Number Theory: Notes on Xie Junyi's classes

BAO

Date: December 24, 2025

Abstract

These are the notes on Prof. Xie Junyi's classes.

Contents

1 Algebraic Integers

1.1 Note on 20250922

COROLLARY 1.1. *Let L be a number field. Then $\mathcal{O}_L$ is the biggest subring of L which is finitely generated as a $\mathbb{Z}$-module.*

Proof. $\mathcal{O}_L$ is f. g. $\mathbb{Z}$-module. Let B be a subring of L which is f. g. as a $\mathbb{Z}$-module. Then for any $b \in B$, b is integral over $\mathbb{Z}$, so $B \subset \mathcal{O}_L$. ■

EXAMPLE 1.2. If $\operatorname{char} p > 0$, there exists DVR, which is not Japanese, i.e. there exists A DVR, L finite field extension of $\operatorname{Frac}(A)$, such that the integral closure B of A in L is not a finitely generated A-module.

For example, let

$$k = \mathbb{F}_p(t_0, t_1, \ldots), \quad K = \mathbb{F}_p(t_0^{1/p}, t_1^{1/p}, \ldots),$$

and

$$A \coloneqq \Big\{h \in K[[x]] \mid h = \sum_{i \geq 0} a_i x^i,\ a_i \in K,\ k(a_0, a_1, \ldots) \text{ is a finite extension over } L\Big\}.$$

Then A is a DVR. Note

$$A^\times = \{a_0 + \cdots \mid a_0 \neq 0\},$$

so

$$f \coloneqq \sum_{i \geq 0} t_i^{1/p} x^i \notin A.$$

Let $R \coloneqq A[f]$. Only need to show the integral closure B of R in $L \coloneqq \operatorname{Frac}(R)$ is not f. g. over R.

For all $n \geq 0$, set

$$h_n \coloneqq \sum_{i \geq n} t_i^{1/p} x^{i-n} = \frac{1}{x^n}\Big(f - \sum_{i<n} t_i^{1/p} x^i\Big) \in L.$$

Moreover,

$$h_n^p = \sum_{i \geq n} t_i x^{p(i-n)} \in A \Longrightarrow h_n \in B, \quad \forall\, n.$$

Hence, $f \in A + x^n B$ for all n.

Assume B is f. g. over A. Take

$$M \coloneqq B/A, \quad N \coloneqq \bigcap_{n \geq 1} x^n M,$$

which are f. g. A-modules, and $xN = N$. By Nakayama's lemma ($\mathfrak{m} = (x)$), $N = 0$. So $f \in A$, which is a contradiction. Q.E.D.

Let $C = \sum A\beta_i \subset B$ with β_i a basis for L/K.

Define

$$\begin{aligned} C^* &:= \{\beta \in L \mid \operatorname{Tr}(\beta \cdot \gamma) \in A,\ \forall r \in C\} \\ &= \{\beta \in L \mid \operatorname{Tr}(\beta \cdot \beta_i) \in A\ i = 1, \ldots, m\} \\ &= \sum A\beta_i', \end{aligned}$$

where $\{\beta_i'\}$ is the dual basis of β_i. We have

$$C = \sum A\beta_i \subset B \subset \sum A\beta_i' = C^*.$$

Then, <u>how to fine C^*?</u>

Assume $L = \mathbb{Q}[\beta]$ with $\beta \in \mathcal{O}_L$. Let $f(x)$ be the minimal polynomial of β with $\deg f = m$. Let

$$C = \mathbb{Z}[\beta] = \bigoplus_{i=0}^{m-1} \beta^i.$$

Want to find C^*.

Lemma 1.3 (Euler).

$$\operatorname{Tr}\left(\beta^i / f'(\beta)\right) = \begin{cases} 0, & 0 \le i \le m-2, \\ 1, & i = m-1. \end{cases}$$

Proof. Let $\beta_1 = \beta, \ldots, \beta_m$ be the roots of f. Then

$$\operatorname{Tr}\left(\beta^i / f'(\beta)\right) = \sum_{j=1}^{m} \frac{\beta_j^i}{\prod_{k \ne j}(\beta_j - \beta_k)}.$$

Consider

$$D_j(x) := \prod_{k \ne j} (x - \beta_j) \in \overline{\mathbb{Q}}[x],$$

$\deg D_j = m - 1$, and

$$\frac{D_j(x)}{D_j(\beta_j)} = \begin{cases} 1, & x = \beta_j, \\ 0, & x = \beta_k,\ k \ne j. \end{cases}$$

So any polynomial $P \in \overline{\mathbb{Q}}[x]$ of deg $\le m-1$, we have

$$P(x) = \sum_{j=1}^{m} \frac{D_j(x)}{D_j(\beta_j)} P(\beta_j),$$

so

$$x^l = \sum_{j=1}^{m} \frac{D_j(x)}{D_j(\beta_j)} \cdot \beta_j^l, \quad l = 0, \ldots, m-1.$$

Compare the coefficients of x^{n-1}. We get

$$\sum_{j=1}^{m} \frac{\beta_j^l}{D_j(\beta_j)} = \begin{cases} 0, & l < m-1, \\ 1, & l = m-1. \end{cases}$$

∎

As

$$\mathbb{Z}[\beta] = \bigoplus_{i=0}^{m-1} \mathbb{Z}\beta^i,$$

Lemma $\implies$

$$\operatorname{Tr}\left(\beta^l/f'(\beta)\right) \in A, \quad \forall\, l \geq 0.$$

Moreover,

$$\det\left(\operatorname{Tr}\left(\beta^i \cdot \frac{\beta^j}{f'(\beta)}\right)_{0\leq i,j\leq m-1}\right) = (-1)^m,$$

which is a unit in $\mathbb{Z}$. Hence,

$$\left\{\frac{\beta^i}{f'(\beta)} \mid i = 0, \ldots, m-1\right\}$$

is a basis of C^* $\implies$

$$C^* = \left(f'(\beta)\right)^{-1} A[\beta].$$

1.1.1 Finding the ring of integers

Let K be a field of char 0.

Proposition 1.4. *Let $L = K[\beta]$ for some β, and $f(x)$ the minimal polynomial of β over K with* $\deg f = m$*. Suppose $\beta_1, \ldots, \beta_m$ are the roots of f in $\overline{K}$. Then the discriminant of f:*

$$D(1, \beta, \ldots, \beta^{m-1}) = \prod_{1\leq i<j\leq m} (\beta_i - \beta_j)^2 = (-1)^{\frac{m(m-1)}{2}} \operatorname{Nm}_{L/K}\left(f'(\beta)\right).$$

Proof.

$$\begin{aligned} D(1, \beta, \ldots, \beta^{m-1}) = \det\left(\sigma_i(\beta^j)\right)^2 &= \det(\beta_i^j)^2 \\ &= \prod_{1\leq i<j\leq m} (\beta_i - \beta_j)^2 \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_i \prod_{j\neq i} (\beta_i - \beta_j) \\ &= (-1)^{\frac{m(m-1)}{2}} \prod_i f'(\beta_i) \\ &= (-1)^{\frac{m(m-1)}{2}} \operatorname{Nm}_{L/K}\left(f'(\beta)\right). \end{aligned}$$

∎

Remark 1.5. *$D(1, \beta, \ldots, \beta^{m-1}) = 0$ iff f has multiple roots.*

Let L be a number field.

Proposition 1.6. *Let $\beta_1, \ldots, \beta_m$ be a basis of $L/\mathbb{Q}$, and $d \coloneqq D(\beta_1, \ldots, \beta_m) \in \mathbb{Z}$. Then*

$$\mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m \subset \mathcal{O}_L \subset \mathbb{Z}\frac{\beta_1}{d} + \cdots + \mathbb{Z}\frac{\beta_m}{d}.$$

Proof. For $\beta \in \mathcal{O}_L$, write

$$\beta = \sum x_i \beta_i, \quad x_i \in \mathbb{Q}.$$

Let $\sigma_1, \ldots, \sigma_m$ be the embeddings of L into $\overline{\mathbb{Q}}$. Then

$$\sigma_j(\beta) = \sum_i x_i \sigma_j(\beta_i), \quad j = 1, \ldots, m.$$

Solve x_i, we get

$$x_i = \frac{A_i}{\det\big(\sigma_j(\beta_k)\big)} \in \frac{\mathcal{O}_L}{\det\big(\sigma_j(\beta_k)\big)}, \quad i = 1, \ldots, m.$$

Note $\det(\sigma_j(\beta_k))^2 = d$. Hence, every $dx_i \in \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$. So $\beta \in \mathbb{Z}\frac{\beta_1}{d} + \cdots + \mathbb{Z}\frac{\beta_m}{d}$. ∎

Now write $L = \mathbb{Q}[\alpha]$ with $\alpha \in \mathcal{O}_L$. Compute $d = D(1, \alpha, \ldots, \alpha^{m-1})$. Then

$$\mathbb{Z}[\alpha] \subset \mathcal{O}_L d^{-1}\mathbb{Z}[\alpha].$$

Note

$$\Big(d^{-1}\mathbb{Z}[\alpha] : \mathbb{Z}[\alpha]\Big) = d^m.$$

For every coset $\beta + \mathbb{Z}[\alpha]$ of $d^{-1}\mathbb{Z}[\alpha]$ is in $\mathcal{O}_L$ iff

$$(\beta + \mathbb{Z}[\alpha]) \cap \mathcal{O}_L \neq \varnothing.$$

Let $\beta_1, \ldots, \beta_m \in d^{-1}\mathbb{Z}[\alpha]$ represent all the cosets of $d^{-1}\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$. Test any β_i whether $\beta_i \in \mathcal{O}_L$ or not.

1.2 Note on 20250924

1.2.1 General strategy

Write $K = \mathbb{Q}[\alpha]$ with $\alpha \in \mathcal{O}_K$. Compute $D(1, \alpha, \ldots, \alpha^{m-1})$. If it is square-free, then $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is automatically an integral basis as

$$D(1, \alpha, \ldots, \alpha^{m-1}) = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})(\mathcal{O}_K : \mathbb{Z}[\alpha])^2.$$

If it is not square-free, $\{1, \alpha, \ldots, \alpha^{m-1}\}\{1, \alpha, \ldots, \alpha^{m-1}\}$ may still be an integral basis. Sometimes we can show this by Stickelberger's thm or look at how prime ramify. If $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is not an integral basis, one has to look for algebraic integers outside $\mathbb{Z}[\alpha]$.

PROPOSITION 1.7. *Let K be a number field.*

(a) The sign of $\operatorname{disc}(K/\mathbb{Q})$ is $(-1)^s$, where $2s$ is the number for homomophisms $K \hookrightarrow \mathbb{C}$ whose image is not in $\mathbb{R}$;

(b) (Stickelberger's thm) $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv 0$ *or* $1 \mod 4$.

Proof. (a) Let $K = \mathbb{Q}[\alpha]$ and $\alpha_1, \ldots, \alpha_r$ be the real conjugates of α, and $\alpha_{r+1}, \overline{\alpha_{r+1}}, \ldots, \alpha_{r+s}, \overline{\alpha_{r+s}}$ be the complex conjugates of α. Then

$$\operatorname{sign}\Big(D(1, \alpha, \ldots, \alpha^{m-1})\Big) = \operatorname{sign}\Big(\prod_{1\le i\le s}(\alpha_{r+i} - \overline{\alpha_{r+i}})\Big)^2 = (-1)^s.$$

(b) Let $\alpha_1, \ldots, \alpha_m$ be an integral basis of $\mathcal{O}_K$. Let $\sigma_1, \ldots, \sigma_m$ be the embeddings of $K \hookrightarrow \overline{\mathbb{Q}}$. Then

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = \det(\sigma_i\alpha_j)^2.$$

Let

$$P = \sum_{\substack{i_1\cdots i_m \\ \text{even permutation}}} (\sigma_{i_1}\alpha_1)\cdots(\sigma_{i_m}\alpha_m),$$

$$N = \sum_{\substack{i_1\cdots i_m \\ \text{odd permutation}}} (\sigma_{i_1}\alpha_1)\cdots(\sigma_{i_m}\alpha_m).$$

Then

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = P^2 - N^2 = (P+N)^2 - 4PN,$$

where $P + N$ and PN are integral over $\mathbb{Z}$.

For any $\tau \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, either $\tau P = P, \tau N = N$ or $\tau P = N, \tau N = P$. So

$$\tau(P+N) = P+N, \quad \tau(PN) = PN,$$

which implies $P + N, PN \in \mathbb{Q} \implies \in \mathbb{Z}$. Then

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) \equiv (P+N)^2 \equiv 0 \text{ or } 1 \mod 4.$$

■

Example 1.8. Consider $K = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$ square-free.

Case $m \equiv 2, 3 \mod 4$. Then

$$D(1, \sqrt{m}) = \operatorname{disc}(x^2 - m) = 4m.$$

By Stickelberger's thm,

$$\operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) = 4m,$$

hence $\{1, \sqrt{m}\}$ is an integral basis.

Case $m \equiv 1 \mod 4$. The element $\dfrac{1+\sqrt{m}}{2}$ is integral, and

$$D\Big(1, \frac{1+\sqrt{m}}{2}\Big) = m.$$

Then $\left\{1, \dfrac{1+\sqrt{m}}{2}\right\}$ is an integral basis.

2 Dedekind Domains and Factorization

- Definition of Dedekind domains;
- Ideals in Dedekind domains factor uniquely into products of prime ideals;
- Rings of integers in number fields are Dedekind domains.

2.1 Note on 20250924

2.1.1 Discrete valuation rings

Definition 2.1. A ring A is called a discrete valuation ring (DVR) if it is a principal ideal domain which has the following equivalent conditions:

(a) A has exactly one non-zero prime ideal $\mathfrak{m}$;

(b) up to a unit, there exists a unique prime element $\pi \in A$;

(c) A is a local ring, and is not a field.

Proof. (a) $\Leftrightarrow$ (b), (c) $\Rightarrow$ (a).

(c) $\Rightarrow$ (a). There exists (π) nonzero maximal ideal $\implies$ $(\pi) \neq (0)$. If $(\pi') \subset (\pi)$ is another nonzero prime ideal, then $\pi' = \pi \cdot h$. If $h \in (\pi')$, then $h = \pi' \cdot g$, then $\pi' = \pi' \pi g$, $\implies$ π is a unit, which is a contradiction. So $h \notin (\pi')$, hence $(\pi') = (\pi)$. ■

Example 2.2.

$$\mathbb{Z}_{(p)} \coloneqq \left\{ \frac{m}{n} \in \mathbb{Q} \mid n \text{ not divisible by } p \right\}$$

is a DVR with the unique maximal ideal $\mathfrak{m} = (p)$.

Recall that any A-module M and $m \in M$, the annihilator of m is defined as

$$\operatorname{Ann}(m) \coloneqq \{a \in A \mid am = 0\},$$

which is an ideal of A, and proper if $m \neq 0$.

Proposition 2.3. *An integral domain A is a DVR iff*

(a) A is Noetherian,

(b) A is integrally closed,

(c) A has exactly one non-zero prime ideal.

Proof. A is a DVR $\implies$ (a), (b), (c).

(a)+(b)+(c) $\implies$ A is a DVR. (c) $\implies$ A is a local ring, not a field. Only need to show A is a PID. Choose $c \in A$ with $c \neq 0$, not a unit. Consider $M \coloneqq A/(c)$. Pick $m \in M \setminus \{0\}$ s.t. $\mathfrak{p} \coloneqq \operatorname{Ann}(m)$ is maximal. Such m exists as M is a f. g. A-module, and A is Noetherian. Write $m = b + (c)$. Then

$$\mathfrak{p} = \{a \in A \colon c \mid ab\}.$$

Claim: $\mathfrak{p}$ is a prime ideal.

Otherwise, $\exists\, x, y \notin \mathfrak{p}$, s.t. $xy \in \mathfrak{p}$. Then $yb + (c) \in M \setminus \{0\}$ as $y \notin \mathfrak{p}$. But,

$$\mathrm{Ann}(yb + (c)) \supset \mathrm{Ann}(ym) \supsetneq \mathrm{Ann}(m),$$

where the last inequality holds as $x \in \mathrm{Ann}(ym) \setminus \mathrm{Ann}(m)$. This contradicts the maximality of $\mathfrak{p}$.

As $m \neq 0$ $c \nmid b$, i.e. $\frac{b}{c} \notin A$.

Claim: $\frac{c}{b} \in A$ and $\mathfrak{p} = \left(\frac{c}{b}\right)$.

$\mathfrak{p} \cdot b \subset (c) \implies \frac{b}{c}\mathfrak{p} \subset A$ is an ideal. If $\frac{b}{c}\mathfrak{p} \subset \mathfrak{p}$, then $\frac{b}{c}$ is integral over A, hence in A as A is integrally closed, which is a contradiction. So $\frac{b}{c}\mathfrak{p} = A$, i.e. $\mathfrak{p} = \left(\frac{c}{b}\right)$.

Let $\pi \coloneqq \frac{c}{b}$. Then $\mathfrak{p} = (\pi)$ is the unique nonzero prime ideal of A. Let $\mathfrak{a}$ be a proper of A. Consider

$$\mathfrak{a} \subset \mathfrak{a}\pi^{-1} \subset \mathfrak{a}\pi^{-2} \subset \cdots.$$

If $\mathfrak{a}\pi^{-r} = \mathfrak{a}\pi^{-r-1}$ for some $r \geq 0$, then $\pi^{-1}(\mathfrak{a}\pi^{-r}) = \mathfrak{a}\pi^{-r} \implies \pi^{-1} \in A$, which is a contradiction. Thus, the sequence is strictly increasing. As A Noetherian, there exists maximal m s.t. $\mathfrak{a}^{-m} \subset A$, $\mathfrak{a}\pi^{-m-1} \not\subset A$. Then $\mathfrak{a}\pi^{-m} \not\subset \mathfrak{p} \implies \mathfrak{a} \cdot \pi^{-m} = A \implies \mathfrak{a} = (\pi^m)$. ■

2.1.2 Dedekind domains

Definition 2.4. A <u>Dedekind domain</u> is a an integral domian A s.t.

(a) A is Noetherian,

(b) A is integrally closed,

(c) A not a field and every nonzero prime ideal $\mathfrak{p}$ is maximal.

Remark 2.5. *Proposition 2.3 $\implies$ A local domain is a Dedekind domain iff it is a DVR.*

Proposition 2.6. *Let A be a domain, and S a multiplicative subset of A.*

(a) If A is Noetherian, so is $S^{-1}A$;

(b) If A is integrally closed, so also is $S^{-1}A$.

Proof. Omit. ■

Proposition 2.7. *Let A be a Noetherian integral domain. Then A is a Dedekind domain iff for every nonzero prime ideal $\mathfrak{p}$ in A, the localization $A_{\mathfrak{p}}$ is a DVR.*

Proof. The "only if" part follows from the above Proposition.

For the "if" part: Only to show A is integrally closed. Let $x \in \mathrm{Frac}(A)$ be integral over A. Set

$$\mathfrak{a} \coloneqq \{a \in A \mid ax \in A\}.$$

If $\mathfrak{a} \neq A$, then there exists a nonzero prime ideal $\mathfrak{p}$ of A s.t. $\mathfrak{a} \subset \mathfrak{p}$. Since $A_{\mathfrak{p}}$ is integrally closed, $x \in A_{\mathfrak{p}}$. Hence, there exists $s \in A \setminus \mathfrak{p}$ s.t. $sx \in A \implies s \in \mathfrak{a} \implies s \in \mathfrak{p}$, which is a contradiction. Thus, $\mathfrak{a} = A \implies x \in A$. ■

2.2 Note on 20250929

2.2.1 Unique factorization of ideals

THEOREM 2.8. *Let A be a Dedekind domain. Then every nonzero ideal $\mathfrak{a}$ of A can be written uniquely (up to ordering) as a product of nonzero prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

where the $\mathfrak{p}_i$ are distinct nonzero prime ideals of A and $r_i \geq 1$.

LEMMA 2.9. *Let A be a Noetherian ring. Then any nonzero ideal $\mathfrak{a}$ in A contains a product of nonzero prime ideals.*

Proof. Suppose not, choose a maximal counterexample $\mathfrak{a}$. Then $\mathfrak{a}$ is not a prime ideal $\implies$ $\exists x, y \in \mathfrak{a}$ but $xy \in \mathfrak{a}$ $\implies$ both $(x) + \mathfrak{a}$ and $(y) + \mathfrak{a}$ strictly contain a $\implies$ each of them contains a product of prime ideals $\implies$ $\mathfrak{a} \supset \big((x) + \mathfrak{a}\big) \cdot \big((y) + \mathfrak{a}\big)$ contains a product of prime ideals, which is a contradiction. ■

LEMMA 2.10. *Let A be a ring, and $\mathfrak{a}, \mathfrak{b}$ be relatively prime ideals on A, i.e. $\mathfrak{a} + \mathfrak{b} = A$. Then for any $m, n \in \mathbb{N}$, $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are relatively prime.*

Proof. Let $a \in \mathfrak{a}$, $b \in \mathfrak{b}$, s.t. $a + b = 1$. Then for $r \geq m + n$,

$$1 = (a+b)^r = \sum_{i=0}^{r} \binom{r}{i} a^i b^{n-i} \in \mathfrak{a}^m + \mathfrak{b}^n.$$

■

LEMMA 2.11. *Let $\mathfrak{p}$ be a maximal ideal of an integral domain A, and $\mathfrak{q} = \mathfrak{p}A_{\mathfrak{p}}$ the maximal ideal of $A_{\mathfrak{p}}$. Then the map*

$$\mathfrak{a} + \mathfrak{p}^m \longmapsto \mathfrak{a} + \mathfrak{q}^m \colon A/\mathfrak{p}^m \longrightarrow A_{\mathfrak{p}}/\mathfrak{q}^m$$

is an isomorphism.

Proof. Injectivity.

Only need to show $\mathfrak{q} \cap A = \mathfrak{p}^m$. Clearly $\mathfrak{p}^m \subset \mathfrak{q}^m \cap A$. Let $a \in \mathfrak{q}^m \cap A$. As $a \in \mathfrak{q}^m$, there exists $s \in A \setminus \mathfrak{p}$ s.t. $as \in \mathfrak{p}^m$ $\implies$ s is invertible in the field $A/\mathfrak{p}$ $\implies$ $\exists t \in A$ s.t. $st = 1 - u$ for $u \in \mathfrak{p}$ $\implies$

$$st' := st(1 + u + \cdots + u^{m-1}) = 1 - u^m,$$

where $u^m \in \mathfrak{p}^m$. Hence, $a - au^m = ast' \in \mathfrak{p}^m \implies a \in \mathfrak{p}^m$.

Surjectivity.

Let $a/s \in A_{\mathfrak{p}}$ with $a \in A$, $s \in A \setminus \mathfrak{p}$. As $\mathfrak{p}$ maximal, $(s) + \mathfrak{p} = A \implies (s) + \mathfrak{p}^m = A$ by Lemma 2.10 $\implies$ $\exists b \in A$, $u \in \mathfrak{p}^m$ s.t. $sb + u = 1$ $\implies$

$$\frac{a}{s} = \frac{ab}{sb} = \frac{ab}{1-u} = ab + \frac{uab}{1-u}.$$

So $a/s + \mathfrak{q}^m = ab + \mathfrak{q}^m$. ■

Proof of Theorem 2.8. Now A is a Dedekind domain.

Existence: We prove that any ideal $\mathfrak{a}$ of A can be factored into a product of prime ideals.

By Lemma 2.9, there exists an ideal $\mathfrak{b} \subset A$ s.t.

$$\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \subset \mathfrak{a},$$

where $\mathfrak{p}_i$ are distinct prime ideals and each two of them are relatively prime. Hence, by Lemma 2.11,

$$A/\mathfrak{b} \simeq A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m},$$

where each $A_{\mathfrak{p}_i}$ is a DVR $\implies$ any ideal in $A_{\mathfrak{p}_i}/\mathfrak{q}_i^{r_i}$ takes form $\mathfrak{q}_i^{s_i}/\mathfrak{q}_i^{r_i}$, $0 \le s_i \le r_i$ $\implies$ $\mathfrak{a}/\mathfrak{b}$ corresponds to

$$\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_m^{r_m}.$$

$\implies$

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}}{\mathfrak{b}} \implies \mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}.$$

Uniqueness.

Suppose

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m}$$

(some s_i, t_j may be 0). Assume $s_i + t_i \ge 1$. Take

$$\mathfrak{b} = \mathfrak{p}_1^{s_1+t_1} \cdots \mathfrak{p}_m^{s_m+t_m}.$$

Consider

$$A/\mathfrak{b} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{s_1+t_1} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{s_m+t_m}.$$

$\implies$ $s_i = t_i$ for all i. ∎

Remark 2.12. $s_i > 0 \iff \mathfrak{a}A_{\mathfrak{p}_i} \neq A_{\mathfrak{p}_i} \iff \mathfrak{a} \subset \mathfrak{p}_i$.

Corollary 2.13. *Let $\mathfrak{a}, \mathfrak{b}$ be two ideals in A. Then $\mathfrak{a} \subset \mathfrak{b} \iff \mathfrak{a}A_{\mathfrak{p}} \subset \mathfrak{b}A_{\mathfrak{p}}$ for every nonzero prime ideal $\mathfrak{p}$ of A.*

In particular, $\mathfrak{a} = \mathfrak{b} \iff \mathfrak{a}A_{\mathfrak{p}} = \mathfrak{b}A_{\mathfrak{p}}$ for all $\mathfrak{p}$.

Proof. "$\Rightarrow$" is clear.

"$\Leftarrow$": Write $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ and $\mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$, where $\mathfrak{p}_i$ distinct, $s_i, r_i \ge 0$. For any i, $\mathfrak{a}A_{\mathfrak{p}_i} \subset \mathfrak{b}A_{\mathfrak{p}_i} \implies r_i \ge s_i \implies \mathfrak{a} \subset \mathfrak{b}$. ∎

Corollary 2.14. *Let A be an integral domain with only finitely many prime ideals. Then A is a Dedekind domain iff it is a principal ideal domain (PID).*

Proof. "$\Leftarrow$" is clear.

Assume A is a Dedekind domain. To show A is a PID, only need to show prime ideals are principle. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be these prime ideals. Choose $x_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. By Chinese Reminder Theorem, $\exists\, x$ s.t.

$$\begin{cases} x \equiv x_1 \mod \mathfrak{p}_1^2; \\ x \equiv 1 \mod \mathfrak{p}_i, \quad \forall\, i > 1. \end{cases}$$

Then $(x) = \mathfrak{p}_1$. ∎

Corollary 2.15. *Let $\mathfrak{a} \supset \mathfrak{b} \neq 0$ be two ideals of a Dedekind domain. Then $\mathfrak{a} = \mathfrak{b} + (c)$ for some $c \in A$.*

Proof. Write $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ and $\mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$, where $\mathfrak{p}_i$ distinct, $s_i, r_i \geq 0$. $\mathfrak{a} \supset \mathfrak{b} \implies s_i \leq r_i$, $\forall\, i$. For $i = 1, \ldots, m$, choose $x_i \in A$ s.t.

$$x_i \in \mathfrak{p}_i^{s_i} \setminus \mathfrak{p}_i^{s_i+1}.$$

By Chinese Reminder Theorem, $\exists\, c \in A$ s.t.

$$c \equiv x_i \mod \mathfrak{p}_i^{r_i}, \quad \forall\, i.$$

Then $\mathfrak{b} + (c) = \mathfrak{a}$. ■

Corollary 2.16. *Let $\mathfrak{a}$ be an ideal of a Dedekind domain. Let $a \in \mathfrak{a} \setminus \{0\}$. Then $\exists\, b \in \mathfrak{a}$ s.t. $\mathfrak{a} = (a, b)$.*

Proof. Take $\mathfrak{b} = (a) \subset \mathfrak{a}$ in the above corollary. ■

Corollary 2.17. *Let $\mathfrak{a}$ be a nonzero ideal in a Dedekind domain A. Then there exists a nonzero ideal $\mathfrak{a}^*$ in A s.t. $\mathfrak{a} \cdot \mathfrak{a}^*$ is principal.*

Moreover, $\mathfrak{a}^*$ can be chosen (but not both):

1. *to be relatively prime any particular ideal $\mathfrak{c}$; and*
2. *s.t. $\mathfrak{a} \cdot \mathfrak{a}^* = (a)$ with any given $a \in \mathfrak{a}$.*

Proof. Let $a \in \mathfrak{a}$, $a \neq 0$. $\mathfrak{a} \supset (a) \implies (a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ and $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$, $s_i \leq r_i$. Take

$$\mathfrak{a}^* = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_m^{r_m - s_m}.$$

Then $\mathfrak{a} \cdot \mathfrak{a}^* = (a)$.

Now show that $\mathfrak{a}^*$ can be chosen relatively prime to $\mathfrak{c}$. We have $\mathfrak{a} \supset \mathfrak{a}\mathfrak{c} \implies \exists\, a \in \mathfrak{a}$ s.t.

$$\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a).$$

Above argument $\implies \exists\, \mathfrak{a}^*$ s.t. $(a) = \mathfrak{a} \cdot \mathfrak{a}^* \implies$

$$(a) = \mathfrak{a} \cdot \mathfrak{a}^* = \mathfrak{a} \cdot \mathfrak{c} \cdot \mathfrak{a}^* + (a) \cdot \mathfrak{a}^* = (a) \cdot \mathfrak{c} + (a) \cdot \mathfrak{a}^*,$$

$\implies \exists\, c \in \mathfrak{c}$, $a' \in \mathfrak{a}^*$ s.t.

$$a = a \cdot c + a \cdot a' \implies (1) = \mathfrak{c} + \mathfrak{a}^*.$$

■

Remark 2.18. *We know PID $\implies$ UFD, but the inverse is not true in general. For example, $k[x, y]$ is UFD but the ideal (x, y) is not principle.*

Proposition 2.19. *Let A be a Dedekind domain. Then A UFD $\implies$ A PID.*

Proof. Only need to show every prime ideal $\mathfrak{p}$ of A is principle.

Let $a \in \mathfrak{p} \setminus \{0\}$. Then

$$a = u\pi_1^{r_1} \cdots \mathfrak{p}_n^{r_n},$$

for u unit, $r_i \geq 1$ and π_i irreducible. Thus, there exists $\pi_i \in \mathfrak{p}$. Hence, (π_i) prime $\implies$ maximal $\implies (\pi_i) = \mathfrak{p}$. ■

2.3 Note on 20251020

2.3.1 Ideal class group

3 Discrete valuations

3.1 Note on 20251022

Let K be a field.

Definition 3.1. A discrete valuation on K is a nonzero homomophism $v\colon K^\times \to \mathbb{Z}$ s.t.

$$v(a+b) \geq \min\{v(a), v(b)\}.$$

v is called normalized if $v(K^\times) = \mathbb{Z}$.

Indeed, if v is not normalized, write $v(K^\times) = m\mathbb{Z}$ for some $m \geq 1$. Then $\frac{1}{m}v\colon K^\times \to \mathbb{Z}$ is a normalized discrete valuation. We extend v to a map

$$v\colon K \to \mathbb{Z} \cup \{+\infty\}$$

sending 0 to $+\infty$.

Example 3.2.
- A = Dedekind domain, $\mathfrak{p} \subset A$ a prime ideal in A. $K := \mathrm{Frac}(A)$. $\forall\, c \in K^\times$, define
$$v_{\mathfrak{p}}(c) = \max\{n \in \mathbb{Z} \mid c \in \mathfrak{p}^n\}.$$
Then $v_{\mathfrak{p}}$ is a normalized discrete valuation on K.
- In particular, when A is PID, π a prime element of A, then for every $c \in K^\times$, write $c = \pi^m \frac{a}{b}$ with $a, b \in A$ not divisible by π. Define $v(c) = m$.
- e.g. $A = \mathbb{Z}$, $\pi = p$ prime number, $K = \mathbb{Q}$. Then for every $\frac{m}{n} \in \mathbb{Q}^\times$, write $\frac{m}{n} = p^r \frac{a}{b}$ with a, b not divisible by p. Define $v_p\left(\frac{m}{n}\right) = r$.
- e.g. $A = \mathbb{C}[x]$, $\mathfrak{p} = (t-a)$ for some $a \in \mathbb{C}$, $K = \mathbb{C}(x)$. Then for every $f(x)/g(x) \in K^\times$, write
$$\frac{f(x)}{g(x)} = (x-a)^r \frac{h(x)}{k(x)}$$
with $h(a), k(a) \neq 0$. Define $v_{\mathfrak{p}}\left(\frac{f(x)}{g(x)}\right) = r$.
- Let U be a connected open subset of $\mathbb{C}$, and
$$\mathcal{M}(U) := \{\text{meromorphic functions on } U\}.$$
Then $K = \mathcal{M}(U)$ is a field. For any $p \in U$, $\forall\, f \in K^\times$, $\mathrm{ord}_p(f) :=$ vanishing order of f at p, i.e. $f = c \cdot (z-p)^{\mathrm{ord}_p f} + o(z^{\mathrm{ord}_p f})$ with $c \neq 0$. Then ord_p is a discrete valuation on K.

Remark 3.3. *$\mathcal{O}(U) := \{$holomorphic functions on $U\}$, $\mathcal{M}(U) = \mathrm{Frac}(\mathcal{O}(U))$. However, $\mathcal{O}(U)$ is not a Dedekind domain in general.*

Fact: $\exists\, x_n \in U$, with $x_n \to x \in \partial U$. For any $m \geq 0$,

$$I_m := \{f \in \mathcal{O}(U) \mid f(x_n) = 0,\ \forall\, n \geq m\}.$$

Then I_m is increasing, and $\exists\, h \in \mathcal{O}(U)$ s.t. $h(x_n) = 0, \forall\, n, \implies I_m \subsetneq I_{m+1}, \forall\, m$. So $\mathcal{O}(U)$ is not Noetherian.

Lemma 3.4. *If $v(a) > v(b)$, then $v(a+b) = v(b)$.*

Proof. $v(a+b) \geq \min\{v(a), v(b)\} = v(b)$. Also,

$$v(b) = v(a+b-a) \geq \min\{v(a+b), v(a)\} = v(a+b).$$

■

Remark 3.5. *v induces a map*

$$\begin{aligned} K &\longrightarrow \mathbb{R} \\ a &\longmapsto e^{-v(a)} = |a|_v. \end{aligned}$$

We can check that $|\cdot|_v$ is a non-archimedean absolute value on K:

$$|a+b| \leq \max\{|a|, |b|\}.$$

Proposition 3.6. *Let v be a discrete valuation on a field K. Then*

$$A \coloneqq \{a \in K \mid v(a) \geq 0\}$$

is a DVR with the unique maximal ideal

$$\mathfrak{m} = \{a \in K \mid v(a) > 0\}.$$

$\exists\, \pi \in A$ s.t. $\mathfrak{m} = (\pi)$, and every $a \in K^\times$ can be written uniquely as $a = u\pi^{v(a)}$.

Proof. Easy. ■

Proposition 3.7. *Let A be a Dedekind domain. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct primes ideals of A, and $x_1, \ldots, x_m \in A$. Then for any $n \in \mathbb{Z}_+$, there exists $x \in A$ s.t.*

$$\operatorname{ord}_{\mathfrak{p}_i}(x - x_i) > n, \quad i = 1, \ldots, m.$$

Proof. The ideals $\mathfrak{p}_i^{n+1}$ are relatively prime two by two. By Chinese Reminder Theorem, $\exists\, x \in A$ s.t.

$$x \equiv x_i \mod \mathfrak{p}_i^{n+1}, \quad i = 1, \ldots, m.$$

$\implies \operatorname{ord}_{\mathfrak{p}_i}(x - x_i) > n$. ■

theorem 3.8. *Let A be a Dedekind domain, and $K = \operatorname{Frac}(A)$. Let L/K be a finite separable field extension, and B the integral closure of A in L. Then B is a Dedekind domain.*

Proof. We have proved that B is Noetherian as an A-mod. Any ideal of B is a finitely generated A-mod $\implies B$ is Noetherian. B is integrally closed by definition. We only need to show that every nonzero prime ideal $\mathfrak{q}$ of B is maximal.

Let $\beta \in \mathfrak{q} \setminus \{0\}$. As β is integral over A, we have

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A,$$

with minimal degree $n \implies a_n \neq 0$. Then $a_n \in \beta B \cap A \implies \mathfrak{q} \cap A \neq 0$. Let $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{p}$ is a nonzero prime ideal of $A \implies \mathfrak{p}$ is maximal $\implies A/\mathfrak{p}$ is a field. $B/\mathfrak{q}$ is an integral domain and algebraic over $A/\mathfrak{p} \implies B/\mathfrak{q}$ is a field $\implies \mathfrak{q}$ is maximal. ■

REMARK 3.9.
- *This Theorem shows $\mathcal{O}_K$ is a Dedekind domain for any number field K.*
- *In fact, we do not need the full strength of separability.*

LEMMA 3.10. *Any integral domain B containing a field k and algebraic over k is itself a field.*

Proof. Let $\beta \in B \setminus \{0\}$. As β is algebraic over k, $\dim_k k[\beta] < \infty$. Consider the k-linear map

$$\begin{aligned} L_\beta \colon k[\beta] &\longrightarrow k[\beta] \\ x &\longmapsto \beta x. \end{aligned}$$

L_β is injective $\implies$ surjective $\implies \exists\, \gamma \in k[\beta] \subset B$ s.t. $L_\beta(\gamma) = 1 \implies \beta\gamma = 1$. ■

4 Factorization in extensions

Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, and L/K a finite separable field extension. Let B be the integral closure of A in L. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then

$$\mathfrak{p}B = \beta_1^{e_1} \cdots \beta_g^{e_g},$$

where β_i are distinct prime ideals of B, and $e_i \geq 1$.

Say e_i is the ramification index. If some $e_i > 1$, then $\mathfrak{p}$ is ramified over in B (or L); if $e_i = 1$ for all i, then $\mathfrak{p}$ is unramified in B (or L).

Say β divides $\mathfrak{p}$ (written $\beta \mid \mathfrak{p}$) if β occurs in the factorization of $\mathfrak{p}$ in B.

$e(\beta/\mathfrak{p}) :=$ ramification index.

$f(\beta/\mathfrak{p}) := [B/\beta : A/\mathfrak{p}]$ (residue class degree).

A prime $\mathfrak{p}$ is said to be split (or split completely) in L if $e_i = f_i = 1$ for all i, and it said to be inert in L if $\mathfrak{p}B$ is a prime ideal ($g = 1$ and $e_1 = 1$).

Example 4.1.

- $(2) = (1+i)^2$ in $\mathbb{Z}[i]$, so (2) ramifies with ramification index 2.
- (3) is inert in $\mathbb{Q}[i]$ as $\mathbb{Z}[i]/(3) \simeq \mathbb{F}_9$.
- $(5) = (2+i)(2-i)$ splits completely in $\mathbb{Q}[i]$.

Lemma 4.2. *A prime ideal β of B divides $\mathfrak{p}$ iff $\mathfrak{p} = \beta \cap K$.*

Proof. "only if": $\mathfrak{p} \subset \beta \cap K$, $\beta \cap K \neq A \implies \mathfrak{p} = \beta \cap K$.

"if": $\mathfrak{p} = \beta \cap K \implies \mathfrak{p}B \subset \beta \implies \beta$ occurs in the factorization of $\mathfrak{p}B$. ■

4.1 Note on 20251027

theorem 4.3. *Let $m = [L : K]$. Let $\beta_1, \ldots, \beta_g$ be the prime ideals dividing $\mathfrak{p}$. Then*

$$\sum_{i=1}^{g} e_i f_i = m. \tag{4.1}$$

If L is Galois over K, then all ramification numbers e_i and the residue class degress f_i are equal $\implies efg = m$.

Proof. To prove (4.1), we shall show each side equals $[B/\mathfrak{p}B : A/\mathfrak{p}] = \dim_{A/\mathfrak{p}}(B/\mathfrak{p}B)$.

First, show $\sum_{i=1}^{g} e_i f_i = [B/\mathfrak{p}B : A/\mathfrak{p}]$. By Chinese Reminder Theorem,

$$B/\mathfrak{p}B = B/\prod_{i=1}^{g} \beta_i^{e_i} \simeq \prod_{i=1}^{g} B/\beta_i^{e_i}.$$

Only need to show $[B/\beta_i^{e_i} : A/\mathfrak{p}] = e_i f_i$. For any $r \geq 0$, $0 \neq \beta_i^r/\beta_i^{r+1}$ is a B/β_i-module, and there is no non-trivial submodule. So β_i^r/β_i^{r+1} is a one-dimensional B/β_i-vector space $\implies$

$$\dim_{A/\mathfrak{p}}(\beta_i^r/\beta_i^{r+1}) = \dim_{A/\mathfrak{p}} B/\beta_i = f_i.$$

Consider the chain

$$B \supset \beta_i \supset \beta_i^2 \cdots \supset \beta_i^{e_i}.$$

Each quotient β_i^r/β_i^{r+1} has dimension f_i over $A/\mathfrak{p} \implies$

$$[B/\beta_i^{e_i} : A/\mathfrak{p}] = \sum_{r=0}^{e_i-1} \dim_{A/\mathfrak{p}}(\beta_i^r/\beta_i^{r+1}) = e_i f_i.$$

Then prove $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$. Want to replace A, B by $A' = A_\mathfrak{p}, B' = B_\mathfrak{p}$ respectively. Note that $K = \mathrm{Frac}(A) = \mathrm{Frac}(A')$, $L = \mathrm{Frac}(B) = \mathrm{Frac}(B')$, and B' is the integral closure of A' in L. Let $\mathfrak{p}' = \mathfrak{p}A'$. Then $\mathfrak{p}'B' = (\mathfrak{p}B)B' = {\beta'_1}^{e_1} \cdots {\beta'_g}^{e_g}$, where $\beta'_i = \beta_i B'$, $B'_i/\beta'_i = B_i/\beta_i$ and $A/\mathfrak{p}' = A/\mathfrak{p} \implies [B'_i/\beta'_i : A'/\mathfrak{p}'] = f_i$. So $[B'/\mathfrak{p}'B' : A'/\mathfrak{p}'] = \sum_{i=1}^g e_i f_i$.

Only need to show $[B/\mathfrak{p}B : A/\mathfrak{p}] = m$ when A is a DVR. In this case B is a free A-module $\implies$ there exists an isomorphism of A-modules $A^n \to B$. Tensoring with K, we get an isomorphism of K-vector spaces $K^n \to B \otimes_A K = L \implies n = m$. We can also show $[B/\mathfrak{p}B : A/\mathfrak{p}] = n$ by tensoring with $A/\mathfrak{p} \implies [B/\mathfrak{p}B : A/\mathfrak{p}] = m$.

Now assume L/K is Galois. Any $\sigma \in \mathrm{Gal}(L/K)$ induces $\sigma\colon B \to B$ isomorphism. For any prime ideal β of B dividing $\mathfrak{p}$, $\sigma(\beta)$ is also a prime ideal of B dividing $\mathfrak{p}$. As σ is invertible, the map $\beta \mapsto \sigma(\beta)$ is a bijection on the set of prime ideals of B dividing $\mathfrak{p} \implies$ the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of prime ideals of B dividing $\mathfrak{p}$.

Suppose both β, β' divide $\mathfrak{p}$, and β' is not conjugate to β, i.e. $\beta' \notin \mathrm{Gal}(L/K)\beta$. By Chinese Reminder Theorem, $\exists\, a \in \beta' \setminus \bigcup_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta)$. Take $b = \mathrm{Nm}(a) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(a)$. Then $a \in \beta' \implies b \in \beta' \cap A = \mathfrak{p}$. On the other hand, any $\sigma \in \mathrm{Gal}(L/K)$, $a \notin \sigma^{-1}(\beta)$ i.e. $\sigma(a) \notin \beta$ for all $\sigma \in \mathrm{Gal}(L/K) \implies b = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(a) \notin \beta \cap A = \mathfrak{p}$. Contradiction! ■

4.1.1 The primes that ramify

THEOREM 4.4. *Let K be a number field, L/K a finite field extension, $A \subset K$ a Dedekind domain (e.g. $A = \mathcal{O}_K$), and B the integral closure of A in L. Assume that B is a free A-mod (true when A is a PID). Then a prime $\mathfrak{p}$ ramifies in L iff $\mathfrak{p} \mid \mathrm{disc}(B/A)$.*

In particular, only finitely many prime ideals ramify.

LEMMA 4.5. *Let A be a ring and B admitting a finite basis $\{e_1, \ldots, e_m\}$ as an A-mod. For any ideal $\mathfrak{a}$ of A, $\{\overline{e_1}, \ldots, \overline{e_m}\}$ is a basis of $B/\mathfrak{a}B$ as an $A/\mathfrak{a}$-mod, and*

$$D(\overline{e_1}, \ldots, \overline{e_m}) \equiv D(e_1, \ldots, e_m) \mod \mathfrak{a}.$$

Proof. Easy. ■

LEMMA 4.6. *Let A be a ring. Let $B_1, \ldots, B_g$ be rings containing A and free of finite rank as A-mods. Then*

$$\mathrm{disc}\Big(\big(\prod B_i\big)/A\Big) = \prod \mathrm{disc}(B_i/A).$$

Proof. Direct computation. ■

We say an element α in a ring is <u>nilpotent</u> if $\exists\, m > 0$ s.t. $\alpha^m = 0$.

<u>Fact</u>: $A =$ring:

$$\mathrm{Rad}(A) \coloneqq \{\alpha \in A \mid \alpha \text{ nilpotent}\} = \bigcap_{\mathfrak{p} \subset A \text{ prime}} \mathfrak{p}.$$

A ring is called <u>reduced</u> if $\mathrm{Rad}(A) = 0$. e.g. $A/\mathrm{Rad}(A)$ is reduced.

Recall that a field k is called <u>perfect</u> if any finite extension K/k is separable.

<u>Fact</u>:

1. If $\operatorname{char} k = 0$, then k is perfect.

2. If $\operatorname{char} k = p > 0$, then k is perfect iff $\forall\, \alpha \in k$, $\exists\, \beta \in k$ s.t. $\beta^p = \alpha$.

LEMMA 4.7. *Let k be a perfect field, and B a finite-dimensional reduced k-algebra. Then B is reduced iff* $\operatorname{disc}(B/k) \neq 0$.

Proof. Let $\beta \neq 0$ be a nilpotent element in B. Let $e_1, \ldots, e_m$ be a k-basis of B with $e_1 = \beta$. Then $e_1 e_j$ are all nilpotent $\implies \operatorname{Tr}(e_1 e_j) = 0 \implies$ the first column of the matrix $(\operatorname{Tr}_{B/k}(e_i e_j))_{1 \leq i,j \leq m}$ is zero $\implies \operatorname{disc}(B/k) = 0$.

... ■

4.2 Note on 20251103

Proposition 4.8. *Let $f(x) \in A[x]$ be an Eisenstein polynomial w.r.t. a prime ideal $\mathfrak{p}$ of a Dedekind domain A. Then $f(x)$ is irreducible, and if α is a root of $f(x)$, then $\mathfrak{p}$ is totally ramified in $K[\alpha]$. In fact, $\mathfrak{p}B = \beta^m$ with $\beta = (\mathfrak{p}, \alpha)$ and $m = \deg f$.*

Proof. $L \coloneqq K(\alpha)$. Then
$$[L : K] \leq m = \deg f.$$
Let β be a prime ideal of B dividing $\mathfrak{p}$ with ramification index e, $e \leq m$. Consider the equation
$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0.$$
Then

- $\mathrm{ord}_\beta(\alpha^m) = m \cdot \mathrm{ord}_\beta(\alpha)$;
- for $1 \leq i \leq m-1$,
$$\begin{aligned}\mathrm{ord}_\beta(a_i\alpha^{m-i}) &= (m-i)\cdot \mathrm{ord}_\beta(\alpha) + \mathrm{ord}_\beta(a_i)\\ &= (m-i)\cdot \mathrm{ord}_\beta(\alpha) + e\cdot \mathrm{ord}_{\mathfrak{p}}(a_i) \geq (m-i)\cdot \mathrm{ord}_\beta(\alpha) + e;\end{aligned}$$
- $\mathrm{ord}_\beta(a_m) = e \cdot \mathrm{ord}_{\mathfrak{p}}(a_m) = e$.

If $\mathrm{ord}_\beta(\alpha) = 0$, then $0 = \mathrm{ord}_\beta(\alpha^m) < \mathrm{ord}_\beta(\text{other terms})$, contradiction. So $\mathrm{ord}_\beta(\alpha) \geq 1$. For all $i = 1, \ldots, m-1$,
$$\mathrm{ord}_\beta(a_i\alpha^{m-i}) \geq (m-i)\cdot \mathrm{ord}_\beta(\alpha) + e > e.$$
$\implies \mathrm{ord}_\beta(\alpha^m) = m\cdot \mathrm{ord}_\beta(\alpha) = \mathrm{ord}_\beta(a_m) = e \implies e = m$ and $\mathrm{ord}_\beta(\alpha) = 1$ since $e \leq m$. ■

5 The finiteness of the class number

5.1 Note on 20251103

5.1.1 Norms of ideals

Let A be a Dedekind domain, $K = \mathrm{Frac}(A)$, and L/K a finite separable field extension. Let B be the integral closure of A in L. We want to define a homomorphism

$$\mathrm{Nm}_{B/A} \colon \mathrm{Id}(B) \longrightarrow \mathrm{Id}(A),$$

makes the following diagram commutes:

$$\begin{tikzcd} L^\times \arrow[r, "b \mapsto (b)"] \arrow[d, "\mathrm{Nm}"] & \mathrm{Id}(B) \arrow[d, "\mathrm{Nm}"] \\ K^\times \arrow[r] & \mathrm{Id}(A) \end{tikzcd}$$

$\mathrm{Id}(B)$ is the free abelian group on the set of prime ideals. Only need to define $\mathrm{Nm}(\mathfrak{p})$ for $\mathfrak{p}$ prime.

Let $\mathfrak{p}$ be a prime ideal of A,

$$\mathfrak{p}B = \prod_i \beta_i^{e_i}.$$

If $\mathfrak{p}$ is principle, say $\mathfrak{p} = (\pi)$, then

$$\mathrm{Nm}(\mathfrak{p}B) = \mathrm{Nm}(\pi B) = \mathrm{Nm}(\pi) \cdot A = (\pi^m) = \mathfrak{p}^m, \quad m = [L : K]. \tag{5.2}$$

Generally,

$$\mathrm{Nm}(\mathfrak{p}B) = \mathrm{Nm}\left(\prod_i \beta_i^{e_i}\right) = \prod_i \mathrm{Nm}(\beta_i)^{e_i}. \tag{5.3}$$

Compare (5.2) and (5.3). Recall $\sum_i e_i f_i = m$. So we can define

$$\mathrm{Nm}(\beta_i) = \mathfrak{p}^{f_i}.$$

Then (5.3) holds.

We take this as our definition:

Definition 5.1. Let β be a prime ideal of B. The norm of β is defined as

$$\mathrm{Nm}(\beta) \coloneqq \mathfrak{p}^{f(\beta/\mathfrak{p})}, \quad \text{where} \quad \mathfrak{p} \coloneqq \beta \cap A, \quad f(\beta/\mathfrak{p}) = [B/\beta : A/\mathfrak{p}].$$

To avoid confusion, we also use $\mathcal{N}$ to denote norms of ideals. If we have a tower of fields $M \supset L \supset K$, then

$$\mathcal{N}_{L/K}(\mathcal{N}_{M/L}\mathfrak{a}) = \mathcal{N}_{M/K}\mathfrak{a}.$$

Proposition 5.2. *1. Any nonzero ideal $\mathfrak{a}$ of a Dedekind domain A,*

$$\mathcal{N}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^m, \quad m = [L : K].$$

2. *Suppose L/K is Galois. Let β be a nonzero prime ideal of B with $\mathfrak{p} = \beta \cap A$. Write $\mathfrak{p}B = (\beta_1 \cdots \beta_g)^e$. Then*

$$\mathcal{N}(\beta) \cdot B = (\beta_1 \cdots \beta_g)^{ef} = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta).$$

3. *Any nonzero $b \in B$,*

$$\mathcal{N}(bB) = (\mathrm{Nm}_{L/K}(b))A.$$

Proof. 1. $\sum_i e_i f_i = m$;

2. $efg = m$;

3. First, treat the case L/K Galois. Let $\mathfrak{b} = bB$. Then the map

$$\begin{aligned} \mathrm{Id}(A) &\longrightarrow \mathrm{Id}(B) \\ \mathfrak{a} &\longmapsto \mathfrak{a}B \end{aligned}$$

is injective (by 1). Only need to show $\mathrm{Nm}(b) \cdot B = \mathcal{N}(\mathfrak{b}) \cdot B$. By 2,

$$\mathcal{N}(\mathfrak{b}) \cdot B = \prod \sigma(bB) = \prod \sigma(b) \cdot B = \mathrm{Nm}(b) \cdot B.$$

In the general case, let E/K be a finite Galois extension s.t. $E \supset L$. $d = [E : L]$. Then we have

$$\begin{aligned} \mathcal{N}_{L/K}(bB)^d &= \mathcal{N}_{L/K}(\mathcal{N}_{E/L}(bC)) = \mathcal{N}_{E/K}(bC) = \mathrm{Nm}_{E/K}(b)A \\ &= \mathrm{Nm}_{L/K}(\mathrm{Nm}_{E/L}(b))A = \mathrm{Nm}_{L/K}(b^d)A = (\mathrm{Nm}_{L/K}(b)A)^d. \end{aligned}$$

$\implies \mathcal{N}_{L/K}(bB) = \mathrm{Nm}_{L/K}(b)A.$

∎

Now assume K is a number field. Every $\mathfrak{a}$ nonzero ideal of $\mathcal{O}_K$ is of finite index in $\mathcal{O}_K$, i.e. $\sharp(\mathcal{O}_K/\mathfrak{a}) < \infty$.

Definition 5.3. Define $\mathscr{N}a := (\mathcal{O}_K : \mathfrak{a}) = \sharp(\mathcal{O}_K/\mathfrak{a}) \in \mathbb{Z}_{\geq 1}$, and call it numerical norm of $\mathfrak{a}$.

Proposition 5.4. 1. *For any ideal $\mathfrak{a}$ in $\mathcal{O}_K$,*

$$\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = (\mathscr{N}(\mathfrak{a})),$$

in particular, $\mathscr{N}(\mathfrak{a}\mathfrak{b}) = \mathscr{N}(\mathfrak{a})\mathscr{N}(\mathfrak{b})$.

2. *Let $\mathfrak{b} \subset \mathfrak{a}$ be fractional ideals in K, then*

$$(\mathfrak{a} : \mathfrak{b}) = \mathscr{N}(\mathfrak{a}^{-1}\mathfrak{b}).$$

Proof. 1. Write $\mathfrak{a} = \prod \beta_i^{r_i}$, $f_i = f(\beta_i/p_i)$, $(p_i) = \beta_i \cap \mathbb{Z}$, where p_i are prime numbers. Then $\mathrm{Nm}(\beta_i) = (p_i)^{f_i}$, and

$$\mathcal{O}_K/\mathfrak{a} \simeq \prod \mathcal{O}_K/\beta_i^{r_i},$$

where

$$\sharp(\mathcal{O}_K/\beta_i^{\gamma_i}) = \prod_{0 \leq s \leq r_i - 1} \sharp(\beta_i^s/\beta_i^{s+1}) = \Big(\sharp(\mathcal{O}_K/\beta_i)\Big)^{r_i},$$

and $[\mathcal{O}_K/\beta_i : \mathbb{Z}/(p_i)] = f_i \implies \sharp(\mathcal{O}_K/\beta_i) = p_i^{f_i}$. Hence, $\mathscr{N}(\mathfrak{a}) = \sharp(\mathcal{O}_K/\mathfrak{a}) = \prod p_i^{f_i r_i}$. $\implies$

$$(\mathscr{N}(\mathfrak{a})) = \prod (p_i)^{f_i r_i} = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}).$$

2. Any $d \in K^*$, the map

$$\begin{aligned}(K,+) &\longrightarrow (K,+)\\ x &\longmapsto d\cdot x\end{aligned}$$

is an isomorphism $\implies (d\mathfrak{a} : a\mathfrak{b}) = (\mathfrak{a} : \mathfrak{b})$. Since $\mathfrak{a}^{-1}\mathfrak{b} = (d\mathfrak{a})^{-1}(a\mathfrak{b})$, may assume $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$. $(\mathfrak{a}^{-1}\mathfrak{b})\mathfrak{a} = \mathfrak{b} \implies \mathscr{N}(\mathfrak{a}^{-1}\mathfrak{b})\mathscr{N}(\mathfrak{a}) = \mathscr{N}(\mathfrak{b})$. Also, $(\mathcal{O}_K : \mathfrak{a})(\mathfrak{a} : \mathfrak{b}) = (\mathcal{O}_K : \mathfrak{b})$. Hence, $(\mathfrak{a} : \mathfrak{b}) = \mathscr{N}(\mathfrak{a}^{-1}\mathfrak{b})$.

■

THEOREM 5.5. *Let K be a number field with $[K : \mathbb{Q}] = n$. Let $\Delta_K = \operatorname{disc}(K/\mathbb{Q})$, and*

$$2s \coloneqq \sharp\{\textit{non-real complex embedding of } K\}.$$

Then there exists a set of representatives for the ideal class group of K consisting of integral ideals $\mathfrak{a}$ with

$$\mathscr{N}(\mathfrak{a}) \le \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

The bound is called the Minkowski bound (denoted by B_K), and the Minkowski constant

$$C_K \coloneqq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s.$$

Note that $(2s \le n)$

$$C_K \approx \sqrt{2\pi n}\frac{1}{e^n}\left(\frac{4}{\pi}\right)^s \le \sqrt{2\pi n}\left(\frac{2}{e\sqrt{\pi}}\right)^n \to 0, \quad n \to \infty.$$

THEOREM 5.6. *The class group number of K is finite.*

Proof. Only need to show for any $M > 0$, the set

$$\sharp\{\mathfrak{a} \mid \text{ integral ideal of } \mathcal{O}_K \text{ with } \mathscr{N}(\mathfrak{a}) < M\} < \infty.$$

If $\mathfrak{a} = \prod \beta_i^{r_i}$, then

$$\mathscr{N}(\mathfrak{a}) = \prod p_i^{r_i f_i}, \quad (p_i) = \beta_i \cap \mathbb{Z},$$

where $p_i > 0$ prime. $\mathscr{N}(\mathfrak{a}) < M \implies p_i < M$ for all $i \implies$ finitely many β_i, $r_i \le n$, $f_i \le n$. ■

5.2 Note on 20251105

Let $S \coloneqq \{$integral ideals in K with norm $< B_K\}$, which is finite, and $\mathrm{Cl}(\mathcal{O}_K) = S/\sim$, where $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a}\cdot\mathfrak{b}^{-1}$ is principal.

To decide whether $\mathfrak{a} \sim \mathfrak{b}$, only need to decide whether $\mathfrak{c} \coloneqq \mathfrak{a}\cdot\mathfrak{b}^{-1}$ is principal. If $\mathfrak{c} = (\gamma)$, then

$$\mathscr{N}(\mathfrak{c}) = |\operatorname{Nm}(\gamma)|,$$

which is a diophatine equation (has algorithm to solve). Fix a $\mathbb{Z}$-basis of $\mathcal{O}_K$, $e_1, \dots, e_m$, and $\gamma = \sum x_i e_i$.

EXAMPLE 5.7. $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $\mathfrak{a}$ with $\mathscr{N}(\mathfrak{a}) \le 0.63 \times \sqrt{20} < 3$. $\Delta_K = 20$.

For $\mathfrak{a} \ne \mathcal{O}_K$, we have $\mathfrak{a} \mid (2)$. $(2) = \mathfrak{p}^2$, where $\mathfrak{p} = (2, 1+\sqrt{-5})$. $\mathscr{N}(\mathfrak{p}^2) = \mathscr{N}(2) = 4 \implies \mathscr{N}(\mathfrak{p}) = 2$. If $\mathfrak{p}$ is principal, then $\mathfrak{p} = (\alpha) = (m + n\sqrt{-5})$, $2 = \mathscr{N}(\mathfrak{p}) = \mathscr{N}(\alpha) = m^2 + 5n^2$. No solution. $\implies \mathrm{Cl}(\mathcal{O}_K)$ has order 2.

DEFINITION 5.8. An extension L of a number field K is said to be <u>unramified</u> over K if no prime ideal of $\mathcal{O}_K$ ramified in $\mathcal{O}_L$.

THEOREM 5.9. *No unramified extension of $\mathbb{Q}$.*

Proof. Let $K/\mathbb{Q}$ be a finite extension of $\mathbb{Q}$. Since a set of representatives for $\mathrm{Cl}(K) \ge 1$, and it has numerical norm ≥ 1. Theorem 5.5 $\implies$

$$|\Delta|^{1/2} \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \ge \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2} =: a_n.$$

Then

- $a_2 > 1$;
- $\frac{a_{n+1}}{a_n} = \left(\frac{\pi}{4}\right)^{1/2}\left(1+\frac{1}{n}\right)^n > 1$.

$\implies a_n > 1, \forall\, n \implies |\Delta| > 1 \implies K$ can not be unramified. ■

COROLLARY 5.10. *No irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 with discriminant $= 1$.*

Proof. Let f be such polynomial. Let α be a root of $f(x)$. Then $\mathrm{disc}(\mathbb{Z}[\alpha]/\mathbb{Z}) = \pm 1 \implies \mathbb{Z}[\alpha]$ is the ring of integers of $K = \mathbb{Q}[\alpha] \implies \mathrm{disc}(\mathcal{O}_K/\mathbb{Z}) = \pm 1$. Contradiction with Theorem 5.9. ■

5.2.1 Lattices

Let V be a $\mathbb{Q}$-vector space, $\dim V = n$.

DEFINITION 5.11. A lattice Λ in V is a subgroup of the form

$$\Lambda = \mathbb{Z}e_1 + \cdots \mathbb{Z}e_r$$

with $e_1, \dots, e_r$ linearly independent elements on V (for $\mathbb{R}$).

Fact: $r \le n$.

When $r = n$, the lattice is said to be full.

A full lattice in V is a subgroup λ for V s.t. the map

$$\mathbb{R} \otimes \Lambda \longrightarrow V$$
$$\sum r_i \otimes x_i \longmapsto \sum r_i x_i$$

is an isomorphism.

EXAMPLE 5.12. The group $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ of $\mathbb{R}$ is a free abelian group of rank 2, but it is not a lattice in $\mathbb{R}$.

LEMMA 5.13. *The following conditions on a subgroup Λ of V are equivalent:*

1. *Λ is a discrete group;*
2. *$\exists$ an open subset U of V s.t. $U \cap \Lambda = \{o\}$;*
3. *$\forall$ compact subset K of V, $\sharp(K \cap \Lambda) < \infty$;*
4. *$\forall$ bounded subset B of V, $\sharp(B \cap \Lambda) < \infty$.*

Proof. Easy. ∎

PROPOSITION 5.14. *A subgroup Λ of V is a lattice if and only if it is discrete.*

Proof. "Only if": $\Lambda = \sum \mathbb{Z}e_i$, $i = 1, \dots, r$, e_i linearly independent. Extend $e_1, \dots, e_r$ to a basis $e_1, \dots, e_n$ of V. Assume $r = n$. Then $U \coloneqq \sum_{i=1}^{n}(-1/2, 1/2)e_i$ is open in V and $U \cap \Lambda = \{o\}$.

"If": Replace V by the $\mathbb{R}$-subspace generated by Λ. We may assume V is generated by Λ (over $\mathbb{R}$). $\exists\, e_1, \dots, e_n \in \Lambda$ forms a $\mathbb{R}$-basis of V.

$$\Lambda' \coloneqq \sum_{i=1}^{n} \mathbb{Z}e_i < \Lambda,$$

and $V/\Lambda' \simeq (\mathbb{R}/\mathbb{Z})^n$ compact. Let $K \coloneqq \sum_{i=1}^{n}[0,1)e_i$ bounded, and $K \to V/\Lambda'$ bijective. Moreover, $K \cap \Lambda \to \Lambda/\Lambda'$ bijection. Λ discrete $\implies$ $K \cap V$ finite $\implies$ Λ/Λ' finite $\implies$ $\exists N \in \mathbb{Z}_{\ge 1}$ s.t. $N \cdot \Lambda/\Lambda' = 0 \implies \Lambda \subset \frac{1}{N}\Lambda' \implies \Lambda$ is free abelian of rank n. Then for $f_1, \dots, f_n$ a $\mathbb{Z}$-basis of Λ, they are linearly independent over $\mathbb{R}$. ∎

DEFINITION 5.15. Let V be a $\mathbb{R}$-vector space, $\dim V = n$, and Λ a full lattice in V. Write $\Lambda = \sum \mathbb{Z}e_i$.

For any $\lambda_0 \in \Lambda$, let

$$D_{(\lambda_0)} \coloneqq \{\lambda_0 + \sum a_i e_i \mid 0 \le a_i < 1\}.$$

Such a set is called a fundamental parallelopipod for Λ.

Its shape depends on the choice of the basis (e_i). Fix e_i,

$$V = \sum_{\lambda\in\Lambda} D_\lambda.$$

REMARK 5.16. *1. $\forall$ FP D of $\Lambda = \mathbb{Z}f_1 + \cdots \mathbb{Z}f_n$ in $\mathbb{R}^n$,*

$$\mathrm{Vol}(D) = |\det(f_1, \ldots, f_n)|.$$

If also $\Lambda = \mathbb{Z}f_1' + \cdots \mathbb{Z}f_n'$, then $\det(f_1', \ldots, f_n') = \pm\det(f_1, \ldots, f_n)$. So $\mathrm{Vol}(D)$ does not depend on the choice of the basis for Λ.

2. When $\Lambda \supset \Lambda'$ are two full lattices in $\mathbb{R}^n$, we can choose the bases (e_i) and (f_i) for Λ and Λ' s.t. $f_i = m_i e_i$, where $m_i \in \mathbb{Z}_{\geq 1}$. With the choice of basis, the FP D' of Λ' is a disjoint union of $(\Lambda : \Lambda')$ FP D of Λ. Hence,

$$\frac{\mu(D')}{\mu(D)} = (\Lambda : \Lambda'). \tag{5.4}$$

The choice of a basis for V determines an isomorphism $V \simeq \mathbb{R}^n$, hence a measure μ on V. μ is invariant under translations $\implies$ μ is well defined up to multiplication by a nonzero constant.

Thus the ratio of measures of two sets is well defined. The equality (5.4) holds for two full lattices $\Lambda \supset \Lambda'$ in V.

THEOREM 5.17. *Let D_0 be a FP for a full lattice V, and S a mesurable subset of V. If $\mu(S) > \mu(D_0)$, then S contains distinct points α and β s.t. $\beta - \alpha \in \Lambda$.*

Proof.

$$\mu(D_0) < \mu(S) = \sum_{\lambda\in\Lambda} \mu(S \cap D_\lambda) = \sum_{\lambda\in\Lambda} \mu\big((S-\lambda) \cap D_0\big),$$

$\implies$ there exists $\lambda_1, \lambda_2 \in \Lambda$ distinct s.t.

$$[(S-\lambda_0) \cap D_0] \cap [(S-\lambda_2) \cap D_0] \neq \varnothing \implies D_0 \cap [(\lambda_1 - \lambda_2) + S] \neq \varnothing.$$

Pick α in the above set, then $\beta = \alpha - (\lambda_1 - \lambda_2) \in S$, $\alpha - \beta \in \Lambda$. ■

5.3 Note on 20251110

Let $T \subset V$. We say T is symmetric in the origin if $\alpha \in T \implies -\alpha \in T$.
If T is convex and symmetric in the origin, we have:

$$\forall\, \alpha, \beta \in T \implies \frac{\alpha - \beta}{2} \in T. \tag{5.5}$$

LEMMA 5.18. *Assume T satisfies (5.5) and $\mu(T) > 2^n \mu(D)$. Then $T \cap (\Lambda \setminus \{o\}) \neq \varnothing$.*

Proof. Let $S = \frac{1}{2}T$. Then $\mu(S) > \mu(D)$. Theorem 5.17 $\implies \exists\, \alpha, \beta \in S$, $\alpha \neq \beta$ s.t. $\alpha - \beta \in \Lambda$. By (5.5), $\alpha - \beta = \frac{2\alpha - 2\beta}{2} \in T$. Hence, $T \cap (\Lambda \setminus \{0\}) \neq \varnothing$. ■

THEOREM 5.19 (Minkowski; 1896). *Let T be a subset of V, that is compact, convex, and symmetric in the origin. If $\mu(T) \geq 2^n \mu(D)$, then T contains a point of the lattice other than the origin.*

Proof. Let $\epsilon > 0$. Since T is compact, for $T_\epsilon = (1+\epsilon)T$, we have $T \subset S$ and $\mu(T_\epsilon) = (1+\epsilon)^n \mu(T) > 2^n \mu(D)$. By the previous lemma, $T_\epsilon \cap (\Lambda \setminus \{0\}) \neq \varnothing \implies T \cap (\Lambda \setminus \{0\}) \neq \varnothing$ by the compactness of T. ■

REMARK 5.20. *Theorem 5.5 has many non-trivial consequences. It was the starting point for "geometry of numbers".*

COROLLARY 5.21. *Any $n \in \mathbb{Z}_{\geq 0}$ is a sum of four squares.*

Proof. From the identity

$$\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
&= (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4)^2 + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)^2 \\
&\quad + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)^2 + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)^2,
\end{aligned}$$

we only need to show that any prime number p is a sum of four squares. $2 = 1^2 + 1^2 + 0^2 + 0^2$. For odd prime p:

Claim: $m^2 + n^2 + 1 \equiv 0 \mod p$ has a solution $(m, n) \in \mathbb{Z}^2$.

Proof of the claim. Consider the sets

$$A = \{m^2 \mid m = 0, 1, \dots, (p-1)/2\}, \quad B = \{-n^2 - 1 \mid n = 0, 1, \dots, (p-1)/2\}.$$

Then $\sharp A = \sharp B = (p+1)/2 \implies A \cap B \neq \varnothing \implies \exists\, m, n$ s.t. $m^2 \equiv -n^2 - 1 \mod p$. ■

Fix a solution (m, n) of the claim. Consider the lattice $\Lambda \subset \mathbb{Z}^4$ consisting of points (a_1, a_2, a_3, a_4) satisfying

$$a_1 \equiv m a_3 + n a_4 \mod p, \quad a_2 \equiv n a_3 - m a_4 \mod p.$$

Then Λ is of index p^2 in $\mathbb{Z}^4$. Let

$$T = \{(a_1, a_2, a_3, a_4) \in \mathbb{R}^4 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2 < r^2\}.$$

Then $\mu(T) = \pi^2 r^4/2$. A FP D of Λ has measure $\mu(D) = p^2$. Let $2p > r^2 > 1.9p$. Then $\mu(T) > 16\mu(D)$. Theorem 5.19 $\implies$ T contains a point of Λ other than the origin, say (a_1, a_2, a_3, a_4). Then

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \mod p, \quad a_1^2 + a_2^2 + a_3^2 + a_4^2 < 2p \implies a_1^2 + a_2^2 + a_3^2 + a_4^2 = p.$$

■

5.3.1 Finiteness of the class number

Let K be a number field, $[K : \mathbb{Q}] = n$. Let r be the number of real embeddings $\{\sigma_1, \dots, \sigma_r\}$ of K, and $2s$ the number of non-real complex embeddings $\{\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}\}$. Then $n = r + 2s$.

We have an embedding

$$\begin{aligned} \sigma \colon K &\longrightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^{r+2s} = \mathbb{R}^n = V \\ \alpha &\longmapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \dots, \sigma_{r+s}(\alpha)). \end{aligned}$$

Metric on V:

$$\|(x_1, \dots, x_r, z_1, \dots, z_s)\| := |x_1|^2 + \dots + |x_r|^2 + 2(|z_1|^2 + \dots + |z_s|^2).$$

Proposition 5.22. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then $\sigma(\mathfrak{a})$ is a full lattice in V with fundamental parallelopipod D satisfying*

$$\mu(D) = 2^{-s}\sqrt{|\Delta_K|} \cdot \mathcal{N}(\mathfrak{a}).$$

Proof. Let $\alpha_1, \dots, \alpha_n$ be a basis of $\mathfrak{a}$ as a $\mathbb{Z}$-module. To prove $\sigma(\mathfrak{a})$ is a lattice, we show that the matrix $A =$

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_1) & \operatorname{Re}(\sigma_{r+1}(\alpha_1)) & \cdots & \operatorname{Re}(\sigma_{r+1}(\alpha_1)) & \operatorname{im}(\sigma_{r+1}(\alpha_1)) & \cdots & \operatorname{im}(\sigma_{r+1}(\alpha_1)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_r(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}(\sigma_{r+s}(\alpha_n)) & \cdots & \operatorname{Re}(\sigma_{r+s}(\alpha_n)) & \operatorname{im}(\sigma_{r+s}(\alpha_n)) & \cdots & \operatorname{im}(\sigma_{r+s}(\alpha_n)) \end{pmatrix}$$

has nonzero determinant. Let the matrix $B =$

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_1) & \sigma_{r+1}(\alpha_1) & \overline{\sigma_{r+1}(\alpha_1)} & \cdots & \sigma_{r+1}(\alpha_s) & \overline{\sigma_{r+s}(\alpha_1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_1(\alpha_n) & \sigma_{r+1}(\alpha_n) & \overline{\sigma_{r+1}(\alpha_n)} & \cdots & \sigma_{r+1}(\alpha_n) & \overline{\sigma_{r+s}(\alpha_n)} \end{pmatrix}.$$

Then $\det(B) = \det(A)\big(\det(1, 1; \mathrm{i}, -\mathrm{i})\big)^s \implies$

$$\det(A) = (-2\mathrm{i})^{-s}\det(B) = \pm(-2\mathrm{i})^{-s} D(\alpha_1, \dots, \alpha_n)^{1/2} \neq 0.$$

Moreover,

$$\begin{aligned} \mu(D) = |\det(A)| &= 2^{-s}|D(\alpha_1, \dots, \alpha_n)|^{1/2} \\ &= 2^{-s}\sqrt{|\Delta_K|} \cdot [\mathcal{O}_K : \mathfrak{a}] \\ &= 2^{-s}\sqrt{|\Delta_K|} \cdot \mathcal{N}(\mathfrak{a}). \end{aligned}$$

■

Proposition 5.23. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$. Then there exists a nonzero element $\alpha \in \mathfrak{a}$ s.t.*

$$|\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot \mathscr{N}(\mathfrak{a}).$$

Proof. Let

$$X_t := \{x \in V \mid \|x\| \leq t\},$$

which is compact, convex, and symmetric in the origin. Choose t s.t. $\mu(X_t) = 2^n \mu(D)$. Then

$$\begin{aligned} t^n \frac{\pi^s}{2^{r+s} n!} &= 2^n \cdot 2^{-s} \sqrt{|\Delta_K|} \cdot \mathscr{N}(\mathfrak{a}) \\ \implies t &= \left(\frac{4}{\pi}\right)^{s/n} \frac{n!^{1/n}}{n} \sqrt[n]{|\Delta_K|} \cdot \mathscr{N}(\mathfrak{a})^{1/n}. \end{aligned}$$

By Theorem 5.19, $\exists\, \alpha \in \mathfrak{a}$, $\alpha \neq 0$ s.t. $\sigma(\alpha) \in X_t$. Then

$$\begin{aligned} |\operatorname{Nm}_{K/\mathbb{Q}}(\alpha)| &= \prod_{i=1}^{r} |\sigma_i(\alpha)| \cdot \prod_{j=1}^{s} |\sigma_{r+j}(\alpha)|^2 \\ &\leq \left(\frac{\|\sigma(\alpha)\|}{n}\right)^n \quad \text{(by AM-GM inequality)} \\ &\leq \left(\frac{t}{n}\right)^n = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot \mathscr{N}(\mathfrak{a}). \end{aligned}$$

■

theorem 5.24. *There exists a set of representatives for the ideal class group of K consisting of integral ideals $\mathfrak{a}$ with*

$$\mathscr{N}(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Proof. Let $\mathfrak{c}$ be a frational ideal of K. We want to show that the class of $\mathfrak{c}$ in $\mathrm{Cl}(K)$ is represented by an integral ideal $\mathfrak{a}$ with $\mathscr{N}(\mathfrak{a}) \leq B_K$. Since $\mathfrak{c}^{-1}$ is a fractional ideal, $\exists\, d \in \mathcal{O}_K$, $d \neq 0$ s.t. $d\mathfrak{c}^{-1} = \mathfrak{b}$ is an integral ideal. By the previous proposition, $\exists\, \beta \in \mathfrak{b}$, $\beta \neq 0$ s.t.

$$|\operatorname{Nm}_{K/\mathbb{Q}}(\beta)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot \mathscr{N}(\mathfrak{b}).$$

Let $\mathfrak{a} = (\beta) d^{-1} \mathfrak{c}$. Then $\mathfrak{a}$ is an integral ideal in the class of $\mathfrak{c}$, and

$$\mathscr{N}(\mathfrak{a}) = |\operatorname{Nm}_{K/\mathbb{Q}}(\beta)| \cdot \mathscr{N}(\mathfrak{b})^{-1} \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_K|}.$$

■

5.3.2 Binary quadratic forms

Let

$$Q(x,y) = ax^2 + bxy + cy^2.$$

We call it integral if $Q(m,n) \in \mathbb{Z}$ for all $m,n \in \mathbb{Z}$, i.e. $a,b,c \in \mathbb{Z}$. Its discriminant is defined as

$$d_Q = b^2 - 4ac.$$

A form is said to be non-degenerate if $d_Q \neq 0$.

Two integral binary quadratic forms Q and Q' are said to be equivalent if there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ s.t.

$$Q'(x,y) = Q(px+qy, rx+sy), \quad M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

The question considered by Gauss was to try to describe the set of equivalence classes of forms with a fixed discriminant.

5.4 Note on 20251117

Let $d \neq 1$ be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$ and $d_K \coloneqq \operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$.

Recall
$$\begin{cases} d_K = 4d & \text{if } d \equiv 2, 3 \mod 4, \\ d_K = d & \text{if } d \equiv 1 \mod 4. \end{cases}$$

Define <u>norm form</u> q_K by
$$q_K(x,y) = \operatorname{Nm}_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2 \quad \text{if } d \equiv 2, 3 \mod 4,$$
and
$$q_K(x,y) = \operatorname{Nm}_{K/\mathbb{Q}}\left(x + y\frac{1+\sqrt{d}}{2}\right) = x^2 + xy + \frac{1-d}{4}y^2 \quad \text{if } d \equiv 1 \mod 4,$$

In general, if Q is an integral binary quadratic form, then $d_Q = d_K \cdot f^2$ for some integer f, where $K = \mathbb{Q}(\sqrt{d_{\mathbb{Q}}})$. Moreover, if $d_Q = d_K$, then Q is primitive, $\gcd(a,b,c) = 1$.

Fix a field $K = \mathbb{Q}(\sqrt{d})$ and an embedding $K \hookrightarrow \mathbb{C}$. Choose $\sqrt{d}$ to be positive if $d > 0$, and have positive imaginary part if $d < 0$.

Write $\operatorname{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$. If $d < 0$, define $\mathrm{Cl}^+(K) \coloneqq \mathrm{Cl}(K)$, and if $d > 0$, define
$$\mathrm{Cl}^+(K) \coloneqq \mathrm{Id}(K)/P^+(K),$$
where $P^+(K)$ is the group of principle ideals of form (α) with $\alpha > 0$ under any embedding of K into $\mathbb{R}$.

Let $\mathfrak{a}$ be a fractional ideal in K, let a_1, a_2 be a basis of $\mathfrak{a}$ as $\mathbb{Z}$-mod. We know
$$\begin{vmatrix} a_1 & a_2 \\ \sigma(a_1) & \sigma(a_2) \end{vmatrix}^2 = d_K \cdot \mathscr{N}(\mathfrak{a})^2.$$
After possibly reorder of a_1, a_2, we may ask
$$\begin{vmatrix} a_1 & a_2 \\ \sigma(a_1) & \sigma(a_2) \end{vmatrix} = \sqrt{d_K} \cdot \mathscr{N}(\mathfrak{a}).$$
For such a pair, define
$$Q_{a_1,a_2}(x,y) = \mathscr{N}(\mathfrak{a})^{-1} \operatorname{Nm}_{K/\mathbb{Q}}(a_1 x + a_2 y).$$
This is an integral binary quadratic form with discriminant d_K.

THEOREM 5.25. *The equivalent class of $Q_{a_1,a_2}(x,y)$ depends only on the image of $\mathfrak{a}$ in $\mathrm{Cl}^+(K)$. Moreover, the map sending $\mathfrak{a}$ to the equivalence class of Q_{a_1,a_2} defines a bijection from $\mathrm{Cl}^+(K)$ to the set of equivalence classes of integral binary quadratic form with discriminant d_K.*

6 The Unit Theorem

Let K be a number field, r be the number of real embeddings of K, and $2s$ be the number of non-real complex embeddings.

Thus,

$$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^s \times \mathbb{C}^s$$

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

THEOREM 6.1. *The group of units in $\mathcal{O}_K$ is finitely generated with rank $= r + s - 1$.*

Denote $U_K \coloneqq \mathcal{O}_K^\times$. The torsion group of U_K is $\mu(K) = \{\text{roots of } 1 \text{ in } K\}$.

EXAMPLE 6.2. Let K be a real quadratic field. Then $\operatorname{rk}(U_K) = 2 + 0 - 1 = 1$.

Let K be a complex quadratic field. Then $\operatorname{rk}(U_K) = 0 + 1 - 1 = 0$.

A set of units $u_1, \dots, u_{r+s-1}$ is called a fundamental system of units, if it forms a basis for U_K modulo torsions i.e. any unit u can be written uniquely in the form

$$u = \xi \cdot u_1^{m_1} \cdots u_{r+s-1}^{m_{r+s-1}}, \quad \xi \in \mu(K),$$

with $m_i \in \mathbb{Z}$.

LEMMA 6.3. *An element $\alpha \in K$ is a unit iff $\alpha \in \mathcal{O}_K$ and $\operatorname{Nm}_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof. If $\alpha \in U_K$, then $\exists\, \beta \in \mathcal{O}_K$ s.t.

$$\alpha \cdot \beta = 1 \implies \operatorname{Nm}(\alpha) \cdot \operatorname{Nm}(\beta) = 1 \implies \operatorname{Nm}(\alpha) = \pm 1.$$

For the converse, fix an embedding $\sigma_0 \colon K \hookrightarrow \mathbb{C}$ and identify K with $\sigma_0(K)$. Then

$$\pm 1 = \operatorname{Nm}(\alpha) = \prod_{\sigma} \sigma(\alpha) = \alpha \prod_{\sigma \neq \sigma_0} \sigma(\alpha) =: \alpha \cdot \beta.$$

Then $\alpha \in \mathcal{O}_K \implies \sigma(\alpha)$ are algebraic integers $\implies \beta$ is an algebraic integer. As $\beta = \pm \alpha^{-1}$, $\beta \in K \implies \beta \in \mathcal{O}_K \implies \alpha \in U_K$. ∎

6.0.1 Proof of that U_K is finitely generated

PROPOSITION 6.4. *Given $m, M > 0$. The set of all algebraic integers α s.t.*

1. *the degree of $\alpha \leq m$; and*
2. *$|\alpha'| \leq M$ for all conjugates α' of α,*

is finite.

Proof. By (1), α is a root of a monic irreducible polynomial of deg $\leq m$ over $\mathbb{Z}$.

By (2), the coefficients of the polynomial are bounded in term of M. Only finitely many such polynomials. ∎

COROLLARY 6.5. *An algebraic integer α, each of whose conjugates, in $\mathbb{C}$ has absolute value 1, is a root of unity.*

Proof. By Proposition 6.4, $\{1, \alpha, \alpha^2, \dots\}$ is a finite set. ∎

Remark 6.6. *It is essential to require α to be an algebraic integer. For example, $\alpha = \frac{3+4i}{5}$ is not a root of unity.*

Consider

$$\begin{aligned} \sigma\colon K &\longrightarrow \mathbb{R}^r \times \mathbb{C}^s \\ \alpha &\longmapsto (\sigma_1\alpha, \ldots, \sigma_r\alpha, \sigma_{r+1}\alpha, \ldots, \sigma_{r+s}\alpha). \end{aligned}$$

Take logarithm, we consider

$$\begin{aligned} L\colon K^\times &\longrightarrow \mathbb{R}^{r+s} \\ \alpha &\longmapsto (\log|\sigma_1\alpha|, \ldots, \log|\sigma_{r+s}\alpha|), \end{aligned}$$

It is a homomophism for $\times$.

For any $u \in U_K$, since $\mathrm{Nm}_{K/\mathbb{Q}}(u) = \pm 1$, we have

$$|\sigma_1 u| \cdots |\sigma_r(u)||\sigma_{r+1}u|^2 \cdots |\sigma_{r+s}u|^2 = 1,$$

$\implies$ $L(u)$ is contained in the hyperplane

$$H\colon x_1 + \ldots + x_r + 2x_{r+1} + \ldots + 2x_{r+s} = 0,$$

$H \simeq \mathbb{R}^{r+s-1}$.

Proposition 6.7. *The image of L in H is a lattice in H.*

$\ker L|_{U_K}$ *is a finite group (hence $= \mu(K)$).*

Proof. Set

$$C = \{x \in H \mid |x_i| \le M\},$$

for which $o \in C$ and bounded. Let $L(u) \in C$, then $|\sigma_i u| \le e^M$ for any j. By Proposition 6.4, only finitely many such $u \in U \coloneqq \sigma(U_K)$, i.e. $\sharp(L^{-1}(C) \cap U_K) < \infty \implies L(U_K)$ is a lattice in H, and $\ker L|_{U_K}$ is finite. ■

Consider the exact sequence:

$$0 \longrightarrow \mu(K) \longrightarrow U_K \xrightarrow{L\circ\sigma} L(U_K) \to 0,$$

where μ_K is finite, and $L(U_K)$ is a lattice in H hence free of rank $\le \dim H = r + s - 1 \implies U_K$ is finitely generated and $\mathrm{rk}(U_K) \le r + s - 1$.

theorem 6.8. *The image $L(U_K)$ in H is a full lattice ($\implies \mathrm{rk}(U_K) = r + s - 1$).*

Proof. We work with

$$\sigma\colon K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^{r+2s}.$$

For $x = (x_1, \ldots, x_r, x_{r+1}, \ldots) \in \mathbb{R}^r \times \mathbb{C}^s$, define

$$\mathrm{Nm}(x) = x_1 \ldots x_r x_{r+1}\overline{x_{r+1}} \cdots x_{r+s}\overline{x_{r+s}}.$$

$L\colon K^\times \to \mathbb{R}^{r+s}$ extends to

$$\begin{aligned} L\colon \mathbb{R}^r \times \mathbb{C}^s &\longrightarrow (\mathbb{R} \cup \{-\infty\})^{r+s} \\ (x_1, \ldots, x_r, x_{r+1}, \ldots) &\longmapsto (\log|x_1|, \ldots, \log|x_{r+1}|, \ldots) \end{aligned}$$

continuous, surjective.

Consider
$$Y \coloneqq \{x \in \mathbb{R}^r \times \mathbb{C}^s \mid |\operatorname{Nm}(x)| = 1\},$$
which is a group for $\times$. Then

- Y is closed;
- $Y = L^{-1}(H)$.

$\implies L|_Y \coloneqq Y \to H$ surjective, continuous, and preserves the multiplication.

Lemma 6.9. *$\exists\, \Omega \subset Y$ compact containing $(1, \dots, 1)$ s.t. $Y = \bigcup_{u \in U} u\Omega$.*

Proof. Let $y \in Y$, the map
$$\begin{aligned} \mathbb{R}^r \times \mathbb{C}^s &\longrightarrow \mathbb{R}^r \times \mathbb{C}^s \\ x &\longmapsto y \cdot x \end{aligned}$$
has |Jacobian| is $|\operatorname{Nm}(y)| = 1$. $\implies$ It preserves the volume. Minkowski's thm $\implies \exists\, B$ s.t. any compact convex subset $T \subseteq \mathbb{R}^r \times \mathbb{C}^s$ symmetric in the origin, if $\mu(T) \geq B$, then $T \cap \big(\sigma(\mathcal{O}_K) \setminus \{0\}\big) \neq \varnothing$.

Pick such T. Any $y \in Y$, $y^{-1}T$ satisfies the same condition. For example, $\mu(y^{-1}T) = \mu(T) \geq B$ $\implies \exists, \gamma_y \in \mathcal{O}_K \setminus \{0\}$ s.t. $\gamma_y \in y^{-1}T \implies \mathscr{N}((\gamma_y)) = \operatorname{Nm}(\gamma_y) \leq \max_{t \in T} \operatorname{Nm}(T) \eqqcolon B_1$.

The set of principle ideals $\mathscr{N}(\gamma) \leq B_1$ is finite. Denote it by $\{(\gamma_1), \dots, (\gamma_m)\}$. Then $(\gamma_y) = (\gamma_i)$ for some $i = 1, \dots, m$. Thus, $\gamma_y = \gamma_i \cdot \varepsilon_y^{-1}$ for some $\varepsilon_y \in U \implies \gamma_i \cdot \varepsilon_y^{-1} \in y^{-1}T \implies y \in \varepsilon_y \cdot \gamma_i^{-1}T$ $\implies$
$$y \in \varepsilon_y \cdot \Big(\bigcup_{i=1}^m \gamma_i^{-1}T\Big).$$
As $y \in Y$, $\varepsilon_y \in Y$, $y \cdot \varepsilon_y^{-1} \in Y \implies$
$$y \cdot \varepsilon_y^{-1} \in Y \cap \Big(\bigcup_{i=1}^m \gamma_i^{-1}T\Big) \eqqcolon \Omega$$
compact, $\implies Y = \bigcup_{\varepsilon \in U} \varepsilon\Omega$. ■

Lemma $\implies$
$$H = L(Y) \subseteq \bigcup_{u \in U} \Big(L(u) + L(\Omega)\Big)$$
$\implies H = \bigcup_{u \in L(U)} (u + L(\Omega)) \implies L(U)$ is full. Otherwise, there exists a nonzero linear function $g \colon H \to \mathbb{R}$ s.t. $g(L(U)) = 0$. Then
$$g(H) = g\Big(\bigcup_{u \in L(U)} (u + L(\Omega))\Big) = g(L(\Omega))$$
is bounded. Contradiction! ■

6.1 Note on 20251119

6.1.1 S-units

Let S be a finite set of prime ideals of $\mathcal{O}_K$.

DEFINITION 6.10. The ring of S-integers is

$$\mathcal{O}_K(S) \coloneqq \bigcap_{\mathfrak{p}\notin S} \mathcal{O}_{\mathfrak{p}} = \{\alpha \in K \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0,\ \forall\, \mathfrak{p} \notin S\}.$$

If $S = \varnothing$, then $\mathcal{O}_K(S) = \mathcal{O}_K$.

DEFINITION 6.11. The group of S-units is

$$U(S) \coloneqq \mathcal{O}_K(S)^\times = \{\alpha \in K \mid \mathrm{ord}_{\mathfrak{p}}(\alpha) = 0,\ \forall\, \mathfrak{p} \notin S\}.$$

Clearly, the torsion subgroup of $U(S)$ is $\mu(K)$.

THEOREM 6.12. *The group of S-units is finitely generated with rank $= r + s + \sharp S - 1$.*

Proof. Write $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$. Consider the homomophism

$$\begin{aligned} \theta\colon U(S) &\longrightarrow \mathbb{Z}^t \\ u &\longmapsto \big(\mathrm{ord}_{\mathfrak{p}_1}(u), \ldots, \mathrm{ord}_{\mathfrak{p}_t}(u)\big), \end{aligned}$$

where $\ker\theta = U(S)$. Only need to show $\mathrm{rk}\,\mathrm{im}(\theta) = t$. Let $h = \sharp\,\mathrm{Cl}(K) < \infty$. Then $\mathfrak{p}_i^h$ is principal for any i. Write $\mathfrak{p}_1^h = (\pi_i)$. Then π_i is an S-unit with

$$\theta(\pi_i) = (0, \ldots, 0, h, 0, \ldots, 0),$$

where h is at the i-th position. $\implies$ $\mathrm{im}(\theta) \supset h\cdot\mathbb{Z}^t$, hence $\mathrm{rk}\,\mathrm{im}(\theta) = t$. ■

EXAMPLE 6.13. $K = \mathbb{Q}$, $S = \{(2), (3), (5)\}$. Then $U(S) = \{\pm 2^k 3^m 5^n \mid k, m, n \in \mathbb{Z}\}$.

6.1.2 Example: CM fields

DEFINITION 6.14. We say a number field K is totally real if all of its embeddings in $\mathbb{C}$ lie in $\mathbb{R}$, i.e. $r = n$, $s = 0$. And it is totally imaginary if non of its embedding in $\mathbb{C}$ is in $\mathbb{R}$, i.e. $r = 0$, $s = n/2$.

A CM field K is a totally imaginary quadratic extension of a totally real field, i.e.

- $K = K^+(\sqrt{\alpha})$;
- K^+ is totally real;
- $\alpha \in K^+$, any conjugate of α is negative.

Such K^+ is unique. Indeed, any $\sigma\colon K \hookrightarrow \mathbb{C}$, $K^+ = \sigma^{-1}(\sigma(K) \cap \mathbb{R})$.

Let K be a CM field. $m = [K^+ : \mathbb{Q}]$ $\implies$ $[K : \mathbb{Q}] = 2m$. So $\mathrm{rk}(U_K) = m - 1 = \mathrm{rk}(U_{K^+})$. $\implies$ $[U_K : U_{K^+}] < \infty$.

PROPOSITION 6.15. *The index of $\mu(K)\cdot U_{K^+}$ in U_K is either 1 or 2.*

Proof. $\underline{\mathrm{Gal}}(K/K^+) = \{\mathrm{Id}, \tau\}$. For any $a \in K$, write $\tau(a) = \overline{a}$. For any field embedding $\rho\colon K \hookrightarrow \mathbb{C}$, we have $\overline{\rho(a)} = \rho(\overline{a}) \implies \forall\, a \in K$, any conjugate of $a/\overline{a}$ in $\mathbb{C}$ has norm 1 $\implies a/\overline{a} \in \mu(K)$.

Consider

$$\begin{aligned} \phi\colon U_K &\longrightarrow \mu(K)/\mu(K)^2 \\ a &\longmapsto \frac{a}{\overline{a}} \mod \mu(K)^2. \end{aligned}$$

Any $u \in \ker(\phi)$, $u/\overline{u} = \xi^2$ for some $\xi \in \mu(K)$. Then

$$\frac{u \cdot \overline{\xi}}{\overline{u} \cdot \xi} = \xi^2 \cdot \frac{\overline{\xi}}{\xi} = 1$$

$\implies u \cdot \overline{\xi} \in K^+ \implies u \in \mu(K) \cdot U_{K^+}$.

Conversely, if $u = \underline{\xi \cdot u^+}$ with $\xi \in \mu(K)$ and $u^+ \in U_{K^+}$, then $u/\overline{u} = \xi^2 \in \ker(\phi)$. So $\ker(\phi) = \mu(K) \cdot U_{K^+}$. Note that $\overline{\mu(K)}$ is a cyclic group $\implies \sharp\mu(K)/\mu(K)^2 \leq 2$. ■

6.1.3 Cyclotomic extensions

Let K be a field.

Definition 6.16. $\xi \in K$ is said to be a <u>primitive</u> n-th root of 1 if $\xi^n = 1$ but $\xi^d \neq 1$ for all $d < n$.

Then the n-th roots of 1 in $\mathbb{C}$ are the numbers $e^{\frac{2\pi i m}{n}}$, $0 \leq m \leq n-1$, which is primitive iff $(m, n) = 1$.

Lemma 6.17. *Let ξ be a primitive n-th primitive root of 1. Then ξ^m is primitive iff $(m, n) = 1$.*

Let $K = \mathbb{Q}[\xi]$, where ξ is a primitive n-th root of 1. Then K is the splitting field of $x^n - 1 \implies K$ is Galois over $\mathbb{Q}$.

Denote $\mathcal{G} := \mathrm{Gal}\left(\mathbb{Q}[\xi]/\mathbb{Q}\right)$.

It permutes the set of primitive n-th root of 1 in K.

For any $\sigma \in \mathcal{G}$, $\sigma(\xi) = \xi^m$ for some m with $(m, n) = 1$. The map

$$\begin{aligned} \mathcal{G} &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\longmapsto [m] \end{aligned}$$

is an isomorphism.

Definition 6.18. The <u>cyclotomic polynomial</u> Φ_n is defined by

$$\Phi_n = \prod_{m \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \xi^m) = \prod_{\xi'\text{: primitive } n\text{-th root of } 1} (x - \xi')$$

$\implies x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Proposition 6.19. *TFAE:*

1. *The map $\mathcal{G} \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism;*
2. *$[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(n)$;*
3. *$\mathcal{G}$ acts transitively on the set of primitive n-th roots of 1;*
4. *$\Phi_n(x)$ is irreducible ($\implies$ it is the minimial polynomial of ξ).*

Proof. Easy. ■

We now prove theses statements.

First treat the case $n = p^r$, where p is prime.

Proposition 6.20. *Let ξ be a primitive p^r-th root of 1 with p prime. Then*

1. $[K:\mathbb{Q}] = \varphi(p^r) = p^{r-1}(p-1)$;
2. $\mathcal{O}_K = \mathbb{Z}[\xi]$;
3. $\pi := 1-\xi$ *is a prime element of* $\mathcal{O}_K$ *and* $(p) = (\pi)^e$ *with* $e = \varphi(p^r)$;
4. *The discriminant of* $\mathcal{O}_K$ *over* $\mathbb{Z}$ *is* $\pm p^c$, *where* $c = p^{r-1}(pr - r - 1)$ ($\implies$ (p) *is the only prime to ramify in* $\mathbb{Q}[\xi]$).

Proof. ξ integral $\implies$ $\mathbb{Z}[\xi] \subset \mathcal{O}_K$. If ξ' is another primitive p^r-th root of 1, then $\xi' = \xi^s$ and $\xi = {\xi'}^t$ s.t. $p \nmid s$, $p \nmid t$. $\implies$ $\mathbb{Z}[\xi] = \mathbb{Z}[\xi']$ and $\mathbb{Q}[\xi] = \mathbb{Q}[\xi']$. Moreover,

$$\frac{1-\xi'}{1-\xi} = \frac{1-\xi^s}{1-\xi} = 1 + \xi + \cdots + \xi^{s-1} \in \mathbb{Z}[\xi].$$

$\frac{1-\xi}{1-\xi'} \in \mathbb{Z}[\xi]$ similarly. $\implies$ $\frac{1-\xi'}{1-\xi}$ is a unit of $\mathbb{Z}[\xi]$. Set $t := x^{p^{r-1}}$. Then

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{t^p - 1}{t-1} = 1 + t + \cdots + t^{p-1},$$

and $\Phi_{p^r}(1) = p$. So

$$p = \Phi_{p^r}(1) = \prod (1-\xi') = \prod \frac{1-\xi'}{1-\xi} \cdot (1-\xi) = u \cdot (1-\xi)^{\varphi(p^r)} \tag{6.6}$$

for some unit u in $\mathbb{Z}[\xi]$.

So we get $(p) = (\pi)^e$, for $\pi = 1-\xi$ and $e = \varphi(p^r)$. $\implies$ (p) has $\geq \varphi(p^r)$ prime factors in $\mathcal{O}_K$. As $[\mathbb{Q}[\xi]:\mathbb{Q}] \leq \deg \Phi_{p^r} = \varphi(p^r)$, we get $= \varphi(p^r)$. $\implies$ (1).

Moreover, $\pi \cdot \mathcal{O}_K$ is a prime ideal, otherwise $(p) \cdot \mathcal{O}_K$ has too many prime ideal factors $\implies$ (3).

Then in $\mathcal{O}_K$,

$$(p) = \mathfrak{p}^{\varphi(p^r)}, \quad \mathfrak{p} = (\pi) \text{ prime}, \quad f(\mathfrak{p}/(p)) = 1.$$

We next show (up to sign) $\mathrm{disc}(\mathbb{Z}[\xi]/\mathbb{Z})$ is a power of p.

Since

$$\mathrm{disc}(\mathcal{O}_{\mathbb{Z}}/\mathbb{Z}) \cdot (\mathcal{O}_K : \mathbb{Z}[\xi])^2 = \mathrm{disc}(\mathbb{Z}[\xi]/\mathbb{Z}),$$

this will imply

- $\mathrm{disc}(\mathcal{O}_K/\mathbb{Z})$ is a power of p;
- $(\mathcal{O}_K : \mathbb{Z}[\xi])$ is a power of p $\implies$

$$p^M \mathcal{O}_K \subseteq \mathbb{Z}[\xi] \text{ for some } M. \tag{6.7}$$

We have

$$\operatorname{disc}(\mathbb{Z}[\xi]/\mathbb{Z}) = \pm \operatorname{Nm}_{K/\mathbb{Q}}(\Phi'_{p^r}(\xi)),$$

where

$$(x^{p^{r-1}} - 1) \cdot \Phi_{p^r}(x) = x^{p^r} - 1 \implies \Phi'_{p^r}(\xi)(\xi^{p^r} - 1) = p^r \xi^{p^r - 1} \implies \Phi'_{p^r}(\xi) = \frac{p^r \xi^{p^r-1}}{\xi^{p^{r-1}} - 1},$$

$\operatorname{Nm}_{K/\mathbb{Q}}(\xi) = \pm 1$, $\operatorname{Nm}_{K/\mathbb{Q}}(p^r) = (p^r)^{\varphi(p^r)} = p^{r\varphi(p^r)}$.

Claim: $\operatorname{Nm}_{K/\mathbb{Q}}(1 - \xi^{p^s}) = \pm p^{p^s}$, $\forall\, 0 \le s \le r$.

Proof of Claim. Case $s = 0$:

The minimal polynomial of $(1-\xi)$ is $\Phi_{p^r}(1-x)$. Then constant term is $\Phi_{p^r}(1) = p \implies \operatorname{Nm}_{K/\mathbb{Q}}(1-\xi) = \pm p$.

Case $1 \le s \le r$:

ξ^{p^s} is a primitive p^{r-s}-th root of 1. The $s = 0$ case for $\mathbb{Q}[\xi^{p^s}]/\mathbb{Q}$ implies $\operatorname{Nm}_{\mathbb{Q}[\xi^{p^s}]/\mathbb{Q}}(1-\xi^{p^s}) = \pm p$, $[\mathbb{Q}[\xi^{p^r}] : \mathbb{Q}[\xi^{p^s}]] = \frac{\varphi(p^r)}{\varphi(p^s)} = p^{r-s} \implies$

$$\operatorname{Nm}_{K/\mathbb{Q}}(1 - \xi^{p^s}) = (\pm p)^{[\mathbb{Q}[\xi^{p^r}]:\mathbb{Q}[\xi^{p^s}]]} = (\pm p)^{p^s}.$$

■

Claim $\implies \operatorname{Nm}_{K/\mathbb{Q}}(\Phi'_{p^r}(\xi)) = \pm p^c$, where $c = r(p-1)p^{r-1} - p^{r-1} = p^{r-1}(pr - r - 1) \implies$ (4).

Recall $\mathfrak{p} = (1-\xi) = (\pi)$ and $f(\mathfrak{p}/(p)) = 1$. Then $\mathbb{Z}/(p) \simeq \mathcal{O}_K/(\pi) \implies$ for any m,

$$\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K = \ldots = \mathbb{Z} + \pi\mathbb{Z} + \cdots + \pi^{m-1}\mathbb{Z} + \pi^m\mathcal{O}_K \subseteq \mathbb{Z}[\xi] + \pi^m\mathcal{O}_K.$$

Recall $p = \pi^{\varphi(n)} \times u$ where u is a unit in $\mathbb{Z}[\xi]$, and $p^M\mathcal{O}_K \subseteq \mathbb{Z}[\xi]$. Then by taking m sufficiently large ($m \gg \varphi(n) \cdot M$), we have

$$\mathcal{O}_K \subseteq \mathbb{Z}[\xi] + \pi^m\mathcal{O}_K \subseteq \mathbb{Z}[\xi].$$

$\implies$ (2). ■

6.2 Note on 20251126

Remark 6.21. *Compute the sign of* $\mathrm{disc}(\mathbb{Q}[\xi]/\mathbb{Q})$. *In our case,* $\mathbb{Q}[\xi]$ *has real embedding unless* $\xi = \pm 1$. *So except this trivial case,*

$$\mathrm{sign}(\mathrm{disc}(\mathbb{Q}[\xi]/\mathbb{Q})) = (-1)^s, \quad s = \frac{1}{2}\varphi(n).$$

If ξ *a primitive* p^r*-th root of* 1, *and* $p^r > 2$, *then*

$$[\mathbb{Q}[\xi] : \mathbb{Q}] = \frac{(p-1)p^{r-1}}{2},$$

which is odd iff $p^r = 4$ *or* $p \equiv 3 \mod 4$.

Remark 6.22. *Let* ξ *and* ξ' *be primitive* p^r*-th and* q^r*-th roots of* 1. *If* p *and* q *are distinct primes, then* $K := \mathbb{Q}[\xi] \cap \mathbb{Q}[\xi'] = \mathbb{Q}$. *Since:*

$K \subseteq \mathbb{Q}[\xi] \implies K$ *unramified except* p, *and* $K \subseteq \mathbb{Q}[\xi'] \implies K$ *unramified except* q, *hence* $K/\mathbb{Q}$ *unramified* $\implies K = \mathbb{Q}$.

theorem 6.23. *Let* ξ *be a primitive* n*-th root of* 1.

1. $[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(n)$;
2. $\mathcal{O}_{\mathbb{Q}[\xi]} = \mathbb{Z}[\xi]$, *so* $1, \xi, \ldots, \xi^{\varphi(n)-1}$ *is an integral basis for* $\mathcal{O}_{\mathbb{Q}[\xi]}$ *over* $\mathbb{Z}$;
3. *If* p *ramifies in* $\mathbb{Q}[\xi]$, *then* $p \mid n$. *Moreover, if* $n = p^r \cdot m$, $p \nmid m$, *then*

$$(p) = (\beta_1 \cdots \beta_g)^{\varphi(p^r)} \quad \textit{in} \quad \mathbb{Q}[\xi]$$

with β_i *distinct primes in* $\mathbb{Q}[\xi]$.

Proof. Induction on the number of primes dividing n.

Suppose $n = p^r \cdot m$, p prime, $r \geq 1$ and $p \nmid m$. May assume the theorem holds for m. Let $\xi_{p^r} := \xi^m$ be a primitive p^r-th root of 1, and $\xi_m := \xi^{p^r}$ be a primitive m-th root of 1.

We have $\mathbb{Q}[\xi] = \mathbb{Q}[\xi_{p^r}]\mathbb{Q}[\xi_m]$:

$$\begin{tikzcd}
 & \mathbb{Q}[\xi] & \\
\mathbb{Q}[\xi_{p^r}] \arrow[ur] & & \mathbb{Q}[\xi_m] \arrow[ul] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

(p) ramifies totally in $\mathbb{Q}[\xi_{p^r}]$, so $(p) = \mathfrak{p}^{\varphi(p^r)}$. But (p) unramifies in $\mathbb{Q}[\xi_m]$ by induction hypothesis. Say $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ where $\mathfrak{p}_i$ are distinct prime ideals.

$\mathbb{Q}[\xi] = \mathbb{Q}[\xi_m][\xi_{p^r}] \implies [\mathbb{Q}[\xi] : \mathbb{Q}[\xi_m]] \leq \varphi(p^r)$. Each $\mathfrak{p}_i\mathcal{O}$ is a $\varphi(p^r)$ power ($\mathcal{O} = \mathcal{O}_{\mathbb{Q}[\xi]}$), i.e. $\mathfrak{p}_i\mathcal{O} = \beta_i^{\varphi(p^r)}$, for β_i some ideals in $\mathcal{O}$. Hence, $\mathfrak{p}_i$ ramifies totally in $\mathbb{Q}[\xi]$, i.e. β_i prime $\implies$

$$[\mathbb{Q}[\xi] : \mathbb{Q}] = \varphi(p^r) \cdot \varphi(m) = \varphi(n).$$

$\implies$ (1).

Lemma 6.24. *Let K, L be finite field extensions of $\mathbb{Q}$, s.t.*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}],$$

and let d be the greatest common divisor of $\operatorname{disc}(\mathcal{O}_K/\mathbb{Z})$ *and* $\operatorname{disc}(\mathcal{O}_L/\mathbb{Z})$*. Then*

$$\mathcal{O}_{KL} \subseteq d^{-1}\mathcal{O}_K\mathcal{O}_L.$$

Proof. Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ be integral bases for $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Then $\{\alpha_i\beta_j\}$ is a basis for KL over $\mathbb{Q}$. Thus, $\gamma \in \mathcal{O}_{KL}$ can be written as

$$\gamma = \sum_{i,j} \frac{a_{ij}}{r}\alpha_i\beta_j, \quad r \in \mathbb{Z},$$

with $\frac{a_{i,j}}{r}$ uniquely determined. We may assume $(r, a_{i,j} \forall\, ij) = 1$. We have to show $r \mid d$.

We identify L with a subfield of $\mathbb{C}$. Any embedding $\sigma \colon K \hookrightarrow \mathbb{C}$ extend uniquely to an embedding $KL \hookrightarrow \mathbb{C}$.

To see this, write $K = \mathbb{Q}[\alpha]$. $KL = L[\alpha]$. The hypothesis on the degree $\implies$ the minimal polynomial of α does not change when we pass from $\mathbb{Q}$ to L. So there exists a unique L-homomorphism $L[\alpha] \hookrightarrow \mathbb{C}$ sending α to $\sigma(\alpha)$.

Applying σ to γ, we get

$$\sigma(\gamma) = \sum_{i,j} \frac{a_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Write $x_i = \sum_j \frac{a_{ij}}{r}\beta_j$ and let $\sigma_1, \ldots, \sigma_m$ be the distinct embeddings of K into $\mathbb{C}$. We get m linear equations:

$$\sum_{j=1}^{m} \sigma_k(\alpha_i)x_i = \sigma_k(\gamma), \quad k = 1, \ldots, m.$$

$\implies$

$$(x_1 \ldots, x_m)^T = \Big(\sigma_k(\alpha_i)\Big)^{-1} \cdot (\sigma_1(\gamma), \ldots, \sigma_m(\gamma))^T.$$

Denote $D \coloneqq \det\big(\sigma_k(\alpha_i)\big)$. Then

$$x_i = \frac{D_i}{D}, \quad D_i \in \mathcal{O}_{KL},$$

and $D^2 = \operatorname{disc}(\mathcal{O}_K/\mathbb{Z}) =: \Delta_K \implies$

$$\sum \frac{\Delta_K a_{ij}}{r}\beta_j = \Delta_K x_i = DD_i \in \mathcal{O}_{KL}.$$

$\implies$

$$\frac{\Delta_K a_{ij}}{r} \in \mathbb{Z},\ \forall\, ij \implies r \mid \Delta_K a_{ij},\ \forall\, ij.$$

$\implies$

$$r \mid (a_{ij}\ \forall\, ij)\Delta_K \implies r \mid \Delta_K.$$

Similarly, $r \mid \Delta_L$. So $r \mid (\Delta_K, \Delta_L)$. ■

Back to prove the theorem.

Induction hypothesis and $p \nmid m \implies$ disc($\mathbb{Q}[\xi_{p^r}]$) and disc($\mathbb{Q}[\xi_m]$) are coprime. Lemma 6.24 $\implies$

$$\mathcal{O}_{\mathbb{Q}[\xi]} = \mathcal{O}_{\mathbb{Q}[\xi_{p^r}]}\mathcal{O}_{\mathbb{Q}[\xi_m]} = \mathbb{Z}[\xi_{p^r}]\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi],$$

$\implies$ (2).

Lemma 6.25. *Same setting of Lemma 6.24, i.e.*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}],$$

and assume $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$. Then

$$\operatorname{disc}(KL/\mathbb{Q}) = \operatorname{disc}(K/\mathbb{Q})^{[L:\mathbb{Q}]} \operatorname{disc}(L/\mathbb{Q})^{[K:\mathbb{Q}]}.$$

Proof. Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_n\}$ be integral bases for $\mathcal{O}_K$ and $\mathcal{O}_L$ respectively. Then $\{\alpha_i\beta_j\}$ is a basis for KL over $\mathbb{Q}$.

Let $\{\sigma_1, \ldots, \sigma_m\}$ and $\{\tau_1, \ldots, \tau_n\}$ be the embeddings of $K \hookrightarrow \mathbb{C}$ and $L \hookrightarrow \mathbb{C}$ respectively.

The proof of Lemma 6.24 shows that there exists a unique embedding $\delta_{st} \colon KL \hookrightarrow \mathbb{C}$ s.t. $\delta_{st}|_K = \sigma_s$ and $\delta_{st}|_L = \tau_t$. Those δ_{st} are all embeddings $KL \hookrightarrow \mathbb{C}$.

$$\det\Big(\delta_{st}(\alpha_i\beta_j)\Big) = \det\Big(\sigma_s(\alpha_i)\tau_t(\beta_j)\Big) = \det\Big(M_{tj}\Big),$$

where

$$M_{tj} = \Big(\tau_t(\beta_j)\cdot\sigma_s(\alpha_i)\Big)_{s,i} = \tau_t(\beta_j)\cdot\Big(\sigma_s(\alpha_i)\Big)_{s,i}.$$

Since M_{tj} commutes with each other,

$$\det\Big(M_{tj}\Big) = \det\left(\det\Big(\tau_t(\beta_j)\Big)\cdot\Big(\sigma_s(\alpha_i)\Big)^n\right) = \left(\det\Big(\tau_t(\beta_j)\Big)\right)^m\cdot\left(\det\Big(\sigma_s(\alpha_i)\Big)\right)^n,$$

$\implies$

$$\operatorname{disc}(KL/\mathbb{Q}) = \operatorname{disc}(K/\mathbb{Q})^{[L:\mathbb{Q}]} \operatorname{disc}(L/\mathbb{Q})^{[K:\mathbb{Q}]}.$$

■

$\implies$ (3) by induction. ■

6.3 Note on 20251201

Remark 6.26.
- *Statement (c) of the above Theorem shows that if $p \mid n$, then p ramifies unless $\varphi(p^r) = 1$, i.e. $p^r = 2$. Thus, if $p \mid n$, then p ramifies in $\mathbb{Q}[\xi_n]$ except $p = 2$ and $n = 2\times$ (odd number).*
- *Let $m \in \mathbb{Z}_{>1}$. Then $\varphi(mn) > \varphi(n)$ except n is odd and $m = 2 \implies \mu(\mathbb{Q}[\xi_n])$ is cyclic of order n (generated by ξ_n) except when n is odd, in which case it is cyclic of order $2n$ (generated by $-\xi_n$).*

theorem 6.27 (Kummer). *Let p be an odd prime. If $p \nmid \mathrm{Cl}\left(\mathbb{Q}[\xi_p]\right)$, then there is no nonzero integer solution (x, y, z) to $x^p + y^p = z^p$.*

Remark 6.28. *If $p \nmid \mathrm{Cl}\left(\mathbb{Q}[\xi_p]\right)$, call p a regular prime.*

Proof of Kummer's theorem for the case p relatively prime to xyz. $p = 3$ case: looking modulo 9.

$p = 5$ case: looking modulo 25.

Now assume $p > 5$. We may assume $(x, y) = 1$, i.e. x, y, z relatively prime in pair.

If $x \equiv y \equiv -z \mod p$, then $-2z^p \equiv z^p \mod p \implies 3z^p \equiv 0 \mod p \implies p \mid 3z \implies p \mid z$ contradiction.

Hence, either $x \not\equiv y$ or $x \not\equiv z \mod p$.

After rewriting the equation to $x^p + (-z)^p = (-y)^p$, we may assume $x \not\equiv y \mod p$.

Set $\xi \coloneqq \xi_p$. The roots of $x^p + 1 = 0$ are $-1, -\xi, \ldots, -\xi^{p-1}$. So

$$X^p + 1 = \prod_{i=0}^{p-1} (X + \xi^i) \implies \prod_{i=0}^{p-1} \left(x + \xi^i y\right) = z^p.$$

Let $\mathfrak{p}$ be the unique prime ideal of $\mathbb{Z}[\xi]$ dividing $p \implies$

$$\mathfrak{p} = (1 - \xi^i), \quad \forall\, 1 \le i \le p - 1.$$

Lemma 6.29. *The elements $x + \xi^i y$ of $\mathbb{Z}[\xi]$ are relatively prime in pairs.*

Proof. Assume there exists a prime ideal $\mathfrak{q}$ dividing $x + \xi^i y$ and $x + \xi^j y$, $i \neq j$, $\implies$

$$\mathfrak{q} \mid (\xi^i - \xi^j)y = \mathfrak{p}y$$

and

$$\mathfrak{q} \mid (\xi^j - \xi^i)x = \mathfrak{p}x.$$

Since $(x, y) = 1$, $\mathfrak{q} \mid \mathfrak{p} \implies \mathfrak{q} = \mathfrak{p}$. As $x + y \equiv (x + \xi^i y) + (1 - \xi^i)y$, we have $\mathfrak{p} \mid x + y \implies p \mid x + y$ $\implies z^p \equiv x^p + y^p \equiv x^p + (-y)^p \equiv 0 \mod p$, contradiction. ■

Lemma 6.30. *Any $\alpha \in \mathbb{Z}[\xi]$, $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\xi]$.*

Proof. $\mathbb{Q}[\xi]/\mathbb{Q}$ totally ramifies at $\mathfrak{p} \implies \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}[\xi]/\mathfrak{p}$. So $\alpha = u + v \in \mathbb{Z} + \mathfrak{p}$. Thus,

$$\alpha^p = (u + v)^p = u^p + \sum_{i=1}^{p-1} \binom{p}{i} u^i v^{p-i} + v^p,$$

where $p \mid \binom{p}{i}$ and $v^p \in \mathfrak{p}^p = (p)$. Hence, $\alpha^p \in \mathbb{Z} + p\mathbb{Z}[\xi]$. ■

Lemma 6.31. *Let*

$$\alpha = a_0 + a_1\xi + \cdots + a_{p-1}\xi^{p-1}$$

with $a_i \in \mathbb{Z}$ *and* $a_0 \cdots a_{p-1} = 0$. *If* $\alpha \in n\mathbb{Z}[\xi]$ *for some* $n \in \mathbb{Z}$, *then* $n \mid a_i, \forall i$.

Proof. Since $1 + \xi + \cdots + \xi^{p-1} = 0$, any subset of $\{1, \xi, \ldots, \xi^{p-1}\}$ with $p - 1$ elements will be a $\mathbb{Z}$-basis. This lemma is clear. ■

View

$$\prod_{i=0}^{p-1}(x + \xi^i y) = (z)^p$$

as an equality in $\mathbb{Z}[\xi]$. Then factors in the LHS are relatively prime in pairs. So each one as an ideal is a p-th power, i.e.

$$(x + \xi^i y) = \mathfrak{a}_i^p$$

for some ideal $\mathfrak{a}_i$ in $\mathbb{Z}[\xi]$.

As $p \nmid \mathrm{Cl}\left(\mathbb{Z}[\xi]\right)$, $\mathfrak{a}_i$ is principal. Say $\mathfrak{a}_i = (\alpha_i)$. Take $i = 1$, we have

$$x + \xi y = u \cdot \alpha_1^p, \quad \text{where } u \in \mathbb{Z}[\xi]^\times.$$

Claim $u = \xi^r \cdot v$, where $v = \overline{v}$.

Then Lemma 6.30 implies there exists $a \in \mathbb{Z}$ s.t.

$$\alpha_1^p \equiv a \mod p \implies x + \xi y = \xi^r v \alpha_1^p \equiv \xi^r v a \mod p.$$

$\implies$

$$x + \overline{\xi} y = \xi^{-r} v \overline{\alpha}^p \equiv \xi^{-r} v a \mod p.$$

Then we get

$$\xi^{-r}(x + \xi y) \equiv \xi^r (x + \xi^1 y) \mod p.$$

$\implies$

$$x + \xi y - \xi^{2r} x - \xi^{2r-1} y \equiv 0 \mod p.$$

If $1, \xi, \xi^{2r-1}, \xi^{2r}$ are distinct, then $p \mid x$, contradiction. The only remaining possibilities are

1. $1 = \xi^{2r}$, then
$$\xi y - \xi^{2r-1} y \equiv 0 \mod p \implies p \mid y,$$
contradiction.

2. $1 = \xi^{2r-1} \Leftrightarrow \xi = \xi^{2r}$. Then
$$(x - y) - (x - y)\xi \equiv 0 \mod p \implies p \mid (x - y),$$
contradiction.

3. $\xi = \xi^{2r-1}$. Then
$$x - \xi^2 x = x - \xi^{2r} x \equiv 0 \mod p \implies p \mid x,$$
contradiction.

Proof of Claim. $\xi = \xi_n$, $n > 2$. Set

$$\mathbb{Q}[\xi]^+ \coloneqq \mathbb{Q}[\xi + \xi^{-1}].$$

Under any embedding $\rho\colon \mathbb{Q}[\xi] \hookrightarrow \mathbb{C}$, $\rho(\xi^{-1}) = \overline{\rho(\xi)}$. So $\mathbb{Q}[\xi]^+$ is a totally real field. Then $\mathbb{Q}[\xi]$ is a CM field. Hence, the index of $\mu(\mathbb{Q}[\xi]) \cdot U_{\mathbb{Q}[\xi]^+}$ in $U_{\mathbb{Q}[\xi]}$ is 1 or 2.

Lemma 6.32. *If n is an odd prime power, then any unit $u \in \mathbb{Q}[\xi]$ can be written as $u = \xi \cdot v$, where ξ is a root of 1, and v is a unit in $\mathbb{Q}[\xi]^+$.*

Proof. By contradiction, if the homomophism ($\mu = \mu(\mathbb{Q}[\xi])$)

$$\begin{aligned} U_{\mathbb{Q}[\xi]} &\longrightarrow \mu/\mu^2 \\ u &\longmapsto u/\overline{u} \end{aligned}$$

were surjective, then there exists $u \in U_{\mathbb{Q}[\xi]}$ s.t. $\overline{u} = \beta u$ where β is a root of 1 which is not a square. As n is odd, $\mu = \{\pm 1\} \cdot \langle \xi \rangle$. So $\mu^2 = \langle \xi \rangle \implies \beta = -\xi^m$ for some $m \in \mathbb{Z}$. Let

$$u = a_0 + \cdots + a_{\varphi(n)-1}\xi^{\varphi(n)-1}, \quad a_i \in \mathbb{Z}.$$

Then

$$\overline{u} = a_0 + \cdots + a_{\varphi(n)-1}\overline{\xi}^{\varphi(n)-1}.$$

Modulo the prime $\mathfrak{p} \coloneqq (1-\xi) = (1-\overline{\xi}) \implies$

$$u \equiv a_0 + \cdots a_{\varphi(n)-1} \equiv \overline{u} \mod \mathfrak{p} \implies u \equiv -\xi^m u \equiv -u \mod p,$$

$\implies 2u \in \mathfrak{p} \implies 2 \in \mathfrak{p}$, contradiction. ∎

Lemma $\implies$ Claim. ∎

The proof is complete. ∎

7 Absolute values

DEFINITION 7.1. An absolute value on a field K is a function

$$\begin{aligned} K &\longrightarrow \mathbb{R}_{\geq 0} \\ x &\longmapsto |x| \end{aligned}$$

s.t.

(a) $|x| = 0$ iff $x = 0$;

(b) $|xy| = |x| \cdot |y|$;

(c) $|x + y \leq |x| + |y|$.

If the stronger condition

(c') $|x + y| \leq \max\{|x|, |y|\}$,

holds, the $|\cdot|$ is called non archimedean. An absolute value is called archimedean if it is not non archimedean.

REMARK 7.2. *(a)(b) $\implies$ $|\cdot|\colon K^\times \to (\mathbb{R}_{>0}, \times)$ is a homomophism. $\mathbb{R}_{>0}$ is torsion free $\implies$ $|\mu(K)| = 1$. In particular, $\forall\, x \in K$, $|x| = |-x|$.*

EXAMPLE 7.3. 1. Let K be a field, and $\sigma\colon K \hookrightarrow \mathbb{C}$. Then we get an archimedean absolute value on K by $|x| \coloneqq |\sigma(x)|$.

2. Let $\operatorname{ord}\colon K^\times \to \mathbb{Z}$ be a discrete valuation, then $|a| \coloneqq c^{-\operatorname{ord}(a)}$ for $c > 1$ is a NA absolute value.

   For example, any prime number p, we have the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$:

   $$|a|_p \coloneqq c^{-\operatorname{ord}_p(a)}, \quad c > 1.$$

   Usually we normalize this by taking $c = p$.

   Similarly, any prime ideal $\mathfrak{p}$ in a number field K, we have a normalized $\mathfrak{p}$-adic absolute value

   $$|a|_{\mathfrak{p}} \coloneqq \left(\frac{1}{\mathcal{N}(\mathfrak{p})}\right)^{\operatorname{ord}_{\mathfrak{p}}(a)}.$$

3. On any field K, we define the trivial absolute value: $|a| = 1$, $\forall\, a \neq 0$.

7.0.1 NA absolute value

Recall (c') $|x + y| \leq \max\{|x|, |y|\}$. Then

$$\Big|\sum_{\text{finite}} x_i\Big| \leq \max\{|x_i|\}.$$

PROPOSITION 7.4. *An absolute value $|\cdot|$ is NA iff $|m \cdot 1|$, $m \in \mathbb{Z}$ is bounded.*

Proof. "Only if" trivial.

"If" part: Assume $|m \cdot 1| \leq N$, $\forall\, m \in \mathbb{Z}$. Then

$$|x+y|^n = \Big|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\Big| \leq \sum_{i=0}^{n} \left\{ \Big| \binom{n}{i} \cdot 1 \Big| |x|^i |y|^{n-i} \right\} \leq (n+1)N \cdot \max\{|x|, |y|\}^n$$

for any $n \geq 1 \implies$

$$|x+y| \leq (n+1)^{1/n} N^{1/n} \max\{|x|, |y|\}$$

$\implies$ (c') by $n \to \infty$. ■

7.1 Note on 20251203

Corollary 7.5. *If* char $K \neq 0$*, then any absolute value on K is NA.*

Proposition 7.6. *Let $|\cdot|$ be a non-trivial NA absolute value and put*

$$v(x) := -\log_c |x|, \quad x \neq 0, \quad c > 1,$$

then $v\colon K^\times \to \mathbb{R}$ satisfies the following conditions:

- $v(xy) = v(x) + v(y)$*;*
- $v(x + y) \geq \min\{v(x), v(y)\}$*.*

If $v(K^\times)$ is discrete in $\mathbb{R}$, then v is a multiple of a normalized discrete valuation ord$\colon K^\times \twoheadrightarrow \mathbb{Z} \subset \mathbb{R}$*.*

We say $|\cdot|$ is discrete when $|K^\times|$ is a discrete subgroup of $\mathbb{R}_{>0}$.

Proposition 7.7. *Let $|\cdot|$ be a NA absolute value. Then*

$$A := \{a \in K \mid |a| \leq 1\}$$

is a subring of K, with

$$U := \{a \in K \mid |a| = 1\}$$

the group of units in A and

$$\mathfrak{m} := \{a \in K \mid |a| < 1\}$$

the unique maximal ideal of A.

In particular, $|\cdot|$ is discrete iff A is a DVR.

Example 7.8. Let $R = \mathbb{Q}[t]$ and $r > 0$. Then any $f = \sum_{i \geq 0} a_i t^i \in R$, define

$$|f|_r := \max\{|a_i| r^i\}$$

where $|a_i|$ denotes the p-adic absolute value with $|p| = p^{-1}$. One can check

- $|f|_r = 0$ iff $f = 0$;
- $|f_1 f_2|_r = |f_1|_r \cdot |f_2|_r$.

Hence $|\cdot|_r$ extends to an absolute value on $K = \mathbb{Q}(t) = \operatorname{Frac}\mathbb{Q}[t]$. If $\log_p r \notin \mathbb{Q}$, then $|\cdot|_r$ is not discrete.

An absolute value $|\cdot|$ defines a metric on K with

$$d(a, b) := |a - b|,$$

which induces a topology on K.

Example 7.9. On $(\mathbb{Q}, |\cdot|_p)$, we have $p^n \to 0$ as $n \to \infty$.

Proposition 7.10. *Let $|\cdot|_1$, $|\cdot|_2$ be absolute values on K, and $|\cdot|_1$ nontrivial. Then TFAE:*

1. *$|\cdot|_1$, $|\cdot|_2$ defines the same topology on K;*
2. $|\alpha|_1 < 1 \implies |\alpha|_2 < 1$*;*

3. $|\cdot|_2 = |\cdot|_1^a$ *for some* $a > 0$.

Proof. (1) $\implies$ (2): If $|\alpha|_1 < 1$, then $\alpha^n \to 0 \implies |\alpha|_2 < 1$.

(2) $\implies$ (3): $|\cdot|_1$ nontrivial $\implies \exists x \in K$ with $|x|_1 > 1 \implies |x|_2 > 1$. Let $y \in K^\times$, $m, n \in \mathbb{Z} \setminus \{0\}$. Then

$$\frac{\log |y|_2}{\log |x|_2} < \frac{m}{n} \iff \left|\frac{y^m}{x^n}\right|_2 < 1 \implies \left|\frac{y^m}{x^n}\right|_1 < 1 \iff \frac{\log |y|_1}{\log |x|_1} < \frac{m}{n},$$

$\implies \dfrac{\log |y|_1}{\log |x|_1} = \dfrac{\log |y|_2}{\log |x|_2}$ (replacing y by y^{-1} for the converse inequality). Set $a := \dfrac{\log |x|_2}{\log |x|_1}$, then $\log |y|_2 = a \log |y|_1$.

(3) $\implies$ (1): Clear. ■

Two absolute values are said to be equivalent if they satisfy the above equivalent conditions.

THEOREM 7.11 (Ostrowski). *Let* $|\cdot|$ *be a nontrivial absolute value on* $\mathbb{Q}$.

- *If* $|\cdot|$ *is archimedean, then* $|\cdot|$ *is equivalent to* $|\cdot|_\infty$*;*
- *If* $|\cdot|$ *is NA, then it is equivalent to* $|\cdot|_p$ *for exactly one prime* p.

Proof. Let $m, n \in \mathbb{Q}_{>1}$. Write

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

with $0 \leq a_i \leq n-1$, $a_r \neq 0$. Then $r \leq \dfrac{\log m}{\log n}$, and

$$|a_i| \leq |1| + \cdots |1| = a_i < n. \tag{7.8}$$

Let $N := \max\{1, |n|\}$. Then

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^r \leq \sum_{i=0}^{r} |a_i| N^r \leq (1+r)n \cdot N^r \leq \left(1 + \frac{\log m}{\log n}\right) n \cdot N^{\log m/\log n}, \tag{7.9}$$

and again applying this to m^t, we get

$$|m|^t \leq \left(1 + t\frac{\log m}{\log n}\right) n \cdot N^{t \cdot \log m/\log n}$$

$\implies$

$$|m| \leq \left(1 + t\frac{\log m}{\log n}\right)^{1/t} n^{1/t} \cdot N^{\log m/\log n}.$$

Letting $t \to \infty$, we get

$$|m| \leq N^{\log m/\log n}. \tag{7.10}$$

Case (i) $|n| > 1$ for any $n > 1$.

Then $N = |n| \implies$

$$|m|^{1/\log m} \leq |n|^{1/\log n}, \quad \forall\, m, n > 1.$$

Hence $|n|^{1/\log n} = c$ a constant $\implies$ $|n| = c^{\log n} = n^{\log c}$. Let $a := \log c$. Then

$$|n| = |n|_\infty^a, \quad \forall\, n \in \mathbb{Z}_{>1}.$$

Note that $|\cdot|$ and $|\cdot|_\infty$ are homomophisms $\mathbb{Q}^\times \to \mathbb{R}$ and $\{\mathbb{Z}_{>1}, \pm 1\}$ generates $\mathbb{Q}^\times$ $\implies$ $|\cdot| = |\cdot|_\infty^a$.

Case (ii) $\exists\, n > 1$ s.t. $|n| \leq 1$.

Now $N = 1$. We then have $|m| \leq 1$ for any $m \in \mathbb{Z}$ $\implies$ $|\cdot|$ is NA. Let

$$A := \{x \in \mathbb{Q} \mid |x| \leq 1\}, \quad \mathfrak{m} := \{x \in \mathbb{Q} \mid |x| < 1\}.$$

Then $\mathfrak{m} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and $\mathfrak{m} \cap \mathbb{Z} \neq 0$. Otherwise, $|\cdot|$ is trivial. So $\mathfrak{m} \cap \mathbb{Z} = (p)$ with p prime.

$$|m| = 1 \quad \text{if} \ \ m \in \mathbb{Z},\ p \nmid m.$$

So for any $x \in \mathbb{Q}^\times$, write $x = \dfrac{m}{n} \cdot p^r$, where $m, n \in \mathbb{Z} \setminus \{0\}$, $p \nmid mn$, $r \in \mathbb{Z}$. Then

$$|x| = \frac{|m|}{|n|} \cdot |p|^r = |p|^r.$$

Let $a := -\log_p |p|$. Then $|x| = |x|_p^a$. ■

THEOREM 7.12 (Product formula). *For p a prime or ∞, let $|\cdot|_p$ be the normalized absolute value on $\mathbb{Q}$. Let $|\cdot|_0$ be the trivial absolute value. Then*

$$\prod_p |a|_p = |a|_0, \quad \forall\, a \in \mathbb{Q}.$$

7.1.1 Places of a number field

Let K be a number field.

DEFINITION 7.13. An equivalence class of absolute values on K is called a place of K.

THEOREM 7.14. *There exists exactly one place of K for*

- *any prime ideal $\mathfrak{p}$;*
- *any real embedding;*
- *any conjugate pair of complex embeddings.*

In each equivalence class, we select a normalized "absolute value"

- any $\mathfrak{p}$ prime ideal of $\mathcal{O}_K$,
$$|a|_p := \left(\frac{1}{\mathcal{N}(\mathfrak{p})}\right)^{\operatorname{ord}_\mathfrak{p}(a)};$$
- any real embedding,
$$\sigma \colon K \hookrightarrow \mathbb{R}, \quad |a| := |\sigma(a)|.$$

- any non-real complex embedding

$$\sigma\colon K \hookrightarrow \mathbb{C}, \quad |a| := |\sigma(a)|^2.$$

  (notice that this is not an absolute value, but we ignore it.)

Let v be a place on K a number field.

- If v is from a prime ideal, call v a <u>finite place</u>.
- If v is from a (real or non-real) embedding, call v an <u>infinite (real or complex) place</u>.

Definition 7.15. We write $|\cdot|_v$ for an absolute value in the equivalence class. If $L \supset K$ and w, v are places of L and K respectively s.t. $|\cdot|_w\big|_K$ is equivalent to $|\cdot|_v$, then we say w <u>divides</u> v or w <u>lies</u> over v. Write $w \mid v$.

For finite places, $w \mid v$ means

$$\beta_w \cap \mathcal{O}_K = \mathfrak{p}_v.$$

For infinite place, $w \mid v$ means

$$\sigma_w\colon L \hookrightarrow \mathbb{C} \text{ extends the } \sigma_v \text{ or } \overline{\sigma_v}\colon K \hookrightarrow \mathbb{C}.$$

7.2 Note on 20251215

THEOREM 7.16 (Product formula). *For any place v, let $|\cdot|_v$ be the normalized absolute value. The for any $\alpha \in K^\times$,*

$$\prod_v |\alpha|_v = 1.$$

Proof. Product formula for $\mathbb{Q}$ plus the next result.

LEMMA 7.17. *L/K finite extension:*

(a) Any place on K extends to a finite number of places of L;

(b) Any place v of K and $\alpha \in L^\times$,

$$\prod_{w|v} |\alpha|_w = \left|\mathrm{Nm}_{L/K}(\alpha)\right|_v.$$

Proof. Next part. ∎

∎

7.2.1 The weak approximation theorem

LEMMA 7.18. *If $|\cdot|_1, \ldots, |\cdot|_n$ are distinct inequivalent nontrivial absolute values of K, then there exists $a \in K$ s.t.*

$$\begin{cases} |a|_1 > 1, \\ |a|_i < 1, \quad \forall\, i \neq 1. \end{cases}$$

Proof. First let $n = 2$. Then $|\cdot|_1$ and $|\cdot|_2$ are not equivalent shows that there exist $b, c \in K$ s.t.

$$\begin{cases} |b|_1 < 1, \quad |b|_2 \geq 1; \\ |c|_1 \geq 1, \quad |c|_2 < 1. \end{cases}$$

Take $a \coloneqq \dfrac{c}{b}$.

By induction, assume this lemma holds for $n-1$ absolute values. Then there exists $b, c \in K$ s.t.

$$\begin{cases} |b|_1 > 1, \quad |b|_i < 1, \quad i = 2, \ldots, n-1; \\ |c|_1 > 1, \quad |c|_n < 1. \end{cases}$$

If $|b|_n \leq 1$, set

$$a \coloneqq c \cdot b^r, \quad r \gg 0.$$

If $|b|_n > 1$, set

$$a \coloneqq \frac{c \cdot b^r}{1 + b^r}, \quad r \gg 0.$$

Note

$$\left|\frac{b^r}{1 + b^r}\right| = \begin{cases} 1, & \text{if } |b| > 1; \\ 0, & \text{if } |b| < 1. \end{cases}$$

Easy to check such a is OK. ∎

Lemma 7.19. *Same situation as Lemma 7.18. There exist $a_r \in K$ for $r \geq 0$, s.t.*

$$|a_r|_1 \to 1 \quad \text{and} \quad |a_r|_i \to 0,\ \forall\, i = 2, \ldots, n.$$

Proof. Pick a as in Lemma 7.18. Set

$$a_r \coloneqq \frac{a^r}{1 + a^r}.$$

■

theorem 7.20. *Let $|\cdot|_1, \ldots, |\cdot|_n$ be distinct inequivalent nontrivial absolute values of K, and $a_1, \ldots, a_n \in K$. For any $\varepsilon > 0$, there exists $a \in K$ s.t.*

$$|a - a_i|_i < \varepsilon, \quad \forall\, i = 1, \ldots, n.$$

Proof. By Lemma 7.19, choose b_i, $i = 1, \ldots, n$ s.t.

$$|b_i - 1|_i \approx 0, \quad |b_i|_j \approx 0,\ \forall\, j \neq i.$$

Set

$$a = a_1 b_1 + \cdots + a_n b_n.$$

■

Remark 7.21. *Let $K_i \coloneqq (K, |\cdot|_i)$.*

We have the following diagonal embedding:

$$\tau \colon K \hookrightarrow \prod_{i=1}^{n} K_i.$$

Theorem 7.20 $\implies$ $\tau(K)$ is dense in $\prod_{i=1}^{n} K_i$.

Corollary 7.22. *Let $|\cdot|_1, \ldots, |\cdot|_n$ be distinct inequivalent nontrivial absolute values of K. If*

$$|a|_1^{r_1} \cdots |a|_n^{r_n} = 1, \quad r_i \in \mathbb{R},$$

for any $a \in K^\times$, then $r_i = 0$ for all i.

Proof. Assume $r_i \neq 0$ for all i. Pick $a_i \in K$ with $|a_i|_i^{r_i} > 1$. Then Theorem 7.20 $\implies$ there exists a s.t. $|a - a_i|_i \approx 0$ for all i $\implies$ $|a_i|_i^{r_i} > 1$ for all i $\implies$ $\prod_{i=1}^{n} |a_i|_i^{r_i} > 1$. ■

8 Completions

Let K be a field with an absolute value $|\cdot|$.

Definition 8.1. A sequence a_n of K is called a Cauchy sequence if $\forall\,\varepsilon > 0$, $\exists\, N \geq 0$ s.t.

$$|a_n - a_m| < \varepsilon, \quad \forall\, m, n \geq N.$$

K is called complete if any Cauchy sequence has a limit in K.

Example 8.2.

$$a_n = 1 + 2 + \cdots + 2^n = 2^{n+1} - 1$$

is a Cauchy sequence for $|\cdot|_2$, and $\lim\limits_{n\to\infty} a_n = -1$.

theorem 8.3. *Let K be a field with an absolute value $|\cdot|$. Then there exists a complete valued field $(\widehat{K}, |\cdot|)$ and a homomophism $K \to \widehat{K}$ preserving the absolute value that is universal in the following sense:*

Any homomophism $K \to L$ from K into a complete valued field $(L, |\cdot|)$ preserving the absolute value, extends uniquely to a homomophism $\widehat{K} \to L$.

Proof. Define

$$\widehat{K} \coloneqq \{\text{Cauchy sequence of } K\}/\sim,$$

where $(a_n) \sim (b_n)$ if $|a_n \to b_n| \to 0$.

Check $\widehat{K}$ is a field.

For $a \in \widehat{K}$, defined by a Cauchy sequence $a_n \in K$, define $|a| \coloneqq \lim\limits_{n\to\infty} |a_n|$.

This is well-defined. Check $|\cdot|$ is an absolute value on $\widehat{K}$, and $(\widehat{K}, |\cdot|)$ is complete.

Check the map

$$\begin{aligned} K &\longrightarrow \widehat{K} \\ a &\longmapsto (a, a, \ldots) \end{aligned}$$

is an isometry.

Let $(L, |\cdot|)$ be a complete valued field with an isometry $\phi\colon K \hookrightarrow L$. It extends uniquely to $\widehat{K} \to L$ by

$$(a_n) \longmapsto \lim_{n\to\infty} \phi(a_n).$$

■

Remark 8.4. *$K \to \widehat{K}$ is uniquely determined up to a uniquely isomorphism by the universal property.*

Remark 8.5. *The image of K in $\widehat{K}$ is dense in $\widehat{K}$.*

Any place v of K, write K_v the completion of K w.r.t. v. When v corresponds to a prime ideal $\mathfrak{p}$, we write $K_{\mathfrak{p}}$ for the completion and $\widehat{\mathcal{O}}_{\mathfrak{p}}$ for the ring of integers in $K_{\mathfrak{p}}$.

For example, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ w.r.t. the p-adic absolute value. Write $\mathbb{Z}_p$ (not $\widehat{\mathbb{Z}}_p$) for the ring of integers in $\mathbb{Q}_p$.

8.0.1 Completion for discrete valuation field

Let $|\cdot|$ be a discrete NA absolute value on K, and A the valuation ring. Let $\mathfrak{m}$ be the maximal ideal of A. Write $\mathfrak{m} = (\pi)$, where π is called a local uniformizing parameter. Then

$$|K| = \{c^m \mid m \in \mathbb{Z}\} \cup \{0\},$$

where $c = |\pi| < 1$.

Let $a \in \widehat{K}^\times$ with $a_n \to a$, where $a_n \in K$. Then $|a_n - a| < |a|$ for $n \gg 0 \implies |a_n| = |a|$ for any $n \gg 0$. So $|\widehat{K}| = |K|$ and $|\cdot|$ is a discrete absolute value on $\widehat{K}$.

Let $\operatorname{ord}\colon K^\times \twoheadrightarrow \mathbb{Z}$ be a normalized discrete valuation on K. It extends to a normalized discrete valuation on $\widehat{K}$.

Define $\widehat{A} := \{a \in \widehat{K} \mid |a| \leq 1\}$, which is the closure of A in $\widehat{K}$, and $\widehat{\mathfrak{m}} := \{a \in \widehat{K} \mid |a| < 1\}$ is the maximal ideal of $\widehat{A}$, $= (\pi)$ in $\widehat{A}$, $=$ the closure of $\mathfrak{m}$ in $\widehat{K}$.

Similarly, $\widehat{\mathfrak{m}}^n =$ the closure of $\mathfrak{m}^n$ in $\widehat{K}$ for any $n \geq 1$.

Lemma 8.6. *The map $A/\mathfrak{m}^n \to \widehat{A}/\widehat{\mathfrak{m}}^n$ is an isomorphism.*

Proof. Easy. ■

Proposition 8.7. *Choose a set $S \ni 0$ of representatives for $A/\mathfrak{m}$. The series $\sum a_i \pi^i$ where every $a_i \in S$ and $a_i = 0$ for $i \ll 0$ converges in $\widehat{K}$ and each element of $\widehat{K}$ has a unique representive of the form.*

Proof. Easy. ■

Remark 8.8. *$S \ni 0$ is necessary. For example, let S^* be a set of representatives if $A/\mathfrak{m} \setminus \{0\}$. Let $s_1 \in S^\times$, set $S := S^* \cup \{s_1\pi\}$. Then*

$$0 = (s_1\pi) \cdot \pi^n - (s_1) \cdot \pi^{n+1}, \quad \forall\, n \in \mathbb{Z}.$$

Example 8.9. Any element of $\mathbb{Q}_p$ can be written as

$$\sum a_i p^i, \quad \begin{aligned} &a_i \in \{0, \dots, p-1\}; \\ &a_i = 0, \quad \forall\, i \ll 0. \end{aligned}$$

Proposition 8.10. *We have a natural isomorphism*

$$\widehat{A} \simeq \varprojlim A/\mathfrak{m}^n.$$

Proof. Define

$$\widehat{A} \to \widehat{A}/\widehat{\mathfrak{m}}^n \simeq A/\mathfrak{m}^n.$$

It induces $\widehat{A} \to \varprojlim A/\mathfrak{m}^n$. Define $\varprojlim A/\mathfrak{m}^n \to \widehat{A}$ as follows:

$$\overline{a_n} \in A/\mathfrak{m}^n \quad \text{with} \quad \overline{a_{n+1}} \mod \mathfrak{m}^n = \overline{a_n} \mod \mathfrak{m}^n.$$

Let $a_n \in A$ with $a_n = \overline{a_n} \mod \mathfrak{m}^n$. Then (a_n) is a Cauchy sequence. Define

$$(a_n) \longmapsto \lim_{n\to\infty} a_n \in \widehat{A}.$$

■

8.0.2 Newton's lemma

Let A be a complete discrete valuation ring and π generates its maximal ideal.

PROPOSITION 8.11. *Let $f(x) \in A[x]$ and a_0 be a simple root of $f(x) \mod \pi$. Then there exists a unique root a of $f(x)$ with $a \equiv a_0 \mod \pi$.*

Proof. Let

$$U := \{x \in A \mid x \equiv a_0 \mod \pi\} \simeq \pi \cdot A,$$

a complete metric space. Define

$$\begin{aligned} F\colon U &\longrightarrow U \\ x &\longmapsto x - \frac{f(x)}{f'(x)}. \end{aligned}$$

Since a_0 is a simple root of $f \mod \pi$, we have

$$\begin{cases} f(a_0) = 0 \mod \pi; \\ f'(a_0) \neq 0 \mod \pi. \end{cases}$$

Hence, for any $x \in U$, we have $|f'(x)| = 1$ and $f(x) = 0 \mod \pi \implies F\colon U \to U$.

For $x_1, x_2 \in U$, $x_2 = x_1 + \Delta$ with $|\Delta| \leq |\pi|$. Then

$$f(x_2) = f(x_1) + f'(x_1)\Delta + \varepsilon,$$

where $\varepsilon \in A \cdot \Delta^2 \implies$

$$F(x_2) - F(x_1)| = \left|\Delta - \frac{f'(x_1)\Delta + \varepsilon}{f'(x_1)}\right| = \left|\frac{\varepsilon}{f'(x_1)}\right| \leq |\Delta|^2 \leq |\pi| \cdot |\Delta|,$$

$\implies F\colon U \to U$ is a contraction map $\implies F$ has a unique fixed point. ■

THEOREM 8.12. *Let $f(x) \in A[x]$, and $a_0 \in A$ satisfying $|f(a_0)| < |f'(a_0)|^2$. Then there exists a unique root a of $f(x)$ s.t.*

$$|a - a_0| \leq \left|\frac{f(a_0)}{f'(a_0)^2}\right|.$$

Proof. Newton's method. ■

8.1 Note on 20251217

8.1.1 Hensel's lemma

Let A be a complete discrete valuation ring and $\mathfrak{m}$ its maximal ideal.

THEOREM 8.13 (Hensel's lemma). *Let $k = A/\mathfrak{m}$ be the residue field of K. For $f(x) \in A[x]$, write $\overline{f}(x)$ its image in $k[x]$.*

Consider a monic polynomial $f(x) \in A[x]$. If $\overline{f}(x)$ factors as $\overline{f} = g_0 h_0$ with g_0, h_0 monic and relatively prime in $k[x]$, then f itself factors as $f = gh$ with g and h monic s.t. $\overline{g} = g_0$, $\overline{h} = h_0$.

Moreover, g and h are uniquely determined and $(g, h) = A[x]$ (called strictly coprime).

LEMMA 8.14. *If $f, g \in A[x]$ s.t. $\overline{f}, \overline{g}$ are relatively prime and f is monic, then $(f, g) = A[x]$.*

More precisely, there exist $u, v \in A[x]$ with $\deg u < \deg g$, $\deg v < \deg f$ s.t. $uf + vg = 1$.

Proof. Set
$$M := A[x]\big/(f, g).$$
As f is monic, M is a finitely generated A-mod. As $(\overline{f}, \overline{g}) = k[x]$, we have
$$(f, g) + \mathfrak{m}A[x] = A[x].$$
$\implies \mathfrak{m}M = M$. Nakayama's lemma $\implies M = 0$. Then there exists $u, v \in A[x]$ s.t.
$$uf + vg = 1.$$

If $\deg v \geq \deg f$, write $v = fq + r$ with $\deg r < \deg f \implies$
$$(u + qg)f + rg = 1,$$
where $\deg(u + qg) < \deg g$, and $\deg r < \deg f$. ∎

We next prove the uniqueness.

LEMMA 8.15. *Suppose $f = gh = g'h'$ with g, h, g', h' monic and $\overline{g} = \overline{g'}$, $\overline{h} = \overline{h'}$ with $\overline{g}, \overline{h}$ relatively prime. Then $g = g'$, $h = h'$.*

Proof. Lemma 8.14 implies $(g, h') = A[x] \implies$ there exists $r, s \in A[x]$ s.t. $gr + h's = 1 \implies$
$$g' = g'gr + g'h's = g'gr + ghs \implies g \mid g'.$$
As g, g' same degree and monic, $g = g'$. ∎

Finally, we prove the existence of g and h.

Proof. There exist monic polynomials $g_0, h_0 \in A[x]$ s.t.
$$f - g_0 h_0 \in \pi \cdot A[x],$$
where $\mathfrak{m} = (\pi)$. Suppose we have constructed monic polynomials g_n, h_n s.t.
$$f - g_n h_n \equiv 0 \mod \pi^{n+1},$$

and

$$g_n \equiv g_0 \mod \pi, \qquad h_n \equiv h_0 \mod \pi.$$

We want to find $u, v \in A[x]$ with $\deg u < \deg g_0$ and $\deg v < \deg h_0$, s.t.

$$f - (g_n + \pi^{n+1} u)(h_n + \pi^{n+1} v) \equiv 0 \mod \pi^{n+2},$$

i.e.

$$(f - g_n h_n) - \pi^{n+1}(u h_n + g_n v) \equiv 0 \mod \pi^{n+2}.$$

Since $f - g_n h_n = \pi^{n+1} \cdot r$, where $r \in A[x]$, this is equivalent to

$$r \equiv u h_n + g_n v \mod \pi.$$

Because g_0, h_0 are monic and relatively prime $(h_n, g_n) = A[x]$, by Lemma 8.14 $\implies \exists$ such u, v. ■

Remark 8.16. *Theorem 8.13 implies: A factorization of f into product of relatively prime polynomials in $k[x]$ lifts to a factorization in $A[x]$.*

For example, in $\mathbb{F}_p[x]$, $x^p - x$ splits into p distinct factors, so it also splits in $\mathbb{Z}_p[x] \implies \mathbb{Z}_p$ contains the $(p-1)$-th roots of 1.

More generally, if K has a residue field k with q elements, then K contains q roots of the polynomials $x^q - x$. Let S be the set of these roots, then

$$a \longmapsto \overline{a} \quad : \quad S \longrightarrow k$$

is a bijection preserving multiplication. The elements of S are called the Teichmüller representatives for the elements of the residue field.

8.1.2 Extensions of NA absolute values

Theorem 8.17. *Let K be complete w.r.t. a discrete absolute value $|\cdot|_K$. Let L be a finite separable extension of K of degree n. Then $|\cdot|_K$ extends uniquely to a discrete absolute value $|\cdot|_L$ on L and L is complete for the extended absolute value: $\forall\, b \in L$,*

$$|b|_L = \left| \mathrm{Nm}_{L/K}(b) \right|_K^{1/n}.$$

Proof. Let A be the valuation ring of K, B the integral closure of A in L, and $\mathfrak{p}$ the maximal ideal of A. Then B is a Dedekind domain. Suppose there exist prime ideals $\beta_1 \neq \beta_2$ in B. Then there exists $b \in \beta_1 \setminus \beta_2$.

Let $f(x) \in A[x]$ be the minimal polynomial for b. Then Hensel's lemma implies $\overline{f}(x) = \overline{g}(x)^l$ power of an irreducible polynomial in $k[x]$ where $k = A/\mathfrak{p}$. Both $\beta_1 \cap A[b]$ and $\beta_2 \cap A[b]$ are distinct prime ideals containing $\mathfrak{p} \implies$

$$\beta_1 \cap A[b] \big/ \mathfrak{p}A[b], \quad \beta_2 \cap A[b] \big/ \mathfrak{p}A[b]$$

are distinct prime ideals of

$$A[b] \big/ \mathfrak{p}A[b] = (A/\mathfrak{p})[x] \big/ \left(\overline{g}(x)^l\right) = k[x] \big/ \left(\overline{g}(x)^l\right),$$

which only has one prime ideal $(\overline{g}(x))$. Contradiction. Hence, B has only one prime ideal $\implies B$ is a DVR with a unique prime ideal β.

Therefore, $|\cdot|_K$ extends to a unqiue absolute value $|\cdot|_L$ on L, which cooresponds to β.

Similarly, $|\cdot|_K$ extends unqiuely to an absolute value $|\cdot|_{L'}$ on a Galois closure L' of L. Any $\sigma \in \mathrm{Gal}(L'/K)$ defines an absolute value on L by $b \longmapsto |\sigma(b)|_{L'}$. Uniqueness $\implies |\sigma(b)|_{L'} = |b|_L = |b|_{L'} \implies$

$$\big|\,\mathrm{Nm}(b)\big|_K = \Big|\prod_\sigma \sigma(b)\Big|_{L'} = |b|_L^n \implies |b|_L = \big|\,\mathrm{Nm}_{L/K}(b)\big|^{1/n}.$$

Finally, we show that $(L, |\cdot|_L)$ is complete. Let $e_1, \ldots, e_n$ be a basis of B as A-mod. Assume $\mathfrak{p} = \beta^e$. Consider

$$\begin{aligned} \phi\colon \bigoplus Ke_i &\longrightarrow L \\ (a_i) &\longmapsto \sum a_i e_i \\ \|(a_i)\| \coloneqq \max_i |a_i| & \qquad |\cdot|_L. \end{aligned}$$

Check

- $\bigoplus Ke_i$ is complete;
- ϕ is bounded.

Only need to show: if $\Big|\sum a_i e_i\Big|_L$ is small, then $\max_i |a_i|$ is small.

If $\beta^l \mid b = \sum a_i e_i$, then $\mathfrak{p}^{\lfloor l/e \rfloor} \mid b = \sum a_i e_i \implies \mathfrak{p}^{\lfloor l/e \rfloor} \mid a_i$ for any i.

$\implies (L, |\cdot|_L)$ is complete. ■

Corollary 8.18. *Let Ω be a possibly infinite separable algebraic extension of K, then $|\cdot|_K$ extends uniquely to an absolute value $|\cdot|_\Omega$ on Ω.*

Proof. $\Omega = \bigcup L$, over all L subfields of Ω with L/K finite extension. ■

Remark 8.19. *In this corollary, $|\cdot|_\Omega$ is still NA, but it need not be complete and need not be discrete.*

However, if Ω is algebraically closed, then $\widehat{\Omega}$ is still algebrailly closed.

Example 8.20.

- $\overline{\mathbb{Q}_p}$ is not discrete:

$$|p^{1/n}| = |p|^{1/n} = p^{-1/n} \to 1.$$

- $\overline{\mathbb{Q}_p}$ is complete; $\dim_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}$ countable.

Define $\mathbb{C}_p \coloneqq \widehat{\overline{\mathbb{Q}_p}}$.

Corollary 8.21. *Let K, L as in Theorem 8.17. Then $n = ef$, where $n = [L : K]$, e is the ramification index, and f is the degree of residue field extension.*

When $e = n$, so $\mathfrak{p}B = \beta^n$, we say L is <u>totally ramified</u> over K.

When $f = n$, we say L is <u>unramified</u> over K.

8.2 Note on 20251222

8.2.1 Newton's polygon

Let $(K, |\cdot|)$ be complete, discrete, where $\operatorname{ord}\colon K^\times \to \mathbb{Z}$ is the cooresponding valuation. It extends to a valuation $\operatorname{ord}\colon \overline{K}^\times \to \mathbb{Q}$.

Definition 8.22. For a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in K,$$

define the Newton polygon of $f(x)$ to be the lower convex hull of the set to points

$$P_i \coloneqq \big(i, \operatorname{ord}(a_i)\big), \quad i = 0, \ldots, n.$$

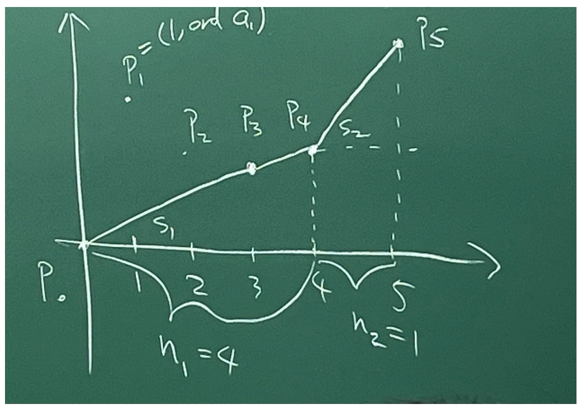

Figure 1: Newton polygon

Proposition 8.23. *Assume* $\operatorname{char} K = 0$. *Suppose that the Newton polygon of* $f(x) \in K[x]$ *has segments of* x*-length* n_i *and slope* s_i. *Then* $f(x)$ *has exactly* n_i *roots* α *in* $\overline{K}$ *with* $\operatorname{ord}(\alpha) = s_i$. *Moreover, the polynomial*

$$f_i(x) = \prod_{\operatorname{ord}(\alpha_i) = s_i} (x - \alpha_i)$$

has coefficients in K.

Proof. For the first part, don't need $f(x)$ has coefficients in K. It suffices to prove the following statement:

Let $f(x) = \prod (x - \alpha_j)$, if exactly n_j of α_j's have order s_j, then the Newton polygon of $f(x)$ has a segment of slope s_j and x-length n_j.

Induction on $n = \deg f$. If $n = 1$, obvious. Assume it holds for n. Let

$$g(x) = (x - \alpha) f(x) = x^{n+1} + b_1 x^n + \cdots + b_{n+1},$$

where $b_i = a_i - \alpha a_{i-1}$.

May assume $\operatorname{ord}\alpha \le s_1$. Then for $i = 1, \ldots, n+1$,

$$\begin{aligned}
\operatorname{ord} b_i &= \operatorname{ord}(a_i - a_{i-1}\alpha) \\
&\ge \min\left\{\operatorname{ord} a_i, \operatorname{ord} a_{i-1} + \operatorname{ord}\alpha\right\} \\
&\ge \min\left\{N(i), N(i-1) + \operatorname{ord}\alpha\right\} \\
&\ge N(i-1) + \operatorname{ord}\alpha.
\end{aligned} \tag{8.11}$$

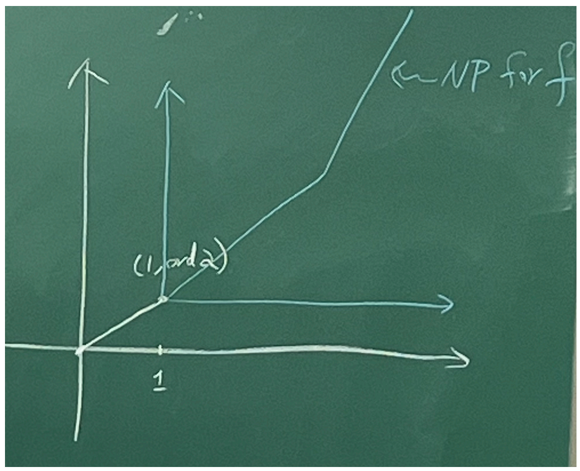

Figure 2: Newton polygons for f and g

For those vertex $i-1$, the "=" in (8.11) holds, i.e. the Newton polygon for g is as Figure 2.
Now prove the second statement.

Let α be any root of $f(x)$ with $\operatorname{ord}\alpha = s_i$. Let $m_\alpha(x)$ be the minimial polynomial of α. Then any root α' of $m_\alpha(x)$ has $\operatorname{ord}\alpha' = s_i \implies m_\alpha(x) \mid f(x) \implies f_i(x)$ has coefficients in K. ■

9 Locally compact field

PROPOSITION 9.1. *Let $(K, |\cdot|)$ be complete, discrete. Let A be the valuation ring of K and $\mathfrak{m}$ the maxiaml ideal of A. Then A is compact iff $A/\mathfrak{m}$ is finite.*

Proof. Let S be the set of representatives for $A/\mathfrak{m}$. Then

$$A = \bigsqcup_{x \in S} (x + \mathfrak{m}),$$

where each $(x + \mathfrak{m})$ is open and nonempty. If A is compact, then $\sharp S < \infty$.

On the other hand,

$$A = \varprojlim_n A/\mathfrak{m}^n \subseteq \prod_{n \geq 1} A/\mathfrak{m}^n,$$

where the last inclusion is a closed embedding. If $A/\mathfrak{m}$ is finite, then every $A/\mathfrak{m}^n$ is finite $\implies$ A is compact. ■

COROLLARY 9.2. *If $A/\mathfrak{m}$ is finite, then $\mathfrak{m}^n$, $1 + \mathfrak{m}^n$ and $A^\times$ are all compact.*

DEFINITION 9.3. A local field is a field K with a nontrivial absolute value $|\cdot|$ s.t. K is locally compact.

Classification of local fields

(a) Archimedean case: $K \simeq \mathbb{C}$ or $\mathbb{R}$;

(b) NA local field of characteristic 0: finite extension of $\mathbb{Q}_p$;

(c) NA for $\operatorname{char} p \neq 0$: isomorphic to the field of formal Laurent series $k((t))$ over a finite field k.

9.0.1 Unramified extensions of a field

Let $(K, |\cdot|)$ be a complete discrete valued field. Assume both K and the residue field k are perfect.

Let L be an algebraic extension of K. We define

- $B := \{\alpha \in L \mid |\alpha| \leq 1\}$;
- $\mathfrak{p} := \{\alpha \in L \mid |\alpha| < 1\}$;
- $l := B/\mathfrak{p}$ the residue field of L.

PROPOSITION 9.4. *There is a one-to-one correspondence:*

$$\begin{aligned} \{K' \subset L, \text{ finite and unramified over } K\} &\longleftrightarrow \{k' \subset l, \text{ finite over } k\} \\ K' &\longleftrightarrow k'. \end{aligned}$$

Moreover,

(a) if $K' \leftrightarrow k'$ and $K'' \leftrightarrow k''$, then $K' \subset K''$ iff $k' \subset k''$;

(b) if $K' \leftrightarrow k'$, then K' Galois over k iff k' is Galois over k, in which case there is a canonical isomorphism

$$\mathrm{Gal}(K'/K) \simeq \mathrm{Gal}(k'/k).$$

Proof. Let k'/k finite extension. Write $k' = k[a]$ for $a \in k' \subset L$. Set $f_0(x)$ to be the minimal polynomial of a over k. Let $f(x)$ be any lifting of $f_0(x)$ in $A[x]$. As a is a simple root of $f_0(x)$ (since K and k are perfect), Newton's lemma shows there exists a **unique** $\alpha \in L$ s.t. $f(\alpha) = 0$ with $\alpha \equiv a \mod \mathfrak{p}$. Then $K[\alpha] \subset L$ is a finite unramified extension over K with residue field $k' \implies K' \to k'$ surjective.

Let $K' \subset L$, K'/K finite unramified with residue field k'. Then

$$[K' : K] = [k' : k]. \tag{9.12}$$

Newton's method implies there exists $\alpha_1 \in K' \subseteq L$ s.t. $f(\alpha_1) = 0$ and $\alpha_1 \equiv \alpha \mod \mathfrak{p} \implies \alpha_1 = \alpha \implies K' \supset K[\alpha]$. By (9.12), $[K' : K] = [k' : k] = [K(\alpha) : K] \implies K' = K[\alpha] \implies$ injective.

(a): $K' \subset K'' \implies k' \subset k''$. Assume $k' \subset k''$. Then there exists a unique $K''' \subset K''$ with $k''' = k'$. Since both K''' and $K' \subset L$, the uniqueness implies $K''' = K' \implies K' \subset K'' \implies$ (a) holds.

(b): Assume K'/K Galois. Since $\mathrm{Gal}(K'/K)$ preserves the valuation ring A' in K' and the maximal ideal, we get $\mathrm{Gal}(K'/K) \to \mathrm{Aut}(k'/k)$. Write $k' = k[a]$ with $g(x) \in A[x]$ s.t. $\overline{g}(x) \in k[x]$ is the minimal polynomial of $a \implies g$ is irreducible.

Let $\alpha \in A'$ be the unique root of $g(x)$ s.t. $\overline{\alpha} = a$. Then K'/K Galois $\implies g(x)$ splits in K' $\implies \overline{g}(x)$ splits in $k' \implies k'$ Galois over k. Let $f = [k' : k] = [K' : K]$, and let $\alpha_1, \ldots, \alpha_f$ be the roots of $g(x)$. Then

$$\{\alpha_1, \ldots, \alpha_f\} = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(K'/K)\}.$$

As $\overline{g}(x)$ is separable, $\alpha_i \mod \mathfrak{p}$ are distinct $\implies$ the image of $\mathrm{Gal}(K'/K)$ in $\mathrm{Gal}(k'/k)$ has order f. So $\mathrm{Gal}(K'/K) \to \mathrm{Gal}(k'/k)$ is an isomorphism.

Conversely, if k'/k is Galois, write $k' = k[a]$ and $\alpha \in A'$ lifts a. The formal proof shows $K' = K[\alpha]$. Hensel's lemma $\implies A'$ contains the conjugates of $a \implies K'$ is Galois over K. ■

Corollary 9.5. *There exists an unramified extension K_0 of K contained in L that contains all unramified extension of K in L.*

When K is finite, it is obtained from K by adjoining all roots of 1 of order prime to $\mathrm{char}\, k$.

Corollary 9.6. *The residue field of $\overline{K}$ is $\overline{k}$. There exists a subfield K^{un} of $\overline{K}$ s.t. a subsfield L of $\overline{K}$ finite over K is unramified iff $L \subset K^{\mathrm{un}}$.*

9.1 Note on 20251224

9.1.1 Totally ramified extension of K

Let $(K, |\cdot|)$ be a complete discrete valued field, and π the local uniformizing parameter of K.

DEFINITION 9.7. A polynomial $f(x) \in K[x]$ is called Eisenstein if it is Eisenstein for (π), i.e.

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

with

$$\operatorname{ord} a_0 = 0, \quad \operatorname{ord} a_i > 0 \text{ for } a_i > 0, \quad \operatorname{ord} a_n = 1,$$

$\iff |a_0| = 1$, $|a_i| < 1$, $|a_n| = |\pi| \iff$ the Newton polygon is as follows:

PROPOSITION 9.8. *L/K finite extension of K. Then L/K is totally ramified iff $L = K[\alpha]$ with α a root of an Eisenstein polynomial.*

Proof. $\Leftarrow$: $L = K[\alpha]$ with α a root of an Eisenstein polynomial $f(x)$ of degree n. Extend ord from K to L. Then $\operatorname{ord}(\alpha) = \frac{1}{n} \implies$ the ramification index of $L/K \geq n$. $[L : K] = n \implies$ totally ramified.

$\Rightarrow$: L totally ramified over K. Let α be a generator of the maximal ideal of $\mathcal{O}_L$. Then $\operatorname{ord} \alpha = \frac{1}{n}$. The elements $1, \alpha, \ldots, \alpha^{n-1}$ represent different cosets of $\operatorname{ord}(K^\times)$ in $\operatorname{ord}(L^\times)$, i.e.

$$\operatorname{ord}(L^\times) \Big/ \operatorname{ord}(K^\times) = \frac{1}{n}\mathbb{Z} \Big/ \mathbb{Z}.$$

$\implies 1, \ldots, \alpha^{n-1}$ are K-linearly independent $\implies$ they are K-basis of $L \implies L = K[\alpha]$, we have a relation

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_n = 0, \quad a_i \in K.$$

There exist at least two terms having minimal order. Note that

$$1 = \operatorname{ord}(\alpha^n) \equiv \operatorname{ord}(a_n) \text{ in } \operatorname{ord} L / \operatorname{ord} K = \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

and $\operatorname{ord}(a_1 \alpha^{n-1}), \ldots, \operatorname{ord}(a_n)$ differ from each other in $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. This happens only if $1 = \operatorname{ord}(\alpha^n) = \operatorname{ord}(a_n)$, and $\operatorname{ord}(a_i \alpha^i) \geq 1$ for all $i = 1, \ldots, n-1$. That is, the polynomial $x^n + a_1 x^{n-1} + \cdots + a_n$ is Eisenstein. ∎

REMARK 9.9. *Let L/K be a finite totally ramified extension, and A, B the valuation rings for K, L. Let π, Π be prime elements in A, B. Then $B = A[\Pi]$.*

Proof. B, A have the same residue field $\implies B/(\Pi) = A/(\pi) \implies$

$$B = A + \Pi B = A + \Pi(A + \Pi B) = \ldots = A[\Pi] + \Pi^m B, \quad \forall m \geq 1.$$

The discriminant of $1, \Pi, \ldots, \Pi^{n-1}$ equals to a unit times π^l for some $l \geq 0 \implies \Pi^c B \subset A[\Pi] \subset B$. Pick $m = c$, $A[\pi] \supset A[\Pi] + \Pi^c B = B$. ∎

9.1.2 Ramification groups

Let L/K be a finite Galois extension. Assume the residue field k of K is perfect. Then $\mathcal{G} \coloneqq \mathrm{Gal}(L/K)$ preserves the absolute value on $L \implies$ it preserves

$$B = \{\alpha \in L \mid |\alpha| \leq 1\}$$
$$\mathfrak{p} = \{\alpha \in L \mid |\alpha| < 1\}.$$

Write $\mathfrak{p} = (\Pi)$. We define a sequence of subgroups

$$\mathcal{G} \supset \mathcal{G}_0 \supset \mathcal{G}_1 \supset \dots$$

by the condition

$$\sigma \in \mathcal{G}_i \iff |\sigma(\alpha) - \alpha| < |\Pi|^i, \quad \forall\, \alpha \in B.$$

Definition 9.10. We call

- $\mathcal{G}_0$ the inertia group;
- $\mathcal{G}_1$ the ramification group;
- $\mathcal{G}_i$, $i > 1$ the higher ramification groups of L over K.

Lemma 9.11. *The $\mathcal{G}_i$ are normal subgroups of $\mathcal{G}$ and $\mathcal{G}_i = \{1\}$ for $i \gg 0$.*

Proof. Easy. ∎

theorem 9.12. *Let L/K be a Galois extension. Assume the residue field extension l/k is separable.*

(a) The fixed field of $\mathcal{G}_0$ is the largest unramified extension K_0 of K in L and

$$\mathcal{G}/\mathcal{G}_0 = \mathrm{Gal}(K_0/K) = \mathrm{Gal}(l/k).$$

(b) For any $i \geq 1$, we have

$$\mathcal{G}_i = \{\sigma \in \mathcal{G}_0 \mid |\sigma\Pi - \Pi| < |\Pi|^i\}.$$

Proof. (a): Let K_0 be the largest unramified extension in L. Then $\sigma(K_0)$ is also unramified $\implies \sigma(K_0) \subset K_0 \implies K_0/K$ Galois.

$$\mathrm{Gal}(K_0/K) \longrightarrow \mathrm{Gal}(l/k)$$

is an isomorphism, and $\mathcal{G}_0 = \ker\big(\mathcal{G} \longrightarrow \mathrm{Gal}(l/k)\big) \implies K_0 = L^{\mathcal{G}_0}$.

(b): Let A_0 be the valuation ring of K_0. Then $B = A[\Pi]$. Since $\mathcal{G}_0$ leaves A_0 fixed, $\sigma \in \mathcal{G}_i$ iff $|\sigma(\Pi) - \Pi| < |\Pi^i|$. ∎

Corollary 9.13. *We have an exhaustive filtration $\mathcal{G} \supset \mathcal{G}_0 \supset \dots$ s.t.*

- $\mathcal{G}/\mathcal{G}_0 = \mathrm{Gal}(l/k)$*;*
- $\mathcal{G}_0/\mathcal{G}_1 \hookrightarrow l^\times$*;*
- $\mathcal{G}_i/\mathcal{G}_{i+1} \hookrightarrow l$, $i \geq 1$.

Therefore, if k is finite, $\mathrm{Gal}(L/K)$ *is solvable.*

Proof. Let $\sigma \in \mathcal{G}_0$, then $\sigma(\Pi)$ is a prime element $\implies$ $\sigma(\Pi) = u\Pi$ where $u \in B^\times$. The map

$$\sigma \longmapsto u \mod \Pi$$

is a homomophism $\mathcal{G}_0 \longrightarrow l^\times$ with kernel $\mathcal{G}_1$.

Let $\sigma \in \mathcal{G}_i$, $i \geq 1$, then $|\sigma(\Pi) - \Pi| \leq |\Pi|^{i+1} \implies \sigma(\Pi) = \Pi + a\Pi^{i+1}$ for some $a \in B$. THe map

$$\sigma \longmapsto a \mod \mathfrak{p}$$

is a homomophism $\mathcal{G}_i \longrightarrow l$ with kernel $\mathcal{G}_{i+1}$. ■

Definition 9.14. An extension L/K is said to be widely ramified if $p \mid e$ where $p = \operatorname{char} k$. Otherwise, it is said to be tamely ramified.

Hence, for a Galois extension L/K,

$$L/K \text{ unramified } \iff \mathcal{G}_0 = \{1\},$$

and

$$L/K \text{ tamely ramified } \iff \mathcal{G}_1 = \{1\}.$$

9.1.3 Krasner's lemma

Let $(K, |\cdot|)$ be complete discrete. Extend $|\cdot|$ to an absolute value on $\overline{K}$.

Proposition 9.15 (Krasner's lemma). *Let $\alpha, \beta \in \overline{K}$ and assume α is separable over $K[\beta]$. If α is closer to β than to any other conjugate of α (over K), then $K[\alpha] \subset K[\beta]$.*

Proof. See Milne p.132. ■

Now assume $\operatorname{char} K = 0$. For $h(x) = \sum c_i x^i$, define $\|h\| := \max\{|c_i|\}$. If $h(x)$ monic,

$$h(x) = x^n + \sum_{i=0}^{n-1} c_i x^i.$$

Let α be any root of $h(x)$ $|\alpha| \leq \|h\|$.

Fix a monic irreducible polynomial $f(x)$ in $K[x]$. Let $g(x)$ be another irreducible polynomial and suppose $\|f - g\|$ is small. For any root β of $g(x)$, $|f(\beta) = |(f-g)(\beta)|$ is small. Write $f(\beta) = \prod(\beta - \alpha_i)$ where α_i are roots of f $\implies$ may assume

$$|\beta - \alpha_1| \leq |f(\beta)|^{1/n}.$$

For $\|f - g\|$ small enough,

$$|f(\beta)| < \left(\min_{i \neq 1} |\alpha_i - \alpha_1|\right)^n$$

$\implies$ $|\beta - \alpha_1| < |\alpha_1 - \alpha_i|$ for $i \neq 1$ (called β belongs to α_1. Now Krasner's lemma implies $K[\alpha_1] \subset K[\beta]$.

If $\deg f = \deg g$, then $K[\alpha_1] = k[\beta]$.

Proposition 9.16. *Let $f(x)$ be a monic irreducible polynomial of $K[x]$. Then any monic polynomial $g(x) \in K[x]$ sufficiently close to $f(x)$ is also irreducible, and each root β of $g(x)$ belongs to some root α of $f(x)$. We have $K[\alpha] = K[\beta]$.*