal{O}_E \cong \mathbb{F}_2[X]/(X^2 - X + \frac{1 - d}{4})$$

so

- 2 splits completely if $\frac{1-d}{4}$ is even, i.e. $d = 1 \pmod 8$.
- 2 is unramified (and not split) if $\frac{1-d}{4}$ is odd, i.e. $d = 5 \pmod 8$.

This is a rather hands-on method and can be inefficient for large number fields. Soon we'll see another method to determine the factorisation of $p\mathcal{O}_E$ for a general number field E based on factorisations in $\mathbb{Q}_p[X]$.

Now suppose A, K, E, B are as before and suppose E/K is Galois with $G = \mathrm{Gal}(E/K)$. Then the action of G on E leaves B invariant.

Proposition 3.6. *Le $Q \subseteq B$ be a non-zero prime ideal, $P = Q \cap A$. Then*

1. *G acts transitively on the set of prime ideals of B which lie above P.*
2. *for all $\sigma \in G$, $f_{\sigma(Q)/P} = f_{Q/P}$ and $e_{\sigma(Q)/P} = e_{Q/P}$.*
3. *If $g_{Q/P}$ is the number of prime ideals lying above P then $e_{Q/P} f_{Q/P} g_{Q/P} = [E : K] = |G|$.*

Proof. If $\sigma \in G$ then $\sigma(Q) \subseteq B$ is a prime ideal and

$$\sigma(Q) \cap A = \sigma(Q) \cap \sigma(A) = \sigma(Q \cap A) = Q \cap A = P.$$

To show the action is transitive, we can assume A is DVR by replacing A with A_P. Then B has only finitely many prime ideals so by example sheet 1 is a PID. Let $\pi \in B$ be a generator of Q. Then

$$N_{E/K}(\pi) = \prod_{\sigma \in G} \sigma(\pi) \in Q \cap A = P.$$

If Q' is another prime ideal of B which lies above P then $N_{E/K}(\pi) \in Q'$ and hence (as Q' is prime) there exists $\sigma \in G$ such that $\sigma(\pi) \in Q'$. Hence $\sigma(Q) \subseteq Q'$ so equality.

For the second part, $\sigma|_B : B \to B$ is an automorphism. If $\sigma(Q) = Q'$ then it descends to an isomorphism $B/Q \cong B/Q'$ which acts as identity on A/P. In other words, σ determines an isomorphism $k_Q \to k_{Q'}$ of extensions of k_P. In particular $f_{Q/P} = f_{Q'/P}$. By definition we can factorise $PB = \prod_Q Q^{e_{Q/P}}$. Then for all $\sigma \in G$,

$$\sigma(PB) = \prod_Q \sigma(Q)^{e_{Q/P}}$$

so by unique factorisation for all Q have $e_{Q/P} = e_{\sigma(Q)/P}$.

Finally

$$[E : K] = \sum_{Q'} e_{Q'/P} f_{Q'/P} = e_{Q/P} f_{Q/P} g_{Q/P}$$

as $e_{Q'/P} = e_{Q/P}, f_{Q'/P} = f_{Q/P}$ for all Q'. □

We just saw that if $\sigma(Q) = Q$ then $\sigma|_B \pmod Q$ is an automorphism of k_Q.

Definition (decomposition group)**.** If $Q \subseteq B$ lies above $P \subseteq A$ then the *decomposition group* $D_{Q/P} = \mathrm{Stab}_G(Q)$.

Proposition 3.7. *Suppose $Q \subseteq B$ is a non-zero prime ideal and $P = Q \cap A$ and suppose k_Q/k_P is separable. Then*

1. *k_Q/k_P is a Galois extension.*
2. *the map $D_{Q/P} \to \mathrm{Gal}(k_Q/k_P), \sigma \mapsto \sigma|_B \pmod Q$ is a surjective group homomorphism.*

Proof.

1. We must show k_Q is normal, i.e. for all $\overline{\alpha} \in k_Q$, all Galois conjugates of $\overline{\alpha}$ in a normal closure of k_Q actually lie in k_Q. Fix $\overline{\alpha} \in k_Q = B/Q$. Choose any $\alpha \in B$ such that $\alpha \pmod Q = \overline{\alpha}$. Define

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha)) \in B[X].$$

The coefficients of $f(X)$ are invariant under G, so lie in $E^G = K$, so in $B \cap K = A$. Define $\overline{f}(X) = f(X) \pmod P \in k_P[X]$. Observe that $\overline{f}(X)$ has $\overline{\alpha}$ as a root and $\overline{f}(X)$ splits into linear factors in $k_Q[X]$. k_Q is normal, hence Galois.

2. Since k_Q/k_P is separable, there exists $\overline{\alpha} \in k_Q$ such that $k_Q = k_P(\overline{\alpha})$, i.e. $\overline{\alpha}$ is a primitive element. Let $Q = Q_1, Q_2, \ldots, Q_r$ be the prime ideals lying above P. By Chinese remainder theorem we can find $\alpha \in B$ such that $\alpha \pmod{Q} = \overline{\alpha}$, and for each $2 < i \leq r$, $\alpha \pmod{Q_i} = 0$. Let $f(X) = \prod_{\sigma \in G}(X - \sigma(\alpha)) \in A[X]$. Let $\overline{f}(X) = f(X) \pmod{Q} \in k_P[X]$. Then

$$\begin{aligned}\overline{f}(X) &= \prod_{\sigma \in G}(X - \sigma(\alpha) \pmod{Q}) \\ &= \prod_{\sigma \in D_{Q/P}}(X - \sigma(\alpha) \pmod{Q}) \cdot \prod_{\sigma \notin D_{Q/P}}(X - \sigma(\alpha) \pmod{Q})\end{aligned}$$

Note if $\sigma \notin D_{Q/P}$ then $\sigma^{-1}(Q) = Q_i$ for some $i > 1$ and hence

$$\sigma(\alpha) \pmod{Q} = \sigma(\alpha) + Q = \sigma(\alpha + \sigma^{-1}(Q)) = \sigma(\alpha + Q_i).$$

By construction $\alpha \in Q_i$ so $\sigma(\alpha) \pmod{Q} = 0$. Hence $\overline{f}(X) = \overline{g}(X)X^d$ where

$$\overline{g}(X) = \prod_{\sigma \in D_{Q/P}}(X - \sigma(\alpha) \pmod{Q}) \in k_P[X]$$

and $d = |G| - |D_{Q/P}|$. Suppose $\tau \in \mathrm{Gal}(k_Q/k_P)$. Then $\tau(\overline{\alpha})$ is also a root of $\overline{g}(X)$. Hence exists $\sigma \in D_{Q/P}$ such that $\sigma(\alpha) \pmod{Q} = \tau(\overline{\alpha})$. Since $k_Q = k_P(\overline{\alpha})$, this forces $\sigma|_B \pmod{Q} = \tau$.

□

As an application, suppose E/K is a Galois extension of number fields. Note if $P \subseteq \mathcal{O}_K$ is a non-zero prime ideal then k_P is a finite field so perfect (i.e. any finite extension is separable). If Q is a prime ideal of $\mathcal{O}_E$ lying above P then $\mathrm{Gal}(k_Q/k_P)$ has a canonical generator, i.e. the Frobenius automorphism $\alpha \mapsto \alpha^{|k_P|}$. Observe that

$$|D_{Q/P}| = |G|/g_{Q/P} = e_{Q/P}f_{Q/P}$$

and $|\mathrm{Gal}(k_Q/k_P)| = f_{Q/P}$ so

$$|\ker(D_{Q/P} \to \mathrm{Gal}(k_Q/k_P))| = e_{Q/P}$$

so if P is unramified in E then $D_{Q/P} \to \mathrm{Gal}(k_Q/k_P)$ is an isomorphism. Thus we can specifiy an element $\mathrm{Frob}_{Q/P} \in D_{Q/P} \subseteq G$ uniquely by defining $\mathrm{Frob}_{Q/P}$ to be the preimage of Frobenius automorphism in $\mathrm{Gal}(k_Q/k_P)$.

Example. Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ irreducible. Let E be the splitting field of $f(X)$ over $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_n \in E$ be the roots of $f(X)$. Then there is an injection $\varphi : \mathrm{Gal}(E/\mathbb{Q}) \hookrightarrow S_n = \mathrm{Sym}(\alpha_1, \ldots, \alpha_n)$.

Suppose p is a prime element such that $\overline{f}(X) = f(X) \pmod{p} \in \mathbb{F}_p[X]$ factors as $\overline{f}(X) = \prod_{i=1}^r \overline{f}_i(X)$ where $\overline{f}_1(X), \ldots, \overline{f}_r(X)$ are distinct monic irreducible polynomials in $\mathbb{F}_p[X]$ (equivalently $p \nmid \mathrm{disc}\, f$).

Proposition 3.8. *The image of* $\mathrm{Gal}(E/\mathbb{Q})$ *in* S_n *contains a permutation of cycle types* $(d_1)(d_2)\cdots(d_r)$ *where* $d_i = \deg \overline{f}_i(X)$.

Proof. Choose $Q \subseteq \mathcal{O}_E$ lying above $(p) \subseteq \mathbb{Z}$. Let $\overline{\alpha}_i = \alpha_i \pmod{Q}$. Note $\overline{\alpha}_i$ are all the roots of $\overline{f}(X)$ so are distinct. The map $D_{Q/P} \to \mathrm{Gal}(k_Q/k_P)$ is injective: if $\sigma \in D_{Q/P}$ lies in the kernel then $\sigma \pmod{Q}$ fixes each $\overline{\alpha}_i$. Since these are distinct, this forces σ to fix α_i so $\sigma = 1$. So $D_{Q/P} \cong \mathrm{Gal}(k_Q/k_P)$ and $e_{Q/P} = 1$ and we can define $\mathrm{Frob}_{Q/P} \in D_{Q/P}$. Claim that $\varphi(\mathrm{Frob}_{Q/P})$ has cycle type $(d_1)\cdots(d_r)$.

Proof. We must show $\mathrm{Frob}_{Q/P}$ has orbits on $\alpha_1, \ldots, \alpha_n$ of size $d_1, \ldots, d_r$, or equivalently $\mathrm{Gal}(k_Q/k_P)$ has orbits on $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ of size $d_1, \ldots, d_r$. Note these orbits are in bijection with irreducible factors of $\overline{f}(X)$

$$\mathcal{O} = \{\beta_1, \ldots, \beta_s\} \longleftrightarrow \prod_{i=1}^{s} (X - \beta_i).$$

This lies in $k_p[X]$ because this is an orbit, and is irreducible because it is a single orbit. □

□

Definition (inertia group)**.** We define the *inertia group* of Q to be

$$I_{Q/P} = \ker(D_{Q/P} \to \mathrm{Gal}(k_Q/k_P)).$$

We've seen that $|I_{Q/P}| = e_{Q/P}$. When ramification occurs, $I_{Q/P}$ is nontrivial and interesting things can happen. To understand $D_{Q/P}$ in such cases we must use completion.

Proposition 3.9. *Let* A *be a Dedekind domain,* $K = \mathrm{Frac}\, A$, E/K *a finite separable extension,* B *the integral closure of* A *in* E. *Let* $P \subseteq A$ *be a non-zero prime ideal and let* $Q \subseteq B$ *be a prime ideal lying above* P. *Then*

1. *there's a natural homomorphism* $\hat{A}_P \to \hat{B}_Q$ *extending* $A \to B$.
2. *Let* $K_P = \mathrm{Frac}\, \hat{A}_P, E_Q = \mathrm{Frac}\, \hat{B}_Q$. *Then* $E_Q = K_P \cdot E$ *is a finite separable extension of* K_P *and* $\hat{B}_Q$ *is the integral closure of* $\hat{A}_P$ *in* E_Q.
3. $e_{Q/P} = e_{Q\hat{B}_Q/P\hat{A}_P}$ *and* $f_{Q/P} = f_{Q\hat{B}_Q/P\hat{A}_P}$ *and* $[E_Q : K_P] = e_{Q/P} f_{Q/P}$.
4. *Suppose further* E/K *is Galois. Then* E_Q/K_P *is also Galois and there is a natural isomorphism* $D_{Q/P} \to \mathrm{Gal}(E_Q/K_P)$.

Proof. Factor

$$PB = Q_1^{e_{Q_1/P}} \cdots Q_r^{e_{Q_r/P}}$$

where $Q_1 = Q$. Then

$$\hat{A}_P = \varprojlim_i A_P/P^i A_P = \varprojlim_i A/P^i$$

and similarly $\hat{B}_Q = \varprojlim_i B/Q^i$. There is a natural map $A/P^i \to B/Q^i$ for any $i \geq 1$ so passage to inverse limits gives a homomorphism $\hat{A}_P \to \hat{B}_Q$.

Note we are free to replace A by A_P and assume wlog that A is a DVR. In this case, we've seen that B is a finite free A-module. Then

$$B/P^iB = B/\prod_{j=1}^{r} Q_j^{ie_{Q_j/P}} \cong \prod_{j=1}^{r} B/Q_j^{ie_{Q_j/P}}$$

so

$$\varprojlim_i B/P^iB \cong \prod_{j=1}^{r} \hat{B}_{Q_j}$$

as $\hat{A}_P$-modules, which are finite free as $\hat{A}_P$-module since each B/P^iB is a finite free A/P^i-module. Thus each summand $\hat{B}_{Q_i}$ is finite free as $\hat{A}_P$-module. In particular $\hat{B}_Q$ is integral over $\hat{A}_P$ so $\hat{B}_Q$ is the integral closure of $\hat{A}_P$ in E_Q.

Note

$$P\hat{B}_Q = \prod_{i=1}^{r} Q_i^{e_{Q_i/P}} \hat{B}_Q = Q^{e_{Q/P}} \hat{B}_Q$$

as for each $i > 1$, $Q_i\hat{B}_Q = \hat{B}_Q$ so $\hat{B}_Q/P\hat{B}_Q$ is isomorphic to $B/Q^{e_{Q/P}}$ as $\hat{A}_P/P\hat{A}_P \cong A/P$-module. Thus the map $B/PB \to \hat{B}_Q/P\hat{B}_Q$ is surjective and by Nakayama, $\hat{B}_Q$ is generated by B as $\hat{A}_P$-module. Passing to fraction field, we see E_Q is generated by E as K_P-vector space. If E/K is separable then every element of E is separable over K so E_Q/K_P is separable. If E/K is Galois then E is the splitting field of a polynomial with coefficients in K, which can be viewed as a polynomial with coefficients in K_P, so E_Q/K_P is Galois.

Note

$$f_{Q\hat{B}_Q/P\hat{A}_P} = [\hat{B}_Q/Q\hat{B}_Q : \hat{A}_P/P\hat{A}_P] = [B/Q : A/P] = f_{Q/P}.$$

In addition

$$(P\hat{A}_P)\hat{B}_Q = P\hat{B}_Q = (Q\hat{B}_Q)^{e_{Q/P}}$$

implies $e_{Q\hat{B}_Q/P\hat{A}_P} = e_{Q/P}$. We know

$$[E_Q : K_P] = e_{Q\hat{B}_Q/P\hat{A}_P} f_{Q\hat{B}_Q/P\hat{A}_P} = e_{Q/P} f_{Q/P}.$$

Now let's assume E/K is Galois and show 4 holds. We've already seen that as $E_Q = K_P E$ and E_Q/K_P is a Galois extension. If $\sigma \in D_{Q/P}$ then $\sigma(Q) = Q$ so $\sigma(Q^i) = Q^i$ for all $i \geq 1$. Hence σ determines an automorphism $\sigma|_B \pmod{Q^i} : B/Q^i \to B/Q^i$. By passage to inverse limit, we get an automorphism $\varprojlim_i \sigma|_B \pmod{Q^i} : \hat{B}_Q \to \hat{B}_Q$. By passsage to fraction field, this determines an element of $\mathrm{Gal}(E_Q/K_P)$. This determines a homomorphism $D_{Q/P} \to \mathrm{Gal}(E_Q/K_P)$. By what we've just show,

$$|\operatorname{Gal}(E_Q/K_P)| = [E_Q : K_P] = e_{Q/P} f_{Q/P} = |D_{Q/P}|$$

so it's enough to show injectivity. If $\sigma \in D_{Q/P}$ gets sent to 1 then it acts as the identity on $E_Q = K_P \cdot E$, so in particular acts as the identity on E. As $D_{Q/P} \subseteq \mathrm{Gal}(E/K)$, this means that $\sigma = 1$ in $D_{Q/P}$. □

At this point one may wonder why we must pass to the completion, instead of using the localsation. If we had done so, then firstly the field of fraction would be the same. Secondly if Q is not the only prime ideal of B lying above P then B_Q would not be a finite A_P-module, so none of the developed techniques are available. For example take $E = \mathbb{Q}(i), K = \mathbb{Q}, A = \mathbb{Z}, B = \mathbb{Z}[i]$. Consider $(5) = (2+i)(2-i)$. Then $\frac{1}{2+i}$ is not integral over $\mathbb{Z}_{(5)}$, as for example its norm is $\frac{1}{5}$. However as an exercise, by writing down the 5-adic expansion of the minimal polynomial, check $\frac{1}{2+i}$ is a integral over $\mathbb{Z}_5$.

Corollary 3.10. *Suppose $E = K(\alpha)$ is finite separable over K and let $f(X) \in K[X]$ be the minimal polynomial of α. For any non-zero prime ideals $P \subseteq A$, there is a bijection between*

$$\left\{ \begin{array}{c} \text{prime ideals } Q \text{ of } B \\ \text{lying above } P \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{irreducible factors} \\ \text{of } f(X) \text{ in } K_P[X] \end{array} \right\}$$

$$Q \mapsto \begin{array}{c} \text{unique irreducible factor} \\ g(X) \text{ of } f(X) \text{ in } K_P[X] \\ \text{such that } g(\alpha) = 0 \text{ in } E_Q \end{array}$$

Proof. Let L/K be the Galois closure of E/K. Let C be the integral closure of A in L. Fix $R \subseteq C$ a prime ideal lying above P. Let $G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/E)$. We know G acts transitively on the set of prime ideals of C lying above P, so by orbit-stabiliser there is a bijection

$$G/D_{R/P} \longleftrightarrow \left\{ \begin{array}{c} \text{primes in } C \\ \text{lying above } P \end{array} \right\}$$
$$\sigma \mapsto \sigma(R)$$

More importantly, the bijection is G-equivariant. We know that H acts transitively on the set of prime ideals of C lying above any give non-zero prime ideals of B, so there is a bijection

$$\left\{ \begin{array}{c} \text{prime ideals of } B \\ \text{lying above } P \end{array} \right\} = \left\{ \begin{array}{c} H\text{-orbits of} \\ \text{prime ideal of } C \\ \text{lying above } P \end{array} \right\} \longleftrightarrow H\backslash G/D_{R/P}$$
$$\sigma(R) \cap B \leftrightarrow \sigma$$

This means every $Q \subseteq B$ lying above P has the form $Q = \sigma(R) \cap B$ for some $\sigma \in G$. If $\sigma, \sigma' \in G$ then $\sigma(R) \cap B = \sigma'(R) \cap B$ if and only if exists $h \in H, d \in D_{R/P}$ such that $\sigma' = h\sigma d$.

On the other hand there is a bijection

$$\{\text{roots of } f(X) \text{ in } L\} \longleftrightarrow G/H$$
$$\sigma(\alpha) \hookleftarrow \sigma$$

which is again G-equivariant. As $\mathrm{Gal}(L_R/K_P) \hookrightarrow \mathrm{Gal}(L/K)$, there is a $\mathrm{Gal}(L_R/K_P)$-equivariant bijection

$$\{\text{roots of } f(X) \text{ in } L_R\} \longleftrightarrow G/H$$
$$\sigma(\alpha) \hookleftarrow \sigma$$

Now irreducible factors of $f(X)$ in $K_P[X]$ corresponds to $\mathrm{Gal}(L_R/K_P) = D_{R/P}$-orbits of roots in L_R so there's a bijection between irreducible factors of $f(X)$ in $K_P[X]$ and $D_{R/P}\backslash G/H$, given by sending σ to the unique $g(X)$ such that $g(\sigma(\alpha)) = 0$ in $L_R = K_P \cdot L$. Since there is an obvious bijection

$$\begin{aligned} H\backslash G/D_{R/P} &\longleftrightarrow D_{R/P}\backslash G/H \\ \sigma &\mapsto \sigma^{-1} \end{aligned}$$

there is also a bijection

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{prime ideals } Q \text{ of } B \\ \text{lying above } P \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{irreducible factors} \\ \text{of } f(X) \text{ in } K_P[X] \end{array} \right\} \\ Q = \sigma(R) \cap B & \mapsto & \begin{array}{c} \text{unique irreducible factor} \\ g(X) \text{ of } f(X) \text{ such that} \\ g(\sigma^{-1}(\alpha)) = 0 \text{ in } L_R \end{array} \end{array}$$

To finish the proof, it's enough to show that this map is the same as that in the statement of the corollary. What we need is to show that for all $\sigma \in G$, $g(\sigma^{-1}(\alpha)) = 0$ in L_R if and only if $g(\alpha) = 0$ in E_Q. At first sight this seems preposterous as L_R and E_Q live in completely different world. The key observation is that $\sigma : L \to L$ extends to an isomorphism $L_R \to L_{\sigma(R)}$ which acts as the identity on K_P: $\sigma(R)^i = \sigma(R^i)$ so σ determines a map $\sigma|_C \pmod{R^i} : C/R^i \to C/\sigma(R)^i$ for every $i \geq 1$. Passage to inverse limits and fraction fields gives the induced map $L_R \to L_{\sigma(R)}$. Hence if $g(X) \in K_P[X]$ is an irreducible factor of $f(X)$ then $g(\sigma^{-1}(\alpha)) = 0$ in L_R if and only if $\sigma(g(\sigma^{-1}(\alpha))) = 0$ in $L_{\sigma(R)}$, if and only if $g(\alpha) = 0$ in $L_{\sigma(R)}$. Note the coefficients of g are in K_P and $\alpha \in E$ so it is equivalent to $g(\alpha) = 0$ in E_Q.

$$\begin{array}{ccccc} L_R & \longleftarrow & L & \hookrightarrow & L_{\sigma(R)} \\ | & & | & & | \\ E_{R\cap B} & \longleftarrow & E & \hookrightarrow & E_Q \\ | & & | & & | \\ K_P & \longleftarrow & K & \hookrightarrow & K_P \end{array}$$

□

Example. Let $K = \mathbb{Q}, E = \mathbb{Q}(i), A = \mathbb{Z}, B = \mathcal{O}_E$. We know $2\mathcal{O}_E = (1+i)^2$ so $X^2 + 1$ is irreducible in $\mathbb{Q}_2[X]$. On the other hand, $5\mathcal{O}_E = (2+i)(2-i)$ splits so X^2+1 must factor in $\mathbb{Q}_5[X]$. By Hensel's lemma, there exists a unique $\theta \in \mathbb{Z}_5$ such that $\theta^2 = -1$ and $\theta = 2 \pmod 5$, and $X^2 + 1 = (X - \theta)(X + \theta)$ in $\mathbb{Q}_5[X]$. The embedding $\mathbb{Q} \to E$ extends to isomorphisms $\mathbb{Q}_5 \to E_{(2+i)}$ and $\mathbb{Q}_5 \to E_{(2-i)}$. Note that $X - \theta = X - 2 \in \mathbb{Q}_5[X]$ and $i = 2 \in E_{(2-i)}$ so $X - \theta$ corresponds to the ideal $(2 - i)$.

Example. Let $K = \mathbb{Q}, E = \mathbb{Q}(\sqrt[3]{2}), P = 5\mathbb{Z}$. How does $5\mathcal{O}_E$ factorise? We need to factor $X^3 - 2$ in $\mathbb{Q}_5[X]$. As $3^3 = 2 \pmod 5$, by Hensel's lemma there exists a unique $\theta \in \mathbb{Z}_5$ such that $\theta^3 = 2$ and $\theta = 3 \pmod{5\mathbb{Z}_5}$. We can write $X^3 - 2 = (X - \theta)g(X)$ in $\mathbb{Q}_5[X]$. In fact $g(X)$ must be irreducible, as any root of $g(X)$ must differ from θ by a primitive 3rd root of unity. Note 3rd roots

of unity in $\mathbb{Q}_5$ are roots of $X^3 - 1$, which by Hensel's lemma are in bijection with roots of $X^3 - 1$ in $\mathbb{F}_5$, so only one such. Thus $5\mathcal{O}_E$ has two distinct prime factors.

4 Extensions of complete DVRs

Definition (complete discrete valuation field)**.** We call a pair (K, v_K) a *complete discrete valuation field* (CDVF) if $v_K : K^\times \to \mathbb{Z}$ is a valuation and the corresponding DVR

$$A_K = \{x \in K^\times : v_K(x) \geq 0\} \cup \{0\}$$

is complete.

We usually have v_K implicit and call K a CDVF, for example $K = \mathbb{Q}_p$. We'll usually write $\pi_K \in A_K$ for a choice of uniformiser and $k_K = A_K/(\pi_K)$ for the residue field.

Next is an extremely important lemma on which almost all results in this chapter depend.

Lemma 4.1. *Let K be a CDVF and let E/K be a finite separable extension. Then E has a natural structure of a CDVF.*

Proof. Let B be the integral closure of A_K in E. By result in last chapter there is a bijection

$$\{\text{non-zero prime ideals of } B\} \longleftrightarrow \{\text{factors of } f(X) \text{ in } K_P[X]\}$$

where $f(X) \in K[X]$ is the minimal polynomial of a generator for E and $P = (\pi_K)$. Since K is a CDVF, $K_P = K$. Since $f(X) \in K[X]$ is irreducible, this shows B has a unique non-zero prime ideal Q, hence is a DVR. Let $v_E : E^\times \to \mathbb{Z}$ be the corresponding valuation. We've seen that $E_Q = K_P \cdot E = K \cdot E = E$, showing (E, v_E) is a CDVF. □

Definition (extension of CDVF)**.** We call E/K an *extension of CDVF* if K is a CDVF, E/K is finite separable and E has the structure of CDVF given by the lemma.

In this situation A_E, A_K are DVRs. We write

$$f_{E/K} = f_{(\pi_E)/(\pi_K)} = [k_E : k_K]$$
$$e_{E/K} = e_{(\pi_E)/(\pi_K)} = v_E(\pi_K)$$

then $[E : K] = e_{E/K} f_{E/K}$.

Remark.

1. If E/K is Galois then for all $\sigma \in \mathrm{Gal}(E/K), x \in E$, $v_E(\sigma(x)) = v_E(x)$. In other words, $\mathrm{Gal}(E/K)$ acts on E by isometry. This is because $\sigma(\pi_E)$ is a uniformiser of A_E as $\sigma|_{A_E}$ is a ring automorphism.

2. In general, without assuming E/K is Galois, we have that for all $x \in E^\times$,

$$v_E(x) = \frac{1}{f_{E/K}} v_K(N_{E/K}(x)).$$

Proof. If E/K is Galois then

$$\text{RHS} = \frac{1}{f_{E/K}} \frac{1}{e_{E/K}} v_E(N_{E/K}(x))$$

as $v_E|_{K^\times} = e_{E/K} v_K$ by checking the uniformisers. But

$$N_{E/K}(x) = \prod_{\alpha \in \mathrm{Gal}(E/K)} \sigma(x)$$

so

$$\text{RHS} = \frac{1}{[E:K]} \sum_{\sigma \in \mathrm{Gal}(E/K)} v_E(\sigma(x)) = v_E(x)$$

as v_E is Galois invariant.

Now suppose E/K is only separable and let L/K be the Galois closure. Then we have for all $x \in L^\times$,

$$v_L(x) = \frac{1}{f_{L/E}} v_E(N_{L/E}(x)) = \frac{1}{f_{L/K}} v_K(N_{L/K}(x))$$

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

$$\frac{[L:E]}{f_{L/E}} v_E(x) = \frac{1}{f_{L/K}} v_K(N_{L/K}(x)) = \frac{[L:E]}{f_{L/K}} v_K(N_{E/K}(x))$$

and hence

$$v_E(x) = \frac{f_{L/E}}{f_{L/K}} v_K(N_{E/K}(x)) = \frac{1}{f_{E/K}} v_K(N_{E/K}(x))$$

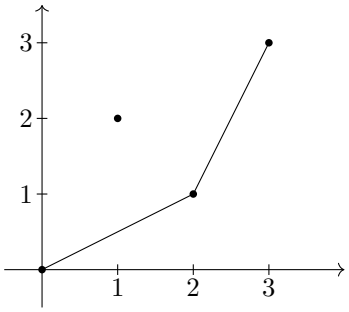
by tower law. □

Definition (Newton polygon)**.** Let A be a DVR, $K = \operatorname{Frac} A$ and let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ be a polynomial in $K[X]$ with $a_n \neq 0$. Then the *Newton polygon* $N_K(f)$ is the graph of the largest piecewise linear continuous function $N : [0, n] \to \mathbb{R}$ such that

1. $N(0) = 0, N(n) = v(a_n)$,
2. for all $0 < j < n$, $N(j) \leq v(a_j)$ if $a_j \neq 0$,
3. N is convex.

Equivalently, N is the lower convex hull of the points $(j, v(a_j))$ for $0 \leq j \leq n$.

Example. Let $f(X) = X^3 + 25X^2 + 5X + 125 \in \mathbb{Q}_5[X]$. Then we have



We define the *slopes* of $N_K(f)$ to be the slopes of the line segments, and the *multiplicity of a slope* is the length of the projection of the corresponding line segment to the x-axis.

In the above example we have slopes $\frac{1}{2}$ with multiplicity 2 and 2 with multiplicity 1.

Lemma 4.2. *Let A be a DVR, $K = \operatorname{Frac} A$, $\alpha_1, \dots, \alpha_n \in K^\times$ and*

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X].$$

Let $\lambda_i = v(\alpha_i)$ for $1 \le i \le n$. Then $\lambda_1, \dots, \lambda_n$ are the slopes of $N_K(f)$ with multiplicity. In particular the slopes of $N_K(f)$ are all integers.

Proof. wlog $\lambda_1 \le \cdots \le \lambda_n$. Let $L(f)$ be the polygon with slopes $\lambda_1, \dots, \lambda_n$. Then if $L : [0, n] \to \mathbb{R}$ is the corresponding function then $L(0) = 0$ by definition, $L(n) = \lambda_1 + \cdots + \lambda_n = v(\alpha_1 \cdots \alpha_n) = v(a_n) = N(n)$, and L is convex. If $0 < j < n$ then $L(j) = \lambda_1 + \cdots + \lambda_j$. Also

$$v(a_j) = v(\alpha_1 \cdots \alpha_j + \sum_{i_1 < \cdots < i_j} \alpha_{i_1} \cdots \alpha_{i_j}) \ge v(\alpha_1 \cdots \alpha_j) = \lambda_1 + \cdots + \lambda_j$$

so in fact $L(f)$ satisfies 1 – 3 in the definition of $N_K(f)$ so $L(f)$ lies below $N_K(f)$ by maximality of $N_K(f)$. To show equality, it is enough to show each vertex of $L(f)$ lies on $N_K(f)$. If $(j, \lambda_1 + \cdots + \lambda_j)$ is a vertex of $L(f)$ then $\lambda_{j+1} > \lambda_j$, i.e. $v(\alpha_{j+1}) > v(\alpha_j)$ since in the above expression for $v(a_j)$, if $(i_1, \dots, i_j) \ne (1, \dots j)$ then

$$v(\alpha_{i_1} \cdots \alpha_{i_j}) \ge \lambda_1 + \cdots + \lambda_{j-1} + \lambda_{j+1} > \lambda_1 + \cdots + \lambda_j$$

so by ultrametric inequality

$$v(a_j) = v(\alpha_1 \cdots \alpha_j) = \lambda_1 + \cdots + \lambda_j.$$

Hence $v(a_j) \ge N(j) \ge L(j) = v(a_j)$ so in fact $(j, v(a_j))$ is a vertex of both $L(f)$ and $N_K(f)$. □

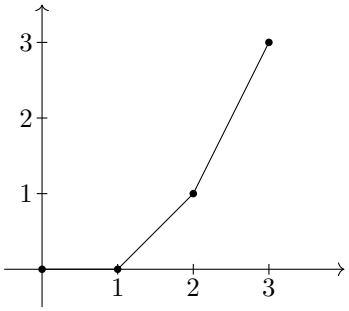
Proposition 4.3. *Let K be a CDVF and let $f(X) \in K[X], a_n \ne 0$ be monic separable. Let $\lambda_1 < \cdots < \lambda_r$ be the slopes of $N_K(f)$ where λ_i occurs with multiplicity $m_i \ge 1$. Then there exists a unique factorisation $f(X) = \prod_{i=1}^{r} g_i(X)$ in $K[X]$ where for all $1 \le i \le r$, $g_i(X)$ is a monic polynomial with degree m_i and $N_K(g)$ has a single slope λ_i.*

Proof. Let L/K be the splitting field of $f(X)$. Let $\alpha_1, \dots, \alpha_n \in L$ be the roots of $f(X)$ in L. Note $N_L(f)$ is the image of $N_K(f)$ under the linear transformation $\left(\begin{smallmatrix} 1 & 0 \\ 0 & e_{L/K} \end{smallmatrix}\right) : \mathbb{R}^2 \to \mathbb{R}^2$, as $v_L(a_j) = e_{L/K} v_K(a_j)$. The slopes of $N_L(f)$ are $e_{L/K}\lambda_1 < \cdots < e_{L/K}\lambda_n$. We define

$$g_i(X) = \prod_{v_L(\alpha_j) = e_{L/K}\lambda_i} (X - \alpha_j) \in L[X].$$

Since $\operatorname{Gal}(L/K)$ leaves v_L invariant, it acts on $\{\alpha_j : v_i(\alpha_j) = e_{L/K}\lambda_i\}$ so by Galois theory $g_i(X) \in K[X]$. By construction $f(X) = \prod_{i=1}^{r} g_i(X)$. Uniqueness follows from essentially the same argument. □

Example. Let $f(X) = X^3 + X^2 + 2X + 8$. Then $N_{\mathbb{Q}_2}(f)$ is



The slopes are $0, 1, 2$ each with multiplicity 1. Thus $f(X)$ splits into linear factors in $\mathbb{Q}_2[X]$.

Definition. If E/K is an extension of CDVF, we say

1. E/K is *unramified* if k_E/k_K is separable and $e_{E/K} = 1$.
2. E/K is *totally ramified* if $f_{E/K} = 1$.

We are going to show how to construct totally ramified extensions, followed by unramified extensions. Then we show everything can be done in these two stages.

Definition (Eisenstein polynomial)**.** Let A be a DVR, $K = \operatorname{Frac} A$. We say $f(X) = X^n + a_1X^{n-1} + \cdots + a_0 \in A[X]$ is *Eisenstein* if $v_K(a_i) \geq 1$ for each $i = 1, \ldots, n-1$ if $a_i \neq 0$ and $v_K(a_n) = 1$.

Eisenstein polynomial has a very simple characterisation in terms of Newton polygon: for any $f(X) \in K[X]$, $f(X)$ is Eisenstein if and only if $N_K(f)$ is a single line segment of slope $\frac{1}{n}$.

Proposition 4.4.

1. *Let E/K be a totally ramified extension of CDVFs. Let $f(X) \in K[X]$ be the minimal polynomial of π_E. Then $f(X)$ is Eisenstein and $E = K(\pi_E)$.*
2. *Let K be a CDVF and let $f(X) \in K[X]$ be a separable polynomial which is Eisenstein. Then $f(X)$ is irreducible and if $E = K[X]/(f(X))$ then E/K is totally ramified and $X \pmod{f(X)}$ is a uniformiser in A_E.*

Proof.

1. Suppose E/K is totally ramified and let $f(X) \in K[X]$ be the minimal polynomial of π_E. Then $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ where $n = [K(\pi_E) : K] \leq [E : K] = e_{E/K}$. We know $N_E(f)$ is the dilation by a factor of $e_{E/K}$ of $N_K(f)$. Note that $N_E(f)$ has a single slope, namely 1 with multiplicity n: the roots of $f(X)$ in a splitting field are all Galois conjugates of π_E, so in particular have the same valuation as π_E. In E,

$v_E(\pi_E) = 1$, so $N_E(f)$ has a single slope of 1. Hence $N_K(f)$ has a single slope $\frac{1}{e_{E/K}}$, and the endpoint is therefore $\frac{n}{e_{E/K}}$. But this is the valuation of the constant term and we know $v_K(a_n) \geq 1$, so must have $n \geq e_{E/K}$. Thus we have equality and $E = K(\pi_E)$. $f(X)$ is Eisenstein.

2. Suppose K is a CDVF and let $f(X) \in K[X]$ be a separable Eisenstein polynomial. Let $E = K(\alpha)$ where α is a root of $f(X)$. Note that a priori this does not give a fixed isomorphism class of extensions E/K, as $f(X)$ is not assumed to be irreducible. Nevertheless E/K is finite and separable so E/K is an extension of CDVF. We know $f(X)$ has a root in E so at least one slope of $N_E(f)$ must be an integer. However as f is Eisenstein, $N_K(f)$ has a single slope $\frac{1}{n}$, hence $N_E(f)$ has a single slope $\frac{e_{E/K}}{n}$. As it is a non-zero integer, $e_{E/K} \geq n$. Conversely,

$$e_{E/K} \leq [E : K] = [K(\alpha) : K] \leq n$$

so equality. $f(X)$ is irreducible and E/K is totally ramified. Moreover $v_E(\alpha) = \frac{e_{E/K}}{n} = 1$ so $\alpha \in A_E$ is a uniformiser.

□

Example. We've seen $(1 + i)^2 = 2\mathcal{O}_E$ where $E = \mathbb{Q}(i)$. Thus $E_{(1+i)}/\mathbb{Q}_2$ is a totally ramified quadratic extension, with uniformiser $1 + i$. So the minimal polynomial of $1 + i$ must be Eisenstein. It is $X^2 - 2X + 2$.

We now show how to construct unramified extensions.

Proposition 4.5. *Let K be a CDVF. Let ℓ/k_K be a finite separable extension. Then there exists an extension L/K of CDVFs and an isomorphism $\iota : \ell \to k_L$ with the following property: for any extension E/K of CDVFs and field homomorphism $j : \ell \to k_E$, there exists a unique K-embedding $J : L \to E$ such that the diagram*

$$\begin{array}{ccc} k_L & \xrightarrow{\iota^{-1}} & \ell \\ & \searrow^{\overline{J}} & \downarrow j \\ & & k_E \end{array}$$

commutes. Moreover L/K is unramified.

In other words, there is an unramified extension L/K such that

$$\mathrm{Hom}_K(L, E) \cong \mathrm{Hom}_{k_K}(\ell, k_E).$$

Proof. Since ℓ/k_K is separable, we can choose a primitive element $\overline{\alpha} \in \ell$. Let $\overline{f}(X) \in k_K[X]$ be the minimal polynomial and let $f(X) \in A_K[X]$ be any monic lift of $\overline{f}(X)$. $f(X)$ is irreducible since $\overline{f}(X)$ is, and is separable since $\operatorname{disc} f \pmod{(\pi_K)} = \operatorname{disc} \overline{f} \neq 0 \in k_K$. We define $L = K[X]/(f(X))$, which is separable, and $\alpha = X \pmod{f(X)} \in L$. Claim $A_L = A_K[\alpha]$: we have $A_K[\alpha] \subseteq A_L$ since α is integral over A_K. There is a ring homomorphism $A_K[\alpha]/(\pi_K) \to A_L/(\pi_K)$, so inducing a ring homomorphism $\iota : \ell \to A_L/(\pi_K)$ as $\ell = k_K[X]/(\overline{f}(X)) = A_K[X]/(f(X), \pi_K)$. To show $A_L = A_K[\alpha]$, take $z \in A_L$

and choose $n \geq 0$ as small as possible such that $\pi_K^n z \in A_K[\alpha]$. Since z is integral over A_K, we can write

$$z^m + a_1 z^{m-1} + \cdots + a_m = 0$$

for $a_i \in A_K$. Then

$$(\pi_K^n z)^m + a_1 \pi_K^n (\pi_K^n z)^{m-1} + \cdots + a_m \pi_K^{nm} = 0$$

in A_L. Reduction modulo π_K gives $(\pi_K^n z)^m \pmod{(\pi_K)} = 0$ in $A_L/(\pi_K)$. But $\pi_K^n z \in A_K[\alpha]$ so $\pi_K^n z \pmod{(\pi_K)}$ is in the image of ι. $\iota(\ell)$ is a field so contains no non-zero nilpotent, so we must have $\pi_K^n z \pmod{(\pi_K)} = 0$. Since ι is injective this means $\pi_K^n z \pmod{(\pi_K)} = 0 \in A_K[\alpha]/(\pi_K)$, i.e. $\pi_K^n z$ is divisible by π_K in $A_K[\alpha]$, so either $\pi_K^{n-1} z \in A_K[\alpha]$ or $n = 0$. The first case contradicts the minimality of n so $n = 0$ and $z \in A_K[\alpha]$. Since z is arbitrary, this show $A_L = A_K[\alpha]$, and also the map $\iota : \ell \to A_L/(\pi_K) = k_L$ is an isomorphism. In particular L/K is unramified.

We need to show that if E/K is an extension of CDVFs then embeddings $L \to E$ correspond to embeddings $\ell \to k_E$. We know

$$\{K\text{-embeddings } L \to E\} \longleftrightarrow \{\text{roots of } f(X) \text{ in } E\} \longleftrightarrow \{\text{roots of } f(X) \text{ in } A_E\}$$

where the last correspondence is because $f(X) \in A_K[X]$ is monic. On the other hand k_K-embeddings $\ell \to k_E$ correspond to roots of $\overline{f}(X)$ in k_E. There is a map

$$\{\text{roots of } f(X) \text{ in } A_E\} \to \{\text{roots of } \overline{f}(X) \text{ in } k_E\}$$

Hensel's lemma shows this map is bijective: $\overline{\alpha}$ is separable so $\overline{f}(X)$ has simple roots. □

Example. Let p be a prime. Then for any $n \geq 1$ there is a unique unramified extension of $\mathbb{Q}_p$ of degreee n up to isomorphism. This follows from uniqueness of finite extension of degree n of finite field and the universal property: there is a unique extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ up to isomorphism. By proposition we can find $L_n/\mathbb{Q}_p$ unramified extension of degree n and an isomorphism $\iota : \mathbb{F}_{p^n} \to k_{L_n}$. To show uniqueness, let $E_n/\mathbb{Q}_p$ be another unramified extension of degree n. Then $k_{E_n}/\mathbb{F}_p$ has degree n, so we can find an isomorphism $j : \mathbb{F}_{p^n} \to k_{E_n}$. Then there is a unique $\mathbb{Q}_p$-embedding $J : L_n \to E_n$ inducing $j \circ \iota^{-1}$ at the level of residue fields. Since L_n, E_n both have degree n over $\mathbb{Q}_p$, J is an isomorphism.

Let E/K be an extension of CDVFs with k_E/k_K separable. Then there exists a unique subextension E_0/K which is unramified, and such that $k_{E_0} = k_E$. Then $f_{E_0/K} = f_{E/K}$ and $e_{E/E_0} = e_{E/K}$. Then we have

$$\begin{array}{c} E \\ \Big| \text{totally ramified} \\ E_0 \\ \Big| \text{unramified} \\ K \end{array}$$

We construct E_0 as follow. Take a pair (L, ι) where L/K is unramified and $\iota : k_E \to k_L$. Then there exists a unique K-embedding $J : L \to E$ inducing

ι^{-1} at the level of residue fields. We define E_0 to be the image $J(L)$ of this embedding. To show uniqueness, note that any embedding of L in E must have image in E_0. Moreover E_0 contains any unramified subextension. E_0 is called the *maximal unramified subextension* of E/K.

Now suppose further that E/K is Galois and $G = \mathrm{Gal}(E/K)$. In this case we know k_E/k_K is also Galois and there is a surjective homomorphism $G \to \mathrm{Gal}(k_E/k_K)$. By Galois theory there is an intermediate extension $E^{I_{E/K}}/K$. Claim that $E^{I_{E/K}} = E_0$.

Proof. By Galois theory it's enough to show that for all $\sigma \in G = \mathrm{Gal}(E/K)$, $\sigma \in I_{E/K}$ if and only if $\sigma|_{E_0} = \mathrm{id}\,|_{E_0}$. Note for all $\sigma \in G$, $\sigma(E_0)/K$ is still an unramified subextension of E/K. As E_0 is the maximal such, we have $\sigma(E_0) = E_0$. In particular E_0/K is Galois. Moreover

$$\mathrm{Hom}_K(E_0, E) = \mathrm{Gal}(E_0/K) \to \mathrm{Gal}(k_E/k_K)$$

is bijective so for all $\sigma \in G$, $\sigma|_{E_0} = \mathrm{id}\,|_{E_0}$ if and only if the image of σ in $\mathrm{Gal}(E_0/K)$ is identity, if and only if the action of σ on k_E is the identity action. □

Thus we have an alternative characterisation of the maximal unramified subextension. As a consequence We have a tower of Galois extensions $E/E_0/K$ with $\mathrm{Gal}(E/E_0) = I_{E/K}, \mathrm{Gal}(E_0/K) = \mathrm{Gal}(k_E/k_K)$.

In fact we can do much more. We assume for the rest of today that E/K is a Galois extension of CDVFs with k_E/k_K separable. For concreteness one might have in mind finite extensions $E/\mathbb{Q}_p$ and $E/\mathbb{Q}((t))$.

Definition (lower ramification group)**.** Let $i \geq 0$. We define the *ith lower ramification group* of $G = \mathrm{Gal}(E/K)$ to be $G_i = \ker(G \to \mathrm{Aut}(A_E/(\pi_E^{i+1})))$. We set $G_{-1} = G$.

Remark.

1. Informally, G_i is the set of elements which fix the first $i+1$ digits of the π_E-adic expansion of elements of A_E.
2. $G_0 = \ker(G \to \mathrm{Gal}(k_E/k_K)) = I_{E/K}$.
3. $G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots$ and $\bigcap_{i \geq 0} G_i = \{1\}$.
4. Each G_i is normal in G. If $E/L/K$ is an intermediate extension and $H = \mathrm{Gal}(E/L)$ then $H_i = H \cap G_i$.

Lemma 4.6. *Suppose $\sigma \in G_0$. Then for any $i \geq 0$, $\sigma \in G_i$ if and only if $v_E(\sigma(\pi_E) - \pi_E) \geq i + 1$.*

Proof. Let E_0/K be the maximal unramified subextension. Then $\sigma \in \mathrm{Gal}(E/E_0)$. Note $A_E = A_{E_0}[\pi_E]$ as any element of A_E admits a π_E-adic expansion with digits in A_{E_0}: since maximal unramified implies they have the same residue field we may choose representatives in A_{E_0}. Thus the map $A_{E_0}[\pi_E] \to A_E/(\pi_E) = A_E/(\pi_K^{e_{E/K}})$ is surjective. We know A_E is a finitely generated A_{E_0}-module so Nakayama implies that $A_{E_0}[\pi_E] = A_E$.

If $\sigma \in G_0$ then the image of σ in $\mathrm{Aut}(A_E/(\pi_E^{i+1}))$ is a ring automorphism and $A_E/(\pi_E^{i+1})$ is generated by $A_{E_0}[\pi_E]$. So the image of σ is trivial if and only if $\sigma(\pi_E) = \pi_E \pmod{\pi_E^{i+1}}$, if and only if $v_E(\sigma(\pi_E) - \pi_E) \geq i+1$. □

Example. Let $K = \mathbb{Q}_2, E = \mathbb{Q}_2(\sqrt{2})$. E is the splitting field of X^2+2 which is Eisenstein so E/K is totally ramified. $G = G_0$ and we can take $\pi_E = \sqrt{2}$. Suppose $G = \{1, s\}$, then

$$v_E(s(\pi_E) - \pi_E) = v_E(-\sqrt{2} - \sqrt{2}) = v_E(-2\sqrt{2}) = v_E(-(\sqrt{2})^3) = 3$$

so by the lemma

$$G = G_0 = G_1 = G_2, \{1\} = G_3 = G_4 = \cdots$$

Example. Let $K = \mathbb{Q}_2, E = \mathbb{Q}_2(i)$ so E is the splitting field of X^2+1. We have $(1+i)^2 = 2i$ so E/K must be a quadratic ramified extension (otherwise $v_E(1+i) = \frac{1}{2}$) with $\pi_E = 1+i$. Suppose $G = \{1, t\}$, then

$$v_E(t(1+i) - (1+i)) = v_E(1-i-(1+i)) = v_E(-2i) = 2.$$

Hence

$$G = G_0 = G_1, \{1\} = G_2 = G_3 = \cdots$$

The extension $\mathbb{Q}_2(\sqrt{2})$ is "more ramified" than $\mathbb{Q}_2(i)$ as it has more non-trivial ramification groups.

Example. Let $K = \mathbb{Q}_2, E = \mathbb{Q}_2(\sqrt{2}, i)$. As $\mathbb{Q}_2(\sqrt{2}) \ncong \mathbb{Q}_2(i)$ by calculation above, E/K is Galois with $G = \{1, s, t, st\}$ where

$$s|_{\mathbb{Q}_2(\sqrt{2})} = s, s|_{\mathbb{Q}_2(i)} = \mathrm{id}_{\mathbb{Q}_2(i)}, \quad t|_{\mathbb{Q}_2(i)} = t, t|_{\mathbb{Q}_2(\sqrt{2})} = \mathrm{id}_{\mathbb{Q}_2(\sqrt{2})}$$

in notations above.

Let $\zeta = \frac{1+i}{\sqrt{2}}$ so $\zeta^2 = \frac{1+2i-1}{2} = i$ so ζ is a primitive 8th roots of unity in $\mathbb{Q}_2(\sqrt{2}, i)$. $\zeta - 1$ satisfies the polynomial

$$(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$$

which is Eisenstein in $\mathbb{Q}_2$. Thus E/K is totally ramified with uniformiser $\pi_E = \zeta - 1$. We now calculate $v_E(\sigma(\pi_E) - \pi_E)$ for all $\sigma \in G = G_0$.

$$v_E(s(\pi_E) - \pi_E) = v_E(-\frac{1+i}{\sqrt{2}} - \frac{1+i}{\sqrt{2}}) = v_E(-2\zeta) = v_E(2) = e_{E/K} = 4$$
$$v_E(t(\pi_E) - \pi_E) = v_E(\frac{1-i}{\sqrt{2}} - \frac{1+i}{\sqrt{2}}) = v_E(-\frac{2i}{\sqrt{2}}) = v_E(\sqrt{2}) = 2$$
$$v_E(st(\pi_E) - \pi_E) = v_E(-\frac{1-i}{\sqrt{2}} - \frac{1+i}{\sqrt{2}}) = v_E(-\frac{2}{\sqrt{2}}) = v_E(\sqrt{2}) = 2$$

Thus

$$G = G_0 = G_1, \{1, s\} = G_2 = G_3, \{1\} = G_4 = G_5 = \cdots$$

In this case there are two jumps in the filtration of G by its lower ramification groups.

Proposition 4.7.

1. *There exists an injective homomorphism $G_0/G_1 \to k_E^\times$. In particular G_0/G_1 is of order prime to p if* $\operatorname{char} k_E = p > 0$.
2. *If $i \geq 1$ then there's an injective homomorphism $G_i/G_{i+1} \to (k_E, +)$. In particular G_i/G_{i+1} is abelian, and is trivial if* $\operatorname{char} k_E = 0$ *and an $\mathbb{F}_p$-vector space if* $\operatorname{char} k_E = p > 0$.

Proof.

1. Note for any $\sigma \in G_0$, we can write $\sigma(\pi_E) = a_\sigma \pi_E \pmod{\pi_E^2}$ for some $a_\sigma \in A_{E_0}$ where E_0/K is the maximal unramified subextension: we can choose $X \subseteq A_{E_0}$ containing 0 and giving a set of representatives of $k_{E_0} = k_E$. Then any $\alpha \in A_E$ has a unique expression $\sum_{i=0}^\infty a(\alpha)_i \pi_E^i$. $\sigma(\pi_E)$ has valuation 1 so equals to $a(\sigma(\pi_E))_1 \pi_E + \pi_E^2 z$ for some $z \in A_E$, so we can take $a_\sigma = a(\sigma(\pi_E))$. Note as well that $a_\sigma \pmod{\pi_E} \neq 0$. Moreover $a_\sigma \pmod{\pi_E}$ depends only on σ and π_E (but not X).

   We define $G_0 \to k_E^\times$ by $\sigma \mapsto a_\sigma \pmod{\pi_E}$. To show $a_{\sigma\tau} = a_\sigma a_\tau \pmod{\pi_E}$, note we have

   $$\sigma\tau(\pi_E) = a_{\sigma\tau}\pi_E \pmod{\pi_E^2}$$

   while

   $$\sigma(\tau(\pi_E)) = \sigma(a_\tau \pi_E + \pi_E^2 z) = a_\tau \sigma(\pi_E) + \pi_E^2 z' = a_\tau a_\sigma \pi_E \pmod{\pi_E^2}$$

   so we must have $a_{\sigma\tau} = a_\sigma a_\tau \pmod{\pi_E}$, so the map is a homomorphism.

   An element $\sigma \in G_0$ lies in the kernel if and only if $\sigma(\pi_E) = \pi_E \pmod{\pi_E^2}$, if and only if $v_E(\sigma(\pi_E) - \pi_E) \geq 2$, if and only if $\sigma \in G_1$. $\operatorname{im}(G_0/G_1 \hookrightarrow k_E^\times)$ is a finite subgroup of $k_E^\times$. Any finite subgroup of the multiplicative group of a field is cyclic, of order prime to p if the characteristic $p > 0$.

2. Observe if $\sigma \in G_i$ for some $i \geq 1$ then we can write

   $$\sigma(\pi_E) = \pi_E + a_\sigma \pi_E^{i+1} \pmod{\pi_E^{i+2}}$$

   where $a_\sigma \in A_{E_0}$ and $a_\sigma \pmod{\pi_E} \in k_E$ depends only on σ and π_E. We thus define $G_i \to (k_E, +)$ by $\sigma \mapsto a_\sigma \pmod{\pi_E}$. This is a homomorphism:

   $$\begin{aligned}
   \sigma(\tau(\pi_E)) &= \sigma(\pi_E + a_\tau \pi_E^{i+1} + \pi_E^{i+2} z) \\
   &= \pi_E + a_\sigma \pi_E^{i+1} + \pi_E^{i+2} z' + \sigma(a_\tau \pi_E^{i+1}) + \sigma(\pi_E^{i+2} z) \\
   &= \pi_E + a_\sigma \pi_E^{i+1} + a_\tau \sigma(\pi_E)^{i+1} \pmod{\pi_E^{i+2}} \\
   &= \pi_E + a_\sigma \pi_E^{i+1} + a_\tau (\pi_E + a_\sigma \pi_E^{i+1})^{i+1} \pmod{\pi_E^{i+2}} \\
   &= \pi_E + (a_\sigma + a_\tau)\pi_E^{i+1} \pmod{\pi_E^{i+2}} \\
   &= \pi_E + a_{\sigma\tau} \pi_E^{i+1} \pmod{\pi_E^{i+2}}
   \end{aligned}$$

   so $a_\sigma + a_\tau = a_{\sigma\tau} \pmod{\pi_E}$.

   σ lies in the kernel if and only if $\sigma(\pi_E) = \pi_E \pmod{\pi^{i+2}}$, if and ony if $v_E(\sigma(\pi_E) - \pi_E) \geq i+2$, if and only if $\sigma \in G_{i+2}$. Thus we have an injective homomorphism $G_i/G_{i+1} \hookrightarrow (k_E, +)$ so G_i/G_{i+1} is abelian.

If $\operatorname{char} k_E = 0$ then k_E is a $\mathbb{Q}$-vector space so contains no non-trivial finite group so $G_i/G_{i+1} = \{1\}$. If $\operatorname{char} k_E = p$ then k_E is an $\mathbb{F}_p$-vector space, so G_i/G_{i+1} is annihilated by p.

□

As a consequence, if $\operatorname{char} k_E = 0$ then G_1 is trivial, as each G_i/G_{i+1} and $\bigcap_{i\geq 0} G_i = \{1\}$. Thus $G_0 = G_0/G_1$ is cyclic. If $\operatorname{char} k_E = p$ then G_0 is solvable since we have

$$G_0 \supseteq G_1 \supseteq \cdots$$

and all quotients G_i/G_{i+1} are abelian. G_1 is the (unique) p-Sylow subgroup of G_0, as G_0/G_1 has order prime to p while G_1 has order a power of p. As all p-Sylow subgroups are conjugate and $G_1 \trianglelefteq G_0$, G_1 is the unique one.

Moreover in the case k_E is finite (such as when $K/\mathbb{Q}_p$ is an extension of CDVFs) then $G/G_0 \cong \operatorname{Gal}(k_E/k_K)$ is cyclic so

$$G \supseteq G_0 \supseteq G_1 \supseteq \cdots$$

and hence $G = \operatorname{Gal}(E/K)$ is solvable (not just G_0).

Definition (tamely/wildly ramified)**.** If E/K is an extension of CDVFs, we say it's *tamely ramified* if either $\operatorname{char} k_E = 0$ or $\operatorname{char} k_E = p > 0$ and $p \nmid e_{E/K}$. Otherwise we say E/K is *wildly ramified*.

Note that if E/K is Galois and k_E/k_K is separable, then E/K is wildly ramified if and only if $G_1 \neq \{1\}$ (and the only case where the inertia group is not cyclic).

Proposition 4.8. *Let E/K be a Galois extension of CDVFs such that it's totally and tamely ramified, i.e. $e_{E/K} = [E : K]$ and if $\operatorname{char} k_E = p > 0$ then $p \nmid e_{E/K}$. Then if $n = [E : K]$ then K contains n nth roots of unity and there exists a uniformiser $\pi_K \in A_K$ such that $E = K(\sqrt[n]{\pi_K})$.*

Eisenstein polynomial $X^n - \pi_K$. Also if and only if (assuming K containing n nth roots of unity).

Proof. Since it is tamely ramified, G_1 is trivial so $G_0 \hookrightarrow k_E^\times = k_K^\times$. Since E/K is totally ramified, $G = G_0$ and so $G = G_0$ is cyclic of order n. Hence k_K contains n nth roots of unity and $f(X) = X^n - 1$ splits into linear factors in $k_K[X]$. $f'(X) = nX^{n-1}$ and $n \pmod{\pi_K} \in k_K^\times$ so the simple version of Hensel's lemma applies to show $X^n - 1$ splits into linear factors in $A_K[X]$ and K contains n nth roots of unity.

Let $\sigma \in \operatorname{Gal}(E/K)$ be a generator and $\pi_E \in A_E$ be a choice of uniformiser. Then exists a unique primitive nth root of unity $\zeta \in A_K$ such that

$$\sigma(\pi_E) = \zeta\pi_E \pmod{\pi_E^2}.$$

If

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

then

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

and $\alpha = n\pi_E \pmod{\pi_E^2}$. So $v_E(\alpha) = 1$ and $\alpha \in A_E$ is a uniformiser and $\sigma(\alpha^n) = (\zeta\alpha)^n = \alpha^n$, so $\alpha^n \in A_K$. Hence $E = K(\sqrt[n]{\pi_K})$ where $\pi_K = \alpha^n$. □

We have seen that $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$ is "more ramified" than $\mathbb{Q}_2(i)/\mathbb{Q}_2$. How can we make this precise? The dream is to define for any $v \in \mathbb{R}_{\geq 0}$ a subfield E^v/K inside E/K. This should have the following property:

1. E^0 is maximal unramified, $E = \bigcup_{v\geq 0} E^v$ and if $v \leq v'$ then $E^v \subseteq E^{v'}$.
2. for any intermediate extension $E/L/K$ with L/K Galois, want $L^v = L \cap E^v$.
3. if L_1, L_2 are intermediate extensions with $E = L_1 \cdot L_2$ then $E^v = L_1^v \cdot L_2^v$.

The naïve idea is to define $E^v = E^{G_v}$ for $v \in \mathbb{N}$. This satisfies 1 as $G_0 = I_{E/K}, \bigcap_{i\geq 0} G_i = \{1\}$ and $G_0 \supseteq G_1 \supseteq \cdots$. However this definition does not satisfy 2 or 3. For 2, this is related to having an equality $(G/H)_i = \mathrm{im}(G_i \to G/H)$ where $H = \mathrm{Gal}(E/L)$ and $G/H = \mathrm{Gal}(L/K)$. Although $G_i \cap H = H_i$, this does not hold in general for quotient group. For example take $E = \mathbb{Q}_2(\sqrt{2}, i), K = \mathbb{Q}_2$. Recall that

$$\mathrm{Gal}(E/K)_i = \begin{cases} \mathrm{Gal}(E/K) & i = 0, 1 \\ \{1, s\} & i = 2, 3 \\ \{1\} & i \geq 4 \end{cases}$$

Look at $\mathrm{im}(\mathrm{Gal}(\mathbb{Q}_2(\sqrt{2}, i)/\mathbb{Q}_2)_3 \to \mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)) = \mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$, which is not the same as $\mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)_3 = \{1\}$.

To solve this problem we introduce the upper ramification groups. These are the same as the lower groups but with a different indexing. First we extend G_u to $u \in \mathbb{R}_{\geq 0}$ by $G_u = G_{\lceil u \rceil}$. We define

$$\varphi_{E/K}(u) = \int_{t=0}^{u} [G_0 : G_t]^{-1} dt.$$

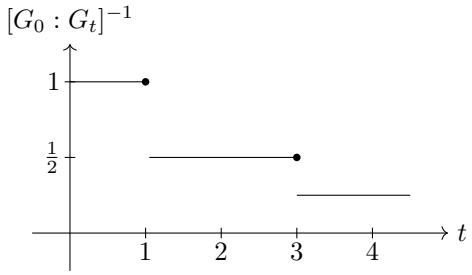
$\varphi_{E/K}$ is a continuous piecewise linear function. The discontinuities of $\varphi'_{E/K}(u)$ occur only at integer values of u. Moreover $\varphi_{E/K}(u)$ is strictly increasing and $\varphi_{E/K}(0) = 0$ so $\varphi_{E/K} : [0, \infty) \to [0, \infty)$ is a homeomorphism. We define $\psi_{E/K} = \varphi_{E/K}^{-1} : [0, \infty) \to [0, \infty)$. Then $\psi_{E/K}$ is also a strictly increasing piecewise linear homeomorphism.

Definition (upper ramification group)**.** If $v \in \mathbb{R}_{\geq 0}$, we define the *vth upper ramification group* to be $G^v = G_{\psi_{E/K}(v)} \leq G = \mathrm{Gal}(E/K)$.

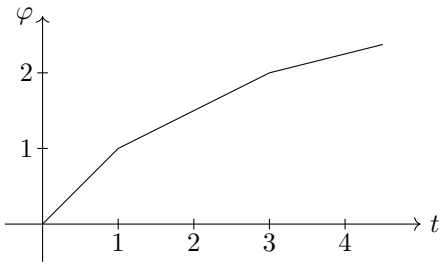
We say v is a jump in the upper ramification group if $G^v \neq G^{v+\varepsilon}$ for any $\varepsilon > 0$.

Warning: by definition, the jumps in the lower ramification groups G_u can only occur at integer values of u. However, the jump in the upper ramification groups can occur at rational but non-integer values of v.

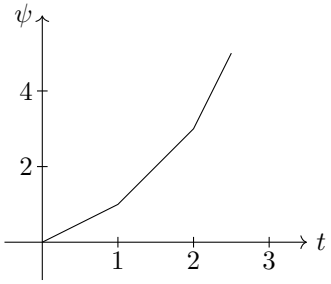
Example. $E = \mathbb{Q}_2(\sqrt{2}, i), K = \mathbb{Q}_2, G = \mathrm{Gal}(E/K)$. First plot $[G_0 : G_t]^{-1}$ against t.



Then plot φ against u.



Its inverse ψ is



so we conclude

$$G^v = \begin{cases} G & v \in [0,1] \\ \{1, s\} & v \in (1,2] \\ \{1\} & v \in (2, \infty) \end{cases}$$

In this case all jumps occur at integer points.

Example. $E = \mathbb{Q}_2(\sqrt{2})$.

$$G^v = \begin{cases} G & v \in [0,2] \\ \{1\} & v \in (2, \infty) \end{cases}$$

Note the map $\mathrm{Gal}(\mathbb{Q}_2(\sqrt{2}, i)/\mathbb{Q}_2) \to \mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$ has kernel $\{1, t\}$ and $\mathrm{im}(\mathrm{Gal}(\mathbb{Q}_2(\sqrt{2}, i)/\mathbb{Q}_2)^v) = \mathrm{Gal}(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)^v$ for any $v \in \mathbb{R}_{\geq 0}$.

To show this works in general, we introduce some more notations. Given a Galois extension E/K of CDVFs with k_E/k_K separable and $G = \mathrm{Gal}(E/K)$, we define $i_G : G \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by

$$i_G(1) = \infty, i_G(s) = \sup\{i : s \in G_{i-1}\} = 1 + \sup\{i : s \in G_i\}$$

so in general $i_G(s) \geq i + 1$ if and only if $s \in G_i$.

Lemma 4.9. *For any $u \in \mathbb{R}_{\geq 0}$ we have*

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

Proof. Both sides are continuous, piecewise linear and linear away from integer value of u and

$$\mathrm{LHS}(0) = 1, \mathrm{RHS}(0) = \frac{1}{|G_0|} \sum_{s \in G} \min(i_G(s), 1) = \frac{1}{|G_0|} \sum_{s \in G_0} 1 = 1.$$

To show they are equal it's enough to show for any $i \in \mathbb{Z}_{\geq 0}$ and for any $t \in (i, i + 1)$, $\mathrm{LHS}'(t) = \mathrm{RHS}'(t)$.

$$\mathrm{LHS}'(t) = [G_0 : G_{i+1}]^{-1} = [G_0 : G_t]^{-1}$$
$$\mathrm{RHS}'(t) = \frac{1}{|G_0|} \sum_{s \in G} \min(i_G(s), u + 1)'(t).$$

We have

$$\min(i_G(s), u + 1) = \begin{cases} i_G(s) & i_G(s) \leq u + 1 \\ u + 1 & i_G(s) \geq u + 1 \end{cases}$$

so for $t \in (i, i + 1)$,

$$\min(i_G(s), u + 1)'(t) = \begin{cases} 0 & i_G(s) \leq t + 1 \\ 1 & i_G(s) \geq t + 1 \end{cases}$$

Recall $s \in G_i$ if and only if $i_G(s) \geq i + 1$ so

$$\mathrm{RHS}'(t) = \frac{1}{|G_0|} \sum_{s \in G_t} 1 = [G_0 : G_t]^{-1} = \mathrm{LHS}'(t).$$

□

Lemma 4.10. *Suppose exists $\alpha \in A_E$ such that $A_E = A_K[\alpha]$. Then $i_G(s) = v_E(s(\alpha) - \alpha)$.*

Proof. By definition, $s \in G_i$ if and only if s acts trivially on $A_E/(\pi_E^{i+1})$, which is generated as a ring by the image of A_K and α, so if and only if s acts trivially on the image of α in $A_E/(\pi_E^{i+1})$, if and only if $s(\alpha) = \alpha \pmod{\pi_E^{i+1}}$. □

Lemma 4.11. *There exists $\alpha \in A_E$ such that $A_E = A_K[\alpha]$.*

Proof. By Nakayama, it's enough to find α such that $A_K[\alpha] \to A_E/(\pi_K)$ is surjective. Let $\overline{y} \in k_E$ be a primitive element and $\overline{f}(X) \in k_K[X]$ be its minimal polynomial, $f(X) \in A_K[X]$ a choice of monic lift of $\overline{f}(X)$, and $y \in A_E$ the unique root of $f(X)$ such that $y \pmod{\pi_E} = \overline{y}$. Since $\overline{f}(X)$ is separable, $\overline{f}'(\overline{y}) \neq 0$ so $f'(y) \in A_E^\times$. Thus

$$f(y + \pi_E) = f(y) + f'(y)\pi_E + \pi_E^2 z$$

has valuation 1 and is a uniformiser for A_E. Moreover $A_K[y + \pi_E] \to k_E$ sends $y + \pi_E \mapsto \overline{y}$ so is surjective, so we can choose a set $X \subseteq A_E$ of representative for k_E with $0 \in X$ and $X \subseteq A_K[y + \pi_K]$. Then any element of $A_E/(\pi_K) = A_E/(\pi_E^{e_{E/K}})$ has a unique representation of the form $\sum_{i=0}^{e_{E/K}-1} a_i f(y+\pi_E)$ with $a_i \in X$. But this lies in $A_K[y + \pi_E]$ so $A_E = A_K[y + \pi_E]$. □

Lemma 4.12. *Let $H \trianglelefteq G, L = E^H$ so $\mathrm{Gal}(L/K) = G/H$. Let $s \in G$. Then*

$$i_{G/H}(sH) = \frac{1}{e_{E/L}} \sum_{t \in H} i_G(st).$$

Proof. Choose $\alpha \in E_E, \beta \in A_L$ such that $A_E = A_K[\alpha], A_L = A_K[\beta]$.

$$\begin{array}{cc} E & A_K[\alpha] \\ | & | \\ L & A_K[\beta] \\ | & | \\ K & A_K \end{array}$$

Then

$$i_{G/H}(sH) = v_L(s(\beta) - \beta) = \frac{1}{e_{E/L}} v_E(s(\beta) - \beta)$$
$$i_G(st) = v_E(st(\alpha) - \alpha)$$

for $t \in H$. We need to show

$$\frac{1}{e_{E/L}} v_E(s(\beta) - \beta) = \frac{1}{e_{E/L}} \sum_{t \in H} v_E(st(\alpha) - \alpha)$$

or equivalently,

$$v_E(s(\beta) - \beta) = v_E(\prod_{t \in H} (st(\alpha) - \alpha)).$$

Let $f(X) \in A_L[X]$ be the minimal polynomial of α over L. Then $f(X) = \prod_{t \in H}(X - t(\alpha))$. Let $s(f)(X)$ denote the polynomial where s acts on the coefficients of $f(X)$ so $s(f)(X) = \prod_{t \in H}(X - st(\alpha))$ and $s(f)(\alpha) = \prod_{t \in H}(\alpha - st(\alpha))$. Write $f(X) = \sum a_i X^i, s(f)(X) = \sum s(a_i) X^i$ for $a_i \in A_L$. Then

$$s(f)(\alpha) = s(f)(\alpha) - f(\alpha) = \sum (s(a_i) - a_i)\alpha^i.$$

Since $A_L = A_K[\beta]$, for $a \in A_L$, $s(a) - a$ is divisible by $s(\beta) - \beta$ so $s(\beta) - \beta \mid s(f)(\alpha) = \prod_{t \in H}(\alpha - st(\alpha))$. Thus

$$v_E(s(\beta) - \beta) \leq v_E(\prod_{t \in H}(\alpha - st(\alpha))).$$

To show the reverse inequality, choose $g(X) \in A_K[X]$ such that $g(\alpha) = \beta$. We can do this since $b \in A_E$ and $A_E = A_K[\alpha]$. Then $g(X) - \beta \in A_L[X]$ has α as a zero, so is divisible by $f(X)$ in $A_L[X]$. Hence $f(X) \mid g(X) - \beta$ in $A_E[X]$, hence $s(f)(X) \mid g(X) - s(\beta)$ in $A_E[X]$. Now evaluate at $X = \alpha$ to get

$$s(f)(\alpha) \mid g(\alpha) - s(\beta) = \beta - s(\beta)$$

in A_E. Equivalently,

$$v_E(\prod_{t \in H}(\alpha - st(\alpha))) \leq v_E(\beta - s(\beta))$$

so equality. □

Lemma 4.13. *Suppose $H \trianglelefteq G$ and $L = E^H$. Define $j : G/H \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $j(sH) = \sup_{t \in H} i_G(st)$. Then*

$$i_{G/H}(sH) = 1 + \varphi_{E/L}(j(sH) - 1).$$

Proof. Recall that

$$\text{LHS} = \frac{1}{e_{E/L}} \sum_{t \in H} i_G(st)$$
$$\text{RHS} = \frac{1}{|H_0|} \sum_{t \in H} \min(i_H(t), j(sH))$$

Note that $e_{E/L} = |H_0|$ and for all $t \in H$, $i_G(t) = i_H(t)$ (as both sides equal $v_E(t(\alpha) - \alpha)$ where $A_E = A_K[\alpha]$). We can assume that the representative for sH is chosen so that $j(sH) = i_G(s)$ or equivalently for all $t \in H$, $i_G(st) \leq i_G(s)$. Therefore it suffices to show

$$\sum_{t \in H} i_G(st) = \sum_{t \in H} \min(i_G(t), i_G(s)).$$

We will show for all $t \in H$, $i_G(st) = \min(i_G(t), i_G(s))$. If $m + 1 = i_G(t) < i_G(s) = n + 1$ then $t \in G_m \setminus G_n, s \in G_n$. Hence $st \in G_m \setminus G_n$ so $i_G(st) = i_G(t)$. On the other hand if $i_G(t) \geq i_G(s)$ then $i_G(st) \geq i_G(s)$. Since s was chosen so that for all $t \in H$, $i_G(st) \leq i_G(s)$, we get $i_G(st) = i_G(s)$. □

Theorem 4.14 (Herbrand)**.** *Suppose $H \trianglelefteq G$ and $L = E^H$. If $u \in \mathbb{R}_{\geq 0}$ and $v = \varphi_{E/L}(u)$ then*

$$(G/H)_v = G_u H/H (= \text{im}(G_u \to G/H)).$$

Proof. For $s \in G$, we have $sH \in G_u H/H$ if and only if exists $t \in H$ such that $i_G(st) \geq u+1$, if and only if $j(sH) \geq u+1$. Since $\varphi_{E/L}$ is strictly increasing, we have $j(sH) \geq u+1$ if and only if $\varphi_{E/L}(j(sH)-1) \geq \varphi_{E/L}(u)$, if and only if $i_{G/H}(sH) \geq \varphi_{E/L}(u)+1$, if and only if $sH \in (G/H)_{\varphi_{E/L}(u)}$. □

Lemma 4.15. *We have* $\varphi_{E/K} = \varphi_{L/K} \circ \varphi_{E/L}$.

Proof. Both sides are piecewise linear continuous functions $[0,\infty) \to [0,\infty)$ which take 0 to 0 so it's enough to show derivatives coincide.

$$\begin{aligned}
\mathrm{LHS}'(u) &= [G_0 : G_u]^{-1} \\
\mathrm{RHS}'(u) &= \varphi'_{L/K}(\varphi_{E/L}(u))\varphi'_{E/L}(u) \\
&= [(G/H)_0 : (G/H)_{\varphi_{E/L}(u)}]^{-1}[H_0 : H_u]^{-1} \\
&= [G_0H/H : G_uH/H]^{-1}[H_0 : H_u]^{-1} \text{ Herbrand}
\end{aligned}$$

Now use isomorphism theorem

$$G_uH/H \cong G_u/G_u \cap H = G_u/H_u$$

(as lower ramification groups are compatible with subgroups) so

$$[G_0H/H : G_uH/H] = \frac{|G_0|}{|H_0|}\frac{|H_u|}{|G_u|} = \frac{[G_0 : G_u]}{[H_0 : H_u]}$$

so the result follows. □

Finally we can deduce upper ramifications groups are compatible with quotients:

Theorem 4.16. *For any* $v \geq 0$,

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

Proof. By definition $G^v = G_{\psi_{E/K}(v)}, (G/H)^v = (G/H)_{\psi_{L/K}(v)}$. $\varphi_{E/K} = \varphi_{E/K}^{-1}$ so by the lemma $\psi_{E/K} = \psi_{E/L} \circ \psi_{L/K}$. Herbrand gives

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

□

Definition. Let E/K be an extension of CDVF (not necessarily Galois) with k_E/k_K separable. If $v \in [0,\infty)$ we define

$$E^v = E \cap L^{G^v}$$

where L/E is any extension of CDVFs with k_L/k_K separable, L/K Galois with $G = \mathrm{Gal}(L/K)$.

This is independent of the choice of L: it's enough to show that if L'/L is a further extension of CDVFs and L'/K is Galois then

$$E \cap L^{G^v} = E \cap (L')^{(G')^v}$$

where $G' = \mathrm{Gal}(L'/K)$. Let $H = \mathrm{Gal}(L'/L)$. Then

$$E \cap L^{G^v} = E \cap L^{(G'/H)^v} = E \cap L^{(G')^v H/H} = E \cap (L')^{(G')^v H} = E \cap (L')^{(G')^v}$$

where the last equality is because $E \subseteq L = (L')^H$.

Proposition 4.17.

1. *E^0 is the maximal unramified subextension and*
$$E^0 = E \cap L^{G^0} = E \cap L^{G_0} = E \cap L_0.$$
2. *If $v \leq v'$ then $E^v \subseteq E^{v'}$. For $v \gg 0, E^v = E$.*
3. *If $E/M/K$ is an intermediate extension then $M^v = M \cap E^v$ (as both are $M \cap L^{G^v}$ for L/E with L/K Galois).*
4. *If $E/M, N/K$ are two intermediate extensions then $M^v \cdot N^v \subseteq (M \cdot N)^v$ (as $(M \cap L^{G^v}) \cdot (N \cap L^{G^v}) \subseteq (M \cdot N) \cap L^{G^v}$). Moreover if $M^v = M, N^v = N$ then $(M \cdot N)^v = M \cdot N$.*

We can think of $\inf\{v : E^v = E\}$ as a measure of "how ramified" an extension E/K is. For example back to the example $E = \mathbb{Q}_2(\sqrt{2}, i), K = \mathbb{Q}_2$. Recall that

$$G^v = \begin{cases} G & v \in [0,1] \\ \{1, s\} & v \in (1,2] \\ \{1\} & v \in (2, \infty) \end{cases}$$

so

$$E^v = \begin{cases} \mathbb{Q}_2 & v \in [0,1] \\ \mathbb{Q}_2(i) & v \in (1,2] \\ E & v \in (2, \infty) \end{cases}$$

This example displays another important feature of the group G^v, which we will not prove:

Theorem 4.18 (Hasse-Arf)**.** *Let $K/\mathbb{Q}_p$ be a finite extension and let E/K be an abelian extension, i.e. E/K is a Galois extension and $\mathrm{Gal}(E/K)$ is abelian. Then all of the jumps in the upper ramification groups are integers.*

The example $\mathbb{Q}_2(\sqrt{2}, i)/\mathbb{Q}_2$ is an application. For counterexample in non-abelian case, example sheet 3 gives $\mathbb{Q}_2(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_2$ in which $\frac{1}{2}$ is a jump.

Definition (conductor ideal)**.** Let $K/\mathbb{Q}_p$ be a finite extension. Let E/K be an abelian extension. We define the *conductor ideal* $C_{E/K}$ of A_K to be

(π_K^a) where

$$a = \inf\{n \in \mathbb{Z}_{\geq 0} : G^n = \{1\}\} = 1 + \text{highest jump}.$$

Proposition 4.19.

1. *$C_{E/K} = A_K$ if and only if E/K is unramified.*
2. *If $E_1, E_2/K$ are abelian extensions then $C_{E_1 \cdot E_2/K} = \mathrm{lcm}(C_{E_1/K}, C_{E_2/K})$, as if $C_{E_i/K} = (\pi_K^{a_i})$ then $a_i = \inf\{n \in \mathbb{Z}_{\geq 0} : E_i^n = E_i\}$, but $(E_1 \cdot E_2)^n = E_1 \cdot E_2$ if and only if $E_1^n = E_1$ and $E_2^n = E_2$.*

This formulation will be important when studying global fields.

5 Global class field theory

What is GCFT? Fix a number field K. Want to give a description of all abelian extensions E/K. We will organise these around the notion of conductor ideal.

Definition (conductor ideal)**.** Let E/K be an abelian extension of number fields. The *conductor ideal* is the unique $C_{E/K} \subseteq \mathcal{O}_K$ with the following property: for any non-zero prime ideal $P \subseteq \mathcal{O}_K$ and any prime ideal $Q \subseteq \mathcal{O}_E$ lying above P, $C_{E/K}A_{K_P} = C_{E_Q/K_P}$. Equivalently $v_P(C_{E/K}) = v_P(C_{E_Q/K_P})$.

This is well-defined as

1. C_{E_Q/K_P} is independent of choice of Q (as $E_Q \cong E_{Q'}$ as extensions of K_P).
2. $C_{E_Q/K_P} = A_{K_P}$ for all but finitely many P (as all but finitely many $P \subseteq \mathcal{O}_K$ are unramified in $\mathcal{O}_E$).
3. existence and uniqueness of $C_{E/K}$ then follows by unique factorisation of ideals in $\mathcal{O}_K$.

We first explain what happens for $K = \mathbb{Q}$. We know that if $N \in \mathbb{Z}_{\geq 1}$ then $\mathbb{Q}(\zeta_N)$ is an abelian extension of $\mathbb{Q}$ and there's an isomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) &\cong (\mathbb{Z}/N\mathbb{Z})^\times \\ \sigma_a &\leftrightarrow a \end{aligned}$$

where $\sigma_a(\zeta_N) = \zeta_N^a$. By Galois theory there's a bijection

$$\left\{ \begin{array}{c} \text{abelian extensions } L/\mathbb{Q} \\ \text{contained in } \mathbb{Q}(\zeta_N)/\mathbb{Q} \end{array} \right\} \longleftrightarrow \{\text{quotients of } (\mathbb{Z}/N\mathbb{Z})^\times\}$$

We have the Kronecker-Weber(-Hilbert) theorem: if $L/\mathbb{Q}$ is any abelian extension then exists $N \in \mathbb{Z}_{\geq 1}$ such that $L \subseteq \mathbb{Q}(\zeta_N)$. In fact, for any $N \in \mathbb{Z}_{\geq 1}$, $L \subseteq \mathbb{Q}(\zeta_N)$ if and only if $C_{L/\mathbb{Q}} \mid (N)$. Thus we get a bijection for any $N \in \mathbb{Z}_{\geq 1}$

$$\left\{ \begin{array}{c} \text{abelian extension } L/\mathbb{Q} \\ \text{in a fixed algebraic closure} \\ \text{such that } C_{L/\mathbb{Q}} \mid (N) \end{array} \right\} \leftrightarrow \{\text{quotients of } (\mathbb{Z}/N\mathbb{Z})^\times\}$$

This is almost GCFT for $K = \mathbb{Q}$, but we still need to give a characterisation of the bijection independent of explicit description of $\mathbb{Q}(\zeta_N)$. We do this using the *Artin symbol*.

Recall that if L/K is a Galois extension of number fields, not necessarily abelian, then for any non-zero prime ideal $P \subseteq \mathcal{O}_K$ and prime ideal $Q \subseteq \mathcal{O}_L$ lying above P such that $e_{Q/P} = 1$ (i.e. P is unramified in $\mathcal{O}_L$), we define $\mathrm{Frob}_{Q/P} \in \mathrm{Gal}(L/K)$ as the unique element such that

1. $\mathrm{Frob}_{Q/P}(Q) = Q$,
2. for all $x \in k_Q$, we have $\mathrm{Frob}_{Q/P}(x) = x^{|k_P|}$, i.e. it is the Frobenius automorphism of k_Q/k_P.

If $\sigma \in \mathrm{Gal}(L/K)$ then there is a commutative diagram

$$\begin{array}{ccc} k_Q & \xrightarrow{x \mapsto x^{|k_P|}} & k_Q \\ \downarrow \sigma & & \downarrow \sigma \\ k_{\sigma(Q)} & \xrightarrow{x \mapsto x^{|k_P|}} & k_{\sigma(Q)} \end{array}$$

so by the characterisation of Frobenius element

$$\mathrm{Frob}_{\sigma(Q)/P} = \sigma \,\mathrm{Frob}_{Q/P}\, \sigma^{-1}.$$

In particular, if $\mathrm{Gal}(L/K)$ is abelian then $\mathrm{Frob}_{\sigma(Q)/P} = \mathrm{Frob}_{Q/P}$, so is independent of choice of Q.

Definition (Artin symbol)**.** If L/K is an abelian extension of number fields and $P \subseteq \mathcal{O}_K$ is a non-zero prime ideal that is unramified in $\mathcal{O}_L$, we define the *Artin symbol* $(P, L/K) \in \mathrm{Gal}(L/K)$ by $(P, L/K) = \mathrm{Frob}_{Q/P}$ for any prime ideal $Q \subseteq \mathcal{O}_L$ lying above P.

This allows us to give a formulation of GCFT over $\mathbb{Q}$ that does not rely on knowing the extension $\mathbb{Q}(\zeta_N)$: for any $N \in \mathbb{Z}_{\geq 1}$, there's a bijection

$$\left\{ \begin{array}{c} \text{abelian extension } L/\mathbb{Q} \\ \text{such that } C_{L/\mathbb{Q}} \mid (N) \end{array} \right\} \longleftrightarrow \{\text{quotients of } (\mathbb{Z}/N\mathbb{Z})^\times\}$$

This may be uniquely characterised as follow: suppose given $L/\mathbb{Q}$. Then there is a unique surjective homomorphism $\phi_{L/\mathbb{Q}} : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$ with the property that for any prime $p \nmid N$,

$$\phi_{L/\mathbb{Q}}(p \bmod N) = ((p), L/\mathbb{Q}).$$

Remark. When $L = \mathbb{Q}(\zeta_N)$ this does recover the inverse of the usual map $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$: need to check that if $p \nmid N$ then $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ equals $((p), \mathbb{Q}(\zeta_N)/\mathbb{Q})$. Let $Q \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_N)}$ be a prime lying above (p). Then $k_Q = \mathbb{F}_p(\zeta_N)$ and

$$((p), \mathbb{Q}(\zeta_N)/\mathbb{Q})(\zeta_N \pmod Q) = \zeta_N^p \pmod Q.$$

But reduction modulo Q gives a bijection between roots of $X^N - 1$ in $\mathbb{Q}(\zeta_N)$ and in k_Q. So we must have

$$((p), \mathbb{Q}(\zeta_N)/\mathbb{Q})(\zeta_N) = \zeta_N^p$$

so $((p), \mathbb{Q}(\zeta_N)/\mathbb{Q}) = \sigma_p$.

The first step is generalising this to arbitrary base number field K. We first need to explain what object will replace $(\mathbb{Z}/N\mathbb{Z})^\times$. This will be ray class group.

Definition (modulus)**.** A *modulus* is a pair $m = (m_0, m_\infty)$ where $m_0 \subseteq \mathcal{O}_K$ is a non-zero ideal and $m_\infty \subseteq \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$, a possibly empty subset.

Recall that for any number field K, $|\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})| = [K:\mathbb{Q}] = r+2s$ where r is the number of real embeddings and s is the number of pairs of complex embeddings.

If $m = (m_0, m_\infty)$ and $n = (n_0, n_\infty)$ are moduli, we write $m \leq n$ if $m_0 \mid n_0$ and $m_\infty \subseteq n_\infty$.

Let K be a number field. We write $\mathcal{I} = \operatorname{Div}\mathcal{O}_K, \mathcal{P} = \{I \in \mathcal{I} : \text{exists } \alpha \in K^\times \text{ such that } I = (\alpha)\}$ the principal fractional ideals. Then $\mathcal{I}/\mathcal{P}$ is the *ideal class group* of $\mathcal{O}_K$. Now let $m = (m_0, m_\infty)$ be a modulus. We define

$$K(m_0) = \left\{ \begin{array}{c} \alpha \in K^\times \text{: for all non-zero prime } P \subseteq \mathcal{O}_K \\ \text{such that } v_P(m_0) > 0,\ v_P(\alpha) = 0 \end{array} \right\}$$

$$K_m = \left\{ \begin{array}{c} \alpha \in K(m_0) \text{: for all non-zero prime } P \subseteq \mathcal{O}_K \\ \text{such that } v_P(m_0) > 0,\ v_P(\alpha - 1) \geq v_P(m_0) \\ \text{and for all } \tau \in m_\infty,\ \tau(\alpha) > 0 \end{array} \right\}$$

$$\mathcal{I}(m_0) = \left\{ \begin{array}{c} I \in \mathcal{I} \text{: for all } P \subseteq \mathcal{O}_K \text{ non-zero prime} \\ \text{such that } v_P(m_0) > 0,\ v_P(I) = 0 \end{array} \right\}$$

$$\mathcal{P}(m_0) = \mathcal{P} \cap \mathcal{I}(m_0) = \{(\alpha) : \alpha \in K(m_0)\}$$

$$\mathcal{P}_m = \left\{ \begin{array}{c} I \in \mathcal{I} \text{: exists } \alpha \in K^\times \text{ such that } (\alpha) = I \\ \text{and for all } P \subseteq \mathcal{O}_K \text{ non-zero prime} \\ \text{such that } v_P(m_0) > 0,\ v_p(\alpha - 1) \geq v_p(m_0) \\ \text{and for all } \tau \in m_\infty,\ \tau(\alpha) > 0 \end{array} \right\}$$

$$= \{(\alpha) : \alpha \in K_m\}$$

Note $\mathcal{P}_m$ is a subgroup of $\mathcal{P}(m_0)$.

Definition (ray class group)**.** The *ray class group* of modulus m is

$$H(m) = \mathcal{I}(m_0)/\mathcal{P}_m.$$

Remark. If m is the trivial modulus $(\mathcal{O}_K, \emptyset)$ then

$$\mathcal{I}(m_0) = \mathcal{I}, \mathcal{P}_m = \mathcal{P}$$

and $H(m) = \mathcal{I}/\mathcal{P}$, the usual ideal class group.

Proposition 5.1.

1. *$H(m)$ is a finite abelian group.*
2. *There are short exact sequences*

$$0 \longrightarrow \mathcal{P}(m_0)/\mathcal{P}_m \longrightarrow H(m) \longrightarrow H_K \longrightarrow 0$$

where H_K is the usual ideal class group of $\mathcal{O}_K$, and

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_m) \longrightarrow (\mathcal{O}_K/m_0)^\times \times \{\pm 1\}^{m_\infty} \longrightarrow \mathcal{P}(m_0)/\mathcal{P}_m \longrightarrow 0$$

In particular

$$|H(m)| = |H_K| \cdot |(\mathcal{O}_K/m_0)^\times| \cdot 2^{|m_\infty|} \cdot |\mathcal{O}_K^\times/\mathcal{O}_K^\times \cap K_m|^{-1}.$$

Proof. 1 follows from 2 and the finiteness of H_K which is done in IID Number Fields. There's a short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{P}(m_0)/\mathcal{P}_m & \longrightarrow & \mathcal{I}(m_0)/\mathcal{P}_m & \longrightarrow & \mathcal{I}(m_0)/\mathcal{P}(m_0) & \longrightarrow & 0 \\ & & & & \| & & & & \\ & & & & H(m) & & & & \end{array}$$

There is a homomorphism $\mathcal{I}(m_0)/\mathcal{P}(m_0) \to \mathcal{I}/\mathcal{P} = H_K$. This is injective as $\mathcal{P}(m_0) = \mathcal{P} \cap \mathcal{I}(m_0)$. We need to show it's surjective, i.e. for any $I \in \mathcal{I}$, exists $\alpha \in K^\times$ such that $\alpha^{-1}I \in \mathcal{I}(m_0)$. Write $I = I_1 I_2^{-1}$ where $I_1, I_2 \subseteq \mathcal{O}_K$ are non-zero ideal. By Chinese remainder theorem we can find $\alpha_1, \alpha_2 \in \mathcal{O}_K$ such that for all $P \subseteq \mathcal{O}_K$ such that $v_P(m_0) > 0$,

$$v_P(I_1) = v_P(\alpha_1), v_P(I_2) = v_P(\alpha_2).$$

Then

$$v_P(\alpha_1^{-1}I_1) = v_P(\alpha_2^{-1}I_2) = 0$$

for all such P, so

$$\alpha_1^{-1}I_1(\alpha_2^{-1}I_2)^{-1} = (\alpha_1/\alpha_2)^{-1}I \in \mathcal{I}(m_0).$$

Set $\alpha = \frac{\alpha_1}{\alpha_2}$.

To obtain the second short exact sequence, we consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & K(m_0) & \longrightarrow & \mathcal{P}(m_0) & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathcal{O}_K^\times \cap K_m & \longrightarrow & K_m & \longrightarrow & \mathcal{P}_m & \longrightarrow & 0 \end{array}$$

By snake lemma there's a short exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times \cap K_m) \longrightarrow K(m_0)/K_m \longrightarrow \mathcal{P}(m_0)/\mathcal{P}_m \longrightarrow 0$$

We need to construct an isomorphism $K(m_0)/K_m \to (\mathcal{O}_K/m_0)^\times \times \{\pm 1\}^{m_\infty}$. There is at least a homomorphism: we can think of

$$(\mathcal{O}_K/m_0)^\times \times \{\pm 1\}^{m_\infty} = \prod_{P : v_P(m_0) > 0} (A_{K_P}^\times/1 + m_0 A_{K_P}) \times \prod_{\tau \in m_\infty} (\mathbb{R}^\times/\mathbb{R}_{>0})$$

For any $P \subseteq \mathcal{O}_K$, there's an inclusion $K^\times \subseteq K_P^\times$. If $v_P(m_0) > 0$, this extends to an inclusion $K(m_0) \subseteq A_{K_P}^\times$. The homomorphism we want is

$$\begin{aligned} K(m_0) &\to \prod_{P : v_P(m_0) > 0} A_{K_P}^\times \times \prod_{\tau \in m_\infty} \mathbb{R}^\times \to \prod_{P : v_P(m_0) > 0} (A_{K_P}^\times/1 + m_0 A_{K_P}) \times \prod_{\tau \in m_\infty} (\mathbb{R}^\times/\mathbb{R}_{>0}) \\ \alpha &\mapsto ((\alpha)_P, (\tau(\alpha))) \end{aligned}$$

The kernel equals K_m by definition. To complete the proof we need to show this homomorphism is surjective. Let $((x_P)_P, (\varepsilon_\tau)_\tau) \in \prod_{P:v_P(m_0)>0}(A_{K_P}^\times/1 + m_0 A_{K_P}) \times \{\pm 1\}^{m_\infty}$. By Chinese remainder theorem exists $x \in \mathcal{O}_K - \{0\}$ such that for all P such that $v_P(m_0) > 0$, $x \pmod{m_0 A_{K_P}} = x_P$. In particular $x \in K(m_0)$. It's now enough to prove that for any $(\varepsilon_\tau)_{\tau \in m_\infty}$, exists $y \in \mathcal{O}_K - \{0\}$ such that for all P such that $v_P(m_0) > 0$, $y = 1 \pmod{m_0 A_{K_P}}$ and for all $\tau \in m_\infty$, $\operatorname{sgn}(\tau(y)) = \varepsilon_\tau$. Equivalently, $y = 1 \pmod{m_0}$ and for all $\tau \in m_\infty$, $\operatorname{sgn}(\tau(y)) = \varepsilon_\tau$. Note $m_0 \cap \mathbb{Z}$ is a non-zero ideal, so we can find $N \geq 2$ such that $N \in m_0 \cap \mathbb{Z}$. We can find $\beta \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\beta)$. Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of β. Then

$$\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\gamma \in \mathbb{C} : f(\gamma) = 0\}$$
$$\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{R}) = \{\gamma \in \mathbb{R} : f(\gamma) = 0\}$$

Let $\gamma_\tau \in \mathbb{R}$ be $\tau(\beta)$ for any $\tau \in m_\infty$. We can find a polynomial $g(X) \in \mathbb{R}[X]$ such that for all $\tau \in m_\infty$, $\operatorname{sgn}(g(\gamma_\tau)) = \varepsilon_\tau$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we can assume that $g(X) \in \mathbb{Q}[X]$. By multiplying $g(X)$ by a positive integer we can assume $g(X) \in \mathbb{Z}[X]$. Then we take $y = 1 + kNg(\beta)$ for some $k \in \mathbb{N}$. Then $y = 1 \pmod{m_0}$ as $N \in m_0$. If k is large enough then

$$\operatorname{sgn}(\tau(y)) = \operatorname{sgn}(1 + kNg(\gamma_\tau)) = \operatorname{sgn}(g(\gamma_\tau)) = \varepsilon_\tau.$$

□

Example. Let $K = \mathbb{Q}, m = (N, \{\tau\})$ where $N \in \mathbb{N}$. Then $H_{\mathbb{Q}} = \{1\}$ so

$$H(m) \cong \frac{(\mathbb{Z}/N\mathbb{Z})^\times \times \{\pm 1\}}{\mathbb{Z}^\times} \cong (\mathbb{Z}/N\mathbb{Z})^\times$$
$$(a \pmod N, 1) \leftarrow\!\shortmid\, a \pmod N$$

So ray class group generalises the classical ideal class group. If instead $m = (N, \emptyset)$ then $H(m) = (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}, d > 1$ squarefree. Then exists $\varepsilon \in \mathcal{O}_K^\times$ such that $\mathcal{O}_K^\times = \{\pm \varepsilon^{\mathbb{Z}}\}$ and there exist two distinct embeddings $\sigma, \tau : K \to \mathbb{R}$ where $\sigma(\sqrt{d}) > 0, \tau(\sqrt{d}) < 0$. Suppose H_K is trivial. Let $m = (\mathcal{O}_K, \{\sigma, \tau\})$. Then

$$H(m) = \frac{\{\pm 1\} \times \{\pm 1\}}{\{(\operatorname{sgn}\sigma(\alpha), \operatorname{sgn}\tau(\alpha)) : \alpha \in \mathcal{O}_K^\times\}} \cong \frac{\{\pm 1\} \times \{\pm 1\}}{\langle (-1,-1), (\operatorname{sgn}\sigma(\varepsilon), \operatorname{sgn}\tau(\varepsilon))\rangle}$$

so two possibilities for $H(m)$: it is trivial if $\sigma(\varepsilon)$ and $\tau(\varepsilon)$ have different signs, or cyclic of order 2 if same sign. Note

$$N_{K/\mathbb{Q}}(\varepsilon) = \sigma(\varepsilon)\tau(\varepsilon) = \begin{cases} 1 & \operatorname{sgn}(\varepsilon) = \tau(\varepsilon) \\ -1 & \operatorname{sgn}(\varepsilon) \neq \tau(\varepsilon) \end{cases}$$

They both occur: if $d = 2$ then $H_K = \{1\}$ and $\varepsilon = 1 + \sqrt{2}$ has norm $N_{K/\mathbb{Q}}(\varepsilon) = 1 - 2 = -2$. If $d = 3$ then $H_K = \{1\}$ and $\varepsilon = 2 + \sqrt{3}$ has norm 1.

Theorem 5.2 (global class field theorem)**.** *Let K be a number field and m a modulus of K.*

1. *Let L/K be an abelian extension. Define its associated modulus $m_{L/K} = (m_{L/K,0}, m_{L/K,\infty})$ where*

$$m_{L/K,0} = C_{L/K}$$
$$m_{L/K,\infty} = \left\{ \begin{array}{c} \tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{R}) \text{: exist no} \\ \tilde{\tau} \in \mathrm{Hom}_{\mathbb{Q}}(L,\mathbb{R}) \text{ such that } \tilde{\tau}|_K = \tau \end{array} \right\}$$

   Define the homomorphism $\psi_{L/K} : \mathcal{I}(C_{L/K}) \to \mathrm{Gal}(L/K)$ as the unique homomorphism such that for any non-zero prime $P \subseteq \mathcal{O}_K$ such that $v_P(C_{L/K}) = 0, \psi_{L/K}(P) = (P, L/K)$. Suppose $m_{L/K} \leq m$. Then $\mathcal{P}_m \subseteq \ker \psi_{L/K}$ so $\psi_{L/K}$ determines a homomorphism $\phi_{L/K} : H(m) \to \mathrm{Gal}(L/K)$ which is surjective.

2. *The assignment $L/K \mapsto \ker \phi_{L/K}$ defines an inclusion-reversing bijection*

$$\left\{ \begin{array}{c} \text{abelian extesion } L/K \\ \text{such that } m_{L/K} \leq m \end{array} \right\} \longleftrightarrow \{\text{subgroup of } H(m)\}$$

   If L corresponds to H then $\phi_{L/K} : H(m)/H \to \mathrm{Gal}(L/K)$ is an isomorphism. In partciular the trivial subgroup of $H(m)$ corresponds to the maximal abelian extension $L(m)/K$ such that $m_{L(m)K} \leq m$. $L(m)$ is called the ray class field of modulus m*, and $\phi_{L(m)/K} : H(m) \cong \mathrm{Gal}(L(m)/K)$.*

Example. For any K there's the ray class field E associated the trivial modulus. This is the maximal extension E/K, everywhere unramified, and such that every embedding $\tau : K \hookrightarrow \mathbb{R}$ extends to an embedding $\tilde{\tau} : E \hookrightarrow \mathbb{R}$. E is called the *Hilbert class field* of K, and comes with an isomorphism $\phi_{E/K} : H_K \cong \mathrm{Gal}(E/K)$.

If K has trivial ideal class group then $E = K$, for example $E = \mathbb{Q}$.

If $K = \mathbb{Q}(\sqrt{-23})$ then E is the splitting field of $X^3 - X + 1$.

Proof. Define L to be the splitting field of $f(X) = X^3 - X + 1$ over $\mathbb{Q}$. Then $\mathrm{disc}\, f = -4a^3 - 27b^2 = -23$ so $\mathbb{Q}(\sqrt{-23}) \subseteq L$ and $f(X)$ is irreducible mod 3 so $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ and $\mathrm{Gal}(L/K)$ is cyclic of order 3. To show L/K is the Hilbert class field, we need to check

1. $m_{L/K} \leq (\mathcal{O}_K, \emptyset)$ (i.e. L/K is everywhere unramified),
2. $|H_K| = 3$.

We take 2 as given. For 1, note that $L/\mathbb{Q}$ is unramified for any prime away from $p = 23$. Note $\mathcal{O}_K$ has a unique prime ideal P lying above 23 as 23 is ramified, i.e. $23\mathcal{O}_K = P^2$ (in fact $P = (\sqrt{-23})$. We need to show P is unramified in L, equivalently that if Q is a prime ideal of $\mathcal{O}_L$ lying above 23 then $e_{Q/(23)} = |I_{Q/(23)}|$ is prime to 3.

If $\overline{f}(X) = f(X) \bmod 23$ then $\overline{f}(X)$ has a repeated root. In fact $\overline{f}(X) = a(X)b(X)^2$ where $a(X), b(X) \in \mathbb{F}_{23}[X]$ of degree 1: a cubic having a repeated

root either has a single root with multiplicity 3 or is of this form. But

$$3f(X) - Xf'(X) = 3x^3 - 3X + 3 - 3X^3 + X = -2X + 3$$

so $(\overline{f}, \overline{f}') \ni (-2X + 3)$ and $\gcd(\overline{f}, \overline{f}')$ has degree 1. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}_L$ be the roots of $f(X)$. Assume they're labeled so that $a(\alpha_1 \pmod{Q}) = 0, b(\alpha_2 \pmod{Q}) = 0$. Recall

$$I_{Q/(23)} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \sigma(Q) = Q, \sigma \pmod{Q} = \mathrm{id}_{k_Q}\}.$$

If $\sigma \in I_{Q/(23)}$ then

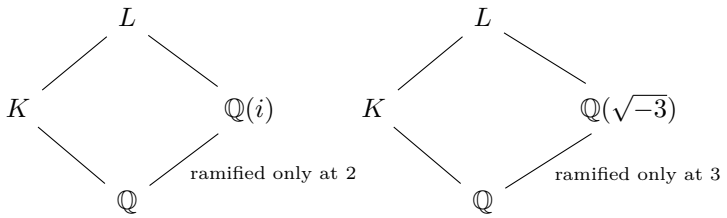
$$\begin{aligned} a(\sigma(\alpha_1) \pmod{Q}) &= 0 \\ b(\sigma(\alpha_2) \pmod{Q}) = b(\sigma(\alpha_3) \pmod{Q}) &= 0 \end{aligned}$$

hence we must have $\sigma(\alpha_1) = \alpha_1, \sigma(\alpha_2) \in \{\alpha_2, \alpha_3\}$ so $I_{Q/(23)} \subseteq \{1, (23)\}$. □

Example. Let $d \in \mathbb{Z}, d > 1$ squarefree and let $K = \mathbb{Q}(\sqrt{d})$. Suppose $H_K = \{1\}$. Recall that if $m = (\mathcal{O}_K, \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R}))$ then

$$H(m) = \begin{cases} \{1\} & N_{K/\mathbb{Q}}(\varepsilon) = -1 \\ \mathbb{Z}/2 & N_{K/\mathbb{Q}}(\varepsilon) = 1 \end{cases}$$

By GCFT if $N_{K/\mathbb{Q}}(\varepsilon) = 1$ then there exists a quadratic extension L/K which is everywhere unramified but with no real embedding. For example let $K = \mathbb{Q}(\sqrt{3})$. Then $H_K = \{1\}, \varepsilon = 2 + \sqrt{3}, N_{K/\mathbb{Q}}(\varepsilon) = 1$. In this case $L = K(i) = K(\sqrt{-23})$ is an everywhere unramified quadratic extension of K.



In the remainder of the course we'll examine the relation between GCFT of imaginary quadratic fields and binary quadratic forms.

Definition (binary quadratic form)**.** A *binary quadratic form* is a polynomial $f(x, y) = ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$. Equivalently

$$f(x, y) = (x, y) \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

We say an integer m is *represented* by $f(x, y)$ if there exist $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = m$.

A classical question in number theory asks: which primes p are represented by a fixed BQF? For example (for p odd)

- $p = x^2 + y^2$ if and only if $p = 1 \pmod{4}$ (Fermat).

- $p = x^2 + 2y^2$ if and only if $p = 1, 3 \pmod 8$ (Euler).
- $p = x^2 + 5y^2$ if and only if $p = 1, 9 \pmod{20}$ (Gauss).
- $p = x^2 + 14y^2$ if and only if the equations $x^2 = -14$ and $(y^2+1)^2 = 8$ both have solutions in $\mathbb{F}_p$.

In fact if $n \in \mathbb{N}$ and $-n = 2, 3 \pmod 4$ squarefree then p is represented by $x^2 + ny^2$ (with $p \nmid 4n$) if and only if p splits completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$.

Definition (discriminant of a BQF)**.** If $f(x, y) = ax^2 + bxy + cy^2$ is a BQF we define its *discriminant* to be $\operatorname{disc} f = b^2 - 4ac$.

$\mathrm{SL}_2(\mathbb{Z})$ acts on the set of BQFs by

$$\gamma \cdot f(x, y) = f(\gamma^{-1} \begin{pmatrix} x \\ y \end{pmatrix})$$

Equivalently $\gamma \cdot f$ is associated to $\gamma^{-T} \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right) \gamma^{-1}$. Since $\operatorname{disc} f = -4 \det \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$ it is invariant under the action.

Remark. If $\operatorname{disc} f < 0$ then $f(x, y)$ is either positive definite ($a > 0$) or negative definite ($a < 0$).

To describe the relation between BQFs and imaginary quadratic fields we need to introduce the *discriminant* of a number field. Recall from IID Number Fields that if $K/\mathbb{Q}$ is a number field of degree $[K : \mathbb{Q}] = n$ and $\alpha_1, \dots, \alpha_n \in K$, we define

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) = \det D^2$$

where $D_{ij} = \sigma_i(\alpha_j), \sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ are the distinct embeddings. This doesn't depend on the ordering of $\sigma_1, \dots, \sigma_n$. If $A \in M_n(\mathbb{Z})$ and $\beta_i = \sum_{j=1}^n A_{ij}\alpha_j$ then

$$\operatorname{disc}(\beta_1, \dots, \beta_n) = \det A^2 \operatorname{disc}(\alpha_1, \dots, \alpha_n).$$

In particular if $M \leq K$ is a free $\mathbb{Z}$-module of rank n then we can define $\operatorname{disc} M = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ is a generating set for M. This does not depends on the choice of α_i's. If $M' \leq M$ are free of rank n then by a similar argument using Smith normal form

$$\operatorname{disc} M' = \operatorname{disc} M \cdot [M : M']^2.$$

Note. $\mathcal{O}_K$ is always free of rank n as a $\mathbb{Z}$-module so we can define $\operatorname{disc} \mathcal{O}_K$. For example if $d \in \mathbb{Z}$ squarefree, $d \neq 0, 1$ then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} & d = 2, 3 \pmod 4 \\ \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2} & d = 1 \pmod 4 \end{cases}$$

so

$$\operatorname{disc} \mathcal{O}_K = \begin{cases} \det \left(\begin{smallmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{smallmatrix}\right)^2 = 4d & d = 2, 3 \pmod 4 \\ \det \left(\begin{smallmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{smallmatrix}\right)^2 = d & d = 1 \pmod 4 \end{cases}$$

Theorem 5.3. *Let $d \in \mathbb{Z}$ squarefree, $d < 0$. Fix an embedding $K = \mathbb{Q}(\sqrt{d}) \to \mathbb{C}$. Then there is a bijection*

$$\mathrm{SL}_2(\mathbb{Z}) \left\{ \begin{array}{c} \text{positive definite BQF} \\ \text{of discriminant } D \end{array} \right\} \longleftrightarrow H_K$$
$$ax^2 + bxy + y^2 \mapsto \mathbb{Z} \oplus \mathbb{Z}\beta$$

where $\beta = \frac{-b+\sqrt{D}}{2a}$.

We first prove

Proposition 5.4. *There is a bijection*

$$\left\{ \begin{array}{c} \text{positive definite BQF} \\ \text{of discriminant } D \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \beta \in K \text{ such that } \operatorname{Im}\beta > 0 \\ \text{and } \mathbb{Z} \oplus \mathbb{Z}\beta \text{ is a} \\ \text{fractional ideal of } \mathcal{O}_K \end{array} \right\}$$

given by the same formula as above. This bijection is $\mathrm{SL}_2(\mathbb{Z})$-equivariant, where $\mathrm{SL}_2(\mathbb{Z})$ acts on $\beta \in K$ with $\operatorname{Im}\beta > 0$ by Möbius transformation

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \beta = \frac{A\beta + B}{C\beta + D}.$$

Proof. First check that $\mathbb{Z} \oplus \mathbb{Z}\beta$ is a fractional ideal of $\mathcal{O}_K$, i.e. it is stable under multiplication by $\mathcal{O}_K$. Note $\beta = \frac{-b+\sqrt{D}}{2a}$ is a root of $f(x,1) = ax^2 + bx + c$ so $a\beta^2 = -(b\beta + c)$ and

$$a\beta \cdot (\mathbb{Z} \oplus \mathbb{Z}\beta) \subseteq \mathbb{Z} \oplus \mathbb{Z}\beta.$$

This implies that $a\beta$ is integral over $\mathbb{Z}$, hence $a\beta \in \mathcal{O}_K$, hence $\mathbb{Z} \oplus \mathbb{Z}a\beta \subseteq \mathcal{O}_K$.

$$\operatorname{disc}(\mathbb{Z} \oplus \mathbb{Z}a\beta) = \det \begin{pmatrix} 1 & a\beta \\ 1 & a\overline{\beta} \end{pmatrix}^2 = a^2(\beta - \overline{\beta})^2 = D = \operatorname{disc} \mathcal{O}_K$$

Hence $\mathbb{Z} \oplus \mathbb{Z}a\beta = \mathcal{O}_K$ so $\mathbb{Z} \oplus \mathbb{Z}\beta$ is a fractional ideal of $\mathcal{O}_K$.

We now define an inverse to the map in the statement of the proposition. It sends β to the binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$ where $ax^2 + bx + c \in \mathbb{Z}[x]$ is the unique quadratic which has β as a root, $\gcd(a,b,c) = 1$ and $a > 0$. We need to check that $\operatorname{disc} f = D$. Note $a\beta^2 = -(b\beta + c)$ so $a\beta \cdot (\mathbb{Z} \oplus \mathbb{Z}\beta) \subseteq \mathbb{Z} \oplus \mathbb{Z}\beta$ and $a\beta \in \mathcal{O}_K$. If $A + B\beta \in \mathcal{O}_K$ for $A, B \in \mathbb{Q}$ then $(A + B\beta) \cdot (\mathbb{Z} \oplus \mathbb{Z}\beta) \subseteq \mathbb{Z} \oplus \mathbb{Z}\beta$ so

$$\begin{aligned} A + B\beta &\in \mathbb{Z} \oplus \mathbb{Z}\beta \\ (A + B\beta)\beta &= A\beta + B(-\frac{b\beta}{a} - \frac{c}{a}) \\ &= -\frac{Bc}{a} + (A - \frac{Bb}{a})\beta \in \mathbb{Z} \oplus \mathbb{Z}\beta \end{aligned}$$

so $A, B \in \mathbb{Z}$ and $-\frac{Bc}{a}, A - \frac{Bb}{a} \in \mathbb{Z}$ so $\frac{B}{a} \in \mathbb{Z}$ (as a, b, c coprime) so $B \in a\mathbb{Z}$. Thus $A + B\beta \in \mathcal{O}_K$ lies in $\mathbb{Z} \oplus \mathbb{Z}a\beta$. Hence $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}a\beta$ and

$$D = \operatorname{disc} \mathcal{O}_K = \operatorname{disc}(\mathbb{Z} \oplus \mathbb{Z}a\beta) = \operatorname{disc} f.$$

This shows the existence of a bijection as in the statement of the proposition. $\mathrm{SL}_2(\mathbb{Z})$-equivariane is left as an exercise. □

Proof of Theorem 5.3. By proposition there's a bijection

$$\mathrm{SL}_2(\mathbb{Z})\backslash\left\{\begin{array}{c}\text{positive definite BQF}\\ \text{of discriminant } D\end{array}\right\}\longleftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash\left\{\begin{array}{c}\beta\in K \text{ such that } \operatorname{Im}\beta>0\\ \text{and } \mathbb{Z}\oplus\mathbb{Z}\beta \text{ is a}\\ \text{fractional ideal of } \mathcal{O}_K\end{array}\right\}$$

We need to show the map

$$\begin{aligned}\text{RHS}&\to H_K\\ \mathbb{Z}\oplus\mathbb{Z}\beta&\mapsto[\mathbb{Z}\oplus\mathbb{Z}\beta]\end{aligned}$$

is an bijection. First show it is well-defined: suppose $\beta,\beta'\in K, \operatorname{Im}\beta>0, \operatorname{Im}\beta'>0$, $\mathbb{Z}\oplus\mathbb{Z}\beta, Z\oplus\mathbb{Z}\beta'$ fractional ideals of $\mathcal{O}_K$ and $\beta=\frac{x\beta+y}{z\beta+w}$ for $\left(\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. Then

$$\mathbb{Z}\oplus\mathbb{Z}\beta'=\mathbb{Z}\oplus\frac{x\beta+y}{z\beta+w}=\frac{1}{z\beta+w}(\mathbb{Z}(z\beta+w)\oplus\mathbb{Z}(x\beta+y))$$

so

$$[\mathbb{Z}\oplus\mathbb{Z}\beta']=[\mathbb{Z}(z\beta+w)\oplus\mathbb{Z}(x\beta+y)]=[\mathbb{Z}\oplus\mathbb{Z}\beta].$$

Now show the map is injective. If $[\mathbb{Z}\oplus\mathbb{Z}\beta]=[\mathbb{Z}\oplus\mathbb{Z}\beta']$ then exists $\alpha\in K^\times$ such that $\mathbb{Z}\oplus\mathbb{Z}\beta=\mathbb{Z}\alpha\oplus\mathbb{Z}\alpha\beta'$, so exists $\left(\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z})$ such that

$$1=x\alpha+y\alpha\beta',\beta=z\alpha+w\alpha\beta'$$

so $\beta=\frac{w\beta'+z}{y\beta'+x}$. Since β,β' both have positive imaginary part, the matrix $\left(\begin{smallmatrix}w & z\\ y & x\end{smallmatrix}\right)$ has determinant $+1$.

Finally we show the map is surjective. Let I be a fractional ideal of $\mathcal{O}_K$. Then I is free of rank 2 as a $\mathbb{Z}$-module, so has a basis α_1,α_2 over $\mathbb{Z}$. wlog we can assume $\operatorname{Im}\frac{\alpha_2}{\alpha_1}>0$. Then

$$[I]=[\mathbb{Z}\alpha_1\oplus\mathbb{Z}\alpha_2]=[\mathbb{Z}\oplus\mathbb{Z}\frac{\alpha_2}{\alpha_1}]$$

which lies in the image. □

This gives an efficient way to compute H_K as a set, using the existence of a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, the upper half plane. We set

$$\mathcal{D}=\{z\in\mathbb{H}:|z|>1,-\frac{1}{2}\le\operatorname{Re}z<\frac{1}{2}\}\cup\{z\in\mathbb{H}:|z|=1,-\frac{1}{2}\le\operatorname{Re}z<0\}.$$

It is a fact that for all $z\in\mathbb{H}$, $\mathrm{SL}_2(\mathbb{Z})\cdot z)\cap\mathcal{D}$ contains exactly one element.

For any orbit of BQFs with discriminant D, there is a unique representative $f(x,y)=ax^2+bxy+cy^2$ such that $\beta=\frac{-b+\sqrt{D}}{2a}\in\mathcal{D}$. e have $|\beta|^2=\frac{c}{a},\operatorname{Re}\beta=-\frac{b}{2a}$. Thus $\beta\in\mathcal{D}$ if and only if

$$\frac{c}{a}>1,a\ge b>-a \text{ or } \frac{c}{a},a\ge b\ge 0.$$

This is usually written as $c\ge a\ge|b|$ and if $c=a$ or $a=|b|$ then $b\ge 0$.

Definition (reduced BQF)**.** A positive definite BQF of disciminant D is called *reduced* if it satisfies the condition above.

Lemma 5.5. *There is a bijection between H_K and the set of reduced positive definite BQFs of discriminant D.*

This also shows H_K is finite, as there are finitely many reduced forms $f(x,y)$: $-D = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2$ so $|b| \leq \sqrt{|D|}3$ so there are only finitely many possibilities for b, hence for a, c.

Proposition 5.6.

1. *The identity $[\mathcal{O}_K] \in H_K$ corresponds to the reduced form*

$$f(x,y) = \begin{cases} x^2 - dy^2 & d = 2,3 \pmod 4 \\ x^2 + xy + \frac{1-d}{4}y^2 & d = 1 \pmod 4 \end{cases}$$

   called principal form of $\mathcal{O}_K$.

2. *A class $[I] \in \mathcal{O}_K$ satisfies $[I]^2 = [\mathcal{O}_K]$ if and only if the corresponding reduced form $ax^2 + bxy + cy^2$ satisfies $c = a, a = b$ or $b = 0$.*

Proof.

1. We do the calculation for $d = 2,3 \pmod 4$. $x^2 - dy^2$ has discriminat D and is reduced. It corresponds to the fractional ideal class $[\mathbb{Z} \oplus \mathbb{Z}\beta]$ where $\beta = \frac{-b+\sqrt{D}}{2a} = \sqrt{d}$. We know $\mathbb{Z} \oplus \mathbb{Z}\sqrt{d} = \mathcal{O}_K$.

2. Observe that $\mathrm{Gal}(K/\mathbb{Q}) = \{1, c\}$ acts on H_K. In fact for any $[I] \in H_K$ we have $[I][c(I)] = [\mathcal{O}_K]$: it's enough to check that if $Q \subseteq \mathcal{O}_K$ is a non-zero prime ideal, $Qc(Q)$ is principal. Say Q lies above $(p) \subseteq \mathbb{Z}$. Then one of the three cases:

   (a) p splits in $\mathcal{O}_K$: $p\mathcal{O}_K = Qc(Q)$ so $Qc(Q) = p\mathcal{O}_K$.
   (b) p is inert: $p\mathcal{O}_K = Q$ so $Qc(Q) = p^2\mathcal{O}_K$.
   (c) p is ramified: $p\mathcal{O}_K = Q^2$ so $Qc(Q) = p\mathcal{O}_K$.

   so we need to show $[I] = [c(I)]$ if and only if $a = c, a = b$ or $b = 0$. wlog $I = \mathbb{Z} \oplus \mathbb{Z}\beta$ where $\beta = \frac{-b+\sqrt{D}}{2a}$ so $c(I) = \mathbb{Z} \oplus \mathbb{Z}\overline{\beta} = \mathbb{Z} \oplus \mathbb{Z}(-\overline{\beta})$. If $f(\beta, 1) = 0$ where $f(x,y) = ax^2 + bxy + cy^2$ then $g(-\overline{\beta}, 1) = 1$ where $g(x,y) = ax^2 - bxy + cy^2$. Thus $[I]^2 = [\mathcal{O}_K]$ if and only if $f(x,y), g(x,y)$ lies in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit.

   If β lies in the interior of $\mathcal{D}$, i.e. if $c > a$ and $a > |b|$ then $\overline{\beta}$ also lies in the interior so $g(x,y)$ is reduced, so $f(x,y), g(x,y)$ lies in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit so by uniqueness $f(x,y) = g(x,y)$ so $b = 0$.

   The other case is when β lies on the boundary of $\mathcal{D}$, i.e. $b = a$ or $c = a$. In this case $-\overline{\beta}$ is not in $\mathcal{D}$ so $g(x,y)$ is not reduced. However $-\overline{\beta}$ *is* $\mathrm{SL}_2(\mathbb{Z})$-conjugate to β to $f(x,y)$, (use, for example, the MMöbius tranformation $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ when $b = 1$) and indeed $[I]^2 = [\mathcal{O}_K]$.

□

Corollary 5.7. *Let $p \nmid D$ be a prime number. Then p is represented by the principal form of $\mathcal{O}_K$ if and only if p splits completely in the Hilbert class field H/K.*

Proof. Suppose $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\beta$ where $\beta = \sqrt{d}\ \frac{1+\sqrt{d}}{2}$. Have

$$f(x,y) = (x+y\beta)(x+y\overline{\beta}) = N_{K/\mathbb{Q}}(x+y\beta)$$

so p is representated by $f(x,y)$ if and only if exists $\alpha \in \mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = p$, if and only if exists $\alpha \in \mathcal{O}_K$ such that $(\alpha)(\overline{\alpha}) = (p)$, if and only if p splits in $\mathcal{O}_K$, $p = Q_1Q_2$ and both Q_1 and Q_2 are principal. Now recall the isomorphism $\phi_{H/K} : H_K \to \mathrm{Gal}(H/K)$ sending $[Q] \mapsto \mathrm{Gal}(Q, H/K)$, $Q \subseteq \mathcal{O}_K$ a non-zero prime ideal, $D_{Q'/Q} = \langle (Q, H/K) \rangle$. So p is represented by $f(x,y)$ if and only if p splits and $\phi_{H/K}(Q_1) = \mathrm{id}_H$, if and only if p splits and Q_1Q_2 splits completely in H/K (?), if and only if p splits completely in $H/\mathbb{Q}$. □

We can show that if $f(x,y)$ is a reduced form of discriminant D then $f(x,y)$ represents a prime $p \mid D$ if and only if p splits $p = Q_1Q_2$ in $\mathcal{O}_K$ and $\phi_{H/K}(Q_i)$ equals $\phi_{H/K}([I])$ for some $i = 1, 2$, where $[I]$ is the class corresponding to $f(x,y)$.

Idea:$H/K/\mathbb{Q}$. p is represented by some form $f(x,y)$ of discriminant D if and only if p splits in $\mathcal{O}_K$, which forms $f(x,y)$ repsent p is determined by the factorisation of p in $\mathcal{O}_H$.

Example. $d = -1, K = \mathbb{Q}(i), D = -4$. There is a unique reduced form $x^2 + y^2$ so if $pndivides2$ then $x^2 + y^2$ represents p if and only if p splits in $\mathbb{Z}[i]$, if and only if $\left(\frac{-1}{p}\right) = 1$, if and only if $p = 1 \pmod 4$.

Example. $d = -5, D = -20$. Have bound $|b| \leq \sqrt{\frac{|D|}{3}} < 3$ so $|b| = 0, 1, 2$. Also $b^2 - 4ac = -20$. If $b = 0$ then there is a unique reduced form $x^2 + 5y^2$. If $b = 2$ then there is a unique reduced form $2x^2 + 2xy + 3y^2$. The Hilbert class field is $H = K(i) = K(\sqrt{5})$. Thus if $p \nmid 20$ then $x^2 + 5y^2$ representes p if and only if p splits in H and $2x^2 + 2xy + 3y^2$ represents p if and only if p splits in K but does not split in $\mathbb{Q}(i)$.

Index