18.785 Number Theory I

Andrew Sutherland

Notes by Serena An

December 19, 2025

Contents

1 Absolute Values and discrete valuations

1.1 Absolute values on a field

Definition 1.1 (absolute value). An *absolute value* on a field k is a map $|\cdot|: k \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in k$,

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$
4. (optional, implies 3) $|x + y| \leq \max(|x|, |y|)$.

If 4 holds, then the absolute value is *non-archimedean*; otherwise it is *archimedean*.

Example 1.2

The normal absolute value on $\mathbb{R}$ is archimedean because $|1+1| \nleq |1|$.

The *trivial absolute value* with $|x| = 1$ for all $x \in k^\times$ and $|0| = 0$ is non-archimedean.

Lemma 1.3

$|\cdot|$ is non-archimedean if and only if for all for all $n \geq 1$,

$$|\underbrace{1 + \cdots + 1}_{n}| \leq 1.$$

Proof. See pset 1. □

Corollary 1.4

1. In a field of positive characteristic, every absolute value is non-archimedean.
2. The only absolute value on a finite field is the trivial absolute value.

Proof.
1. We use Lemma 1.3. In a field of characteristic p, all elements $n = 1 + \cdots + 1$ lie in $\mathbb{F}_p$ and satisfy $n^p = n$, so $|n|^p = |n|$ and $|n| = 0$ or 1.
2. If k is finite with say cardinality q, then $x^q = x$ for all $x \in k$, so $|x|^q = |x|$ and $|x| = 1$ for all $x \neq 0$. □

Definition 1.5 (equivalent). Two absolute values $|\cdot|$, $|\cdot|'$ on k are *equivalent* if there exists $\alpha \in \mathbb{R}_{>0}$ such that $|x| = |x|^\alpha$ for all $x \in k$.

1.2 Absolute values on $\mathbb{Q}$

We denote usual absolute value on $\mathbb{Q} \subset \mathbb{R}$ by $|\cdot|_\infty$. It is archimedean, since $|1+1| > \max(|1|, |1|)$.

There are other absolute values as follows. We write $x \in \mathbb{Q}^\times$ as $x = \pm \prod_q q^{e_q}$ for primes q and $e_q \in \mathbb{Z}$.

Definition 1.6 (p-adic valuation)**.** Fix a prime p. The *p-adic valuation* $\nu_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is defined by

$$\nu_p\Big(\pm \prod_q q^{e_q}\Big) := e_p, \quad \nu_p(0) := \infty.$$

The *p-adic absolute value* is defined by

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

where $p^{-\infty} := 0$.

Theorem 1.7 (Ostrowski)

Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some $p \leq \infty$.

Theorem 1.8 (Product formula)

For all $x \in \mathbb{Q}$,

$$\prod_{p \leq \infty} |x|_p = 1.$$

Proof. See pset 1. □

1.3 Discrete valuations

Definition 1.9 (valuation)**.** A *valuation* on k is a group homomorphism $\nu\colon k^\times \to \mathbb{R}$ such that for all $x, y \in k$, we have

$$\nu(x+y) \geq \min(\nu(x), \nu(y)).$$

We can extend ν to a map $k \to \mathbb{R} \cup \{\infty\}$ by defining $\nu(0) := \infty$.

We can then define a non-archimedean absolute value by $|x|_\nu := c^{\nu(x)}$ for any $0 < c < 1$.

Intuitively, if $p^m \mid x$ and $p^n \mid y$, then $x + y$ is divisible by $\min(p^m, p^n)$. For the p-adic absolute value, we let $c = p^{-1}$.

Definition 1.10 (value group, discrete valuation)**.** The *value group* of ν is the image of ν in $\mathbb{R}$. A *discrete valuation* is a valuation with value group precisely $\mathbb{Z}$.

Definition 1.11 (valuation ring given k, ν)**.** The *valuation ring* of k with respect to ν is the set

$$A := \{x \in k : \nu(x) \geq 0\}.$$

Definition 1.12 (DVR 1)**.** A *discrete valuation ring* (DVR) is an integral domain A that is the valuation ring of its fraction field $k = \operatorname{Frac} A$ with respect to some discrete valuation.

Remark 1.13. A DVR is not a field. By definition, $\nu(\operatorname{Frac} A) = \mathbb{Z}$, but $\nu(A) = \mathbb{Z}_{\geq 0}$.

For all $x \in k^\times$, we have $\nu(\frac{1}{x}) = \nu(1) - \nu(x) = -\nu(x)$, so at least one of x and $\frac{1}{x}$ lies in A. Then $x \in A$ is *invertible* if and only if $\nu(x) = 0$, and

$$A^\times = \{x \in k : \nu(x) = 0\}.$$

Definition 1.14 (valuation ring)**.** A *valuation ring* is an integral domain A with fraction field k such that for all $x \in k$, either $x \in A$ or $x^{-1} \in A$.

Now suppose A is a DVR. Any element $\pi \in A$ with $\nu(\pi) = 1$ is called a *uniformizer*, and uniformizers exist because $\nu(A) = \mathbb{Z}_{\geq 0}$. If we fix a uniformizer $\pi \in A$, then every $x \in k^\times$ can be written uniquely as $x = u\pi^n$ for $n = \nu(x)$ and a unit $u = x/\pi^n \in A^\times$. This implies A is a UFD, and in fact a PID whose ideals are $(1) \supset (\pi) \supset (\pi^2) \supset \cdots \supset (0)$, where

$$(\pi^n) = \{a \in A : \nu(a) \geq n\}.$$

There is a unique maximal ideal

$$\mathfrak{m} = (\pi) = \{a \in A : \nu(a) > 0\}.$$

Definition 1.15 (local ring, residue field)**.** A *local ring* is a ring A with a unique maximal ideal $\mathfrak{m}$. The *residue field* is $A/\mathfrak{m}$.

Given a DVR A with unique maximal ideal $\mathfrak{m}$, define $\nu\colon A \to \mathbb{Z}_{\geq 0}$ by letting $\nu(a)$ be the unique integer n with $(a) = \mathfrak{m}^n$. We can extend ν to a discrete valuation on k by $\nu(a/b) = \nu(a) - \nu(b)$, and $A = \{x \in k : \nu(x) \geq 0\}$ is the valuation ring from Definition 1.11.

Example 1.16

The p-adic valuation $\nu_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ has valuation ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$ with maximal ideal $\mathfrak{m} = (p)$ and residue field $\mathbb{Z}_{(p)}/(p) \simeq \mathbb{F}_p$.

Example 1.17

The field of *Laurent series* $k((t))$ has valuation $\nu\colon k((t)) \to \mathbb{Z} \cup \{\infty\}$ defined by

$$\nu\Big(\sum_{n \geq n_0} a_n t^n\Big) = n_0$$

for $a_{n_0} \neq 0$. This measures the "order of vanishing at 0." The valuation ring is $k[[t]]$.

1.4 Discrete valuation rings

The following are nice properties of DVRs.

- *Noetherian*: Every increasing sequence of ideals $I_1 \subseteq I_2 \subseteq \cdots$ stabilizes (ACC). Equivalently, every ideal is finitely generated.
- *PID*: Every ideal is principal.
- *local*: Unique maximal ideal.
- *dimension one*: The Krull dimension, which is the maximum length of a chain of prime ideals $(0) \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots$, is one.
- *regular*: If local, $\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim A$.
- *integrally closed (normal)*: Every nonzero element of $\operatorname{Frac} A$ that is the root of a monic polynomial $f \in A[x]$ lies in A.
- *maximal*: No rings between A and $\operatorname{Frac} A$.

Theorem 1.18

For an integral domain A, TFAE:

- A is a DVR.
- A is a Noetherian valuation ring that is not a field.
- A is a local PID that is not a field.
- A is an integrally closed Noetherian local ring of dimension one.
- A is a regular Noetherian local ring of dimension one.
- A is a Noetherian local ring with nonzero principal maximal ideal.
- A is a maximal Noetherian ring of dimension one.

1.5 Integral extensions

Definition 1.19 (integral over)**.** Given a ring extension $A \subseteq B$, an element $b \in B$ is *integral over* A if it is the root of some monic polynomial $f \in A[x]$. B is *integral over* A if all $b \in B$ are.

Proposition 1.20

Let $\alpha, \beta \in B$ be integral over $A \subseteq B$. Then $\alpha + \beta$ and $\alpha\beta$ are also integral over A.

Definition 1.21 (integral closure)**.** Given a ring extension B/A, the ring $\widetilde{A} = \{b \in B : b \text{ integral over } A\}$ is the *integral closure* of A in B. If $\tilde{A} = A$, then A is *integrally closed* in B. An integral domain A is *integrally closed* if it is in $\operatorname{Frac} A$.

Proposition 1.22

Given ring extensions $A \subseteq B \subseteq C$, if C/B and B/A are integral, then C/A is integral.

Corollary 1.23

The integral closure of $A \subseteq B$ is integrally closed in B.

Proof. Let A' be the integral closure of A in B, and let A'' be the integral closure of A' of B. By Proposition 1.22, A'' is integral over A. Every element of B that is integral over A lies in A' by definition, so $A'' \subset A'$ which shows $A' = A''$. □

Proposition 1.24

$\mathbb{Z}$ is integrally closed.

Proof. If $\frac{r}{s} \in \mathbb{Q}$ is integral over $\mathbb{Z}$ with $\gcd(r, s) = 1$, then it satisfies a monic polynomial

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

with $a_i \in \mathbb{Z}$. Clearing denominators shows $s \mid r^n$, which means $s = \pm 1$ and $\frac{r}{s} \in \mathbb{Z}$. □

Corollary 1.25

The same proof works for any UFD where $r \perp s$ makes sense. In particular, any PID is integrally closed.

Example 1.26

$\mathbb{Z}[\sqrt{5}]$ is not a UFD (and thus not a PID), because it is not integrally closed. Consider $\phi = \frac{1+\sqrt{5}}{2}$ which is a root of $x^2 - x - 1$ and thus integral over $\mathbb{Z}[\sqrt{5}]$, but $\phi \notin \mathbb{Z}[\sqrt{5}]$.

Definition 1.27 (number field, ring of integers)**.** A *number field* is a finite extension K of $\mathbb{Q}$. The *ring of integers* $\mathcal{O}_K$ of a number field is the integral closure of $\mathbb{Z}$ in K.

Example 1.28

For $K = \mathbb{Q}[\sqrt{5}]$, the ring of integers is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ (not $\mathbb{Z}[\sqrt{5}]$, which is not integrally closed).

Definition 1.29 (order)**.** An *order* in a $\mathbb{Q}$-algebra K of dimension r is a subring of K that is a free $\mathbb{Z}$-module of rank r.

$\mathcal{O}_K$ is an order in K, and in fact the *maximal order* (it contains every order in K).

Proposition 1.30

Let A be an integrally closed domain with fraction field K. Let $\alpha \in L/K$ with minimal polynomial $f \in K[x]$, where $[L : K] < \infty$. Then α is integral over A if and only if $f \in A[x]$.

Proof. If $f \in A[x]$, then α is integral over A, as the minimal polynomial is monic. Now suppose α is integral over A, and let $g \in A[x]$ be monic with $g(\alpha) = 0$. Over $\overline{K}[x]$, we can factor

$$f(x) = \prod_i (x - \alpha_i).$$

For each α_i, there is an embedding $K(\alpha) = K[x]/(f) \to \overline{K}$ sending $\alpha \mapsto \alpha_i$. In $\overline{K}$, we have $g(\alpha_i) = 0$ since $f(\alpha_i) = 0$ and $f \mid g$. Thus, each $\alpha_i \in \overline{K}$ is integral over A (as $g \in A[x]$) and lies in the integral closure of A in $\overline{K}$. All coefficients of f are sums of products of the α_i and thus elements of $\widetilde{A}$ that lie in K. We have $A = \widetilde{A} \cap K$ as A is integrally closed in K, so $f \in A[x]$. □

Example 1.31

We saw $\frac{1+\sqrt{5}}{2}$ that is integral over $\mathbb{Z}$. What about $\frac{1+\sqrt{7}}{2}$? Its minimal polynomial in $\mathbb{Q}[x]$ is $x^2 - x - \frac{3}{2} \notin \mathbb{Z}[x]$, so it is not integral over $\mathbb{Z}$ by Proposition 1.30.

2 Localization

2.1 Localization of a ring

We can think of $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}_{\neq 0}/\sim$ where $(a, s) \sim (a', s') \iff as' = a's$.

Definition 2.1 (localization)**.** Let A be a ring and $S \subset A$ be a *multiplicative subset*, meaning that it is closed under finite products (including the empty product which is 1). The *localization* of A at S, denoted $S^{-1}A$ or $A[S^{-1}]$, is the ring with the following universal property: there is a morphism $\iota\colon A \to S^{-1}A$ with $\varphi(S) \subset (S^{-1}A)^\times$ such that given $\varphi\colon A \to B$ with $\varphi(S) \subset B^\times$, then there exists a unique map $S^{-1}A \to B$ making the following diagram commute.

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\iota"] & B \\
S^{-1}A \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

By the universal property, $S^{-1}A$ is unique if it exists. For existence, consider $S^{-1}A \coloneqq A \times S/\sim$ where $(a, s) \sim (b, t) \iff$ there exists $v \in S$ such that $(at - bs)v = 0$. We also denote (a, s) by a/s. Define $\iota\colon A \to S^{-1}A$ by $a \mapsto (a, 1) = a/1$. We can check $S^{-1}A$ is a ring and ι is a ring homomorphism with $\iota(S) \subset (S^{-1}A)^\times$, as $(s/1)(1/s) = s/s = 1/1 = 1$.

We now check the universal property. If $\varphi\colon A \to B$ is a homomorphism with $\varphi(S) \subset B^\times$, we claim that there is a unique map $\pi\colon S^{-1}A \to B$ satisfying $\varphi = \pi \circ \iota$, as

$$\pi(a/s) = \pi(\iota(a)\iota(s)^{-1}) = \pi(\iota(a))\pi(\iota(s))^{-1} = \varphi(a)\varphi(s)^{-1}$$

is uniquely determined.

Remark 2.2. If A is an integral domain then ι is injective, and we can simplify the equivalence relation as $(a, s) \sim (b, t) \iff at = bs$.

Given two multiplicative sets $S \subset T$, we have $S^{-1}(A) \subset T^{-1}(A)$. In particular, $S^{-1}A \subset \operatorname{Frac} A$, where $\operatorname{Frac} A$ is A localized at $A_{\neq 0}$.

Localization yields a local ring (in the cases we care about), which is the reason behind its name.

2.2 Ideals in localizations

Let $\varphi\colon A \to B$ be a ring homomorphism. If $\mathfrak{b}$ is a B-ideal, then $\varphi^{-1}(\mathfrak{b})$ is an A-ideal, sometimes denoted $\mathfrak{b}^c$, and called the *contraction* of $\mathfrak{b}$ to A. When $A \subset B$ is a subring, then $\mathfrak{b}^c = \mathfrak{b} \cap A$. If $\mathfrak{a}$ is an A-ideal, then $\varphi(\mathfrak{a})$ is not necessarily a B-ideal, but it generates a B-ideal $\mathfrak{a}^e$ called the *extension* of $\mathfrak{a}$ to B.

We are interested in the case $\iota\colon A \to S^{-1}A$ with A a domain, so ι is injective and can be viewed as inclusion. If $A \subset B$, then

$$\mathfrak{a}^e = \mathfrak{a}B = (ab : a \in \mathfrak{a}, b \in B). \tag{2.1}$$

In general, $\mathfrak{a} \subseteq \varphi^{-1}((\varphi(\mathfrak{a}))) = \mathfrak{a}^{ec}$ and $\mathfrak{b}^{ce} = \varphi(\varphi^{-1}(\mathfrak{b})) \subseteq \mathfrak{b}$. Usually $\mathfrak{a} \subsetneq \mathfrak{a}^{ec}$: take for example $B = S^{-1}A$ with $\mathfrak{a} \cap S \neq \emptyset$, so $\mathfrak{a}^e = \mathfrak{a}B = B$ and $\mathfrak{a}^{ec} = B \cap A = A$, but we need not have $\mathfrak{a} = A$. However, when $B = S^{-1}A$, we always have $\mathfrak{b}^{ce} = \mathfrak{b}$.

Remark 2.3. In the context of (2.1), if $\mathfrak{a} = (a_1, \ldots, a_n)$ is finitely generated, then $\mathfrak{a}^e = \mathfrak{a}B = (a_1, \ldots, a_n)$ is also generated by the same elements. For $B = S^{-1}A$, we have $\mathfrak{b} = \mathfrak{b}^{ce}$, meaning that every B-ideal is the extension of an A-ideal. Thus if A is a Noetherian domain (all ideals finitely generated), then so is every localization $S^{-1}A$, and if A is a PID, then so is $S^{-1}A$.

Theorem 2.4

Let S be a multiplicative subset of a domain A. There is a 1-to-1 correspondence between

$$\{\text{prime ideals of } S^{-1}A\} \longleftrightarrow \{\text{prime ideals of } A \text{ that don't intersect } S\}$$

given by $\mathfrak{q} \mapsto \mathfrak{q} \cap A$ and $\mathfrak{p}S^{-1}A \leftarrow\!\shortmid \mathfrak{p}$.

Let $\mathfrak{p} \subset A$ be a prime ideal so that $S = A - \mathfrak{p}$ is a multiplicative set. Let

$$A_{\mathfrak{p}} = \left\{\frac{a}{b} : a \in A, b \notin \mathfrak{p}\right\}/\!\sim$$

denote the localization of A at $A - \mathfrak{p}$.

Warning 2.5. For $\frac{a}{b} \in \operatorname{Frac} A$, it is not true that $\frac{a}{b} \in A_{\mathfrak{p}} \iff b \notin \mathfrak{p}$. It can be true that $\frac{a}{b} \sim \frac{a'}{b'}$ where $b \in \mathfrak{p}$ and $b \notin \mathfrak{p}$. For example, taking $A = \mathbb{Z}$ and $\mathfrak{p} = (3)$, we have $\frac{9}{3} = \frac{3}{1}$. In general, A need not be a UFD, so there is no canonical way to pick a representative for each element in $S^{-1}A$.

Example 2.6

Let $A = k[x]$ and $\mathfrak{p} = (x-2)$. Then $A_{\mathfrak{p}} = \{f \in k(x) : f \text{ is defined at } 2\}$. A is a PID, so $A_{\mathfrak{p}}$ is PID with a unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}} = \{f \in k(x) : f(2) = 0\}$. Hence $A_{\mathfrak{p}}$ is a DVR (Theorem 1.18), and the valuation on $k(x) = \operatorname{Frac} A$ measures the "order of vanishing" of f at 2. The residue field is $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq k$, with quotient map $f \mapsto f(2)$.

Example 2.7

Let $p \in \mathbb{Z}$ be prime, so $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$. $\mathbb{Z}$ is a PID, so $\mathbb{Z}_{(p)}$ is a PID with unique maximal ideal $(p)\mathbb{Z}_{(p)}$, and thus a DVR. The valuation on $\mathbb{Q} = \operatorname{Frac}\mathbb{Z}$ is the p-adic valuation. The residue field is $\mathbb{Z}_{(p)}/(p)\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$ with quotient map $\mathbb{Z}_{(p)} \to \mathbb{F}_p$ as reduction mod p.

These are essentially the same example, with reduction mod $(x-2)$ and reduction mod p. Note $\mathbb{Z}_{(p)} \neq \mathbb{Z}_p$ which will later denote the p-adic integers.

2.3 Localization of modules

Definition 2.8 (localization of module)**.** The *localization* $S^{-1}M$ of an A-module M with respect to a multiplicative set $S \subset A$ is an $S^{-1}A$-module equipped with an A-module homomorphism $\iota\colon M \to S^{-1}M$ satisfying the following universal property: if N is an $S^{-1}A$-module and $\varphi\colon M \to N$ is an A-module homomorphism, then φ factors uniquely through $S^{-1}M$.

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\iota"] & N \\
S^{-1}M \arrow[ur, dashed, "\exists!"'] &
\end{tikzcd}$$

We use the same construction: $S^{-1}M := M \times S/\!\sim$ where $(a, s) \sim (b, t) \iff$ there exists $v \in S$ such that $(at - bs)v = 0$. In other words, $S^{-1}M = M \otimes_A S^{-1}A$ is the base change of M from A to $S^{-1}A$.

The map $\iota\colon M \to S^{-1}M$ is injective if and only if $M \xrightarrow{\times s} M$ is injective for all $s \in S$. This is a strong condition that does not hold in general, even when A is a domain, but it holds for the cases we care about. In particular, if A lies in a field K and M lies in a K-vector space, then $\iota\colon M \to S^{-1}M$ is injective, and we can view M as a submodule of $S^{-1}M$.

Proposition 2.9

Let A be a subring of a field K, and M be an A-module in a K-vector space V. Then

$$M = \bigcap_{\mathfrak{m}\in\operatorname{Max} A} M_{\mathfrak{m}} = \bigcap_{\mathfrak{p}\in\operatorname{Spec} A} M_{\mathfrak{p}}.$$

We will use this a lot, since many things are easy to check locally on $M_{\mathfrak{p}}$ but hard to check in general.

Proof. $M \subseteq \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$ is clear because ι is injective in this case. For the reverse direction, suppose $x \in \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$, and consider the A-ideal $\mathfrak{a} := \{a \in A : ax \in M\}$. For each maximal ideal $\mathfrak{m}$, write $x = m/s$ for some $m \in M$, $s \in A - \mathfrak{m}$. Then $sx \in M$ so $s \in \mathfrak{a}$. However, $s \notin \mathfrak{m}$, so $\mathfrak{a} \not\subseteq \mathfrak{m}$. This is true for all maximal ideals $\mathfrak{m}$, so $\mathfrak{a} = A$ and $1 \in \mathfrak{a}$. Thus $1x \in M$, as desired.

For the second equality, every prime ideal $\mathfrak{p}$ lies in some maximal ideal $\mathfrak{m}$ for which $M_{\mathfrak{m}} \subseteq M_{\mathfrak{p}}$, so $\bigcap_{\mathfrak{m}} M_{\mathfrak{m}} \subseteq \bigcap_{\mathfrak{p}} M_{\mathfrak{p}}$. Also every maximal ideal is prime, so $\bigcap_{\mathfrak{m}} M_{\mathfrak{m}} \supseteq \bigcap_{\mathfrak{p}} M_{\mathfrak{p}}$. □

An important special case is $K = \operatorname{Frac} A$ and $V = L/K$. When $L = K$, $M \subseteq K$ is an A-submodule of K. In particular, every A-ideal I is an A-submodule of $K = \operatorname{Frac} A$. Localizing I at $\mathfrak{p}$ is the same as extending I to $A \subseteq A_{\mathfrak{p}}$:

$$I_{\mathfrak{p}} = \left\{\frac{i}{s} : i \in I, s \in A - \mathfrak{p}\right\} = \left\{\frac{ia}{s} : i \in I, a \in A, s \in A - \mathfrak{p}\right\} = IA_{\mathfrak{p}}.$$

Corollary 2.10

For an integral domain A, every A-ideal I satisfies

$$I = \bigcap_{\mathfrak{m}\in\operatorname{Max} A} I_{\mathfrak{m}} = \bigcap_{\mathfrak{p}\in\operatorname{Spec} A} I_{\mathfrak{p}}.$$

Example 2.11

For $A = \mathbb{Z}$, we have $\mathbb{Z} = \bigcap_p \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$.

3 Dedekind domains

Proposition 3.1 (Dedekind domain)

Let A be a Noetherian domain. TFAE:

1. For every nonzero $\mathfrak{p} \in \operatorname{Spec} A$, $A_{\mathfrak{p}}$ is a DVR.
2. A is integrally closed and has Krull dimension $\dim A \leq 1$.

If either holds, A is called a *Dedekind domain (DD).*

The second best thing to being a DVR is for all localizations to be DVRs.

Proof. If A is a field, then 1 and 2 both hold: there are no nonzero $\mathfrak{p}$, and fields are integrally closed with dimension 0. Now assume A is not a field and let $K = \operatorname{Frac} A$.

($\Rightarrow$): Every chain of prime ideals $(0) \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ corresponds to a chain in $A_{\mathfrak{p}_n}$, and conversely such a chain can be contracted to A. Thus,

$$\dim A = \sup\{\dim A_{\mathfrak{p}} : \mathfrak{p} \in \operatorname{Spec} A\} = 1,$$

assuming that all $A_{\mathfrak{p}}$ are DVRs. To show A is integrally closed, consider any $x \in K$ integral over A which means it is integral over every $A_{\mathfrak{p}} \supset A$. However, the $A_{\mathfrak{p}}$ are integrally closed in $\operatorname{Frac} A_{\mathfrak{p}} = \operatorname{Frac} A$ (by being DVRs), so $x \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}} = A$, and A is integrally closed.

($\Leftarrow$): We claim that the following properties are preserved by localization:

- no zero divisors
- Noetherian
- dim ≤ 1 (dimension can only decrease upon localization)
- integrally closed.

To prove the last item, suppose $x \in K$ is integral over $A_{\mathfrak{p}}$. Then $x^n + \frac{a_{n-1}}{s_{n-1}} x^{n-1} + \cdots + \frac{a_0}{s_0} = 0$ for some $a_i \in A$, $s_i \in A - \mathfrak{p}$. Let $s = s_0 \cdots s_{n-1}$, so we can clear denominators by multiplying by s^n and get a polynomial for sx with coefficents in A, so sx is integral over A. Thus $sx \in A$, by the assumption that A is integrally closed. Then $\frac{sx}{s} = x \in A_{\mathfrak{p}}$, so $A_{\mathfrak{p}}$ is integrally closed. □

Corollary 3.2

Every PID is a Dedekind domain. In particular, $\mathbb{Z}$ and $k[x]$ are Dedekind domains.

PIDs are integrally closed and have dimension ≤ 1.

Remark 3.3. Every PID is a UFD and a DD, but not every UFD is a DD. For example, take $k[x, y]$ which has dimension 2. Also, not every DD is a UFD, e.g. $\mathbb{Z}[\sqrt{-13}]$ because $14 = (1+\sqrt{-13})(1-\sqrt{-13}) = 2\cdot 7$.

3.1 Fractional ideals

Definition 3.4 (fractional ideal)**.** A *fractional ideal* of a Noetherian domain A is a finitely generated A-submodule of $\operatorname{Frac} A$.

The following is the motivation behind the name “fractional.”

Lemma 3.5

Let A be a Noetherian domain, $K = \operatorname{Frac} A$, and $I \subseteq K$ be an A-module. Then I is finitely generated if and only if $aI \subseteq A$ for some nonzero $a \in A$.

Proof. ($\Rightarrow$): If $\frac{r_1}{s_1}, \ldots, \frac{r_n}{s_n}$ generate I as an A-module, then $aI \subseteq A$ for $a = s_1 \cdots s_n$.

($\Leftarrow$): If $aI \subseteq A$, then aI is an ideal and is finitely generated, since A is Noetherian. If $(a_1, \ldots, a_n) = aI$, then $(\frac{a_1}{a}, \ldots, \frac{a_n}{a})$ generate I as an A-module. □

Corollary 3.6

Every fractional ideal of A can be written as $\frac{1}{a} I$ for some nonzero $a \in A$ and A-ideal I.

Definition 3.7 (principal fractional ideal)**.** A fractional ideal is *principal* if it is generated by one element. Let $(x) := xA$ denote the principal fractional ideals for $x \in K = \operatorname{Frac} A$.

We can add and multiply fractional ideals in the same way as normal ideals:

$$I + J := (i + j : i \in I, j \in J)$$

$$IJ := (ij : i \in I, j \in J).$$

However, there is a new *division* operation

$$I \div J := \{x \in K : xJ \subseteq I\},$$

called "the quotient of I by J." It is not the same as a quotient of A-modules, e.g. $\mathbb{Z}/\mathbb{Z} = \{0\}$, but $\mathbb{Z} \div \mathbb{Z} = \mathbb{Z}$.

Lemma 3.8

Let I, J be fractional ideals of a Noetherian domain A, with $J \neq (0)$. Then $(I \div J)$ is a fractional ideal of A.

Proof. $I \div J$ is closed under addition and multiplication by A, and hence is an A-module. We need to check that it is finitely generated.

First suppose that I, J are A-ideals. For nonzero $j \in J \subseteq A$, we have $j(I \div J) \subseteq I \subseteq A$ by definition; then take generators of I and divide them by j to obtain finitely many generators for $I \div J$. In general, choose $a, b \in A$ such that $aI \subseteq A$ and $bJ \subseteq A$. Then $I \div J = abI \div abJ$ where now abI, abJ are A-ideals. □

Definition 3.9 (invertible)**.** A fractional ideal is *invertible* if $IJ = A$ for some fractional ideal J.

Inverses are unique if they exist: $J = JA = JIJ' = AJ' = J'$.

Lemma 3.10

A fractional ideal I of A is invertible if and only if $I(A \div I) = A$, in which case $A \div I$ is the inverse.

Proof. ($\Rightarrow$): Note $I(A \div I) \subseteq A$ by definition. Suppose $IJ = A$ so that $J \subseteq A \div I$. Then

$$A = IJ \subseteq I(A \div I) \subseteq A,$$

so $IJ = I(A \div I) = A$, and $J = A \div I$ by uniqueness.

The reverse direction is immediate. □

Example 3.11 (noninvertible fractional ideal)

Let $A = \mathbb{Z} + 2i\mathbb{Z}$ which is a subring of $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$. Let $I = 2\mathbb{Z}[i]$ so that $A \div I = \mathbb{Z}[i]$. However, $I(A \div I) = 2\mathbb{Z}[i] \subsetneq A$.

In a DD, all fractional ideals will be invertible, so we had to find a weird example.

3.2 Ideal class group

Fractional ideal multiplication is commutative and associative (w.r.t. addition). Thus, the nonzero fractional ideals of a Noetherian domain form an abelian monoid under multiplication with $A = (1)$. The subset of invertible fractional ideals is an abelian group.

Definition 3.12 (ideal group)**.** Let A be a Noetherian domain. The *ideal group* of A, denoted $\mathcal{I}_A$, is the group of invertible fractional ideals.

Every nonzero principal fractional ideal (x) is invertible, since $(x)(\frac{1}{x}) = A$. Products of principal fractional ideals are principal: $(x)(y) = (xy)$. Thus, the principal fractional ideals are a subgroup $\mathcal{P}_A \subseteq \mathcal{I}_A$.

Definition 3.13 (ideal class group)**.** The quotient $\mathrm{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$ is the *ideal class group* of A.

This is also known as the Picard group $\mathrm{Pic}(A)$ for a Noetherian domain.

Remark 3.14. The ideal class group $\mathrm{cl}(A)$ is trivial if and only if A is a PID.

It turns out that a DD is a UFD if and only if $\mathrm{cl}(A)$ is trivial, i.e. if and only if it is a PID.

4 Properties of Dedekind domains

Let A be a Noetherian domain. Today we will present eight equivalent definitions for DDs and show that our original definition in Proposition 3.1 satisfies them. Pset 2.1 shows the reverse direction.

Lemma 4.1

Let I, J be fractional ideals in A and $\mathfrak{p}$ be a prime ideal. Then $I_\mathfrak{p}, J_\mathfrak{p}$ are fractional ideals of $A_\mathfrak{p}$ with

1. $(I + J)_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p}$
2. $(IJ)_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p}$
3. $(I \div J)_\mathfrak{p} = (I_\mathfrak{p} \div J_\mathfrak{p})$.

Proof. Because I is finitely generated as an A-module, $I_\mathfrak{p} = IA_\mathfrak{p}$ is finitely generated as an $A_\mathfrak{p}$-module and is a fractional $A_\mathfrak{p}$-ideal by Definition 3.4. The same is true for $J_\mathfrak{p}$.

1. $(I + J)_\mathfrak{p} = (I + J)A_\mathfrak{p} = IA_\mathfrak{p} + JA_\mathfrak{p} = I_\mathfrak{p} + J_\mathfrak{p}$. For the second equality, $\subseteq$ is clear, and $\supseteq$ follows from using common denominators.
2. $(IJ)_\mathfrak{p} = (IJ)A_\mathfrak{p} = I_\mathfrak{p} J_\mathfrak{p}$. For the second equality, $\subseteq$ is clear, and $\supseteq$ follows from using common denominators.
3. $(I \div J)_\mathfrak{p} = \{x \in K : xJ \subseteq I\}_\mathfrak{p} = \{x \in K : xJ_\mathfrak{p} \subseteq I_\mathfrak{p}\} = I_\mathfrak{p} \div J_\mathfrak{p}$. □

Actually, all three parts hold for any multiplicative subset S of A; the fact that $S = A - \mathfrak{p}$ was not used.

Theorem 4.2

In a Noetherian domain A, a fractional ideal I is invertible if and only if its localization at every maximal (or prime) ideal is invertible.

Proof. ($\Rightarrow$) Suppose I is invertible, so $I(A \div I) = A$ by Lemma 3.10. For any maximal ideal $\mathfrak{m}$, we have $I_\mathfrak{m}(A_\mathfrak{m} \div I_\mathfrak{m}) = A_\mathfrak{m}$ by Lemma 4.1, so $I_\mathfrak{m}$ is invertible.

($\Leftarrow$) Now suppose $I_\mathfrak{m}$ is invertible for all $\mathfrak{m} \in \operatorname{Max} A$. Then

$$I(A \div I) = \bigcap_{\mathfrak{m}} (I(A \div I))_\mathfrak{m} = \bigcap_{\mathfrak{m}} I_\mathfrak{m}(A_\mathfrak{m} \div I_\mathfrak{m}) = \bigcap_{\mathfrak{m}} A_\mathfrak{m} = A$$

by Corollary 2.10 and Lemma 4.1.

The same proof works for prime ideals instead of maximal ideals. □

Corollary 4.3

In a Dedekind domain A, every nonzero fractional ideal I is invertible.

Proof. The localizations $A_\mathfrak{p}$ at nonzero prime ideals are DVRs. In particular, they are PIDs in which every nonzero fractional ideal $I_\mathfrak{p}$ is invertible. Then by Theorem 4.2, I is invertible. □

Lemma 4.4

In a Noetherian local domain A, a nonzero fractional ideal I is invertible if and only if it is principal.

Proof. ($\Leftarrow$) If $I = (x)$ is principal, then it is invertible with inverse $(\frac{1}{x})$.

($\Rightarrow$) Now suppose I is invertible, and let $\mathfrak{m}$ be the maximal ideal of A. We have $II^{-1} = A$ so there is some linear combination $\sum_{i=1}^n a_i b_i = 1$ with $a_i \in I$, $b_i \in I^{-1}$. Note that each summand $a_i b_i$ lies in $II^{-1} = A$. At least one summand $a_i b_i$ must be a unit because each element in a local ring is a unit or in $\mathfrak{m}$, but $\sum_{i=1}^n a_i b_i = 1 \notin \mathfrak{m}$. Say $a_1 b_1 \in A^\times$. For every $x \in I$, we have $a_1 b_1 x \in (a_1)$ because $b_1 \in I^{-1}$ and $b_1 x \in A$. Then $x = (a_1 b_1)^{-1} a_1 b_1 x \in (a_1)$, which shows $I \subseteq (a_1)$. As $(a_1) \subseteq I$ by construction, $I = (a_1)$ is principal. □

Corollary 4.5

In a Noetherian domain A, a nonzero fractional ideal I is invertible if and only if it is *locally principal*, i.e. all localizations at maximal ideals are principal.

Proof. Combine Theorem 4.2 and Lemma 4.4. □

Lemma 4.6

Let A be a DD and $a \in A$ nonzero. The set of $\mathfrak{p} \in \operatorname{Spec} A$ containing a is finite.

Proof. Consider subsets S, T of $\mathcal{I}_A$ with

$$S := \{I \in \mathcal{I}_A : (a) \subseteq I \subseteq A\}$$
$$T := \{I \in \mathcal{I}_A : A \subseteq I \subseteq (a^{-1})\}.$$

S and T are nonempty because they both contain A, and define partial orders by inclusion. Consider the bijections $\varphi_1 \colon S \to T$ with $I \mapsto I^{-1}$ and $\varphi_2 \colon T \to S$ with $I \mapsto aI$ where φ_1 is order reversing and φ_2 is order preserving. Then $\varphi := \varphi_2 \circ \varphi_1$ is an order-reversing bijection of S. Since A and thus S satisfies ACC by being Noetherian, $\varphi(S)$ satisfies DCC.

Now suppose a lies in infinitely many distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$. Then

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \cdots$$

is a descending chain in S as (a) is contained in all intersections, the ideals are finitely generated (fractional) because $\mathfrak{p}_1$ is, and fractional ideals are invertible in a DD by Corollary 4.3. The chain stabilizes, so there is some $n > 1$ for which

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_{n-1} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n \subseteq \mathfrak{p}_n.$$

In other words, $\mathfrak{p}_n$ contains some $\mathfrak{p}_j$ and there is a chain

$$(0) \subsetneq \mathfrak{p}_j \subsetneq \mathfrak{p}_n$$

contradicting $\dim A \leq 1$. Note that $(0) \subsetneq (a) \subseteq \mathfrak{p}_j$ is how a is used. □

Corollary 4.7

Let I be a nonzero ideal in a DD A. The number of prime ideals that contain I is finite.

Proof. Pick an element of I and apply Lemma 4.6 to it. □

Example 4.8

$A = \mathbb{C}[t]$ is a DD with uncountably many prime ideals $\mathfrak{p}_r = (t - r)$ for $r \in \mathbb{C}$. By Lemma 4.6, any nonzero $f \in \mathbb{C}[t]$ lies in finitely many $\mathfrak{p}_r$. In other words, there are finitely many $r \in \mathbb{C}$ for which $f(r) = 0$, and f has finitely many roots. (This is a sledgehammer.)

Let $\mathfrak{p}$ be a nonzero prime ideal in a DD A with $K = \operatorname{Frac} A$. Let π be a uniformizer for the DVR $A_\mathfrak{p}$, and let I be a nonzero fractional ideal of A. Then $I_\mathfrak{p}$ is a nonzero fractional ideal of $A_\mathfrak{p}$ and of the form (π^n) for some $n \in \mathbb{Z}$. Extend the valuation $\nu_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$ to fractional ideals via $\nu_\mathfrak{p}(I) = n$ and $\nu_\mathfrak{p}((0)) = \infty$. Then $\nu_\mathfrak{p}((x)) = \nu_\mathfrak{p}(x)$. The map

$$\nu_\mathfrak{p} \colon \mathcal{I}_A \to \mathbb{Z}, \qquad I \mapsto \nu_\mathfrak{p}(I)$$

is a group homomorphism, i.e. $\nu_\mathfrak{p}(IJ) = \nu_\mathfrak{p}(I) + \nu_\mathfrak{p}(J)$. It is order-reversing with respect to the partial ordering on $\mathcal{I}_A$ by inclusion and the usual order on $\mathbb{Z}$: if $I \subseteq J$, then $\nu_\mathfrak{p}(I) \geq \nu_\mathfrak{p}(J)$.

Lemma 4.9

Let $\mathfrak{p}$ be a nonzero prime ideal of a DD A. For any ideal $I \subseteq A$, $\nu_\mathfrak{p}(I) = 0$ if and only if $I \not\subseteq \mathfrak{p}$.

In particular, if $\mathfrak{q} \neq \mathfrak{p}$ is another nonzero prime ideal of A, then $\nu_\mathfrak{q}(\mathfrak{p}) = \nu_\mathfrak{p}(\mathfrak{q}) = 0$, by $\dim A \leq 1$.

Proof. If $I \subseteq \mathfrak{p}$, then $\nu_\mathfrak{p}(I) \geq \nu_\mathfrak{p}(\mathfrak{p}) = 1$ is nonzero. If $I \not\subseteq \mathfrak{p}$, then pick $a \in I - \mathfrak{p}$ so that

$$0 = \nu_\mathfrak{p}((a)) \geq \nu_\mathfrak{p}(I) \geq \nu_\mathfrak{p}(A) = 0,$$

where we note $A_\mathfrak{p} = (\pi^0)$ so $\nu_\mathfrak{p}(A) = 0$. □

Corollary 4.10

For any $I \in \mathcal{I}_A$, we have $\nu_{\mathfrak{p}}(I) = 0$ for all but finitely many nonzero $\mathfrak{p} \in \operatorname{Spec} A$.

In particular, for all $x \in K^\times$ we have $\nu_{\mathfrak{p}}(x) = 0$ for all but finitely many $\mathfrak{p}$.

Proof. If $I \subseteq A$, then this follows from Corollary 4.7 and Lemma 4.9. In general for a fractional ideal $\frac{1}{a}I$ with $a \in A$, $I \subseteq A$, we have $\nu_{\mathfrak{p}}(\frac{1}{a}I) = \nu_{\mathfrak{p}}(I) - \nu_{\mathfrak{p}}(a) = 0 - 0 = 0$ for all but finitely many $\mathfrak{p}$. □

Theorem 4.11

The ideal group $\mathcal{I}_A$ for a DD A is isomorphic to the free abelian group generated by the nonzero prime ideals of A. The isomorphism $\mathcal{I}_A \simeq \bigoplus_{\mathfrak{p} \neq (0)} \mathbb{Z}$ is given by

$$\begin{aligned} I &\mapsto (\dots, \nu_{\mathfrak{p}}(I), \dots) \\ \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}} &\hookleftarrow (\dots, e_{\mathfrak{p}}, \dots). \end{aligned}$$

In particular, every ideal in a DD has a unique factorization into prime ideals.

Writing $I = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ and $J = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}}$, we have

$$\begin{aligned} IJ &= \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}} + f_{\mathfrak{p}}} \\ (I \div J) &= \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}} - f_{\mathfrak{p}}} \\ I + J &= \prod_{\mathfrak{p}} \mathfrak{p}^{\min(e_{\mathfrak{p}}, f_{\mathfrak{p}})} = \gcd(I, J) \\ I \cap J &= \prod_{\mathfrak{p}} \mathfrak{p}^{\max(e_{\mathfrak{p}}, f_{\mathfrak{p}})} = \operatorname{lcm}(I, J). \end{aligned}$$

Then $J \supseteq I$ if and only if $e_{\mathfrak{p}} \geq f_{\mathfrak{p}}$ for all nonzero $\mathfrak{p} \in \operatorname{Spec} A$. So $J \supseteq I$ if and only if J divides I. It is always true that to divide ($JH = I$) implies to contain ($J \supseteq I$), but the reverse is only true for DD.

Proof. The map is well defined because all but finitely many entries of the direct sum are 0 by Corollary 4.10.

As the maps $I \mapsto \nu_{\mathfrak{p}}(I)$ and $\mathfrak{p}^{e_{\mathfrak{p}}} \hookleftarrow e_{\mathfrak{p}}$ are group homomorphisms, both maps in the theorem statement for $\mathcal{I}_A \simeq \bigoplus_{\mathfrak{p}} \mathbb{Z}$ are group homomorphisms. The forward map is injective because if $\nu_{\mathfrak{p}}(I) = \nu_{\mathfrak{p}}(J)$, then $I_{\mathfrak{p}} = J_{\mathfrak{p}}$. If this holds for every $\mathfrak{p}$ then $I = \bigcap_{\mathfrak{p}} I_{\mathfrak{p}} = \bigcap_{\mathfrak{p}} J_{\mathfrak{p}} = J$.

For surjectivity, given $(\dots, e_{\mathfrak{p}}, \dots)$ with all but finitely many entries zero, consider $\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$. It is indeed true that $\nu_{\mathfrak{q}}(\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}) = \sum_{\mathfrak{p}} e_{\mathfrak{p}} \nu_{\mathfrak{q}}(\mathfrak{p}) = e_{\mathfrak{q}}$. □

Corollary 4.12

A DD is a UFD if and only if it is a PID, or equivalently if and only if $\operatorname{cl}(A)$ is trivial.

Proof. PIDs are UFDs, so it remains to show the other direction. It suffices to show that every prime ideal is principal. Suppose $\mathfrak{p}$ is a nonzero prime ideal in a DD that is a UFD. Pick a nonzero element $a \in \mathfrak{p}$ and let $a = p_1 \cdots p_n$ be the factorization of a into irreducibles in the UFD A. Then $\mathfrak{p}$ contains and therefore divides $(a) = (p_1)\cdots(p_n)$, so $\mathfrak{p}$ divides and therefore contains some (p_i). However, (p_i) is a nonzero prime ideal (because p_i is irreducible) so $\mathfrak{p} = (p_i)$ is principal. □

Here is a summary of the properties of a Dedekind domain from Lecture Notes 3.

Theorem 4.13 (Dedekind domain)

For an integral domain A, TFAE:

1. A is an integrally closed Noetherian domain of dimension at most one.
2. A is Noetherian and its localizations $A_{\mathfrak{p}}$ at nonzero prime ideals are DVRs.
3. Every nonzero ideal in A is invertible.
4. Every nonzero ideal in A is a (finite) product of prime ideals.
5. A is Noetherian and "to contain is to divide" holds for A-ideals.
6. For every ideal $I \subseteq A$ there is an ideal $J \subseteq A$ such that IJ is principal.
7. Every quotient A/I of A by a nonzero ideal I is a principal ideal ring.
8. For every nonzero ideal $I \subseteq A$ and nonzero $a \in I$ we have $I = (a, b)$ for some $b \in I$.

5 Separability and étale algebras

5.1 Separability

For a polynomial $f = \sum_i a_i x^i \in A[x]$, define $f' := \sum_i i a_i x^{i-1} \in A[x]$.

Definition 5.1 (separable polynomial). Let K be a field. A polynomial $f \in K[x]$ is *separable* if as ideals $(f, f') = (1)$. Otherwise, f is *inseparable*.

Example 5.2

For $K = \mathbb{F}_p(t)$, the polynomial $x^p - t$ is inseparable.

Definition 5.3 (separable element). Let L/K be an algebraic extension. We call $\alpha \in L$ *separable* if $f(\alpha) = 0$ for some separable f. We say that L/K is *separable* if every $\alpha \in L$ is separable over K.

Lemma 5.4

An **irreducible** polynomial $f \in K[x]$ is inseparable if and only if $f' = 0$.

Proof. Since f' has lower degree than f, it has common roots with f irreducible if and only if $f' = 0$. □

Corollary 5.5

Let $f \in K[x]$ be irreducible and $\operatorname{char} K = p$. Then $f(x) = g(x^{p^n})$ for some separable g and $n \geq 0$ (uniquely determined by f).

Corollary 5.6

If $\operatorname{char} K = 0$, then every irreducible $f \in K[x]$ is separable.

Lemma 5.7

Let $L = K(\alpha)$ be an algebraic extension of K in $\overline{K}$, and let $f \in K[x]$ the minimal polynomial of α over K. Then

$$\#\operatorname{Hom}_K(L, \overline{K}) = \#\{\beta \in \overline{K} : f(\beta) = 0\} \leq [L : K] = \deg f$$

with equality if and only if α is separable over K.

Proof. Each element of $\operatorname{Hom}_K(L, \overline{K})$ is uniquely determined by the image of α, which must be sent to a root β of $f(x)$ in $\overline{K}$. The number of roots equals $[L : K] = \deg f$ when f, and thus α, is separable over K. □

Definition 5.8 (separable degree)**.** Let L/K be a finite extension of fields. The *separable degree* of L/K is

$$[L : K]_s \coloneqq \#\operatorname{Hom}_K(L, \overline{K}).$$

The *inseparable degree* of L/K is

$$[L : K]_i \coloneqq [L : K]/[L : K]_s.$$

The inseparable degree turns out to be an integer (Corollary 5.24).

Theorem 5.9

Let L/K be an algebraic extension and $\phi_K \colon K \to \Omega$ be an embedding into an algebraically closed field. Then ϕ_K extends to an embedding $\phi_L \colon L \to \Omega$.

Proof. We use Zorn's lemma. Define a partial ordering on the set $\mathcal{F}$ of pairs (F, ϕ_F) where

- F/K is a subextension of L/K,
- $\phi_F \colon F \to \Omega$ extends $\phi_K \colon K \to \Omega$.

We say $(F_1, \phi_{F_1}) \leq (F_2, \phi_{F_2})$ whenever $F_1 \subseteq F_2$ and ϕ_{F_2} extends ϕ_{F_1}. Note $\mathcal{F}$ is nonempty because $(K, \phi_K) \in \mathcal{F}$. For any totally ordered chain $\mathcal{C} \subseteq \mathcal{F}$, there is a maximal element (E, ϕ_E) with $E \coloneqq \bigcup\{F : (F, \phi_F) \in \mathcal{C}\}$, and $\phi_E \colon E \to \Omega$ by $x \mapsto \phi_F(x)$ for any $F \ni x$.

By Zorn's lemma, $\mathcal{F}$ contains a maximal element (M, ϕ_M); we claim that $M = L$. Suppose not, and let $\alpha \in L - M$. Consider $F = M(\alpha) \subseteq L$, where $M \subsetneq M(\alpha)$. Extend ϕ_M to ϕ_F by letting ϕ_F be any root of $\alpha_M(f)$, where $\alpha(f) \in \Omega[x]$ is obtained by applying ϕ_M to the minimal polynomial $f \in M[x]$ of α over M. Then (M, ϕ_M) is dominated by (F, ϕ_F), a contradiction. □

Lemma 5.10

Let $L/F/K$ be a tower of finite extensions and $\overline{K}$ be an algebraic closure containing L. Then

$$\#\operatorname{Hom}_K(L, \overline{K}) = \#\operatorname{Hom}_K(F, \overline{K})\#\operatorname{Hom}_F(L, \overline{K}).$$

Corollary 5.11

Let $L/F/K$ be a tower of finite extensions. Then

$$[L:K]_s = [L:F]_s[F:K]_s$$
$$[L:K]_i = [L:F]_i[F:K]_i.$$

Theorem 5.12

Let L/K be a finite extension. TFAE:

1. L/K is separable.
2. $[L:K]_s = [L:K]$.
3. $L = K(\alpha)$ for some $\alpha \in L$ separable over K.
4. $L \simeq K[x]/(f)$ for some irreducible separable $f \in K[x]$.

Corollary 5.13

Let L/K be a finite extension. Then $[L:K]_s \leq [L:K]$ with equality if and only if L/K is separable.

Corollary 5.14

Let $L/F/K$ be a tower of algebraic extensions. L/K is separable if and only if L/F and F/K separable.

Corollary 5.15

Let L/K be an algebraic extension. Then $F \coloneqq \{\alpha \in L : \alpha \text{ separable over } K\}$ is a separable field extension.

Definition 5.16 (separable closure)**.** Let L/K be an algebraic extension.

$$F \coloneqq \{\alpha \in L : \alpha \text{ separable over } K\}$$

is the *separable closure of* K *in* L. When L is an algebraic closure, it is called the *separable closure of* K and denoted by K^{sep}.

Definition 5.17 (perfect)**.** A field is *perfect* if every algebraic extension is separable.

Example 5.18

Characteristic 0 fields and finite fields are perfect.

Definition 5.19 (separably closed)**.** K is *separably closed* if no nontrivial separable extensions of K exist.

The following theorem can be used to show that finite fields are perfect.

Theorem 5.20

If $\operatorname{char} K = p > 0$, then K is perfect if and only if $K = K^p$, or equivalently, if and only if $x \mapsto x^p$ is an automorphism.

Definition 5.21 (purely inseparable)**.** An algebraic extension is *purely inseparable* if $[L : K]_s = 1$.

The trivial extension is separable and purely inseparable. From Example 5.2 $x^p - t$ is a purely inseparable extension of degree p.

Proposition 5.22

Let $\operatorname{char} K = p > 0$. If L/K is a purely inseparable extension of degree p, then $L = K(a^{1/p}) \simeq K[x]/(x^p - a)$ for some $a \in K - K^p$.

Theorem 5.23

Let L/K be an algebraic extension and F be the separable closure of K in L. Then L/F is purely inseparable.

Proof. If L/K is separable, then we are done because $L = F$ and the trivial extension L/L is purely separable. Otherwise, we have $\operatorname{char} K = p > 0$. Fix an algebraic closure $\overline{K}$ of K containing L. Let $\alpha \in L - F$ have minimal polynomial f over F. By Corollary 5.5, we can write $f(x) = g(x^{p^n})$ with $g \in K[x]$ separable and $n \geq 0$. We need $\deg g = 1$, as otherwise there would be a separable element not in F. Then $f(x) = x^{p^n} - a$ for some $a \in F$, or $f(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$ for some $\alpha \in F$. Thus

$$\# \operatorname{Hom}_F(F(\alpha), \overline{K}) = 1.$$

Since f only has one root, there is only one place to send α. We can continue this process if there are more elements in $L - F(\alpha)$, and the upshot is that

$$[L : F]_s = \# \operatorname{Hom}_F(L, \overline{K}) = 1$$

which is the definition of purely inseparable. □

Corollary 5.24

Every algebraic extension L/K can be written uniquely as $L/F/K$ with F/K separable and L/F purely inseparable.

Proof. Take F to be the separable closure of K in L. □

Corollary 5.25

The inseparable degree is a power of $\operatorname{char} K = p$. (This is also true for $p = 0$, using $0^0 = 1$.)

5.2 Étale algebras

Every finite separable extension L/K looks like $L = K[x]/(f)$ for some $f \in K[x]$.

Let $f = f_1 \cdots f_n$ be the irreducible factorization in $K[x]$. Suppose f is separable so that the f_i are distinct. Then

$$K[x]/(f) = K[x]/(f_1 \cdots f_n) \simeq K[x]/(f_1) \times \cdots \times K[x]/(f_n)$$

by the Chinese remainder theorem. This is a finite product of finite separable extensions of K.

Definition 5.26 (étale). An *étale* K-algebra is a K-algebra L which is isomorphic to a finite product of finite separable field extensions.

Remark 5.27. Finite products and finite direct sums are same as K-vector spaces but not as K-algebras. A direct sum sends $1 \mapsto (1, 0, \ldots, 0)$, but for a homomorphism we need $1 \mapsto (1, \ldots, 1)$. Products have projection maps, so it's important we are using ×.

Example 5.28

If $K = K^{\text{sep}}$, then every étale K-algebra is isomorphic to $K^n = K \times \cdots \times K$ for some $n \geq 1$.

Étale algebras are *semisimple* algebras. A *simple* ring is nonzero and has no nonzero proper ideals, and a *semisimple* ring is a finite product of simple rings. Note that a **commutative** ring is simple if and only if it is a field. Ideals in a semisimple commutative ring $R = \prod R_i$ are a product of some of the R_i.

Proposition 5.29

Let $A = \prod K_i$ be a K-algebra that is a product of field extensions K_i/K. Every surjective homomorphism $\varphi\colon A \to B$ of K-algebras corresponds to a projection onto a subproduct.

Corollary 5.30

The decomposition of an étale K-algebra into a product of fields is unique up to isomorphism.

Definition 5.31 (base change). Let $\varphi\colon A \to B$ be a ring homomorphism (so B is an A-module). Let M be any A-module. The *base change* of M from A to B is the B-module $M \otimes_A B$ with $b(m \otimes b') := m \otimes bb'$.

If M is an A-algebra, then $M \otimes_A B$ is a B-algebra.

Example 5.32

$M_{\mathfrak{p}} = M \otimes_A A_{\mathfrak{p}}$.

Proposition 5.33

Suppose L is an étale K-algebra and K'/K is **any** field extension. Then $L \otimes_K K'$ is an étale K'-algebra with the same dimension as L.

Proof. WLOG L is a field, or L is a product of fields and we can apply this reasoning to each factor. Then $L \simeq K[x]/(f)$ for some irreducible separable f. Let $f = f_1 \cdots f_n \in K'[x]$ be the factorization into irreducibles. Then

$$L \otimes_K K' \simeq K'[x]/(f) \simeq \prod_i K'[x]/(f_i)$$

because f is separable. Thus $L \otimes_K K'$ is an étale K'-algebra, and the dimension is preserved: $\dim_K L = \deg f = \dim_{K'} K'[x]/(f)$. □

Example 5.34

Any finite dimensional $\mathbb{R}$-vector space V is an étale $\mathbb{R}$-algebra (say $\simeq \mathbb{R}^n$ with multiplication defined component-wise w.r.t. some basis). Then $V \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C}^n$ is an étale $\mathbb{C}$-algebra of the same dimension.

Corollary 5.35

Let $L = K[x]/(f)$ be a finite separable extension of K with $f \in K[x]$ irreducible and separable. Let K'/K be any field extension, and let $f = f_1 \cdots f_n$ be the factorization of f into distinct irreducible $f_i \in K'[x]$. Then there is an isomorphism of étale K'-algebras

$$L \otimes_K K' = K'[x]/(f) \simeq \prod_i K'[x]/(f_i).$$

Theorem 5.36

Let L be a commutative K-algebra of finite dimension and assume $\dim L < \# K$. TFAE:

1. L is an étale K-algebra.
2. Every element of L is separable over K.
3. $L \otimes_K K'$ is reduced for every extension K'/K.
4. $L \otimes_K K'$ is semisimple for every extension K'/K.
5. $L = K[x]/(f)$ for some separable $f \in K[x]$.

Definition 5.37 (reduced). An ring element $\alpha \in R$ is *nilpotent* if $\alpha^n = 0$ for some n. R is *reduced* if it contains no nonzero nilpotents.

6 Dedekind extensions

6.1 Norm and trace

Definition 6.1 (norm, trace). Let B/A be an extension of rings with B a free A-module of finite rank (so $B \simeq A^n$). Then the *norm* $\mathrm{N}_{B/A}(b)$ and *trace* $\mathrm{T}_{B/A}(b)$ are the determinant and trace of the A-linear map

$$B \xrightarrow{\times b} B, \quad x \mapsto bx.$$

As maps, we have $\mathrm{N}_{B/A}\colon B^\times \to A^\times$ (multiplicative group) and $\mathrm{T}_{B/A}\colon B \to A$ (additive group).

For $x = (x_1, x_2) \in B_1 \times B_2$,

$$\mathrm{N}_{B_1 \times B_2/A}(x) = \mathrm{N}_{B_1/A}(x_1)\,\mathrm{N}_{B_2/A}(x_2)$$
$$\mathrm{T}_{B_1 \times B_2/A}(x) = \mathrm{T}_{B_1/A}(x_1) + \mathrm{T}_{B_2/A}(x_2).$$

Example 6.2

Let $A = \mathbb{R}$ and $B = \mathbb{C}$ which has an A-module basis of $\{1, i\}$. Let $b = 2 + 3i$. Then

$$\mathrm{N}_{\mathbb{C}/\mathbb{R}}(2+3i) = \det \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix} = 13$$
$$\mathrm{T}_{\mathbb{C}/\mathbb{R}}(2+3i) = \operatorname{tr} \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix} = 4.$$

Norm and trace are well-behaved with respect to base change.

Lemma 6.3

Let B/A be a free A-module of rank n. Given $\varphi\colon A \to A'$, the base change $B' = B \otimes_A A'$ is a free A'-module of rank n. Then

$$\varphi(\mathrm{N}_{B/A}(b)) = \mathrm{N}_{B'/A'}(b \otimes 1)$$
$$\varphi(\mathrm{T}_{B/A}(b)) = \mathrm{T}_{B'/A'}(b \otimes 1).$$

Theorem 6.4

Let K be a field with Ω as the separable closure, and let L be an étale K-algebra. Then

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha)$$
$$\mathrm{T}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_K(L,\Omega)} \sigma(\alpha).$$

Proof. $L \otimes_k \Omega \to \prod_\sigma \Omega = \Omega^n$ sends $\alpha \otimes 1 \mapsto (\sigma_1(\alpha), \dots, \sigma_n(\alpha))$. □

Proposition 6.5

Let L/K be a finite extension of fields and $\overline{K}$ be an algebraic closure containing L. Suppose $\alpha \in L^\times$ has minimal polynomial $f \in K[x]$ where $f(x) = \prod_{i=1}^d (x - \alpha_i) \in \overline{K}[x]$, $e \coloneqq [L : K(\alpha)]$. Then

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^d \alpha_i^e, \quad \mathrm{T}_{L/K}(\alpha) = e \sum_{i=1}^d \alpha_i.$$

In particular, if $f(x) = \sum_{i=1}^d a_i x^i$, then $\mathrm{N}_{L/K}(\alpha) = (-1)^{de} a_0^e$ and $\mathrm{T}_{L/K}(\alpha) = -e a_{d-1}$

Proof. See pset 3.5. □

Corollary 6.6

Let A be a domain with $K = \operatorname{Frac} A$, and let L/K be a finite extension. If $\alpha \in L$ is integral over A, then $\mathrm{N}_{L/K}(\alpha) \in A$ and $\mathrm{T}_{L/K}(\alpha) \in A$.

Proof. This follows from $\mathrm{N}_{L/K}(\alpha) = (-1)^{de}a_0^e$ and $\mathrm{T}_{L/K}(\alpha) = -ea_{d-1}$ in Proposition 6.5, and how α integral over A means $f(x) = \sum_{i=1}^d a_i x^i \in A[x]$ by Proposition 1.30. □

Theorem 6.7 (Transitivity of norm and trace)

Given $C/B/A$ where C is free of finite rank over B, and B is finite rank over A, then

$$\mathrm{N}_{C/A} = \mathrm{N}_{B/A} \circ \mathrm{N}_{C/B}$$
$$\mathrm{T}_{C/A} = \mathrm{T}_{B/A} \circ \mathrm{T}_{C/B}$$

6.2 Dual modules, pairings, and lattices

Definition 6.8 (dual module). For an A-module, M, its *dual module* is the A-module

$$M^\vee = \mathrm{Hom}_A(M, A)$$

with scalar multiplication $(af)(m) = af(m)$.

Given $\varphi\colon M \to N$, there is a natural map $\varphi^\vee\colon N^\vee \to M^\vee$ defined by $\varphi^\vee(g)(m) = g(\varphi(m))$ for $g \in N^\vee$.

The dual preserves the identity morphism and is compatible with composition, so we get a covariant functor from the category of A-modules to itself. It is also compatible with sums: $(M \oplus N)^\vee \simeq M^\vee \oplus N^\vee$ with inverse maps $\varphi \mapsto (m \mapsto \varphi(m, 0), n \mapsto \varphi(0, n))$ and $((m, n) \mapsto \phi(m) + \psi(n)) \leftarrow\!\shortmid (\phi, \psi)$.

Remark 6.9. If A is a field and M is finitely generated (i.e. finite dimensional vector space), then $M^\vee$ is the dual space and $M^{\vee\vee} \simeq M$. However, this is not true in general.

Proposition 6.10

Let A be an integral domain with $K = \operatorname{Frac} A$, and let M be a nonzero A-submodule of K. Then

$$M^\vee \simeq A \div M := \{x \in K : xM \subseteq A\}.$$

In particular if M is an invertible fractional ideal, then $M^\vee \simeq M^{-1}$ and $M^{\vee\vee} \simeq M$.

Example 6.11

As a $\mathbb{Z}$-module, $\mathbb{Q}$ is not finitely generated. However, $\mathbb{Q}^\vee = \{0\}$ because there are no nontrivial $\mathbb{Z}$-linear homomorphisms $\mathbb{Q} \to \mathbb{Z}$. Consequently $\mathbb{Q}^{\vee\vee} = \{0\}$ (although as $\mathbb{Q}$-modules, $\mathbb{Q} \simeq \mathbb{Q}^\vee \simeq \mathbb{Q}^{\vee\vee}$). Similarly, the dual of any finite abelian group ($\mathbb{Z}$-module) is $\{0\}$, as is its double dual.

Theorem 6.12

Let M be a free A-module of rank n. Then $M^\vee$ is also a free A-module of rank n, and each A-basis $(e_1, \ldots, e_n)$ of M uniquely determines a dual basis $(e_1^\vee, \ldots, e_n^\vee)$ with $e_i^\vee(e_j) = \delta_{ij}$.

Proof. If $n = 0$, then $M = M^\vee = \{0\}$. Now assuming $n \geq 1$, fix $e = (e_1, \ldots, e_n)$ an A-basis for M. For $a := (a_1, \ldots, a_n) \in A^n$, define $f_a \in M^\vee$ by $f_a(e_i) = a_i$ and extending A-linearly. The map $a \mapsto f_a$ is an A-module map $A^n \to M^\vee$ with inverse $f \mapsto (f(e_1), \ldots, f(e_n))$, so it's an isomorphism and $M^\vee \simeq A^n$.

Now let $e_i^\vee := f_{\hat{i}}$ where $\hat{i} = (0, \ldots, 0, 1, 0, \ldots, 0) \in A^n$. Then $e^\vee := (e_1^\vee, \ldots, e_n^\vee)$ is an A-basis for $M^\vee$ since $(\hat{1}, \ldots, \hat{n})$ is a basis for A^n, and $e_i^\vee(e_j) = \delta_{ij}$. The basis $e^\vee$ is uniquely determined by e: it must be the image of $(\hat{1}, \ldots, \hat{n})$ under $a \mapsto f_a$. □

Definition 6.13 (bilinear pairing)**.** Let M be an A-module. A *bilinear pairing* on M is an A-linear map $\langle \cdot, \cdot \rangle \colon M \times M \to A$, meaning for all $\lambda \in A$ and $u, v, w \in M$ that

$$\begin{aligned} \langle u + v, w \rangle &= \langle u, w \rangle + \langle v, w \rangle \\ \langle v, v + w \rangle &= \langle u, v \rangle + \langle u, w \rangle \\ \langle \lambda u, v \rangle &= \langle u, \lambda v \rangle = \lambda \langle u, v \rangle. \end{aligned}$$

It is

- *symmetric* if $\langle v, w \rangle = \langle w, v \rangle$
- *skew-symmetric* if $\langle v, w \rangle = -\langle w, v \rangle$
- *alternating* if $\langle v, v \rangle = 0$ (equivalent to skew-symmetric if char $A \neq 2$)
- *nondegenerate* if the induced map $\varphi \colon M \to M^\vee$ by $m \mapsto (n \mapsto \langle m, n \rangle)$ has trivial kernel
- *perfect* if the induced map is an isomorphism.

Example 6.14

Perfect implies nondegenerate, but the converse is not true. For example, $\langle x, y \rangle := 2xy$ is nondegenerate but not a perfect pairing on $\mathbb{Z}$.

Proposition 6.15

Let M be a free A-module of rank n with a perfect pairing $\langle \cdot, \cdot \rangle$. For each A-basis $(e_1, \ldots, e_n)$ of M there is a unique A-basis $(e_1', \ldots, e_n')$ of M with $\langle e_i', e_j \rangle = \delta_{ij}$.

Definition 6.16 (lattice)**.** Let A be an integral domain, $K = \operatorname{Frac} A$, and V be a K-vector space. A *(full) A-lattice* in V is a finitely generated A-submodule M in V that spans V as a K-vector space.

Remark 6.17. A-lattices do not need to be free A-modules, although this is true for $A = \mathbb{Z}$ or another PID.

Definition 6.18. Let A be a Noetherian domain and $K = \operatorname{Frac} A$. Let V be a K-vector space with a perfect pairing $\langle \cdot, \cdot \rangle$. If M is an A-lattice in V, its *dual lattice* (with respect to the perfect pairing) is the A-module

$$M^* := \{x \in V : \langle x, m \rangle \in A, \ \forall m \in M\}.$$

M^* is an A-submodule, and in fact $M^* \simeq M^\vee$. In particular, this implies M^* is finitely generated.

Theorem 6.19

M^* is an A-lattice in V isomorphic to $M^\vee$.

Corollary 6.20

If M_1, M_2 are A-lattices in K-vector space V_1, V_2 with pairings $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$, then $\langle\cdot,\cdot\rangle_1 + \langle\cdot,\cdot\rangle_2$ is a perfect pairing on $V_1 \oplus V_2$, and $(M \oplus N)^* \simeq M^* \oplus N^*$.

Corollary 6.21

If M is a **free** A-lattice in V with basis $(e_1, \ldots, e_n)$, then M^* is also a free A-lattice with basis $(e_1^*, \ldots, e_n^*)$ satisfying $\langle e_i^*, e_j\rangle = \delta_{ij}$.

Is $M^{**} = M$? No in general, but yes if A is a DD and the perfect pairing is symmetric.

Lemma 6.22

Let S be a multiplicative set of a Noetherian domain A, and let M be an A-lattice in $\operatorname{Frac} A$-vector space V. Then $S^{-1}M$ and $S^{-1}M^*$ are $S^{-1}A$-lattices in V with $(S^{-1}M)^* = S^{-1}M^*$.

Proposition 6.23

Let A be a DD and $K = \operatorname{Frac} A$. Let V be a K-vector space of finite dimension with a symmetric perfect pairing. For an A-lattice M in V, we have $M^{**} = M$.

Proof. It suffices to show that $(M^{**})_\mathfrak{p} = M_\mathfrak{p}$ for all maximal ideals $\mathfrak{p}$. We have $(M^{**})_\mathfrak{p} = M_\mathfrak{p}^{**}$ by Lemma 6.22, so it suffices to prove the proposition with A replaced by $A_\mathfrak{p}$ which is a DVR.

Thus we may assume A is a DVR; as M and M^* are torsion-free modules over a PID, they are free A-modules. Choose an A-module basis $(e_1, \ldots, e_n)$ for M. Let $(e_1^*, \ldots, e_n^*)$ be the unique A basis for M^* with $\langle e_i^*, e_j\rangle = \delta_{ij}$. Now let $(e_1^{**}, \ldots, e_n^{**})$ be the unique A-basis for M^{**} with $\langle e_i^{**}, e_j^*\rangle = \delta_{ij}$. By symmetry, $\langle e_i, e_j^*\rangle = \delta_{ij}$, so $e_i = e_i^{**}$ by uniqueness. Since M and M^{**} have the same basis, they are equal. □

6.3 Extensions of Dedekind domains

Proposition 6.24

Let A be a DD and $K = \operatorname{Frac} A$. Let L/K be a finite extension and B be the integral closure of A in L. (**AKLB setup**)

Every $x \in L$ can be written as $\frac{b}{a}$ with $b \in B, a \in A$. In particular, B spans L as a K-vector space.

Proof. For $\alpha \in L$, we clear denominators in its minimal polynomial over K to get

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

with $a_i \in A$. We can make this monic by replacing x with $\frac{x}{a_n}$ and multiplying by a_n^{n-1} to get

$$a_n^{n-1} g\left(\frac{x}{a_n}\right) = x^n + a_{n-1}x^{n-1} + a_n a_{n-2} x^{n-2} + \cdots + a_n^{n-1} a_0.$$

This has $a_n\alpha$ as a root, so $a_n\alpha \in B$ and $\alpha = \frac{b}{a_n}$ for some $b \in B$ and $a_n \in A$.

B generates L as a K-vector space, as $\alpha = b \cdot \frac{1}{a_n}$ for $\frac{1}{a_n} \in K$. Also $B \subseteq L \subseteq \operatorname{Frac} B$ implies $L = \operatorname{Frac} B$. □

Proposition 6.25

AKLB. Then $\mathrm{N}_{L/K}(b) \in A$ and $\mathrm{T}_{L/K}(b) \in A$ for all $b \in B$.

Definition 6.26 (trace pairing)**.** Let B/A be a ring extension with B a free A-module of finite rank. The *trace pairing* on B is $\langle x, y\rangle_{B/A} \coloneqq \mathrm{T}_{B/A}(xy)$. (Think $B = L$, $A = K$.)

Theorem 6.27

Let L be a commutative K-algebra of finite dimension. The trace pairing $\langle \cdot, \cdot\rangle_{L/K}$ is a symmetric bilinear pairing. It is a perfect pairing if and only if L is a finite étale K-algebra.

Proposition 6.28

AKLB. B is an A-lattice in L. In particular, it is finitely generated as an A-module.

Proof. Let $(e_1, \ldots, e_n)$ be a basis for L inside B. Let $M \subseteq B$ be the A-span of this basis. The dual lattice M^* contains

$$B^* \coloneqq \{x \in L : \langle x, b\rangle_{L/K} \in A,\ \forall b \in B\}.$$

By Proposition 6.25, $B \subseteq B^*$, so

$$M \subseteq B \subseteq B^* \subseteq M^*.$$

M^* is an A-lattice by Theorem 6.19, hence finitely generated and Noetherian. All of its A-submodules including B are finitely generated in L, i.e. an A-lattice. □

Theorem 6.29

AKLB. B is a DD.

In particular, B is integrally closed, a finitely generated Noetherian ring, and $\dim B \leq \dim A \leq 1$.

The ring of integers of a number field is a DD, as it is the integral closure of $\mathbb{Z}$.

In the AKLB setup, recall that A is a DD, $K = \operatorname{Frac} A$, and L/K is finite separable. B is the integral closure of A in L and also a DD with $L = \operatorname{Frac} B$.

As shorthand, "prime of $A/B/K/L$" means a **nonzero** prime ideal, or a maximal ideal. From now on we assume $A \neq K$ because DD stuff becomes trivial in that case.

Let $\mathfrak{p}$ be a prime of A, and suppose its extension in B factors as

$$\mathfrak{p}B = \prod_{\mathfrak{q} \in \operatorname{Spec} B} \mathfrak{q}^{e_\mathfrak{q}}.$$

Definition 6.30 (ramification index, residue degree)**.** The exponent $e_\mathfrak{q}$ in this factorization is the *ramification index* of $\mathfrak{q}$. The *residue degree* is $f_\mathfrak{q} \coloneqq [B/\mathfrak{q} : A/\mathfrak{p}]$.

More specifically, we can write $e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{p}}$ if we have a tower of extensions. For just one extension B/A, it is unambiguous because each $\mathfrak{q} \subset B$ has one $\mathfrak{p} \subset A$ lying underneath it by $\mathfrak{p} = \mathfrak{q} \cap A$ (although $\mathfrak{p}$ may have multiple $\mathfrak{q}$ lying over it).

Lemma 6.31

Let $C/B/A$ be a tower of DDs corresponding to $M/L/K$ a tower of finite separable extensions (B, C are the integral closures of A in L, M). If $\mathfrak{r}$ is a prime of M above $\mathfrak{q}$ a prime of L above $\mathfrak{p}$ a prime of K ($\mathfrak{q} = \mathfrak{r} \cap B$, $\mathfrak{p} = \mathfrak{r} \cap A$), then $e_{\mathfrak{r}/\mathfrak{p}} = e_{\mathfrak{r}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{r}/\mathfrak{p}} = f_{\mathfrak{r}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}$.

Example 6.32

Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $L = \mathbb{Q}(i)$, where $[L : K] = 2$. Then $B = \mathbb{Z}[i]$.

The prime $\mathfrak{p} = (5) \subset \mathbb{Z}$ factors in $\mathbb{Z}[i]$ as

$$5\mathbb{Z}[i] = (2 + i)(2 - i),$$

so $e_{(2+i)} = 1$ and $e_{(2-i)} = 1$ because they have exponent 1. The residue field $A/\mathfrak{p} = \mathbb{Z}/(5)$ is isomorphic to $\mathbb{F}_5$, as is $B/\mathfrak{q} = \mathbb{Z}[i]/(2 + i)$, so $f_{(2+i)} = 1$ and similarly $f_{(2-i)} = 1$.

The prime $\mathfrak{p} = (7) \subset \mathbb{Z}$ stays prime in $\mathbb{Z}[i]$:

$$7\mathbb{Z}[i] = (7).$$

Then $e_{(7)} = 1$ and $f_{(7)} = 2$ because $\mathbb{Z}/(7) \simeq \mathbb{F}_7$ but $\mathbb{Z}[i]/(7) \simeq \mathbb{F}_{49}$. It is a degree 2 extension of $\mathbb{F}_7$, and in general $B/\mathfrak{q}$ is an extension of $A/\mathfrak{p}$.

The prime $\mathfrak{p} = (2) \subset \mathbb{Z}$ factors as

$$2\mathbb{Z}[i] = (1 + i)^2.$$

Here $e_{(1+i)} = 2$ and $f_{(1+i)} = 1$ because $\mathbb{Z}/(2) \simeq \mathbb{F}_2 \simeq \mathbb{Z}[i]/(1 + i)$.

We compute $\sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$:

$$\sum_{\mathfrak{q}|(5)} e_{\mathfrak{q}} f_{\mathfrak{q}} = 1 \cdot 1 + 1 \cdot 1 = 2$$

$$\sum_{\mathfrak{q}|(7)} e_{\mathfrak{q}} f_{\mathfrak{q}} = 1 \cdot 2 = 2$$

$$\sum_{\mathfrak{q}|(2)} e_{\mathfrak{q}} f_{\mathfrak{q}} = 2 \cdot 1 = 2$$

In all cases, it equals $[L : K] = [\mathbb{Q}(i) : \mathbb{Q}] = 2$, which is not a coincidence.

Example 6.33

Let $A = \mathbb{R}[x]$, $K = \mathbb{R}(x)$, and $L = K(\sqrt{x^3+3x})$. Then $B = \mathbb{R}[x,y]/(y^2 - x^3 - 3x)$, and $[L : K] = 2$ because we're adjoining a square root.

The prime $(x-1)$ factors in B as

$$(x-1) = (x-1, y-2)(x-1, y+2)$$

since $y^2 - 4 = x^3 + 3x - 4 \in (x-1)$. Then $e_{(x-1,y\pm 2)} = 1$ and $f_{(x-1,y\pm 2)} = 1$ because $[B/(x-1,y-2) : A/(x-1)] = [\mathbb{R} : \mathbb{R}] = 1$.

The prime $(x+1)$ remains prime in B because $y^2 = -4$ has no solutions in $\mathbb{R}$. Then $e_{(x+1)} = 1$, $f_{(x+1)} = 2$.

The prime (x) factors in B as

$$(x) = (x, y)^2$$

so $e_{(x,y)} = 2$, $f_{(x,y)} = 1$.

Lemma 6.34

AKLB. Let $\mathfrak{p}$ be a prime of A. The dimension of $B/\mathfrak{p}B$ as an $A/\mathfrak{p}$-vector space is equal to $[L : K]$, the dimension of L as a K-vector space.

Proof. Localize "at $\mathfrak{p}$": $B_\mathfrak{p} := S^{-1}B$ as an A-module where $S = A - \mathfrak{p}$. Then $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = S^{-1}A/(\mathfrak{p}S^{-1}A) \simeq A/\mathfrak{p}$ and $B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p} = S^{-1}B/(\mathfrak{p}S^{-1}B) \simeq B/\mathfrak{p}B$. We have reduced to showing the lemma for for A a DVR, and in particular a PID.

By Proposition 6.28, B is finitely generated as an A-module, and torsion free by being an integral domain containing A. By the structure theorem, B is free of finite rank over A. On the other hand, we know by Proposition 6.24 that B spans L, so any A-basis for B is a K-basis for L.

This means B has rank $n := [L : K]$ as a free A-module. Then $\mathfrak{p}B \simeq \mathfrak{p}A^n \simeq (\mathfrak{p}A)^n$ is an isomorphisms of A-modules, and $B/\mathfrak{p}B \simeq A^n/(\mathfrak{p}A)^n \simeq (A/\mathfrak{p})^n$ is an isomorphism of $A/\mathfrak{p}$-modules. □

Example 6.35

Let $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$, and consider $\mathfrak{p} = (2)$. Then $\mathfrak{p}B = 2\mathbb{Z}[i] = (1+i)^2$ and $B/\mathfrak{p}B = \mathbb{Z}[i]/(1+i)^2$ is ring of cardinality 4 and an $\mathbb{F}_2$-algebra isomorphic to $\mathbb{F}_2[x]/(x^2)$.

Theorem 6.36

AKLB. For every prime $\mathfrak{p}$ of A, we have $\sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q} = [L : K]$.

We write $\mathfrak{q} \mid \mathfrak{p}$ as shorthand for $\mathfrak{q} \mid \mathfrak{p}B$.

Proof. By the Chinese remainder theorem, we have

$$B/\mathfrak{p}B \simeq B/\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}.$$

By the above Lemma 6.34, we know

$$\begin{aligned}[L:K] &= [B/\mathfrak{p}B : A/\mathfrak{p}] \\ &= \sum_{\mathfrak{q}|\mathfrak{p}} [B/\mathfrak{q}^{e_\mathfrak{q}} : A/\mathfrak{p}] \\ &= \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q}[B/\mathfrak{q} : A/\mathfrak{p}],\end{aligned}$$

where the last equality is from $B/\mathfrak{q}^{e_\mathfrak{q}}$ having dimension $e_\mathfrak{q}$ as a $B/\mathfrak{q}$-vector space. Indeed,

$$\mathfrak{q}^{e_\mathfrak{q}} = \{x \in B : \nu_\mathfrak{q}(x) \geq e_\mathfrak{q}\}.$$

Letting $\pi \in \mathfrak{q}$ be a uniformizer for $B_\mathfrak{q}$ (we can assume it lies in $\mathfrak{q}$ by multiplying by units), the images of $(\pi^0, \pi^1, \dots, \pi^{e_\mathfrak{q}-1})$ in $B/\mathfrak{q}^{e_\mathfrak{q}}$ is a $B/\mathfrak{q}$-basis for $B/\mathfrak{q}^{e_\mathfrak{q}}$. □

Corollary 6.37

AKLB. Let $\mathfrak{p}$ be a prime of A. Then $g_\mathfrak{p} := \#\{\mathfrak{q} \in \operatorname{Spec} B : \mathfrak{q} \mid \mathfrak{p}\}$ is an integer in $[1, n]$ where $n = [L:K]$, as are $e_\mathfrak{q}$ and $f_\mathfrak{q}$ for each $\mathfrak{q} \mid \mathfrak{p}$.

Definition 6.38 (totally ramified, unramified). **AKLB**. Let $\mathfrak{p}$ be a prime of A.

- L/K is *totally ramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = [L:K]$ is as large as it can be. Equivalently, $f_\mathfrak{q} = g_\mathfrak{p} = 1$.
- L/K is *unramified at* $\mathfrak{q}$ if $e_\mathfrak{q} = 1$ **and** $B/\mathfrak{q}$ is separable over $A/\mathfrak{p}$.
- L/K is *unramified above* $\mathfrak{p}$ if it is unramified at all $\mathfrak{q} \mid \mathfrak{p}$. Equivalently, $B/\mathfrak{p}B$ is a finite étale algebra over $A/\mathfrak{p}$.

Definition 6.39. When L/K is unramified above $\mathfrak{p}$ we say

- $\mathfrak{p}$ *remains inert* if $\mathfrak{q} = \mathfrak{p}B$ is prime (equivalently $e_\mathfrak{q} = g_\mathfrak{p} = 1$, $f_\mathfrak{q} = [L:K]$).
- $\mathfrak{p}$ *splits completely* if $g_\mathfrak{p} = [L:K]$ (equivalently $e_\mathfrak{q} = f_\mathfrak{q} = 1$ for all $\mathfrak{q} \mid \mathfrak{p}$).

7 Ideal norms

Recall for a ring extension B/A with B free of finite rank, we defined the norm map $\mathrm{N}_{B/A}\colon B \to A$ by

$$\mathrm{N}_{B/A}(b) := \det(B \xrightarrow{\times b} B).$$

7.1 Module index

Let A be a DD with $K = \operatorname{Frac} A$. Let V be a K-vector space of dimension n, and let M, N be A-lattices in V. $A_\mathfrak{p}$ is a DVR and thus PID, so by the structure theorem $M_\mathfrak{p} \simeq A_\mathfrak{p}^n \simeq N_\mathfrak{p}$ are free (there is no torsion in a vector space). Choose $\phi_\mathfrak{p}\colon M_\mathfrak{p} \xrightarrow{\sim} N_\mathfrak{p}$, and let $\hat{\phi}_\mathfrak{p}$ be the unique extension of $\phi_\mathfrak{p}$ to $V \to V$.

Definition 7.1 (module index). The *module index* is the principal fractional $A_\mathfrak{p}$-ideal generated by $\det \hat{\phi}_\mathfrak{p}$:

$$[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}} \coloneqq (\det \hat{\phi}_\mathfrak{p})$$

Note $\det \hat{\phi}_\mathfrak{p}$ is nonzero because $\hat{\phi}_\mathfrak{p}$ is invertible. The fractional ideal generated by $\det \hat{\phi}_\mathfrak{p}$ depends only on $M_\mathfrak{p}$ and $N_\mathfrak{p}$, not any choices for $\phi_\mathfrak{p}$.

In general, for A not necessarily a DVR, the *module index* is the A-module

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

Each $[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}}$ is an A-submodule of K (not necessarily finitely generated). The intersection $[M : N]_A$ is clearly an A-submodule of K, and it turns out to finitely generated and nonzero.

Claim 7.2 — $[M : N]_A$ is a nonzero fractional ideal whose localizations agree with $[M_\mathfrak{p} : N_\mathfrak{p}]_{A_\mathfrak{p}}$, i.e.

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

The case of when $M \simeq A^n \simeq N$ are free is easy. Then we could fix a global determinant ϕ and $(\det \hat{\phi})_\mathfrak{p} = (\det \hat{\phi}_\mathfrak{p})$. In general, M, N are just A-lattices, and we would potentially choose a different $\hat{\phi}_\mathfrak{p}$ for each $\mathfrak{p}$.

The proof involves a gluing argument. As a sketch, M, N are locally free so we can pick $a_1, \dots, a_n \in A$ generating the unit ideal such that each $M[\frac{1}{a_i}]$ is a free $A[\frac{1}{a_i}]$-module. Do the same thing for B with b_i.

Claim 7.2 implies that $[M : N]_A \in \mathcal{I}_A$ is a fractional ideal. For M, N, P A-lattices in V (no containments assumed), we can take products

$$[M : N]_A [N : P]_A = [M : P]_A.$$

Taking $P = M$ yields

$$[M : N]_A [N : M]_A = [M : M]_A = A.$$

where for the second equality we can take $\phi = \mathrm{id}$. Thus $[M : N]_A$ and $[N : M]_A$ are inverses in $\mathcal{I}_A$.

If $N \subseteq M$, then $[M : N]_A$ is indeed an ideal (not just a fractional ideal).

Remark 7.3. In the special case when $V = K$,

$$[M : N]_A = N \div M.$$

Example 7.4

Note that the order of M and N are swapped above. For example, $[\mathbb{Z} : 2\mathbb{Z}]_\mathbb{Z} = ([\mathbb{Z} : 2\mathbb{Z}]) = (2)$, but $\mathbb{Z} \div 2\mathbb{Z} = (1) \div (2) = (\frac{1}{2})$.

7.2 Ideal norm

AKLB. The inclusion $A \subseteq B$ induces a homomorphism $\mathcal{I}_A \to \mathcal{I}_B$ by $I \mapsto IB$. We wish to define an inverse map $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$.

Definition 7.5 (ideal norm). **AKLB**. The *ideal norm* $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$ is given by $I \mapsto [B : I]_A$. We extend $N_{B/A}$ to the zero ideal by $N_{B/A}((0)) = (0)$.

Proposition 7.6

AKLB. For all $\alpha \in L$, the ideal norm is compatible with the field norm: $N_{B/A}((\alpha)) = (\mathrm{N}_{L/K}(\alpha))$.

Proof. We have

$$\begin{aligned} N_{B/A}((\alpha)) &= [B : \alpha B]_A \\ &= \bigcap_{\mathfrak{p} \in \operatorname{Max} A} [B_\mathfrak{p} : \alpha B_\mathfrak{p}]_{A_\mathfrak{p}} \\ &= (\det(L \xrightarrow{\times\alpha} L)) \\ &= (\mathrm{N}_{L/K}(\alpha)) \end{aligned}$$

since each $B_\mathfrak{p} \xrightarrow{\times\alpha} \alpha B_\mathfrak{p}$ is an isomorphism of free $A_\mathfrak{p}$-modules. □

Proposition 7.7

AKLB. The map $N_{B/A} \colon \mathcal{I}_B \to \mathcal{I}_A$ is a group homomorphism.

Proof. For all $I, J \in \mathcal{I}_B$, we have

$$\begin{aligned} N_{B/A}(IJ) &= \bigcap_{\mathfrak{p}} N_{B_\mathfrak{p}/A_\mathfrak{p}}(I_\mathfrak{p} J_\mathfrak{p}) \\ &= \bigcap_{\mathfrak{p}} N_{B_\mathfrak{p}/A_\mathfrak{p}}(I_\mathfrak{p}) N_{B_\mathfrak{p}/A_\mathfrak{p}}(J_\mathfrak{p}) \\ &= N_{B/A}(I) N_{B/A}(J) \end{aligned}$$

where we use the fact that $N_{B_\mathfrak{p}/A_\mathfrak{p}} \colon \mathcal{I}_{B_\mathfrak{p}} \to \mathcal{I}_{A_\mathfrak{p}}$ is a homomorphism: All elements of $\mathcal{I}_{B_\mathfrak{p}}$ are principal, so by Proposition 7.6, $N_{B_\mathfrak{p}/A_\mathfrak{p}}$ is a group homomorphism because $\mathrm{N}_{L/K}$ is. □

Corollary 7.8

AKLB. For all $I, J \in \mathcal{I}_B$,

$$[I : J]_A = N_{B/A}(I^{-1}J) = N_{B/A}(J \div I).$$

Proof. The second equality is because $J \div I = I^{-1}J$ by B DD. For the first equality,

$$\begin{aligned} [I : J]_A &= [I : B]_A [B : J]_A \\ &= [B : I]_A^{-1} [B : J]_A \\ &= N_{B/A}(I^{-1}) N_{B/A}(J) \\ &= N_{B/A}(I^{-1}J). \end{aligned}$$

□

Corollary 7.9

AKLB. $N_{B/A}(I) = (\mathrm{N}_{L/K}(\alpha) : \alpha \in I)$ for all $I \in \mathcal{I}_B$.

The new part that we did today is the map $L^\times \xrightarrow{\mathrm{N}_{L/K}} K^\times$.

$$\begin{tikzcd}
K^\times \arrow[r, hook] \arrow[d, "(x)"] & L^\times \arrow[d, "(y)"] \\
\mathcal{I}_A \arrow[r, "I \mapsto IB"] & \mathcal{I}_B
\end{tikzcd}
\qquad
\begin{tikzcd}
L^\times \arrow[r, "\mathrm{N}_{L/K}"] \arrow[d, "(y)"] & K^\times \arrow[d, "(x)"] \\
\mathcal{I}_B \arrow[r, "N_{B/A}"] & \mathcal{I}_A
\end{tikzcd}$$

Composing the top row $K^\times \hookrightarrow L^\times \to K^\times$ corresponds to exponentiating by $n = [L : K]$ (pset 2), and same for the bottom row.

7.3 Ideal norm in number fields

Specialize the AKLB setup to $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $B = \mathcal{O}_L$, the ring of integers of some number field L (finite extension of $\mathbb{Q}$). For some $\mathfrak{q} \in \operatorname{Max} B$, let $(p) = \mathfrak{q} \cap \mathbb{Z}$. Writing N in place of $N_{B/A}$, we have

$$\mathrm{N}(\mathfrak{q}) = (p^f)$$

where $f = [B/\mathfrak{q} : \mathbb{Z}/p\mathbb{Z}]$.

Definition 7.10 (absolute norm)**.** The *absolute norm* is

$$\mathrm{N}(\mathfrak{q}) = [\mathcal{O}_L : \mathfrak{q}]_{\mathbb{Z}} = ([\mathcal{O}_L : \mathfrak{q}]).$$

Proposition 7.11

More generally for any nonzero $\mathcal{O}_L$-ideal $\mathfrak{a}$, define

$$\mathrm{N}(\mathfrak{a}) = ([\mathcal{O}_L : \mathfrak{a}]).$$

If $\mathfrak{b} \subseteq \mathfrak{a}$ are nonzero fractional ideals of $\mathcal{O}_L$, then $[\mathfrak{a} : \mathfrak{b}]_{\mathbb{Z}} = ([\mathfrak{a} : \mathfrak{b}])$.

The absolute norm $\mathrm{N}\colon \mathcal{I}_{\mathcal{O}_L} \to \mathcal{I}_{\mathbb{Z}}$ can be viewed as a map $\mathcal{I}_{\mathcal{O}_L} \to \mathbb{Q}_{>0}$ because fractional ideals of $\mathbb{Z}$ can be identified with a positive rational number. When $\mathfrak{a} = (a)$ is a principal fractional ideal, then we write $\mathrm{N}(a) := \mathrm{N}((a)) = \left|\mathrm{N}_{L/\mathbb{Q}}(a)\right|$.

7.4 Dedekind–Kummer

AKLB. Recall that we assume L/K is separable, so $L = K(\alpha)$ for some $\alpha \in L$ (or even $\alpha \in B$ by clearing denominators). However, it is not always true that $B = A[\alpha]$, such as when $A = \mathbb{Z}, K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{5})$, then $B = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ not $\mathbb{Z}[\sqrt{5}]$. However if $B = A[\alpha]$ for **some** $\alpha \in B$, then we call B (and L) *monogenic*. In our example, B and L are still monogenic.

Theorem 7.12 (Dedekind–Kummer)

AKLB. Let $L = K(\alpha)$ for $\alpha \in B$. Let $f \in A[x]$ be the minimal polynomial of α. Let $\mathfrak{p}$ be a prime of A and suppose

$$\overline{f} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r} \in (A/\mathfrak{p})[x]$$

is the factorization of the mod $\mathfrak{p}$ reduction of f into monic irreducibles $\overline{g}_i \in (A/\mathfrak{p})[x]$. Let

$$\mathfrak{q}_i \coloneqq (\mathfrak{p}, g_i(\alpha))$$

where $g_i \in A[x]$ is any lift of $\overline{g}_i$. If $B = A[\alpha]$, then

$$\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

and $f_{\mathfrak{q}_i} = \deg \overline{g}_i$.

This might be on the midterm for small p.

Example 7.13

Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_5)$ which is a degree 4 extension. So $\alpha = \zeta_5$ and $f(x) = x^4+x^3+x^2+x+1$. By pset 4.2, $B = \mathcal{O}_L = \mathbb{Z}[\zeta_5]$, and we can use Dedekind–Kummer to factor any prime of $\mathbb{Z}$ in $\mathcal{O}_L$.

- (2): f is irreducible in $\mathbb{F}_2[x]$, so $e_2 = 1$ and $f_2 = 4$. (2) is an inert prime in $\mathbb{Q}(\zeta_5)$.
- (5): $\overline{f}(x) \equiv (x-1)^4 \pmod 5$, so $5\mathbb{Z}[\zeta_5] = (5, \zeta_5 - 1)^4$ and $e = 4$, $f = 1$. (5) is totally ramified in $\mathbb{Q}(\zeta_5)$.
- (11): $\overline{f}(x) \equiv (x-4)(x-9)(x-5)(x-3) \pmod{11}$ so

  $$11\mathbb{Z}[\zeta_5] = (11, \zeta_5 - 4)(11, \zeta_5 - 9)(11, \zeta_5 - 5)(11, \zeta_5 - 3)$$

  and $e_{\mathfrak{q}} = 1$, $f_{\mathfrak{q}} = 1$ for each $\mathfrak{q}$. (11) splits completely.
- (19): $\overline{f}(x) \equiv (x^2+5x+1)(x^2-4x+1) \pmod{19}$ so

  $$19\mathbb{Z}[\zeta_5] = (19, \zeta_5^2 + 5\zeta_5 + 1)(19, \zeta_5^2 - 4\zeta_5 + 1)$$

  and $e_{\mathfrak{q}} = 1$, $f_{\mathfrak{q}} = 2$ for each $\mathfrak{q}$.

Proof. We first show that each $\mathfrak{q}_i$ is prime in B. From $B = A[\alpha] \simeq A[x]/(f)$, we have

$$\frac{B}{\mathfrak{q}_i} = \frac{A[\alpha]}{(\mathfrak{p}, g_i(\alpha))} \simeq \frac{A[x]}{(f(x), \mathfrak{p}, g_i(x))} \simeq \frac{(A/\mathfrak{p})[x]}{(\overline{f}(x), \overline{g}_i(x))} = \frac{(A/\mathfrak{p})[x]}{(\overline{g}_i(x))}$$

because $\overline{g}_i \mid \overline{f}$. Also, $\overline{g}_i$ is irreducible, so the last quotient is a field and $\mathfrak{q}_i \subset B$ is a maximal ideal. Thus $\mathfrak{q}_i$ is a prime over $\mathfrak{p}$ with $f_{\mathfrak{q}_i} = \deg \overline{g}_i$.

We use unique factorization into prime ideals after we know $\mathfrak{q}_i$ is prime. The ideal

$$\prod_i \mathfrak{q}_i^{e_i} = \prod_i (\mathfrak{p}, g_i(\alpha))^{e_i} = \prod_i (\mathfrak{p}B + (g_i(\alpha)))^{e_i}$$

is divisible by $\mathfrak{p}B$, because all terms in the expansion have $\mathfrak{p}B$ in it except the last term which is

$$\prod_i (g_i(\alpha))^{e_i} \equiv (f(\alpha)) \equiv (0) \pmod{\mathfrak{p}B}.$$

The $\overline{g}_i(x)$ are distinct in $(A/\mathfrak{p})[x]/(f(x)) \simeq A[x]/(\mathfrak{p}, f(x)) \simeq A[\alpha]/\mathfrak{p}A[\alpha]$, so the $g_i(\alpha)$ are distinct mod $\mathfrak{p}B = \mathfrak{p}A[\alpha]$. This implies the $\mathfrak{q}_i$ are all distinct primes of B. Also $e_i \geq e_{\mathfrak{q}_i}$ (the ramification index) and $\{\mathfrak{q} \mid \mathfrak{p}\} \subseteq \{\mathfrak{q}_i\}_i$ in order for $\prod_i \mathfrak{q}_i^{e_i}$ to be divisible by $\mathfrak{p}B$. We already noted that each $\mathfrak{q}_i \mid \mathfrak{p}$, so indeed $\{\mathfrak{q} \mid \mathfrak{p}\} = \{\mathfrak{q}_i\}_i$.

It remains to show $e_i = e_{\mathfrak{q}_i}$. From

$$N_{B/A}\Big(\prod_i \mathfrak{q}_i^{e_i}\Big) = N_{B/A}(\mathfrak{q}_i)^{e_i} = \prod_i (\mathfrak{p}^{f_{\mathfrak{q}_i}})^{e_i} = \prod_i \mathfrak{p}^{e_i \deg \overline{g}_i} = \prod_i \mathfrak{p}^{\deg f} = \mathfrak{p}^{[L:K]},$$

we see $\sum_i e_i f_{\mathfrak{q}_i} = [L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}$ so we need $e_i = e_{\mathfrak{q}_i}$ or the LHS would be too big. □

7.5 Conductor of a ring

Definition 7.14 (conductor). Let S/R be an extension of commutative rings. The *conductor of R in S* is the largest S-ideal that is an R-ideal. Equivalently, it is the ideal

$$\mathfrak{c} := \{\alpha \in S : \alpha S \subseteq R\} = \{\alpha \in R : \alpha S \subseteq R\}.$$

When R is an integral domain, the *conductor of R* is the conductor of R in its integral closure.

Example 7.15

The conductor of $\mathbb{Z} \subseteq \mathbb{Z}[i]$ is (0). $\mathbb{Z}[i]$ is "too far away" from $\mathbb{Z}$, as multiplying by i will not land in $\mathbb{Z}$.

The conductor of $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\zeta_3]$ is $(2, 1+\sqrt{-3}) = 2\mathbb{Z}[\zeta_3]$. Note it is principal in $\mathbb{Z}[\zeta_3]$ but not in $\mathbb{Z}[\sqrt{-3}]$.

Lemma 7.16

Let R be a Noetherian domain with integral closure S. The conductor of R in S is nonzero if and only if S is finitely generated as an R-module.

Definition 7.17 (order). An *order* $\mathcal{O}$ is a Noetherian domain of dimension 1 whose conductor is nonzero, or equivalently, whose integral closure is finitely generated as an $\mathcal{O}$-module.

Example 7.18

Any DD that is not a field is an order.

In **AKLB** assuming $L \neq K$, B is finitely generated as an A-module and thus over every intermediate ring between A and B. If $A[\alpha]$ and B have the same fraction field, then $A[\alpha]$ is an order in B. So the conductor of A is nonzero.

Definition 7.19 (A-order). Let A be a Noetherian domain with $K = \operatorname{Frac} A$, and let L be a K-algebra of finite dimension (not necessarily commutative). An *A-order* in L is an A-lattice that is a ring.

All A-orders are orders in AKLB, since A-lattices have to span.

An A-order is *maximal* if it is not properly contained in another A-order. When A is a DD, every A-order is contained in a maximal A-order. In AKLB, B is the unique maximal A-order in L.

Definition 7.20 (prime to). Let A be a Noetherian domain and J an A-ideal. A fractional ideal I is *prime to* J if $IA_{\mathfrak{p}} = A_{\mathfrak{p}}$ for all $\mathfrak{p} \supseteq J$. Let $\mathcal{I}_A^J \subseteq \mathcal{I}_A$ be the fractional ideals prime to J.

Theorem 7.21

AKLB. Let $\mathcal{O}$ be an order with integral closure B. Let $\mathfrak{c}$ be any ideal of B contained in the conductor of $\mathcal{O}$. The map $\mathfrak{q} \mapsto \mathfrak{q} \cap \mathcal{O}$ induces a group homomorphism $\mathcal{I}_B^{\mathfrak{c}} \to \mathcal{I}_{\mathcal{O}}^{\mathfrak{c}}$, and both groups are isomorphic to the free abelian group generated by their prime ideals. In particular, every fractional ideal $I \in \mathcal{I}_{\mathcal{O}}^{\mathfrak{c}}$ has a unique factorization into prime ideals $\prod_i \mathfrak{p}_i^{e_i}$ that matches $IB = \prod_i \mathfrak{q}_i^{e_i}$ with $\mathfrak{p}_i = \mathfrak{q}_i \cap \mathcal{O}$.

Corollary 7.22

The assumption $B = A[\alpha]$ in the Dedekind–Kummer theorem can be replaced by "$\mathfrak{p}B$ is prime to the conductor of $A[\alpha]$."

Remark 7.23. For $A = \mathbb{Z}$ and $L = \mathbb{Q}(\alpha)$, the ideal $p\mathcal{O}_L$ is prime to the conductor of $A[\alpha]$ if and only if p does not divide $[\mathcal{O}_L : A[\alpha]]$.

8 Galois extensions

Definition 8.1 (left G-module). Let G be a group. A *left G-module* is an abelian group M equipped with a left G-action compatible with the group structure: $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$ for all $a, b \in M$.

AKLBG setup: AKLB and L/K Galois with $\mathrm{Gal}(L/K) = G$. We show that $\mathcal{I}_B$ is a left G-module.

Theorem 8.2

AKLBG. For each $I \in \mathcal{I}_B$ and $\sigma \in G$, define $\sigma(I) = \{\sigma(x) : x \in I\}$. Then $\sigma(I) \in \mathcal{I}_B$ and this defines a G-action on $\mathcal{I}_B$.

Moreover, the restriction of this action to $\operatorname{Spec} B$ is a G-set, i.e. G sends prime ideals to prime ideals.

Proof. We first claim that $\sigma(B) = B$. Every $b \in B$ is the root of some monic $f \in A[x]$. Then

$$0 = \sigma(0) = \sigma(f(b)) = f(\sigma(b)),$$

so $\sigma(b)$ is another root of f. Thus $\sigma(b) \in B$, and $\sigma(B) \subseteq B$. We analogously have $\sigma^{-1}(B) \subseteq B$, so $B \subseteq \sigma(B)$.

Since I is a finitely generated B-module in L, $\sigma(I)$ is a finitely generated $\sigma(B)$-module (i.e. B-module), so $\sigma(I) \in \mathcal{I}_B$. As $\sigma((0)) = (0)$, σ permutes the nonzero fractional ideals $\mathcal{I}_B$. To see that σ is a group action, we have

$$(\sigma\tau)(I) = \{(\sigma\tau)(x) : x \in I\} = \{\sigma(\tau(x)) : x \in I\} = \sigma(\tau(I)).$$

To see that $\mathcal{I}_B$ is a left G-module, let $I, J \in \mathcal{I}_B$ and $\sigma \in G$. Each $x \in IJ$ has the form $x = a_1b_1 + \cdots + a_nb_n$ with $a_i \in I, b_i \in J$. As $\sigma(x) = \sigma(a_1)\sigma(b_1) + \cdots + \sigma(a_n)\sigma(b_n) \in \sigma(I)\sigma(J)$, $\sigma(IJ) \subseteq \sigma(I)\sigma(J)$. Applying the same argument to $\sigma(I), \sigma(J), \sigma^{-1}$ yields $\sigma^{-1}(\sigma(I)\sigma(J)) \subseteq IJ$. Thus $\sigma(IJ) = \sigma(I)\sigma(J)$ and $\mathcal{I}_B$ is a left G-module.

For the second part, let $\mathfrak{q} \in \mathcal{I}_B$ be a prime ideal, and let $\sigma(\mathfrak{q}) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$ be the unique factorization in B. Then

$$\mathfrak{q} = \sigma^{-1}(\mathfrak{q}_1)^{e_1} \cdots \sigma^{-1}(\mathfrak{q}_n)^{e_n},$$

but since $\mathfrak{q}$ is prime, we need $n = 1$ and $e_1 = 1$. Then $\sigma(\mathfrak{q}) = \mathfrak{q}_1$ is a nonzero prime ideal, and $\operatorname{Spec} B$ is a G-set. □

Recall that $\mathfrak{q} \mid \mathfrak{p}$ for $\mathfrak{q} \in \operatorname{Spec} B$, $\mathfrak{p} \in \operatorname{Spec} A$ means $\mathfrak{q}$ is in the prime factorization of $\mathfrak{p}B$ (or $\mathfrak{p} = A \cap \mathfrak{q}$). In other words, $\{\mathfrak{q} \mid \mathfrak{p}\}$ is the fiber of $\operatorname{Max} B \to \operatorname{Max} A$ above $\mathfrak{p}$. If $\mathfrak{p}B = \prod_i \mathfrak{q}_i^{e_i}$, then

$$\mathfrak{p}B = \sigma(\mathfrak{p}B) = \prod_i \sigma(\mathfrak{q}_i)^{e_i}$$

implying that σ can only permute the primes above a given $\mathfrak{p}$. G therefore acts on $\{\mathfrak{q} \mid \mathfrak{p}\}$, and it turns out this action is transitive.

Corollary 8.3

AKLBG. For all $\mathfrak{p} \in \operatorname{Max} A$, G acts transitively on $\{\mathfrak{q} \mid \mathfrak{p}\}$.

Proof. Let $\{\mathfrak{q} \mid \mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$. FSOC suppose $\mathfrak{q}_1, \mathfrak{q}_2$ lie in distinct G-orbits. By the Chinese remainder theorem, we have

$$B/\mathfrak{q}_1 \cdots \mathfrak{q}_n \simeq B/\mathfrak{q}_1 \times \cdots \times B/\mathfrak{q}_n.$$

Choose $b \in B$ such that $b \equiv 0 \pmod{\mathfrak{q}_2}$ and $b \equiv 1 \pmod{\sigma(\mathfrak{q}_1)}$ for all $\sigma \in G$ (by assumption $\sigma(\mathfrak{q}_1) \neq \mathfrak{q}_2$ for any $\sigma \in G$). Then $b \in \mathfrak{q}_2$ and

$$N_{L/K}(b) = \prod_{\sigma \in G} \sigma(b) \equiv 1 \pmod{\mathfrak{q}_1}$$

so $N_{L/K}(b) \notin \mathfrak{q}_1 \cap A = \mathfrak{p}$. This contradicts $N_{L/K}(b) \in N_{L/K}(\mathfrak{q}_2) = \mathfrak{p}^{f_{\mathfrak{q}_2}} \subseteq \mathfrak{p}$. □

Corollary 8.4

AKLBG. The residue field degrees $f_{\mathfrak{q}} := [B/\mathfrak{q} : A/\mathfrak{p}]$ and the ramification indices $e_{\mathfrak{q}} := \nu_{\mathfrak{q}}(\mathfrak{p}B)$ are the same for all $\mathfrak{q} \mid \mathfrak{p}$.

Proof. For each $\sigma \in G$, we have an isomorphism $B/\mathfrak{q} \simeq B/\sigma(\mathfrak{q})$ that fixes $A/\mathfrak{p}$, so $f_{\mathfrak{q}} = f_{\sigma(\mathfrak{q})}$. From $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(B) = B$, we have $\sigma(\mathfrak{p}B) = \mathfrak{p}B$ and

$$e_{\mathfrak{q}} = \nu_{\mathfrak{q}}(\mathfrak{p}B) = \nu_{\mathfrak{q}}(\sigma(\mathfrak{p}B)) = \nu_{\mathfrak{q}}\Big(\prod_{\mathfrak{r} \mid \mathfrak{p}} \sigma(\mathfrak{r})^{e_{\mathfrak{r}}}\Big) = \nu_{\mathfrak{q}}\Big(\prod_{\mathfrak{r} \mid \mathfrak{p}} \mathfrak{r}^{e_{\sigma^{-1}(\mathfrak{r})}}\Big) = e_{\sigma^{-1}(\mathfrak{q})}.$$ □

This means we can unambiguously define $f_{\mathfrak{p}} := f_{\mathfrak{q}}$ and $e_{\mathfrak{p}} := e_{\mathfrak{q}}$. Recall $g_{\mathfrak{p}} = \#\{\mathfrak{q} \mid \mathfrak{p}\}$.

Corollary 8.5

AKLBG. $e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = [L : K]$.

Proof. This follows from Theorem 6.36 and Corollary 8.4. □

Example 8.6

If $n = [L : K]$ is a prime number, the possibilities are

- $e_{\mathfrak{p}} = n$, so $\mathfrak{p}$ is totally ramified in L.
- $f_{\mathfrak{p}} = n$, so $\mathfrak{p}$ is inert.
- $g_{\mathfrak{p}} = n$, so $\mathfrak{p}$ splits completely.

In the last two cases, we assume $B/\mathfrak{p}B$ is a finite étale $A/\mathfrak{p}$-algebra, which is automatically true when $A/\mathfrak{p}$ is finite (hence perfect).

8.1 Decomposition and inertia groups

Definition 8.7 (decomposition group)**.** **AKLBG**. The *decomposition group* $D_{\mathfrak{q}}$ is the G-stabilizer of $\mathfrak{q}$.

Lemma 8.8

AKLBG. Let $\mathfrak{p} \in \operatorname{Max} A$. The $D_{\mathfrak{q}}$ for $\mathfrak{q} \mid \mathfrak{p}$ are conjugate subgroups of G with $\#D_{\mathfrak{q}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ and $[G : D_{\mathfrak{q}}] = g_{\mathfrak{p}}$.

Proof. Note that stabilizers of elements in an orbit are always conjugate. The orbit-stabilizer theorem says $[G : D_{\mathfrak{q}}] = g_{\mathfrak{p}}$, the size of the orbit $\{\mathfrak{q} \mid \mathfrak{p}\}$. Then $\#D_{\mathfrak{q}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$ is deduced from Corollary 8.5. □

Now fix $\mathfrak{q} \mid \mathfrak{p}$. Each $\sigma \in G$ induces $\overline{\sigma} \in \operatorname{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma(\mathfrak{q}))$. For $\sigma \in D_{\mathfrak{q}}$, we have $\sigma(\mathfrak{q}) = \mathfrak{q}$, so $\overline{\sigma} \in \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$. The map $\sigma \mapsto \overline{\sigma}$ defines a group homomorphism

$$\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}),$$

as $\overline{\sigma\tau}(\overline{x}) = \overline{\sigma\tau(x)} = \overline{\sigma(\tau(x))} = \overline{\sigma}(\overline{\tau(x)}) = \overline{\sigma}(\overline{\tau}(x))$.

Proposition 8.9

AKLBG. Let $\mathfrak{q} \mid \mathfrak{p}$ be a prime of B. The homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ defined by $\sigma \mapsto \overline{\sigma}$ is surjective, and $B/\mathfrak{q}$ is a normal extension of $A/\mathfrak{p}$.

Proof. Let F be the separable closure of $A/\mathfrak{p}$ in $B/\mathfrak{q}$. For $\overline{b} \in F$, pick $b \in B$ such that $b \equiv \overline{b} \pmod{\mathfrak{q}}$. By CRT, we can find $b \equiv 0 \pmod{\sigma^{-1}(\mathfrak{q})}$ for all $\sigma \in G - D_{\mathfrak{q}}$, as the maximal ideals $\mathfrak{q}$, $\sigma^{-1}(\mathfrak{q})$ are all distinct and thus coprime. Then $\sigma(b) \equiv 0 \pmod{\mathfrak{q}}$, and we let

$$g(x) \coloneqq \prod_{\sigma \in G} (x - \sigma(b)) \in A[x].$$

Let $\overline{g} \in (A/\mathfrak{p})[x]$ be the reduction mod $\mathfrak{p}$. By construction, $\overline{g}(\overline{b}) = 0$ and $\overline{g}$ splits completely in $(B/\mathfrak{q})[x]$. This holds for every $\overline{b} \in F^{\times}$, so F is a normal (hence Galois) extension of $A/\mathfrak{p}$. Then $\operatorname{Gal}(F/(A/\mathfrak{p})) \simeq \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$, since F is the separable closure.

For $\sigma \in G - D_{\mathfrak{q}}$ we have $\overline{\sigma}(\overline{b}) = 0$, so 0 is a root of $\overline{g}$ with multiplicity at least $m = \#(G - D_{\mathfrak{q}})$. The remaining roots are $\overline{\sigma}(\overline{b})$ for $\sigma \in D_{\mathfrak{q}}$, which are $\operatorname{Gal}(F/(A/\mathfrak{p}))$-conjugates of $\overline{B}$. Thus $\overline{g}(x)/x^m$ is a polynomial dividing a power of the minimal polynomial $f(x)$ of $\overline{b}$. However, the minimal polynomial is irreducible, so $\overline{g}(x)/x^m$ is a power of $f(x)$. In other words, every $\operatorname{Gal}(F/(A/\mathfrak{p}))$-conjugate of $\overline{b}$ is of the form $\overline{\sigma}(b)$ for some

$\sigma \in D_{\mathfrak{q}}$. Applying this to the $\bar{b}$ such that $F = (A/\mathfrak{p})(\bar{b})$ (by the primitive element theorem) shows that $\pi_q \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ is surjective.

To show $B/\mathfrak{q}$ is normal, proceed as above, replacing F with $B/\mathfrak{q}$. For $b \in B$, define $g \in A[x]$ and $\overline{g} \in (A/\mathfrak{p})[x]$ as before to show every $\bar{b} \in B/\mathfrak{q}$ is a root of a polynomial in $(A/\mathfrak{p})[x]$ that splits completely in $(B/\mathfrak{q})[x]$. □

Definition 8.10 (inertia group). **AKLBG**. The *inertia group* $I_{\mathfrak{q}}$ is the kernel of the surjective homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$.

Corollary 8.11

For all $\mathfrak{q} \mid \mathfrak{p} \in \operatorname{Max} B$, we have an exact sequence

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \to \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \to 1,$$

and $\# I_{\mathfrak{q}} = e_{\mathfrak{q}}[B/\mathfrak{q} : A/\mathfrak{p}]_i$.

We have shown that $B/\mathfrak{q}$ is always a normal extension of $A/\mathfrak{p}$. Now suppose it is also a separable extension (which always holds when $A/\mathfrak{p}$ is finite). Then

$$D_{\mathfrak{q}}/I_{\mathfrak{q}} \simeq \operatorname{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \simeq \operatorname{Gal}((B/\mathfrak{q})/(A/\mathfrak{p})).$$

Proposition 8.12

AKLBG. Let $\mathfrak{q} \in \operatorname{Max} B$ with $\mathfrak{q} \mid \mathfrak{p}$ and $B/\mathfrak{q}$ a separable extension of $A/\mathfrak{p}$. We have a tower of field extensions $K \subseteq L^{D_{\mathfrak{q}}} \subseteq L^{I_{\mathfrak{q}}} \subseteq L$ with

$$\begin{aligned} e_{\mathfrak{p}} &= [L : L^{I_{\mathfrak{q}}}] = \# I_{\mathfrak{q}} \\ f_{\mathfrak{p}} &= [L^{I_{\mathfrak{q}}} : L^{D_{\mathfrak{q}}}] = \# D_{\mathfrak{q}} / \# I_{\mathfrak{q}} \\ g_{\mathfrak{p}} &= [L^{D_{\mathfrak{q}}} : K] = \#\{\mathfrak{q} \mid \mathfrak{p}\}. \end{aligned}$$

$L^{D_{\mathfrak{q}}}$ is the *decomposition field* at $\mathfrak{q}$, and $L^{I_{\mathfrak{q}}}$ is the *inertia field* at $\mathfrak{q}$.

Proposition 8.13

AKLBG. Suppose there is a field E with $K \subseteq E \subseteq L$. For $\mathfrak{q} \in \operatorname{Max} B$, define $\mathfrak{q}_E := \mathfrak{q} \cap E$. Let $\mathfrak{p} = \mathfrak{q} \cap K$. Then

$$I_{\mathfrak{q}}(L/E) = I_{\mathfrak{q}}(L/K) \cap \operatorname{Gal}(L/E)$$
$$D_{\mathfrak{q}}(L/E) = D_{\mathfrak{q}}(L/K) \cap \operatorname{Gal}(L/E).$$

If E/K is also Galois like L/K, then we get a commutative diagram

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & I_{\mathfrak{q}}(L/E) \arrow[r] \arrow[d] & I_{\mathfrak{q}}(L/K) \arrow[r] \arrow[d] & I_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & D_{\mathfrak{q}}(L/E) \arrow[r] \arrow[d] & D_{\mathfrak{q}}(L/K) \arrow[r] \arrow[d] & D_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \overline{G}_{\mathfrak{q}}(L/E) \arrow[r] \arrow[d] & \overline{G}_{\mathfrak{q}}(L/K) \arrow[r] \arrow[d] & \overline{G}_{\mathfrak{q}_E}(E/K) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

where $\overline{G}_{\mathfrak{q}}(\bullet)$ is Gal of the residue field.

Definition 8.14. **AKLBG**. Let $I_{\mathfrak{p}}$ be the group generated by $I_{\mathfrak{q}}$ for $\mathfrak{q} \mid \mathfrak{p}$, and let $D_{\mathfrak{p}}$ be the group generated by $D_{\mathfrak{q}}$, called the *inertia group* and *decomposition group* of $\mathfrak{p}$.

Proposition 8.15

The inertia field $L^{I_{\mathfrak{p}}}$ and decomposition field $L^{D_{\mathfrak{p}}}$ are always Galois extensions of K.

If $A/\mathfrak{p}$ is perfect, then the inertia field $L^{I_{\mathfrak{p}}}$ is the largest subfield in which $\mathfrak{p}$ is unramified. The decomposition field $L^{D_{\mathfrak{p}}}$ is the largest subfield in which $\mathfrak{p}$ splits completely.

8.2 Frobenius elements

Now assume that $A/\mathfrak{p}$ is finite (and thus $B/\mathfrak{q}$) for all primes $\mathfrak{p}$ of K. We write $\mathbb{F}_{\mathfrak{q}} = B/\mathfrak{q}$ and $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$. Recall the exact sequence

$$1 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \xrightarrow{\pi_{\mathfrak{q}}} \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) \to 1$$

where $\pi_{\mathfrak{q}}$ sends $\sigma \mapsto \overline{\sigma}$ for $\overline{\sigma} \in \operatorname{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma(\mathfrak{q}))$ satisfying $\overline{\sigma}(\overline{x}) := \overline{\sigma(x)}$.

If $\mathfrak{p}$ (equivalently $\mathfrak{q}$) is unramified, then $I_{\mathfrak{q}} = 1$ and we have an isomorphism

$$\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \xrightarrow{\sim} \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}).$$

$\operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is the cyclic group of order $f_{\mathfrak{p}} = [\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_{\mathfrak{p}}]$ generated by the *Frobenius automorphism*

$$x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}.$$

Definition 8.16 (Frobenius element)**.** The *Frobenius element* is $\pi_{\mathfrak{q}}^{-1}(x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}) \in D_{\mathfrak{q}}$, denoted $\sigma_{\mathfrak{q}}$ or $\operatorname{Frob}_{\mathfrak{q}}$.

Definition 8.17 (Frobenius class)**.** **AKLBG** with finite residue fields. Let $\mathfrak{p}$ be an unramified prime of A. The *Frobenius class* is the G-conjugacy class $\operatorname{Frob}_{\mathfrak{p}} = \{\sigma_{\mathfrak{q}} : \mathfrak{q} \mid \mathfrak{p}\}$.

If G is abelian, then each conjugacy class consists of a single element and $\operatorname{Frob}_{\mathfrak{p}} = \{\operatorname{Frob}_{\mathfrak{q}}\}$ is a singleton.

Proposition 8.18

AKLBG with finite residue fields. Let $\mathfrak{q} \mid \mathfrak{p}$ be unramified. The Frobenius element $\operatorname{Frob}_{\mathfrak{q}}$ is the unique element $\sigma \in G$ such that for all $x \in B$ we have $\sigma(x) \equiv x^{\#\mathbb{F}_{\mathfrak{p}}} \pmod{\mathfrak{q}}$.

This is saying $\operatorname{Frob}_{\mathfrak{q}}$ can be characterized without looking at the exact sequence.

Proof. $\operatorname{Frob}_{\mathfrak{q}}$ satisfies this, so we just need to show uniqueness. Suppose $\sigma \in G$ has this property. Then if $x \in \mathfrak{q}$ we have $x \equiv 0 \pmod{\mathfrak{q}} \implies \sigma(x) \equiv x^{\#\mathbb{F}_{\mathfrak{p}}} \equiv 0 \pmod{\mathfrak{q}}$ so $\sigma(x) \in \mathfrak{q}$ and $\sigma \in D_{\mathfrak{q}}$ (stabilizers). The isomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \operatorname{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ maps both σ and $\operatorname{Frob}_{\mathfrak{q}}$ to $x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}}$, so they are the same. □

8.3 Artin symbols

Throughout this section, assume **AKLBG** with finite residue fields.

Definition 8.19 (Artin symbol)**.** For each unramified $\mathfrak{q} \in \operatorname{Max} B$, the *Artin symbol* is $\left(\frac{L/K}{\mathfrak{q}}\right) := \operatorname{Frob}_{\mathfrak{q}}$.

Proposition 8.20

$\mathfrak{p}$ splits completely in L if and only if $\left(\frac{L/K}{\mathfrak{q}}\right) = 1$ for all $\mathfrak{q} \mid \mathfrak{p}$.

Proof. $\mathfrak{p}$ splits completely $\iff e_{\mathfrak{p}} f_{\mathfrak{p}} = 1 \iff \#D_{\mathfrak{q}} = 1$ by Lemma 8.8 $\iff \operatorname{Frob}_{\mathfrak{q}} = 1$ as $D_{\mathfrak{q}} = \langle \operatorname{Frob}_{\mathfrak{q}} \rangle$. □

We extend $\left(\frac{L/K}{\mathfrak{q}}\right)$ to $\mathcal{I}_A^S$, the fractional ideals coprime to S where $S \supseteq \{\mathfrak{p} \text{ ramified}\}$ (i.e. $\nu_{\mathfrak{p}}(I) = 0$ for all $\mathfrak{p} \in S$). When $\operatorname{Gal}(L/K)$ is abelian, $\operatorname{Frob}_{\mathfrak{q}}$ is equal for all $\mathfrak{q} \mid \mathfrak{p}$ and we write $\left(\frac{L/K}{\mathfrak{p}}\right)$.

Definition 8.21 (Artin map)**.** The *Artin map* is the homomorphism

$$\begin{aligned} \left(\frac{L/K}{\bullet}\right) \colon \mathcal{I}_A^S &\to \operatorname{Gal}(L/K) \\ \prod_{i=1}^m \mathfrak{p}_i^{e_i} &\mapsto \prod_{i=1}^m \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}. \end{aligned}$$

This group homomorphism is remarkable because $\mathcal{I}_A^S$ doesn't know anything about L. By understanding structure of subgroups of I_A, we can understand all abelian extensions of K.

9 Complete fields and valuation rings

9.1 Completions

Recall that a *metric* on a set X is a function $d\colon X \times X \to \mathbb{R}_{\geq 0}$ satisfying

1. $d(x,y) = 0 \iff x = y$
2. $d(x,y) = d(y,x)$
3. $d(x,z) \leq d(x,y) + d(y,z)$.

If also $d(x,z) \leq \max\{d(x,y), d(y,z)\}$, then d is a *non-archimedean* metric.

There is a topology on X generated by *open balls*

$$B_{<r}(x) \coloneqq \{y \in X : d(x,y) < r\}$$

where $r \in \mathbb{R}_{>0}$ and $x \in X$. It is Hausdorff. The *closed balls*

$$B_{\leq r}(x) \coloneqq \{y \in X : d(x,y) \leq r\}$$

are closed in this topology.

Every absolute value $|\cdot|$ on a ring X induces a metric via

$$d(x,y) \coloneqq |x-y|\,,$$

although not every metric comes from an absolute value.

Definition 9.1 (convergence, Cauchy, complete)**.** In a metric space X, a sequence (x_n) *converges* (to x) if there exists $x \in X$ such that $\forall \epsilon > 0$, $\exists N \in \mathbb{Z}_{>0}$ such that $d(x_n, x) < \epsilon$ for all $n \geq N$. The limit x is unique if it exists.

The sequence (x_n) is *Cauchy* if $\forall \epsilon > 0$, $\exists N \in \mathbb{Z}_{>0}$ such that $d(x_m, x_n) < \epsilon$ for all $m, n \geq N$. Convergent sequences are Cauchy, but the converse is not always true.

If every Cauchy sequence converges, then X is *complete.*

Definition 9.2 (topological group)**.** An abelian group G is a *topological group* if it is a topological space in which the group operations $G \times G \to G$ by $(x,y) \mapsto x+y$ and $G \to G$ by $x \mapsto x^{-1}$ are continuous.

A commutative ring R is *topological ring* if it is a topological space in which addition and multiplication $R \times R \to R$ are continuous. Note $R^\times$ might not be a topological group.

A field K is a *topological field* if it is a topological ring, and its unit group $K^\times$ is a topological group.

Definition 9.3 (equivalent)**.** In a metric space X, two Cauchy sequences $(x_n), (y_n)$ are *equivalent* if $d(x_n, y_n) \to 0$ as $n \to \infty$.

This is an equivalence relation on Cauchy sequences, and let $[(x_n)]$ denote the equivalence class.

Definition 9.4 (completion)**.** The *completion* of a metric space X is the metric space $\widehat{X}$ whose elements are equivalence classes of Cauchy sequences with

$$d([(x_n)], [(y_n)]) := \lim_{n\to\infty} d(x_n, y_n).$$

We embed X in $\widehat{X}$ via $x \mapsto \widehat{x} := [(x, x, x, \dots)]$.

If X is a topological ring, we extend the ring operations to $\widehat{X}$ via $[(x_n)] + [(y_n)] := [(x_n + y_n)]$ and $[(x_n)][(y_n)] := [(x_n y_n)]$. Then $0 := \widehat{0}$ and $1 := \widehat{1}$. If d comes from an absolute value $|\cdot|$ on X, then we define

$$|[(x_n)]| := \lim_{n\to\infty} |x_n|.$$

If $|\cdot|$ arises from a discrete valuation ν on a field K, meaning $|x| = c^{\nu(x)}$ for some $0 < c < 1$, we can extend ν to $\widehat{X}$ by defining

$$\nu([(x_n)]) := \lim_{n\to\infty} \nu(x_n) \in \mathbb{Z}$$

for $[(x_n)] \neq \widehat{0}$, and as usual $\nu(\widehat{0}) := \infty$. The sequence of integers $\nu(x_n)$ is eventually constant, so it converges to an integer. We will have

$$|[(x_n)]| = c^{\nu([(x_n)])}.$$

Proposition 9.5

K be a topological field under the metric induced by $|\cdot|$, and let $\widehat{K}$ be its completion. Then $\widehat{K}$ is complete and has the following universal property: every embedding of K into a complete field L can be uniquely extended to an embedding $\widehat{K} \hookrightarrow L$ (as topological fields, so it's continuous). This extension is an isomorphism when K is dense in L. Up to canonical isomorphism, $\widehat{K}$ is the unique topological field with this property.

Theorem 9.6 (Weak approximation)

Let K be a field and $|\cdot|_1, \dots, |\cdot|_n$ be pairwise nonequivalent nontrivial absolute values on K. Let $a_1, \dots, a_n \in K$ and $\epsilon_1, \dots, \epsilon_n > 0$. Then there exists $x \in K$ such that $|x - a_i|_i < \epsilon_i$ for $1 \le i \le n$.

Corollary 9.7

Two absolute values on a field K induce the same topology if and only if they are equivalent.

"Completion is like localization but on steroids."

Unintuitive facts about a non-archimedean topology on X:

- We can have $B_{<r}(x) = B_{<s}(x)$ for $r \neq s$, such as when $|\cdot| : X \to \mathbb{R}_{\ge 0}$ comes from a discrete valuation and has a discrete image (powers of c).
- Every point in an open ball is a center, i.e. $B_{<r}(y) = B_{<r}(x)$ for all $y \in b_{<r}(x)$.
- Any two open balls are either concentric or disjoint.
- Every open ball is closed, and every closed ball is open.
- X is *totally disconnected*, meaning singletons are the only connected components.

9.2 Valuation rings in complete fields

We now consider absolute values induced by a discrete valuation $\nu\colon K^\times \twoheadrightarrow \mathbb{Z}$. Picking $0 < c < 1$ and defining

$$|x|_\nu := c^{\nu(x)}, \quad |0|_\nu := 0$$

yields a nontrivial non-archimedean absolute value. Let $K_\nu := \widehat{K}$ be the completion with respect to $|\cdot|_\nu$. Different choices of c yield equivalent absolute values and do not change the topology or K_ν.

The valuation ring

$$A_\nu = \{x \in K_\nu : \nu(x) \geq 0\} = \{x \in K_\nu : |x|_\nu \leq 1\}$$

which is a closed (and thus open) ball. It is thus complete as a closed subset of a complete topological space.

Proposition 9.8

Let K be a field with absolute value $|\cdot|_\nu$ induced by discrete valuation ν. Let A be the valuation ring and π be a uniformizer. The valuation ring A_ν of K_ν is a complete DVR with uniformizer π, and we have an isomorphism of **topological rings**

$$A_\nu \simeq \varprojlim_{n\to\infty} A/\pi^n A.$$

Proof. Read carefully in the notes. It's important that the isomorphism is of topological rings (not just rings). A key step is that $\bigcap \pi^n A_\nu = \{0\}$. □

Example 9.9

For $K = \mathbb{Q}$, let ν_p be the p-adic valuation and $|x|_p = p^{-\nu_p(x)}$. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is $\widehat{\mathbb{Q}} = \mathbb{Q}_p$ (p-adic numbers). The valuation ring of $\mathbb{Q}$ is the local ring $\mathbb{Z}_{(p)}$, so the valuation ring of $\mathbb{Q}$ is $\mathbb{Z}_p$ (p-adic integers): taking $\pi = p$ as the uniformizer, we have

$$\widehat{\mathbb{Z}_{(p)}} \simeq \varprojlim_{n\to\infty} \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \simeq \varprojlim_{n\to\infty} \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p.$$

Example 9.10

For $K = \mathbb{F}_q(t)$, let ν_t be the t-adic valuation and $|x|_t := q^{-\nu_t(x)}$. The completion of $\mathbb{F}_q(t)$ with respect to $|\cdot|_t$ is $\mathbb{F}_q((t))$. The valuation ring of $\mathbb{F}_q(t)$ is $\mathbb{F}_q[t]_{(t)}$, so the valuation ring of $\mathbb{F}_q((t))$ is $\mathbb{F}_q[[t]]$: taking $\pi = t$ as the uniformizer, we have

$$\widehat{\mathbb{F}_q[t]_{(t)}} \simeq \varprojlim_{n\to\infty} \mathbb{F}_q[t]_{(t)}/t^n\mathbb{F}_q[t]_{(t)} \simeq \varprojlim_{n\to\infty} \mathbb{F}_q[t]/t^n\mathbb{F}_q[t] \simeq \mathbb{F}_q[[t]].$$

Example 9.11

The isomorphism $\mathbb{Z}_p \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ gives a canonical way to represent $a \in \mathbb{Z}_p$ as a sequence (a_n) with $a_{n+1} \equiv a_n \pmod{p^n}$ and $0 \leq a_n < p^n$. For example in $\mathbb{Z}_7$, we have

$$\begin{aligned} 2 &= (2, 2, 2, \dots) \\ 2002 &= (0, 42, 287, 2002, 2002, \dots) \\ -2 &= (5, 47, 341, 2399, 16805, \dots) \\ 2^{-1} &= (4, 25, 172, 1201, 8404, \dots) \\ \sqrt{2} &= \begin{cases} (3, 10, 108, 2166, 4567, \dots) \\ (4, 39, 235, 235, 12240, \dots) \end{cases} \\ \sqrt[3]{2} &= (4, 46, 95, 1124, 15530, \dots). \end{aligned}$$

To compute 2^{-1}, we find $2^{-1} \equiv 4 \pmod 7$, etc. For $\sqrt{2}$, we see that $3^2 \equiv 4^2 \equiv 2 \pmod 7$, then lift to mod 49 etc.

$\mathbb{Z}_7$ turns out to not be algebraically closed, e.g. there is no 5th root of 2 $\pmod 7$.

There is redundancy as knowing a_n determines all $a_1, \dots, a_{n-1}$. A more compact way to represent is the following.

Definition 9.12 (p-adic expansion). Let $a = (a_n)$ be a p-adic integer with $a_n \in [0, p^n - 1]$. The *p-adic expansion* is $(b_0, b_1, b_2, \dots)$ with $b_0 = a_1$ and $b_n = (a_{n+1} - a_n)/p^n$.

Example 9.13

The sequences from before become

$$\begin{aligned} 2 &= (2, 0, 0, \dots) \\ 2002 &= (0, 6, 5, 5, 0, 0, \dots) \\ -2 &= (5, 6, 6, 6, \dots) \\ 2^{-1} &= (4, 3, 3, 3, \dots) \\ \sqrt{2} &= \begin{cases} (3, 1, 2, 6, 1, 2, 1, 2, 4, 6, \dots) \\ (4, 5, 4, 0, 5, 4, 5, 4, 2, 0, \dots) \end{cases} \\ \sqrt[3]{2} &= (4, 6, 1, 3, 6, 4, 3, 5, 4, 6, \dots). \end{aligned}$$

Addition in $\mathbb{Z}_p$ is done by adding p-adic expansions $(b_0, b_1, \dots) + (c_0, c_1, \dots)$ component-wise mod p and carrying to the right. Multiplication is by formal power series multiplication $(\sum b_n p^n)(\sum c_n p^n)$.

9.3 Extending valuations

Definition 9.14 (extends). Let L/K be a finite separable extension, and let ν_1 and ν_2 be discrete valuations on K and L respectively. If $\nu_2|_K = e\nu_1$ for some $e \in \mathbb{Z}_{>0}$, then ν_2 *extends* ν_1 with index e.

Theorem 9.15

AKLB. Let $\mathfrak{p}$ be a prime of A. Then for all $\mathfrak{q} \mid \mathfrak{p}$, the discrete valuation $\nu_{\mathfrak{q}}$ extends $\nu_{\mathfrak{p}}$ with index $e_{\mathfrak{q}}$, and every discrete valuation on L that extends $\nu_{\mathfrak{p}}$ arises this way. In other words, the map $\mathfrak{q} \mapsto \nu_{\mathfrak{q}}$ is a bijection from $\{\mathfrak{q} \mid \mathfrak{p}\}$ to valuations of L extending $\nu_{\mathfrak{p}}$.

10 Local fields and Hensel's lemmas

10.1 Local fields

Definition 10.1 (global field)**.** A *global field* is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$.

Definition 10.2 (local field)**.** A *local field* is a field with a nontrivial absolute value that is *locally compact* in the induced topology, meaning every point lies in a compact neighborhood.

Example 10.3

$\mathbb{R}$ and $\mathbb{C}$ are local fields, and in fact the only archimedean local fields. $\mathbb{Q}$ is not a local field.

It turns out that local fields are the completion of a global field with respect to some absolute value.

Lemma 10.4

Let K be a field with a nontrivial absolute value. Then K is a local field if and only if every (equivalently, any) closed ball is compact.

Proof. ($\Rightarrow$) Suppose K is a local field. For all $z \in K$, the map $x \mapsto x + z$ is continuous, so it suffices to show that every closed ball about 0 is compact. 0 lies in a compact neighborhood containing a closed ball $B_{\leq s}(0)$ which is compact. Now fix $\alpha \in K^\times$ with $|\alpha| > 1$. The map $x \mapsto \alpha x$ is continuous and $|\cdot|$ is multiplicative, so $B_{\leq |\alpha|^n s}(0)$ is compact for every $n \geq 1$. Then every closed ball $B_{\leq r}(0)$ about 0 is compact, because it is a closed subset of some $B_{\leq |\alpha|^n s}(0)$ with increasing radii $|\alpha|^n s$.

($\Leftarrow$) This is immediate. "Any" implies "every" because we can replace $B_{\leq s}(0)$ with any closed ball. □

Corollary 10.5

If K is a local field, then K is complete.

Proof. Suppose not, and consider a Cauchy sequence (x_n) in K converging to $x \in \widehat{K} - K$. Pick $N \in \mathbb{Z}_{>0}$ such that $|x_n - x| < \frac{1}{2}$ for all $n \geq N$. Consider $S := B_{\leq 1}(x_N)$. Then (x_n) has a convergent subsequence in $S \subseteq K$, contradicting the fact that S is compact (Lemma 10.4). (We are using the fact that in a metric space, compact implies sequentially compact.) □

This is another proof that $\mathbb{Q}$ is not a local field.

Proposition 10.6

Let K be a field with absolute value $|\cdot|_\nu$ induced by a discrete valuation. Let $A = \{x \in K : |x|_\nu \leq 1\}$ be the valuation ring with uniformizer π. Then K is a local field if and only if K is complete and $A/\pi A$ is finite.

Proof. ($\Rightarrow$) After Corollary 10.5, it remains to show that $A/\pi A$ is finite. We know that $A = B_{\leq 1}(0)$ is compact. The cosets $x + \pi A$ of the subgroup $\pi A \subseteq A$ are open balls $B_{<1}(x)$ since $y \in x + \pi A$ if and only if $|x-y|_\nu \leq |\pi|_\nu < 1$. The cosets $\{x + \pi A : x \in A\}$ form an open cover of A, which is compact, so there is a finite subcover. Thus, $A/\pi A$ is finite.

($\Leftarrow$) K complete implies A complete, and we have $A = \widehat{A} \simeq \varprojlim_n A/\pi^n A$. Each quotient $A/\pi^n A$ is finite and therefore compact, so the inverse limit A is compact. Then A is a compact closed ball, which implies K is a local field by Lemma 10.4. □

Corollary 10.7

Let L be a global field with $|\cdot|_\nu$ any nontrivial absolute value. Then the completion L_ν is a local field.

Proof. We know L/K is a finite extension where $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$. Then $A = \mathbb{Z}$ or $\mathbb{F}_q[t]$ is a DD, as is its integral closure B inside L. If $|\cdot|_\nu$ is archimedean, then $K = \mathbb{Q}$, and L_ν is a finite extension of $\mathbb{R}$. Then L_ν is $\mathbb{R}$ or $\mathbb{C}$, both of which are local fields.

Now suppose $|\cdot|_\nu$ is non-archimedean, and we claim it is induced by a discrete valuation. Let

$$C \coloneqq \{x \in L : |x| \leq 1\}, \quad \mathfrak{m} = \{x \in L : |x|_\nu < 1\}.$$

Note $\mathfrak{m} \neq 0$. The restriction of $|\cdot|_\nu$ to K is still non-archimedean, and from pset 1 we know that it is induced by a discrete valuation. In particular, $|x|_\nu \leq 1$ for all $x \in A$, so $A \subseteq C$. C is integrally closed in its fraction field L (true in general for valuation rings), so $B \subseteq C$. Let $\mathfrak{q} = \mathfrak{m} \cap B$ which is a maximal ideal of B. The DVR $B_\mathfrak{q}$ is contained in $C \subseteq L$, and in fact we must have $B_\mathfrak{q} = C$ because there are no rings properly between a DVR $B_\mathfrak{q}$ and its fraction field L. Then $|\cdot|_\nu \simeq |\cdot|_{\nu_\mathfrak{q}}$.

The residue field $B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} \simeq B/\mathfrak{q}$ is finite, since $B/\mathfrak{q}$ is a finite extension of the finite field $A/\mathfrak{p}$, where $\mathfrak{p} = \mathfrak{q} \cap A$. Now consider the completion L_ν with valuation ring B_ν. Taking a uniformizer π of $\mathfrak{q} \subseteq B$ as a uniformizer for B_ν, we have

$$B/\mathfrak{q} \simeq B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} \simeq B_\mathfrak{q}/\pi B_\mathfrak{q} \simeq B_\nu/\pi B_\nu$$

so $B_\nu/\pi B_\nu$ is finite. Thus L_ν is complete with an absolute value induced by a discrete valuation and finite residue field, which implies it is a local field (Proposition 10.6). □

Proposition 10.8

A locally compact topological vector space over a nondiscrete locally compact field has finite dimension.

Theorem 10.9

Let L be a local field. If L is archimedean, then $L = \mathbb{R}$ or $\mathbb{C}$. Otherwise, L is isomorphic to a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$.

Proof. We know L is complete. If $\operatorname{char} L = 0$ then $\mathbb{Q} \subseteq L$ which implies $\mathbb{R} \subseteq L$ if archimedean, or $\mathbb{Q}_p \subseteq L$ if non-archimedean (pset 1). If $\operatorname{char} L = p > 0$, then $\mathbb{F}_p \subseteq L$, and L contains a transcendental element $s \in L$, because no algebraic extension of $\mathbb{F}_p$ has a nontrivial absolute value. So $\mathbb{F}_p(s) \subseteq L$, which means $\mathbb{F}_q((t)) \subseteq L$ for some q a power of p. In summary, L contains a subfield K isomorphic to

- $\mathbb{R}$ if $\operatorname{char} L = 0$ archimedean
- $\mathbb{Q}_p$ if $\operatorname{char} L = 0$ non-archimedean
- $\mathbb{F}_q((t))$ if $\operatorname{char} L = p > 0$.

In all cases, K is a local field and thus locally compact. It is also a finite extension by Proposition 10.8. □

10.2 Hensel's lemmas

Let R be a commutative ring with formal derivatives $f \mapsto f'$ on $R[x]$. It satisfies the usual properties of

$$\begin{aligned}(af+bg)' &= af' + bg' \\ (fg)' &= f'g + fg' \\ (f \circ g)' &= (f' \circ g)g'\end{aligned}$$

for $f, g \in R[t]$.

Lemma 10.10

Given $f = \sum_i f_i x^i \in R[x]$ and $a \in R$, we have

$$f(x) = f(a) + f'(a)(x-a) + g(x)(x-a)^2$$

for a unique $g \in R[x]$.

Proof. By the binomial theorem, we have

$$f(x) = f(a + (x-a)) = \sum_i f_i(a + (x-a))^i = f(a) + f'(a)(x-a) + g(x)(x-a)^2.$$

□

This is like the Taylor expansion $f(x) = \sum_i \frac{f^{(i)}(a)}{i!}(x-a)^i$, but we should be careful as $i!$ could be a zero divisor. Actually $f^{(i)}/i!$ is a well-defined element of R.

Corollary 10.11

We have $f(a) = f'(a) = 0$ if and only if $f(x) = (x-a)^2 g(x)$ for some $g \in R[x]$.

Definition 10.12 (simple root)**.** If $f(a) = 0$ and $f'(a) \neq 0$, then a is a *simple root* of f.

Lemma 10.13 (Hensel I)

Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field $k = A/\mathfrak{p}$. Let $f \in A[x]$ be monic with reduction $\overline{f} \in k[x]$ has $\overline{a} \in k$ as a simple root. Then there exists a lift $a \in A$ of $\overline{a}$ such that $f(a) = 0$.

It turns out this lift will also be unique.

Proof. Work in $K = \operatorname{Frac} A$, and let a_0 be any lift of $\overline{a}$. We construct a Cauchy sequence (a_n) such that each a_n is a root of f mod $\mathfrak{p}^{2^n}$. Fix $0 < c < 1$ and define $|\cdot| = c^{\nu_\mathfrak{p}(\cdot)}$. Since $f(a_0) \in \mathfrak{p}$ but $f'(a_0) \notin \mathfrak{p}$, we have $|f(a_0)| \le c < 1$ and $|f'(a_0)| = 1$. Let

$$\epsilon := \frac{|f(a_0)|}{|f'(a_0)|^2} < 1.$$

We define

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

and can show by induction that

1. $|a_n| \le 1$, so $a_n \in A$.
2. $|a_n - a_0| \le \epsilon < 1$, so $a_n \equiv a_0 \pmod{\mathfrak{p}}$, and a_n is a lift of $\overline{a}$.
3. $|f'(a_n)| = |f'(a_0)|$, so $f'(a_n) \mid f(a_n)$ and a_{n+1} is well defined.
4. $|f(a_n)| \le \epsilon^{2^n} |f'(a_0)|^2$, so $|f(a_n)|$ and $f(a_n)$ converge to 0 rapidly.

Then $|a_{n+1} - a_n| \le \epsilon^{2^n} \to 0$ so (a_n) is Cauchy. The limit $a \in A$ (by A complete) is a root of f and satisfies $a \equiv a_0 \pmod{\mathfrak{p}}$. □

To prove Hensel I, we only needed $\epsilon < 1$, not that $\overline{a}$ is a simple root. A seemingly stronger version is the following, but it turns out they are equivalent.

Lemma 10.14 (Hensel II)

Let A be a DVR. Let $f \in A[x]$, and suppose $a_0 \in A$ satisfies $|f(a_0)| < |f'(a_0)|^2$. Defining

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

the sequence (a_n) is well defined and converges to a unique $a \in A$ such that $|a - a_0| \le \epsilon := \frac{|f(a_0)|}{|f'(a_0)|^2}$ and $|f(a_n)| \le \epsilon^{2^n} |f'(a_n)|^2$ for all $n \ge 0$.

Lemma 10.15 (Hensel III)

Let A be a complete DVR with maximal ideal $\mathfrak{p}$ and residue field $k = A/\mathfrak{p}$. Let $f \in A[x]$ and $\overline{f} \in k[x]$. If $\overline{f} = \overline{g}\overline{h}$ for coprime $\overline{g}, \overline{h} \in k[x]$, then there exist lifts $g, h \in A[x]$ (so $g \equiv \overline{g} \pmod{\mathfrak{p}}$, $h \equiv \overline{h} \pmod{\mathfrak{p}}$) such that $f = gh$ with $\deg g = \deg \overline{g}$.

Lemma 10.16 (Hensel–Kürshák)

Let A be a complete DVR and $K = \operatorname{Frac} A$. If $f \in K[x]$ is **irreducible** with leading and constant coefficients in A, then $f \in A[x]$.

Proof. Let $\mathfrak{p} = (\pi)$ be the maximal ideal of A and $k := A/\mathfrak{p}$. Suppose $f = \sum_{i=0}^n f_i x^i$ is irreducible, so $f_0, f_n \neq 0$. Let $m := \min\{\nu_\mathfrak{p}(f_i)\}$. FSOC suppose $m < 0$, and let $g := \pi^{-m} f = \sum_{i=0}^n g_i x^i \in A[x]$. Then g is irreducible and $g_0, g_n \in \mathfrak{p}$ as $m < 0$ and $f_0, f_n \in A$. Also, g_i is a unit for some $0 < i < n$. The reduction $\overline{g} \in k[x]$ has positive degree, but the constant term is 0, so let $\overline{u} = x^d$ be the largest power of x dividing $\overline{g}$ where $0 < d \le \deg \overline{g} < n$. Let $\overline{v} = \overline{g}/\overline{u} \in k[x]$, which is coprime to $\overline{u}$.

By Hensel III, $g = uv$ for lifts $u, v \in A[x]$ with $0 < \deg u = \deg \overline{u} < n$, which contradicts g irreducible. □

Corollary 10.17

Let A be a complete DVR with $K = \operatorname{Frac} A$, and let L/K be a finite extension. Then $\alpha \in L$ is integral over A if and only $\mathrm{N}_{L/K}(\alpha) \in A$.

Theorem 10.18

AKLB. Suppose A is a **complete** DVR with maximal ideal $\mathfrak{p}$. Then B is a DVR whose maximal ideal $\mathfrak{q}$ is the unique prime above $\mathfrak{p}$.

Proof. There is some $\mathfrak{q} \mid \mathfrak{p}$ by considering the prime factorization of $\mathfrak{p}B$. FSOC there exist $\mathfrak{q}_1, \mathfrak{q}_2 \mid \mathfrak{p}$, with $\mathfrak{q}_1 \neq \mathfrak{q}_2$. Choose $b \in \mathfrak{q}_1 - \mathfrak{q}_2$ and consider $A[b] \subseteq B$. Then $\mathfrak{q}_1 \cap A[b]$ and $\mathfrak{q}_2 \cap A[b]$ are distinct prime ideals of $A[b]$ containing $\mathfrak{p}A[b]$. Both are maximal because they are nonzero and $\dim A[b] = \dim A = 1$.

The quotient ring $A[b]/\mathfrak{p}A[b]$ thus has two distinct maximal ideals. Let $f \in A[x]$ be the minimal polynomial of b over K, and let $\overline{f} \in (A/\mathfrak{p})[x]$ be the reduction. Then

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

and $(A/\mathfrak{p})[x]/(\overline{f})$ has at least two maximal ideals. Then $\overline{f}$ has to be divisible by at least two irreducible polynomials, so we can write $\overline{f} = \overline{g}\overline{h}$ for $\overline{g}, \overline{h}$ coprime and lift to $f = gh$ which is a contradiction as $\deg g = \deg \overline{g} \neq 0$. □

Remark 10.19. The assumption that A is complete is necessary. For example, if $A = \mathbb{Z}_{(5)}$, $K = \mathbb{Q}$, and $L = \mathbb{Q}(i)$, then $B = \mathbb{Z}_{(5)}[i]$ which is a PID but not a DVR. In particular, $(1 + 2i)$ and $(1 - 2i)$ are both maximal.

11 Extensions of complete DVRs

11.1 Norms

AKLB. Let A be a complete DVR, so B is a DVR by Theorem 10.18. We will show that B is also complete.

Definition 11.1 (norm). Let K be a field with absolute value $|\cdot|$, and let V be a K-vector space. A *norm* on V is a function $||\cdot|| \colon V \to \mathbb{R}_{\geq 0}$ such that

- $||v|| = 0 \iff v = 0$
- $||\lambda v|| = |\lambda| \, ||v||$ for all $\lambda \in K, v \in V$
- $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$.

The norm induces a topology on V via $d(v, w) := ||v - w||$.

Example 11.2 (supremum norm)

Let V be a K-vector space with basis (e_i). For $v \in V$, let $v_i \in K$ denote the coefficient of e_i in $v = \sum_i v_i e_i$. The *supremum norm* $||v||_\infty := \sup_i |v_i|$ is a norm (so every K-vector space has a norm).

If V is a K-algebra, then an absolute value $||\cdot||$ on V is a norm if and only if it extends the absolute value on K: $||\lambda|| \, ||v|| = ||\lambda v|| = |\lambda| \, ||v|| \iff ||\lambda|| = |\lambda|$.

Proposition 11.3

Let V be a finite dimensional K-vector space over a complete field K. Every norm on V induces the same topology, under which V a complete metric space.

Proof. See pset 6. □

Theorem 11.4

Let $(A, \mathfrak{p})$ be a complete DVR with $K = \operatorname{Frac} A$, discrete valuation $\nu_\mathfrak{p}$, and absolute value $|x|_\mathfrak{p} := c^{\nu_\mathfrak{p}(x)}$ with $0 < c < 1$. Let L/K be a finite extension of degree n. Then

(i) There exists a unique absolute value $|x| := \left|\mathrm{N}_{L/K}(x)\right|_\mathfrak{p}^{1/n}$ on L that extends $|\cdot|_\mathfrak{p}$.

(ii) L is complete with respect to $|\cdot|$, and the valuation ring $\{x \in L : |x| \le 1\}$ is the integral closure B of A in L.

(iii) If L/K is separable, then B is a complete DVR whose maximal ideal $\mathfrak{q}$ induces

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

where $e_\mathfrak{q}$ is the ramification index, i.e. $\mathfrak{p}B = \mathfrak{q}^{e_\mathfrak{q}}$.

Proof. It is not obvious that $|\cdot|$ is an absolute value, but assume that it is for now. For all $x \in K$, we have

$$|x| := \left|\mathrm{N}_{L/K}(x)\right|_\mathfrak{p}^{1/n} = |x^n|_\mathfrak{p}^{1/n} = |x|_\mathfrak{p},$$

so $|\cdot|$ extends $|\cdot|_\mathfrak{p}$, and is a norm on L. Since $|\cdot|_\mathfrak{p}$ is nontrivial, we have $|x|_\mathfrak{p} \ne 1$ for some $x \in K^\times$. From $|x|^a = |x|_\mathfrak{p} = |x| \iff a = 1$, $|\cdot|$ is the unique absolute value (in its equivalence class) extending $|\cdot|_\mathfrak{p}$. Every norm induces the same topology by Proposition 11.3, so every absolute value on L is equivalent to $|\cdot|$.

Now we check that $|\cdot|$ is an absolute value.

- $|x| = 0 \iff x = 0$ by construction.
- $|\cdot|$ is multiplicative by construction.
- Triangle inequality: it suffices to show that $|x| \le 1 \implies |x+1| \le |x| + 1$. We have

$$|x| \le 1 \iff \left|\mathrm{N}_{L/K}(x)\right|_\mathfrak{p} \le 1 \iff \mathrm{N}_{L/K}(x) \in A \iff x \in B$$

  where the last equivalence is by Corollary 10.17. Finally, $x \in B \iff x + 1 \in B \iff |x+1| \le 1$ by reversing the above chain of equivalences with $x+1$ instead of x. This is in fact even stronger than the triangle inequality.

This proves (i) and (ii).

For (iii), we now assume L/K is separable. B is a DVR and is complete because it is the valuation ring of L. Letting $\mathfrak{q}$ denote the maximal ideal of B, then $\nu_\mathfrak{q}$ extends $\nu_\mathfrak{p}$ with index $e_\mathfrak{q}$ by Theorem 9.15. So $\nu_\mathfrak{q}(x) = e_\mathfrak{q}\nu_\mathfrak{p}(x)$ for all $x \in K$. Since $0 < c^{1/e_\mathfrak{q}} < 1$, $|x|_\mathfrak{q} := (c^{1/e_\mathfrak{q}})^{\nu_\mathfrak{q}(x)}$ is an absolute value of L. To show $|\cdot| = |\cdot|_\mathfrak{q}$, it suffices to show by the uniqueness in (i) that $|\cdot|_\mathfrak{q}$ extends $|\cdot|_\mathfrak{p}$. Indeed, for all $x \in K$,

$$|x|_\mathfrak{q} = c^{\nu_\mathfrak{q}(x)/e_\mathfrak{q}} = c^{\nu_\mathfrak{p}(x)} = |x|_\mathfrak{p}.$$

□

Remark 11.5. Another definition of a Henselian valuation ring A is that the absolute value of K can be uniquely extended to $\overline{K}$.

Corollary 11.6

AKLB. Let $(A, \mathfrak{p})$ be a complete DVR, and let $\mathfrak{q} \mid \mathfrak{p}$ (which is unique because B is a DVR). Then $\nu_{\mathfrak{q}}(x) = \frac{1}{f_{\mathfrak{q}}}\nu_{\mathfrak{p}}(\mathrm{N}_{L/K}(x))$ for all $x \in L$.

Proof. $\nu_{\mathfrak{p}}(\mathrm{N}_{L/K}(x)) = \nu_{\mathfrak{p}}(\mathrm{N}_{L/K}((x))) = \nu_{\mathfrak{p}}(\mathrm{N}_{L/K}(\mathfrak{q}^{\nu_{\mathfrak{q}}(x)})) = \nu_{\mathfrak{p}}(\mathfrak{p}^{f_{\mathfrak{q}}\nu_{\mathfrak{q}}(x)}) = f_{\mathfrak{q}}\nu_{\mathfrak{q}}(x)$. □

11.2 Local Dedekind–Kummer theorem

Lemma 11.7 (Nakayama)

Let $(A, \mathfrak{p})$ be a local ring, and let M be a finitely generated A-module. If the images of $x_1, \ldots, x_n \in M$ generate $M/\mathfrak{p}M$ as an $(A/\mathfrak{p})$-vector space, then $x_1, \ldots, x_n$ generate M as an A-module.

Corollary 11.8

Let $(A, \mathfrak{p})$ be a local Noetherian ring, $g \in A[x]$ monic, and $B = A[x]/(g(x))$. Then every maximal ideal $\mathfrak{m}$ of B contains $\mathfrak{p}B$.

Corollary 11.9

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

This is similar to the Dedekind–Kummer theorem.

Proof. $B \to B/\mathfrak{p}B$ gives a 1-to-1 correspondence of maximal ideals, and

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

The maximal ideals in $(A/\mathfrak{p})[x]/(\overline{g}(x))$ correspond to irreducible factors of $\overline{g}$ because $(A/\mathfrak{p})[x]$ is a PID. □

Theorem 11.10

AKLB. Let $(A, \mathfrak{p}), (B, \mathfrak{q})$ be DVRs with residue fields $k := A/\mathfrak{p}, \ell := B/\mathfrak{q}$. If ℓ/k is separable, then $B = A[\alpha]$ for some $\alpha \in B$ (monogenic). Moreover if L/K is unramified, then this holds for every lift α of any generator $\overline{\alpha}$ for $\ell = k(\overline{\alpha})$.

Proof. Let $\mathfrak{p}B = \mathfrak{q}^e$ and $f = [\ell : k]$. Then $ef = n := [L : K]$. Since ℓ/k is separable, we can write $\ell = k(\overline{\alpha_0})$ for some $\overline{\alpha_0} \in \ell$ whose minimal polynomial $\overline{g}$ is separable of degree f. Let $g \in A[x]$ be a monic lift of $\overline{g}$, and let $\alpha_0 \in B$ be any lift of $\overline{\alpha_0}$. If $\nu_{\mathfrak{q}}(g(\alpha_0)) = 1$, let $\alpha := \alpha_0$. Otherwise, let π_0 be a uniformizer of B and set $\alpha := \alpha_0 + \pi_0 \in B$ so $\alpha \equiv \overline{\alpha_0} \pmod{\mathfrak{q}}$. Writing $g(x + \pi_0) = g(x) + \pi_0 g'(x) + \pi_0^2 h(x)$ for some $h \in A[x]$ by Lemma 10.10, we have

$$\nu_{\mathfrak{q}}(g(\alpha)) = \nu_{\mathfrak{q}}(g(\alpha_0 + \pi_0)) = \nu_{\mathfrak{q}}(g(\alpha_0) + \pi_0 g'(\alpha_0) + \pi_0^2 h(\alpha_0)) = 1.$$

In both cases, $\pi := g(\alpha)$ is also a uniformizer for B.

Now we claim $B = A[\alpha]$, or equivalently that $1, \alpha, \ldots, \alpha^{n-1}$ is an A-module basis for B. By Nakayama, it suffices to show that $1, \alpha, \ldots, \alpha^{n-1}$ span $B/\mathfrak{p}B$ as a k-vector space. Since $\mathfrak{p}B = \mathfrak{q}^e = (\pi^e)$, each element of $B/\mathfrak{p}B$ is a coset

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

where $b_0, \ldots, b_{e-1}$ are determined up to equivalence mod πB. Now $1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1}$ is a basis for $B/\pi B = B/\mathfrak{q} = \ell = k(\overline{\alpha_0})$ and $\pi = g(\alpha)$ so

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

Now $\deg g = f$ and $n = ef$, so this expresses $b + \mathfrak{p}B$ in the form $b' + \mathfrak{p}B$ with b' in the A-span of $1, \ldots, \alpha^{n-1}$. Thus $B = A[\alpha]$ by Nakayama.

If L/K is unramified, then ℓ/k is separable and $e = 1, f = n$. We don't need to require $g(\alpha)$ a uniformizer and can just take $\alpha = \alpha_0$ to be any lift of $\overline{\alpha_0}$. □

11.3 Unramified extensions of a complete DVR

Now let $(A, \mathfrak{p})$ be a complete DVR with $K := \operatorname{Frac} A$ and $k := A/\mathfrak{p}$. Every finite unramified extension L/K of degree n yields a corresponding residue field extension ℓ/k of degree n that is separable.

Finite unramified extensions L/K form a category $\mathcal{C}_K^{\text{unr}}$ whose morphisms are K-algebra homomorphisms. Finite separable extensions ℓ/k form a category $\mathcal{C}_k^{\text{sep}}$ whose morphisms are k-algebra homomorphisms.

Theorem 11.11

Let $(A, \mathfrak{p})$ be a complete DVR with $K := \operatorname{Frac} A$ and $k := A/\mathfrak{p}$. There is an equivalence of categories $F\colon \mathcal{C}_K^{\text{unr}} \to \mathcal{C}_k^{\text{sep}}$ sending each unramified extension L/K to its residue field ℓ/k.

Each K-algebra homomorphism $\varphi\colon L_1 \to L_2$ is sent to $\overline{\varphi}\colon \ell_1 \to \ell_2$ defined in the obvious way: $\overline{\varphi}(\overline{\alpha}) = \overline{\varphi(\alpha)}$ where $\alpha \in B_1$ is any lift of $\overline{\alpha} \in \ell_1 = B/\mathfrak{q}_1$ and $\overline{\varphi(\alpha)}$ is the reduction of $\varphi(\alpha) \in B_2$ to $\ell_2 = B_2/\mathfrak{q}_2$.

In particular if L_1, L_2 have residue fields ℓ_1, ℓ_2, then we have a bijection of sets

$$\operatorname{Hom}_K(L_1, L_2) \xrightarrow{\sim} \operatorname{Hom}_k(\ell_1, \ell_2).$$

Proof (sketch). We can check that F is well defined. We need to show that it is essentially surjective (every separable ℓ/k is isomorphic to the residue field of some L/K) and fully faithful (bijection of Hom sets). For essentially surjective, ℓ/k separable implies $\ell \simeq k(\overline{\alpha}) = k[x]/(\overline{g}(x))$ for some $\overline{g}$ monic, separable, and irreducible of degree $n = [\ell : k]$. We lift $\overline{g}$ to a monic, irreducible, separable $g \in A[x]$ of degree n. Let $L := K[x]/(g(x)) = K(\alpha)$ where α is the image of x in $K[x]/(g(x))$. By the Dedekind–Kummer theorem, $(\mathfrak{p}, g(\alpha)) = \mathfrak{p}A[\alpha]$ is the unique maximal ideal of $A[\alpha]$. Then

$$\frac{B}{\mathfrak{q}} \simeq \frac{A[\alpha]}{(\mathfrak{p}, g(\alpha))} \simeq \frac{A[x]}{(\mathfrak{p}, g(x))} \simeq \frac{(A/\mathfrak{p})[x]}{(\overline{g}(x))} \simeq \ell.$$

L/K has degree $[L : K] = \deg g = [\ell : k] = n$, so L/K is an unramified extension of degree $n = [\ell : k]$.

See notes for fully faithful. □

Corollary 11.12

AKLB. Let A be a complete DVR with residue field k. Then L/K is unramified if and only if $B = A[\alpha]$ for some $\alpha \in L$ whose minimal polynomial $g \in A[x]$ has a separable reduction $\overline{g} \in k[x]$.

Proof. The forward direction was proven in the above theorem. For the reverse direction, note that $\overline{g}$ must be irreducible. Then ℓ/k is separable and has the same degree as L/K, so L/K is unramified. □

Corollary 11.13

AKLB, A a complete DVR. Let ζ_n be a primitive nth root of unity in $\overline{K}$, with n coprime to $\operatorname{char} k$. Then $K(\zeta_n)/K$ is unramified.

$K(\zeta_n)$ is the splitting field of $x^n - 1 \in K[x]$, which is separable because n is coprime to $\operatorname{char} k$.

Corollary 11.14

AKLB, A a complete DVR. Now assume the residue field $A/\mathfrak{p} = \mathbb{F}_q$ is finite. Suppose the degree of L/K is n. Then L/K is unramified if and only if $L \simeq K(\zeta_{q^n-1})$. When this holds, $A[\zeta_{q^n-1}]$ is the integral closure of A in L, and L/K is Galois with $\operatorname{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$.

Definition 11.15 (maximal unramified extension)**.** For L/K separable, the *maximal unramified extension of K in L* is the subfield

$$\bigcup_{\substack{K \subseteq E \subseteq L \\ E/K \text{ fin. unram.}}} E \subseteq L$$

where the union is over finite unramified subextensions E/K.

When $L = K^{\text{sep}}$, this is the *maximal unramified extension of K*, denoted K^{unr}.

12 Totally ramified extensions and Krasner's lemma

12.1 Totally ramified extensions

AKLB. Suppose $(A, \mathfrak{p})$ is a complete DVR, so $(B, \mathfrak{q})$ is a complete DVR, and $[L : K] = e_{L/K} f_{L/K}$, where we write $e_{L/K} = e_{\mathfrak{q}}$ and $f_{L/K} = f_{\mathfrak{q}}$. We can uniquely decompose L/K as $L/E/K$ such that E/K is unramified ($e_{E/K} = 1$, $f_{E/K} = f_{L/K}$) and L/E is totally ramified ($e_{L/E} = e_{L/K}$, $f_{L/E} = 1$).

Definition 12.1 (Eisenstein)**.** Let $(A, \mathfrak{p})$ be a DVR. A monic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x]$$

is *Eisenstein* if $a_i \in \mathfrak{p}$ for $0 \leq i < n$ and $a_0 \notin \mathfrak{p}^2$ (i.e. $v_{\mathfrak{p}}(a_0) = 1$ and a_0 is a uniformizer).

Lemma 12.2 (Eisenstein irreducibility)

If $f \in A[x]$ is Eisenstein, then f is irreducible in $A[x]$ and $K[x]$.

Lemma 12.3

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

Theorem 12.4

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

Proof. Let $n = [L : K]$, $\mathfrak{p}$ be the maximal ideal of A, and $\mathfrak{q}$ be the maximal ideal of B. Let $f \in A[x]$ be the minimal polynomial of π.

($\Leftarrow$) If $B = A[\pi]$ and f is Eisenstein, then $\mathfrak{p}B = \mathfrak{q}^n$ by local Dedekind–Kummer (Corollary 11.9). Therefore $\nu_\mathfrak{q}$ extends $\nu_\mathfrak{p}$ with index $e_\mathfrak{q} = n$, and L/K is totally ramified.

($\Rightarrow$) Suppose L/K is totally ramified. Then $\nu_\mathfrak{q}$ extends $\nu_\mathfrak{p}$ with index $e_{L/K} = n$, so $\nu_\mathfrak{q}(K) = n\mathbb{Z}$. The set $\{\pi^0, \pi^1, \dots, \pi^{n-1}\}$ is linearly independent over K because the π^i have distinct valuations modulo $\nu_\mathfrak{q}(K) = n\mathbb{Z}$, so $L = K(\pi)$. Let $f = \sum_i a_i x^i \in A[x]$ be the minimal polynomial of π. From $\nu_\mathfrak{q}(a_i\pi^i) \equiv i \pmod{n}$ for all $0 \le i < n$, we need

$$\nu_\mathfrak{q}(a_0) = \nu_\mathfrak{q}(a_0\pi^0) = \nu_\mathfrak{q}(a_n\pi^n) = n < \nu_\mathfrak{q}(a_i\pi^i) \quad (0 < i < n)$$

to get $\nu_q(f(\pi)) = \infty$. Then $\nu_\mathfrak{p}(a_0) = 1$ ($\nu_\mathfrak{q}$ extends $\nu_\mathfrak{p}$ with index n) and $\nu_\mathfrak{p}(a_i) \ge 1$ for $0 \le i < n$, so f is Eisenstein. By Lemma 12.3, $A[\pi] \subseteq B$ is a DVR, but DVRs are maximal so $A[\pi] = B$. □

Example 12.5

For $K = \mathbb{Q}_3$, there are three distinct quadratic extensions: $\mathbb{Q}_3(\sqrt{2})$, $\mathbb{Q}_3(\sqrt{3})$, and $\mathbb{Q}_3(\sqrt{6})$. The extension $\mathbb{Q}_3(\sqrt{2}) = \mathbb{Q}_3(\zeta_8)$ is the unique unramified quadratic extension of $\mathbb{Q}_3$. The other two are ramified and equal $\mathbb{Q}_3[x]/(x^2-3)$ and $\mathbb{Q}_3[x]/(x^2-6)$, where x^2-3 and x^2-6 are Eisenstein.

Definition 12.6 (tame, wild). **AKLB**, $(A, \mathfrak{p})$ complete DVR, separable residue field extension with char $A/\mathfrak{p} = p \ge 0$. L/K is

- *tamely ramified* if $p \nmid e_{L/K}$ (always true if $p = 0$). Note that unramified extensions ($e_{L/K} = 1$) are tamely ramified.
- *wildly ramified* if $p \mid e_{L/K}$.
- *totally tamely ramified* if $p \nmid e_{L/K} = [L : K]$.
- *totally wildly ramified* if $e_{L/K} = [L : K]$ is a power of p.

Since ramification indices multiply in towers, and separability is transitive in towers, we have the following.

Proposition 12.7

Being unramified, tamely ramified, wildly ramified, totally tamely ramified, or totally wildly ramified are transitive in towers of fraction fields of complete DVRs with separable residue field extensions (including all local fields).

Remark 12.8. A composite of totally ramified extensions need not be totally ramified. For example, $\mathbb{Q}_3(\sqrt{3}, \sqrt{6})$ contains $\mathbb{Q}_3(\sqrt{2})$ which is unramified and not totally ramified.

Theorem 12.9

AKLB, $(A, \mathfrak{p})$ complete DVR, separable residue field extension. Suppose $\operatorname{char} A/\mathfrak{p} = p \geq 0$ does not divide $n = [L : K]$. Then L/K is totally tamely ramified if and only if $L = K(\pi_A^{1/n})$ for some uniformizer π_A of A.

Proposition 12.10

Let A be a complete DVR and L be a totally ramified extension of $K = \operatorname{Frac} A$. There is a unique intermediate field E such that E/K is totally tamely ramified and L/E is totally wildly ramified.

We can split up any L/K as $L/E_0/E_1/K$ where L/E_0 is totally wildly ramified, E_0/E_1 is totally tamely ramified, and E_1/K is unramified.

12.2 Krasner's lemma

Let K be the fraction field of a complete DVR A, with absolute value $|\cdot|$. Recall that we can uniquely extend $|\cdot|$ to any finite extension L/K via $|x| \coloneqq \left|\mathrm{N}_{L/K}(x)\right|^{1/[L:K]}$ (Theorem 11.4). In particular, this induces a unique absolute value on $\overline{K}$ which restricts to $|\cdot|$ on K.

Lemma 12.11

For all $\alpha \in \overline{K}$ and $\sigma \in \operatorname{Aut}_K(\overline{K})$, we have $|\sigma(\alpha)| = |\alpha|$.

Proof. Note α and $\sigma(\alpha)$ have the same minimal polynomial $f \in K[x]$ because $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$. Then $\mathrm{N}_{K(\alpha)/K}(\alpha) = (-1)^n f(0) = \mathrm{N}_{K(\sigma(\alpha))/K}(\sigma(\alpha))$, where $n = [K(\alpha) : K] = [K(\sigma(\alpha)) : K]$. Then

$$|\sigma(\alpha)| = \left|\mathrm{N}_{K(\sigma(\alpha))/K}(\sigma(\alpha))\right|^{1/n} = \left|\mathrm{N}_{K(\alpha)/K}(\alpha)\right|^{1/n} = |\alpha|. \qquad \square$$

Definition 12.12. For $\alpha, \beta \in \overline{K}$, we say β *belongs to* α if $|\beta - \alpha| < |\beta - \sigma(\alpha)|$ for all $\sigma \in \operatorname{Aut}_K(\overline{K})$ with $\sigma(\alpha) \neq \alpha$.

In other words, β is closer to α than α's Galois conjugates. By the non-archimedean triangle inequality, this is also equivalent to $|\beta - \alpha| < |\alpha - \sigma(\alpha)|$ (each triangle is isosceles and has a shortest side).

Lemma 12.13 (Krasner)

For $\alpha, \beta \in \overline{K}$, if β belongs to α and α is separable over K, then $K(\alpha) \subseteq K(\beta)$.

Proof. Suppose not, so β belongs to α but $\alpha \notin K(\beta)$. Then $K(\alpha, \beta)/K(\beta)$ is a nontrivial separable extension, so there exists $\sigma \in \operatorname{Aut}_{K(\beta)}(\overline{K})$ such that $\sigma(\alpha) \neq \alpha$ (send α to a different root of the minimal polynomial of α over $K(\beta)$). By Lemma 12.11, we have $|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\beta - \sigma(\alpha)|$ which β belonging to α. $\square$

Definition 12.14 (L^1-norm). The L^1*-norm* of $f = \sum_i f_i x^i \in K[x]$ is

$$\|f\|_1 \coloneqq \sum_i |f_i|.$$

$\|\cdot\|_1$ is a norm on the K-vector space $K[x]$.

Lemma 12.15

Let K be a field with absolute value $|\cdot|$, and let $f \coloneqq \prod_{i=1}^{n}(x-\alpha_i) \in K[x]$ be monic with roots $\alpha_i \in L$. Extending $|\cdot|$ to L, then $|\alpha_i| < ||f||_1$ for all α_i.

Theorem 12.16 (Continuity of roots)

Let K be the fraction field of a complete DVR and $f \in K[x]$ be monic, irreducible, and separable. There exists $\delta = \delta(f) \in \mathbb{R}_{>0}$ such that for every monic $g \in K[x]$ with $||f-g||_1 < \delta$, every root β of g belongs to a root α of f for which $K(\beta) = K(\alpha)$.

In particular, every such g is separable, irreducible, and has the same splitting field as f.

12.3 Local extensions come from global extensions

Let $\widehat{L}$ be a local field, so it is a finite extension of $\widehat{K} = \mathbb{Q}_p$ $(p \le \infty)$ or $\mathbb{F}_q((t))$ by Theorem 10.9. We also know that the completion of a global field L at some nontrivial absolute value is a local field. Can we find a global field L such that $\widehat{L}$ is the completion of L? The answer is yes, and in fact there is a more general statement.

Theorem 12.17

Let K be a global field with a nontrivial absolute value $|\cdot|$ and completion $\widehat{K}$. Every finite separable extension $\widehat{L}/\widehat{K}$ is the completion of a finite separable extension L/K with respect to an absolute value extending $|\cdot|$. Moreover, we can choose L such that $[L:K] = [\widehat{L}:\widehat{K}]$, in which case $\widehat{L} = \widehat{K} \cdot L$ (compositum).

Proof. If $|\cdot|$ is archimedean, then $\widehat{K} = \mathbb{R}$ or $\mathbb{C}$, and $\widehat{L}$ is a trivial or quadratic extension. The only nontrivial case is when $\widehat{K} \simeq \mathbb{R}$ and $\widehat{L} = \widehat{K}(\sqrt{d}) \simeq \mathbb{C}$ for some $d \in \mathbb{Z}_{<0}$. Then we can take $L \coloneqq K(\sqrt{d})$ and define $\left|\sqrt{d}\right| = \sqrt{-d}$.

If $|\cdot|$ is non-archimedean, then the valuation ring of $\widehat{K}$ is a complete DVR, and $|\cdot|$ is induced by the discrete valuation. By the primitive element theorem, $\widehat{L} = \widehat{K}[x]/(f)$ for some monic irreducible separable $f \in \widehat{K}[x]$. K is dense in $\widehat{K}$, so we can find a monic $g \in K[x] \subseteq \widehat{K}[x]$ such that $||g-f||_1 < \delta$ for any $\delta > 0$. By continuity of roots, $\widehat{L} = \widehat{K}[x]/(g)$ and g is separable and irreducible.

Let $L \coloneqq K[x]/(g)$. Then $[\widehat{L}:\widehat{K}] = \deg g = [L:K]$. The field $\widehat{L}$ contains $\widehat{K}$ and L, and is the smallest field that does by inspection, so it is the compositum $\widehat{K} \cdot L$. The absolute value on $\widehat{L}$ restricts to an absolute value on L extending $|\cdot|$ on K. $\widehat{L}$ is complete, so it contains the completion of L. On the other hand, the completion of L contains L and $\widehat{K}$, so it must be $\widehat{L}$. □

Example 12.18

Let $K = \mathbb{Q}$, $\widehat{K} = \mathbb{Q}_7$, and $\widehat{L} = \widehat{K}[x]/(x^3-2)$. $\widehat{L}/\widehat{K}$ is Galois, since $\widehat{K}$ contains ζ_3 (we can lift the root 2 of $x^2+x+1 \in \mathbb{F}_7[x]$ to a root of $x^2+x+1 \in \mathbb{Q}_7[x]$ by Hensel's lemma). Thus x^3-2 splits completely in $\widehat{L}$. However, $L = K[x]/(x^3-2)$ is not Galois because it does not contain ζ_3.

However, if we replace K with $\mathbb{Q}(\zeta_3)$, then $L = K[x]/(x^3-2)$ is a Galois extension of K.

Corollary 12.19

For every finite Galois extension $\widehat{L}/\widehat{K}$ of local fields, there exists a finite Galois extension L/K of global fields and an absolute value $|\cdot|$ on L such that $\widehat{L}, \widehat{K}$ are the completions of L, K with respect to $|\cdot|, |\cdot|$ restricted to K, and $\operatorname{Gal}(L/K) \simeq \operatorname{Gal}(\widehat{L}/\widehat{K})$.

Theorem 12.20

AKLB. Let $\mathfrak{p}$ be a prime of A with $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$. Let $K_\mathfrak{p}$ be the completion of K with respect to $|\cdot|_\mathfrak{p}$, and for each $\mathfrak{q} \mid \mathfrak{p}$ let $L_\mathfrak{q}$ be the completion of L with respect to $|\cdot|_\mathfrak{q}$. Let $\widehat{\mathfrak{p}}$ and $\widehat{\mathfrak{q}}$ be the maximal ideals of the valuation rings of $K_\mathfrak{p}$ and $L_\mathfrak{q}$, respectively.

1. Each $L_\mathfrak{q}/K_\mathfrak{p}$ is a finite separable extension with $[L_\mathfrak{q} : K_\mathfrak{p}] \le [L : K]$.
2. Each $\widehat{\mathfrak{q}}$ is the unique prime above $\widehat{\mathfrak{p}}$ in $L_\mathfrak{q}/K_\mathfrak{p}$.
3. Each $\widehat{\mathfrak{q}}$ has ramification index $e_{\widehat{\mathfrak{q}}} = e_\mathfrak{q}$ and residue field degree $f_{\widehat{\mathfrak{q}}} = f_\mathfrak{q}$.
4. $[L_\mathfrak{q} : K_\mathfrak{p}] = e_\mathfrak{q} f_\mathfrak{q}$.
5. The map $L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$ defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$ is an isomorphism of finite étale $K_\mathfrak{p}$-algebras.
6. If L/K is Galois, then each $L_q/K_\mathfrak{p}$ is Galois with $D_\mathfrak{q} \simeq D_{\widehat{\mathfrak{q}}} = \operatorname{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ and $I_\mathfrak{q} \simeq I_{\widehat{\mathfrak{q}}}$.

"If you want to know what is happening at $\mathfrak{p}$, take the completion."

Proof.

1. The embedding of fields $K \hookrightarrow L$ induces $K_\mathfrak{p} \hookrightarrow L_\mathfrak{q}$ by sending $[(x_n)] \mapsto [(x_n)]$; a sequence that is Cauchy in K with respect to $|\cdot|_\mathfrak{p}$ is also Cauchy in L with respect to $|\cdot|_\mathfrak{q}$ because $\nu_\mathfrak{q}$ extends $\nu_\mathfrak{p}$. Then $K_\mathfrak{p}$ is a topological subfield of $L_\mathfrak{q}$, and we claim that $[L_\mathfrak{q} : K_\mathfrak{p}] \le [L : K]$ because any K-basis for L spans L_q as a $K_\mathfrak{p}$-vector space. Given a Cauchy sequence $y := (y_n)$ in L, write $y_n = x_{1,n}b_1 + \cdots + x_{m,n}b_m$ where $b_1, \ldots, b_m$ is a K-basis for L and $x_{i,j} \in K$. Then letting $x_1 := (x_{1,n}), \ldots, x_m := (x_{m,n})$, we can write $[y] = [x_1]b_1 + \cdots + [x_m]b_m$ as a $K_\mathfrak{p}$-linear combination of $b_1, \ldots, b_m$.

   Since L/K is separable, L is a finite étale K-algebra, and the base change $L \otimes_K K_\mathfrak{p}$ is a finite étale $K_\mathfrak{p}$-algebra by Proposition 5.33. Consider the $K_\mathfrak{p}$-algebra homomorphism $\phi_\mathfrak{q} \colon L \otimes_K K_\mathfrak{p} \to L_\mathfrak{q}$ by $\ell \otimes x \mapsto \ell x$. Since $\phi_\mathfrak{q}(b_i \otimes 1) = b_i$ and the b_i span $L_\mathfrak{q}$ as a $K_\mathfrak{p}$-vector space, $\phi_\mathfrak{q}$ is surjective. By Proposition 5.29, $L_\mathfrak{q}$ is isomorphic to a subproduct and thus also a finite étale $K_\mathfrak{p}$-algebra. In particular, $L_\mathfrak{q}/K_\mathfrak{p}$ is separable.

2. Since $K_\mathfrak{p}$ and $L_\mathfrak{q}$ are fraction fields of complete DVRs, this follows from Theorem 10.18.

5. Let $\phi = \prod_{\mathfrak{q}|\mathfrak{p}} \phi_\mathfrak{q} \colon L \otimes_K K_\mathfrak{p} \to \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$ send $(\ell \otimes x) \mapsto (\ell x, \ldots, \ell x)$. Then ϕ is a $K_\mathfrak{p}$-algebra homomorphism. By Proposition 5.33 and part 4,

$$\dim_{K_\mathfrak{p}}(L \otimes_K K_\mathfrak{p}) = \dim_K L = [L : K] = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q} = \sum_{\mathfrak{q}|\mathfrak{p}} [L_\mathfrak{q} : K_\mathfrak{p}] = \dim_{K_\mathfrak{p}} \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}. \qquad \square$$

Corollary 12.21

AKLB. For $\mathfrak{p}$ a prime of A and $\alpha \in L$, we have

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{N}_{L_\mathfrak{q}/K_\mathfrak{p}}(\alpha), \quad \mathrm{T}_{L/K}(\alpha) = \sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{T}_{L_\mathfrak{q}/K_\mathfrak{p}}(\alpha).$$

Corollary 12.22

AKLB. Let $\widehat{A}_\mathfrak{p}$ be the completion of A with respect to $|\cdot|_\mathfrak{p}$ and $\widehat{B}_\mathfrak{q}$ be the completion of B with respect to $|\cdot|_\mathfrak{q}$. Then $B \otimes_A \widehat{A}_\mathfrak{p} \simeq \prod_{\mathfrak{q}|\mathfrak{p}} \widehat{B}_\mathfrak{q}$ as $\widehat{A}_\mathfrak{p}$-algebras.

Remark 12.23. Localizing and completing is equivalent to completing (and localizing, although it's not needed). Both yield complete DVRs.

13 Different and discriminant

13.1 Different

Recall that an A-lattice M in a K-vector space has a dual lattice

$$M^* := \{x \in L : \mathrm{T}_{L/K}(xm) \in A, \forall m \in M\},$$

which is an A-lattice in L isomorphic to $M^\vee := \mathrm{Hom}_A(M, A)$. Under **AKLB**, $M^{**} = M$.

In particular, every nonzero fractional ideal I of B is finitely generated as a B-module, and thus as an A-module (B is finite over A). I spans L because B does, so it is an A-lattice in L.

Lemma 13.1

AKLB. If $I \in \mathcal{I}_B$, then $I^* \in \mathcal{I}_B$.

Proof. We previously showed that the dual lattice I^* is a finitely generated A-module. To show that it is a finitely generated B-module, we need to check that it is closed under multiplication by B. Let $b \in B$ and $x \in I^*$. Then for all $m \in I$, we have $\mathrm{T}_{L/K}((bx)m) = T_{L/K}(x(bm)) \in A$ since $bm \in I$. This implies $bx \in I^*$, so I^* is a fractional ideal. □

Definition 13.2 (different)**.** **AKLB**. The *different* $\mathcal{D}_{L/K}$ (or $\mathcal{D}_{B/A}$) of L/K is the inverse of B^* in $\mathcal{I}_B$.

Explicitly, $B^* := \{x \in L : \mathrm{T}_{L/K}(xb) \in A, \forall b \in B\}$, and the inverse is

$$\mathcal{D}_{L/K} = \mathcal{D}_{B/A} := B \div B^* = \{x \in L : xB^* \subseteq B\}.$$

We know $B \subseteq B^*$ by Proposition 6.25, so the different $\mathcal{D}_{B/A} = (B^*)^{-1} \subseteq B^{-1} = B$ is in fact a B-ideal.

Proposition 13.3

AKLB. The different is compatible with localization and completion:

1. $S^{-1}\mathcal{D}_{B/A} = \mathcal{D}_{S^{-1}B/S^{-1}A}$ for any multiplicative subset S of A.
2. For any $\mathfrak{q} \mid \mathfrak{p}$, $\mathcal{D}_{\widehat{B}_\mathfrak{q}/\widehat{A}_\mathfrak{p}} = \mathcal{D}_{B/A}\widehat{B}_\mathfrak{q}$.

Definition 13.4 (discriminant)**.** Let S/R be a ring extension with S a free R-module of rank n. For any $x_1, \ldots, x_n \in S$, define the *discriminant*

$$\mathrm{disc}(x_1, \ldots, x_n) = \mathrm{disc}_{S/R}(x_1, \ldots, x_n) := \det[\mathrm{T}_{S/R}(x_i x_j)]_{i,j} \in R.$$

In the **AKLB** setup, we consider a K-basis $e_1, \ldots, e_n \in B$ for L for which

$$\operatorname{disc}(e_1, \ldots, e_n) = \det[\mathrm{T}_{L/K}(e_i e_j)]_{ij} \in A.$$

Proposition 13.5

Let L/K be finite separable of degree n and Ω/K be an extension with $\sigma_1, \ldots, \sigma_n \in \operatorname{Hom}_K(L, \Omega)$ distinct. For any $e_1, \ldots, e_n \in L$,

$$\operatorname{disc}(e_1, \ldots, e_n) = \det[\sigma_i(e_j)]_{ij}^2.$$

Also for any $x \in L$,

$$\operatorname{disc}(1, x, x^2, \ldots, x^{n-1}) = \prod_{i<j}(\sigma_i(x) - \sigma_j(x))^2.$$

Proof. We have $\mathrm{T}_{L/K}(e_i e_j) = \sum_{k=1}^n \sigma_k(e_i e_j)$ by Theorem 6.4. Then

$$\begin{aligned}\operatorname{disc}(e_1, \ldots, e_n) &= \det[\mathrm{T}_{L/K}(e_i e_j)]_{ij} \\ &= \det([\sigma_k(e_i)]_{ik}[\sigma_k(e_j)]_{kj}) \\ &= \det[\sigma_i(e_j)]_{ij}^2,\end{aligned}$$

because the determinant is multiplicative and does not change under transposes.

The second statement then follows from the Vandermonde determinant:

$$\operatorname{disc}(1, x, x^2, \ldots, x^{n-1}) = \det[\sigma_i(x^{j-1})]_{ij}^2 = \det[\sigma_i(x)^{j-1}]_{ij}^2 = \prod_{i<j}(\sigma_i(x) - \sigma_j(x))^2.$$

□

Definition 13.6 (discriminant)**.** The *discriminant* of $f(x) = \prod_i (x - \alpha_i)$ is

$$\operatorname{disc}(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

Equivalently, if A is a DD, $f \in A[x]$ is monic separable, and α is the image of x in $A[x]/(f(x))$, then

$$\operatorname{disc}(f) = \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \in A.$$

Example 13.7

$\operatorname{disc}(x^2 + bx + c) = b^2 - 4c$ and $\operatorname{disc}(x^3 + ax + b) = -4a^3 - 27b^2$.

AKLB. Let M be an A-lattice in L, so M is a finitely generated A-module which contains a K-basis for L. We want to define the discriminant of M without needing to choose a basis.

First suppose M is a free A-module. Let $e := (e_1, \ldots, e_n)$ and $e' := (e'_1, \ldots, e'_n)$ be two A-bases for M. We claim that

$$\operatorname{disc}(e'_1, \ldots, e'_n) = u^2 \operatorname{disc}(e_1, \ldots, e_n)$$

for a unit $u \in A^\times$. Letting $P \in A^{n\times n}$ be the change of basis matrix so that $e' = eP$, then

$$\begin{aligned}\operatorname{disc}(e') &= \det[\mathrm{T}_{L/K}(e'_i e'_j)]_{ij}\\ &= \det[\mathrm{T}_{L/K}((eP)_i(eP)_j)]_{ij}\\ &= \det[P^T[T_{L/K}(e_ie_j)]_{ij}P]\\ &= \det P^T \operatorname{disc}(e)\det P\\ &= u^2\operatorname{disc}(e).\end{aligned}$$

where $u = \det P$ is a unit because P is invertible.

Definition 13.8 (discriminant). **AKLB**. Let M be an A-lattice in L and $n = [L:K]$. The *discriminant* $D(M)$ is the A-module generated by $\{\operatorname{disc}(x_1,\ldots,x_n) : x_i \in M\}$.

Lemma 13.9

AKLB. If $M' \subseteq M$ are both free A-lattices in L, then the discriminants $D(M') \subseteq D(M)$ are nonzero principal fractional ideals.

If $D(M') = D(M)$, then $M' = M$.

Proof. Let $e = (e_1,\ldots,e_n)$ be an A-basis for M, so $\operatorname{disc}(e) \in D(M)$. For any row vector $x = (x_1,\ldots,x_n)$ with entries in M, there exists a matrix $P \in A^{n\times n}$ such that $x = eP$ and $\operatorname{disc}(x) = (\det P)^2\operatorname{disc}(e)$. Then

$$D(M) = (\operatorname{disc}(e))$$

is a principal fractional A-ideal. It is nonzero because e is a basis and the trace pairing is nondegenerate. Similarly, $D(M') = (\operatorname{disc}(e'))$ if e' is an A-basis for M'. The assumption $M' \subseteq M$ means that $e' = eP$ for some matrix $P \in A^{n\times n}$. Then $\operatorname{disc}(e') = (\det P)^2\operatorname{disc}(e)$ and $D(M') \subseteq D(M)$.

If $D(M') = D(M)$, then $\det P$ must be a unit. In particular, P is invertible and $e = e'P^{-1}$, which implies $M \subseteq M'$ and $M' = M$. □

Proposition 13.10

AKLB. For any A-lattice M in L, $D(M) \in \mathcal{I}_A$.

Proof. The A-module $D(M) \subseteq K$ is nonzero because M contains a K-basis e for L, and $\operatorname{disc}(e) \neq 0$ because the trace pairing is nondegenerate. Let N be the free A-lattice in L generated by the K-basis e. Pick a nonzero $a \in A$ such that $M \subseteq a^{-1}N$; such an a exists because we can write each A-module generator for M in terms of the K-basis e, and let a be the product of all denominators. Then $D(M) \subseteq D(a^{-1}N)$, and $D(a^{-1}N)$ is a principal fractional ideal in $\mathcal{I}_A$, hence a Noetherian A-module (by A Noetherian). Its submodule $D(M)$ is Noetherian, hence finitely generated. □

Definition 13.11 (discriminant). **AKLB**. The *discriminant* $D_{L/K}$ of L/K (or $D_{A/B}$ of B/A) is the discriminant of B as an A-lattice in L:

$$D_{L/K} = D_{B/A} \coloneqq D(B) \in \mathcal{I}_A.$$

The discriminant $D_{L/K}$ is an A-ideal, since $\operatorname{disc}(x_1,\ldots,x_n) = \det[\mathrm{T}_{B/A}(x_ix_j)]_{ij} \in A$ for all $x_1,\ldots,x_n \in B$.

Like the different, the discriminant is compatible with localization and completion.

Example 13.12

Let $A = \mathbb{Z}, K = \mathbb{Q}, L = \mathbb{Q}(i), B = \mathbb{Z}[i]$. Then B is a free A-module with basis $(1, i)$, and we compute $D_{L/K}$ in three ways.

- $\operatorname{disc}(1, i) = \det \begin{bmatrix} \mathrm{T}_{L/K}(1 \cdot 1) & \mathrm{T}_{L/K}(1 \cdot i) \\ \mathrm{T}_{L/K}(i \cdot 1) & \mathrm{T}_{L/K}(i \cdot i) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} = -4.$
- The nontrivial automorphism of L/K sends $i \mapsto -i$, so $\operatorname{disc}(1, i) = \left(\det \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}\right)^2 = (-2i)^2 = -4.$
- $B = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1)$, and $\operatorname{disc}(x^2 + 1) = -4$.

In all cases, $D_{L/K}$ is the ideal $(-4) = (4)$.

Theorem 13.13

AKLB. $D_{B/A} = \mathrm{N}_{B/A}(\mathcal{D}_{B/A})$.

Proof. Because D and N are compatible with localization, it suffices to consider the case where A is a DVR, so B is a free A-lattice in L. Let $(e_1, \ldots, e_n)$ be an A-basis for B. The dual A-lattice

$$B^* = \{x \in L : \mathrm{T}_{L/K}(xb) \in A, \forall b \in B\} \in \mathcal{I}_B$$

is also a free A-lattice in L, with basis $(e_1^*, \ldots, e_n^*)$ uniquely determined by $\mathrm{T}_{L/K}(e_i^* e_j) = \delta_{ij}$. Writing $e_i = \sum a_{ij} e_j^*$, we have

$$\mathrm{T}_{L/K}(e_i e_j) = \mathrm{T}_{L/K}\left(\sum_k a_{ik} e_k^* e_j\right) = \sum_k a_{ik} \, \mathrm{T}_{L/K}(e_k^* e_j) = \sum_k a_{ik} \delta_{kj} = a_{ij}.$$

Thus $P = [\mathrm{T}_{L/K}(e_i e_j)]_{ij}$ is the change of basis matrix from e^* to e, i.e. $e = e^* P$. Let ϕ be the K-linear transformation defined by P, so ϕ is an isomorphism of free A-modules and

$$D_{B/A} = (\det[\mathrm{T}_{L/K}(e_i e_j)]_{ij}) = (\det \phi) = [B^* : B]_A.$$

Then by Corollary 7.8,

$$D_{B/A} = [B^* : B]_A = \mathrm{N}_{B/A}(B \div B^*) = \mathrm{N}_{B/A}((B^*)^{-1}) = \mathrm{N}_{B/A}(\mathcal{D}_{B/A}).$$ □

The module index was defined in Definition 7.1 such that this theorem holds.

13.2 Ramification

AKLB. Let $\mathfrak{p}B = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$, so $B/\mathfrak{p}B \simeq B/\mathfrak{q}_1^{e_1} \times \cdots \times B/\mathfrak{q}_r^{e_r}$. This is an $A/\mathfrak{p}$-algebra of dimension $\sum_i e_i f_i$ where $f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$. It is a product of fields when all $e_i = 1$, and it is an étale $A/\mathfrak{p}$-algebra if also all residue field extensions are separable (always in our setting).

Lemma 13.14

Let k be a field and R be a commutative k-algebra with k-basis $r_1, \ldots, r_n$. Then R is an étale k-algebra if and only if $\operatorname{disc}(r_1, \ldots, r_n) \neq 0$.

Proof (sketch). By Theorem 6.27, R is an étale k-algebra if and only the trace pairing is perfect. Since k is a field, this is equivalent to the trace pairing being nondegenerate. □

Theorem 13.15

AKLB. Suppose $\mathfrak{q}$ is a prime of B lying above the prime $\mathfrak{p}$ of A such that $B/\mathfrak{q}$ a separable extension of $A/\mathfrak{p}$. Then L/K is

- unramified at $\mathfrak{q}$ if and only if $\mathfrak{q} \nmid \mathcal{D}_{B/A}$,
- unramified at $\mathfrak{p}$ if and only if $\mathfrak{p} \nmid D_{B/A}$.

Proof. The different $\mathcal{D}_{B/A}$ is compatible with completion, so WLOG A and B are complete DVRs. Then $[L : K] = e_{\mathfrak{q}} f_{\mathfrak{q}}$ and $\mathfrak{p}B = \mathfrak{q}^{e_{\mathfrak{q}}}$. B is a DVR with maximal ideal $\mathfrak{q}$, so $\mathcal{D}_{B/A} = \mathfrak{q}^m$ for some $m \geq 0$. By Theorem 13.13,

$$D_{B/A} = \mathrm{N}_{B/A}(\mathcal{D}_{B/A}) = N_{B/A}(\mathfrak{q}^m) = \mathfrak{p}^{f_{\mathfrak{q}} m},$$

so $\mathfrak{q} \mid \mathcal{D}_{B/A}$ if and only if $\mathfrak{p} \mid D_{B/A}$. Since A is a PID, B is a free A-module, and we can choose an A-basis $e_1, \ldots, e_n$ for B, which is also a K-basis for L. Let $k = A/\mathfrak{p}$, and let $\overline{e}_1, \ldots, \overline{e}_n$ be the reductions mod $\mathfrak{p}$ to the k-algebra $B/\mathfrak{p}B$. Then $(\overline{e}_1, \ldots, \overline{e}_n)$ is a k-basis for $B/\mathfrak{p}B$: it spans, and

$$[B/\mathfrak{p}B : k] = [B/\mathfrak{q}^{e_{\mathfrak{q}}} : A/\mathfrak{p}] = e_{\mathfrak{q}} f_{\mathfrak{q}} = [L : K] = n.$$

Since B has an A-module basis, its discriminant is

$$D_{B/A} = (\mathrm{disc}(e_1, \ldots, e_n)).$$

Then $\mathfrak{p} \mid D_{B/A}$ if and only if $\mathrm{disc}(e_1, \ldots, e_n) \in \mathfrak{p}$, or $\mathrm{disc}(\overline{e}_1, \ldots, \overline{e}_n) = 0$. By Lemma 13.14, $\mathrm{disc}(\overline{e}_1, \ldots, \overline{e}_n) = 0$ if and only if $B/\mathfrak{p}B$ is not an étale k-algebra, which is if and only if $\mathfrak{p}$ is ramified. There is only one prime $\mathfrak{q}$ above $\mathfrak{p}$, so this is if and only if $\mathfrak{q}$ is ramified. □

Corollary 13.16

AKLB. Only finitely many primes are ramified.

14 Global fields and the product formula

14.1 Places of a field

Definition 14.1 (place). A *place* ν of a field K is an equivalence class of nontrivial absolute values. Places are in one-to-one correspondence with completions.

Let M_K denote the set of places of K. Let K_ν denote the completion of K at a place represented by $|\cdot|_\nu$. A place ν is *(non-)archimedean* if and only if K_ν is.

For a global field K, the completion K_ν is a local field by Corollary 10.7. From the classification of local fields in Theorem 10.9, we have $K_\nu \simeq \mathbb{R}$ or $\mathbb{C}$ (if K_ν is archimedean), or the absolute value of K_ν is induced by a discrete valuation.

- If $K_\nu \simeq \mathbb{R}$, then ν is a *real place*.
- If $K_\nu \simeq \mathbb{C}$, then ν is a *complex place*.
- If $|\cdot|_\nu$ is induced by a discrete valuation $\nu_{\mathfrak{p}}$ corresponding to a prime ideal $\mathfrak{p}$ of the valuation ring of K, then ν is a *finite place*. Otherwise, ν is an *infinite place*.

Example 14.2

Every finite place is non-archimedean. Infinite places are archimedean if $\operatorname{char} K = 0$, and non-archimedean if $\operatorname{char} K > 0$. Every archimdean place is an infinite place, but non-archimedean places may be finite or infinite (if $\operatorname{char} K > 0$).

In our case (finite extension of a global field), there are finitely many infinite places.

Example 14.3

$M_{\mathbb{Q}}$ consists of finite places p corresponding to p-adic absolute values $|\cdot|_p$, and one archimedean infinite place ∞ corresponding to the Euclidean absolute value $|\cdot|_\infty$.

$M_{\mathbb{F}_q(t)}$ consists of finite places corresponding to irreducible polynomials in $\mathbb{F}_q[t]$, and one archimedean infinite place ∞ corresponding to $|\cdot|_\infty = q^{\deg(\cdot)}$.

Definition 14.4 (extends)**.** If L/K is an extension of global fields, a place $|\cdot|_w$ of L restricts to a place $|\cdot|_\nu$ of K. We write $w \mid \nu$ and say that w *extends* ν, or w *lies above* ν.

Theorem 14.5

Let L/K be a finite separable extension of global fields and ν be a place of K. There is an isomorphism of finite étale K_ν-algebras

$$L \otimes_K K_\nu \xrightarrow{\sim} \prod_{w \mid \nu} L_w$$

defined by $\ell \otimes x \mapsto (\ell x, \ldots, \ell x)$.

We already proved this for finite places ν in Theorem 12.20.

Corollary 14.6

Same hypotheses as above. Suppose $f \in K[x]$ is monic irreducible such that $L \simeq K[x]/(f)$. Then there is a bijection

$$\{\text{irreducible factors of } f \text{ in } K_\nu[x]\} \longleftrightarrow \{\text{places } w \mid \nu \text{ of } L\}.$$

If $f = f_1 \cdots f_r \in K_\nu[x]$ (note f_i distinct because f separable), we can order $\{w \mid \nu\} = \{w_1, \ldots, w_r\}$ such that $L_{w_i} \simeq K_\nu[x]/(f_i)$ for $1 \leq i \leq r$.

Suppose L/K is a finite separable extension of global fields, and ν is a place of K. Consider the algebraic closure $\overline{K}_\nu$ of K_ν, and consider $\operatorname{Hom}_K(L, \overline{K}_\nu)$. There is a group action with $\sigma \in \operatorname{Gal}(\overline{K}_\nu/K_\nu)$ acting on $\tau \in \operatorname{Hom}_K(L, \overline{K}_\nu)$ by $\sigma \circ \tau \in \operatorname{Hom}_K(L, \overline{K}_\nu)$.

Corollary 14.7

There is a bijection

$$\operatorname{Hom}_K(L, \overline{K}_\nu)/\operatorname{Gal}(\overline{K}_\nu/K_\nu) \longleftrightarrow \{w \mid \nu\}.$$

For $K = \mathbb{Q}$ and $\nu = \infty$, we get a bijection between $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})/\operatorname{Gal}(\mathbb{C}/\mathbb{R})$ and the infinite places of L. $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) \simeq C_2$ generated by complex conjugation, so the orbits of $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ have size 1 or 2. Orbits of size 1 correspond to real places, and orbits of size 2 correspond to complex places.

Definition 14.8 (real, complex embedding). Let L be a number field. Elements of $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{R})$ are *real embeddings*. Elements of $\operatorname{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ that are not real embeddings are *complex embeddings*.

Corollary 14.9

Let L be a number field with r real places and s complex places. Then $[L : \mathbb{Q}] = r + 2s$.

Example 14.10

Let $K = \mathbb{Q}[x]/(x^3 - 2)$. There are three embeddings $K \hookrightarrow \mathbb{C}$, namely $x \mapsto \sqrt[3]{2}$, $x \mapsto e^{2\pi i/3}\sqrt[3]{2}$, and $x \mapsto e^{4\pi i/3}\sqrt[3]{2}$. The first embedding is real, while the last two are complex embeddings in the same complex place.

Proposition 14.11

Let K be a number field with s complex places. The absolute discriminant $D_K \in \mathbb{Z}$ has sign $(-1)^s$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and let $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$. Then $D_k = (\det A)^2$ where $A := [\sigma_i(\alpha_j)]_{ij}$ and $\det A = x + iy \in \mathbb{C}$. Each real embedding σ_i corresponds to a row of A fixed by complex conjugation, while each pair of complex conjugate embeddings corresponds to two rows of A interchanged by complex conjugation. Thus $\det A = (-1)^s \det \overline{A} = (-1)^s(x - iy)$. If $(-1)^s = 1$ then $y = 0$ and $D_K = x^2$ has sign 1. If $(-1)^s = -1$ then $x = 0$ and $D_K = -y^2$ has sign -1. □

14.2 Haar measures

Definition 14.12 (σ-algebra). Let X be a locally compact Hausdorff space. The *σ-algebra* Σ of X is the collection of subsets of X generated by all of the open and closed sets under countable unions, intersections, and complements. Elements of Σ are *measurable (Borel) sets*.

Definition 14.13 (Borel measure). A *Borel measure* on X is a countably additive function

$$\mu \colon \Sigma \to \mathbb{R}_{\geq 0} \cup \{\infty\}.$$

Definition 14.14 (Radon measure). A *Radon measure* is a Borel measure for which

1. $\mu(S) < \infty$ if S is compact.
2. $\mu(S) = \inf\{\mu(U) : S \subseteq U,\ U \text{ open}\}$.
3. $\mu(S) = \sup\{\mu(C) : C \subseteq S,\ C \text{ compact}\}$.

Definition 14.15 (locally compact). A *locally compact* group G is a topological group that is Hausdorff and locally compact (each point has a compact neighborhood).

Definition 14.16 (Haar measure). A *(left) Haar measure* μ on a locally compact group G is a nonzero Radon measure that is translation invariant: $\mu(S) = \mu(x + S)$ for all $x \in G$ and $S \subseteq G$ measurable.

Compact groups are locally compact. In a compact group G, every measurable set has finite measure, so we can say WLOG $\mu(G) = 1$.

Theorem 14.17 (Weil)

Every locally compact group G has a Haar measure, and if μ and μ' are two Haar measures on G, then $\mu' = \lambda\mu$ for some $\lambda \in \mathbb{R}_{>0}$.

Proposition 14.18

Let K be a local field with discrete valuation ν, residue field k, and absolute value $|x|_\nu := (\#k)^{-\nu(x)}$. Let μ be a Haar measure on K (as an additive topological group). For all $x \in K$ and measurable $S \subseteq K$,

$$\mu(xS) = |x|_\nu \, \mu(S).$$

Moreover, $|\cdot|_\nu$ is the unique absolute value compatible with the topology of K for which this holds.

We know that μ is invariant under addition, but this proposition states how it changes under multiplication. The number $|x|_\nu$ is uniquely determined, because changing scaling the Haar measure μ multiplies both sides by the same constant.

Proof. Let A be the valuation ring $\{x \in K : |x|_\nu \leq 1\}$ with maximal ideal $\mathfrak{p}$. The proposition is true for $x = 0$, so let $x \neq 0$. The map $\phi_x \colon y \mapsto xy$ is an automorphism of K, so $\mu_x := \mu \circ \phi_x$ is another Haar measure. By Weil's theorem (Theorem 14.17), $\mu_x = \lambda_x \mu$ for some $\lambda_x \in \mathbb{R}_{>0}$. Define $\chi \colon K^\times \to \mathbb{R}_{>0}$ by $x \mapsto \lambda_x = \mu_x(A)/\mu(A)$. Then $\mu_x = \chi(x)\mu$, and for all $x, y \in K^\times$,

$$\chi(xy) = \frac{\mu_{xy}(A)}{\mu(A)} = \frac{\mu_x(yA)}{\mu(A)} = \frac{\chi(x)\mu_y(A)}{\mu(A)} = \frac{\chi(x)\chi(y)\mu(A)}{\mu(A)} = \chi(x)\chi(y),$$

so χ is multiplicative.

We in fact claim that $\chi(x) = |x|_\nu$ for all $x \in K^\times$. Since χ is multiplicative, it suffices to consider $x \in A \setminus \{0\}$. The ideal xA equals $\mathfrak{p}^{\nu(x)}$ since A is a DVR. The residue field $k = A/\mathfrak{p}$ is finite, so A/xA is also finite, and in fact a k-vector space of dimension $\nu(x)$ and cardinality $[A : xA] = (\#k)^{\nu(x)}$. Then

$$\mu(A) = [A : xA]\mu(xA) = (\#k)^{\nu(x)}\chi(x)\mu(A),$$

so $\chi(x) = (\#k)^{-\nu(x)} = |x|_\nu$. Then $\mu(xS) = \mu_x(S) = \chi(x)\mu(S) = |x|_\nu \, \mu(S)$ for all $x \in K$ and S measurable.

For uniqueness, if $|\cdot|$ is another equivalent absolute value on K with $|\cdot| = |\cdot|_\nu^c$ for some $0 < c \leq 1$, then

$$\frac{\mu(xA)}{\mu(A)} = |x| = |x|_\nu^c = \left(\frac{\mu(xA)}{\mu(A)}\right)^c$$

implies $c = 1$. □

14.3 Product formula for global fields

Definition 14.19 (normalized absolute value)**.** Let K be a global field. The *normalized absolute value* $||\cdot||_\nu \colon K_\nu \to \mathbb{R}_{\geq 0}$ is given by

$$||x||_\nu = \frac{\mu(xS)}{\mu(S)}$$

where μ is any Haar measure on K_ν and $S \subseteq K_\nu$ is any measurable set with $0 < \mu(S) < \infty$.

Note this definition is independent of μ and S by the above proposition.

- If ν is a non-archimedean place, then $||\cdot||_\nu = (\#k)^{-\nu(\cdot)}$.
- If ν is a real place, then $||\cdot||_\nu$ is the Euclidean absolute value $|\cdot|_\mathbb{R}$.
- If ν is a complex place, then $||\cdot||_\nu = |\cdot|_\mathbb{C}^2$.

Example 14.20

When ν is a complex place, $||\cdot||_\nu$ is **not** an absolute value. For example in $\mathbb{Q}(i)$, suppose $\nu \mid \infty$ is a complex place. Then $||1||_\nu = |1|_{\mathbb{C}}^2 = 1$, but $||1+1||_\nu = |2|_{\mathbb{C}}^2 = 4 > 2$, so the triangle inequality doesn't hold.

Lemma 14.21

Let L/K be a finite separable extension of global fields, ν a place of K, and $w \mid \nu$ a place of L. Then

$$||x||_w = \left|\left|\mathrm{N}_{L_w/K_\nu}(x)\right|\right|_\nu .$$

Theorem 14.22 (Product formula)

Let L be a global field. For all $x \in L^\times$,

$$\prod_{\nu \in M_L} ||x||_\nu = 1.$$

Proof. Let $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$, $\nu \mid \mathfrak{p}$. Let p be a place of K. Any basis for L as a K-vector space is also a basis for $L \otimes_K K_p \simeq \prod_{\nu|p} L_\nu$ as a K_p-vector space, so

$$\mathrm{N}_{L/K}(x) = \mathrm{N}_{(L\otimes_K K_p)/K_p}(x) = \prod_{\nu|p} \mathrm{N}_{L_\nu/K_p}(x).$$

Then

$$\left|\left|\mathrm{N}_{L/K}(x)\right|\right|_p = \prod_{\nu|p} \left|\left|\mathrm{N}_{L_\nu/K_p}(x)\right|\right|_p = \prod_{\nu|\mathfrak{p}} |x|_p .$$

Taking the product over all $p \in M_K$ and using the product formula for K (pset 1), we have

$$1 = \prod_{p\in M_K} \left|\left|\mathrm{N}_{L/K}(x)\right|\right|_p = \prod_{p\in M_K}\prod_{\nu|p} ||x||_\nu = \prod_{\nu\in M_L} ||x||_\nu .$$ □

Definition 14.23 (global field). A *global field* is a field K (with at least one place) whose completion at each $\nu \in M_K$ is a local field, and

$$\prod_{\nu\in M_K} ||x||_\nu = 1$$

where each $||\cdot||_\nu$ satisfies $||\cdot||_\nu = |\cdot|_\nu^{m_\nu}$ for some $m_\nu \in \mathbb{R}_{>0}$.

15 Geometry of numbers

15.1 Lattices in real vector spaces

Recall that if V is an $\mathbb{R}$-vector space with $\dim V = n$, then $V \simeq \mathbb{R}^n$ is a locally compact group.

Definition 15.1 (discrete, cocompact). A subgroup H of a topological group G is *discrete* if it has the discrete topology (every point is open). H is *cocompact* if it is normal in G, and G/H is compact.

Lemma 15.2

A subgroup $G \leq V \simeq \mathbb{R}^n$ is discrete if and only if it is generated by a finite $\mathbb{R}$-linearly independent set, in which case $G \simeq \mathbb{Z}^m$ for some $m \leq n$. G is cocompact if and only if $m = n$.

Definition 15.3 (lattice)**.** A *(full) lattice* Λ in $V \simeq \mathbb{R}^n$ is a $\mathbb{Z}$-submodule generated by an $\mathbb{R}$-basis, or equivalently, a discrete cocompact subgroup.

We have $\Lambda \simeq \mathbb{Z}^n$ and $V \simeq \mathbb{R}^n$, so $V/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^n$ is an n-torus.

Any basis $v_1, \ldots, v_n$ for V determines a *fundamental parallelepiped*

$$F(v_1, \ldots, v_n) \coloneqq \{t_1 v_1 + \cdots + t_n v_n : t_i \in [0,1)\}.$$

Normalize the Haar measure on V such that $\mu(F(v_1, \ldots, v_n)) = 1$, so $\mu(S) = \mu_{\mathbb{R}^n}(\varphi(S))$ for $\varphi\colon V \xrightarrow{\sim} \mathbb{R}^n$ the isomorphism sending $F(v_1, \ldots, v_n) \mapsto [0,1]^n$. For any other basis $e_1, \ldots, e_n$ of V, letting $E = [e_{ij}]_{ij}$ where $e_j = \sum_i e_{ij} v_i$, then

$$\mu(F(e_1, \ldots, e_n)) = |\det E| = \sqrt{\det E^T \det E} = \sqrt{\det[\langle e_i, e_j\rangle]_{ij}}.$$

Proposition 15.4

Let $T\colon V \to V$ be a linear transformation, μ be any Haar measure, and S be any measurable set. Then

$$\mu(T(S)) = |\det T|\, \mu(S).$$

If $\Lambda = e_1\mathbb{Z} \oplus \cdots \oplus e_n\mathbb{Z}$ is a lattice, then V/Λ is a compact group that can be identified with the parallelepiped $F(e_1, \ldots, e_n) \subseteq V$, which is a *fundamental domain* for Λ.

Definition 15.5 (fundamental domain)**.** Let Λ be a lattice in $V \simeq \mathbb{R}^n$. A *fundamental domain* for Λ is a measurable set $F \subseteq V$ such that $V = \bigsqcup_{\lambda \in \Lambda} (F + \lambda)$.

In other words, F is a measurable set of coset representatives for V/Λ.

Proposition 15.6

Every fundamental domain for Λ has the same Haar measure.

Proof. Let F, G be two fundamental domains for Λ. Using the translation invariance and countable additivity of μ, we have

$$\begin{aligned}
\mu(F) &= \mu\Big(F \cap \bigsqcup_{\lambda \in \Lambda} (G + \lambda)\Big) \\
&= \mu\Big(\bigsqcup_{\lambda \in \Lambda} (F \cap (G + \lambda))\Big) \\
&= \sum_{\lambda \in \Lambda} \mu(F \cap (G + \lambda)) \\
&= \sum_{\lambda \in \Lambda} \mu((F - \lambda) \cap G) \\
&= \sum_{\lambda \in \Lambda} \mu(G \cap (F + \lambda)) \\
&= \mu(G).
\end{aligned}$$

The second-to-last equality is because Λ is closed under negation. □

Definition 15.7 (covolume)**.** Let Λ be a lattice in $V \simeq \mathbb{R}^n$ and μ be a Haar measure. The *covolume* of Λ is $\operatorname{covol}(\Lambda) := \mu(F) \in \mathbb{R}_{>0}$ for any fundamental domain F.

Proposition 15.8

If $\Lambda' \subseteq \Lambda$ are lattices in $V \simeq \mathbb{R}^n$, then the $\operatorname{covol}(\Lambda') = [\Lambda : \Lambda'] \operatorname{covol}(\Lambda)$.

Definition 15.9 (symmetric, convex)**.** A subset S of $V \simeq \mathbb{R}^n$ is *symmetric* if it is closed under negation, and *convex* if $\{tx + (1-t)y : t \in [0,1]\} \subseteq S$ for all $x, y \in S$.

Theorem 15.10 (Minkowski's lattice point theorem)

Let Λ be a lattice in $V \simeq \mathbb{R}^n$ and μ be a Haar measure on V. If $S \subseteq V$ is a symmetric, convex, measurable subset of V, and

$$\mu(S) > 2^n \operatorname{covol}(\Lambda),$$

then S contains a nonzero element $\lambda \in \Lambda$.

15.2 Canonical inner product

In the AKLB setup, we now take $A = \mathbb{Z}$, $K = \mathbb{Q}$, and $L = K$ a number field. Suppose $K/\mathbb{Q}$ is a number field of degree n with r real places and s complex places, so $n = r + 2s$. We consider the two base changes

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s$$
$$K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C}^n.$$

We have a sequence of injective homomorphisms of topological rings

$$\mathcal{O}_K \hookrightarrow K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$$

where

- $\mathcal{O}_K \hookrightarrow K$ is the inclusion.
- $K \hookrightarrow K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ is the canonical embedding $\alpha \mapsto \alpha \otimes 1$.
- $K_{\mathbb{R}} \simeq \mathbb{R}^r \times \mathbb{C}^s \hookrightarrow \mathbb{C}^r \times \mathbb{C}^{2s} \simeq K_{\mathbb{C}}$ is $\mathbb{R} \hookrightarrow \mathbb{C}$ by $x \mapsto x$, and $\mathbb{C} \hookrightarrow \mathbb{C} \times \mathbb{C}$ by $z \mapsto (z, \bar{z})$.

The composition $K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}$ is $x \mapsto (\sigma_1(x), \ldots, \sigma_n(x))$ where $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$.

Fixing a $\mathbb{Z}$-basis for $\mathcal{O}_K$, we may view the above injections are inclusions of topological groups (but not topological rings)

$$\mathbb{Z}^n \hookrightarrow \mathbb{Q}^n \hookrightarrow \mathbb{R}^n \hookrightarrow \mathbb{C}^n.$$

In particular, $\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}} \simeq \mathbb{R}^n$, which inherits a canonical inner product on $K_{\mathbb{C}} \simeq \mathbb{C}^n$ via

$$\langle z, z' \rangle := \sum_{i=1}^{n} z_i \bar{z}'_i \in \mathbb{C}.$$

Then for all $x, y \in K$,

$$\langle x, y \rangle := \sum_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \sigma(x)\overline{\sigma(y)}.$$

Now write $z \in K_{\mathbb{C}} \simeq \mathbb{C}^n$ as vectors (z_σ) induced by $\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. For real embeddings $\sigma = \overline{\sigma}$, we have $z_\sigma \in \mathbb{R}$ while for complex embeddings $\sigma \neq \overline{\sigma}$, we have $(z_\sigma, z_{\overline{\sigma}}) = (z_\sigma, \overline{z_\sigma}) \in \mathbb{C} \times \mathbb{C}$. Each $z \in K_{\mathbb{R}}$ can be uniquely written as

$$(w_1, \ldots, w_r, x_1 + iy_1, x_1 - iy_1, \ldots, x_s + iy_s, x_s - iy_s).$$

for $w_i, x_j, y_j \in \mathbb{R}$. The canonical inner product on $K_{\mathbb{R}}$ can then be written as

$$\langle z, z' \rangle = \sum_{i=1}^{r} w_i w_i' + 2\sum_{j=1}^{s}(x_j x_j' + y_j y_j')$$

Taking $w_1, \ldots, w_r, x_1, y_1, \ldots, x_s, y_s$ as coordinates for $K_{\mathbb{R}} \simeq \mathbb{R}^n$, we normalize a Haar measure μ on $K_{\mathbb{R}}$ to be consistent with the Lebesgue measure $\mu_{\mathbb{R}^n}$ on $\mathbb{R}^n$ by defining

$$\mu(S) \coloneqq 2^s \mu_{\mathbb{R}^n}(S)$$

for any measurable $S \subseteq K_{\mathbb{R}} \simeq \mathbb{R}^n$.

For any $\mathbb{R}$-basis $e_1, \ldots, e_n$ of $K_{\mathbb{R}}$, we still have $\mu(F(e_1, \ldots, e_n)) = \sqrt{|\det[\langle e_i, e_j \rangle]_{ij}|}$ using the Hermitian inner product on $K_{\mathbb{R}} \subseteq K_{\mathbb{C}} \simeq \mathbb{C}^n$ (instead of the dot product on $K_{\mathbb{R}} \simeq \mathbb{R}^n$ as before).

15.3 Covolumes of fractional ideals

We now have fixed a normalized Haar measure μ on $K_{\mathbb{R}}$. Recall that the discriminant of a number field K is

$$D_K = \operatorname{disc} \mathcal{O}_K \coloneqq \operatorname{disc}(e_1, \ldots, e_n) \in \mathbb{Z}$$

for any $\mathbb{Z}$-basis $e_1, \ldots, e_n$ of $\mathcal{O}_K$.

Proposition 15.11

Let K be a number field and μ be the normalized Haar measure on $K_{\mathbb{R}}$. Then

$$\operatorname{covol}(\mathcal{O}_K) = \sqrt{|D_K|}.$$

Proof. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, and let $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \{\sigma_1, \ldots, \sigma_n\}$. Let $A = [\sigma_i(e_j)]_{ij} \in \mathbb{C}^{n \times n}$, so $D_K = \operatorname{disc}(e_1, \ldots, e_n) = (\det A)^2$. We have

$$\operatorname{covol}(\mathcal{O}_K) = \mu(F(e_1, \ldots, e_n)) = \sqrt{|\det[\langle e_i, e_j \rangle]_{ij}|},$$

where $\det[\langle e_i, e_j \rangle]_{ij} = \det[\sum_k \sigma_k(e_i)\overline{\sigma_k(e_j)}]_{ij} = \det(A^T \overline{A}) = (\det A)(\det \overline{A})$. $(\det A)^2 \in \mathbb{Z}$, so $\operatorname{covol}(\mathcal{O}_K)^2 = \left|(\det A)^2\right| = |D_k|$. □

Recall the absolute norm map on ideals $\mathrm{N}\colon \mathcal{I}_{\mathcal{O}_K} \to \mathcal{I}_{\mathbb{Z}}$ sending $I \mapsto [\mathcal{O}_K : I]_{\mathbb{Z}}$ with image in $\mathbb{Q}_{>0}$. When $I = (a)$ for $a \in K$, we write $\mathrm{N}(a) \coloneqq \mathrm{N}((a)) = \left|\mathrm{N}_{K/\mathbb{Q}}(a)\right|$.

Corollary 15.12

For all $I \in \mathcal{I}_{\mathcal{O}_K}$, $\operatorname{covol}(I) = \mathrm{N}(I)\sqrt{|D_K|}$.

15.4 Minkowski bound

Theorem 15.13 (Minkowski bound)

Let K be a number field of degree n with r real places and s complex places ($r + 2s = n$). Define the *Minkowski constant*

$$m_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|D_K|}.$$

Then for all nonzero $I \in \mathcal{I}_{\mathcal{O}_K}$, there exists a nonzero $a \in I$ for which

$$\mathrm{N}(a) \le m_K\,\mathrm{N}(I).$$

Lemma 15.14

For $t \in \mathbb{R}_{>0}$, the measure of $S_t := \{(z_\sigma) \in K_\mathbb{R} : \sum_\sigma |z_\sigma| \le t\} \subseteq K_\mathbb{R}$ is $\mu(S_t) = 2^r\pi^s\frac{t^n}{n!}$.

Proof. Write $(z_\sigma) = (w_1, \ldots, w_r, x_1 + iy_1, x_1 - iy_1, \ldots, x_s + iy_s, x_s - iy_s)$ for $w_i, x_j, y_j \in \mathbb{R}$. Then $\sum_\sigma |z_\sigma| \le t$ if and only if

$$\sum_{i=1}^{r} |w_i| + 2\sum_{j=1}^{s} \sqrt{|x_j|^2 + |y_j|^2} \le t. \tag{15.1}$$

The volume of

$$U_t := \{(u_1, \ldots, u_n) \in \mathbb{R}^n_{\ge 0} : u_1 + \cdots + u_n \le t\}$$

is $\mu_{\mathbb{R}^n}(U_t) = \frac{t^n}{n!}$. Fixing all coordinates of (z_σ) except for (x_s, y_s), then (x_s, y_s) ranges over a disk of some radius $d \in [0, \frac{t}{2}]$ determined by (15.1). If we replace (x_s, y_s) with (u_{n-1}, u_n) in the triangular region bounded by $u_{n-1} + u_n \le 2d$ and $u_{n-1}, u_n \ge 0$, we need to incorporate a factor of $\frac{\pi}{2}$ to account for the areas $\frac{(2d)^2}{2} = 2d^2$ vs. πd^2. Repeat this s times for all (x_j, y_j). Similarly if w_r is replaced by u_r, then $w_r \in [-d, d]$ for some $t \in [0, t]$, but $u_r \in [0, d]$ is nonnegative, so we need a factor of 2. Repeat this r times for all w_i. The upshot is that

$$\mu(S_t) = 2^s\mu_{\mathbb{R}^n}(S_t) = 2^s\left(\frac{\pi}{2}\right)^s 2^r\mu_{\mathbb{R}^n}(U_t) = 2^r\pi^s\frac{t^n}{n!}.$$ □

Proof of Theorem 15.13. For $I \in \mathcal{I}_{\mathcal{O}_K}$, choose t such that $\mu(S_t) > 2^n \operatorname{covol}(I)$ so that S_t contains a nonzero $a \in I$ by Minkowski's lattice point theorem (Theorem 15.10). By the above lemma, it suffices for t to satisfy

$$\left(\frac{t}{n}\right)^n = \frac{n!\,\mu(S_t)}{n^n 2^r \pi^s} > \frac{n!\,2^n}{n^n 2^r \pi^s}\operatorname{covol}(I) = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^r \sqrt{|D_K|}\,\mathrm{N}(I) = m_K\,\mathrm{N}(I).$$

Pick t such that $(\frac{t}{n})^n > m_K\,\mathrm{N}(I)$, then S_t contains a nonzero $a \in I$ with $\sum_\sigma |\sigma(a)| \le t$. By AM-GM,

$$\mathrm{N}(a) = \left(\prod_\sigma |\sigma(a)|^{1/n}\right)^n \le \left(\frac{1}{n}\sum_\sigma |\sigma(a)|\right)^n \le \left(\frac{t}{n}\right)^n.$$

Take the limit as $(\frac{t}{n})^n \to m_K\,\mathrm{N}(I)$ from above yields $\mathrm{N}(a) \le m_K N(I)$. □

15.5 Finiteness of the class group

Theorem 15.15

Let K be a number field. Then every ideal class in $\operatorname{cl}\mathcal{O}_K$ contains some ideal $I \subseteq \mathcal{O}_K$ with absolute norm $\mathrm{N}(I) \le m_K$.

Proof. Let $[J] \in \operatorname{cl}\mathcal{O}_K$. By the Minkowski bound (Theorem 15.13), there exists a nonzero $a \in J^{-1}$ such that $\mathrm{N}(a) \le m_K \mathrm{N}(J^{-1}) = m_K \mathrm{N}(J)^{-1}$, so $\mathrm{N}(aJ) = \mathrm{N}(a)\mathrm{N}(J) \le m_K$. Since $a \in J^{-1}$, $aJ \subseteq J^{-1}J = \mathcal{O}_K$ and $I = aJ$ is an $\mathcal{O}_K$-ideal in $[J]$ with $\mathrm{N}(I) \le m_K$. □

Lemma 15.16

Let K be a number field of degree n. The number of $\mathcal{O}_K$-ideals of norm $\mathrm{N}(I) \le M$ for any $M \in \mathbb{R}_{>0}$ is at most $(nM)^{\log_2 M}$ (in particular, it is finite).

Proof. Suppose $\mathrm{N}(I) \le M$, and factor $I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ into (not necessarily distinct) prime ideals. Since $\mathrm{N}(\mathfrak{p}_i) \ge 2$, $k = \log_2 M$. There are at most M primes $p \le M$, and at most n primes $\mathfrak{p}$ of O_K with $\mathfrak{p} \mid p$, so there are at most $(nM)^{\log_2 M}$ $\mathcal{O}_K$-ideals I with $\mathrm{N}(I) \le M$. □

Corollary 15.17

The class group $\operatorname{cl}\mathcal{O}_K$ is finite.

Proof. Combine the bound $\mathrm{N}(I) \le m_K$ from Theorem 15.15 with Lemma 15.16. □

This is also true for global function fields (see pset 8).

Corollary 15.18

Let K be a number field of degree n with s complex places. Then

$$|D_K| \ge \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^{2s} > \frac{1}{e^2 n}\left(\frac{\pi e^2}{4}\right)^n.$$

Corollary 15.19

If $K \ne \mathbb{Q}$ is a number field, then $|D_K| > 1$; i.e. there are no nontrivial unramified extensions of $\mathbb{Q}$.

Theorem 15.20

For every real number $M > 0$, the set of number fields with discriminant $|D_K| < M$ is finite.

Theorem 15.21 (Hermite)

Let S be a finite set of places of $\mathbb{Q}$. The number of extensions $K/\mathbb{Q}$ of a fixed degree n that are unramified outside S is finite.

16 Dirichlet's unit theorem

Let K be a number field. Last time we proved that $\operatorname{cl}\mathcal{O}_K$ is finite. Today we will prove that $\mathcal{O}_K^\times$ is finitely generated.

16.1 Arakelov divisors

Let M_K denote the set of places of K. Given a place $\nu \in M_K$, let K_ν be the completion with respect to $||\cdot||_\nu : K \to \mathbb{R}_{\geq 0}$ where $||x||_\nu := \frac{\mu(xS)}{\mu(S)}$ for a Haar measure μ and a measurable set S. Recall that

$$||x||_\nu = \begin{cases} |x|_\nu = (\#k)^{-\nu(x)} & \text{if } \nu \text{ archimedean} \\ |x|_\mathbb{R} & \text{if } \nu \text{ real} \\ |x|_\mathbb{C}^2 & \text{if } \nu \text{ complex} \end{cases}.$$

Definition 16.1 (Arakelov divisor)**.** An *Arakelov divisor* is a sequence of positive real numbers (c_ν) indexed by $\nu \in M_K$ with $c_\nu = 1$ for all but finitely many ν.

Arakelov divisors form an abelian group called $\operatorname{Div} K$ under pointwise multiplication: $(c_\nu)(d_\nu) = (c_\nu d_\nu)$. The multiplicative group $K^\times$ is embedded in $\operatorname{Div} K$ via $x \mapsto (||x||_\nu)$, which is a subgroup $\operatorname{Prin} K$ of *principal Arakelov divisors.*

Definition 16.2 (size)**.** The *size* of $c \in \operatorname{Div} K$ is $||c|| := \prod_{\nu \in M_K} c_\nu \in \mathbb{R}_{>0}$.

The map $\operatorname{Div} K \to \mathbb{R}_{>0}$ given by $c \mapsto ||c||$ is a group homomorphism with $\operatorname{Prin} K$ in the kernel by the product formula (Theorem 14.22).

Corresponding to each $c \in \operatorname{Div} K$ is a subset $L(c)$ of K defined by

$$L(c) := \{x \in K : ||x||_\nu \leq c_\nu, \forall \nu \in M_K\}.$$

and a fractional ideal $I_c \in \mathcal{I}_{\mathcal{O}_K}$ defined by

$$I_c := \prod_{\nu | \infty} \mathfrak{q}_\nu^{\nu(c)}$$

where $\mathfrak{q}_\nu := \{a \in \mathcal{O}_K : \nu(a) > 0\}$ and $\nu(c) := -\log_{\#k_\nu}(c_\nu) \in \mathbb{Z}$. There is another group homomorphism $\operatorname{Div} K \to \mathcal{I}_{\mathcal{O}_K}$ given by $c \mapsto I_c$. Note that $L(c) \subseteq I_c$.

Remark 16.3. The Arakelov class group is $\operatorname{Pic}^0 K = \operatorname{Div}^0 K / \operatorname{Prin} K$, where $\operatorname{Div}^0 K = \{c : ||c|| = 1\}$.

$$\begin{tikzcd}
\operatorname{Div} K \arrow[r] \arrow[d] & \mathcal{I}_{\mathcal{O}_K} \arrow[d] \\
\operatorname{Pic} K \arrow[r] & \operatorname{cl} \mathcal{O}_K
\end{tikzcd}$$

We have

$$\mathrm{N}(I_c) = \prod_{\nu \nmid \infty} \mathrm{N}(\mathfrak{q}_\nu)^{\nu(c)} = \prod_{\nu \nmid \infty} (\#k_\nu)^{\nu(c)} = \prod_{\nu \nmid \infty} c_\nu^{-1}$$

so

$$||c|| = \mathrm{N}(I_c)^{-1} \prod_{\nu | \infty} c_\nu.$$

We also define

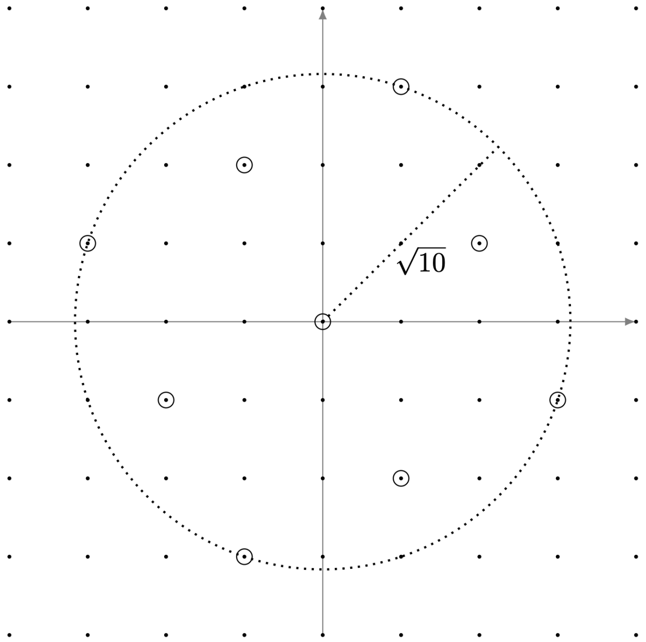
$$R_c := \{c \in K_\mathbb{R} : ||x||_\nu \leq c_\nu, \forall \nu \mid \infty\}.$$

This set is compact, convex, and symmetric in $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R} \simeq \mathbb{R}^r \times \mathbb{C}^s$, where r, s are the number of real and complex places. There is a natural inclusion $K \hookrightarrow K_\mathbb{R}$ by $x \mapsto x \otimes 1$. Viewing I_c and $L(c)$ as subsets of $K_\mathbb{R}$, we have

$$L(c) = I_c \cap R_c.$$

Example 16.4

Let $K = \mathbb{Q}(i)$ and $I_c = (2+i)$ which corresponds to a place ν_1. Let $\nu_2 \mid \infty$ be the unique complex conjugate. Let $c_{\nu_1} = \frac{1}{5}$, $c_{\nu_2} = 10$, and $c_\nu = 1$ for all $\nu \neq \nu_1, \nu_2$. Then $L(c) = \{x \in (2+i) : ||x||_{\nu_2} \leq 10\}$, where $||x||_{\nu_2} \leq 10$ is a circle of radius $\sqrt{10}$. In this case, $\#L(c) = 9$.



Lemma 16.5

$L(c)$ is finite.

Corollary 16.6

Let K be a global field and μ_K be the torsion subgroup of $K^\times$. Then μ_K is finite and equal to the kernel of the map $K^\times \to \operatorname{Div} K$ given by $x \mapsto (||x||_\nu)$. It is also the torsion subgroup of $\mathcal{O}_K^\times$.

As a result, for all global fields K we have an exact sequence of abelian groups

$$1 \to \mu_K \to K^\times \to \operatorname{Div} K \to \operatorname{Pic} K \to 1.$$

Proposition 16.7

Let K be a number field with s complex places, and define $B_K := (\frac{2}{\pi})^s\sqrt{|D_K|}$. If $c \in \operatorname{Div} K$ with $||c|| > B_K$, then $L(c)$ contains an element of $K^\times$.

Proof. We apply the Minkowski lattice point theorem (Theorem 15.10) to R_c and the lattice $I_c \subseteq K \subseteq K_\mathbb{R}$. We need to show that $||c|| > B_K$ implies $\mu(R_c) > 2^n \operatorname{covol}(I_c)$ where $n = [K : \mathbb{Q}]$.

For each real place ν, the constraint $||x||_\nu = |x|_\mathbb{R} \leq c_\nu$ contributes a factor of $2c_\nu$, while for a complex place ν, the constraint $||x||_\nu = |x|_\mathbb{C} \leq c_\nu$ contributes a factor of πc_ν. Then

$$\frac{\mu(R_c)}{\operatorname{covol}(I_c)} = \frac{2^s \mu_{\mathbb{R}^n}(R_c)}{\operatorname{covol}(I_c)} = \frac{2^s(\prod_{\nu \text{ real}} 2c_\nu)(\prod_{\nu \text{ complex}} \pi c_\nu)}{\operatorname{covol}(I_c)} = \frac{2^r(2\pi)^s \prod_{\nu\mid\infty} c_\nu}{\sqrt{|D_K|}\,\mathrm{N}(I_c)} = \frac{2^r(2\pi)^s}{\sqrt{|D_K|}}||c|| = \frac{||c||}{B_K}2^n. \quad \square$$

16.2 Unit group of a number field

We have an isomorphism of topological groups

$$K_{\mathbb{R}}^{\times} \simeq \prod_{\nu|\infty} K_{\nu}^{\times} \simeq \prod_{\nu \text{ real}} \mathbb{R}^{\times} \prod_{\nu \text{ complex}} \mathbb{C}^{\times} = (\mathbb{R}^{\times})^{r} \times (\mathbb{C}^{\times})^{s}.$$

Write elements of $K_{\mathbb{R}}^{\times}$ as vectors $x = (x_\nu)$. Define

$$\operatorname{Log}\colon K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r+s}, \quad (x_\nu) \mapsto (\log ||x_\nu||_\nu)$$

which is surjective, continuous, and a group homomorphism.

Recall that infinite places are in bijection with $\operatorname{Gal}(\mathbb{C}/\mathbb{R})$-orbits of $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. For each $\nu \mid \infty$, pick $\sigma_\nu \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ in the corresponding orbit. Then

$$||x||_\nu = \begin{cases} |\sigma_\nu(x)|_{\mathbb{R}} & \text{if } \nu \text{ real} \\ |\sigma_\nu(x)\overline{\sigma}_\nu(x)|_{\mathbb{R}} & \text{if } \nu \text{ complex} \end{cases}.$$

The absolute norm $\mathrm{N}\colon K^{\times} \to \mathbb{Q}_{>0}$ extends to a continuous homomorphism of locally compact groups

$$\mathrm{N}\colon K_{\mathbb{R}}^{\times} \to \mathbb{R}_{>0}, \quad (x_\nu) \mapsto \prod_{\nu|\infty} ||x_\nu||_\nu .$$

It is compatible with the canonical embedding $K^{\times} \hookrightarrow K_{\mathbb{R}}^{\times}$ because for all $x \in K^{\times}$,

$$\mathrm{N}(x) = |\mathrm{N}_{K/\mathbb{Q}}(x)| = \left|\prod_{\sigma} \sigma(x)\right|_{\mathbb{R}} = \prod_{\nu|\infty} ||x||_\nu .$$

We thus have a commutative diagram

$$\begin{tikzcd}
K^{\times} \arrow[r, hook] \arrow[d, "\mathrm{N}"] & K_{\mathbb{R}}^{\times} \arrow[r, "\operatorname{Log}"] \arrow[d, "\mathrm{N}"] & \mathbb{R}^{r+s} \arrow[d, "\mathrm{T}"] \\
\mathbb{Q}_{>0}^{\times} \arrow[r, hook] & \mathbb{R}_{>0}^{\times} \arrow[r, "\log"] & \mathbb{R}
\end{tikzcd}$$

where $\mathrm{T}\colon \mathbb{R}^{r+s} \to \mathbb{R}$ is defined by $(x_i) \mapsto \sum x_i$. To summarize, $\mathrm{T}(\operatorname{Log} x) = \log \mathrm{N}(x)$.

Since $\mathrm{N}(\mathcal{O}_K^{\times})$ is a unit in $\mathbb{Z}$ and has absolute value 1, $\mathcal{O}_K^{\times} \subseteq \ker(\log \circ \mathrm{N})$, so $\mathcal{O}_K^{\times} \subseteq \ker(\mathrm{T} \circ \operatorname{Log})$. $\operatorname{Log}(\mathcal{O}_K^{\times})$ is a subgroup of the *trace zero hyperplane*

$$\mathbb{R}_0^{r+s} := \{x \in \mathbb{R}^{r+s} : \mathrm{T}(x) = 0\}.$$

Proposition 16.8

Let K be a number field with r real and s complex places. Let $\Lambda_K := \operatorname{Log}(\mathcal{O}_K^{\times}) \subseteq \mathbb{R}_0^{r+s}$. Then

1. We have a split exact sequence of finitely generated abelian groups

$$1 \to \mu_K \to \mathcal{O}_K^{\times} \xrightarrow{\operatorname{Log}} \Lambda_K \to 0.$$

2. Λ_K is a lattice in the trace zero hyperplane $\mathbb{R}_0^{r+s}$.

Proof. 1. To show exactness, let $Z = \ker(\mathcal{O}_K^\times \xrightarrow{\text{Log}} \Lambda_K)$. We have $\mu_K \subseteq Z$ since $\Lambda_K \subseteq \mathbb{R}_0^{r+s}$ is torsion free. Let $c \in \operatorname{Div} K$ satisfy $I_c = \mathcal{O}_K$ and $c_\nu = 2$ for $\nu \mid \infty$, so

$$L(c) = \{x \in \mathcal{O}_K : ||x||_\nu \leq 2, \forall \nu \mid \infty\}.$$

For $x \in \mathcal{O}_K^\times$, we have

$$x \in L(c) \iff \operatorname{Log}(x) \in \{z \in \mathbb{R}^{r+s} : z_i \leq \log 2\}.$$

Note that 0 is in the set on the RHS, so $Z \subseteq L(c)$. $L(c)$ is finite by Lemma 16.5, so Z is finite. Any finite subgroup $Z \subseteq \mathcal{O}_K$ is in the torsion subgroup, so $Z \subseteq \mu_K$.

To show that the short exact sequence splits, we first note $\Lambda_K \cap \operatorname{Log}(R_c) = \operatorname{Log}(\mathcal{O}_K^\times \cap L(c))$ is finite because $L(c)$ is finite. Therefore 0 is an isolated point of Λ_K in $\mathbb{R}^{r+s}$ and in $\mathbb{R}_0^{r+s}$, so Λ_K is a discrete subgroup of $\mathbb{R}_0^{r+s}$, hence finitely generated (Lemma 15.2). This implies $\mathcal{O}_K^\times$ is also finitely generated, as the other terms μ_K and Λ_K in the exact sequence are. By the structure theorem for finitely generated abelian groups, the sequence splits as $\mathcal{O}_K^\times \simeq \mu_K \times \Lambda_K$, since μ_K is the torsion subgroup.

2. Let V be the subspace of $\mathbb{R}_0^{r\times s}$ spanned by Λ_K. FSOC suppose $\dim V < \dim \mathbb{R}_0^{r+s} = r+s-1$. Then the orthogonal subspace $V^\perp$ contains a unit vector u, and for all $\lambda \in \mathbb{R}_{>0}$, the ball $B_{<\lambda}(\lambda u)$ does not intersect Λ_K. It would suffice to show that there exists some $M \in \mathbb{R}_{>0}$ such that for all $h \in \mathbb{R}_0^{r+s}$, there exists some point $\ell \in \Lambda_K$ such that $||h - \ell|| := \max_i |h_i - \ell_i| < M$. Fix a constant $B > B_K$ (from Proposition 16.7). Then for all $c \in \operatorname{Div} K$ with $||c|| > B$, $L(c)$ contains a nonzero element. Fix $b \in \mathbb{R}^{r+s}$ with $b_i \geq 0$ such that $T(b) = \sum_i b_i = \log B$. Let $(\alpha_1), \ldots, (\alpha_m)$ be all nonzero principal ideals with $\mathrm{N}(\alpha_j) \leq B$ (it is a finite list by Lemma 15.16).

Let $M = 2\max\{(r+s)B, \max_j ||\operatorname{Log}(\alpha_j)||\}$. For $h \in \mathbb{R}_0^{r+s}$, define $c \in \operatorname{Div} K$ by $I_c = \mathcal{O}_K$ and $c_\nu := \exp(h_\nu + b_\nu)$ for $\nu \mid \infty$. Then from $\mathrm{T}(h) = 0$,

$$||c|| = \prod_\nu c_\nu = \exp\Big(\sum_\nu (h_\nu + b_\nu)\Big) = \exp \mathrm{T}(h+b) = \exp(\mathrm{T}(h) + \mathrm{T}(b)) = \exp \mathrm{T}(b) = B > B_K.$$

Thus $L(c)$ contains a nonzero $\gamma \in I_c \cap K = \mathcal{O}_K$, and $g = \operatorname{Log}\gamma$ satisfies $g_\nu \leq \log c_\nu = h_\nu + b_\nu$. Also $\mathrm{T}(g) = \mathrm{T}(\operatorname{Log}\gamma) = \log \mathrm{N}(\gamma) \geq 0$ since $\mathrm{N}(\gamma) \geq 1$ for all nonzero $\gamma \in \mathcal{O}_K$. Let $w := g - h \in \mathbb{R}^{r+s}$, so

$$\sum_\nu w_\nu = \mathrm{T}(w) = \mathrm{T}(g) - \mathrm{T}(h) = \mathrm{T}(g) \geq 0$$

and $w_\nu \leq b_\nu < \log B$. Then $||w|| \leq (r+s)B$ so $||g - h|| = ||w|| \leq \frac{M}{2}$. Also

$$\log \mathrm{N}(\gamma) = \mathrm{T}(\operatorname{Log}\gamma) \leq \mathrm{T}(h+b) = \mathrm{T}(b) = \log B$$

so $\mathrm{N}(\gamma) \leq B$ and $(\gamma) = (\alpha_j)$ for some j. Thus $\frac{\gamma}{\alpha_j} \in \mathcal{O}_K^\times$ and $\ell := \operatorname{Log}(\frac{\gamma}{\alpha_j}) = \operatorname{Log}(\gamma) - \operatorname{Log}(\alpha_j) \in \Lambda_K$ satisfies $||g - \ell|| = ||\operatorname{Log}(\alpha_j)|| \leq \frac{M}{2}$ by the definition of M, so by the triangle inequality $||h - \ell|| \leq ||h - g|| + ||g - \ell|| \leq M$. □

Theorem 16.9 (Dirichlet)

Let K be a number field with r real and s complex places. Then $\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r+s-1}$ is finitely generated.

16.3 Regulator of a number field

Definition 16.10 (regulator)**.** The *regulator* of K is

$$R_K := \operatorname{covol}(\pi(\operatorname{Log}(\mathcal{O}_K^\times))) \in \mathbb{R}_{>0}$$

where $\pi\colon \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1}$ is a coordinate projection.

We can compute this explicitly. If $\epsilon_1, \dots, \epsilon_{r+s-1}$ is a basis for the free part of $\mathcal{O}_K^\times$, then R_K is the absolute value of the determinant of any $(r+s-1) \times (r+s-1)$ minor in the $(r+s) \times (r+s)$ matrix with columns as $\operatorname{Log}(\epsilon_i)$.

17 Riemann zeta function and prime number theorem

17.1 Riemann zeta function

Definition 17.1 (Riemann zeta function)**.** $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$.

It is a complex function defined for for $\operatorname{Re}(s) > 1$ (note it converges absolutely on $\operatorname{Re}(s) > 1$).

Theorem 17.2 (Euler product)

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

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1}$$

where the product converges absolutely. In particular, $\zeta(s) \neq 0$ on $\operatorname{Re}(s) > 1$.

Proof. We have

$$\sum_{n \geq 1} n^{-s} = \sum_{n \geq 1} \prod_p p^{-\nu_p(n)s} = \prod_p \sum_{e \geq 0} p^{-es} = \prod (1 - p^{-s})^{-1}.$$

To justify the second equality, consider the partial zeta function

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

where $S_m = \{n \in \mathbb{Z}_{\geq 1} : p \mid n \implies p \leq m\}$ (i.e. no prime factors $p > m$). Fixing $\delta > 0$, the sequence of functions $\zeta_m(s)$ converges uniformly on $\operatorname{Re}(s) > 1 + \delta$: for all $\epsilon > 9$, we have

$$|\zeta_m(s) - \zeta(s)| \leq \left| \sum_{n > m} n^{-s} \right| \leq \sum_{n > m} |n^{-s}| = \sum_{n > m} n^{-\operatorname{Re}(s)} \leq \int_m^\infty x^{-1-\delta}\, dz \leq \frac{1}{\delta} m^{-\delta} < \epsilon$$

for all sufficiently large m.

Thus the $\zeta_m(s)$ converge locally uniformly to $\zeta(s)$ on $\operatorname{Re}(s) > 1$. Also the functions $\prod_{p \leq m} (1 - p^{-s})^{-1}$ converge locally uniformly to $\prod_p (1 - p^{-s})^{-1}$ whenever $\prod_p (1 - p^{-s})^{-1}$ is (absolutely) convergent. For any s with $\operatorname{Re}(s) > 1$,

$$\sum_p \left| \log(1 - p^{-s})^{-1} \right| = \sum_p \left| \sum_{e \geq 1} \frac{1}{e} p^{-es} \right| \leq \sum_p \sum_{e \geq 1} |p^{-s}|^e = \sum_p (|p^s| - 1)^{-1} < \infty,$$

where the first equality is by $\log(1 - z) = -\sum_{n \geq 1} \frac{1}{n} z^n$ for $|z| < 1$. Therefore $\prod_p (1 - p^{-s})^{-1}$ is absolutely convergent on $\operatorname{Re}(s) > 1$. □

Theorem 17.3 (Analytic continuation I)
For $\mathrm{Re}(s) > 1$, we have

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

for $\phi(s)$ holomorphic on $\mathrm{Re}(s) > 0$. Thus $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$, with a simple pole at $s = 1$ with residue 1, and no other poles on $\mathrm{Re}(s) > 0$.

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

$$\zeta(s) - \frac{1}{s-1} = \sum_{n\geq 1} n^{-s} - \int_1^\infty x^{-s}\,dx = \sum_{n\geq 1}\int_n^{n+1} (n^{-s} - x^{-s})\,dx.$$

For each $n \in \mathbb{Z}_{\geq 1}$, define $\phi_n(s) := \int_n^{n+1}(n^{-s} - x^{-s})\,dx$ which is holomorphic on $\mathrm{Re}(s) > 0$. For each fixed s with $\mathrm{Re}(s) > 0$ and $x \in [n, n+1]$,

$$\left|n^{-s} - x^{-s}\right| = \left|\int_n^x st^{-s-1}\,dt\right| \leq \int_n^x \frac{|s|}{|t^{s+1}|}\,dt = \int_n^x \frac{|s|}{t^{1+\mathrm{Re}(s)}}\,dt \leq \frac{|s|}{n^{1+\mathrm{Re}(s)}}.$$

Therefore

$$|\phi_n(s)| \leq \int_n^{n+1} \left|n^{-s} - x^{-s}\right|\,dx \leq \frac{|s|}{n^{1+\mathrm{Re}(s)}}.$$

Now for any s_0 with $\mathrm{Re}(s_0) > 0$, let $\epsilon := \mathrm{Re}(s_0)/2$ and $U := B_{<\epsilon}(s_0)$ so for each $n \geq 1$,

$$\sup_{s\in U} |\phi_n(s)| \leq \frac{|s_0| + \epsilon}{n^{1+\epsilon}} =: M_n.$$

Since $\sum_{n\geq 1} M_n = (|s_0| + \epsilon)\zeta(1+\epsilon)$ converges, $\sum_{n\geq 1}\phi_n$ converges locally normally on $\mathrm{Re}(s) > 0$. By the Weierstrass M-test, $\sum_{n\geq 1}\phi_n$ converges to $\phi(s) = \zeta(s) - \frac{1}{s-1}$ and it is holomorphic on $\mathrm{Re}(s) > 0$. □

We next show there are no zeros on the line $\mathrm{Re}(s) = 1$ (much weaker than the Riemann hypothesis, but needed for the prime number theorem).

Lemma 17.4 (Mertens)
For $x, y \in \mathbb{R}$ with $x > 1$, we have $\left|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)\right| \geq 1$.

Proof. We have

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

using that $\log|z| = \mathrm{Re}\log z$ and $\log(1-z) = -\sum_{n\geq 1}\frac{z^n}{n}$. Plug in $s = x + iy$ to get

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

since $\operatorname{Re}(p^{-ns}) = p^{-nx}\operatorname{Re}(e^{-iny\log p}) = p^{-nx}\cos(-ny\log p) = p^{-nx}\cos(ny\log p)$. Then

$$\begin{aligned}\log\left|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)\right| &= \sum_p\sum_{n\ge 1}\frac{3+4\cos(ny\log p)+\cos(2ny\log p)}{np^{nx}}\\ &\ge 0\end{aligned}$$

by the double angle identity $\cos(2\theta) = 2\cos^2\theta - 1 \implies 3+4\cos\theta+\cos 2\theta = 2(1+\cos\theta)^2 \ge 0$. Exponentiating yields $\left|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)\right| \ge 1$. □

Corollary 17.5

$\zeta(s)$ has no zeros on $\operatorname{Re}(s) \ge 1$.

Proof. By the Euler product (Theorem 17.2), we already know that there are no zeros on $\operatorname{Re}(s) > 1$. Now suppose $\zeta(1+iy) = 0$ for some $y \in \mathbb{R}$. We know $y \ne 0$, since there is a pole at $s = 1$, so there is no pole at $1+2iy$. Then

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

because at $x = 1$, $\zeta(x)^3$ has a pole of order 3, $\zeta(x+iy)^4$ has a zero of order 4, and $\zeta(x+2iy)$ has no pole. However, this contradicts Lemma 17.4. □

17.2 Prime theorem theorem

Definition 17.6 (prime counting function). $\pi(x) := \sum_{p\le x} 1$.

$\pi\colon \mathbb{R} \to \mathbb{Z}_{\ge 0}$ counts the number of primes up to x.

The prime number theorem (PNT) says that

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

which means $\lim_{x\to\infty}\frac{\pi(x)\log x}{x} = 1$. A more precise statement is that

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

(logarithmic integral).

Definition 17.7 (log-weighted prime counting function). $\vartheta(x) := \sum_{p\le x}\log p$

$\vartheta(x)$ should be asymptotic to x.

Theorem 17.8 (Chebyshev)

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

Proof. Since $0 \le \vartheta(x) \le \pi(x)\log x$, we have $\frac{\vartheta(x)}{x} \le \frac{\pi(x)\log x}{x}$. For $\epsilon \in (0,1)$,

$$\begin{aligned}\vartheta(x) &\ge \sum_{x^{1-\epsilon}<p\le x}\log p\\ &\ge (1-\epsilon)(\log x)(\pi(x)-\pi(x^{1-\epsilon}))\\ &\ge (1-\epsilon)(\log x)(\pi(x)-x^{1-\epsilon})\end{aligned}$$

so $\pi(x) \le \frac{1}{1-\epsilon}\frac{\vartheta(x)}{\log x} + x^{1-\epsilon}$ and

$$\frac{\vartheta(x)}{x} \le \frac{\pi(x)\log x}{x} \le \frac{1}{1-\epsilon}\frac{\vartheta(x)}{x} + \frac{\log x}{x^{\epsilon}},$$

where $\frac{\log x}{x^{\epsilon}} \to 0$ as $x \to \infty$. We can make $\epsilon \to 0$. □

The goal now is to show that $\vartheta(x) \sim x$. It's easy to show combinatorially that $\vartheta(x) = O(x)$, and even that $\vartheta(x) \le (4\log 2)x$, but we need to replace the constant by 1 and show the lower bound.

Lemma 17.9

Let $f\colon \mathbb{R}_{\ge 1} \to \mathbb{R}$ be nondecreasing. If $\int_1^\infty \frac{f(t)-t}{t^2}\,dt$ converges, then $f(x) \sim x$.

We want to apply the lemma to $f = \vartheta$. Define

$$H(t) := \vartheta(e^t)e^{-t} - 1.$$

The change of variables $t \mapsto e^u$ implies $\int_1^\infty \frac{\vartheta(t)-t}{t^2}\,dt$ converges if and only if $\int_0^\infty H(u)\,du$ converges.

Definition 17.10 (Laplace transform). For a piecewise continuous function $h\colon \mathbb{R}_{\ge 0} \to \mathbb{R}$, the *Laplace transform* $\mathcal{L}h$ is the complex function

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

It is holomorphic on $\operatorname{Re}(s) > 0$ for any $c \in \mathbb{R}$ for which $h(t) = O(e^{ct})$.

The Laplace transform satisfies

- $\mathcal{L}(g+h) = \mathcal{L}g + \mathcal{L}h$ and $\mathcal{L}(ah) = a\mathcal{L}h$.
- If $h(t) = a$ is constant, then $\mathcal{L}h(s) = \frac{a}{s}$.
- $\mathcal{L}(e^{at}h(t))(s) = \mathcal{L}(h)(s-a)$ for all $a \in \mathbb{R}$.

Now define

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

Lemma 17.11

$\mathcal{L}(\vartheta(e^t))(s) = \frac{\Phi(s)}{s}$ is holomorphic on $\operatorname{Re}(s) > 1$.

Proof. Since $\vartheta(e^t) = O(e^t)$, we know $\mathcal{L}(\vartheta(e^t))$ is holomorphic on $\operatorname{Re}(s) > 1$. Let p_n be the nth prime and $p_0 := 1$, so $\vartheta(e^t)$ is constant on $t \in (\log p_n, \log p_{n+1})$ and

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

Then

$$\begin{aligned}(\mathcal{L}\vartheta(e^t))(s) = \int_0^\infty e^{-st}\vartheta(e^t)\,dt &= \frac{1}{s}\sum_{n=1}^\infty \vartheta(p_n)(p_n^{-s} - p_{n+1}^{-s}) \\ &= \frac{1}{s}\sum_{n=1}^\infty (\vartheta(p_n) - \vartheta(p_{n-1}))p_n^{-s} \qquad (\vartheta(p_0) = 0) \\ &= \frac{1}{s}\sum_{n=1}^\infty p_n^{-s}\log p_n \\ &= \frac{\Phi(s)}{s}. \end{aligned}$$

□

Now the Laplace transform of $H(t) = \vartheta(e^t)e^{-t} - 1$ is

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

on $\mathrm{Re}(s) > 0$, where the last equality is by Lemma 17.11.

Lemma 17.12

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

Proof. Recall from analytic continuation (Theorem 17.3) that $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$ with only a simple pole at $s = 1$ and no zeros on $\mathrm{Re}(s) > 1$. Thus $\frac{\zeta'(s)}{\zeta(s)}$ is meromorphic on $\mathrm{Re}(s) > 0$, with only a simple pole at $s = 1$ and residue -1. We have

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

The RHS converges absolutely to a holomorphic function on $\mathrm{Re}(s) > \frac{1}{2}$; the LHS is meromorphic on $\mathrm{Re}(s) > 0$, and on $\mathrm{Re}(s) \geq 1$ it has a simple pole at $s = 1$ with residue 1. Then we have the desired for $\Phi(s) - \frac{1}{s-1}$. □

Corollary 17.13

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

Proof. The function

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

is meromorphic on $\operatorname{Re}(s) > -\frac{1}{2}$ and holomorphic on $\operatorname{Re}(s) \geq 0$ because both summands are. □

Theorem 17.14 (Newman)

Let $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}$ be bounded and piecewise continuous. Suppose $\mathcal{L}f$ extends to a holomorphic function $g(s)$ on $\operatorname{Re}(s) \geq 0$. Then $\int_0^\infty f(t)\,dt$ converges to and equals $g(0)$.

Theorem 17.15 (Prime number theorem)

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

Proof. $H(t) := \vartheta(e^t)e^{-t} - 1$ is piecewise continuous and bounded by Chebyshev (Theorem 17.8), and $\mathcal{L}H$ extends to a holomorphic function on $\operatorname{Re}(s) \geq 0$ by Corollary 17.13. By Newman (Theorem 17.14),

$$\int_0^\infty H(t)\,dt = \int_0^\infty (\vartheta(e^t)e^{-t} - 1)\,dt$$

converges. Replacing t with $\log x$ shows that

$$\int_1^\infty \left(\vartheta(x)\frac{1}{x} - 1\right)\frac{dx}{x} = \int_1^\infty \frac{\vartheta(x) - x}{x^2}\,dx$$

converges, which implies $\vartheta(x) \sim x$ by Lemma 17.9. □

Remark 17.16. The currently known bound $\pi(x) = \operatorname{Li}(x) + O(\frac{x}{\exp((\log x)^{3/5+o(1)})})$ is subexponential, so it is better than any polynomial bound $O(\frac{x}{(\log x)^n})$ with $n \geq 1$. Assuming the Riemann hypothesis, which states that all zeros of $\zeta(s)$ in $0 < \operatorname{Re}(s) < 1$ have real part $\frac{1}{2}$, we get $\pi(x) = \operatorname{Li}(x) + O(x^{1/2+o(1)})$. More generally, if there are no zeros with real part greater than some $c > \frac{1}{2}$ (say $c = 0.999$), then $\pi(x) = \operatorname{Li}(x) + O(x^{c+o(1)})$ which would beat the current record which has held for 50+ years.

18 The functional equation

Recall that last time we proved that $\zeta(s)$ extends to a meromorphic function on $\operatorname{Re}(s) > 0$. It only has a simple pole at $s = 1$ and no zeros on $\operatorname{Re}(s) \geq 1$. Today we derive a functional equation between $\zeta(s)$ and $\zeta(1-s)$ which extends $\zeta(s)$ to a meromorphic function on $\mathbb{C}$.

18.1 Fourier transform and Poisson summation

Definition 18.1 (Schwartz function). A *Schwartz function* on $\mathbb{R}$ is a complex-valued C^∞ function $f\colon \mathbb{R} \to \mathbb{C}$ that decays rapidly to 0: for all $m, n \in \mathbb{Z}_{\geq 0}$,

$$\sup_{x\in\mathbb{R}} \left| x^m f^{(n)}(x) \right| < \infty.$$

The *Schwartz space* $\mathcal{S}(\mathbb{R})$ of all such functions is a (non-unital) $\mathbb{C}$-algebra of infinite dimension.

Example 18.2

Examples of Schwartz functions include any compactly-supported C^∞-function and the Gaussian $g(x) = e^{-\pi x^2}$.

Nonexamples include polynomials, $\frac{1}{1+x^{2n}}$, and $e^{-x^2}\sin(e^{x^2})$.

$\mathcal{S}(\mathbb{R})$ is closed under differentiation, multiplication by polynomials, and linear change of variables. It is also invariant under convolution: if $f, g \in \mathcal{S}(\mathbb{R})$, then $f * g \in \mathcal{S}(\mathbb{R})$, where

$$(f * g)(x) \coloneqq \int_{\mathbb{R}} f(y)g(x-y)\,dy.$$

Definition 18.3 (Fourier transform). The *Fourier transform* of $f \in \mathcal{S}(\mathbb{R})$ is

$$\widehat{f}(y) \coloneqq \int_{\mathbb{R}} f(x)e^{-2\pi ixy}\,dx,$$

which is also a Schwartz function.

We can recover f from $\widehat{f}$ by

$$f(x) = \int_{\mathbb{R}} \widehat{f}(y)e^{2\pi ixy}\,dy.$$

The maps $f \mapsto \widehat{f}$ and $\widehat{f} \mapsto f$ are thus inverse linear operators on $\mathcal{S}(\mathbb{R})$. We also have

$$\widehat{f * g} = \widehat{f}\widehat{g}, \quad \widehat{fg} = \widehat{f} * \widehat{g},$$

so the Fourier transform is an isomorphism of (non-unital) $\mathbb{C}$-algebras $(\mathcal{S}(\mathbb{R}), +, \times) \to (\mathcal{S}(\mathbb{R}), +, *)$.

Lemma 18.4

For all $a \in \mathbb{R}_{>0}$ and $f \in \mathcal{S}(\mathbb{R})$, $\widehat{f(ax)}(y) = \frac{1}{a}\widehat{f}(\frac{y}{a})$.

Proof. By the substitution $t = ax$,

$$\widehat{f(ax)}(y) = \int_{\mathbb{R}} f(ax)e^{-2\pi ixy}\,dx = \frac{1}{a}\int_{\mathbb{R}} f(t)e^{-2\pi ity/a}\,dt = \frac{1}{a}\widehat{f}\Big(\frac{y}{a}\Big).$$ □

Lemma 18.5

For all $f \in \mathcal{S}(\mathbb{R})$, we have $\frac{d}{dy}\widehat{f}(y) = -2\pi i\,\widehat{xf(x)}(y)$ and $\widehat{\frac{d}{dx}f(x)}(y) = 2\pi iy\widehat{f}(y)$.

The Fourier transform is compatible with the inner product $\langle f,g\rangle = \int_{\mathbb{R}} f(x)\overline{g(x)}\,dx$ on $L^2(\mathbb{R})$ in that

$$\langle f,g\rangle = \int_{\mathbb{R}} f(x)\overline{g(x)}\,dx = \int_{\mathbb{R}}\int_{\mathbb{R}} \widehat{f}(y)\overline{g(X)}e^{2\pi ixy}\,dxdy = \int_{\mathbb{R}} \widehat{f}(y)\overline{\widehat{g}(y)}\,dy = \langle \widehat{f},\widehat{g}\rangle$$

which is known as *Parseval's identity*. The case of $g = f$ is *Plancherel's identity*:

$$||f||_2^2 = \langle f,f\rangle = \langle \widehat{f},\widehat{f}\rangle = ||\widehat{f}||_2^2.$$

Theorem 18.6 (Poisson summation)

For all $f \in \mathcal{S}(\mathbb{R})$,

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$

Proof. Because $f \in \mathcal{S}(\mathbb{R})$, both sums are absolutely convergent. Let $F(x) := \sum_{n\in\mathbb{Z}} f(x+n)$ which is a periodic C^∞-function, so it has a Fourier series expansion $F(x) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi inx}$. The coefficients are

$$c_n = \int_0^1 F(t)e^{-2\pi int}\,dt = \int_0^1 \sum_{m\in\mathbb{Z}} f(t+m)e^{-2\pi int}\,dt = \int_{\mathbb{R}} f(t)e^{-2\pi int}\,dt = \widehat{f}(x).$$

Then

$$\sum_{n\in\mathbb{Z}} f(n) = F(0) = \sum_{n\in\mathbb{Z}} c_n = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$ □

Lemma 18.7

The Gaussian function $g(x) = e^{-\pi x^2}$ satisfies $\widehat{g} = g$.

Proof. Note that g satisfies $g' + 2\pi xg = 0$ with $g(0) = 1$. Multiplying by $-i$ and taking the Fourier transform yields

$$0 = -i(\widehat{g'} + 2\pi\widehat{xg}) = -i(2\pi iy\widehat{g} + i\widehat{g}') = \widehat{g}' + 2\pi y\widehat{g},$$

where the second equality is by Lemma 18.5. Thus, $\widehat{g}$ satisfies the same ODE and has the same initial value $\widehat{g}(0) = \int_{\mathbb{R}} e^{-\pi x^2}\,dx = 1$. □

Definition 18.8 (Jacobi theta function). $\Theta(\tau) := \sum_{n\in\mathbb{Z}} e^{\pi in^2\tau}$.

The sum is absolutely convergent on $\operatorname{im}\tau > 0$ and is periodic mod 2: $\Theta(\tau+2) = \Theta(\tau)$.

Lemma 18.9

For all $a \in \mathbb{R}_{>0}$, we have $\Theta(ia) = \frac{1}{\sqrt{a}}\Theta(\frac{i}{a})$.

Proof. Let $g(x) := e^{-\pi x^2}$ and $h(x) := g(\sqrt{a}x) = e^{-\pi x^2 a}$. By Lemma 18.4 and the fact that $\widehat{g} = g$,

$$\widehat{h}(y) = \widehat{g(\sqrt{a}x)}(y) = \frac{1}{\sqrt{a}}\widehat{g}\Big(\frac{y}{\sqrt{a}}\Big) = \frac{1}{\sqrt{a}}g\Big(\frac{y}{\sqrt{a}}\Big).$$

Now letting $\tau = ia$ and using the Poisson summation (Theorem 18.6) so

$$\Theta(ia) = \sum_{n\in\mathbb{Z}} e^{-i\pi^2 a} = \sum_{n\in\mathbb{Z}} h(n) = \sum_{n\in\mathbb{Z}} \widehat{h}(n) = \sum_{n\in\mathbb{Z}} \frac{1}{\sqrt{a}}g\Big(\frac{n}{\sqrt{a}}\Big) = \frac{1}{\sqrt{a}}\Theta\Big(\frac{i}{a}\Big).$$ □

18.2 Gamma function and functional equation

Definition 18.10 (Mellin transform)**.** The *Mellin transform* of $f\colon \mathbb{R}_{>0} \to \mathbb{C}$ is

$$\mathcal{M}(f)(s) := \int_0^\infty f(t)t^{s-1}\, dt$$

whenever the integral converges.

It is holomorphic on $\mathrm{Re}(s) \in (a, b)$ wherever $\int_0^\infty |f(t)|\, t^{\sigma-1}\, dt$ converges for all $\sigma \in (a, b)$.

Definition 18.11 (Gamma function)**.** The *Gamma function* is

$$\Gamma(s) := \mathcal{M}(e^{-t})(s) = \int_0^\infty e^{-t}t^{s-1}\, dt.$$

The Gamma function is the Mellin transform of e^{-t} and is holomorphic on $\mathrm{Re}(s) > 0$.

Integrating by parts,

$$\Gamma(s) = \frac{t^s e^{-t}}{s}\bigg|_0^\infty + \frac{1}{s}\int_0^\infty e^{-t}t^s\, dt = \frac{\Gamma(s+1)}{s}.$$

There is a simple pole at $s = 0$ with residue 1, so

$$\Gamma(s+1) = s\Gamma(s)$$

for $\mathrm{Re}(s) > 0$. In particular for all integers $n > 0$,

$$\Gamma(n+1) = n!\,\Gamma(1) = n!\,.$$

We can also extend $\Gamma(s)$ to a meromorphic function on $\mathbb{C}$ with simple poles at $0, -1, -2, \ldots$ (and no others).

Theorem 18.12 (Euler's reflection formula)

$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$ are meromorphic functions with simple poles on $\mathbb{Z}$ and no others.

Corollary 18.13

$\Gamma(s)$ has no zeros on $\mathbb{C}$.

Example 18.14

Letting $s = \frac{1}{2}$, we have $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Define

$$F(s) := \pi^{-s}\Gamma(s)\zeta(2s)$$

which is holomorphic on $\mathrm{Re}(s) > \frac{1}{2}$. In this region, we have an absolutely convergent sum

$$F(s) = \pi^{-s}\Gamma(s)\sum_{n\geq 1} n^{-2s} = \sum_{n\geq 1}(\pi n^2)^{-s}\Gamma(s) = \sum_{n\geq 1}\int_0^\infty (\pi n^2)^{-s}t^{s-1}e^{-t}\, dt.$$

Substituting $t = \pi n^2 y$ so $dt = \pi n^2 dy$,

$$F(s) = \sum_{n\geq 1}\int_0^\infty (\pi n^2)^{-s}(\pi n^2 y)^{s-1}e^{-\pi n^2 y}\pi n^2\, dy = \sum_{n\geq 1}\int_0^\infty y^{s-1}e^{-\pi n^2 y}\, dy.$$

By Fubini–Tonelli, we can swap the sum and integral:

$$F(s) = \int_0^\infty y^{s-1} \sum_{n\geq 1} e^{-\pi n^2 y}\, dy.$$

Since $\Theta(iy) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = 1 + 2\sum_{n\geq 1} e^{-\pi n^2 y}$, we have

$$\begin{aligned} F(s) &= \frac{1}{2}\int_0^\infty y^{s-1}(\Theta(iy)-1)\, dy \\ &= \frac{1}{2}\Big(\int_0^\infty y^{s-1}\Theta(iy)\, dy - \frac{1}{s} + \int_1^\infty y^{s-1}(\Theta(iy)-1)\, dy\Big). \end{aligned}$$

Substituting $t = \frac{1}{y}$ into the first integral yields

$$\begin{aligned} \int_0^\infty y^{s-1}\Theta(iy)\, dy &= \int_\infty^1 t^{1-s}\Theta\Big(\frac{i}{t}\Big)(-t^{-2})\, dt \\ &= \int_1^\infty t^{-s-1}\Theta\Big(\frac{i}{t}\Big)\, dt \\ &= \int_1^\infty t^{-s-\frac{1}{2}}(\Theta(it)-1)\, dt + \int_1^\infty t^{-s-\frac{1}{2}}\, dt \\ &= \int_1^\infty t^{-s-\frac{1}{2}}(\Theta(it)-1)\, dt - \frac{1}{\frac{1}{2}-s}. \end{aligned}$$

For the third equality, we use $\Theta(\frac{i}{t}) = \sqrt{t}\Theta(it)$.

All together,

$$F(s) = \frac{1}{2}\int_1^\infty (y^{s-1} + y^{-s-\frac{1}{2}})(\Theta(iy)-1)\, dy - \frac{1}{2s} - \frac{1}{1-2s}$$

on $\mathrm{Re}(s) > \frac{1}{2}$. Note that $F(s) = F(\frac{1}{2}-s)$ for $s \neq 0, \frac{1}{2}$. $F(s)$ was originally defined on $\mathrm{Re}(s) > 0$, but we can now extend it to a meromorphic function on $\mathbb{C}$ with poles at $s = 0, \frac{1}{2}$.

Definition 18.15 (completed zeta function)**.** $Z(s) := \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$.

$Z(s)$ is meromorphic on $\mathbb{C}$ and satisfies $Z(s) = Z(1-s)$. It has simple poles at 0, 1 and no others. The only zeros on $\mathrm{Re}(s) > 0$ are the zeros of $\zeta(s)$, so all zeros lie in the critical strip $0 < \mathrm{Re}(s) < \frac{1}{2}$.

We can use the functional equation to extend $\zeta(s)$ to a meromorphic function on all of $\mathbb{C}$. Recall that $\zeta(s)$ has a pole at $s = 1$ and zeros at $-2, -4, -6, \ldots$ (called trivial zeros of ζ).

Example 18.16

We compute $\zeta(0)$ with the functional equation. First,

$$\zeta(s) = \frac{Z(s)}{\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})} = \frac{Z(1-s)}{\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})} = \frac{\pi^{\frac{s-1}{2}}\Gamma(\frac{1-s}{2})}{\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})}\zeta(1-s) = \frac{\pi^{s-\frac{1}{2}}\Gamma(\frac{1-s}{2})}{\Gamma(\frac{s}{2})}\zeta(1-s).$$

We know that

$$1 = \lim_{s\to 1^+}(s-1)\zeta(s) = \lim_{s\to 1^+}\frac{(s-1)\pi^{s-\frac{1}{2}}\Gamma(\frac{1-s}{2})}{\Gamma(\frac{s}{2})}\zeta(1-s).$$

When $s=1$, we have $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ which cancels out with $\pi^{s-\frac{1}{2}}$. Using $\Gamma(z) = \frac{1}{z}\Gamma(z+1)$ to shift $\Gamma(\frac{1-s}{2})$, we have

$$1 = \lim_{s\to 1^+}(s-1)\frac{2}{1-s}\Gamma\left(\frac{3-s}{2}\right)\zeta(1-s) = -2\Gamma(1)\zeta(0) = -2\zeta(0),$$

so $\zeta(0) = -\frac{1}{2}$.

18.3 Gamma factors and holomorphic zeta function

From the formula $\Gamma(2z) = \pi^{-\frac{1}{2}}2^{2z-1}\Gamma(z)\Gamma(z+\frac{1}{2})$, the functional equation is often written as

$$\zeta(s) = 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s).$$

Define the *Gamma factor* $\Gamma_{\mathbb{R}}(s) := \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$ which corresponds to the ∞ place of $\mathbb{Q}$. Then

$$Z(s) = \Gamma_{\mathbb{R}}(s)\prod_p(1-p^{-s})^{-1}.$$

Theorem 18.17 (Analytic continuation II)

The function $\xi(s) := \binom{s}{2}\Gamma_{\mathbb{R}}(s)\zeta(s)$ is holomorphic on $\mathbb{C}$ and satisfies $\xi(s) = \xi(1-s)$. All zeros lie in $0 < \operatorname{Re}(s) < 1$. Note: $\binom{s}{2} := \frac{s(s-1)}{2}$.

Note that $\overline{\zeta(s)} = \zeta(\overline{s})$. There are no zeros on the real line (we didn't prove this, but it's supposedly not hard), so we can restrict our attention to the upper half plane. Let $N(T)$ be the number of zeros of $\xi(s)$ in the rectangle $R = (0,1) + i(0,T)$. By Cauchy's argument principle, we have

$$N(T) = \frac{1}{2\pi i}\int_{\partial R}\frac{\xi'(s)}{\xi(s)}\,ds$$

(provided there are no zeros on $\operatorname{Re}(s) = T$). One can use this to show that $N(T) \sim \frac{1}{2\pi}T\log(\frac{T}{2\pi e})$.

One can compare $N(T)$ to the number of zeros of the Hardy Z-function $e^{-\theta(t)}\zeta(\frac{1}{2}+it)$ in $0 \le t < T$ where $\theta(t) := \arg(\Gamma(\frac{2it+1}{4})) - \frac{\log\pi}{2}t$. For $T \le 10^{13}$, all zeros lie on the critical line.

19 Dirichlet's theorem

19.1 Infinitely many primes

Theorem 19.1 (Dirichlet 1837)

For all coprime integers $a, m > 0$, there are infinitely many primes $p \equiv a \pmod{m}$.

To motivate the proof, we first give a (silly) proof of there being infinitely many primes. It suffices to show that $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ diverges for $s \to 1^+$. We already know this because $\zeta(s)$ has a pole at $s = 1$, but we reprove it in a different way. Take logarithms to obtain

$$\log \zeta(s) = -\sum_p \log(1-p^{-s}) = \sum_p p^{-s} + O(1)$$

as $s \to 1^+$, since $-\log(1-x) = x + O(x^2)$ as $x \to 0$, and $\sum_p O(p^{-2s}) = O(1)$ for $\operatorname{Re}(s) > \frac{1}{2} + \epsilon$. The following theorem estimates $\sum_{p \le x} \frac{1}{p}$.

Theorem 19.2 (Mertens 1874)

As $x \to \infty$, we have

1. $\sum_{p \le x} \frac{\log p}{p} = \log x + R(x)$ with $|R(x)| < 2$.
2. $\sum_{p \le x} \frac{1}{p} = \log\log x + B + O(\frac{1}{\log x})$ where $B = 0.261497\ldots$ (Merten's constant).
3. $\sum_{p \le x} \log(1 - \frac{1}{p}) = -\log\log x - \gamma + O(\frac{1}{\log x})$ where $\gamma = 0.577216\ldots$ (Euler's constant).

Remark 19.3. Part 2 with $o(\frac{1}{\log x})$ instead of $O(\frac{1}{\log x})$ is equivalent to the prime number theorem.

19.2 Dirichlet characters

Definition 19.4 (arithmetic function). An *arithmetic function* is a function $f\colon \mathbb{Z} \to \mathbb{C}$.

A function f is *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $\gcd(m,n) = 1$, and *totally multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}$.

Definition 19.5 (m-periodic). For $m \in \mathbb{Z}_{>0}$, a function f is *m-periodic* if $f(n+m) = f(n)$ for all $n \in \mathbb{Z}$. The least such m is the *period* of f.

Definition 19.6 (Dirichlet character). A *Dirichlet character* is a periodic, totally multiplicative, arithmetic function $\chi\colon \mathbb{Z} \to \mathbb{C}$.

The function $\mathbb{1} : n \mapsto 1$ is the *trivial* Dirichlet character (unique Dirichlet character with period 1). Every m-periodic Dirichlet character induces a group character on $(\mathbb{Z}/m\mathbb{Z})^\times$, i.e. a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. Conversely, every group character on $(\mathbb{Z}/m\mathbb{Z})^\times$ can be extended to a Dirichlet character χ with $\chi(n) = 0$ for all $\gcd(m,n) \neq 1$ (*extension by zero*).

Definition 19.7 (of modulus m). A Dirichlet character *of modulus m* is an m-periodic Dirichlet character that is the extension by zero of some character on $(\mathbb{Z}/m\mathbb{Z})^\times$. Equivalently, it is an m-periodic Dirichlet character χ with $\chi(n) = 0$ for all $\gcd(m,n) \neq 1$.

Dirichlet characters of modulus m form a group under pointwise multiplication, isomorphic to the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 19.8

Let χ be a Dirichlet character of period m. Then χ is a Dirichlet character of modulus m' if and only if $m \mid m'$ and $m' \mid m^k$ for some $k \in \mathbb{Z}_{>0}$.

Definition 19.9 (induced). Let χ_1, χ_2 be Dirichlet characters of moduli m_1, m_2 with $m_1 \mid m_2$. If $\chi_1(n) = \chi_2(n)$ for all $n \in (\mathbb{Z}/m_2\mathbb{Z})^\times$, then χ_2 is *induced* by χ_1.

Definition 19.10 (primitive). A Dirichlet character not induced by any character other than itself is *primitive*.

Lemma 19.11

A Dirichlet character χ_2 of modulus m_2 is induced by some Dirichlet character χ_1 of modulus $m_1 \mid m_2$ if and only if χ_2 is constant on residue classes of $(\mathbb{Z}/m_2\mathbb{Z})^\times$ that are equivalent modulo m_1.

When this holds, χ_1 is uniquely determined.

Definition 19.12 (principal). A Dirichlet character induced by the trivial character $\mathbb{1}$ is *principal*. Let $\mathbb{1}_m$ denote the principal Dirichlet character of modulus m; it corresponds to the trivial character on $(\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 19.13

If χ is a Dirichlet character of modulus m, then $\sum_{n \in \mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0 \iff \chi = \mathbb{1}_m$.

Proof. Orthogonality of characters. □

Proposition 19.14

Let G be a finite abelian group. For all $g_1, g_2 \in G$, we have

$$\langle g_1, g_2 \rangle \coloneqq \frac{1}{\#G} \sum_{\chi \in \widehat{G}} \chi(g_1)\overline{\chi(g_2)} = \begin{cases} 1 & \text{if } g_1 = g_2 \\ 0 & \text{else} \end{cases}.$$

For all $\chi_1, \chi_2 \in \widehat{G}$,

$$\langle \chi_1, \chi_2 \rangle \coloneqq \frac{1}{\#G} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{if } \chi_1 = \chi_2 \\ 0 & \text{else} \end{cases}.$$

Theorem 19.15

Every Dirichlet character χ is induced by a primitive $\widetilde{\chi}$ that is uniquely determined by χ.

Proof. Partially order the Dirichlet characters with $\chi_1 \preceq \chi_2$ if χ_1 induces χ_2. Let χ be a Dirichlet character of period m, and consider $X \coloneqq \{\chi' : \chi' \preceq \chi\}$. Each $\chi' \in X$ has period $m' \mid m$, and there is at most one $\chi' \in X$ for each $m' \mid m$ (so X is finite). Suppose $\chi_1, \chi_2 \in X$ have periods m_1, m_2, so $m_1, m_2 \mid m$. Let

$m_3 := \gcd(m_1, m_2) \mid m$, so we have a commutative diagram of reduction maps.

$$\begin{tikzcd}
(\mathbb{Z}/m\mathbb{Z})^\times \arrow[r, two heads] \arrow[d, two heads] & (\mathbb{Z}/m_1\mathbb{Z})^\times \arrow[d, two heads] \\
(\mathbb{Z}/m_2\mathbb{Z})^\times \arrow[r, two heads] & (\mathbb{Z}/m_3\mathbb{Z})^\times
\end{tikzcd}$$

Since χ is constant on residue classes of $(\mathbb{Z}/m\mathbb{Z})^\times$ that are congruent mod m_1, or mod m_2, it is constant on residue classes congruent mod $\gcd(m_1, m_2) = m_3$. Thus there is a unique Dirichlet character χ_3 of modulus m_3 that induces χ_1, χ_2, χ, so $\chi_3 \in X$. Therefore every pair $\chi_1, \chi_2 \in X$ has a lower bound χ_3 under $\preceq$ and with respect to the total ordering by period. Thus X contains a unique minimal element (w.r.t. both orderings) inducing everything, and it must be primitive. □

Definition 19.16 (conductor)**.** The *conductor* of χ is the period of the unique primitive $\widetilde{\chi}$ inducing χ.

Corollary 19.17

If χ is a Dirichlet character of modulus m, then $\sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) \neq 0$ if and only if χ has conductor 1.

This is rephrasing Lemma 19.13.

Corollary 19.18

Let $M(m)$ denote the set of Dirichlet characters of modulus m, $X(m)$ denote the set of primitive Dirichlet characters with conductor dividing m, and $\widehat{G}(m)$ denote the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$. There are canonical bijections $M(m) \xrightarrow{\sim} X(m) \xrightarrow{\sim} \widehat{G}(m)$ with $\chi \mapsto \widetilde{\chi} \mapsto (n \mapsto \overline{\chi}(n))$.

Remark 19.19. Since $M(m)$ is a group, we can make $X(m)$ into a group via $\widetilde{\chi_1}\widetilde{\chi_2} := \widetilde{\chi_1\chi_2}$. However, note that $\widetilde{\chi_1\chi_2}$ is not necessarily the pointwise product of $\widetilde{\chi_1}$ and $\widetilde{\chi_2}$; it is the unique primitive character inducing $\widetilde{\chi_1}\widetilde{\chi_2}$.

19.3 Dirichlet L-functions

Definition 19.20 (Dirichlet L-function)**.** The *Dirichlet L-function* associated to a Dirichlet character χ is

$$L(s, \chi) := \prod_p (1 - \chi(p)p^{-s})^{-1} = \sum_{n\geq 1} \chi(n)n^{-s}.$$

The sum and product converge on $\mathrm{Re}(s) > 1$.

Note that

$$L(s, \mathbb{1}) = \zeta(s) = L(s, \mathbb{1}_m) \prod_{p\mid m} (1 - p^{-s})^{-1}.$$

Then $L(s, \mathbb{1}_m)$ has a simple pole at $s = 1$ like $\zeta(s)$ with residue

$$\mathrm{res}_{s=1} L(s, \mathbb{1}_m) = \lim_{s\to 1^+} (s-1)\zeta(s) \prod_{p\mid m} (1 - p^{-s}) = \prod_{p\mid m} (1 - p^{-1}) = \frac{\phi(m)}{m}.$$

Proposition 19.21

Let χ be a nonprincipal Dirichlet character of modulus m. Then $L(s,\chi)$ extends to a holomorphic function on $\operatorname{Re}(s) > 0$.

Proof. Define $T\colon \mathbb{R}_{\geq 0} \to \mathbb{C}$ by $x \mapsto \sum_{0<n\leq x} \chi(n)$. Then

$$T(x+m) - T(x) = \sum_{x<n\leq x+m} \chi(n) = \sum_{n\in\mathbb{Z}/m\mathbb{Z}} \chi(n) = 0,$$

so T is periodic modulo m, hence bounded. Integrating by parts,

$$\begin{aligned} L(s,\chi) &= \sum_{n\geq 1} \chi(n)n^{-s} \\ &= \int_0^\infty x^{-s}\, dT(x) \\ &= x^{-s}T(x)\Big|_0^\infty - \int_0^\infty T(x)\, d(x^{-s}) \\ &= 0 - \int_0^\infty T(x)(-sx^{-s-1})\, dx \\ &= s\int_0^\infty T(x)x^{-s-1}\, dx \end{aligned}$$

which is holomorphic on $\operatorname{Re}(s) > 0$ since it is the limit of uniformly converging $\phi_n(s) \coloneqq s\int_0^n T(x)x^{-s-1}\, dx$ (here we use T bounded). □

Remark 19.22. If $f, g\colon [a,b] \to \mathbb{R}$ with g' continuous, then $\int_a^b f\, dg = \int_a^b f(x)g'(x)\, dx$.

19.4 Primes in arithmetic progressions

To prove Dirichlet's theorem, it suffices to show that $\sum_{p\equiv a \pmod m} p^{-s}$ is unbounded as $s \to 1^+$. Consider the indicator function

$$\frac{1}{\phi(m)} \sum_{\chi\in X(m)} \chi\left(\frac{p}{a}\right) = \begin{cases} 1 & \text{if } p \equiv a \pmod m \\ 0 & \text{else} \end{cases}$$

where $\frac{p}{a}$ is done mod m. As $s \to 1^+$,

$$\begin{aligned} \sum_{p\equiv a \pmod m} p^{-s} &= \sum_p p^{-s} \frac{1}{\phi(m)} \sum_{\chi\in X(m)} \chi\left(\frac{p}{a}\right) \\ &= \sum_{\chi\in X(m)} \frac{\chi(\frac{1}{a})}{\phi(m)} \sum_p \chi(p)p^{-s} \\ &= \sum_{\chi\in X(m)} \frac{\chi(\frac{1}{a})}{\phi(m)} (\log L(s,\chi) + O(1)) \\ &= \frac{\log\zeta(s)}{\phi(m)} + \sum_{\chi\in X(m), \chi\neq\mathbb{1}} \frac{\chi(\frac{1}{a})}{\phi(m)} \log L(s,\chi) + O(1). \end{aligned}$$

The key claim is that $L(1,\chi) \neq 0$ for all nonprincipal χ. Then $\log L(s,\chi) = O(1)$ as $s \to 1^+$, so

$$\sum_{p \equiv a \pmod{m}} p^{-s} = \frac{\log \zeta(s)}{\phi(m)} + O(1).$$

This is unbounded as $s \to 1^+$, since $\log \zeta(s)$ is. Also, Mertens' theorem implies that

$$\sum_{p \leq x, p \equiv a \pmod{m}} \frac{1}{p} \sim \frac{\log \log x}{\phi(m)},$$

so there are infinitely many primes $p \equiv a \pmod{m}$.

Definition 19.23 (Dirichlet, natural density)**.** The *Dirichlet density* of a set of primes S is

$$d(S) \coloneqq \lim_{s \to 1^+} \frac{\sum_{p \in S} p^{-s}}{\sum_p p^{-s}}.$$

The *natural density* of S is

$$\delta(S) \coloneqq \lim_{x \to \infty} \frac{\#\{p \leq x : p \in S\}}{\#\{p \leq x\}}.$$

For $S = \{p \equiv a \pmod{m}\}$, we have

$$d(S) = \lim_{s \to 1^+} \frac{\sum_{p \equiv a \pmod{m}} p^{-s}}{\sum_p p^{-s}} = \lim_{s \to 1^+} \frac{\log \zeta(s)/\phi(m)}{\log \zeta(s)} = \frac{1}{\phi(m)},$$

independent of a. Note this is weaker than the prime number theorem for arithmetic progressions, which states

$$\pi(x; m, a) \coloneqq \{p \equiv a \pmod{m} : p \leq x\} \sim \frac{1}{\phi(m)} \pi(x),$$

where $\pi(x; m, a)$ is the number of primes $p \leq x$ with $p \equiv a \pmod{m}$.

20 Analytic class number formula

Definition 20.1 (Dedekind zeta function)**.** The *Dedekind zeta function* of a number field K is

$$\zeta_K(z) \coloneqq \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-z} = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-z})^{-1}$$

where $\mathfrak{a}$ ranges over nonzero $\mathcal{O}_K$-ideals and $\mathfrak{p}$ ranges over nonzero prime ideals.

The product converges absolutely on $\mathrm{Re}(z) > 1$.

Theorem 20.2 (Analytic class number formula)

Let K be a number field with r real and s complex places of degree $n = r + 2s$. Then $\zeta_K(z)$ extends to a meromorphic function on $\mathrm{Re}(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$ with residue

$$\lim_{z \to 1^+} (z-1)\zeta_K(z) = \frac{2^r (2\pi)^s h_K R_K}{w_K \, |D_K|^{\frac{1}{2}}}$$

where $h_K \coloneqq \#\,\mathrm{cl}(\sigma_K)$ is the class number, R_K is the regulator, w_k is the number of roots of unity, and $D_K \coloneqq \operatorname{disc} \mathcal{O}_K$ is the absolute discriminant.

Example 20.3

For $K = \mathbb{Q}$, we have $n = 1, r = 1, s = 0, h = 1, w = 2, D = 1, R = 1$. Then $\zeta_{\mathbb{Q}}(z) = \zeta(z)$ is holomorphic on $\operatorname{Re}(z) > 1 - \frac{1}{1} = 0$ except for a simple pole at $z = 1$ with residue $\lim_{z\to 1^+}(z-1)\zeta_{\mathbb{Q}}(z) = \frac{2^1(2\pi)^0 \cdot 1 \cdot 1}{2\cdot |1|^{\frac{1}{2}}} = 1$.

20.1 Lipschitz parameterizability

Definition 20.4 (Lipschitz continuous)**.** Let X, Y be metric spaces. A function $f\colon X \to Y$ is *Lipschitz continuous* if there exists $c \in \mathbb{R}_{>0}$ such that for all $u, v \in X$, $d(f(u), f(v)) \le c d(u, v)$.

Definition 20.5. A set B in a metric space X is *d-Lipschitz parameterizable* if it is the union of the images of a finite number of Lipschitz continuous functions $f_i\colon [0,1]^d \to X$.

Recall the asymptotic notation $f(t) = g(t) + O(h(t))$ means $\limsup_{t\to\infty} \left|\frac{f(t)-g(t)}{h(t)}\right| < \infty$.

Lemma 20.6

Let $S \subseteq \mathbb{R}^n$ be a measurable set whose boundary $\partial S := \overline{S} - S^\circ$ is $(n-1)$-Lipschitz parameterizable. As $t \to \infty$,

$$\#(tS \cap \mathbb{Z}^n) = \mu(S)t^n + O(t^{n-1}).$$

It reduces the problem of counting lattice points to computing the measure of S.

Corollary 20.7

Let Λ be a lattice in $V \simeq \mathbb{R}^n$, and let $S \subseteq V$ be a measurable set whose boundary is $(n-1)$-Lipschitz parameterizable. Then as $t \to \infty$,

$$\#(tS \cap \Lambda) = \frac{\mu(S)}{\operatorname{covol}(\Lambda)} t^n + O(t^{n-1}).$$

Proof. If $\Lambda \subseteq \mathbb{Z}^n$, then it follows from the above lemma. Also if the corollary holds for $s\Lambda$ for some $s > 0$, then it holds for Λ, since $\#(tS \cap s\Lambda) = \#(\frac{t}{s}S \cap \Lambda)$. For any Λ, we can pick s such that $s\Lambda$ is very close to a sublattice of $\mathbb{Z}^n$; e.g. take s to be the product of all denominators in rational approximations of the real coefficients of an $\mathbb{R}$-basis for Λ. □

20.2 Counting algebraic integers of bounded norm

Recall the unit group $K_{\mathbb{R}}^\times$ of $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$ is the locally compact group

$$K_{\mathbb{R}}^\times \simeq \prod_{\nu|\infty} K_\nu^\times \simeq \prod_{\text{real } \nu|\infty} \mathbb{R}^\times \times \prod_{\text{complex } \nu|\infty} \mathbb{C}^\times.$$

There is a natural embedding $K^\times \hookrightarrow K_{\mathbb{R}}^\times$ by $x \mapsto (x_\nu)$ where ν ranges over the $r+s$ archimedean places of K. Then we can view $K^\times$ as a subgroup of $K_{\mathbb{R}}^\times$ that contains all nonzero elements of $\mathcal{O}_K$. We also defined $\operatorname{Log}\colon K_{\mathbb{R}}^\times \to \mathbb{R}^{r+s}$ by $(x_\nu) \mapsto (\log ||x_\nu||_\nu)$. From Proposition 16.8, there is an exact sequence

$$1 \to \mu_K \to \mathcal{O}_K^\times \xrightarrow{\operatorname{Log}} \Lambda_K \to 0$$

where Λ_K is in the trace zero hyperplane $\mathbb{R}_0^{r+s} = \{x \in \mathbb{R}^{r+s} : \mathrm{T}(x) = 0\}$. The regulator R_K is the covolume of Λ_K in $\mathbb{R}_0^{r+s}$ where $\mathbb{R}_0^{r+s}$ has measure induced by any coordinate projection $\mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1} \simeq \mathbb{R}^{r+s}$. Dirichlet's unit theorem says that $\mathcal{O}_K^\times = U \times \mu_K$ where μ_K are the roots of unity and $U \subseteq \mathcal{O}_K^\times$ is the free $\mathbb{Z}$-module of rank $r+s-1$.

We want to estimate

$$\#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \leq t\}.$$

To simplify matters, start with the principal ideals $\mathfrak{a} = (\alpha)$, so we want to estimate $\#\{(\alpha) : \mathrm{N}(\alpha) \leq t\}$. For nonzero $\alpha, \alpha' \in K^\times$, $(\alpha) = (\alpha') \iff \frac{\alpha}{\alpha'} \in \mathcal{O}_K^\times$ is a unit. So equivalently, we consider

$$\{\alpha \in K^\times \cap \mathcal{O}_K : \mathrm{N}(\alpha) \leq t\}/\mathcal{O}_K^\times,$$

where $S/\mathcal{O}_K^\times$ for $S \subseteq K_\mathbb{R}^\times$ means $\alpha \sim \alpha' \iff \alpha = u\alpha'$ for some $u \in \mathcal{O}_K^\times$. Now defining

$$K_{\mathbb{R},\leq t}^\times \coloneqq \{x \in K_\mathbb{R}^\times : \mathrm{N}(x) \leq t\} \subseteq K_\mathbb{R}^\times \subseteq K_\mathbb{R},$$

we want to estimate $\#(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/\mathcal{O}_K^\times$. Now replace $\mathcal{O}_K^\times$ with $U \subseteq \mathcal{O}_K^\times$, so there is a w_K-to-1 map $(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/U \to (K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/\mathcal{O}_K^\times$, and we now want to estimate $\#(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K)/U$.

Recall for $x = (x_\nu) \in K_\mathbb{R}^\times$, the norm map $\mathrm{N}\colon K_\mathbb{R}^\times \to \mathbb{R}_{>0}^\times$ is defined by

$$\mathrm{N}(x) \coloneqq \prod_{\nu|\infty} ||x_\nu||_\nu = \prod_{\nu \text{ real}} |x_r|_\mathbb{R} \times \prod_{\nu \text{ complex}} |x_\nu|_\mathbb{C}^2$$

and satisfies $\mathrm{T}(\log x) = \log \mathrm{N}(x)$ for all $x \in K_\mathbb{R}^\times$. Now define the surjective homomorphism $\gamma\colon K_\mathbb{R}^\times \to K_{\mathbb{R},1}^\times$ by $x \mapsto x\,\mathrm{N}(x)^{-\frac{1}{n}}$. Then $\mathrm{Log}(K_{\mathbb{R},1}^\times) = \mathbb{R}_0^{r+s}$. Fix a fundamental domain F for Λ_K in $\mathbb{R}_0^{r+s}$, so $S \coloneqq \gamma^{-1}(\mathrm{Log}^{-1}(F))$ is a set of unique coset representatives for $K_\mathbb{R}^\times/U$. Defining $S_{\leq t} \coloneqq \{x \in S : \mathrm{N}(x) \leq t\} \subseteq K_\mathbb{R}$, we want to estimate the cardinality of $S_{\leq t} \cap \mathcal{O}_K$. Now $\mathcal{O}_K$ is a lattice in $K_\mathbb{R}$ and $tS_{\leq 1} = S_{\leq t^n}$, so we can estimate $S_{\leq t} = t^{\frac{1}{n}} S_{\leq 1}$ using $S_{\leq 1}$, as long as the boundary of $S_{\leq 1}$ is $(n-1)$-Lipschitz parameterizable which we now show.

Since $\ker(\mathrm{Log}) = \{\pm 1\}^r \times U(1)^s$ where $U(1) \subset \mathbb{C}$ is the unit circle, we have a continuous isomorphism of locally compact groups

$$\begin{aligned} K_\mathbb{R}^\times = (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s &\xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\}^r \times [0, 2\pi)^s \\ x = (x_1, \ldots, x_r, z_1, \ldots, z_s) &\mapsto (\mathrm{Log}\, x) \times (\operatorname{sgn} x_1, \ldots, \operatorname{sgn} x_r) \times (\arg z_1, \ldots, \arg z_s). \end{aligned}$$

The set $S_{\leq 1}$ has 2^r connected components, one for each element of $\{\pm 1\}^r$. Parameterize each component using n real parameters:

- $r+s-1$ parameters in $[0,1)$ encoding points in F as $\mathbb{R}$-linear combinations of $\mathrm{Log}(\epsilon_1), \ldots, \mathrm{Log}(\epsilon_{r+s-1})$ where $\epsilon_1, \ldots, \epsilon_{r+s-1}$ is a basis for U.
- s parameters in $[0,1)$ encoding elements of $U(1)^s$ (take the angle and scale by 2π).
- 1 parameter in $(0,1]$ encoding the nth root of the norm.

We thus have a continuously differentiable bijection from $C = [0,1)^{n-1} \times (0,1] \subseteq [0,1]^n$ to each of the 2^n components of $S_{\leq 1}$. The boundary $\partial C = \partial [0,1]^n$ is $(n-1)$-Lipschitz parameterizable, and thus each component of $S_{\leq 1}$ and $S_{\leq 1}$ itself are $(n-1)$-Lipschitz parameterizable.

We now can apply Corollary 20.7 to get

$$\begin{aligned} \#(S_{\leq t} \cap \mathcal{O}_K) &= \frac{\mu(S_{\leq 1})}{\mathrm{covol}(\mathcal{O}_K)} (t^{1/n})^n + O\left((t^{1/n})^{n-1}\right) \\ &= \frac{\mu(S_{\leq 1})}{|D_K|^{\frac{1}{2}}} t + O\left(t^{1-1/n}\right). \end{aligned} \tag{20.1}$$

Next we compute $\mu(S_{\leq 1})$. Recall the normalized Haar measure μ on $K_{\mathbb{R}} = \prod_{\nu|\infty} K_\nu \simeq \mathbb{R}^r \times \mathbb{C}^s$. In terms of the Lebesgue measures dx on $\mathbb{R}$ and dA on $\mathbb{C}$, we have $\mu = (dx)^r (2dA)^s$ (get a 2 by taking derivative of the square). Now define the map $\mathbb{R}^\times \xrightarrow{\sim} \mathbb{R} \times \{\pm 1\}$ by $x \mapsto (\log|x|, \operatorname{sgn} x)$, so $\pm e^\ell \mapsfrom (\ell, \pm 1)$ and $dx \mapsto e^\ell d\ell \mu_{\{\pm 1\}}$. Define $\mathbb{C}^\times \xrightarrow{\sim} \mathbb{R} \times [0, 2\pi)$ by $z \mapsto (2\log|z|, \arg z)$, so $e^{\ell/2 + i\theta} \mapsfrom (\ell, \theta)$ and $2dA \mapsto 2e^{\ell/2} d(e^{\ell/2}) = e^\ell d\ell d\theta$ where $d\ell$ is the Lebesgue measure on $\mathbb{R}$, $\mu_{\{\pm 1\}}$ is the counting measure on $\{\pm 1\}$, and $d\theta$ is the Lebesgue measure on $[0, 2\pi)$. All together, we have a map

$$\begin{gathered} K_{\mathbb{R}}^\times \xrightarrow{\sim} \mathbb{R}^{r+s} \times \{\pm 1\} \times [0, 2\pi)^s \\ \mu \mapsto e^{T(\bullet)} \mu_{\mathbb{R}^{r+s}} \mu^r_{\{\pm 1\}} \mu^s_{[0,2\pi)}. \end{gathered}$$

Finally, consider the change of coordinates

$$\begin{gathered} \mathbb{R}^{r+s} \to \mathbb{R}^{r+s-1} \times \mathbb{R} \\ x = (x_1, \ldots, x_{r+s}) \mapsto (x_1, \ldots, x_{r+s-1}, y := \mathrm{T}(x)) \\ e^{\mathrm{T}(x)} \mu_{\mathbb{R}^{r+s}} \mapsto e^y \mu_{\mathbb{R}^{r+s-1}} dy. \end{gathered}$$

We thus have a bijection

$$\begin{gathered} S_{\leq 1} \xrightarrow{\sim} F + (-\infty, 0] \left(\frac{1}{n}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{2}{n} \right) \times \{\pm 1\}^\sigma \times [0, 2\pi)^s \\ x = \mathrm{N}(x)^{\frac{1}{n}} \gamma(x) \mapsto \mathrm{Log}(x) + \log \mathrm{N}(x) \left(\frac{1}{n}, \ldots, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{2}{n} \right) \times (\operatorname{sgn} x_1, \ldots, \operatorname{sgn} x_r) \times (\arg z_1, \ldots, \arg z_s). \end{gathered}$$

Then $K_{\mathbb{R}}^\times \xrightarrow{\sim} \mathbb{R}^{r+s-1} \times \mathbb{R} \times \{\pm 1\}^r \times [0, 2\pi)^s$ and $S_{\leq 1} \xrightarrow{\sim} \pi_0(F) \times (-\infty, 0] \times \{\pm 1\}^r \times [0, 2\pi)^s$. By definition, $R_K = \mu_{\mathbb{R}^{r+s-1}}(\pi_0(F))$, so

$$\mu(S_{\leq 1}) = \int_{-\infty}^0 e^y R_K 2^r (2\pi)^s \, dy = 2^r (2\pi)^s R_K.$$

Plugging this into (20.1) yields

$$\#(S_{\leq t} \cap \mathcal{O}_K) = \frac{2^r (2\pi)^s R_K}{|D_K|^{\frac{1}{2}}} t + O(t^{1-\frac{1}{n}}).$$

20.3 Proof of the analytic class number formula

Theorem 20.8

Let K be a number field of degree n. As $t \to \infty$, the number of nonzero $\mathcal{O}_K$-ideals $\mathfrak{a}$ of norm $\mathrm{N}(\mathfrak{a}) \leq t$ is

$$\frac{2^r (2\pi)^s h_K R_K}{w_K |D_K|^{\frac{1}{2}}} t + O\left(t^{1-1/n}\right).$$

Proof. By the w_K-to-1 map $S_{\leq t} \cap \mathcal{O}_K \to (K^\times_{\mathbb{R}, \leq t} \cap \mathcal{O}_K)/\mathcal{O}_K^\times$, we know

$$\#\{(\alpha) \subseteq \mathcal{O}_K : \mathrm{N}(\alpha) \leq t\} = \frac{2^r (2\pi)^s R_K}{w_K |D_K|^{\frac{1}{2}}} t + O\left(t^{1-1/n}\right). \tag{20.2}$$

It remains to show that the nonzero ideals $\mathfrak{a}$ of norm $\mathrm{N}(\mathfrak{a}) \leq t$ are asymptotically equidistributed among ideal classes. Given an ideal class $[\mathfrak{a}] \in \operatorname{cl} \mathcal{O}_K$, multiplication by $\mathfrak{a}$ gives a bijection

$$\begin{aligned} \{\text{ideals } \mathfrak{b} \in [\mathfrak{a}^{-1}] : \mathrm{N}(\mathfrak{b}) \leq t\} &\xrightarrow{\times \mathfrak{a}} \{\text{nonzero principal ideals } (\alpha) \subseteq \mathfrak{a} : \mathrm{N}(\alpha) \leq t\,\mathrm{N}(\mathfrak{a})\} \\ &\to \{\text{nonzero } \alpha \in \mathfrak{a} : \mathrm{N}(\alpha) \leq t\,\mathrm{N}(\mathfrak{a})\}/\mathcal{O}_K^\times. \end{aligned}$$

Let $S_{[a],\leq t}$ denote the last set. Replace $\mathcal{O}_K$ with $\mathfrak{a}$ in (20.2) to get

$$\#S_{[a],\leq t} = \frac{2^r(2\pi)^s R_K}{w_K\,\mathrm{covol}(\mathfrak{a})} t\,\mathrm{N}(\mathfrak{a}) + O\left(t^{1-1/n}\right)$$

where $\mathrm{covol}(\mathfrak{a}) = \mathrm{covol}(\mathcal{O}_K)\,\mathrm{N}(\mathfrak{a})$ so it cancels and $\mathrm{covol}(\mathcal{O}_K) = |D_K|^{\frac{1}{2}}$. Summing over ideal classes yields the desired equation. □

Lemma 20.9

Let $a_1, a_2, \dots$ be a sequence in $\mathbb{C}$ and $\sigma \in \mathbb{R}$. If $a_1 + \dots + a_t = O(t^\sigma)$ as $t \to \infty$, then $\sum a_n n^{-s}$ is holomorphic on $\mathrm{Re}(s) > \sigma$.

Lemma 20.10

Let $a_1, a_2, \dots$ be a sequence in $\mathbb{C}$ satisfying $a_1 + \dots + a_t = \rho t + O(t^\sigma)$ for $\rho \in \mathbb{C}^\times$ and $\sigma \in [0,1)$. Then $\sum a_n n^{-s}$ converges on $\mathrm{Re}(s) > 1$ and has a meromorphic continuation to $\mathrm{Re}(s) > \sigma$ that is holomorphic except a simple pole at $s = 1$ with residue ρ.

Proof of the analytic class number formula (Theorem 20.2). Recall we are trying to prove that $\zeta_K(z)$ extends to a meromorphic function on $\mathrm{Re}(z) > 1 - \frac{1}{n}$ that is holomorphic except for a simple pole at $z = 1$ with residue

$$\lim_{z \to 1^+} (z-1)\zeta_K(z) = \rho_K := \frac{2^r(2\pi)^s h_K R_K}{w_K\,|D_K|^{\frac{1}{2}}}.$$

We have $\zeta_K(z) = \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-z} = \sum_{t \geq 1} a_t t^{-z}$ where $a_t = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = t\}$. By Theorem 20.8,

$$a_1 + \dots + a_t = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \leq t\} = \rho_K t + O(t^{1-\frac{1}{n}})$$

as $t \to \infty$. By the above lemmas, $\zeta_K(z) = \sum a_t t^{-z}$ extends to a meromorphic function on $\mathrm{Re}(z) > 1 - \frac{1}{n}$ with a simple pole at $z = 1$ of residue ρ_K. □

Remark 20.11. Hecke showed that $\zeta_K(z)$ can be extended to all of $\mathbb{C}$. Moreover, letting $\Gamma_{\mathbb{R}} := \pi^{-z/2}\Gamma(\frac{z}{2})$ and $\Gamma_{\mathbb{C}}(z) := \Gamma_{\mathbb{R}}(z)\Gamma_{\mathbb{R}}(z+1) = 2(2\pi)^{-s}\Gamma(z)$, then the *completed zeta function* $\xi_K(z) := |D_K|^{z/2}\,\Gamma_{\mathbb{R}}(z)^r\Gamma_{\mathbb{C}}(z)^s\zeta_K(z)$ satisfies the functional equation $\xi_K(z) = \xi_K(1-z)$.

Note if $K = \mathbb{Q}(\zeta_m)$ is a cyclotomic field, then $\zeta_K(s) = \prod_\chi L(s,\chi)$. See notes to conclude the proof of Dirichlet's theorem.

21 Ring of adeles

21.1 Restricted product

Recall $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} \simeq \prod_p \mathbb{Z}_p$. We know the $\mathbb{Z}_p$ are compact topological groups (B_1 in $\mathbb{Q}_p$) so the product $\widehat{\mathbb{Z}}$ is compact. However, $\prod_p \mathbb{Q}_p$ is a product of locally compact groups but is not locally compact. The problem is that the product topology is too weak. Recall on $(X_i)_{i \in I}$, the product topology is the weakest topology making $\pi_i \colon (X_i)_{i \in I} \to X_i$ continuous, generated by $\pi_i^{-1}(U_i)$ with $U_i \subseteq X_i$ open. So each open set is a union of $\prod_{i \in S} U_i \times \prod_{i \notin S} X_i$ for some finite subset $S \subseteq I$.

Definition 21.1 (restricted product)**.** Let $(X_i)_{i\in I}$ be topological spaces and $U_i \subseteq X_i$ be open sets. The *restricted product* is the topological space

$$\prod_{i\in I}(X_i, U_i) \coloneqq \{(x_i) : x_i \in X_i \text{ and } x_i \in U_i \text{ for almost all } i \in I\} \subseteq \prod_{i\in I} X_i.$$

A basis of open sets is

$$\mathcal{B} \coloneqq \left\{ \prod_{i\in I} V_i : V_i \subseteq X_i \text{ open } \forall i \in I, V_i = U_i \text{ for almost all } i \right\}.$$

The projections $\pi_i \colon \prod(X_i, U_i) \to X_i$ by $(x_i) \mapsto x_i$ are continuous. Note $\prod_{i\in I} U_i \subseteq \prod(X_i, U_i) \subseteq \prod X_i$ where the first containment is open, but $\prod_{i\in I} U_i$ might not be open in the larger $\prod X_i$, because the restricted product topology is finer than the product topology.

Each $x \in X \coloneqq \prod(X_i, U_i)$ determines some finite $S(x) \coloneqq \{i \in I : x_i \notin U_i\}$. Given a finite $S \subseteq I$, define

$$X_S \coloneqq \{x \in X_i : S(x) \subseteq S\} = \prod_{i\in S} X_i \times \prod_{i\notin S} U_i.$$

Then $X_S \in \mathcal{B}$, and we can view X_S as a subspace of X or as a direct product. Note that $X_S \subseteq X_T$ whenever $S \subseteq T$, so we can partially order the finite $S \subseteq I$ by inclusion. Then the $\{X_S \colon S \subseteq I \text{ finite}\}$ with inclusion maps $\{i_{ST} \colon X_S \hookrightarrow X_T \mid S \subseteq T\}$ form a direct system with

$$\varinjlim_S X_S \coloneqq \bigsqcup X_S/\sim$$

where $x \sim i_{ST}(x)$ for all $S \subseteq T$. It turns out that

$$\varinjlim_S X_S \simeq \prod(X_i, U_i).$$

Proposition 21.2

Let $(X_i)_{i\in I}$ be a family of locally compact topological spaces and $(U_i)_{i\in I}$ be a family of open $U_i \subseteq X_i$ with almost all compact. Then $X \coloneqq \prod(X_i, U_i)$ is locally compact.

Proof. Take a finite $S \subseteq I$ and consider $X_S \coloneqq \prod_{i\in S} X_i \times \prod_{i\notin S} U_i$. X_S is locally compact because it is a finite product of the locally compact spaces $\prod_{i\in S} X_i$ and the compact space $\prod_{i\notin S} U_i$. Then X is locally compact by direct limits.

Alternatively, because each $x \in X$ lies in some X_S, in that X_S it has an open neighborhood containing a compact neighborhood, and this carries over to X. □

21.2 Ring of adeles

For non-archimedean ν, we let $\mathcal{O}_\nu$ be the valuation ring of K_ν, while for the finite number of archimedean ν, we just define $\mathcal{O}_\nu \coloneqq K_\nu$.

Definition 21.3 (adele ring)**.** Let K be a global field. The *adele ring* of K is the restricted product

$$\mathbb{A}_K = \prod_{\nu\in M_K}(K_\nu, \mathcal{O}_\nu) \coloneqq \left\{(a_\nu) \in \prod_\nu K_\nu : a_\nu \in \mathcal{O}_\nu \text{ for almost all } \nu\right\}.$$

For any finite set of places S, the subring of *S-adeles* is

$$\mathbb{A}_{K,S} \coloneqq \prod_{\nu \in S} K_\nu \times \prod_{\nu \notin S} \mathcal{O}_\nu.$$

Then $\mathbb{A}_K \simeq \varinjlim_S \mathbb{A}_{K,S}$, so $\mathbb{A}_K$ is also a topological ring. The canonical embedding $K \hookrightarrow K_\nu$ induces $K \hookrightarrow \mathbb{A}_K$ by $x \mapsto (x, x, x, \dots)$. The image of K in $\mathbb{A}_K$ is the subring of *principal adeles*.

Example 21.4

For $K = \mathbb{Q}$, $A_\mathbb{Q}$ is the union of $\mathbb{R} \times \prod_{p \in S} \mathbb{Q} \times \prod_{p \notin S} \mathbb{Z}_p$ for S a finite set of primes. Equivalently, $A_\mathbb{Q} = \{a \in \prod_p \mathbb{Q}_p : ||a||_p \leq 1 \text{ for almost all } p\}$.

Proposition 21.5

$\mathbb{A}_K$ is locally compact and Hausdorff.

Thus, the additive group of $\mathbb{A}_K$ is a locally compact group, so it has a Haar measure μ which we normalize as follows:

- $\mu_\nu(\mathcal{O}_\nu) = 1$ for all non-archimedean ν
- $\mu_\nu(S) = \mu_\mathbb{R}(S)$ for $K_\nu \simeq \mathbb{R}$
- $\mu_\nu(S) = 2\mu_\mathbb{C}(S)$ for $K_\nu \simeq \mathbb{C}$.

A basis for the σ-algebra of measurable sets is $\prod_\nu B_\nu$ with $B_\nu \subseteq K_\nu$ measurable, $\mu_\nu(B_\nu) < \infty$, and $B_\nu = \mathcal{O}_\nu$ for almost all ν. Define

$$\mu\Big(\prod_\nu B_\nu\Big) \coloneqq \prod_\nu \mu_\nu(B_\nu).$$

The embedding $K \hookrightarrow \mathbb{A}_K$ makes $\mathbb{A}_K$ a K-vector space. For a finite extension L/K, the base change $\mathbb{A}_K \otimes_K L$ is an L-vector space. The topology on $\mathbb{A}_K \otimes L$ is the product topology on $[L : K]$ copies of $\mathbb{A}_K$.

Proposition 21.6

Let K be a global field and L/K be a finite separable extension. There is a natural isomorphism of topological rings $\mathbb{A}_L \simeq \mathbb{A}_K \otimes_K L$ such that the following diagram commutes.

$$\begin{tikzcd}
L \arrow[r, "\sim"] \arrow[d] & K \otimes_K L \arrow[d] \\
\mathbb{A}_L \arrow[r, "\sim"] & \mathbb{A}_K \otimes_K L
\end{tikzcd}$$

Corollary 21.7

If $[L : K] = n$, then $\mathbb{A}_L \simeq \mathbb{A}_K^{\oplus n}$ restricts to $L \simeq K^{\oplus n}$.

Theorem 21.8

For each global field L, the principal adeles $L \subseteq \mathbb{A}_L$ are a discrete cocompact subgroup of the additive group $\mathbb{A}_L$.

Proof. Let K be a rational subfield of L (so $K = \mathbb{Q}$ or $\mathbb{F}_q(t)$). By Corollary 21.7, if the theorem holds for K then it holds for L, so it suffices to consider $L = K$. Identify K with its image in $\mathbb{A}_K$.

For discreteness, because K is a topological group, it suffices to show that 0 is isolated. Consider the open set

$$U := \{a \in \mathbb{A}_K : ||a||_\infty < 1, ||a||_\nu \leq 1 \ \forall \nu < \infty\}.$$

The product formula says that $||a|| = 1$ for all nonzero $a \in K$, but not for any nonzero $a \in U$. Then $U \cap K = \{0\}$.

For cocompactness, we want $\mathbb{A}_K/K$ to be compact. Consider $W := \{a \in \mathbb{A}_K : ||a||_\nu \leq 1 \ \forall \nu\}$, and let $U_\infty := \{x \in K_\infty : ||x||_\infty \leq 1\}$. Then $W = U_\infty \times \prod_{\nu<\infty} \mathcal{O}_\nu \subseteq \mathbb{A}_{K,\{\infty\}} \subseteq \mathbb{A}_K$ is a product of compact sets and is compact. Thus, the image of W in $\mathbb{A}_K \to \mathbb{A}_K/K$ is compact, so we need the map to be surjective.

Letting $a = (a_\nu) \in \mathbb{A}_K$, we want to show $a = b + c$ for some $b \in W$ and $c \in K$. For $\nu < \infty$, let $x_\nu \in K$ be defined as

- $x_\nu := 0$ if $||a_\nu||_\nu \leq 1$ for almost all ν
- otherwise, choose $x_\nu \in K$ such that $||a_\nu - x_\nu|| \leq 1$ and $||x_\nu||_w \leq 1$ for $w \neq \nu$.

To show x_ν exists, first suppose $a_\nu = \frac{r}{s} \in K$ with $r, s \in \mathcal{O}_K$ coprime. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_\nu$ (DVR). Then $\mathfrak{p}^{\nu(s)}$ and $\mathfrak{p}^{-\nu(s)}(s)$ are coprime, so $r = r_1 + r_2$ with $r_1 \in \mathfrak{p}^{\nu(s)}, r_2 \in \mathfrak{p}^{-\nu(s)}(s)$. Consequently, $a_\nu = \frac{r_1}{s} + \frac{r_2}{s}$ with $\nu(\frac{r_1}{s}) \geq 0$ and $w(\frac{r_2}{s}) \geq 0$ for $w \neq \nu$. Letting $x_\nu = \frac{r_2}{s}$, then $||a_\nu - x_\nu||_\nu = \left|\left|\frac{r_1}{s}\right|\right|_\nu \leq 1$ and $||x_\nu||_w = \left|\left|\frac{r_2}{s}\right|\right|_w \leq 1$ for all $w \neq \nu$.

We can approximate any $a'_\nu \in K_\nu$ by such an $a_\nu \in K$ with $||a'_\nu - a_\nu||_\nu < \epsilon$ for all $\epsilon > 0$. Construct x_ν similarly, so $||a_\nu - x_\nu||_\nu \leq 1$ and $||a'_\nu + x_\nu||_\nu \leq 1 + \epsilon$ by the triangle inequality. Taking $\epsilon \to 0$ forces $||a'_\nu + x_\nu||_\nu \leq 1$ since $||\cdot||_\nu$ is non-archimedean hence discrete.

Now let $x := \sum_{\nu<\infty} x_\nu \in K$, and choose $x_\infty \in \mathcal{O}_K$ such that $||a_\infty - x - x_\infty||_\infty \leq 1$. For $a_\infty - x \in \mathbb{Q}_\infty = \mathbb{R}$, take $x_\infty \in \mathbb{Z}$ in $[a_\infty - x - 1, a_\infty - x + 1)$. For $a_\infty - x \in \mathbb{F}_q(t)_\infty = \mathbb{F}_q((t^{-1}))$, take $x_\infty \in \mathbb{F}_q[t]$ to be the polynomial of least degree such that $a_\infty - x - x_\infty \in \mathbb{F}_q[[t^{-1}]]$.

Finally, let $c := \sum_{\nu\leq\infty} x_\nu \in K \subseteq \mathbb{A}_K$ and $b := a - c$, so it remains to show $b \in W$. For $\nu < \infty$, we have $x_w \in \mathcal{O}_\nu$ for all $w \neq \nu$ and

$$||b||_\nu = ||a - c||_\nu = \left|\left|a - \sum_{w\leq\infty} x_w\right|\right|_\nu \leq \max(||a_\nu - x_\nu||_\nu, \max\{||x_w||_\nu : w \neq \nu\}) \leq 1$$

by the non-archimedean triangle inequality. For $\nu = \infty$, $||b_\infty|| = ||a_\infty - c||_\infty \leq 1$ by the choice of x_∞. □

Lemma 21.9 (Adelic Blichfeldt–Minkowski lemma)

Let K be a global field. There is a constant $B_K > 0$ such that for all $a \in \mathbb{A}_K$ with $||a|| > B_K$, there exists a nonzero principal adele $x \in K \subseteq \mathbb{A}_K$ with $||x||_\nu \leq ||a||_\nu$ for all $\nu \in M_K$.

Proof. Let $b_0 := \operatorname{covol}(K)$ which is the measure of any finite region for K in $\mathbb{A}_K$ under the normalized Haar measure μ on $\mathbb{A}_K$. By Theorem 21.8, K is cocompact so b_0 is finite. Let

$$b_1 := \mu\Big(\Big\{z \in \mathbb{A}_K : ||z||_\nu \leq 1 \ \forall \nu, ||z||_\nu \leq \frac{1}{4} \ \forall \nu \text{ archimedean}\Big\}\Big).$$

Note $b_1 \neq 0$ since only finitely many μ are archimedean. Let $B_K := \frac{b_0}{b_1} > 0$.

Suppose $a \in \mathbb{A}_K$ satisfies $||a|| > B_K$. Then $||a||_\nu \leq 1$ for almost all ν, so from $||a|| \neq 0$, $||a||_\nu = 1$ for almost all ν. Consider

$$T := \Big\{t \in \mathbb{A}_K : ||t||_\nu \leq ||a||_\nu \ \forall \nu, ||t||_\nu \leq \frac{1}{4}||a||_\nu \ \forall \nu \text{ archimedean}\Big\}.$$

Then $\mu(T) = b_1 \|a\| > b_0$ implies T is not contained in any fundamental region for K. There must exist distinct $t_1, t_2 \in T$ with the same image in $\mathbb{A}_K/K$ with $x = t_1 - t_2$ a nonzero element of $K \subseteq \mathbb{A}_K$. In all cases, we will have $\|x\|_\nu = \|t_1 - t_2\|_\nu \le \|a\|_\nu$:

$$\|t_1 - t_2\|_\nu \le \begin{cases} \max(\|t_1\|_\nu, \|t_2\|_\nu) & \text{if } \nu \text{ non-archimedean} \\ \|t_1\|_\nu + \|t_2\|_\nu & \text{if } \nu \text{ real} \\ (\|t_1 - t_2\|_\nu^{1/2})^2 & \text{if } \nu \text{ complex} \end{cases}.$$

□

Theorem 21.10 (Strong approximation)

Let K be a global field. $M_K = S \sqcup T \sqcup \{w\}$ be a partition with S finite. Fix $a_\nu \in K$ and $\epsilon_\nu \in \mathbb{R}_{>0}$ for $\nu \in S$. Then there exists $x \in K$ such that $\|x - a_\nu\|_\nu \le \epsilon_\nu$ for all $\nu \in S$ and $\|x\|_\nu \le 1$ for all $\nu \in T$.

Proof. As before, let $W := \{z \in \mathbb{A}_K : \|z\|_\nu \le 1 \ \forall \nu\}$ be a complete set of coset representatives for $K \subseteq \mathbb{A}_K$, so $\mathbb{A}_K = K + W$. Given a nonzero $u \in K$, we also have $\mathbb{A}_K = K + uW$: given any $c \in \mathbb{A}_K$, we can write $u^{-1}c \in \mathbb{A}_K$ as $u^{-1}c = a + b$ for $a \in K$, $b \in W$, so $c = ua + ub$ with $ua \in K$, $ub \in uW$. Now choose $z \in \mathbb{A}_K$ such that

- $0 < \|z\|_\nu \le \epsilon_\nu$ for $\nu \in S$
- $0 \le \|z\|_\nu \le 1$ for $\nu \in T$
- $\|z\|_w > B_K \prod_{\nu \ne w} \|z\|_\nu^{-1}$.

Then $\|z\| > B_K$ so there exists a nonzero $u \in K \subseteq \mathbb{A}_K$ with $\|u\|_\nu \le \|z\|_\nu$ for all ν. Define the adele $a \in \mathbb{A}_K$ with the given a_ν for $\nu \in S$ and $a_\nu = 0$ for all $\nu \notin S$. From $\mathbb{A}_K = K + uW$, we have $a = x + y$ for $x \in K$, $y \in uW$, so

$$\|x - a\|_\nu = \|y\|_\nu \le \|u\|_\nu \le \|z\|_\nu \le \begin{cases} \epsilon & \text{if } \nu \in S \\ 1 & \text{if } \nu \in T \end{cases}.$$

□

22 Idele group, profinite groups, infinite Galois theory

22.1 Idele group

Recall $\mathbb{A}_K = \prod_{\nu \in M_K} (K_\nu, \mathcal{O}_\nu)$ is the ring of adeles of a global field K. Consider the unit group

$$\mathbb{A}_K^\times = \{(a_\nu) \in \mathbb{A}_K : a_\nu \in K_\nu^\times \ \forall \nu \in M_K, a_\nu \in \mathcal{O}_\nu^\times \text{ for almost all } \nu \in M_K\},$$

where $\mathcal{O}_\nu^\times := K_\nu^\times \cap \mathcal{O}_\nu$ if ν is nonarchimedean, and $\mathcal{O}_\nu^\times = \mathbb{R}^\times$ or $\mathbb{C}^\times$ appropriately if ν is real or complex.

$\mathbb{A}_K^\times$ is not a topological group because the inverse map $a \mapsto a^{-1}$ is not continuous.

Example 22.1

Consider $K = \mathbb{Q}$ and for each prime p the adele $a(p) = (1, \dots, 1, p, 1, \dots) \in \mathbb{A}_\mathbb{Q}$. Every basic open set containing 1 looks like $U = \prod_{\nu \in S} U_\nu \times \prod_{\nu \notin S} \mathcal{O}_\nu$ where $S \subseteq M_K$ is finite. Since every U contains $a(p)$ for all sufficiently large p, $\lim_{p \to \infty} a(p) = 1$. However, $a(p)^{-1} \notin U$ as $p \to \infty$.

We give the group $R^\times$ the weakest topology to make it a topological group. Consider the embedding $\phi \colon R^\times \to R \times R$ by $r \mapsto (r, r^{-1})$. Declare $\phi \colon R^\times \to \phi(R^\times)$ to be a homeomorphism (i.e. throw in enough open sets to make it continuous). Then $r \mapsto r^{-1}$ is continuous because it equals $\pi_2 \circ \phi$.

The topology on $\mathbb{A}_K^\times$ now has basic open sets $U' = \prod_{\nu \in S} U_\nu \times \prod_{\nu \notin S} \mathcal{O}_\nu^\times$ where $U_\nu \subseteq K_\nu^\times$ and $S \subseteq M_K$ finite.

Definition 22.2 (idele group)**.** Let K be a global field. The *idele group* of K is the topological group

$$\mathbb{I}_K := \coprod_{\nu \in M_K} (K_\nu^\times, \mathcal{O}_\nu^\times).$$

The canonical embedding $K \hookrightarrow \mathbb{A}_K$ restricts to $K^\times \hookrightarrow \mathbb{I}_K$.

Definition 22.3 (idele class group)**.** The *idele class group* is $C_K := \mathbb{I}_K / K^\times$.

Remark 22.4. In the literature, the notation $\mathbb{I}_K$ and $\mathbb{A}_K^\times$ are used interchangeably, but we currently use $\mathbb{A}_K^\times$ to mean the unit group of $\mathbb{A}_K$.

There is a surjective homomorphism

$$\mathbb{I}_K \twoheadrightarrow \mathcal{I}_K, \quad a \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}(a)}$$

where $\mathfrak{p}$ ranges of primes of K and $\nu_\mathfrak{p}(a) := \nu_\mathfrak{p}(a_w)$ where w is the place associated to p. The composition $K^\times \hookrightarrow \mathbb{I}_K \twoheadrightarrow \mathcal{I}_K$ has image as the subgroup of principal fractional ideals $\mathcal{P}_K$. This induces a surjective homomorphism $C_K \twoheadrightarrow \mathrm{Cl}_K$, where $C_K = \mathbb{I}_K / K^\times$ and $\mathrm{Cl}_K = \mathcal{I}_K / \mathcal{P}_K$.

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r] \arrow[d, "x \mapsto (x)"] & \mathbb{I}_K \arrow[r] \arrow[d, two heads] & C_K \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & P_K \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

Proposition 22.5

$\mathbb{I}_K$ is a locally compact group.

Proof. Each $\mathcal{O}_\nu^\times = \{x \in K_\nu^\times : ||x||_\nu = 1\} \subseteq \mathcal{O}_\nu$ is compact. The $K_\nu^\times$ are locally compact, so $\mathbb{I}_K = \coprod (K_\nu^\times, \mathcal{O}_\nu^\times)$ is locally compact. $\mathbb{I}_K$ is Hausdorff because its topology is finer than $\mathbb{A}_K^\times \subseteq \mathbb{A}_K$ which is Hausdorff by Proposition 21.5. □

Proposition 22.6

$K^\times$ is a discrete subgroup of $\mathbb{I}_K$.

Proof (sketch). Consider $K^\times \hookrightarrow K \times K \subseteq \mathbb{A}_K \times \mathbb{A}_K$ and how a subset of a discrete subset is still discrete. □

Remark 22.7. K is cocompact in $\mathbb{A}_K$, but $K^\times$ is not cocompact in $\mathbb{I}_K$. Thus C_K is locally compact but not compact.

The norm map restricts to a map $||\cdot|| : \mathbb{I}_K \to \mathbb{R}_{>0}^\times$ by $a \mapsto ||a|| := \prod_\nu ||a||_\nu$.

Definition 22.8 (1-ideles)**.** The group of *1-ideles* is $\mathbb{I}_K^1 := \ker ||\cdot|| = \{a \in \mathbb{I}_K : ||a|| = 1\}$.

$\mathbb{I}_K^1$ contains $K^\times$ by the product formula.

Lemma 22.9

$\mathbb{I}_K^1$ has the same topology as a subspace of $\mathbb{I}_K$ and a subspace of $\mathbb{A}_K$.

Theorem 22.10 (Fujisaki)

$K^\times$ is a discrete cocompact subgroup of $\mathbb{I}_K^1$.

Proof. $K^\times$ is discrete in $\mathbb{I}_K$ by Proposition 22.6, hence in $\mathbb{I}_K^1$. It suffices to exhibit a compact $W \subseteq \mathbb{A}_K$ such that $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$. Choose $a \in \mathbb{A}_K$ with $||a|| > B_K$, and let

$$W \coloneqq L(a) = \{x \in \mathbb{A}_K : ||x||_\nu \leq ||a||_\nu \ \forall \nu \in M_K\}.$$

For $u \in \mathbb{I}_K^1$, we have $||u|| = 1 \implies \left|\left|\frac{a}{u}\right|\right| = ||a|| > B_K$, so there exists $z \in K^\times$ such that $||z||_\nu \leq \left|\left|\frac{a}{u}\right|\right|_\nu$ for all $\nu \in M_K$. Then $zu \in W$, so $u = z^{-1} \cdot zu$ and $W \cap \mathbb{I}_K^1$ surjects onto $\mathbb{I}_K^1/K^\times$. □

Definition 22.11 (norm-1 idele class group). The compact group $C_K^1 \coloneqq \mathbb{I}_K^1/K^\times$ is the *norm-1 idele class group*.

22.2 Profinite groups

Definition 22.12 (profinite group). A *profinite group* is a topological group that is the inverse limit of finite groups with the discrete topology.

Given any topological group G, we can take the *profinite completion*

$$\widehat{G} \coloneqq \varprojlim_N G/N \subseteq \prod_N G/N$$

over finite index open normal subgroups N. Given any group, we can give it the *profinite topology* by making every finite quotient discrete. In other words, take all cosets of finite index normal subgroups as a basis. There is a canonical map $G \to \widehat{G}$ from the inverse limit.

Example 22.13

- For G finite, $G \xrightarrow{\sim} \widehat{G}$ is an isomorphism.
- $\widehat{\mathbb{Z}} \coloneqq \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod_p \mathbb{Z}_p$. The map $\mathbb{Z} \to \widehat{\mathbb{Z}}$ is injective but not surjective.
- $\widehat{\mathbb{Q}} = \{0\}$ because $\mathbb{Q}$ has no finite index subgroups other than $\mathbb{Q}$. Thus $\mathbb{Q} \to \widehat{\mathbb{Q}}$ is surjective but not injective.

Lemma 22.14

G is dense in $\widehat{G}$.

Theorem 22.15

G is profinite if and only if it is totally disconnected and compact.

Corollary 22.16

G profinite implies $G \xrightarrow{\sim} \widehat{G}$ is an isomorphism.

22.3 Infinite Galois theory

Lemma 22.17

Let L/K be a Galois extension (not necessarily finite) and $G \coloneqq \mathrm{Gal}(L/K)$. Let F/K be a normal subextension of L/K. Then $H \coloneqq \mathrm{Gal}(L/F)$ is a normal subgroup of G with fixed field F, and there is an exact sequence

$$1 \to \mathrm{Gal}(L/F) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K) \to 1$$

where the first arrow is inclusion, and the second is restriction. Also,

$$G/H \simeq \mathrm{Gal}(F/K).$$

We have $H \lhd \mathrm{Gal}(L/K)$ with $L^H = F$. It may not be the case that $H = \mathrm{Gal}(L/F)$, as it could be smaller.

Definition 22.18 (Krull topology)**.** For L/K Galois and $G \coloneqq \mathrm{Gal}(L/K)$, the *Krull topology* on G has the basis consisting of cosets of $H_F \coloneqq \mathrm{Gal}(L/F)$ for F/K a finite subextension of L/K.

In the Krull topology, every open normal subgroup has finite index, but not every normal subgroup of finite index is open.

Theorem 22.19

Under the Krull topology, restriction maps induce a natural isomorphism of topological groups

$$\phi\colon \mathrm{Gal}(L/K) \to \varprojlim_F \mathrm{Gal}(F/K)$$

where F ranges over finite Galois extensions F/K. In particular, $\mathrm{Gal}(L/K)$ is profinite with open normal subgroups of the form $\mathrm{Gal}(L/F)$ for some *finite* normal F/K.

Theorem 22.20 (Fundamental theorem of Galois theory)

Let L/K be Galois and $G \coloneqq \mathrm{Gal}(L/K)$ with the Krull topology. The maps $F \mapsto \mathrm{Gal}(L/F)$ and $L^H \leftarrow\!\shortmid H$ define inclusion-reversing bijections

$$\{\text{subextensions } F/K \text{ of } L/K\} \longleftrightarrow \{H \leq G \text{ closed}\}.$$

Finite degree n subextensions correspond to index n subgroups, and normal subextensions F/K correspond to normal subgroups $H \lhd G$ such that $\mathrm{Gal}(F/K) \simeq G/H$.

Corollary 22.21

Let L/K be Galois and $H \leq \mathrm{Gal}(L/K)$ with fixed field F. Then $\overline{H} = \mathrm{Gal}(L/F)$.

23 Local class field theory

The goal of class field theory is to classify finite abelian extensions.

Definition 23.1 (maximal abelian, unramified extension)**.** Let K be a local field with separable closure K^{sep}. The *maximal abelian extension* of K is

$$K^{\mathrm{ab}} := \bigcup_{\substack{L \subseteq K^{\mathrm{sep}} \\ L/K \text{ finite abelian}}} L.$$

The *maximal unramified extension* of K is

$$K^{\mathrm{unr}} := \bigcup_{\substack{L \subseteq K^{\mathrm{sep}} \\ L/K \text{ finite unramified}}} L.$$

We have

$$K \subseteq K^{\mathrm{unr}} \subseteq K^{\mathrm{ab}} \subseteq K^{\mathrm{sep}}.$$

By Theorem 22.19,

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim_{L} \mathrm{Gal}(L/K)$$

where L ranges over finite extensions of K in K^{ab}. Then there is a bijection

$$\{\text{extensions of } K \text{ in } K^{\mathrm{ab}}\} \longleftrightarrow \{\text{closed subsets of } \mathrm{Gal}(K^{\mathrm{ab}}/K)\}$$

by $L \mapsto \mathrm{Gal}(K^{\mathrm{ab}}/L)$ and $(K^{\mathrm{ab}})^H \mapsfrom H$. Finite abelian L/K correspond to open subgroups of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Now assume K is a non-archimedean local field with ring of integers $\mathcal{O}_K$, maximal ideal $\mathfrak{p}$, and residue field $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$. If L/K is finite unramified with residue field $\mathbb{F}_{\mathfrak{q}} := \mathcal{O}_L/\mathfrak{q}$, then

$$\phi\colon \mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}}) = \langle x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}} \rangle.$$

In this case, the Artin map

$$\psi_{L/K}\colon \mathcal{I}_K \to \mathrm{Gal}(L/K)$$

sends $\mathfrak{p} \mapsto \mathrm{Frob}_{L/K}$, where we think of $\mathrm{Frob}_{L/K} = \phi^{-1}(x \mapsto x^{\#\mathbb{F}_{\mathfrak{p}}})$. Since $\mathcal{I}_K \simeq \mathbb{Z}$, this corresponds to the quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ where $n = [L : K]$. We can extend the Artin map to $K^\times$ via $\psi_{L/K}(x) := \psi_{L/K}((x))$. This sends every uniformizer π to $\mathrm{Frob}_{L/K}$.

23.1 Local Artin reciprocity

Theorem 23.2 (Local Artin reciprocity)

Let K be a local field. There exists a unique continuous homomorphism

$$\theta_K\colon K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

such that for each finite extension L/K in K^{ab}, it induces $\theta_{L/K}\colon K^\times \to \mathrm{Gal}(L/K)$ by composing θ_K with the restriction map $\mathrm{res}_{L/K}\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$. It also satisfies

- If K is non-archimedean and L/K is unramified, then $\theta_{L/K}(\pi) = \mathrm{Frob}_{L/K}$ for every uniformizer π of $\mathcal{O}_K$.
- $\theta_{L/K}$ is surjective with kernel $\mathrm{N}_{L/K}(L^\times)$, inducing $K^\times/\mathrm{N}_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$.

The natural map $\mathrm{res}_{L/K}\colon \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathrm{Gal}(L/K)$ can be viewed as

- The map induced by $\sigma \mapsto \sigma|_L$. Note $\sigma(L) = L$ because L/K is Galois.
- The quotient map $\mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)/\mathrm{Gal}(K^{\mathrm{ab}}/L)$.
- The projection from $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim_L \mathrm{Gal}(L/K)$.

23.2 Norm group

Definition 23.3 (norm group)**.** A *norm group* in $K^\times$ is any subgroup $\mathrm{N}(L^\times) := \mathrm{N}_{L/K}(L^\times) \subseteq K^\times$ with L/K a finite (abelian) extension.

Corollary 23.4

The map $L \to \mathrm{N}(L^\times)$ induces an inclusion-reversing bijection

$$\{\text{finite } L/K \text{ in } K^{\mathrm{ab}}\} \longleftrightarrow \{\text{norm groups in } K^\times\}$$

where

$$\mathrm{N}((L_1L_2)^\times) = \mathrm{N}(L_1^\times) \cap \mathrm{N}(L_2^\times), \quad \mathrm{N}((L_1 \cap L_2)^\times) = \mathrm{N}(L_1^\times)\,\mathrm{N}(L_2^\times).$$

In particular, every norm group has finite index in $K^\times$, and every subgroup of $K^\times$ containing a norm group is a norm group.

Norm groups $\mathrm{N}(L^\times)$ are open.

Theorem 23.5 (Local existence)

Let K be a local field and H a finite index open subgroup of $K^\times$. Then there exists a unique finite abelian extension L/K with $\mathrm{N}(L^\times) = H$.

Theorem 23.6 (Main theorem of local class field theory)

The local Artin homomorphism θ_K induces a canonical isomorphism $\widehat{\theta_K}\colon \widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of profinite groups.

Recall that $\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim_L \mathrm{Gal}(L/K)$ and $\widehat{K^\times} \simeq \varprojlim_L K^\times/\mathrm{N}(L^\times)$ for finite L/K in K^{ab}, using the existence theorem (Theorem 23.5).

Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_K$, so we have an isomorphism $K^\times \simeq \mathcal{O}_K^\times \times \mathbb{Z}$ by $x \mapsto (x/\mathfrak{p}^{\nu(x)}, \nu(x))$. Taking profinite completions, $\widehat{K^\times} \simeq \mathcal{O}_K^\times \times \widehat{\mathbb{Z}}$, so we have the exact sequences

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\sim"] & K^\times \arrow[r] \arrow[d, "\theta_K"] & \mathbb{Z} \arrow[r] \arrow[d, hook, "\phi"] & 0 \\
1 \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{unr}}) \arrow[r] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r] & \mathrm{Gal}(K^{\mathrm{unr}}/K) \arrow[r] & 1
\end{tikzcd}$$

The map ϕ is $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} \simeq \mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}}) \simeq \mathrm{Gal}(K^{\mathrm{unr}}/K)$.

Example 23.7

Take $K = \mathbb{Q}_p$ and $\pi = p$. The decomposition $K^{\mathrm{ab}} = K^{\mathrm{unr}} \cdot K_\pi$ is $\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_n \mathbb{Q}_p(\zeta_{p^n}) \cdot \bigcup_{m \perp p} \mathbb{Q}_p(\zeta_m)$.

24 Global class field theory

Recall the ring of adeles

$$\mathbb{A}_K \coloneqq \prod_\nu (K_\nu, \mathcal{O}_\nu) = \{(a_\nu \in \prod_\nu K_\nu : a_\nu \in \mathcal{O}_\nu \text{ for almost all } \nu\}$$

and the idele group

$$\mathbb{I}_K \coloneqq \prod_\nu (K_\nu^\times, \mathcal{O}_\nu^\times) = \{(a_\nu \in \prod_\nu K_\nu^\times : a_\nu \in \mathcal{O}_\nu^\times \text{ for almost all } \nu\}.$$

24.1 Idele norm

There is a surjection $\varphi\colon \mathbb{I}_K \to \mathcal{I}_K$ by $a \mapsto \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(a)}$ for $\mathfrak{p}$ finite.

$$\begin{tikzcd}
1 \arrow[r] & K^\times \arrow[r] \arrow[d, "x\mapsto(x)"] & \mathbb{I}_K \arrow[r] \arrow[d, "\varphi"] & C_K \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & P_K \arrow[r] & \mathcal{I}_K \arrow[r] & \mathrm{Cl}_K \arrow[r] & 1
\end{tikzcd}$$

Definition 24.1 (idele norm). Let L/K be a finite separable extension of global fields. The idele norm $\mathrm{N}_{L/K}\colon \mathbb{I}_L \to \mathbb{I}_K$ is defined by sending $\mathrm{N}_{L/K}(b_w) = (a_\nu)$ where $a_\nu \coloneqq \prod_{w|\nu} \mathrm{N}_{L_w/K_\nu}(b_w)$.

The idele norm $\mathrm{N}_{L/K}\colon \mathbb{I}_L \to \mathbb{I}_K$ is compatible with the field norm $\mathrm{N}_{L/K}\colon L^\times \to K^\times$ on the subgroup of principal ideles $L^\times \subseteq \mathbb{I}_L$.

$$\begin{tikzcd}
L^\times \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathbb{I}_L \arrow[r] \arrow[d, "\mathrm{N}_{L/K}"] & \mathcal{I}_L \arrow[d, "\mathrm{N}_{L/K}"] \\
K^\times \arrow[r] & \mathbb{I}_K \arrow[r] & \mathcal{I}_K
\end{tikzcd}$$

Take quotients to get the following.

$$\begin{tikzcd}
C_L \arrow[r, two heads] \arrow[d, "\mathrm{N}_{L/K}"] & \mathrm{Cl}_L \arrow[d, "\mathrm{N}_{L/K}"] \\
C_K \arrow[r, two heads] & \mathrm{Cl}_K
\end{tikzcd}$$

24.2 Artin homomorphism

Let K be a global field, $\nu \in M_K$, and $\theta_{K_\nu}\colon K_\nu^\times \to \mathrm{Gal}(K_\nu^{\mathrm{ab}}/K_\nu)$ be the local Artin homomorphism. For each finite abelian L/K and each $w \in M_L$, we compose θ_{K_ν} with $\mathrm{Gal}(K_\nu^{\mathrm{ab}}/K_\nu) \to \mathrm{Gal}(L_w/K_\nu)$ to get

$$\theta_{L_w/K_\nu}\colon K_\nu^\times \to \mathrm{Gal}(L_w/K_\nu)$$

with kernel $\mathrm{N}_{L_w/K_w}(L_w^\times)$. Note that every finite separable extension of K_ν is L_w for some $w \mid \nu$ in L by Corollary 12.19.

We define an embedding

$$\begin{aligned} \varphi_w\colon \mathrm{Gal}(L_w/K_\nu) &\hookrightarrow \mathrm{Gal}(L/K) \\ \sigma &\mapsto \sigma|_L \end{aligned}$$

If ν is a finite place and $\mathfrak{q}$ is the prime of L corresponding to $w \mid \nu$, then $\varphi_w(\operatorname{Gal}(L_w/K_\nu)) = D_\mathfrak{q} \subseteq \operatorname{Gal}(L/K)$. The composition $\varphi_w \circ \theta_{L_w/K_\nu}$ defines a map $K^\times \to \operatorname{Gal}(L/K)$ that is independent of the choice of $w \mid \nu$. This is because $\varphi_w(\theta_{L_w/K_\nu}(\pi_\nu)) = \operatorname{Frob}_\nu$ for every π_ν, and the π_ν generate $K_\nu^\times$. Define

$$\begin{aligned}\iota_\nu \colon K_\nu^\times &\hookrightarrow \mathbb{I}_K\\ \alpha &\mapsto (1, \dots, 1, \alpha, 1, \dots)\end{aligned}$$

which is compatible with the idele norm: if w extends ν, then

$$\begin{tikzcd} L_w^\times \arrow[r, "\mathrm{N}_{L_w/K_\nu}"] \arrow[d, hook, "\iota_w"] & K_\nu^\times \arrow[d, hook, "\iota_\nu"] \\ \mathbb{I}_L \arrow[r, "\mathrm{N}_{L/K}"] & \mathbb{I}_K \end{tikzcd}$$

commutes.

Let L/K be a finite abelian extension (i.e. $\operatorname{Gal}(L/K)$ is abelian), and pick $\nu \in M_K$ and $w \mid \nu$. Then define

$$\begin{aligned}\theta_{L/K} \colon \mathbb{I}_K &\to \operatorname{Gal}(L/K)\\ (a_\nu) &\mapsto \prod_\nu \varphi_w(\theta_{L_w/K_\nu}(a_\nu)).\end{aligned}$$

Almost all $a_\nu \in \mathcal{O}_\nu^\times$ and almost all ν are unramified in L, which implies $\varphi_w(\theta_{L_w/K_\nu}(a_\nu)) = \operatorname{Frob}_\nu^{\nu(a_\nu)} = 1$ for almost all ν. $\theta_{L/K}$ is well defined, a group homomorphism, and continuous. If $L_1 \subseteq L_2$ are two finite abelian extensions of K, then $\theta_{L_1/K}(a) = \theta_{L_2/K}(a)|_{L_1}$ for all $a \in \mathbb{I}_K$. The $\theta_{L/K}$ form a compatible system of homomorphisms from $\mathbb{I}_K$ to $\varprojlim_L \operatorname{Gal}(L/K) \simeq \operatorname{Gal}(K^{\mathrm{ab}}/K)$. By the universal property for profinite completions, they determine a unique homomorphism θ_K.

Definition 24.2 (global Artin homomorphism). The *global Artin homomorphism* is the continuous homomorphism $\theta_K \colon \mathbb{I}_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$.

Proposition 24.3

Let K be a global field. Then θ_K is the unique continuous homomorphism $\mathbb{I}_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ such that for every finite abelian L/K and $w \mid \nu \in L$, the following diagram commutes.

$$\begin{tikzcd} K_\nu^\times \arrow[r, "\theta_{L_w/K_\nu}"] \arrow[d, hook, "\iota_\nu"] & \operatorname{Gal}(L_w/K_\nu) \arrow[d, hook, "\varphi_w"] \\ \mathbb{I}_K \arrow[r, "\theta_{L/K}"] & \operatorname{Gal}(L/K) \end{tikzcd}$$

24.3 Main theorems of global class field theory

Theorem 24.4 (Global Artin reciprocity)

Let K be a global field. Then $K^\times \subseteq \ker \theta_K$, and we have a continuous homomorphism

$$\theta_K \colon C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$$

with the property that for every finite abelian L/K, $\theta_{L/K} \colon C_K \to \operatorname{Gal}(L/K)$ obtained by composing θ_K with $\operatorname{res}_{L/K} \colon \operatorname{Gal}(K^{\mathrm{ab}}/K) \to \operatorname{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}(C_L)$, inducing an isomorphism $C_K/\mathrm{N}_{L/K}(C_L) \simeq \operatorname{Gal}(L/K)$.

Instead of $K^\times$ in the local case, we now have C_K.

Theorem 24.5 (Global existence)

Let K be a global field. For every finite index open subgroup $H \subseteq C_K$, there exists a unique finite abelian extension L/K in K^{ab} with $\mathrm{N}_{L/K}(C_L) = H$.

Theorem 24.6 (Main theorem of global class field theory)

The global Artin homomorphism θ_K induces a canonical isomorphism $\widehat{\theta_K}\colon \widehat{C_K} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of profinite groups. There is an inclusion-reversing bijection

$$\{\text{finite index open subgroups } H \subseteq C_K\} \longleftrightarrow \{\text{finite abelian } L/K \text{ in } K^{\mathrm{ab}}\}$$

by $H \mapsto (K^{\mathrm{ab}})^{\theta_K(H)}$ and $\mathrm{N}_{L/K}(C_L) \mapsfrom L$.

Theorem 24.7 (Functoriality)

Let K be a global field and L/K a finite separable extension. The following commutes.

$$\begin{tikzcd}
C_L \arrow[r, "\theta_L"] \arrow[d, "\mathrm{N}_{L/K}"] & \mathrm{Gal}(L^{\mathrm{ab}}/L) \arrow[d, "res"] \\
C_K \arrow[r, "\theta_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

24.4 Chebotarev density theorem

Theorem 24.8 (Chebotarev density theorem)

Let L/K be a finite Galois extension with Galois group G. Let $C \subseteq G$ be stable under conjugation. Let S be the set of primes of K that are unramified in L with $\mathrm{Frob}_{\mathfrak{p}} \subseteq C$. Then $d(S) = \frac{\#C}{\#G}$.

Corollary 24.9 (abelian case)

Let L/K be a finite abelian extension with Galois group G. Then for all $\sigma \in G$, the Dirichlet density of the set S of primes $\mathfrak{p}$ of K unramified in L for which $\mathrm{Frob}_{\mathfrak{p}} = \{\sigma\}$ is $\frac{1}{\#G}$.

It is straightforward to prove the Chebotarev density theorem from the abelian case.