Algebraic Number Theory

read by Prof. Dr. Werner Bley

notes by Stefan Albrecht

Ludwig-Maximilians-Universität München – winter term 2025/26

Contents

0 Motivation

Lecture 1
Oct 15, 2025

Theorem 0.1 (Lagrange). *Let p be an odd prime. Then*

$$p = x^2 + y^2 \text{ with } x, y \in \mathbb{Z} \text{ if and only if } p \equiv 1 \bmod 4.$$

Proof. For any integer x we have $x^2 \equiv 0, 1 \bmod 4$, hence $x^2 + y^2 \equiv 0, 1$ or $2 \bmod 4$ for all $x, y \in \mathbb{Z}$, hence $p \not\equiv 3 \bmod 4$.

Conversely, assume that $p \equiv 1 \bmod 4$. Then $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, so there exists some $\overline{m} \in \mathbb{F}_p^\times$ of order 4. Thus there is $m \in \mathbb{Z}$ with $m^2 \equiv -1 \bmod p$, i.e. $p \mid m^2 + 1 = (m+i)(m-i) \in \mathbb{Z}[i]$. Since the Gaussian integers form a Euclidean ring, it is in particular a PID.

Consider its norm $N : \mathbb{Z}[i] \to \mathbb{Z}$, $\alpha = a + bi \mapsto \alpha\overline{\alpha} = a^2 + b^2$, which is a multiplicative function. Suppose that $p \mid m + i$. Then $p \mid m - i$ as well, hence $p \mid 2i$, which is clearly wrong. Hence p is not a prime element in $\mathbb{Z}[i]$. Since we are in a PID, p is reducible in $\mathbb{Z}[i]$, i.e. there exist non-units $\alpha = x + yi, \beta = x' + y'i \in \mathbb{Z}[i]$ such that $p = \alpha\beta$. Now we see $p^2 = N(\alpha)N(\beta) = (x^2 + y^2)(x'^2 + y'^2)$. Since α, β aren't units, each factor is > 1, hence $p = x^2 + y^2 = x'^2 + y'^2$. □

Definition 0.2. A finite extension K of $\mathbb{Q}$ is called a *number field*.

Example 0.3. $\mathbb{Q}(i)$ is a number field of degree 2. In the above example, we worked in $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$. We want to generalize this.

Definition 0.4. Let $K/\mathbb{Q}$ be a number field. Then

$$\mathcal{O}_K := \{\alpha \in K \mid \exists f \in \mathbb{Z}[x] \text{ normalized s.t. } f(\alpha) = 0\},$$

i.e. the integral closure of $\mathbb{Z}$ in K, is called the *ring of integers* in K.

We will show: $\mathcal{O}_K$ is a Dedekind domain.

Example 0.5.
(i) For $K = \mathbb{Q}(i)$ we have $\mathcal{O}_K = \mathbb{Z}[i]$
(ii) For $K = \mathbb{Q}(\sqrt{2})$ one gets $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$
(iii) For $K = \mathbb{Q}(\sqrt{-6})$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$
(iv) (Exercise) More generally, for $d \in \mathbb{Z} \setminus \{0, 1\}$ squarefree, the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\omega]$, where
$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \bmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Theorem 0.6. *Let p be an odd prime. Then*

$$p = x^2 - 2y^2 \text{ with } x, y \in \mathbb{Z} \text{ if and only if } p \equiv \pm 1 \bmod 8.$$

Proof. The forward direction follows as in the first theorem. For the converse, we work in $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Q}(\sqrt{2})$. Consider the norm $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$, $\alpha = x + y\sqrt{2} \mapsto \alpha\sigma(\alpha) = x^2 - 2y^2$, where $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}) = \langle\sigma\rangle$. We will see later (Quadratic Reciprocity) that $p \equiv \pm 1 \bmod 8$ is equivalent to $(\frac{2}{p}) = 1$, i.e. 2 being a square $\mathrm{mod} p$.

Hence there exists $m \in \mathbb{Z}$ with $p \mid m^2 - 2 = (m - \sqrt{2})(m + \sqrt{2})$. As before, we see that p is not prime, hence reducbile ($\mathbb{Z}[\sqrt{2}]$ is again Euclidean) and we finish as before. □

The main difference between theorems 0.1 and 0.6 is that the unit group of $\mathbb{Z}[i]$ is finite, while $\mathbb{Z}[\sqrt{2}]^\times = \{\pm 1\} \times (1+\sqrt{2})^{\mathbb{Z}}$ is infinite[1]. This implies that $p = x^2 - 2y^2$ has infinitely many solutions for $p \equiv \pm 1 \bmod 8$, for $N((1+\sqrt{2})^{2k}\alpha) = N(\alpha)$ for all $k \in \mathbb{Z}$.

In this vein, an important goal of this lecture is

Theorem 0.7 (Dirichlet's unit theorem). *Let $K/\mathbb{Q}$ be a number field. Let s be the number of real embeddings and let t be the number of pairs of complex embeddings of K. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r = s + t - 1$, i.e. there exist* fundamental units *$\varepsilon_1, \dots, \varepsilon_r$ and $\zeta \in \mu_K = \{$roots of unity in $K\}$ such that each $\varepsilon \in \mathcal{O}_K^\times$ can be uniquely written in the form*

$$\varepsilon = \zeta^l \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$$

with $a_i \in \mathbb{Z}$ and $l \in \mathbb{Z}/\operatorname{ord}(\zeta)\mathbb{Z}$.

Example 0.8. For $K = \mathbb{Q}(\sqrt{2})$ we have $\mu_K = \{\pm 1\}$, $\varepsilon_1 = 1 + \sqrt{2}$ and $r = 2 + 0 - 1 = 1$, since both embeddings $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{2} \mapsto -\sqrt{2}$ are real.

Let $K/\mathbb{Q}$ be a number field. We choose the algebraic closure $\mathbb{Q}^c$ of $\mathbb{Q}$ that sits inside of $\mathbb{C}$, so we may, and will, always assume $K \subseteq \mathbb{C}$. $K/\mathbb{Q}$ is separable, so we may write $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$. Let $f \in \mathbb{Q}(\alpha)$ be the minimal polynomial of α. Then we have embeddings $\sigma : K \hookrightarrow \mathbb{C}$ corresponding to the zeroes $\alpha = \alpha_1, \dots, \alpha_n$ of f, i.e. the conjugates of α. σ is called a real embedding if $\sigma(K) \subseteq \mathbb{R}$, or equivalently if the corresponding $\alpha_i \in \mathbb{R}$. Otherwise it is called a complex embedding. These come in pairs, because if α_i is a conjugate of α, so is $\overline{\alpha_i}$.

Example 0.9. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. If $d > 0$ we find as before that $s = 2, t = 0$, so $r = 1$. If, on the other hand, $d < 0$, then $s = 0, t = 1$, hence $r = 0$ and $\mathcal{O}_K^\times$ is finite.

Question Which odd primes p can be written in the form $p = x^2 + 6y^2$ with $x, y \in \mathbb{Z}$? As in the previous theorems, we write this as $(x + y\sqrt{-6})(x - y\sqrt{-6}) = N(x + y\sqrt{-6})$ in the number field $K = \mathbb{Q}(\sqrt{-6})$ with ring of integers $\mathbb{Z}[\sqrt{-6}]$. However, our previous proof strategy does *not* work, because $\mathbb{Z}[\sqrt{-6}]$ is not a PID (e.g. $2 \cdot 3 = -\sqrt{-6} \cdot \sqrt{-6}$ are two essentially different factorizations of 6 into irreducibles).

This leads naturally to the question when $\mathcal{O}_K$ is a PID. To investigate this, we will introduce the *class group*: The nonzero ideals of $\mathcal{O}_K$ form a monoid w.r.t. multiplication.

Definition 0.10. Write I_K for the group of fractional nonzero ideals and $P_K = \{\alpha\mathcal{O}_K \mid \alpha \in K^\times\}$ the subgroup of principal fractional ideals. The quotient $\mathrm{cl}_K = I_K/P_K$ is called the *ideal class group*

One sees directly that $\mathrm{cl}_K = 1$ if and only if $\mathcal{O}_K$ is a PID. We will prove

Theorem 0.11. $|\mathrm{cl}_K| < \infty$.

In any case $\mathcal{O}_K$ is Dedekind, which is equivalent to prime factorization of *ideals*, i.e. each ideal $(0) \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K$ can be uniquely written as a product of prime ideals

$$\mathfrak{a} = \prod_{\substack{\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K) \\ \mathfrak{p} \neq 0}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}, \qquad v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}_{\geq 0}, \text{ almost all } v_\mathfrak{p}(\mathfrak{a}) = 0.$$

[1] $\supseteq$ is easy by direct computation, which is all we use here. We will see how to prove $\subseteq$ later.

Example 0.12. In $\mathbb{Z}[\sqrt{-6}]$ we have $2\mathcal{O}_K = \mathfrak{p}_2^2$ with $\mathfrak{P}_2 = \langle 2, \sqrt{-6}\rangle_{\mathbb{Z}}$, $3\mathcal{O}_K = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = \langle 3, \sqrt{-6}\rangle_{\mathbb{Z}}$ and $\sqrt{-6}\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_3$, so the "problematic" factorization $2 \cdot 3 = -\sqrt{-6}^2$ becomes $\mathfrak{p}_2^2\mathfrak{p}_3^2 = (\mathfrak{p}_2\mathfrak{p}_3)^2$ when passing to ideals.

Given an extension of number fields L/K, and a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, by the above the ideal $\mathfrak{p}\mathcal{O}_L$ splits into a product of prime ideals $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ in $\mathcal{O}_L$. A further goal of this lecture is to understand and compute this factorization. Denoting $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, we will for example be able to show $[L : K] = \sum_{i=1}^r e_i f_i$.

Definition 0.13. Let p be a prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then the *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution in } \mathbb{Z}, \\ -1 & \text{otherwise.} \end{cases}$$

Also set $(\frac{a}{p}) = 0$ if $p \mid a$.

We will show: Let $K = \mathbb{Q}(\sqrt{d})$. Let $p \neq 2$. Then

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}} \text{ prime} & \text{if } (\frac{d}{p}) = 1, \\ \mathfrak{p},\ \mathfrak{p} \text{ prime} & \text{if } (\frac{d}{p}) = -1, \\ \mathfrak{p}^2,\ \mathfrak{p} \text{ prime} & \text{if } p \mid d. \end{cases} \tag{$*$}$$

Law of quadratic reciprocity Let p, q be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \text{ and } q \equiv 3 \bmod 4 \end{cases}.$$

Further, we have the two supplements $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ and $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. This theorem allows quick computation of Legendre symbols.

Lecture 2
Oct 17, 2025

Using the above, we will be able to generalize the theorems from the beginning:

Corollary 0.14. *Let d be a squarefree integer. A prime $p \neq 2$ can be written in the form $p = x^2 - dy^2$ for $x, y \in \mathbb{Z}$ if and only if $(\frac{d}{p}) = 1$ and $\mathfrak{p}$ is a principal ideal, where $\mathfrak{p}$ is as in $(*)$.*

1 Integrality

Rings are always commutative and contain a multiplicative unit, unless explicitly stated otherwise.

Definition 1.1. Let $A \subseteq B$ be a ring extension. An element $b \in B$ is *integral* over A if there exists a normalized polynomial $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1X + a_0 \in A[X]$ such that $f(b) = 0$. B is *integral* over A if every $b \in B$ is integral over A.

Example 1.2. Let K be a number field. Then $\mathcal{O}_K$ is integral (over $\mathbb{Z}$).
If B/A is a field extension, then B is integral over A if and only if B is algebraic over A.

We want to show that the set of all integral elements form a ring, i.e. that given integral elements $b_1, b_2 \in B$, $b_1 + b_2$ and b_1b_2 are integral as well.

Theorem 1.3. *Let $b_1, \ldots, b_n \in B$. Then $b_1, \ldots, b_n$ are integral over A if and only if $A[b_1, \ldots, b_n]$ is a finitely generated A-module.*

Proof. "$\Rightarrow$": By induction. For $n = 1$ let $b \in B$ be integral over A. Let $f(b) = 0$. Then $b^m = -\sum_{i=0}^{m-1} a_ib^i$, so $A[b]$ is generated by $1, b, \ldots, b^{m-1}$ as a A-module.
More explicitly: Let $g(b) \in A[b]$ be some element. Since f is normalized, we can perform division with remainder to write $g = qf + r$ with $q, r \in A[x]$ with $\deg(r) < m$. Hence $g(b) = q(b)f(b) + r(b) = r(b)$, which is a linear combination of b^i, $i < m$.
For the inductive step, we have to prove that $A \subseteq A[b_1, \ldots, b_n] \subseteq A[b_1, \ldots, b_{n+1}]$ is finitely generated, knowing that the first extension is finitely generated. Since b_{n+1} is integral over A, it is also finitely generated over $A[b_1, \ldots, b_n]$, hence $A[b_1, \ldots, b_n] \subseteq A[b_1, \ldots, b_{n+1}]$ is finitely generated by the $n = 1$ case, hence we are done.
"$\Leftarrow$": Let $\omega_1, \ldots, \omega_r$ be a set of A-generators of $A[b_1, \ldots, b_n]$. For $b \in A[b_1, \ldots, b_n]$ we have

$$b\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j \qquad \text{with } a_{ij} \in A.$$

Hence $(bE - M)(\omega_1, \ldots, \omega_r)^t = 0$, where $M = (a_{ij})_{ij} \in A^{r\times r}$. By cofactor expansion, see lemma 1.4, this implies that $\det(bE - M)\omega_i = 0$ for all $i = 1, \ldots, r$, hence $\det(bE - M) = 0$ since the ω_i generate $A[b_1, \ldots, b_n]$. Hence $\det(XE - M) \in A[X]$ is a normalized equation for b, i.e. b is integral over A. □

Lemma 1.4. *Let A a ring and $M \in A^{r\times r}$. If $Mx = 0$, then $\det(M)x = 0$.*

Proof. Let M^* be the adjoint matrix, i.e. $(M^*)_{ij}$ is $(-1)^{i+j}$ times the determinant of the matrix M with the j-th row and i-th column removed. Then $M^*M = MM^* = \det(M)E$. From $Mx = 0$ we then get $0 = M^*Mx = \det(M)x$. □

Example 1.5. $K = \mathbb{Q}(\sqrt{2}) \supseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. Proceeding as in the proof, we can compute an integral equation for, say, $\alpha = 1 + 2\sqrt{2}$: Take $\omega_1 = 1$, $\omega_2 = \sqrt{2}$. Consider

$$T_\alpha : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}], \qquad x \mapsto \alpha x,$$

which has matrix representation w.r.t. the ω_i as $M = \left(\begin{smallmatrix} 1 & 2 \\ 4 & 1 \end{smallmatrix}\right)$. Now $\det(XE - M) = X^2 - 2X - 7$ is the desired relation.

In the exercises, we will show the following slight generalization of proposition 1.3.

Proposition 1.6. *Let A be a ring. Then the following are equivalent:*

(i) *b is integral over A.*

(ii) *$A[b]$ is finitely generated as an A-module.*

(iii) *There exists an $A[b]$-module M that is finitely generated as an A-module.*

Theorem 1.7. *Let $A \subseteq B \subseteq C$ be extensions of rings. Let B/A be integral and let $c \in C$ be integral over B. Then c is also integral over A.*

Proof. Let $c^n + b_{n-1}c^{n-1} + \ldots + b_0$ with $b_i \in B$. Then $A \subseteq A[b_0, \ldots, b_{n-1}] \subseteq A[b_0, \ldots, b_{n-1}][c]$ is a composition of finitely generated ring extensions by theorem 1.3, hence finitely generated. Again by theorem 1.3, we are done. □

Definition 1.8. Let $A \subseteq B$ be a ring extension.

(a) Then $\overline{A} = \mathcal{O}_{A,B} := \{b \in B \mid b \text{ integral over } A\}$ is called the *integral closure* of A in B.

(b) A is called *integrally closed* in B if $\mathcal{O}_{A,B} = A$.

Note that by theorem 1.3, the integral closure of A in B is a ring. In particular, the ring of integers $\mathcal{O}_K$ of a number field K is indeed a ring.

Example 1.9. $\mathcal{O}_{A,B}$ is integrally closed in B.

$\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. More generally, $\mathcal{O}_K$ is integrally closed in K, for if $\alpha \in K$ is integral over $\mathcal{O}_K$, by transitivity 1.7 it is then integral over $\mathbb{Z}$, hence $\alpha \in \mathcal{O}_K$.

$R = \mathbb{Z}[\sqrt{-3}] \subseteq K = \mathbb{Q}(\sqrt{-3})$ is not integrally closed in K, because $\frac{1}{2}(1 + \sqrt{-3}) \notin R$ is integral (even over $\mathbb{Z}$).

Theorem 1.10. *Let R be a UFD and $K = \operatorname{Quot}(R)$. Then R is integrally closed in K.*

Proof. Let $\frac{a}{b} \in K$ be integral over R, with $a, b \in R$ coprime. Let

$$X^n + c_{n-1}X^{n-1} + \ldots + c_1 X + c_0 = 0 \qquad \text{with } c_i \in R$$

be an integral relation for $\frac{a}{b}$. Multiplying by b^n, we get

$$a^n + c_{n-1}ba^{n-1} + \ldots + c_1 ab^{n-1} + c_0 b^n = 0.$$

Suppose $b \notin R^\times$, then there exists a prime element $\pi \in R$ dividing b. Looking at the equation $\operatorname{mod} \pi$, we see that $\pi \mid a^n$; i.e. $\pi \mid a$, contradicting the coprime assumption. □

Let A be an integral domain which is integrally closed in $K = \operatorname{Quot}(A)$. Let L/K be a finite field extension and let $B = \mathcal{O}_{A,L}$ be the integral closure of A in L.

$$\begin{tikzcd} L & B \arrow[l, hook'] \\ K \arrow[u, dash] & A \arrow[l, hook'] \arrow[u, dash] \end{tikzcd}$$

Then, by transitivity, B is integrally closed in L.

Lemma 1.11. *In the above situation, $L = \operatorname{Quot}(B)$. More precisely, each $\beta \in L$ can be written in the form $\frac{b}{a}$ with $b \in B$ and $a \in A$.*

Proof. For $\beta \in L$, let $a_n\beta^n + \ldots + a_1\beta + a_0 = 0$ with $a_i \in A$ Multiplying by a_n^{n-1}, we obtain

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + \ldots + a_1 a_n^{n-2}(a_n\beta) + a_0 a_n^{n-1} = 0.$$

Thus $a_n\beta$ is integral over A, and $\beta = \frac{a_n\beta}{a_n}$ has the desired form. □

Lemma 1.12. *One has $\beta \in B$ if and only if its minimal polynomial $\mu = \operatorname{mipo}_{\beta,K}$ over K has coefficients in A.*

Proof. Let $g(\beta) = 0$ with $g \in A[X]$ normalized. Then $\mu \mid g$ in $K[X]$. Thus all zeroes of μ (in some algebraic closure of K) are integral over A. Since the coefficients of μ are the elementary symmetric functions in its zeroes, the coefficients of μ are integral over A. Since by assumption A is integrally closed in K, it follows that $\mu \in A[X]$. □

We recall from Algebra the notions of trace and norm. Let L/K be a finite field extension of degree n, and let $x \in L$. Let $T_x : L \to L, y \mapsto xy$. Lecture 3 Oct 22, 2025

Definition 1.13. We define $\operatorname{Tr}_{L/K}(x) := \operatorname{Tr}(T_x)$ and $\operatorname{N}_{L/K}(x) := \det(T_x)$.

Lemma 1.14. *(i) Let $\chi_x(t) = \det(tE - T_x) \in K[t]$ be the characteristic polynomial of T_x. Let $\chi_x(t) = t^n - a_1 t^{n-1} + \ldots + (-1)^n a_n$. Then $a_1 = \operatorname{Tr}_{L/K}(x)$ and $a_n = \operatorname{N}_{L/K}(x)$.*

(ii) $\operatorname{Tr}_{L/K}$ is K-linear.

(iii) $\operatorname{N}_{L/K}$ is multiplicative

Proof. Everything follows from linear algebra once translated to the linear maps T_x. □

Theorem 1.15. *Let L/K be separable. Let $G = G(L/K, K^c/K)$ be the set of all homomorphisms $\sigma : L \to K^c$ that fix K. (By separability we have $|G| = [L : K]$.) Then*

(i) $\chi_x(t) = \prod_{\sigma\in G}(t - \sigma(x))$

(ii) $\operatorname{Tr}_{L/K}(x) = \sum_{\sigma\in G}\sigma(x)$

(iii) $\operatorname{N}_{L/K}(x) = \prod_{\sigma\in G}\sigma(x)$

Proof. (ii) and (iii) follow from (i) using lemma 1.14(i). Let $\mu_x(t)$ be the minimal polynomial of T_x. Then $\mu_x(T_x) = 0$, hence also $\mu_x(x) = 0$ in L. Further $\mu_x(\sigma(x)) = \sigma(\mu_x(x)) = 0$, so $\mu_x(t) = \prod_{\sigma\in G(K(x)/K, K^c/K)}(t - \sigma(x))$. We conclude with

$$\chi_x(t) = \mu_x(t)^{[L:K(x)]} = \prod_{\sigma\in G}(t - \sigma(x)),$$

where both steps need further explanation: Let $\sigma \in G(K(x)/K, K^c/K)$. Then there are $[L : K(x)]$ extensions $\widetilde{\sigma}$ of σ, which thus all have the same value at x. This explains the second equality. For the first, choose bases $\omega_1, \ldots, \omega_m$ and $1, x, \ldots, x^{n-1}$ of $L/K(x)$ and $K(x)/K$, respectively. Then $\omega_i x^j$ is a basis of L/K, and T_x w.r.t. this basis has as matrix representation a block-diagonal matrix with each block equal to the matrix representation of μ_x w.r.t. the basis $1, x, \ldots, x^{n-1}$. □

Example 1.16. (i) $K = \mathbb{Q}(\sqrt{d})$ is a quadratic extension with $G = \{\mathrm{id}, \sigma : \sqrt{d} \mapsto -\sqrt{d}\}$. Hence for $\alpha = a + b\sqrt{d}$ one has $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$ and $\operatorname{N}_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d$.

(ii) Let L/K be a finite field extension of degree m. Let $\alpha \in K$. Then $\operatorname{Tr}_{L/K}(\alpha) = m\alpha$ and $\operatorname{N}_{L/K}(\alpha) = \alpha^m$.

(iii) Let $L = \mathbb{Q}(\alpha)/K = \mathbb{Q}$, where $\alpha^3 = 2$, $\alpha \in \mathbb{R}$. In the exercises we will see $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Let $x = 1 + \alpha$. We have

$$(1+\alpha)\begin{pmatrix}1\\ \alpha\\ \alpha^2\end{pmatrix} = \begin{pmatrix}1+\alpha\\ \alpha+\alpha^2\\ \alpha^2+2\end{pmatrix} = \underbrace{\begin{pmatrix}1&1&0\\0&1&1\\2&0&1\end{pmatrix}}_{=:M}\begin{pmatrix}1\\ \alpha\\ \alpha^2\end{pmatrix},$$

so $\mathrm{Tr}_{L/K}(1+\alpha) = \mathrm{Tr}(M) = 3$ and $\mathrm{N}_{L/K}(1+\alpha) = \det(M) = 3$. Alternatively, we could have calculated

$$\mathrm{Tr}_{L/\mathbb{Q}}(1+\alpha) = \mathrm{Tr}_{L/\mathbb{Q}}(1) + \mathrm{Tr}_{L/\mathbb{Q}} = 3 + 0 = 3,$$

since the minimal polynomial $t^3 - 2$ of α has no t^2-term.

Corollary 1.17. *Let $M/L/K$ be a tower of finite field extensions. Then for $\alpha \in M$ one has*

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) \quad \textit{and} \quad \mathrm{N}_{M/K}(\alpha) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\alpha)).$$

Proof. For $\sigma_i : L/K \to K^c/K$, we have $[M : L]$ extensions $\sigma_{ij} : M \to K^c$. Fix one such extension $\widehat{\sigma}_i$.

$$\begin{tikzcd}
M \arrow[r, "\widehat{\sigma}_i"] \arrow[rr, bend left, "\sigma_{ij}"] \arrow[d, dash] & \widehat{\sigma}_i(M) \arrow[r] \arrow[d, dash] & K^c \arrow[d, dash] \\
L \arrow[r, "\sigma_i"] \arrow[d, dash] & \sigma_i(L) \arrow[r, "\mathrm{id}"] \arrow[d, dash] & \sigma_i(L) \\
K \arrow[r, "\sigma_i"] & \sigma_i(K) = K &
\end{tikzcd}$$

Then

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i,j} \sigma_{ij}(\alpha) = \sum_i \mathrm{Tr}_{\widehat{\sigma}_i M/\sigma_i L}(\widehat{\sigma}_i(\alpha)). \tag{$*$}$$

Let $\omega = (\omega_1, \dots, \omega_m)^t$ be a L-basis of M. Then $\widehat{\sigma}_i(\omega_1), \dots, \widehat{\sigma}_i(\omega_m)$ is a $\sigma_i(L)$-basis of $\widehat{\sigma}_i(M)$. Let $\alpha\omega = M_\alpha \omega$ with $M_\alpha \in L^{m\times m}$. Then $\widehat{\sigma}_i(\alpha)\widehat{\sigma}_i(\omega) = \sigma_i(M_\alpha)\widehat{\sigma}_i(\omega)$, where the actions on vectors and matrices is understood to be component-wise. Therefore,

$$\mathrm{Tr}_{\widehat{\sigma}_i(M)/\sigma_i(L)}(\widehat{\sigma}_i(\alpha)) = \mathrm{Tr}(\sigma_i(M_\alpha)) = \sigma_i(\mathrm{Tr}(M_\alpha)) = \sigma_i(\mathrm{Tr}_{M/L}(\alpha)).$$

Continuing from $(*)$ we get

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_i \sigma_i(\mathrm{Tr}_{M/L}(\alpha)) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)).$$

The same proof works for the norm, with all sums replaced by products. □

Let L/K be a finite separable extension of fields. Let $\alpha_1, \dots, \alpha_n$ be $[L : K]$-many elements of L.

Definition 1.18. The discriminant of $\alpha_1, \dots, \alpha_n$ is defined as

$$d(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))^2_{i,j=1,\dots,n},$$

where $\{\sigma_1, \dots, \sigma_n\} = G(L/K, K^c/K)$.

Lemma 1.19. *(i) $d(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{1\le i,j\le n}$.*

(ii) For $\theta \in L$ we have $d(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2$, where $\theta_i := \sigma_i(\theta)$.

Proof. One calculates

$$(\sigma_k(\alpha_i))_{k,i}^t(\sigma_k(\alpha_j))_{kj} = \left(\sum_{k=1}^n \sigma_k(\alpha_i\alpha_j)\right)_{i,j} = (\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j}$$

and takes determinants for the first part. For the second, the matrix in the definition 1.18 of d is the Vandermonde matrix of the θ_i. ☐

Theorem 1.20. *Let L/K be a finite separable field extension of degree n. Let $\alpha_1, \dots, \alpha_n \in L$. Then*

(i) $\alpha_1, \dots, \alpha_n$ is a K-basis of L if and only if $d(\alpha_1, \dots, \alpha_n) \neq 0$.

(ii) The bilinear map $\langle -, - \rangle : L \times L \to K$, $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ (called trace form*) is nondegenerate.*

Proof. For (ii), separability of L/K implies that $L = K(\theta)$ for some $\theta \in L$. The structure matrix of the bilinear form is given by

$$M = (\langle \theta^i, \theta^j \rangle)_{i,j} = (\mathrm{Tr}_{L/K}(\theta^i\theta^j))_{i,j}.$$

Thus $\det(M) = d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0$ by lemma 1.19.

Now let $\alpha_1, \dots, \alpha_n$ be elements of L. Let S be the transition matrix from $1, \theta, \dots, \theta^{n-1}$ to $\alpha_1, \dots, \alpha_n$. Then S^tMS is the structure matrix of $\langle -, - \rangle$ w.r.t. the α_i, so

$$d(\alpha_1, \dots, \alpha_n) = \det(S^tMS) = \det(S)^2 \det(M).$$

Hence $d(\alpha_1, \dots, \alpha_n) = 0$ iff $\det(S) = 0$ iff $\alpha_1, \dots, \alpha_n$ is not a basis. ☐

As before, let A be an integral domain which is integrally closed in $K = \mathrm{Quot}(A)$. Let L/K be a finite separable extension and $B = \mathcal{O}_{A,L} \subseteq L$ the integral closure of A in L. Lecture 4 Oct 24, 2025

Lemma 1.21. *For $b \in B$, one has $\mathrm{Tr}_{L/K}(b), \mathrm{N}_{L/K}(b) \in A$. Further, $b \in B$ is a unit if and only if $\mathrm{N}_{L/K}(b) \in A^\times$.*

Proof. If b is integral, so is $\sigma(b)$ for all $\sigma \in G = G(L/K, K^c/K)$. Thus $\mathrm{Tr}_{L/K}(b) = \sum_\sigma \sigma(b)$ $Norm_{L/K}(b) = \prod_\sigma \sigma(b) \in K \cap B = A$, since A is integrally closed.

Let $b \in B^\times$, then $bc = 1$ for some $c \in B$. It follows that

$$1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(bc) = \mathrm{N}_{L/K}(b)\,\mathrm{N}_{L/K}(c),$$

so $\mathrm{N}_{L/K}(b) \in A^\times$.

Conversely, let $a = \mathrm{N}_{L/K}(b) \in A^\times$. Then

$$1 = a^{-1}\,\mathrm{N}_{L/K}(b) = a^{-1}\prod_{\sigma\in G}\sigma(b) = b\,\underbrace{a^{-1}\prod_{\mathrm{id}\neq\sigma\in G}\sigma(b)}_{\in L,\ \text{integral} \Rightarrow \in B}$$

☐

Example 1.22. Let $L = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$, $\alpha^3 = 2$. Then

$$d(1, \alpha, \alpha^2) = \det(\mathrm{Tr}_{L/\mathbb{Q}}(\alpha^i\alpha^j))_{0\leq i,j\leq 2} = \det\begin{pmatrix}3 & 0 & 0\\ 0 & 0 & 6\\ 0 & 6 & 0\end{pmatrix} = -108.$$

In the exercises we will use this to prove $\mathcal{O}_L = \mathbb{Z}[\alpha]$.

Further we compute

$$\mathrm{N}_{L/\mathbb{Q}}(1-\alpha) = (1-\alpha)(1-\zeta_3\alpha)(1-\zeta_3^2\alpha) = -1,$$

so by the above lemma $1-\alpha \in \mathcal{O}_L^\times$. (Alternatively, we could have noticed that $(\alpha-1)^{-1} = \frac{\alpha^3-1}{\alpha-1} = 1+\alpha+\alpha^2 \in \mathcal{O}_L$.) Actually, we have $\mathcal{O}_L^\times = \{\pm 1\} \times (1-\alpha)^{\mathbb{Z}}$, which agrees with the result of Dirichlet's unit theorem 0.7, since there is one real and one pair of complex embeddings.

Lemma 1.23. *Let $\alpha_1, \dots, \alpha_n \in B$ be a K-basis of L. Let $d = d_{L/K}(\alpha_1, \dots, \alpha_n) \in A$. Then*

$$dB \subseteq A\alpha_1 \oplus \dots \oplus A\alpha_n.$$

Proof. Let $B \ni \alpha = a_1\alpha_1 + \dots + a_n\alpha_n$ with $a_i \in K$. Then $\mathrm{Tr}_{L/K}(\alpha_i\alpha) = \sum_{j=1}^n a_j \mathrm{Tr}_{L/K}(\alpha_i\alpha_j)$, hence $(a_1, \dots, a_n)$ is a solution of

$$\sum_{j=1}^n \underbrace{\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)}_{=:A} x_j = \mathrm{Tr}_{L/K}(\alpha_i\alpha), \qquad i = 1, \dots, n.$$

Cramer's rule shows that $a_j = \frac{\det A_j}{\det A} = \frac{\det A_j}{d}$, where A_j is the matrix A with j-th column replaced by the vector $(\mathrm{Tr}_{L/K}(\alpha_i\alpha))_i$. Hence $d(a_1, \dots, a_n) \in A^n$ □

Recall that for R a PID, each finitely generated torsion-free R-module M is free of finite rank, i.e. $M \cong R^n$, $n < \infty$. Further, if M is a free R-module and $N \subseteq M$ is an R-submodule, then N is free of rank at most the rank of M.

Theorem 1.24. *Assume further that A is a PID. Then any finitely generated B-submodule $0 \neq M \subseteq L$ is a free A-module of rank $n = [L : K]$. In particular, B has an* integral basis *over A, i.e. there exist $\omega_1, \dots, \omega_n \in B$ such that $B = A\omega_1 \oplus \dots \oplus A\omega_n$.*

Proof. Let $\alpha_1, \dots, \alpha_n \in B$ be a K-basis of L. Let $\mu_1, \dots, \mu_r \in M \subseteq L$ be a B-generating system of M. Let $0 \neq a \in A$ such that $a\mu_i \in B$ (possible by lemma 1.11). Let $d = d_{L/K}(\alpha_1, \dots, \alpha_n)$, which is nonzero by theorem 1.20. Then $daM \subseteq dB \subseteq A\alpha_1 \oplus \dots \oplus A\alpha_n \cong A^n$ by lemma 1.23. It follows that $daM \cong A^m$ with $m \leq n$, hence also $M \cong A^m$.

Let $0 \neq \mu \in M$. Then $\mu\alpha_1, \dots, \mu\alpha_n \in M$ are a K-basis of L, so they are certainly linearly independent in M as well, hence $m \geq n$. □

Example 1.25.
(i) $L = \mathbb{Q}(\sqrt{d})$, $\omega = \sqrt{d}$ for $d \equiv 2, 3 \bmod 4$ or $\omega = \frac{1+\sqrt{d}}{2}$ for $d \equiv 1 \bmod 4$ as before. Then $1, \omega$ is an integral basis of $\mathcal{O}_L$.
(ii) $L = \mathbb{Q}(\alpha)$, $\alpha^3 = 2$. In the exercises we will see that $1, \alpha, \alpha^2$ is an integral basis of $\mathcal{O}_L$.
(iii) Let K be a number field. Let $0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K$. Then $\mathfrak{a}$ has a $\mathbb{Z}$-basis, equivalently $\mathfrak{a}$ is free over $\mathbb{Z}$ of rank n.

Remark 1.26. Let $L/K/\mathbb{Q}$ be number fields. Then $\mathcal{O}_K$ is in general not a PID, so theorem 1.24 is not applicable to $\mathcal{O}_L/\mathcal{O}_K$. However, one can look at the localization $\mathcal{O}_{L,\mathfrak{p}} = S^{-1}\mathcal{O}_L$ at $S = \mathcal{O}_K \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. Then $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{\mathcal{O}_{K,\mathfrak{p}},L}$ is an $\mathcal{O}_{K,\mathfrak{p}}$-module and a DVR, so the theorem can be applied to this ring extension.

Definition 1.27. Let $L/\mathbb{Q}$ be a number field. Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$ be an integral basis, i.e. $\mathcal{O}_L = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$. Then $d_L = d_{L/\mathbb{Q}} := d_{L/\mathbb{Q}}(\alpha_1, \dots, \alpha_n)$ is called the *discriminant* of L (over $\mathbb{Q}$). More generally, if $0 \neq M \subseteq L$ is a finitely generated $\mathcal{O}_L$-module, then $d_L(M) = d_{L/\mathbb{Q}}(M) := d(m_1, \dots, m_n)$ for some integral basis $m_1, \dots, m_n$ of M.

d_L is well-defined: Let $\beta_1, \ldots, \beta_n$ be another integral basis. Let $S \in \mathrm{GL}_n(\mathbb{Z})$ be the transition matrix from the α_i to the β_i. Then

$$\begin{aligned} d_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n) &= \det(\mathrm{Tr}_{L/\mathbb{Q}}(\beta_i \beta_j)) = \det(S^t (\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i \alpha_j))_{ij} S) \\ &= \det(S)^2 \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) = d_{L/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n). \end{aligned}$$

Example 1.28. $L = \mathbb{Q}(\sqrt{d})$, $d \equiv 2, 3 \bmod 4$. Then

$$d_{L/\mathbb{Q}} = d_{L/\mathbb{Q}}(1, \sqrt{d}) = \det(\mathrm{Tr}_{L/\mathbb{Q}}(\sqrt{d}^{i+j}))_{0 \le i,j \le 1} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Similarly one computes $d_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} = d$ for $d \equiv 1 \bmod 4$.

Remark 1.29. (i) We will show that a prime p is ramified in $L/\mathbb{Q}$ if and only if $p \mid d_{L/\mathbb{Q}}$ (where p is called ramified if the factorization $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ has some $e_i > 1$).

(ii) If L/K are number fields. One can easily define a "relative" discriminant $d_{L/K}$ if $\mathcal{O}_K$ is a PID by the same procedure as above, except that it is only well-defined up to units, i.e. the ideal $d_{L/K} := (d_{L/K}(\alpha_1, \ldots, \alpha_n))$ for an integral basis α_i is well-defined.

Now assume $\mathcal{O}_K$ is arbitrary. As in remark 1.26, consider the extensions $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K/\mathfrak{p}}$ for prime ideals $\mathfrak{p} \trianglelefteq \mathcal{O}_K$. As above, we may define thus "local" discriminant ideals $d_{L/K,\mathfrak{p}} \trianglelefteq \mathcal{O}_{K,\mathfrak{p}}$. One can then prove that there exists a unique ideal $\mathfrak{D} \trianglelefteq \mathcal{O}_K$ such that $\mathfrak{D}_\mathfrak{p} = d_{L/K,\mathfrak{p}}$ called the relative discriminant.

Lecture 5
Oct 29, 2025

Theorem 1.30. *Let $L/\mathbb{Q}$ be a number field. Let $0 \neq \mathfrak{a} \subseteq \mathfrak{a}'$ be $\mathcal{O}_L$-submodules of L. Then*

$$d_L(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]^2 d_L(\mathfrak{a}').$$

In particular, $[\mathfrak{a}' : \mathfrak{a}]$ is finite.

Proof. Let $\alpha'_1, \ldots, \alpha'_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}'$ and $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Let T be the transition matrix, i.e. $\alpha_i = \sum_{j=1}^n t_{ij} \alpha'_j$, $t_{ji} \in \mathbb{Z}$. As before, we see that $d(\mathfrak{a}) = \det(T)^2 d(\mathfrak{a}')$. So it remains to show that $|\det(T)| = [\mathfrak{a}' : \mathfrak{a}]$. By the elementary divisor theorem, we may assume that T is a diagonal matrix, from where the claim follows easily. ☐

Corollary 1.31. *Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$. If $d_L(\alpha_1, \ldots, \alpha_n)$ is squarefree, then $\alpha_1, \ldots, \alpha_n$ is an integral basis.*

Remark 1.32. This is not a necessary condition: In example 1.28 we saw $4 \mid d_{\mathbb{Q}(\sqrt{d})}$ for $d \equiv 2, 3 \bmod 4$.

2 Ideals

Noetherian Rings Let R be a ring. Recall from commutative algebra that an R-module M is called *Noetherian* if all submodules of M are finitely generated. In particular, M is finitely generated. For $M = R$ this says that R is Noetherian if all ideals of R are finitely generated. For example, PIDs, finite rings, or finite modules are clearly Noetherian.

Further recall that if R is noetherian and M a finitely generated R-module, then M is noetherian; as well as the following

Theorem 2.1. *The following are equivalent:*

(i) M is Noetherian

(ii) Each ascending chain $M_1 \subseteq M_2 \subseteq \ldots$ of submodules of M stabilizes, i.e. there exists $n_0 \in \mathbb{N}$ s.t. $M_i = M_{n_0}$ for all $i \geq n_0$.

(iii) Every non-empty family of R-submodules of M contains maximal elements.

Theorem 2.2. *Let $K/\mathbb{Q}$ be a number field. Then $\mathcal{O}_K$ is Noetherian, integrally closed and of dimension 1, i.e. each non-zero prime ideal is maximal.*

Proof. Each ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ has a finite $\mathbb{Z}$-basis by theorem 1.24, hence in particular finitely generated. Thus $\mathcal{O}_K$ is noetherian. $\mathcal{O}_K$ is integrally closed by definition and transitivity 1.7.

Finally, for $0 \neq \mathfrak{p}$ prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain which is finite by theorem 1.30, hence a field. Therefore, $\mathfrak{p}$ is maximal. □

Definition 2.3. A noetherian, integrally closed integral domain of dimension 1 is called a *Dedekind* domain.

Example 2.4. By theorem 2.2, $\mathcal{O}_K$ is a Dedekind domain. Further, any PID is clearly Dedekind.

Our next goal will be to show that in a Dedekind domain $\mathcal{O}$, every ideal factors uniquely as a product of prime ideals.

Definition 2.5. Let R be a ring and $\mathfrak{a}, \mathfrak{b}$ be ideals.

(i) We write $\mathfrak{a} \mid \mathfrak{b}$ for $\mathfrak{b} \subseteq \mathfrak{a}$.

(ii) The ideal sum $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ is also called the gcd of $\mathfrak{a}$ and $\mathfrak{b}$.

(iii) The intersection $\mathfrak{a} \cap \mathfrak{b}$ is also called the lcm of $\mathfrak{a}$ and $\mathfrak{b}$.

Theorem 2.6. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{a} \subseteq \mathcal{O}$ an ideal, $\mathfrak{a} \neq (0), (1)$. Then there exists a unique presentation (up to order) of $\mathfrak{a}$ in the form*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \tag{$*$}$$

with prime ideals $\mathfrak{p}_i \neq (0)$. If we write $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ with pairwise distinct primes $\mathfrak{p}_j$, then also $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \ldots \cap \mathfrak{p}_s^{e_s}$

Proof. We start with the second statement: In general, one has $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$ for coprime ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ for any ring R. Also, if $\mathfrak{p}, \mathfrak{q}$ are coprime, then so are $\mathfrak{p}^e$ and $\mathfrak{q}^f$.

For the main statement, we will need the following lemmas:

Lemma 2.7. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal. Then there are non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, $r \geq 1$, s.t. $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}$*

Proof. Let

$$\mathcal{M} := \{0 \neq \mathfrak{a} \subseteq \mathcal{O} \text{ ideal} \mid \mathfrak{a} \text{ does not satisfy the statement of the lemma}\}.$$

Suppose $\mathcal{M} \neq \emptyset$. Since $\mathcal{O}$ is noetherian, by theorem 2.1 there exists a maximal element $\mathfrak{a} \in \mathcal{M}$. Then $\mathfrak{a}$ is not a prime ideal, so there exist $b_1, b_2 \in \mathcal{O}$ such that $b_1 b_2 \in \mathfrak{a}$, but $b_1, b_2 \notin \mathfrak{a}$. Let $\mathfrak{a}_i := \mathfrak{a} + (b_i)$. By choice of $\mathfrak{a}$, we have $\mathfrak{a}_i \notin \mathcal{M}$, hence we can write

$$\mathfrak{a}_1 \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_s, \qquad \mathfrak{a}_2 \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

for nonzero prime ideals $\mathfrak{p}_i, \mathfrak{q}_j$. But then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_r \subseteq \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a} + (b_1 b_2) \subseteq \mathfrak{a},$$

contradicting $\mathfrak{a} \in \mathcal{M}$. □

Lemma 2.8. *Let $0 \neq \mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal. Let $K := \mathrm{Quot}(\mathcal{O})$ and*

$$\mathfrak{p}^{-1} := \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\} \subseteq K.$$

Then $\mathfrak{p}^{-1} \supseteq \mathcal{O}$ is a non-zero $\mathcal{O}$-module, and for any ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ one has $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$.

Proof. Everything is clear but the strictness of the final inclusion. Let $0 \neq a \in \mathfrak{p}$. By lemma 2.7 there exists a product of nonzero prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a)$ with r minimal. Since $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}$ and all these ideals are maximal, we have $\mathfrak{p}_1 = \mathfrak{p}$, say. By minimality of r, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$, so there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$, hence $a^{-1}b \notin \mathcal{O}$. On the other hand $b\mathfrak{p} \subseteq (a)$, so $a^{-1}b\mathfrak{p} \subseteq \mathcal{O}$, i.e. $a^{-1}b \in \mathfrak{p}^{-1}$. Hence $\mathfrak{p}^{-1} \supsetneq \mathcal{O}$.

Let now $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an ideal. Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$ and suppose $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Let $x \in \mathfrak{p}^{-1}$. Then

$$x\alpha_i = \sum_{j=1}^{n} a_{ji}\alpha_j, \qquad a_{ji} \in \mathcal{O}.$$

Let $A = (xE - (a_{ji}))$. Then $A(\alpha_1, \ldots, \alpha_n)^t = 0$, so by lemma 1.4, $\det(A)\alpha_i = 0$, so x is a zero of the normalized polynomial $\det(tE - (\alpha_{ji})) \in \mathcal{O}[t]$, hence x is integral over $\mathcal{O}$. But $\mathcal{O}$ is integrally closed by definition, so $x \in \mathcal{O}$. Thus we have shown $\mathfrak{p}^{-1} \subseteq \mathcal{O}$, contradicting the previous paragraph. □

Now we can return to the proof of theorem 2.6. Let

$$\mathcal{M} := \{\mathfrak{a} \subseteq \mathcal{O} \text{ ideal } \mid \mathfrak{a} \neq (0), (1);\ \mathfrak{a} \text{ cannot be written as in } (*)\}.$$

Suppose $\mathcal{M} \neq \emptyset$. Since $\mathcal{O}$ is Noetherian, by theorem 2.1 there exists a maximal element $\mathfrak{a} \subseteq \mathcal{M}$. Let $\mathfrak{p} \supseteq \mathfrak{a}$ be a maximal ideal containing $\mathfrak{a}$. By lemma 2.8, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ and $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. Since $\mathfrak{p}$ is maximal, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. By choice of $\mathfrak{a}$, we know that $\mathfrak{a}\mathfrak{p}^{-1} \notin M$, so there is a factorization

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_s \quad \Longrightarrow \quad \mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_s\mathfrak{p}.$$

This contradicts $\mathfrak{a} \in \mathcal{M}$, showing the existence of ideal factorizations.

For uniqueness, suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{p}_1$, so one of the factors is already contained in $\mathfrak{p}_1$, wlog $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since $\mathfrak{q}_1$ is maximal, $\mathfrak{q}_1 = \mathfrak{p}_1$. Then multiply the original equation by $\mathfrak{p}_1^{-1}$ and proceed inductively. □

For convenience, we will often write prime ideal factorizations in the form $\mathfrak{a} = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$, Lecture 6
where $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{N}_0$ is zero for almost all $\mathfrak{p}$. By the Chinese Remainder Theorem, we have Oct 31, 2025

$$\mathcal{O}/\mathfrak{a} \cong \prod_{\mathfrak{p} \neq 0} \mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}.$$

Definition 2.9. A *fractional ideal* in $K = \mathrm{Quot}(\mathcal{O})$ is a nonzero finitely generated $\mathcal{O}$-submodule of K.

Example 2.10.
(i) For $a \in K^\times$, $(a) = a\mathcal{O}$ is a principal fractional ideal.
(ii) More generally, $c\mathfrak{a}$ is a fractional ideal for $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ an ideal and $c \in K^\times$.

Lemma 2.11. $\mathfrak{a} \subseteq K$ *be a fractional ideal if and only if there exists $c \in \mathcal{O} \setminus \{0\}$ such that $c\mathfrak{a}$ is an ideal of $\mathcal{O}$.*

Proof. The backwards direction is clear. Let $\mathfrak{a} = (\alpha_1, \ldots, \alpha_s)$ be a fractional ideal. Write $\alpha_1 = \frac{b_i}{c_i}$ with $b_i, c_i \in \mathcal{O}$. Then $\prod c_i\mathfrak{a} \subseteq \mathcal{O}$ is an ideal of $\mathcal{O}$. □

To better distinguish fractional ideals and ideals contained in $\mathcal{O}$, we will often call the latter "integral ideals".

Theorem 2.12. *Let $J_{\mathcal{O}}$ be the set of fractional ideals. Then $J_{\mathcal{O}}$ is an abelian group w.r.t. multiplication of ideals. The identity element is $\mathcal{O}$, and the inverse of $\mathfrak{a}$ is given by $\mathfrak{a}^{-1} = (\mathcal{O} : \mathfrak{a})$, where*

$$(\mathfrak{b} : \mathfrak{c}) := \{x \in K \mid x\mathfrak{c} \subseteq \mathfrak{b}\}$$

Proof. In the proof of theorem 2.6 we have seen $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Let know $\mathfrak{a}$ be an integral ideal. For $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, we have the inverse $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. By lemma 2.11, each fractional ideal has an inverse.

Let now $\mathfrak{a}$ be a fractional ideal and $\mathfrak{b}$ its inverse, we want to show $\mathfrak{b} = (\mathcal{O} : \mathfrak{a})$. The inclusion $\mathfrak{b} \subseteq (\mathcal{O} : \mathfrak{a})$ is clear from the definition of inverse. If $x \in (\mathcal{O} : \mathfrak{a})$. Then $x\mathfrak{a} \subseteq \mathcal{O}$, so $x\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$, i.e. $x \in \mathfrak{b}$, finishing the proof. □

Corollary 2.13. *Let $\mathfrak{a} \in J_{\mathcal{O}}$ be a fractional ideal. Then we have a unique representation of $\mathfrak{a}$ in the form*

$$\mathfrak{a} = \prod_{\mathfrak{p} \neq 0} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

with $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$ and almost all $v_{\mathfrak{p}}(\mathfrak{a}) = 0$. Further, we can uniquely write $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1} =: \frac{\mathfrak{b}}{\mathfrak{c}}$ with $\mathfrak{b}, \mathfrak{c} \subseteq \mathcal{O}$ integral ideals s.t. $(\mathfrak{b}, \mathfrak{c}) = 1$.

Lemma 2.14. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}$ be an integral ideal, and let $\mathfrak{p} \neq 0$ be a prime ideal. Let $\mathfrak{a} = \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}\mathfrak{b}$ with $v_{\mathfrak{p}}(\mathfrak{a}) \geq 0$ and $\mathfrak{p} \nmid \mathfrak{b}$. Then $v_{\mathfrak{p}}(\mathfrak{a}) = n$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}^n$ and $\mathfrak{a} \not\subseteq \mathfrak{p}^{n+1}$, i.e. $v_{\mathfrak{p}}(\mathfrak{a})$ is the highest power of $\mathfrak{p}$ dividing $\mathfrak{a}$.*

Proof. If $\mathfrak{a} = \mathfrak{p}^n\mathfrak{b}$, it is clear that $\mathfrak{a} \subseteq \mathfrak{p}^n$, and if $\mathfrak{a} \subseteq \mathfrak{p}^{n+1}$, then we would have $\mathfrak{b} \subseteq \mathfrak{p}$.

Conversely, suppose $\mathfrak{a} \subseteq \mathfrak{p}^n$. Then $\mathfrak{b} := \mathfrak{a}\mathfrak{p}^{-n} \subseteq \mathcal{O}$ is an ideal, and $\mathfrak{a} = \mathfrak{b}\mathfrak{p}^n$ shows $v_{\mathfrak{p}}(\mathfrak{a}) \geq n$. Suppose $\mathfrak{p} \mid \mathfrak{b}$, i.e. $\mathfrak{b} \subseteq \mathfrak{p}$. Then $\mathfrak{a} = \mathfrak{p}^n\mathfrak{b} \subseteq \mathfrak{p}^{n+1}$, contradicting the assumption. □

Definition 2.15. Let $\mathcal{O}$ be a Dedekind domain and $K = \mathrm{Quot}(\mathcal{O})$. Set $P_{\mathcal{O}} = \{x\mathcal{O} \mid x \in K^\times\} \subseteq J_{\mathcal{O}}$ be the subgroup of principal fractional ideals. Then $\mathrm{cl}_{\mathcal{O}} := J_{\mathcal{O}}/P_{\mathcal{O}}$ is called the *ideal class group* of $\mathcal{O}$.

In the case of a number field $K/\mathbb{Q}$ with ring of integers $\mathcal{O}_K$, write $\mathrm{cl}_K = \mathrm{cl}_{\mathcal{O}_K}$ and similarly for J_K and P_K. Our next aim is to prove that cl_K is a finite group. This is not true for general Dedekind domains.

Remark 2.16. From the definition it is clear that a Dedekind domain $\mathcal{O}$ is a PID if and only if $|\,\mathrm{cl}_{\mathcal{O}}\,| = 1$. In general, we have the following exact sequence

$$1 \to \mathcal{O}^\times \hookrightarrow K^\times \xrightarrow{a \mapsto (a)} J_{\mathcal{O}} \xrightarrow{\mathfrak{a} \mapsto [\mathfrak{a}]} \mathrm{cl}_{\mathcal{O}} \to 1$$

Theorem 2.17. *Let $\mathcal{O}$ be a Dedekind domain with finitely many prime ideals. Then $\mathcal{O}$ is a PID.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the nonzero prime ideals of $\mathcal{O}$. It suffices to show that each $\mathfrak{p}_i$ is principal, the result then follows from the prime ideal factorization 2.6. Let $a_1 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. By the Chinese Remainder Theorem, there exists $a \in \mathcal{O}$ such that $a \equiv a_1 \bmod \mathfrak{p}_1^2$ and $a \equiv 1 \bmod \mathfrak{p}_i$ for $i > 1$.

Then $\mathfrak{p}_1 = a\mathcal{O}$. Indeed, let $a\mathcal{O} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_n^{\nu_n}$. Since $a \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ and $a \in \mathcal{O} \setminus \mathfrak{p}_i$, lemma 2.14 shows $\nu_1 = 1$ and $\nu_i = 0$ for $i > 1$. □

Let $\mathcal{O} \subseteq K = \mathrm{Quot}(\mathcal{O})$ be a Dedekind domain and $S \subseteq \mathcal{O}$ be a multiplicative subset. Then $S^{-1}\mathcal{O}$ is still Dedekind: It is clearly a noetherian integral domain of dimension 1, by the correspondence of ideals in $\mathcal{O}$ and $S^{-1}\mathcal{O}$. For integrally closed check in general that $S^{-1}\mathcal{O}_{B,C} = \mathcal{O}_{S^{-1}B,S^{-1}C}$.

Now take a prime $\mathfrak{p} \neq 0$ and $S = S_\mathfrak{p} := \mathcal{O} \setminus \mathfrak{p}$. Then $\mathcal{O}_\mathfrak{p} = S_\mathfrak{p}^{-1}\mathcal{O}$ is a Dedekind domain with exactly one prime $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, hence a PID by theorem 2.17, even a DVR.

Theorem 2.18. *Let $0 \neq \mathfrak{m} \subseteq \mathcal{O}$ be an ideal. Let $c \in \mathrm{cl}_\mathcal{O}$ be an ideal class. Then c contains an integral ideal $\mathfrak{a} \subseteq \mathcal{O}$ with $(\mathfrak{a}, \mathfrak{m}) = 1$.*

Proof. If there are only finitely many primes, then $\mathrm{cl}_\mathcal{O} = 1$ by theorem 2.17, so we may take $\mathfrak{a} = \mathcal{O}$. Suppose now we have infinitely many primes. Let $\mathfrak{m} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_s^{f_s}$ be the unique prime ideal factorization of $\mathfrak{m}$ and $c = [\mathfrak{a}]$, wlog $\mathfrak{a} \subseteq \mathcal{O}$. Let $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}\mathfrak{b}$, $r \leq s$ and $(\mathfrak{b}, \mathfrak{m}) = 1$. Choose $\alpha_i \in \mathfrak{p}_i^{e_i} \setminus \mathfrak{p}_i^{e_{i+1}}$ for $i = 1, \ldots, r$. By the Chinese Remainder Theorem, there is $\alpha \in \mathcal{O}$ such that

$$\alpha \equiv \alpha_i \bmod \mathfrak{p}_i^{e_i+1} \qquad \text{for } i = 1, \ldots, r,$$
$$\alpha \equiv 1 \bmod \mathfrak{p}_i \qquad \text{for } i = r+1, \ldots, s.$$

Then by lemma 2.14 $\alpha\mathcal{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}\mathfrak{c}$ for an integral ideal $\mathfrak{c}$ with $(\mathfrak{c}, \mathfrak{m}) = 1$. □

In general, $\mathcal{O}$ is not a PID, but

Lecture 7
Nov 5, 2025

Theorem 2.19. *Each ideal $\mathfrak{a} \in J_\mathcal{O}$ can be generated by two elements. In fact, given $0 \neq \alpha \in \mathfrak{a}$, then there exists $\beta \in \mathfrak{a}$ with $\mathfrak{a} = (\alpha, \beta)$.*

Proof. Suffices to consider $\mathfrak{a} \subseteq \mathcal{O}$. Claim: If $0 \neq \mathfrak{b} \subseteq \mathcal{O}$ is an ideal, then every ideal of $\mathcal{O}/\mathfrak{b}$ is principal.

Given this, let $0 \neq \alpha \in \mathfrak{a}$ and let $\pi : \mathcal{O} \to \mathcal{O}/(\alpha)$ be the canonical projection. Then the image of $\mathfrak{a}$ under π is principal by the claim, say $\overline{\mathfrak{a}} = (\overline{\beta})$. Hence $\mathfrak{a} = \pi^{-1}((\overline{\beta})) = (\alpha, \beta)$.

Hence it remains to prove the claim. Write $\mathfrak{b} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with $e_i \geq 1$ and $(\mathfrak{p}_i, \mathfrak{p}_j) = 1$. Let $\overline{\mathfrak{c}} \subseteq \mathcal{O}/\mathfrak{b}$ be an ideal, with $\mathfrak{c} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r}$, $f_i \leq e_i$ the corresponding ideal in $\mathcal{O}$. By the Chinese Remainder Theorem, $\mathcal{O}/\mathfrak{b} \cong \mathcal{O}/\mathfrak{p}_1^{e_1} \times \ldots \times \mathcal{O}/\mathfrak{p}_r^{e_r}$, let $\mathfrak{q}_1 \times \ldots \times \mathfrak{q}_r$ be the image of $\mathfrak{p}_i$ under this isomorphism. It suffices to show that the $\mathfrak{q}_j$ are principal. But $\mathfrak{q}_j = 1$ for $i \neq j$, and $\mathfrak{q}_i = \mathfrak{p}_i/\mathfrak{p}_i^{e_1}$.

More generally, $\mathfrak{p}^i/\mathfrak{p}^e$ is principal in $\mathcal{O}/\mathfrak{p}^e$: Take $\alpha \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, then $\alpha\mathcal{O} + \mathfrak{p}^e = \mathfrak{p}^i$ by lemma 2.14, so $(\overline{\alpha}) = \mathfrak{p}^i/\mathfrak{p}^e$. □

In general, computing integral bases is difficult. However, sometimes they can be pieced together from smaller rings: Let K, L be number fields of degree n, m, respectively. Let $M = KL$ be their composite. Then $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_M$.

Theorem 2.20. *Assume that $[M : \mathbb{Q}] = mn$. Let $d := \gcd(d_K, d_L)$. Then $\mathcal{O}_M \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.*

Corollary 2.21. *If $[M : \mathbb{Q}] = mn$ and $\gcd(d_K, d_L) = 1$, then $\mathcal{O}_M = \mathcal{O}_L\mathcal{O}_K$. In addition, $d_M = d_L^n d_K^m$.*

Example 2.22. For $m \in \mathbb{N}$ let ζ_m be a primitive m-th root of unity. Then $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is a number field, called *cyclotomic field*, of degree $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$, and a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, where the isomorphism is given by $k \mapsto \sigma_k : \zeta_m \mapsto \zeta_m^k$.

We will show $\mathcal{O}_{\mathbb{Q}(\zeta_{p^n}} = \mathbb{Z}[\zeta_{p^n}]$ and that $d_{\mathbb{Q}(\zeta_{p^n})}$ is a power of p. Further it is easy to see that $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ for m, n coprime. So corollary 2.21 implies $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ and gives a formula for the discriminant of $\mathbb{Q}(\zeta_m)$.

Proof. Claim: Let $\sigma : K \to \mathbb{C}$, $\tau : L \to \mathbb{C}$ be embeddings. Then there exists a unique embedding $\kappa : M \to \mathbb{C}$ such that $\kappa|_K = \sigma$ and $\kappa|_L = \tau$. For the restriction map $\mathrm{Hom}_{\mathbb{Q}}(M, \mathbb{C}) \to \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) \times \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ is clearly injective and between finite sets of the same size nm, so bijective.

Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$, and $\beta_1, \ldots, \beta_m$ an integral basis of $\mathcal{O}_L$. Then $\alpha_i\beta_j$ form a $\mathbb{Z}$-basis of $\mathcal{O}_K\mathcal{O}_L$. Any $\alpha \in \mathcal{O}_N$ can be written in the form $\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j$ with $m_{ij}, r \in \mathbb{Z}$ and $\gcd(r, \gcd(m_{ij})_{ij}) = 1$. To show: $r \mid d$.

By symmetry, it suffices to show $r \mid d_K$. By the claim, for each $\sigma : K \to \mathbb{C}$ there exists a unique $\widetilde{\sigma} : M \to \mathbb{C}$ such that $\widetilde{\sigma}|_K = \sigma$ and $\widetilde{\sigma}|_L = \mathrm{id}_L$. Then

$$\widetilde{\sigma}(\alpha) = \sum_{i,j} \frac{m_{ij}}{r}\widetilde{\sigma}(\alpha_i\beta_j) = \sum_{i,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j.$$

Set $x_i = \sum_{j=1}^m \frac{m_{ij}}{r}\beta_j$. Then we have n equations $\widetilde{\sigma}(\alpha) = \sum_{i=1}^n \sigma(\alpha_i)x_i$, one for each σ. By Cramer's rule, $x_i = \frac{\gamma_i}{\delta}$, where $\delta = \det(\sigma(\alpha_i))_{\sigma,i}$. Clearly, $\gamma_i, \delta_i \in \mathcal{O}_M$, and by definition $\delta^2 = d_K$. Hence $d_K x_i = \delta\gamma_i$, so $d_K x_i = \sum_j \frac{d_K m_{ij}}{r}\beta_j \in \mathcal{O}_N \cap L = \mathcal{O}_L$. But this means $r \mid d_K m_{ij}$ for all i, j, so $r \mid d_K$ by the coprimiality assumption.

For the discriminant formula in the corollary, we now know that $\alpha_i\beta_j$ is a $\mathbb{Z}$-basis of $\mathcal{O}_M$, hence Lecture 8 Nov 7, 2025

$$\begin{aligned}
d_N = d(\alpha_i\beta_j) &= \det(\mathrm{Tr}_{M/\mathbb{Q}}(\alpha_i\beta_j\alpha_k\beta_l)) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{M/K}(\alpha_i\beta_j\alpha_k\beta_l))) \\
&= \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_k \,\mathrm{Tr}_{M/K}(\beta_j\beta_l))) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_k \,\mathrm{Tr}_{L/\mathbb{Q}}(\beta_j\beta_l))) \\
&= \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_k)\,\mathrm{Tr}_{L/\mathbb{Q}}(\beta_j\beta_l)) = \det((\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_k)) \otimes (\mathrm{Tr}_{L/\mathbb{Q}}(\beta_j\beta_l))) \\
&= d_K^m d_L^n,
\end{aligned}$$

where we used the fact from linear algebra that $A \otimes B = (a_{ij}B) \in R^{nm\times nm}$ for $A \in R^{n\times n}, B \in R^{m\times m}$ satisfies $\det(A \otimes B) = \det(A)^m \det(B)^n$ □

3 Lattices

Definition 3.1. Let V be an n-dimensional $\mathbb{R}$-vector space. A *lattice* in V is a subgroup Γ of V of the form $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ with linearly independent vectors $v_1, \ldots, v_m \in V$, $m \leq n$. The set $\Phi = \{x_1v_1 + \ldots + x_mv_m \mid 0 \leq x_i < 1\}$ is called a *fundamental domain* of Γ. Further, Γ is a *full* lattice if $m = n$.

Definition 3.2. A subgroup Γ of V is called discrete if for each $\gamma \in \Gamma$ there exists a neighbourhood U such that $\Gamma \cap U = \{\gamma\}$

Lemma 3.3. *If Γ is a discrete subgroup of V, then Γ is closed.*

Proof. Claim: Each $a \in V \setminus \Gamma$ has an open neighbourhood U with $|\Gamma \cap U| < \infty$.

Then since V is Hausdorff, there exists an open neighbourhood $\widetilde{U}$ of a that avoids these finitely many points, so $(U \cap \widetilde{U}) \cap \Gamma = \emptyset$, i.e. $U \cap \widetilde{U}$ is a neighbourhood of a in $V \setminus \Gamma$.

To prove the claim, let $a \in V \setminus \Gamma$. By assumption, there exists an open $\widetilde{U} \subseteq V$ such that $\widetilde{U} \cap \Gamma = \{0\}$. Since $V \times V \to V$, $(a, b) \mapsto a - b$ is continuous, there exists an open neighbourhood U of 0 such that $U - U \subseteq \widetilde{U}$. Then $a + U$ is an open neighbourhood of a, suppose there are $\gamma_1, \gamma_2 \in \Gamma \cap (a + U)$. But then $\gamma_1 - \gamma_2 \in \widetilde{U}$, so $\gamma_1 = \gamma_2$. □

Lemma 3.4. *Let Γ be a subgroup of V. Then Γ is discrete if and only if for all bounded $C \subseteq V$ one has $|C \cap \Gamma| < \infty$.*

Proof. Let Γ be discrete. Wlog C is compact. If $C \cap \Gamma$ were infinite, then by Bolzano-Weierstrass, there is an accumulation point $\gamma \in C \cap \Gamma$ (by lemma 3.3), contradicting the definition.

Conversely, let $\gamma \in \Gamma$. Choose an open ball around γ. By assumption, this ball contains only finitely many $\gamma_i \in \Gamma$, which, as before, can be separated from γ using the Hausdorff property. $\square$

Example 3.5. Let $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}[\sqrt{2}]$ is not a lattice in $V = \mathbb{R}$, but $\mathcal{O}_K$ becomes a lattice in $\mathbb{R}^2$ via

$$j : \mathcal{O}_K \hookrightarrow \mathbb{R}^2, \qquad a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2}).$$

We will prove soon (in general) that $j(\mathcal{O}_K) \subseteq \mathbb{R}^2$ is a lattice.

Theorem 3.6. *Let $\Gamma \subseteq V$ be a subgroup. Then Γ is a lattice if and only if Γ is discrete.*

Proof. Let $\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m$ be a lattice. Choose a basis $v_1, \ldots, v_m, v_{m+1}, \ldots, v_n$ of V. Let $\gamma = a_1v_1 + \ldots + a_mv_m$. Consider

$$U := \{x_1v_1 + \ldots + x_nv_n \mid x_i \in \mathbb{R} \mid |a_i - x_i| < 1 \text{ for } i \leq m\}.$$

Then U is open and $U \cap \Gamma = \{\gamma\}$.

Conversely, let Γ be discrete. Let V_0 be the $\mathbb{R}$-subspace of V generated by Γ and denote $m := \dim_{\mathbb{R}} V_0$. Choose a $\mathbb{R}$-basis $u_1, \ldots, u_m$ of V_0 with $u_i \in \Gamma$. Consider $\Gamma_0 := \mathbb{Z}u_1 \oplus \ldots \oplus \mathbb{Z}u_m \subseteq V_0$, which is a lattice by definition.

Claim: $q := (\Gamma : \Gamma_0) < \infty$. Then $\Gamma_0 \subseteq \Gamma \subseteq \frac{1}{q}\Gamma_0$ is a subgroup of a free abelian group, so is itself free (of rank m).

To prove the claim, let $\{\gamma_i\}_{i \in I}$ be a set of representatives of Γ/Γ_0. Let $\Phi_0 = \{x_1u_1 + \ldots + x_mu_m \mid 0 \leq x_i < 1\}$ be a fundamental domain of Γ_0. Then $\bigcup_{\gamma \in \Gamma_0}(\gamma + \Phi_0) = V$, hence $\gamma_i = \gamma_{0i} + \mu_i$ with $\gamma_{0i} \in \Gamma_0$ and $\mu_i \in \Phi_0$. Then the bounded Φ_0 contains all the $\mu_i = \gamma_i - \gamma_{0i} \in \Gamma$, hence I is finite by lemma 3.4. $\square$

Lemma 3.7. *Let $\Gamma \subseteq V$ be a lattice. Then Γ is full if and only if there exists a bounded subset $M \subseteq V$ such that $\bigcup_{\gamma \in \Gamma} \gamma \in \Gamma(\gamma + M) = V$.*

Proof. If Γ is full, take M to be a fundamental domain. Conversely, let V_0 be the $\mathbb{R}$-span of Γ. Let $v \in V$. For $\nu \in \mathbb{N}$ write $\nu v = \gamma_\nu + a_\nu$ with $\gamma_\nu \in \Gamma$ and $a_\nu \in M$. Since M is bounded, $\frac{a_\nu}{\nu} \xrightarrow{\nu \to \infty} 0$. Hence

$$v = \lim_{\nu \to \infty} \frac{\gamma_\nu + a_\nu}{\nu} = \lim_{\nu \to \infty} \frac{\gamma_\nu}{\nu} \in V_0,$$

since $V_0 \subseteq V$ is closed. $\square$

Now let V be an euclidean vector space with inner product $\langle -, - \rangle : V \times V \to \mathbb{R}$. Let $e_1, \ldots, e_n$ be an orthonormal basis. Then we define a volume. For the "unit cube" Lecture 9 Nov 12, 2025

$$E := \left\{ \sum_i \alpha_i e_i \mid 0 \leq \alpha_i \leq 1 \right\},$$

we set $\mathrm{Vol}\,(E) = 1$. More generally, let $v_1, \ldots, v_n$ be an $\mathbb{R}$-basis of V and let $\Phi := \{\sum_i x_iv_i \mid 0 \leq x_i \leq 1\}$. Let $A = (a_{ji}) \in \mathrm{GL}_n(\mathbb{R})$ be the transition matrix, $v_i = \sum_j a_{ji}e_j$.

Lemma 3.8. *One has* $\mathrm{Vol}(\Phi) = |\det(A)| = \sqrt{\det(\langle v_i, v_j \rangle_{ij})}$.

Proof.

$$\mathrm{Vol}(\Phi) = \int_\Phi dx = \int_E |\det(A)| dx = |\det(A)| \,\mathrm{Vol}(E) = |\det(A)|.$$

The second equality follows from $\langle v_i, v_j \rangle_{ij} = A^t \langle e_i, e_j \rangle_{ij} A = A^t A$. $\square$

Definition 3.9. Let $\Gamma \subseteq V$ be a full lattice. Then we define $\operatorname{Vol}(\Gamma) := \operatorname{Vol}(\Phi)$ for any fundamental domain Φ for Γ.

This is well-defined, i.e. independent of the choice of Φ, since different $\mathbb{Z}$-bases of Γ differ by a transition matrix $T \in \mathrm{GL}_n(\mathbb{Z})$, i.e. $\det(T) = \pm 1$, so the absolute value of the determinant does not change.

Definition 3.10. Let $X \subseteq V$ be a subset. X is called *central-symmetric* if for all $x \in X$ we have $-x \in X$. X is *convex* if for all $x, y \in X$ also $tx + (1-t)y \in X$ for $0 \leq t \leq 1$.

For example, a ball centered around 0 is both central-symmetric and convex.

Theorem 3.11 (Minkowski's Lattice Point Theorem)**.** *Let* $\Gamma \subseteq V$ *be a full lattice in an eucliden vector space of dimension* $\dim_{\mathbb{R}}(V) = n$. *Let* $X \subseteq V$ *be a central-symmetric, convex subset with* $\operatorname{Vol}(X) > 2^n \operatorname{Vol}(\Gamma)$. *Then there exists a* $0 \neq \gamma \in \Gamma$ *with* $\gamma \in X$.

Proof. It suffices to show that there are $\gamma_1 \neq \gamma_2 \in \Gamma$ such that $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2) \neq \emptyset$. Indeed, let $v = \frac{1}{2}x_1 + \gamma_1 + \frac{1}{2}x_2 + \gamma_2$ be an element of the intersection. Then

$$\gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1) = \frac{1}{2}x_2 + \left(1 - \frac{1}{2}\right)(-x_1) \in X$$

by central-symmetry and convexity.

To prove the claim, suppose that the sets $(\frac{1}{2}X + \gamma)$, $\gamma \in \Gamma$ are pairwise disjoint. Then so are the sets $\Phi \cap (\frac{1}{2} + \gamma)$ for a fundamental domain Φ of Γ. Hence

$$\operatorname{Vol}(\Gamma) = \operatorname{Vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \operatorname{Vol}(\Phi \cap (\gamma + \frac{1}{2}X)) = \sum_{\gamma \in \Gamma} \operatorname{Vol}((\Phi - \gamma) \cap \frac{1}{2}X).$$

Since $\Phi - \gamma$ covers all of X, cf. lemma 3.7. Therefore

$$\operatorname{Vol}(\Gamma) \geq \operatorname{Vol}(\frac{1}{2}X) = 2^{-n} \operatorname{Vol}(X),$$

contradicting our assumption. □

4 Minkowski Theory

Let $K/\mathbb{Q}$ be a number field of degree n. Of the embeddings $\tau : K \to \mathbb{C}$, we distinguish real embeddings $\rho_1, \ldots, \rho_r : K \to \mathbb{R}$ and pairs of complex embeddings $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s : K \to \mathbb{C}$ with image not contained in $\mathbb{R}$, with $n = r + 2s$.

Definition 4.1. We define *Minkowski Space* of K as

$$K_{\mathbb{R}} := \left\{ (z_\tau) \in \prod_{\tau : K \to \mathbb{C}} \mathbb{C} \mid z_\rho \in \mathbb{R}, z_{\overline{\sigma}} = \overline{z_\sigma} \right\}$$

Remark 4.2. $K_{\mathbb{R}}$ is an $\mathbb{R}$-vector space of dimension $r + 2s = n$.

Example 4.3. Let $K = \mathbb{Q}(\sqrt{d})$. If $d > 0$, then $K_{\mathbb{R}} = \mathbb{R}\rho_1 + \mathbb{R}\rho_2$. If, on the other hand, $d < 0$, then $K_{\mathbb{R}} = \{(\beta, \overline{\beta}) \mid \beta \in \mathbb{C}\} \subseteq \mathbb{C}^2$.

Example 4.4. For $K = \mathbb{Q}(\omega)$ with $\omega \in \mathbb{R}$, $\omega^3 = 2$, we have $K_{\mathbb{R}} = \{(\alpha, \beta, \overline{\beta}) \mid \alpha \in \mathbb{R}, \beta \in \mathbb{C}\}$.

On $K_{\mathbb{R}}$ we define the inner product

$$\langle x, y\rangle := \sum_{\tau} x_\tau \overline{y_\tau}.$$

It is clear that this is bilinear and positive definite; we check that the image is contained in $\mathbb{R}$:

$$\langle x, y\rangle = \sum_{\rho} x_\rho y_\rho + \sum_{\sigma} (x_\sigma \overline{y_\sigma} + \underbrace{x_{\overline{\sigma}} \overline{y_{\overline{\sigma}}}}_{=\overline{x}_\sigma y_\sigma}).$$

Hence the terms of the last sum are stable under conjugation, thus they lie in $\mathbb{R}$.

Theorem 4.5. *Consider the isomorphism of $\mathbb{R}$-vector spaces*

$$f : K_{\mathbb{R}} \to \prod_{\tau} \mathbb{R}, \quad (z_\tau)_\tau \mapsto (z_{\rho_1}, \dots, z_{\rho_r}, \mathrm{Re}(z_{\sigma_1}), \mathrm{Im}(z_{\sigma_1}), \dots, \mathrm{Re}(z_{\sigma_s}), \mathrm{Im}(z_{\sigma_s})).$$

For $(-,-) : (\prod_\tau \mathbb{R})^2 \to \mathbb{R}$ defined by $(x, y) := \sum \alpha_\tau x_\tau y_\tau$ with $\alpha_\tau = 1$ if τ is real and $\alpha_\tau = 2$ if τ is complex, we have $\langle x, y\rangle = (f(x), f(y))$ for all $x, y \in K_{\mathbb{R}}$.

Proof. Exercise. □

Remark 4.6. By the above theorem, $\mathrm{Vol}_{(-,-)} = 2^s \mathrm{Vol}_{\text{Lebesgue}}$, since an orthonormal basis w.r.t. $(-,-)$ is given by $e_1, \dots, e_r, \frac{1}{\sqrt{2}} e_{r+1}, \dots, \frac{1}{\sqrt{2}} e_{r+2s}$.

Generalizing example 3.5, define

$$j : K \hookrightarrow K_{\mathbb{R}}, \qquad \alpha \mapsto (\tau(\alpha))_{\tau : K \to \mathbb{C}}.$$

This is a $\mathbb{Q}$-linear embedding.

Theorem 4.7. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal. Then $\Gamma := j(\mathfrak{a})$ is a full lattice in $K_{\mathbb{R}}$ with* $\mathrm{Vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O}_K : \mathfrak{a}]$.

Proof. Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Consider $A = (\tau_l(\alpha_i))_{il}$. Then $d(\mathfrak{a}) = \det(A)^2 = [\mathcal{O}_K : \mathfrak{a}]^2 d_K$. On the other hand, $j(\alpha_1), \dots, j(\alpha_n)$ is a $\mathbb{Z}$-basis of Γ. We have $j(\alpha_i) = (\tau_l(\alpha_i))_l$, so that

$$\langle j(\alpha_i), j(\alpha_k)\rangle = \sum_{l} \tau_l(\alpha_i) \overline{\tau_l(\alpha_k)}.$$

Hence the structure matrix of $\langle -,-\rangle$ is $(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k} = A\overline{A}^t$, so

$$\mathrm{Vol}(\Gamma) = \sqrt{\det(A\overline{A}^t)} = |\det(A)| = [\mathcal{O}_K : \mathfrak{a}]\sqrt{|d_K|}.$$

In particular, the volume of a fundamental domain is nonzero, so the lattice is full. □

Theorem 4.8. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an ideal. Let $c_\tau \in \mathbb{R}_{>0}$ such that $c_\tau = c_{\overline{\tau}}$. Assume that $\prod_\tau c_\tau > (\frac{2}{\pi})^s \sqrt{|d_k|}[\mathcal{O}_K : \mathfrak{a}]$. Then there exists $0 \neq a \in \mathfrak{a}$ with $|\tau(a)| < c_\tau$ for all τ.*

Proof. Look at $X := \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau\}$. Then X is convex and central-symmetric. One computes

$$\mathrm{Vol}(X) = 2^{r+s}\pi^s \prod_{\tau} c_\tau > 2^n \mathrm{Vol}(j(\mathfrak{a})).$$

Therefore, the conditions of Minkowski's Lattice Point Theorem 3.11 are satisfied, so there exists $0 \neq j(a) \in j(\mathfrak{a}) \cap X$. This is the desired $a \in \mathfrak{a}$. □

Lecture 10
Nov 14, 2025

Definition 4.9. For $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ we define its norm

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

In the exercises we saw that this ideal norm is multiplicative, hence we may extend it to a multiplicative function $\mathrm{N} : I_K \to \mathbb{Z}$ on all fractional ideals.

Lemma 4.10. *Let* $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$. *Then there exists* $0 \neq a \in \mathfrak{a}$ *with* $|\mathrm{N}_{K/\mathbb{Q}}(a)| \leq (\frac{2}{\pi})^s \sqrt{|d_K|}\,\mathrm{N}(\mathfrak{a})$.

Proof. For $\varepsilon > 0$ choose $c_\tau \in \mathbb{R}_{>0}$, $c_{\overline{\tau}} = c_\tau$ such that $\prod_\tau c_\tau = (\frac{2}{\pi})^s \sqrt{|d_K|}\,\mathrm{N}(\mathfrak{a}) + \varepsilon$. By theorem 4.8, there exists $0 \neq a \in \mathfrak{a}$ such that $|\tau(a)| < c_\tau$, hence

$$|\mathrm{N}_{K/\mathbb{Q}}(a)| = \prod_\tau |\tau(a)| < \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathrm{N}(\mathfrak{a}) + \varepsilon.$$

Since the norm is an integer, for small enough ε we get the claim. □

Theorem 4.11. *The class number is finite:* $h_K := |\mathrm{cl}_K| < \infty$.

Proof. For each $M > 0$, there are only finitely many integral ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ with $\mathrm{N}(\mathfrak{a}) < M$. Indeed, since each such integral ideal factors into prime ideals, it suffices to show that there are only finitely many prime ideals of bounded norm. But by the exercises, $\mathrm{N}(\mathfrak{p})$ is a p-power, where $p \in \mathbb{Z}$ is the prime such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Since there are only finitely many prime ideals containing each prime p, we are done.

Hence it suffices to show that each ideal class $c \in \mathrm{cl}_K$ contains an integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ such that $\mathrm{N}(\mathfrak{a}) \leq (\frac{2}{\pi})^s \sqrt{|d_K|}$. So let $\mathfrak{b} \in c$ be a representative. Choose $\gamma \in \mathcal{O}_K$ such that $\gamma\mathfrak{b}^{-1} \subseteq \mathcal{O}_K$ is an integral ideal. Then by the previous lemma, there exists $0 \neq \alpha \in \gamma\mathfrak{b}^{-1}$ such that

$$|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}\,\mathrm{N}(\gamma\mathfrak{b}^{-1}).$$

Using the following lemma, the integral ideal $\alpha\gamma^{-1}\mathfrak{b}$ satisfies $\mathrm{N}(\alpha\gamma^{-1}\mathfrak{b}) \leq (\frac{2}{\pi})^s \sqrt{|d_K|}$. □

Lemma 4.12. *For* $0 \neq \alpha \in K$ *one has* $\mathrm{N}(\alpha\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$.

Proof. Let $\omega_1, \ldots, \omega_n$ be an integral basis of $\mathcal{O}_K$. Let $\alpha(\omega_1, \ldots, \omega_n)^t = A(\omega_1, \ldots, \omega_n)^t$ for $A \in M_n(\mathbb{Z})$. Then $[\mathcal{O}_K : \alpha\mathcal{O}_K] = |\det(A)| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$. □

Remark 4.13. The proof of theorem 4.11 yields a finite generating set for the class group:

$$\mathrm{cl}_K = \langle [\mathfrak{a}] \mid 0 \neq \mathfrak{a} \subseteq \mathcal{O}_K, \mathrm{N}(\mathfrak{a}) \leq (\tfrac{2}{\pi})^s \sqrt{|d_K|} \rangle.$$

In fact, the bound on $\mathrm{N}(\mathfrak{a})$ can be improved: Let

$$X = \left\{ (z_\tau)_\tau \in K_\mathbb{R} \mid \sum_\tau |z_\tau| < t \right\}.$$

Then X is central-symmetric, convex, and $\mathrm{Vol}(X) = 2^r \pi^s \frac{t^n}{n!}$. Repeating the above proofs with this set, one obtains

Theorem 4.14. *Let* $0\mathfrak{a} \subseteq \mathcal{O}_K$ *be an integral ideal. Then there exists* $0 \neq a \in \mathfrak{a}$ *such that* $|\mathrm{N}_{K/\mathbb{Q}}(a)| \leq M \cdot \mathrm{N}(\mathfrak{a})$ *with the* Minkowski constant

$$M := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}.$$

Therefore, cl_K *is generated by classes of ideals* $\mathfrak{a}$ *with* $\mathrm{N}(\mathfrak{a}) \leq M$.

Proof. Exercise. □

Example 4.15. (i) Let $K = \mathbb{Q}(\sqrt{2})$. Then $M = \sqrt{2} \approx 1.41$. But the only integral ideal with norm 1 is $\mathcal{O}_K$, so $\mathrm{cl}_K = 1$.

(ii) Let $K = \mathbb{Q}(\sqrt{-5})$. Then $M = \frac{4}{\pi}\sqrt{5} \approx 2.84$. Hence cl_K is generated by the classes of integral ideals of norm ≤ 2. By factoring (2), one can compute directly that the only such ideals are $\mathcal{O}_K$ and $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle_{\mathbb{Z}}$ with $\mathrm{ord}([\mathfrak{p}]) \leq 2$ since $\mathfrak{p}^2 = (2)$. So $\mathrm{cl}_K = 1$ if $\mathfrak{p}$ is principal, or $\mathrm{cl}_K = \mathbb{Z}/2\mathbb{Z}$ otherwise. Here, the latter is the case, so $h_K = 2$.

Generalizing the last example, we can give a general procedure for computing the class group: List all prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ with $\mathrm{N}(\mathfrak{p}_i) \leq M$, by factoring $p\mathcal{O}_K$ for $p \leq M$ prime. Then cl_K is generated by their classes (it suffices to consider prime ideals by prime ideal factorization). Let $\pi : \mathbb{Z}^m \to \mathrm{cl}_K$, $a \mapsto \prod_i [\mathfrak{p}_i]^{a_i}$ and $\Lambda := \ker \pi$. This gives an exact sequence

$$0 \to \Lambda \to \mathbb{Z}^m \xrightarrow{\pi} \mathrm{cl}_K \to 1.$$

Every relation comes from an equation $\alpha\mathcal{O}_K = \prod_i \mathfrak{p}_i^{a_i}$, $\alpha \in K^\times$. Finding sufficiently many of such relations, one can determine the class group.

Lemma 4.16. *Let $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ be an integral ideal. Then $\mathfrak{a}$ is a principal ideal if and only if $\mathrm{N}(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)|$ for some $\alpha \in \mathfrak{a}$.*

Proof. One direction was proven in lemma 4.12. Conversely, suppose α as in the statement exists. Then $\alpha\mathcal{O}_K \subseteq \mathfrak{a}$ is a submodule, but again by lemma 4.12, their indices in $\mathcal{O}_K$ are equal. □

5 Dirichlet's Unit Theorem

5.1 Statement and Proof

Lecture 11
Nov 19, 2025

The next goal is to understand the unit group of a number ring. Let

$$K_{\mathbb{R}}^\times := \{(z_\tau)_\tau \in K_{\mathbb{R}} \mid z_\tau \neq 0 \text{ for all } \tau\}$$

and consider the map

$$l : K_{\mathbb{R}}^\times \to \mathbb{R}^{r+s}, \qquad (z_\tau)_\tau \mapsto (\log|x_{\rho_1}|, \dots, \log|x_{\rho_r}|, 2\log|x_{\sigma_1}|, \dots, 2\log|x_{\sigma_s}|).$$

Then clearly $l(xy) = l(x) + l(y)$ for $x, y \in K_{\mathbb{R}}^\times$. Further define a norm $\mathrm{N} : K_{\mathbb{R}}^\times \to \mathbb{R}^\times$ and trace $\mathrm{Tr} : \mathbb{R}^{r+s} \to \mathbb{R}$ by $\mathrm{N}((z_\tau)_\tau) := \prod_\tau z_\tau$ and $\mathrm{Tr}(x) = \sum_{i=1}^{r+s} x_i$ Putting everything together, we have the following commutative diagram of group homomorphisms:

$$\begin{tikzcd} K^\times \arrow[r, "j"] \arrow[d, "\mathrm{N}_{K/\mathbb{Q}}"] & K_{\mathbb{R}}^\times \arrow[r, "l"] \arrow[d, "\mathrm{N}"] & \mathbb{R}^{r+s} \arrow[d, "\mathrm{Tr}"] \\ \mathbb{Q}^\times \arrow[r, hook] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R} \end{tikzcd}$$

Also let $\lambda := l \circ j$. Since units in $\mathcal{O}_K$ are characterized by their norm being ± 1, further define

$$S := \{y \in K_R^\times \mid \mathrm{N}(y) = \pm 1\}, \qquad H = \{x \in \mathbb{R}^{r+s} \mid \mathrm{Tr}(x) = 0\}.$$

Then $j(\mathcal{O}_K^\times) \subseteq S$ and $l(S) = H$.

Definition 5.1. $\Gamma := \lambda(\mathcal{O}_K^\times) \subseteq H$

Theorem 5.2. *(i) There is a short exact sequence* $1 \to \mu_K \to \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \to 0$*, where* $\mu_K := \{x \in K^\times \mid \operatorname{ord}(x) < \infty\}$.
(ii) $|\mu_K| < \infty$.

Proof. We have to show that $\ker(\lambda) = \mu_K$. "$\supseteq$" is clear, either by direct computation or by noticing that H has no torsion elements. Conversely, let $\alpha \in \ker\lambda$. Then $|\tau(\alpha)| = 1$ for all τ, hence also $|\tau(\alpha^n)| = 1$ for all $n \geq 1$. Looking at $\chi_{\alpha^n}(t) = \prod_\tau(t - \tau(\alpha^n))$, we see that all coefficients are bounded. Hence there are only finitely many possilbe characteristic polynomials, each with finitely many zeroes, among the α^n. So $\alpha^i = \alpha^j$ for some $i > j$, i.e. $\alpha^{i-j} = 1$. The same argument also shows (ii). □

Lemma 5.3. *Up to multiplication by elements in* $\mathcal{O}_K^\times$*, there are only finitely many* $\alpha \in \mathcal{O}_K$ *with* $|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| = a$*, where* $a \in \mathbb{N}$ *is given.*

Proof. We have $|\operatorname{N}_{K/\mathbb{Q}}(\alpha)| = \operatorname{N}(\alpha\mathcal{O}_K)$ by lemma 4.12, but in the proof of theorem 4.11, we already showed that there are only finitely many ideals of bounded norm. □

Theorem 5.4. Γ *is a full lattice in* H*, i.e.* $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Proof. To show that Γ is a lattice, we may show by theorem 3.6 that it is discrete. By lemma 3.4, it suffices to show that for all $c \in \mathbb{R}_{>0}$ one has $B_c \cap \Gamma$ finite, where $B_c := \{(x_\tau) \in \mathbb{R}^{r+s} \mid |x_\tau| < c\}$. But by definition of the map l, this is the same as requiring $e^{-c} < x_\rho < e^c$ for real embeddings and $e^{-\frac{1}{2}c} < x_\sigma < e^{\frac{1}{2}c}$ for complex embeddings, which is finite again by lemma 3.4, since $j(\mathcal{O}_K) \supseteq j(\mathcal{O}_K^\times)$ is a lattice by theorem 4.7.

We now have to show that Γ has full rank. We want to apply lemma 3.7, i.e. construct a bounded set $M \subseteq H$ s.t. $\bigcup_{\gamma\in\Gamma} \gamma + H = H$. For this, we construct a bounded set $T \subseteq S$ s.t. $S = \bigcup_{\varepsilon\in\mathcal{O}_K^\times} Tj(\varepsilon)$. Then by surjectivity of λ the translates of $M := l(T)$ clearly cover H. Let $x \in T$. Then $|x_\tau|$ is bounded from above since T is bounded. But then $|x_\tau|$ is also bounded from below (away from 0) because $\prod_\tau |x_\tau| = 1$. Therefore, $\log|x_\tau|$, and hence M, are bounded, and the theorem follows.

To construct T, choose $c_\tau > 0$ with $c_{\overline{\tau}} = c_\tau$ and $C := \prod_\tau c_\tau > (\frac{2}{\pi})^s\sqrt{|d_K|}$. Consider $X = \{(z_\tau)_\tau \in K_\mathbb{R} \mid |z_\tau| < c_\tau\}$. For $y \in S$ one has $Xy = \{z \in K_\mathbb{R} \mid |z_\tau| < c'_\tau\}$ with $c'_\tau = c_\tau|y_\tau|$, $c'_{\overline{\tau}} = c'_\tau$ and $\prod_\tau c'_\tau = C\prod_\tau |y_\tau| = C$. Hence by lemma 4.10 there exists $0 \neq a \in \mathcal{O}_K$ with $j(a) \in Xy$.

By lemma 5.3 there exist $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$ such that each $a \in \mathcal{O}_K$ with $0 < |\operatorname{N}_{K/\mathbb{Q}}(a)| < C$ is associated to one of the α_i. Now set

$$T := S \cap \bigcup_{i=1}^N Xj(\alpha_i)^{-1}.$$

We claim this T has the required properties. It is clear that T is bounded, since X is. So let $y \in S$. By the previous paragraph, there exists $0 \neq a \in \mathcal{O}_K$ with $j(a) \in Xy^{-1}$, i.e. $j(a) = xy^{-1}$ for some $x \in X$. Since $|\operatorname{N}_{K/\mathbb{Q}}(a)| = |\operatorname{N}(xy^{-1})| = |\operatorname{N}(x)| < C$, there exists α_i such that $\alpha_i = \varepsilon a$, $\varepsilon \in \mathcal{O}_K^\times$. Then $y = xj(a)^{-1} = xj(\alpha_i\varepsilon)^{-1} = xj(\alpha_i)^{-1}j(\varepsilon)^{-1}$, hence $xj(\alpha_i)^{-1} \in S \cap Xj(\alpha_i)^{-1} \subseteq T$. Therefore $y \in Tj(\varepsilon)^{-1}$, which finishes the proof. □

Combining theorems 5.2 and 5.4, let $s : \Gamma \to \mathcal{O}_K^\times$ be a splitting of $1 \to \mu_K \to \mathcal{O}_K^\times \to \Gamma \to 0$, which exists since Γ is free. Then $\mu_K \times \Gamma \cong \mathcal{O}_K^\times$, $(\varepsilon, \gamma) \mapsto \varepsilon \cdot s(\gamma)$ is an isomorphism. That is, we have proven

Theorem 5.5. *$\mathcal{O}_K^\times$ is a finitely generated group of rank $t := r + s - 1$. Explicitly, there exist so-called* fundamental units *$\varepsilon_1, \ldots, \varepsilon_t \in \mathcal{O}_K^\times$ such that each $\varepsilon \in \mathcal{O}_K^\times$ has a unique representation of the form*

$$\varepsilon = \zeta \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t}$$

with $k_i \in \mathbb{Z}$ and $\zeta \in \mu_K$.

Lecture 12
Nov 21, 2025

Example 5.6. Let $K = \mathbb{Q}(\sqrt{d})$, $d > 1$ squarefree. Then $t = 1$ and $\mu_K = \{\pm 1\}$, hence there is a single fundamental unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\mathcal{O}_K^\times = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$.

5.2 The Regulator

Let K be a number field and $\varepsilon_1, \ldots, \varepsilon_t$ be fundamental units. Let $\lambda_0 := \frac{1}{\sqrt{r+s}}(1, \ldots, 1)^t \in \mathbb{R}^{r+s}$ so that $\|\lambda_0\| = 1$ and $\lambda_0 \perp H$. Hence the t-dimensional volume of Γ is equal to the $(r+s)$-dimensional volume of the $\mathbb{Z}$-span of $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$, i.e. of the matrix

$$M = \begin{pmatrix} \frac{1}{\sqrt{r+s}} & \log|\tau_1(\varepsilon_1)| & \cdots & \log|\tau_1(\varepsilon_t)| \\ \vdots & \vdots & & \vdots \\ \frac{1}{\sqrt{r+s}} & \log|\tau_{r+s}(\varepsilon_1)| & \cdots & \log|\tau_{r+s}(\varepsilon_t)| \end{pmatrix}$$

Let Φ be a fundamental domain of $\Gamma = \lambda(\mathcal{O}_K^\times)$. Then $\operatorname{Vol}(\Phi) = |\det(M)|$.

Theorem 5.7. $\operatorname{Vol}(\Gamma) = \sqrt{r+s}R$*, where R is an arbitrary $t \times t$-minor of* $(\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t))$.

Definition 5.8. $R_K := R$ as in theorem 5.7 is called the *regulator* of K (Exercise: It is independent of the choice of fundamental units).

Proof. Fix some i and add all rows to the i-th row. Then this row becomes $(\sqrt{r+s}, 0, \ldots, 0)$. □

Lemma 5.9. *Let V be a finite-dimensional $\mathbb{R}$-vector space. Let $\Gamma \subseteq V$ be a full lattice, and $\Gamma' \subseteq V$ be a sublattice. Then Γ' is full if and only if* $\operatorname{Vol}(\Gamma') \neq 0$*, and in this case* $[\Gamma : \Gamma'] = \operatorname{Vol}(\Gamma')/\operatorname{Vol}(\Gamma)$.

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis of Γ, and $\omega_1', \ldots, \omega_n'$ a $\mathbb{Z}$-basis of Γ'. Let Φ, Φ' be the corresponding fundamental domains, and let $\omega_i' = \sum_i t_{ji}\omega_j$, with $t_{ji} \in \mathbb{Z}$. Then $T = (t_{ji}) \in \mathrm{GL}_n(\mathbb{Q})$ and

$$\operatorname{Vol}(\Gamma') = \operatorname{Vol}(\Phi') = \int_{\Phi'} dx = \int_{\Phi} |\det(T)| dx = |\det(T)| \operatorname{Vol}(\Gamma) = [\Gamma : \Gamma'] \operatorname{Vol}(\Gamma).$$

The other direction is clear. □

Theorem 5.10. *Let $\eta_1, \ldots, \eta_t \in \mathcal{O}_K^\times$. Then the η_i are independent (i.e. $[\mathcal{O}_K^\times : \langle \eta_1, \ldots, \eta_t\rangle] < \infty$) if and only if $R(\eta_1, \ldots, \eta_t) \neq 0$, where $R(\eta_1, \ldots, \eta_t)$ is defined as a $t \times t$-minor of the matrix $(\lambda(\eta_1), \ldots, \lambda(\eta_t))$ as before. Further, $[\mathcal{O}_K^\times/\mu_K : \langle \eta_1, \ldots, \eta_t\rangle\mu_K/\mu_K] = R(\eta_1, \ldots, \eta_t)/R_K$.*

Proof. Exercise. □

Remark 5.11. Regulators are in general transcendental numbers.

Let $\zeta_K(s) := \sum_{0 \neq \mathfrak{a} \trianglelefteq \mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}}(1 - \frac{1}{\mathrm{N}(\mathfrak{p})^s})^{-1}$ for $\mathrm{Re}(s) > 1$ be the Dedekind L-function of K. In the special case $K = \mathbb{Q}$, this is the usual Riemann zeta function. As in this special case, ζ_K can be analytically extended to a meromorphic function on all of $\mathbb{C}$, with a simple pole only at $s = 1$. Further, ζ_K satisfies a functional equation of the form

$$\zeta_K(1-z) = 2|d_K|^{s-1/2} \cos(\tfrac{\pi z}{2})^{r+s} \sin(\tfrac{\pi z}{2})^s (2\pi)^{-z}\Gamma(z)\zeta_K(z).$$

$\zeta_K(s)$ has a zero at $s = 0$ of order t and the leading term is $\pm h_K R_K$. This is the so-called *analytic class number formula*, which is proved in analytic number theory.

Example 5.12. (i) For imaginary quadratic fields, one has $t = 0$, so $\mathcal{O}_K^\times$ is finite.

(ii) For real quadratic fields, one has $t = 1$, and we will see how to compute a fundamental unit.

(iii) Let $K = \mathbb{Q}(\sqrt[3]{m})$ for m cubefree. Then $t = 1 + 1 - 1 = 1$.

(iv) Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field. Then $K/\mathbb{Q}$ is a Galois extension with Galois group $G = (\mathbb{Z}/m\mathbb{Z})^\times$. We have $\varphi(m)$ complex embeddings $\sigma_a : \zeta_m \mapsto \zeta_m^a$, so $t_K = \frac{1}{2}\varphi(m) - 1$. Let $K^+ := \mathbb{Q}(\zeta_m + \zeta_m^{-1}) = K \cap \mathbb{R}$ be the fixed field of σ_{-1}. This is the largest totally real subfield of K of degree $\frac{1}{2}\varphi(m)$, so $t_{K^+} = \frac{1}{2}\varphi(K) - 1 = t_K =: t$. Let $\mathcal{O}_{K^+}^\times = \pm\varepsilon_1^{\mathbb{Z}} \cdots \varepsilon_t^{\mathbb{Z}}$, then $[\mathcal{O}_K^\times : \mathcal{O}_{K^+}] < \infty$. Actually the index is small, cf. exercises.

For $m = p$, p an odd prime, the element $\frac{\zeta_p^a - 1}{\zeta_p - 1}$, $(a, p) = 1$ is a unit, since if $ab = 1 \bmod p$, then

$$\frac{\zeta_p - 1}{\zeta_p^a - 1} = \frac{\zeta_p^{ab} - 1}{\zeta_p^a - 1} = \sum_{i=0}^{b-1} \zeta_p^{ai} \in \mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K.$$

Hence we have $p - 2$ nontrivial units (for $a = 2, \ldots, p - 1$), called *cyclotomic units*. One can show that the index of the subgroup generated by them depends explicitly on h_K. (The above can be generalized to $\mathbb{Q}(\zeta_m)$ for m not a prime.) See Washington, Cyclotomic Units for details.

5.3 The fundamental unit in a real quadratic field

Let $d > 1$ be squarefree, and $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K \ni \alpha = \frac{1}{2}(x + y\sqrt{d})$, $x, y \in \mathbb{Z}$, is a unit if and only if $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Corollary 5.13. *The units of $\mathcal{O}_K$ are in 1-1 correspondence with the solutions $(x, y) \in \mathbb{Z}^2$ of the (generalized)* Pell's equation $x^2 - dy^2 = \pm 4$.

Let $\pm 1 \neq \eta \in \mathcal{O}_K^\times$. Then $\eta, \eta^{-1}, -\eta, -\eta^{-1}$ are four different units. Let τ be the nontrivial Galois automorphism of K, then $\tau(\eta) = \pm\eta^{-1}$. Then if $\eta = x + y\sqrt{d}$, then

$$\{\eta, \eta^{-1}, -\eta, -\eta^{-1}\} = \{\eta, \tau(\eta), -\eta, -\tau(\eta)\} = \{\pm x \pm y\sqrt{d}\},$$

so there is exactly one fundamental unit $\varepsilon > 0$ with $\varepsilon > 1$. Such a unit $\frac{1}{2}(a + b\sqrt{d})$ with $a, b > 0$ is called *normalized*.

Lecture 13
Nov 26, 2025

Theorem 5.14. *$\eta = a + b\sqrt{d}$ with $a, b \in \frac{1}{2}\mathbb{Z}$, $a, b > 0$ is the normalized fundamental unit if and only if for any unit $\varepsilon = c + e\sqrt{d} > 1$ we have $a < c$.*

Proof. Let $u = p + q\sqrt{d}$ be the normalized fundamental unit. Let $\varepsilon = c + d\sqrt{d} > 1$ be a unit. Then $\varepsilon = u^m =: p_m + q_m\sqrt{d}$ for some $m > 0$. Hence it suffices to show that $(p_m)_m$ is strictly increasing. Note that $p_{m+1} = pp_m + dqq_m$, $q_{m+1} = pq_m + qp_m$, so if $p \geq 1$ (in particular if $d \not\equiv 1 \bmod 4$) we immediately see $p_{m+1} > p_m$. Otherwise, assume that $p = \frac{1}{2}$. Then $\frac{1}{4} - q^2 d = \pm 1$ by Pell's equation, which immediately implies $q = \frac{1}{2}, d = 5$. Here we have $u = \frac{1+\sqrt{5}}{2}$. □

Example 5.15. Using the above theorem, we can algorithmically calculate the normalized fundamental unit by finding the solution of $x^2 - dy^2 = \pm 4$ with smallest $x > 0$. We find

d	2	3	5	13	46
ε	$1 + \sqrt{2}$	$2 + \sqrt{3}$	$\frac{1+\sqrt{5}}{2}$	$\frac{3+\sqrt{13}}{2}$	$24335 + 3588\sqrt{46}$

This last example shows that fundamental units can be very large compared to d, so our naive algorithm can be very inefficient. There are better algorithms, for example using continued fractions.

6 Extensions of Dedekind Domains

Let L/K be an extension of number fields. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal. We want to understand how the ideal $\mathfrak{p}\mathcal{O}_L$ of $\mathcal{O}_L$ factors.

Note first that $\mathfrak{p}\mathcal{O}_L \subsetneq \mathcal{O}_L$. Indeed, let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Then $\pi\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{a} + \mathfrak{p} = \mathcal{O}_K$. Write $1 = b + s$ with $s \in \mathfrak{a}, b \in \mathfrak{p}$. Then $s\mathfrak{p} \subseteq \mathfrak{a}\mathfrak{p} = \pi\mathcal{O}_K$. Suppose now $\mathfrak{p}\mathcal{O}_L = \mathcal{O}_L$. Then $s\mathcal{O}_L = s\mathfrak{p}\mathcal{O}_L \subseteq \pi\mathcal{O}_L$, i.e. $s = \pi x$ with $x \in \mathcal{O}_L \cap K = \mathcal{O}_K$. But then $s \in \mathfrak{p}$, contradiction.

So let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ be the nonempty prime factorization of $\mathfrak{p}\mathcal{O}_L$. Then the $\mathfrak{P}_i$ are precisely the primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$, i.e. $\mathfrak{P}_i \cap \mathcal{O}_L = \mathfrak{p}$. (Exercise) In this case we also write $\mathfrak{P} \mid \mathfrak{p}$, and call $\mathfrak{P}$ a prime divisor of $\mathfrak{p}$.

The exponents e_i are called *ramification indices*. Furthermore, $f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ is called the residue field degree or *inertia degree*. Here, the field extension is induced by the natural map $\mathcal{O}_K \hookrightarrow \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}_i$.

Theorem 6.1. *Let L/K be separable[2]. Then $\sum_{i=1}^r e_i f_i = n := [L : K]$.*

Proof. By the Chinese Remainder Theorem, we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_L/\mathfrak{P}_1^{e_1} \times \cdots \times \mathcal{O}_L/\mathfrak{P}_r^{e_r}.$$

Let $k := \mathcal{O}_K/\mathfrak{p}$. It suffices to show $\dim_k \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$ and $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$.

Let $\omega_1, \dots, \omega_m \in \mathcal{O}_L$ such that $\overline{\omega}_1, \dots, \overline{\omega}_m \in \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ are a k-basis. We will show that $\omega_1, \dots, \omega_m$ are a K-basis of L (hence $m = n$). Let $a_1\omega_1 + \ldots + a_m\omega_m = 0$ with $a_i \in \mathcal{O}_K$ not all 0. Then $\mathfrak{a} = (a_1, \dots, a_m) \neq 0$. Choose $a \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. Then $a\mathfrak{a} \not\subseteq \mathfrak{p}$, hence $aa_1, \dots, aa_m \in \mathcal{O}_K$ are not all contained in $\mathfrak{p}$. But then $a(a_1\omega_1 + \ldots + a_m\omega_m) \equiv 0 \bmod \mathfrak{p}\mathcal{O}_L$ contradicts the independence of the $\overline{\omega}_i$. Hence $\omega_1, \dots, \omega_m$ are linearly independent.

Consider $M = \mathcal{O}_K\omega_1 + \ldots + \mathcal{O}_K\omega_n \subseteq \mathcal{O}_L$ and $N = \mathcal{O}_L/M$. Then $\mathfrak{p}N = (\mathfrak{p}\mathcal{O}_L + M)/M = N$. Let $\alpha_1, \dots, \alpha_s \in N$ be a set of generators of N over $\mathcal{O}_K$. Then we find relations $\alpha_i = \sum_{j=1}^s a_{ij}\alpha_j$ with $a_{ij} \in \mathfrak{p}$. Let $A = (a_{ij}) - E_s$. Then $A(\alpha_1, \dots, \alpha_s)^t = 0$, so by 1.4 we find $\det(A)N = 0$ with $\det(A) \equiv \det(-E_s) = \pm 1 \bmod p$, in particular $\det(A) \neq 0$. Hence $\det(A)\mathcal{O}_L \subseteq M = \mathcal{O}_K\omega_1 + \ldots + \mathcal{O}_K\omega_n$, so $L = K\omega_1 + \ldots + K\omega_n$.

Thus $\dim_k \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = n$. For $\dim_k \mathcal{O}_L/\mathfrak{P}_i^{e_i}$, look at the filtration $\mathcal{O}_L \supseteq \mathfrak{P} \supseteq \mathfrak{P}^2 \supseteq \ldots \supseteq \mathfrak{P}^e$. By induction, it suffices to prove $\dim_k(\mathfrak{P}^i/\mathfrak{P}^{i+1}) = f_i$, which was done in the exercises. □

Note that for $L/\mathbb{Q}$ we can give a much simpler proof: By definition of the f_i we have

$$p^n = \mathrm{N}_{L/\mathbb{Q}}(p) = \mathrm{N}(p\mathcal{O}_L) = \prod_i \mathrm{N}(\mathfrak{P}_i)^{e_i} = \prod_i p^{e_i f_i} = p^{\sum_i e_i f_i}$$

Assume L/K separable and $L = K(\theta)$ with $\theta \in \mathcal{O}_L$. Let $f \in \mathcal{O}_K[X]$ be the minimal polynomial of θ. Set $\mathcal{O} := \mathcal{O}_K[\theta] \subseteq \mathcal{O}_L$.

Definition 6.2. $\mathfrak{f} := \{\alpha \in \mathcal{O}_L \mid \alpha\mathcal{O}_L \subseteq \mathcal{O}\}$ is called the *conductor* of $\mathcal{O}$ in $\mathcal{O}_L$.

Note that $\mathfrak{f}$ is the largest $\mathcal{O}_L$-ideal which is contained in $\mathcal{O}$. In particular, $\mathcal{O} = \mathcal{O}_L$ if and only if $\mathfrak{f} = 1$.

Lemma 6.3. *Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal. Then $\mathfrak{p}$ is not invertible if and only if $\mathfrak{f} \subseteq \mathfrak{p}$*

Proof. Exercise. □

[2]That is, more generally, we may consider a finite separable field extension L/K with Dedekind domains $R \subseteq K$, $\mathcal{O} \subseteq L$ such that $\mathcal{O} = \mathcal{O}_{R,L}$ and $\mathrm{Quot}(R) = K$

Theorem 6.4. *Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal with $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$. Let*

$$\overline{f}(x) = \overline{f}_1(x)^{e_1} \cdots \overline{f}_r(x)^{e_r} \qquad \text{in } k[x] := \mathcal{O}_K/\mathfrak{p}[x]$$

with pairwise distinct irreducible polynomials $\overline{f}_i \in k[x]$. Then the $\mathfrak{P}_i := \mathfrak{p}\mathcal{O}_L + f_i(\theta)\mathcal{O}_L$, $i = 1, \ldots, r$ are exactly the primes of $\mathcal{O}_L$ over $\mathfrak{p}$. We have $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and $f_i = \deg(\overline{f}_i)$.

Example 6.5. Let $L = \mathbb{Q}(\sqrt{d})$ with $d \equiv 2, 3 \bmod 4$ squarefree. Then $f(X) = X^2 - d$ and $\mathfrak{f} = 1$. If $p \mid d$, then $\overline{f} = X^2$, so $p\mathcal{O}_L = (p, \sqrt{d})^2 = \langle p, \sqrt{d} \rangle_{\mathbb{Z}}$. If $p \nmid d$ and d is a square mod p, then $X^2 - d \equiv (X - \overline{a})(X + \overline{a}) \bmod p$ for some a, so $p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$ with $\mathfrak{P}_{1,2} = (p, a \pm \sqrt{d})$. Finally, if $p \nmid d$ and d is not a square mod p, then $\overline{f}$ is irreducible and $p\mathcal{O}_L = (p)$. Similar calculations work for $d \equiv 1 \bmod 4$ as well, except that $\mathfrak{f} = 2\mathcal{O}_L$, so $p = 2$ has to be treated separately.

Proof. Consider the maps Lecture 14 Nov 28, 2025

$$k[x]/(\overline{f}(x)) \xrightarrow{\overline{\alpha}} \mathcal{O}/\mathfrak{p}\mathcal{O} \xrightarrow{\overline{\beta}} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

induced by $\alpha(\overline{g}) := g(\theta) + \mathfrak{p}\mathcal{O}$ and $\beta(\alpha) = \alpha + \mathfrak{p}\mathcal{O}_L$.

By universal properties, $\overline{\alpha}$ and $\overline{\beta}$ are well-defined. Further α is surjective since any element $g(\theta) + \mathfrak{p}\mathcal{O}$ is hit by $\overline{g}(x)$. If $\overline{g} \in \ker \alpha$, then $g(\theta) \in \mathfrak{p}\mathcal{O} = \mathfrak{p}[\theta]$. Hence $g(\theta) = h(\theta)$ for some $h \in \mathfrak{p}[\theta]$, i.e. $f \mid g - h$ in $\mathcal{O}_K[x]$. But then $\overline{f} \mid \overline{g}$, so $\overline{\alpha}$ is an isomorphism.

By assumption, $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$, hence also $\mathfrak{p}\mathcal{O}_L + \mathcal{O} = \mathcal{O}_L$, so β is surjective. Clearly $\mathfrak{p}\mathcal{O} \subseteq \ker \beta$. For the converse, we will show

$$\mathfrak{p} + (\mathfrak{f} \cap \mathcal{O}_K) = \mathcal{O}_K. \tag{$*$}$$

Then $\ker \beta = \mathcal{O} \cap \mathfrak{p}\mathcal{O}_L \subseteq (\mathfrak{p} + \mathfrak{f})(\mathcal{O} \cap \mathfrak{p}\mathcal{O}_L) \subseteq \mathfrak{p}\mathcal{O}$. To prove $(*)$, suppose $\mathfrak{f} \cap \mathcal{O}_K \subseteq \mathfrak{p}$. Let $\mathfrak{f} = \mathfrak{q}_1^{s_1} \cdots \mathfrak{q}_m^{s_m}$. Then $\mathfrak{f} \cap \mathcal{O}_K = (\mathfrak{q}_1^{s_1} \cap \mathcal{O}_K) \cap \ldots \cap (\mathfrak{q}_m^{s_m} \cap \mathcal{O}_K)$, so say $\mathfrak{q}_1^{s_1} \cap \mathcal{O}_K \subseteq \mathfrak{p}$. Hence $\mathfrak{p} \mid (\mathfrak{q}_1 \cap \mathcal{O}_K)^{s_1}$, and since $\mathfrak{q}_1 \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, we have $\mathfrak{p} = \mathfrak{q}_1 \cap \mathcal{O}_K$. Hence $\mathfrak{q}_1$ occurs in the prime decomposition of both $\mathfrak{f}$ and $\mathfrak{p}$, in contradiction to the coprime assumption.

Hence $\overline{\beta} \circ \overline{\alpha}$ is an isomorphism. In particular, prime ideals of $k[x]$ above $\overline{f}(x)$ correspond bijectively to prime ideals of $\mathcal{O}_L$ above $\mathfrak{p}\mathcal{O}_L$. But the former are exactly of the form $(\overline{f}_i(x))$, which are mapped to $\mathfrak{p}\mathcal{O}_L + f_i(\theta)\mathcal{O}_L$. ☐

Warning: There are extensions L/K such that there exists no $\theta \in \mathcal{O}_L$ with $\mathcal{O}_L = \mathcal{O}_K[\theta]$.

Definition 6.6. In the notation of the theorem, $\mathfrak{p}$ is called *completely or totally split* if $r = n$, and *unramified* if $e_i = 1$ for all i.

Theorem 6.7. *There are only finitely many ramified prime ideals.*

Proof. Let $L = K(\theta)$, $\theta \in \mathcal{O}_L$. Let $d := d(\theta) = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2 \in \mathcal{O}_K$. Let $\mathfrak{f}$ be the conductor of $\mathcal{O} = \mathcal{O}_K[\theta]$ in $\mathcal{O}_L$. Then every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_L$ prime to $d\mathfrak{f}$ is unramified.

Indeed, by theorem 6.4, the decomposition of $\mathfrak{p}\mathcal{O}_L$ corresponds to the decomposition of $\overline{f} \in k[x]$. Since $\overline{d} \neq 0 \in k$, the polynomial $\overline{f}$ has no multiple roots. Hence all $e_i = 1$. ☐

This result can be improved considerably. Without proof, we mention the following

Theorem 6.8. $\mathfrak{p}$ *is ramified in L/K if and only if* $\mathfrak{p} \mid d_{L/K}$.

Here, $d_{L/K}$ is defined as the integral ideal in $\mathcal{O}_K$ such that for every prime ideal $\mathfrak{p}$, its image in $\mathcal{O}_{K,\mathfrak{p}}$ is the discriminant $d_{L/K,\mathfrak{p}}$ of $\mathcal{O}_{L,\mathfrak{p}}/\mathcal{O}_{K,\mathfrak{p}}$, cf. remark 1.29. Such an ideal exists since $d_{L/K,\mathfrak{p}} = 1$ for almost all $\mathfrak{p}$, which follows from the following

Lemma 6.9. *With the notation as before, if $\mathfrak{p}\mathcal{O}_L + \mathfrak{f} = \mathcal{O}_L$, then $d_{L/K,\mathfrak{p}} = 1$.*

Proof. Exercise. $\square$

Remark 6.10. If $K = \mathbb{Q}$, then $\mathfrak{f} \mid d(\theta)$, for $d(\theta)\mathcal{O}_L \subseteq \mathcal{O}_K[\theta]$ by lemma 1.23.

We prove one direction of theorem 6.8 in the most interesting case $K = \mathbb{Q}$:

Theorem 6.11. *Let $K = \mathbb{Q}$. Then p is ramified only if $p \mid d_L$.*

Proof. Assume $p\mathcal{O}_L = \mathfrak{p}^e\mathfrak{a}$ with $\mathfrak{p} + \mathfrak{a} = \mathcal{O}_L$ and $e > 1$. Let $\mathfrak{b} = \mathfrak{p}^{e-1}\mathfrak{a}$, then all primes above p occur in $\mathfrak{b}$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings $L \to \mathbb{C}$, and let M be the normal closure of $L/\mathbb{Q}$. Let $\widehat{\sigma}_1, \ldots, \widehat{\sigma}_n$ be extensions of the σ_i to L. Let $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Take $\alpha \in \mathfrak{b} \setminus p\mathcal{O}_K$. Then α is contained in all primes in $\mathcal{O}_L$ above p. Let $\alpha = m_1\alpha_1 + \ldots + m_n\alpha_n$ with $m_i \in \mathbb{Z}$, wlog $p \nmid m_1$. Then $d(\alpha, \alpha_2, \ldots, \alpha_n) = d(m_1\alpha_1, \alpha_2, \ldots, \alpha_n) = m_1^2 d_L$. Hence it suffices to show $p \mid d(\alpha, \alpha_2, \ldots, \alpha_n) = \det(\sigma_i(\alpha \mid \alpha_j))_{ij}$. Let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Then $\widehat{\sigma}_i^{-1}(\mathfrak{P})$ is lying above p, so $\alpha \in \widehat{\sigma}_i^{-1}(\mathfrak{P})$ and $\sigma_i(\alpha) = \widehat{\sigma}_i(\alpha) \in \mathfrak{P}$. Hence the first column of $(\sigma_i(\alpha \mid \alpha_j))_{ij}$ is contained in $\mathfrak{P}$, so $d(\alpha, \alpha_2, \ldots, \alpha_n) \in \mathfrak{P} \cap \mathbb{Z} = (p)$. $\square$

7 Hilbert's Ramification Theory

We now assume that the extension L/K is Galois with Galois group G. Then G acts on all of $L, \mathcal{O}_L, I_L, \mathcal{O}_L^\times, \mathrm{cl}_L$.

Lecture 15
Dec 3, 2025

By a theorem of algebra, there exists a *normal basis element* $\alpha \in L$, s.t. $\{\sigma(\alpha) \mid \sigma \in G\}$ is a K-basis of L. In other words: Consider the (commutative iff G abelian) group ring $K[G] := \{\sum_{\sigma\in G} a_\sigma\sigma \mid a_\sigma \in K\}$ (with the obvious addition and multiplication). Then L becomes a $K[G]$-module via the natural action $\sum_\sigma a_\sigma\sigma \cdot \beta = \sum_\sigma a_\sigma\sigma(\beta)$, and $L \cong K[G]$ as $K[G]$-modules via $K[G] \ni \lambda \mapsto \lambda(\alpha) \in L$.

In the same way, $\mathcal{O}_K[G]$ acts on $\mathcal{O}_L$. Hence one may ask the same question: Is $\mathcal{O}_L \cong \mathcal{O}_K[G]$ as $\mathcal{O}_K[G]$-modules? The answer is negative, in general there is no integral normal basis.

Example 7.1. Let L/K be *tame*. Then $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-projective, hence $\mathcal{O}_L$ defines a class in $K_0(\mathcal{O}_K[G])$.[3]

$\mathcal{O}_L^\times$ is a $\mathbb{Z}[G]$-module via $\sum_\sigma a_\sigma\sigma \cdot u := \prod_\sigma \sigma(u)^{a_\sigma}$. Almost nothing is known about the $\mathbb{Z}[G]$-module structure of $\mathcal{O}_L^\times$.

Now we look at the action of G on I_L. If $\mathfrak{a} \in I_L$, then $\sigma(\mathfrak{a}) \in I_L$ for $\sigma \in G$. If $\mathfrak{P} \mid \mathfrak{p}$ and $\sigma \in G$, then $\sigma(\mathfrak{P}) \mid \mathfrak{p}$.

Theorem 7.2. *G acts transitively on the set of prime ideals above a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$.*

Proof. Let $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}\mathcal{O}_L$. Assume $\mathfrak{P}' \neq \sigma\mathfrak{P}$ for all $\sigma \in G$. By the Chinese Remainder Theorem, there exists $x \in \mathcal{O}_L$ with $x \equiv 0 \bmod \mathfrak{P}'$ and $x \equiv 1 \bmod \sigma\mathfrak{P}$ for all $\sigma \in G$. Then $\mathrm{N}_{L/K}(x) = \prod_\sigma \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$. On the other hand, $x \notin \sigma(\mathfrak{P})$ for all $\sigma \in G$. Hence $\mathrm{N}_{L/K}(x) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. $\square$

Definition 7.3. For a prime ideal $\mathfrak{P} \subseteq \mathcal{O}_L$, the subgroup $G_\mathfrak{P} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \subseteq G$ is called the *decomposition group* of $\mathfrak{P}$. Let $Z_\mathfrak{P} := L^{G_\mathfrak{P}}$ be the fixed field of $G_\mathfrak{P}$.

Then $\sigma \mapsto \sigma(\mathfrak{P})$ induces a bijection from $G/G_\mathfrak{P}$ to the set of primes above $\mathfrak{p}$ by the orbit-stabilizer theorem.

[3] For more in this direction, look up Fröhlich's conjecture, proven by M. Taylor, 1985.

Lemma 7.4. *(i) There are $|G/G_{\mathfrak{P}}|$ many primes of $\mathcal{O}_L$ above $\mathfrak{p}$.*
(ii) $G_{\mathfrak{P}} = 1 \iff Z_{\mathfrak{P}} = L \iff \mathfrak{p}$ is completely split.
(iii) $G_{\mathfrak{P}} = G \iff Z_{\mathfrak{P}} = K \iff \mathfrak{p}$ is fully inert, i.e. there is exactly one $\mathfrak{P}$ above $\mathfrak{p}$.
(iv) $G_{\sigma(\mathfrak{P})} = \sigma G_{\mathfrak{P}} \sigma^{-1}$.

Proof. (i)-(iii) are clear. For (iv), we have $\tau \in G_{\sigma(\mathfrak{P})}$ if and only if $\tau\sigma(\mathfrak{P}) = \sigma(\mathfrak{P})$, i.e. $\sigma^{-1}\tau\sigma \in G_{\mathfrak{P}}$. □

Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be prime. Recall that for its factorization in $\mathcal{O}_L$, we had the formula $[L : K] = n = \sum_{i=1}^{r} e_i f_i$.

Proposition 7.5. *In the above formula, one has $f := f_1 = \ldots = f_r$ and $e := e_1 = \ldots = e_r$, hence $n = ref$ and $\mathfrak{p} = \prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma(\mathfrak{P})^e$.*

Proof. Let $\mathfrak{P}, \mathfrak{P}'$ be above $\mathfrak{p}$. Let $\mathfrak{P}' = \sigma(\mathfrak{P})$, $\sigma \in G$. Then σ induces an isomorphism $\mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}'$ of $\mathcal{O}_K/\mathfrak{p}$-extensions, thus $f_{\mathfrak{P}} = f_{\mathfrak{P}'}$.

Since $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$, we see $\mathfrak{P}^\nu \mid \mathfrak{p}\mathcal{O}_L$ if and only if $(\mathfrak{P}')^\nu \mid \mathfrak{p}\mathcal{O}_L$. Since the ramification index is characterized as the highest power satisfying this divisibility, all these indices are equal. □

Theorem 7.6. *Let $\mathfrak{P} \mid \mathfrak{p}$. Let $\mathfrak{P}_Z := \mathfrak{P} \cap Z_{\mathfrak{P}}$. Then*

(i) There is exactly one prime of L above $\mathfrak{P}_Z$, namely $\mathfrak{P}$.
(ii) $\mathfrak{P}$ has ramification degree e and inertia degree f in $L/Z_{\mathfrak{P}}$, i.e. $\mathfrak{P}_Z\mathcal{O}_L = \mathfrak{P}^e$ and $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{P}_Z] = f$.
(iii) The ramification index and inertia degree of $\mathfrak{P}_Z/\mathfrak{p}$ are 1.

In addition, if $G_{\mathfrak{P}}$ is a normal subgroup, then $\mathfrak{p}$ is completely split in $Z_{\mathfrak{P}}$.

Proof. (i) $L/Z_{\mathfrak{P}}$ is Galois with $\mathrm{Gal}(L/Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$. This group acts transitively on the primes of L above $\mathfrak{P}_Z$ by lemma 7.2, yet fixes $\mathfrak{P}$.

(ii) and (iii) Let e', f' be the ramification index and inertia degree of $\mathfrak{P}_Z/\mathfrak{p}$, and e'', f'' be the corresponding numbers for $\mathfrak{P}/\mathfrak{P}_Z$. We know $e = e'e''$, $f = f'f''$ (cf. Exercises), $|G| = n = ref$ and $r = |G/G_{\mathfrak{P}}| = [Z_{\mathfrak{P}} : K]$. Hence $[L : Z_{\mathfrak{P}}] = ef$. On the other hand, $[L : Z_{\mathfrak{P}}] = 1e''f''$. Since $e'' \leq e$ and $f'' \leq f$, we get $e'' = e$, $f'' = f$, and therefore $e' = 1 = f'$. □

We want to characterize e group-theoretically. Since we already have $ef = |G_{\mathfrak{P}}|$, this automatically yields a group-theoretic characterization of f as well.

Let $\sigma \in G_{\mathfrak{P}}$. Then σ induces an isomorphism $\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$, $\alpha + \mathfrak{P} \mapsto \sigma(\alpha) + \mathfrak{P}$ with $\overline{\sigma}|_{\mathcal{O}_K/\mathfrak{p}} = \mathrm{id}$.

Definition 7.7. For a prime ideal $\mathfrak{p}$ of a number field K, write $\kappa(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ for the residue field.

Theorem 7.8. *The map $G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, $\sigma \mapsto \overline{\sigma}$ is surjective.*

Recall that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is an extension of finite fields. Since there is only one such field of each degree, we know that any such extension is cyclic, with Galois group generated by the Frobenius $\varphi(\alpha) = \alpha^{|\kappa(\mathfrak{p})|}$.

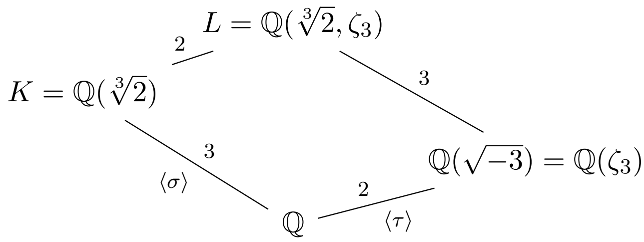
Definition 7.9. $I_{\mathfrak{P}} := \ker(\sigma \mapsto \overline{\sigma})$ is called the *inertia group* or *ramification group*.

By the above theorem, one has $G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Therefore, $|I_{\mathfrak{P}}| = e$.

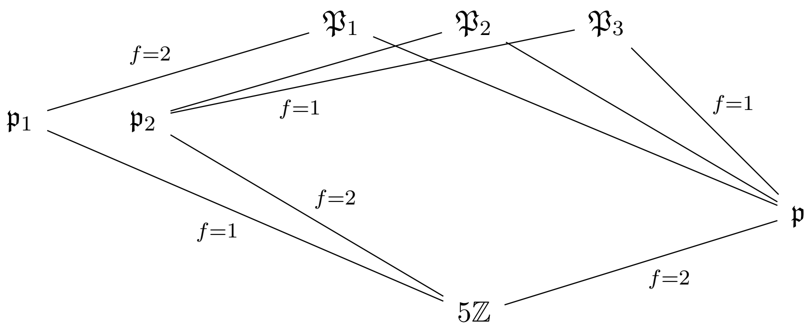
Proof. Since $\mathcal{O}_{Z_\mathfrak{P}}/\mathfrak{P}_Z = \mathcal{O}_K/\mathfrak{p}$ by theorem 7.6, we may wlog assume $Z_\mathfrak{P} = K$. Hence $G = G_\mathfrak{P}$. Let $\overline{\theta}$ be a primitive element for $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. Let $f \in K[X]$ be the minimal polynomial of $\theta \in L$, and $\overline{g} \in \kappa(\mathfrak{p})[X]$ be the minimal polynomial of $\overline{\theta}$. Then $\overline{f}(\overline{\theta}) = 0$, so $\overline{g} \mid \overline{f}$ in $\kappa(\mathfrak{p})[X]$. Let $f(X) = \prod_i (X - \theta_i)$ be the factorization of f in $L[X]$. Then $\overline{f} = \prod_i (X - \overline{\theta}_i)$, with $\overline{\theta}_i \in \kappa(\mathfrak{P})$.

Let $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Then $\overline{\sigma}(\overline{\theta}) = \overline{\theta}_i$ for some i. There is $\sigma_1' \in G(K(\theta)/K, K^c/K)$ with $\sigma_1'(\theta) = \theta_i$. Let $\sigma_1 \in G$ be an extension of σ_1'. Then $\overline{\sigma}_1 = \overline{\sigma}$, since they agree on the generator $\overline{\theta}$. □

Example 7.10. Consider the number fields



By theorem 6.11 and a short calculation, one sees that 5 is unramified in $L/\mathbb{Q}$. From 6.4, we see $5\mathbb{Z} = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathcal{O}_K$, with $f_1 = 1$, $f_2 = 2$. Then $\mathfrak{p}_1\mathcal{O}_L = \mathfrak{P}_1$, because $X^2 + X + 1$ is irreducible in $\mathcal{O}_K/\mathfrak{p}_1[X] \cong \mathbb{Z}/5\mathbb{Z}[X]$. Hence $G_{\mathfrak{P}_1|5} = \langle\tau\rangle$. Now we see by 7.5 that there are two prime ideals above $\mathfrak{p}_2$, both with inertia degree 1. By example 6.5, $5\mathbb{Z}$ is inert in $\mathbb{Q}(\sqrt{-3})$, so we have the following diagram of primes above 5:



Note that by definition $I_\mathfrak{P} = \{\sigma \in G_\mathfrak{P} \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}, \forall \alpha \in \mathcal{O}_L\}$. In the exercises we will show that one can replace $\sigma \in G_\mathfrak{P}$ by $\sigma \in G$ in the last set. Let $T_\mathfrak{P} = L^{I_\mathfrak{P}}$ be the fixed field of $I_\mathfrak{p}$. Lecture 16 Dec 5, 2025

Theorem 7.11. *(i) $T_\mathfrak{P}/Z_\mathfrak{P}$ is a Galois extension with Galois group $G_\mathfrak{P}/I_\mathfrak{P} \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Recall that this is a cyclic group generated by the Frobenius $\overline{\varphi}_\mathfrak{P}$.*

(ii) $|I_\mathfrak{P}| = e$, $|G_\mathfrak{P}/I_\mathfrak{P}| = f$.

(iii) $e(\mathfrak{P}|\mathfrak{P}_T) = e$ and $e(\mathfrak{P}_T|\mathfrak{P}_Z) = e(\mathfrak{P}_Z|\mathfrak{p}) = 1$, as well as $f(\mathfrak{P}_T|\mathfrak{P}_Z) = f$ and $f(\mathfrak{P}_Z|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{P}_Z) = 1$.

Proof. (i) and (ii) are clear. For (iii), by multiplicativity of e and f, as well as propositions 7.5 and 6.1, it suffices to show $\kappa(\mathfrak{P}_T) = \kappa(\mathfrak{P})$. Consider the inertia group of $\mathfrak{P}$ in $L/T_\mathfrak{P}$,

$$I_\mathfrak{P}(L/T_\mathfrak{P}) = \{\sigma \in I_\mathfrak{P} \mid \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}, \forall \alpha \in \mathcal{O}_L\} = I_\mathfrak{P},$$

so $f(\mathfrak{P}|\mathfrak{P}_T) = 1$, because then the surjective map $I_\mathfrak{P} \twoheadrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T))$ has full kernel, so its image is trivial. □

In total, we have the following diagram of fields (with Galois groups) and primes between $\mathfrak{P}$ and $\mathfrak{p}$, with ramification indices indicated on the left, and inertia degrees on the right:

$$\begin{tikzcd}
L \arrow[d, dash, "I_{\mathfrak{P}}"] \arrow[dd, dash, bend right, "G_{\mathfrak{P}}"'] \arrow[ddd, dash, bend right=60, "G"'] & & \mathfrak{P} \arrow[d, dash, "e"', "1"] \\
T_{\mathfrak{P}} \arrow[d, dash, "G_{\mathfrak{P}}/I_{\mathfrak{P}}"] & & \mathfrak{P}_T \arrow[d, dash, "1"', "f"] \\
Z_{\mathfrak{P}} \arrow[d, dash] & & \mathfrak{P}_Z \arrow[d, dash, "1"', "1"] \\
K & & \mathfrak{p}
\end{tikzcd}$$

Theorem 7.12. *Let L/K be Galois. Let $\mathfrak{P} \subseteq \mathcal{O}_L$ be unramified. There is a unique element $\varphi_{\mathfrak{P}} \in G$ with*

$$\varphi_{\mathfrak{P}}(\alpha) \equiv \alpha^q \mod \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_L$, where $q = |\kappa(\mathfrak{p})|$. In addition, $G_{\mathfrak{P}} = \langle \varphi_{\mathfrak{P}} \rangle$.

Proof. Since $I_{\mathfrak{P}} = 1$, we have $G_{\mathfrak{P}} \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = \langle \overline{\varphi}_q \rangle$. Taking a preimage of $\overline{\varphi}_q : \overline{\alpha} \mapsto \overline{\alpha}^q$ yields the desired element. □

Remark 7.13. If L/K is abelian, then $\varphi_{\mathfrak{P}}$ only depends on $\mathfrak{p}$, then denoted $\varphi_{\mathfrak{p}}$, since the same is true for $G_{\mathfrak{P}}$ by lemma 7.4. Similarly, $\varphi_{\sigma(\mathfrak{P})} = \sigma \varphi_{\mathfrak{P}} \sigma^{-1}$. This Frobenius plays a crucial role in class field theory.

Corollary 7.14. *If L/K is Galois, but not cyclic, then there are at most finitely many primes $\mathfrak{p} \subseteq \mathcal{O}_K$ which do not split.*

Proof. If $\mathfrak{p}$ is not split and unramified, then $G = G_{\mathfrak{P}}$ since $\mathfrak{p}$ is non-split, and by the previous theorem, G would by cyclic. □

We will aplly this theory to the study of cyclotomic fields: A cyclotomic field is a field of the form $K = \mathbb{Q}(\zeta_m)$, with ζ_m a primitive m-th root of unity. Without loss we may take $\zeta_m = \exp(2\pi i/m)$, for example. These fields play an important role in algebraic number theory. For example, by a famous theorem of Kronecker-Weber, every abelian number field is contained in some cyclotomic extension.[4]

Recall the following facts from Algebra: $K = \mathbb{Q}(\zeta_m)/\mathbb{Q}$ is the splitting field of $X^m - 1$, in particular a Galois extension. We have $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$, given by $\overline{a} \mapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a)$. Its order is $\varphi(m) := (\mathbb{Z}/m\mathbb{Z})^\times = [K : \mathbb{Q}]$. If p is an odd prime, then $\mathbb{Q}(\zeta_{p^\nu})/\mathbb{Q}$ is a cyclic extension, because $(\mathbb{Z}/p^\nu\mathbb{Z})^\times$ is a cyclic group of $\varphi(p) = (p-1)p^{\nu-1}$. Let $\Phi_m(X)$ be the minimal polynomial of ζ_m, hence $\Phi_m(X) = \prod_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} (X - \zeta_m^a)$. This is the m-th cyclotomic polynomial. We have the formula $X^m - 1 = \prod_{d|m} \Phi_d(X)$. In particular,

$$\Phi_{p^\alpha} = \frac{X^{p^\alpha} - 1}{\prod_{i=0}^{\alpha-1} \Phi_{p^i}(X)} = \frac{X^{p^\alpha} - 1}{X^{p^{\alpha-1}} - 1} = \left(X^{p^{\alpha-1}}\right)^{p-1} + \ldots + X^{p^{\alpha-1}} + 1.$$

Lemma 7.15. *(i) Let $K = \mathbb{Q}(\zeta_{p^\nu})/\mathbb{Q}$. Set $\pi := 1 - \zeta_{p^\nu}$. Then $\pi\mathcal{O}_K$ is a prime ideal of degree 1 (i.e. $f = 1$) and we have $p\mathcal{O}_K = (\pi)^{\varphi(p^\nu)}$. In other words, p is totally ramified in K.*

[4] The goal of Class Field Theory is to describe in more generality, given a number field K, all abelian extension L/K with data in K, see lectures next term.

(ii) $d(\zeta_{p^\nu}) = \pm p^s$ *with* $s = p^{\nu-1}(\nu p - \nu - 1)$.

Proof. (i) Write $\zeta = \zeta_{p^\nu}$. Setting $X = 1$ in $\Phi_{p^\nu}(X)$ yields

$$p = \prod_{a \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times} (1 - \zeta^a).$$

Recall that, for general $(m, a) = 1$, we have $\frac{1-\zeta_m^a}{1-\zeta_m} \in \mathbb{Z}[\zeta]^\times \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_m)}^\times$, see example 5.12(iv). Hence $p = u(1-\zeta)^{\varphi(p^\nu)}$ for some unit u, and $p\mathcal{O}_K = (1-\zeta)^{\varphi(p^\nu)}$. Now everything follows from $[K : \mathbb{Q}] = \varphi(p^\nu) = efr$.

(ii) By definition,

$$d(\zeta) = d(1, \zeta, \ldots, \zeta^{\varphi(p^\nu)-1}) = \prod_{i \neq j} (\zeta_i - \zeta_j) = \prod_{i=1}^{\varphi(p^\nu)} \Phi'_{p^\nu}(\zeta_i),$$

since by the product rule, $\Phi_{p^\nu}(X) = \prod_{j \neq i}(X - \zeta_j) + (X - \zeta_i)g$ for some polynomial g. Hence $d(\zeta) = \mathrm{N}_{K/\mathbb{Q}}(\Phi'_{p^\nu}(\zeta))$. Differentiate $(X^{p^{\nu-1}} - 1)\Phi_{p^\nu}(X) = X^{p^\nu} - 1$ to obtain at $X = \zeta$

$$(\zeta^{p^{\nu-1}} - 1)\Phi'_{p^\nu}(\zeta) = p^\nu \zeta^{p^\nu - 1} \qquad \text{and} \qquad \mathrm{N}_{K/\mathbb{Q}}(p^\nu \zeta^{p^\nu - 1}) = \pm p^{\nu\varphi(p^\nu)}$$

So it remains to show that $\mathrm{N}_{K/\mathbb{Q}}(\zeta^{p^{\nu-1}} - 1) = p^{p^{\nu-1}}$. But $\zeta^{p^{\nu-1}}$ is a primitive p-th root of unity ζ_p, so $p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = (1-\zeta_p)^{p-1}$ by (i), hence

$$p^{p-1} = \mathrm{N}(p\mathcal{O}_{\mathbb{Q}(\zeta_p)}) = |\,\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)|^{p-1}.$$

Thus $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p) = p$, and $\mathrm{N}_{K/\mathbb{Q}}(1-\zeta_p) = p^{[K:\mathbb{Q}(\zeta_p)]} = p^{p^{\nu-1}}$ □

Theorem 7.16. *Let* $n \in \mathbb{N}$ *and* $K = \mathbb{Q}(\zeta_n)$. *Then* $\mathcal{O}_K = \mathbb{Z}[\theta_n]$ Lecture 17 Dec 10, 2025

Proof. First assume $n = p^\nu$ is a prime power. Then $p^s\mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$. Let $\pi = 1 - \zeta$. Then $\mathcal{O}_K/\pi\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}$ by lemma 7.15(i), hence $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K$.

We claim $\pi^t\mathcal{O}_K + \mathbb{Z}[\zeta] = \mathcal{O}_K$ for all $t \geq 1$. By the above, $t = 1$ is clear. Proceeding inductively, multiply $\pi^t\mathcal{O}_K + \mathbb{Z}[\zeta] = \mathcal{O}_K$ by π to obtain

$$\pi^{t+1}\mathcal{O}_K + \pi\mathbb{Z}[\zeta] = \pi\mathcal{O}_K \Longrightarrow \mathcal{O}_K = \mathbb{Z}[\zeta] + \pi^{t+1}\mathcal{O}_K.$$

Now take $t = s\varphi(p^\nu)$, with s as in lemma 7.15. Then $\mathcal{O}_K = \pi^t\mathcal{O}_K + \mathbb{Z}[\zeta] = p^s\mathcal{O}_K + \mathbb{Z}[\zeta] = \mathbb{Z}[\zeta]$ by the first observation.

Let $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ be arbitrary. Then $\mathbb{Q}(\zeta_{p_i^{\nu_i}}) \cap \mathbb{Q}(\zeta_{p_j^{\nu_j}}) = \mathbb{Q}$ (for example, because p_i is totally ramified in the first, but unramified in the second extension), so $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{\nu_1}}) \cdots \mathbb{Q}(\zeta_{p_r^{\nu_r}})$, and the result follows by induction from corollary 2.21, also cf. example 2.22. □

Theorem 7.17. *Let* $n = \prod_p p^{\nu_p}$, $\nu_p \in \mathbb{Z}_{\geq 0}$, *almost all* 0. *Let* p *be prime. Let* $f_p \in \mathbb{N}$ *be minimal with* $p^{f_p} \equiv 1 \mod n/p^{\nu_p}$. *Then*

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$$

and each $\mathfrak{p}_i$ *has inertia degree* f_p. *Hence* $\varphi(n) = r\varphi(p^{\nu_p})f_p$

Corollary 7.18. *Precisely the divisors of* n *are ramified in* $\mathbb{Q}(\zeta_n)$, *unless* $p = 2 = (4, n)$. *A prime* $p \neq 2$ *is totally split iff* $p \equiv 1 \bmod n$.

Proof. $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, so $\mathfrak{f} = 1$. Hence we may apply the polynomial decomposition law 6.4 for all p. So we have to factor $\Phi_n(X) = (\overline{p_1}(X) \cdots \overline{p_r}(x))^e \mod p$. First consider $p \nmid n$. Then $X^n - 1$ is separable $\mod p$, hence so is Φ_n. In other words, if $\mathfrak{p} \mid p$, then$\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{p})^\times$ is injective on μ_n. But then μ_n is contained in $\mathcal{O}_K/\mathfrak{p}$. One has $\mu_n \subseteq \mathbb{F}_{p^f}^\times$ iff $p^f \equiv 1 \mod n$, hence $\mathbb{F}_{p^{f_p}}$ is the splitting field of $\overline{\Phi}_n \in \mathbb{F}_p[X]$. If $\overline{\Phi}_n(X) = \overline{p}_1(X) \cdots \overline{p}_r(X)$ with $\overline{p}_i(X) \in \mathbb{F}_p[X]$ irreducible and pairwise distinct, then each $\overline{p}_i$ is a minimal polynomial of a primitive root of unity in $\mathbb{F}_{p^{f_p}}$, hence of degree f_p.

Now let n be general. Write $n = p^\nu m$, $p \nmid m$. Let ξ_i, η_j denote the primitive m-th, and p^ν-th roots of unity, respectively. Then $\Phi_n(X) = \prod_{i,j}(X - \xi_i\eta_j)$. Because $X^{p^\nu} - 1 = (X-1)^{p^\nu} \mod p$ we have $(\eta_j - 1)^{p^\nu} \equiv 0 \mod \mathfrak{p}$ for all j and $\mathfrak{p} \mid p$. Hence $\eta_j \equiv 1 \mod \mathfrak{p}$. Then

$$\Phi_n(X) \equiv \prod_{i,j}(X - \xi_i) = \prod_i (X - \xi_i)^{\varphi(p^\nu)} = \Phi_m(X)^{\varphi(p^\nu)} \mod \mathfrak{p}$$

and the result follows from the first case, since $p \nmid m$. □

8 Valuations

Let $\mathcal{O}$ be a Dedekind domain with $K = \mathrm{Quot}(\mathcal{O})$. Let $\mathfrak{p} \subseteq \mathcal{O}$ be a maximal ideal. Then $0 \neq \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}$, $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$.

Definition 8.1. $v_{\mathfrak{p}} : K \to \mathbb{Z} \cup \{\infty\}$, $K^\times \ni x \mapsto v_{\mathfrak{p}}(x\mathcal{O})$ and $0 \mapsto \infty$ is called the *valuation at* $\mathfrak{p}$.

Lemma 8.2. *$v_{\mathfrak{p}}$ is a valuation, that is*

(i) $v_{\mathfrak{p}}(ab) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$,
(ii) $v_{\mathfrak{p}}(a+b) \geq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b))$, *with equality if* $v_{\mathfrak{p}}(a) \neq v_{\mathfrak{p}}(b)$.

Proof. (i) is clear, for (ii) wlog $a, b \in \mathcal{O}$, then write $a\mathcal{O} = \mathfrak{p}^{v_{\mathfrak{p}}(a)}\mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{a}$ and $b\mathcal{O} = \mathfrak{p}^{v_{\mathfrak{p}}(b)}\mathfrak{b}$, $\mathfrak{p} \nmid \mathfrak{b}$. Assume $v_{\mathfrak{p}}(a) \leq v_{\mathfrak{p}}(b)$. Now $\mathfrak{p}^{v_{\mathfrak{p}}(a)} \mid a\mathcal{O}, b\mathcal{O}$, hence also $(a+b)\mathcal{O}$.

Assume $v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(b)$, Then $a \in \mathfrak{p}^{v_{\mathfrak{p}}(a)} \setminus \mathfrak{p}^{v_{\mathfrak{p}}(a)+1}$ and $b \in \mathfrak{p}^{v_{\mathfrak{p}}(a)+1}$, so $a + b \notin \mathfrak{p}^{v_{\mathfrak{p}}(a)+1}$. □

Definition 8.3. Let K be a number field and $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_K$. Let $x \in K^\times$. Then $|x|_{\mathfrak{p}} := \mathrm{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$ is called the $\mathfrak{p}$-*adic value* of x. Further $|0|_{\mathfrak{p}} := 0$.

Example 8.4. For $K = \mathbb{Q}$, $\mathcal{O} = \mathbb{Z}$ one has $v_3(27) = 3, v_3(10) = 0$ and $|27|_3 = 3^{-3}$, $|10|_3 = 1$.

For $K = \mathbb{Q}(\sqrt{2})$, $2\mathcal{O}_K = \mathfrak{p}^2$ with $\mathfrak{p} = \sqrt{2}\mathcal{O}_K$. $|2|_{\mathfrak{p}} = 2^{-2} = \frac{1}{4}$. Note that in addition to the $\mathfrak{p}$-adic values, we also have two archemedian values given by the usual absolute value $|\cdot|$, and $|\cdot| \circ \tau$, where τ denotes conjugation.

In general, if $K/\mathbb{Q}$ is a number field, one has $\mathfrak{p}$-adic values, and $r + s$ archemidean values $|\cdot|_\rho = |\cdot| \circ \rho$, $|\cdot|_\sigma = |\cdot| \circ \sigma$ for each real embedding $\rho : K \to \mathbb{R}$ and pairs of complex embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$. One can show that these are all values on $K/\mathbb{Q}$ up to equivalence. Just as $\mathbb{R}$ can be thought of as the completion of $\mathbb{Q}$ w.r.t. the usual absolute value, we want to construct "completions" for the $\mathfrak{p}$-adic values.

Motivation: Let L/K be number fields. Given an ideal factorization $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, one can pass to the localization at $\mathfrak{p}$. Then $\mathcal{O}_{K,\mathfrak{p}}$ is a discrete valuation ring, and $\mathcal{O}_{L,\mathfrak{p}}$ is a Dedekind domain with primes $S_{\mathfrak{p}}^{-1}\mathfrak{P}_i$, hence a PID by lemma 2.17. One still has $\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}} = (S_{\mathfrak{p}}^{-1}\mathfrak{P}_1)^{e_1} \cdots (S_{\mathfrak{p}^{-1}}\mathfrak{P}_r)^{e_r}$, so all the information is still present in these easier rings.

In another direction, we will define a completion at $\mathfrak{P}$, which yields a field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ with corresponding discrete valuation rings. For the corresponding prime ideals, one has $\widehat{\mathfrak{P}} \mid \widehat{\mathfrak{p}}$ and $\widehat{\mathfrak{p}\mathcal{O}_{L_{\mathfrak{P}}}} = \widehat{\mathfrak{P}}^e$. So completion is an even finer construction than localization, such that everything becomes local and therefore often easier to deal with.

8.1 The p-adic Numbers

Lecture 18
Dec 12, 2025

Let $f \in \mathbb{N}$. Then f has a p-adic expansion $f = a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n$ with $0 \le a_i < p$, e.g. $100 = 1 + 2 \cdot 3^2 + 3^4$.

Definition 8.5. Let p be a prime. An *integral p-adic number* is defined as a formal infinite series $a_0 + a_1 p + \ldots = \sum_{i=0}^{\infty} a_i p^i$ with $0 \le a_i < p$. Two series coincide iff all coefficients coincide. Write $\mathbb{Z}_p$ for the set of all integral p-adic numbers.

Example 8.6. $-1 = (p-1)+p(-1) = (p-1)+p((p-1)+p(-1)) = \ldots = \sum_{i=0}^{\infty}(p-1)p^i \in \mathbb{Z}_p$.

Theorem 8.7. *The residue classes $a \bmod p^n$ in $\mathbb{Z}/p^n\mathbb{Z}$ are uniquely given by*

$$a \equiv a_0 + a_1 p + \ldots + a_{n-1} p^{n-1} \mod p^n, \qquad 0 \le a_i < p$$

Proof. Clear. □

Thus each $f \in \mathbb{Z}$ uniquely defines an integral p-adic number by successively reading $f \bmod p, p^2, p^3$. For example, $-2 \equiv 1 \bmod 3$ and $-2 \equiv 7 \bmod 9$, so the 3-adic expansion starts $-2 = 1 + 2 \cdot 3 + \ldots$

Notation: Write $s_n = f \mod p^n$, Then $s_n = \sum_{i=0}^{n-1} a_i p^i \bmod p^n$ for all $i \ge 1$.

Definition 8.8. The formal (Laurent) series $\sum_{\nu=-n}^{\infty} a_\nu p^\nu$, $0 \le a_\nu < p$ for $n \in \mathbb{Z}$ are denoted by $\mathbb{Q}_p$.

We next want to define a ring structure on $\mathbb{Z}_p$. $\mathbb{Z}_p$ will be a domain with $\operatorname{Quot}(\mathbb{Z}_p) = \mathbb{Q}_p$. For this, we will define a bijection $\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, where the latter is naturally a ring, so we can transport the ring structure to $\mathbb{Z}_p$.

Projective Limits Let (A_n, φ_{nm}) be an inverse system of abelian groups (or rings, modules, top. spaces, etc.), i.e. for $n \ge m$ we have a morphism $\varphi_{n,m} : A_n \to A_m$ s.t. $\varphi_{nn} = \mathrm{id}$ and $\varphi_{km} \circ \varphi_{nm} = \varphi_{nk}$ for $k \le m \le n$. Then

$$\varprojlim_n A_n := \left\{ (a_n)_n \in \prod_n A_n \mid \varphi_{nm}(a_n) = a_m,\ \forall n \ge m \right\}$$

is called the projective limit of (A_n, φ_{nm}). For instance, we have canonical maps $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, $a + p^n\mathbb{Z} \to a + p^m\mathbb{Z}$ for $m \le n$, so we may define $\widehat{\mathbb{Z}}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. In general: If the A_n are abelian groups (etc.), then so is $\varprojlim_n A_n$ by componentwise operations.

Theorem 8.9. *Let (A_n, φ_{nm}) be an inverse system. Then $\varprojlim_n A_n$ satisfies the following universal property: There are morphisms $\pi_n : \varprojlim_n A_n \to A_n$ s.t. $\varphi_{nm} \circ \pi_n = \pi_m$, and given a commutative diagram of solid arrows as in the picture, there exists a unique dashed arrow making the diagram commute.*

$$\begin{tikzcd}
 & & A_n \arrow[dd, "\varphi_{nm}"] \\
Y \arrow[r, dashed, "\exists!\psi"] \arrow[urr, bend left, "\psi_n"] \arrow[drr, bend right, "\psi_m"'] & \varprojlim_n A_n \arrow[ur, "\pi_n"] \arrow[dr, "\pi_m"] & \\
 & & A_m
\end{tikzcd}$$

Proof. Set $\psi(y) = (\psi_n(y))_n$. □

Theorem 8.10. *The map (of sets)*

$$\mathbb{Z}_p \to \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \qquad \sum_{i=1}^{\infty} a_i p^i \mapsto \left(\sum_{i=0}^{n-1} a_i p^i\right)_n$$

is a bijection.

Proof. Clear from theorem 8.7. □

As mentioned before, we use this bijection to define a ring structure on $\mathbb{Z}_p$.

Lemma 8.11. *(i) $\alpha = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p^\times$ if and only if $a_0 \neq 0$.*
(ii) $\mathbb{Z}_p$ is a domain.

Proof. (i) By definition, $\alpha \in \mathbb{Z}_p^\times$ if and only if $s_n = \sum_{i=0}^{n-1} a_i p^i \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ if and only if $p \nmid s_n$ for all n if and only $p \nmid a_0$.

(ii) Let $0 \neq \alpha = \sum_i a_i p^i$, and let n_0 be the smallest index with $a_{n_0} \neq 0$, so that $\alpha = p^{n_0}(a_{n_0} + a_{n_0+1}p + \ldots)$. Then the part in parentheses is a unit, and p^{n_0} is not a zero divisor. □

Proposition 8.12. $\mathrm{Quot}(\mathbb{Z}_p) = \mathbb{Q}_p$.

Proof. Let $\frac{\alpha}{\beta} \in \mathrm{Quot}(\mathbb{Z}_p)$, with $\alpha = \sum_{i \geq m_1} a_i p^i$, $\beta = \sum_{i \geq m_2} b_i p^i$ and $a_{m_1} b_{m_2} \neq 0$. Then $\frac{\alpha}{\beta} = p^{-m_2}\alpha(\sum_{i \geq 0} b_{i-m_2} p^i)^{-1}$, where the element in parentheses is a unit by the lemma. □

We have now two representations of the p-adic numbers, and natural maps $\mathbb{Z} \to \mathbb{Z}_p$ (by p-adic expansion), $\mathbb{Z} \to \widehat{\mathbb{Z}}_p$ (by the universal property), which clearly agree under the identification $\mathbb{Z}_p \to \widehat{\mathbb{Z}}_p$, and similarly for their quotient fields. In particular, $\mathbb{Q}_p/\mathbb{Q}$ is a field extension.

We now give a third construction of $\mathbb{Z}_p$: Recall from definition 8.3 the absolute value $|a|_p := p^{-v_p(a)}$ for $a \in \mathbb{Q}$. Note that the summands of $\sum_{i=0}^{\infty} a_i p^i$ form a zero series w.r.t. $|\cdot|_p$. From lemma 8.2 it follows immediately that $|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p$, so $|\cdot|_p$ is an absolute value in the general sense.

Theorem 8.13. *Let $a \in \mathbb{Q}^\times$. Write $|\cdot|_\infty$ for the usual real value, and let $P = \{primes\} \cup \{\infty\}$. Then $\prod_{p \in P} |a|_p = 1$.*

Proof. $a = \pm \prod_{p \neq \infty} p^{\nu_p(a)} = \frac{a}{|a|_\infty} \prod_{p \neq \infty} |a|_p^{-1}$. □

More generally, if $K/\mathbb{Q}$ is a number field, we constructed absolute values $|\cdot|_\mathfrak{p}, |\cdot|_\rho, |\cdot|_\sigma$ for prime ideals $\mathfrak{p}$, real embeddings ρ, and pairs of complex embedings $\sigma, \overline{\sigma}$. Then $\prod |\alpha|_v = 1$, where $|\cdot|_v$ runs over all the above values. (Exercise.)

Now we can construct the completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ as it was done in analysis for $|\cdot|_\infty$: Consider Cauchy sequences in $\mathbb{Q}$ w.r.t. $|\cdot|_p$, e.g. partial sums of $\sum_{i \geq -n}^{\infty} a_i p^i$, $0 \leq a_i < p$. Let R be the ring of Cauchy sequences w.r.t. $|\cdot|_p$, and $\mathfrak{n} \subseteq R$ be the ideal of sequences converging to 0.

Lemma 8.14. *$\mathfrak{n}$ is a maximal ideal.*

Proof. Let $\mathfrak{n} \subsetneq \mathfrak{a} \subseteq R$ be an ideal. Let $x \in \mathfrak{a} \setminus \mathfrak{n}$. Then there exist $\varepsilon > 0$ and $n_0 \in \mathbb{N}$ s.t. $|x_n|_p \geq \varepsilon$ for all $n \geq n_0$. Let now $y_n = \frac{1}{x_n}$ for $n \geq n_0$. Then $y = (y_n)$ is a Cauchy sequences, because $|y_n - y_m|_p = \frac{|x_n - x_m|_p}{|x_n x_m|_p} \leq \frac{1}{\varepsilon^2}|x_n - x_m|_p \to 0$ for $n, m \geq n_0$. Then $y \in R$, and $xy \in \mathfrak{a}$ is eventually constant with value 1. Adjusting the first terms (by adding a null series), we see $1 \in \mathfrak{a}$. □

Now we can (re-)define $\mathbb{Q}_p := R/\mathfrak{n}$. We have an embedding $\mathbb{Q} \to \mathbb{Q}_p$ by sending $a \in \mathbb{Q}$ to the constant sequence $(a, a, \ldots) + \mathfrak{n}$. We can extend $|\cdot|_p$ to $\mathbb{Q}_p$ by $|[(x_n)_n]|_p := \lim_{n\to\infty} |x_n|_p \in \mathbb{R}$. One can show that $\mathbb{Q}_p$ is complete w.r.t. $|\cdot|_p$. For details and proofs of this construction, see e.g. *Gerhard Frey, Elementary number theory*.

Lecture 19
Dec 17, 2025

Theorem 8.15. *(i) $\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) \geq 0\}$ is a ring. $\mathbb{Z}_p$ is the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.*
(ii) Each $\alpha \in \mathbb{Z}_p$ is represented by a Cauchy sequence $(\alpha_n)_n$ with $\alpha_n \in \mathbb{Z}$.

Proof. (ii) Wlog $\alpha_n = \frac{a_n}{b_n}$ with $p \nmid b_n$ and $(a_n, b_n) = 1$. Choose $y_n \in \mathbb{Z}$ s.t. $b_n y_n = a_n \bmod p^n$, then $|a_n - y_n|_p = |\frac{1}{b_n}|_p |a_n - b_n y_n|_p \leq \frac{1}{p^n}$, hence $\alpha = (y_n)_n + \mathfrak{n}$.

(i) $\mathbb{Z}_p$ is a ring becuase of $|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p)$ and $|\alpha\beta|_p = |\alpha|_p |\beta|_p$. Let $\varepsilon > 0$ and $\alpha \in \mathbb{Z}_p$. By (ii) we may write $\alpha = (a_n)_n + \mathfrak{n}$ with $a_n \in \mathbb{Z}$. Since $(a_n)_n$ is Cauchy, there is m s.t. $|a_n - a_m|_p < \varepsilon$ for all $n \geq m$. Hence $|\alpha - a_m|_p \leq \varepsilon$. $\square$

Lemma 8.16. $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p = 1\} = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) = 0\}$.

Proof. $|\frac{1}{\alpha}|_p = \frac{1}{|\alpha|_p}$. $\square$

Lemma 8.17. *Every $\alpha \in \mathbb{Q}_p^\times$ has a unique representation in the form $\alpha = p^m u$, $u \in \mathbb{Z}_p^\times$ with $m = v_p(\alpha)$.*

Proof. $v_p(\alpha p^{-m}) = 0$, so $\alpha p^{-m} \in \mathbb{Z}_p^\times$ by lemma 8.16. $\square$

Theorem 8.18. *The nonzero ideals of $\mathbb{Z}_p$ are given by $p^n\mathbb{Z}_p$, $n \geq 0$. We have $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. Let $0 \neq \mathfrak{a} \subseteq \mathbb{Z}_p$ be an ideal. Choose $\alpha = p^m u \in \mathfrak{a}$ as in lemma 8.17 with m minimal. Then $\mathfrak{a} = p^m\mathbb{Z}_p$. Now consider

$$\varphi : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p, \qquad a \mapsto a + p^n\mathbb{Z}_p.$$

Then $a \in \ker\varphi$ iff $v_p(a) \geq n$, so iff $a \in p^n\mathbb{Z}$. It remains to show that φ is surjective. Let $\alpha \in \mathbb{Z}_p$. By theorem 8.15 we have an $a \in \mathbb{Z}$ with $|\alpha - a| \leq \frac{1}{p^n}$. But this is equivalent to $\alpha \equiv a \bmod p^n\mathbb{Z}_p$, i.e. $\varphi(a) = \alpha + p^n\mathbb{Z}_p$. $\square$

Theorem 8.19. *The canonical homomorphism*

$$\mathbb{Z}_p \to \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

is an isomorphism.

Proof. $\ker\alpha = \bigcap_n p^n\mathbb{Z}_p = \{0\}$. For surjectivity, note that the partial sums of elements $\sum_{i=0}^\infty a_i p^i$ in our old $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ form Cauchy sequences. $\square$

Remark 8.20. A series $\sum_{i=0}^\infty b_i$ converges in $\mathbb{Q}_p$ if and only if $b_i \to 0$, since for the partial sums $(s_n)_n$ we have

$$|s_n - s_m|_p = \left|\sum_{i=m}^{n-1} b_i\right|_p \leq \max(|b_i|_p \mid i = m, \ldots, n-1)$$

8.2 Valued Fields

Definition 8.21. A *value* on a field K is a function $|\cdot| : K \to \mathbb{R}$ with

(i) $|x| \geq 0$, and $|x| = 0$ iff $x = 0$,
(ii) $|xy| = |x| \cdot |y|$ for all $x, y \in K$,
(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Such a value defines a distance function, so valued fields become metric and hence topological spaces. By convention, we exclude the trivial value ($|x| = 1$ for all $x \neq 0$) from all considerations.

Definition 8.22. Two values $|\cdot|_1, |\cdot|_2$ are called *equivalent* if they generate the same topology on K.

Theorem 8.23. *$|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there exists $s \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.*

Proof. "$\Leftarrow$": We have $|x|_1 < \varepsilon$ iff $|x|_2 < \varepsilon^{1/s}$, so the two values generate the same open balls, hence the same metric.

"$\Rightarrow$": Note that for any metric $|x| < 1$ iff $(x^n)_n$ is a zero series. Hence we have

$$|x|_1 < 1 \quad \Longrightarrow \quad |x|_2 < 1. \tag{$*$}$$

Let $y \in K$ with $|y|_1 > 1$. Let $x \in K^\times$. Define α by $|x|_1 = |y|_1^\alpha$, $\alpha \in \mathbb{R}$. Let $\frac{m_i}{n_i} \searrow \alpha$ be a rational series approximating α from above. Then $|x|_1 < |y|_1^{m_i/n_i}$, i.e. $|\frac{x^{n_i}}{y^{m_i}}| < 1$. By $(*)$, also $|\frac{x^{n_i}}{y^{m_i}}|_2 < 1$, and $|x|_2 < |y|_2^{m_i/n_i}$. In the limit we therefore get $|x|_2 \leq |y_2|^\alpha$. Repeating this argument with a series converging from below yields the opposite inequality, so in fact $|x|_2 = |y|_2^\alpha$. Therefore, $s := \frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2}$ for all $x \in K^\times$, i.e. $|x|_1 = |x|_2^s$. $\square$

Lecture 20 Jan 7, 2026

Theorem 8.24 (Weak Approximation Theorem)**.** *Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent values on a field K, and let $a_1, \ldots, a_n \in K$. Let $\varepsilon > 0$. Then there exists $x \in K$ s.t. $|x - a_i|_i < \varepsilon$ for all $i = 1, \ldots, n$.*

Proof. We first show the existence of $z \in K$ with $|z|_1 > 1$ and $|z|_j < 1$ for $j \neq 1$, by induction. For $n = 2$, this is exactly the statement $(*)$ from the last proof. So let $z \in K$ with $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n-1$. Then if $|z|_n \leq 1$, let $y \in K$ with $|y|_1 > 1$ and $|y|_n < 1$, and consider $z^m y$ for m large enough. Otherwise, take $\frac{z^m}{1+z^m} y$.

For a $z \in K$ as required, we note that $\frac{z^m}{1+z^m}$ converges to 1 w.r.t. $|\cdot|_1$ and to 0 w.r.t. $|\cdot|_j$ for $j \neq 1$. Repeating this construction for different indices, for $i \in \{1, \ldots, n\}$ we find $z_i \in K$ s.t. $|z_i - 1|_i$ and $|z_i|_j$ are very small, for all $i \neq j$. Then one checks that $x = \sum_i a_i z_i$ satisfies the claim of the theorem. $\square$

Remark 8.25. Let $K = \mathbb{Q}$ and $p_1, \ldots, p_n$ pairwise distinct primes. Set $|\cdot|_i = |\cdot|_{p_i}$. Then the Weak Approximation Theorem is equivalent to $x \equiv a_i \mod p_i^m$, for some m large enough (so that $|p_i^m|_i < \varepsilon$ for all i), hence to the Chinese Remainder Theorem.

Definition 8.26. A value $|\cdot|$ is called *finite* or *non-archimedean* if $|n|$ is bounded for $n \in \mathbb{N}$. Otherwise $|\cdot|$ is called *archimedean*

Theorem 8.27. *A value $|\cdot|$ is finite if and only if $|x + y| \leq \max(|x|, |y|)$ for all $x, y \in K$.*

Proof. "$\Rightarrow$": $|n| = |1 + \ldots + 1| \leq \max(|1|, \ldots, |1|)$ is bounded.

"$\Leftarrow$": Let $|n| \leq N$ for all $n \in \mathbb{N}$. Let $x, y \in K$ with $|x| \leq |y|$. Then

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

so taking n-th roots and letting $n \to \infty$ shows $|x+y| \leq |y|$. □

Theorem 8.28. *Each value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. (only the non-archimedean case) Let $|\cdot|$ be a finite value on $\mathbb{Q}$. Since $|-1| = |1| = 1$, we have $|n| \leq 1$ for all $n \in \mathbb{Z}$ by the strong triangle inequality. Let p be a prime with $|p| < 1$. (If no such prime exists, then $|\cdot| \equiv 1$ by unique prime factorization.) Let $\mathfrak{a} := \{a \in \mathbb{Z} \mid |a| < 1\}$. By the strong triangle inequality, this is an ideal of $\mathbb{Z}$ which satisfies $p\mathbb{Z} \subseteq \mathfrak{a}$ and $1 \notin \mathfrak{a}$. By maximality of $p\mathbb{Z}$, we have $\mathfrak{a} = p\mathbb{Z}$.

Now let $a \in \mathbb{Q}$ and write $a = bp^m$ with $p \nmid b$. Then $b \notin \mathfrak{a}$, so $|a| = |p|^m = |a|_p^s$ with $s = -\frac{\log|p|}{\log p}$. □

As before, given a value $|\cdot|$ on K, we may define a valuation v on K by $v(x) := -\log|x|$ for $x \in K^\times$ and $v(0) := \infty$. One checks directly that this is indeed a valuation, and by theorem 8.23 we have $v_1 \sim v_2$ if and only if $v_1 = sv_2$ for some $s > 0$.

Theorem 8.29.

$$\mathcal{O} := \{x \in K \mid |x| \leq 1\} = \{x \in K \mid v(x) \geq 0\}$$

is an integral local ring with unique maximal ideal

$$\mathfrak{m} = \{x \in K \mid |x| < 1\} = \{x \in K \mid v(x) > 0\}.$$

Proof. One has $\mathcal{O}^\times = \{x \in K \mid |x| = 1\}$, so $\mathfrak{m} = \mathcal{O} \setminus \mathcal{O}^\times$ is an ideal, i.e. $\mathcal{O}$ is local. □

Remark 8.30. Equivalent valuation yield the same valuation rings. For $x \in K$ one has $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$, so these rings are valuation rings in the sense of commutative algebra.

Definition 8.31. A valuation v on K is called *discrete* if it has a minimal positive value s.

In this case, one easily sees $v(K^\times) = s\mathbb{Z}$, since if $v(\pi) = s$, then $v(\pi^n) = ns$, and if $\alpha \in K^\times$ with $v(\alpha) = ts$, then $v(\alpha\pi^n) = (t+n)s$, so if $t \notin \mathbb{Z}$ one could find n with $0 < v(\alpha\pi^n) < s$.

Definition 8.32. A discrete valuation v is called *normalized* if $v(K^\times) = \mathbb{Z}$. Each $\pi \in K$ with $v(\pi) = 1$ is called a *prime* or *uniformizing* element.

Lemma 8.33. *Let v be a normalized discrete valuation, let $\pi \in K$ with $v(\pi) = 1$. Every $x \in K^\times$ has a unique representation $x = \pi^m u$ with $U \in \mathcal{O}^\times$ and $m = v(x)$.*

Proof. $v(x\pi^{-m}) = m - m = 0$, so $x\pi^{-m} \in \mathcal{O}^\times$. □

Example 8.34.

(i) Let $K = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$, p a prime. Then $v = v_p$, and $\pi = p$ is a uniformizing element. One has $\mathcal{O} = Z_{(p)}$.

(ii) Let K be a number field and $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ a maximal ideal. Then $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(\alpha\mathcal{O}_K)$ is a valuation, the set of corresponding prime elements is exactly $\mathfrak{p} \setminus \mathfrak{p}^2$. One has $\mathcal{O} = (\mathcal{O}_K)_\mathfrak{p}$

Theorem 8.35. *Let v be a discrete valuation on K. Then $\mathcal{O}$ is a PID. If v is normalized, then the set of ideals of $\mathcal{O}$ is given by*

$$\pi^n\mathcal{O} = \{x \in K \mid v(x) \geq n\}, \qquad n \geq 0.$$

Let $\mathfrak{p} = \pi\mathcal{O}$, then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}$.

Proof. Exactly as for $\mathbb{Z}_p$ in theorem 8.18. □

8.3 Completions

Lecture 21
Jan 14, 2026

Just as we defined $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ w.r.t. $|\cdot|_p$, one may construct the completion of a valued field K as the set of all Cauchy sequences, modulo null sequences. We omit the details.

Let $(K, |\cdot|)$ be a valued field, and denote its completion by $\widehat{K}$. If $a = [(a_n)_n] \in \widehat{K}$, define $|a| := \lim_n |a_n|$. Since $||a_n| - |a_m|| \leq |a_n - a_m| \to 0$, $(|a_n|)_n$ is a Cauchy sequence, hence converges in $\mathbb{R}$. Similarly, $v(a) := -\log|a| = \lim_n v(a_n)$.

Note that for $a \neq 0$, we have $v(a) = v(a - a_n + a_n) = \min(v(a - a_n), v(a_n)) = v(a_n)$ for n large enough, hence $v(\widehat{K}^\times) = v(K^\times)$ and if (K, v) is discrete, then so is $(\widehat{K}, v)$.

Theorem 8.36. *Let v be a discrete normlalized valuation on K. Let $\mathcal{O}$ be the valuation ring of v as before, with maximal ideal $\mathfrak{p}$. Denote by $\widehat{K}$ the completion of K w.r.t. v, and let*

$$\widehat{\mathcal{O}} := \{x \in \widehat{K} \mid v(x) \geq 0\} \supseteq \widehat{\mathfrak{p}} := \{x \in \widehat{K} \mid v(x) > 0\}.$$

Then $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n$ for all $n \geq 1$.

Proof. Similar as for $\mathbb{Q}_p$, see theorem 8.18. □

Theorem 8.37. *Let $R \subseteq \mathcal{O}$ be a set of representatives of $\mathcal{O}/\mathfrak{p}$ with $0 \in R$, let $\pi \in \mathcal{O}$ be a prime element. Then each $x \in \widehat{K}^\times$ has a unique representation*

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \ldots)$$

with $a_i \in R$, $a_0 \neq 0$ and $m = v(x) \in \mathbb{Z}$.

Proof. By lemma 8.33 we may assume $m = 0$ and $x \in \widehat{\mathcal{O}}^\times$. Since $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$, there exists $a_0 \in R$ with $x \equiv a_0 \bmod \widehat{\mathfrak{p}}$, so $x = a_0 + b_0\pi$. Repeating this argument for b_0, we proceed inductively. □

Example 8.38. Let $K = \mathbb{Q}(i)$ and $\mathfrak{p} = (2+i)$, $\pi = 2+i$. Then $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/5\mathbb{Z}$, so we may take $R = \{0, \ldots, 4\}$. Let $\alpha = 11$. One finds $\alpha \equiv 1 \bmod \pi$, so $\alpha = 1 + \pi(2(2-i))$. Then $2(2-i) \equiv 3 \bmod \pi$, so $\alpha = 1 + 3\pi + \pi^2(-i)$, etc. One also writes $\alpha = 1 + 3\pi + O(\pi^2)$ to denote the start of the series expansion.

Let K be complete w.r.t. a non-archimedean value $|\cdot|$. Let $\mathcal{O}$ be the valuation ring and $\mathfrak{p}$ the maximal ideal. Let $k := \mathcal{O}/\mathfrak{p}$.

Definition 8.39. For $f = \sum_i a_i X^i \in K[X]$ set $|f| := \max\{|a_i|\}_i$. If $f \in \mathcal{O}[X]$ satisfies $|f| = 1$ (equivalently $f \not\equiv 0 \bmod \mathfrak{p}$), f is called *primitive*.

Theorem 8.40 (Hensel's Lemma)**.** *Let $f \in \mathcal{O}[X]$ be primitive. If $f \bmod \mathfrak{p}$ has a decomposition $f \equiv \overline{g}\overline{h} \bmod p$ with coprime $\overline{g}, \overline{h} \in k[X]$, then $f = gh$ with $g, h \in \mathcal{O}[X]$, $\deg(g) = \deg(\overline{g})$ and $g \equiv \overline{g}, h \equiv \overline{h} \bmod p$.*

Proof. See Neukirch, II.4.6. □

Corollary 8.41. *Let $f \in \mathcal{O}[X]$ be primitive and suppose $(\overline{f}, \overline{f}') = 1$. Let $a \in k$ such that $\overline{f}(a) = 0$. Then there exists $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $\alpha \equiv a \bmod \mathfrak{p}$.*

Proof. Exercise. □

Example 8.42. By repeatedly applying the previous corollary to $X^{p-1} - 1 \in \mathbb{Z}_p[X]$, one sees $\mu_{p-1} \subseteq \mathbb{Z}_p$

Corollary 8.43. *Let K be complete w.r.t. the non-archimedean value $|\cdot|$. Let $f = \sum_i a_i X^i \in K[X]$ be irreducible. Then $|f| = \max(|a_0|, |a_n|)$. In particular, if f is normalized and $a_0 \in \mathcal{O}$, then $f \in \mathcal{O}[X]$.*

Proof. Wlog we may assume $f \in \mathcal{O}[X]$ and $|f| = 1$. Let a_r be the first coefficient with $|a_r| = 1$. Then $f \equiv x^r(a_r + \ldots + a_n x^{n-r}) \bmod \mathfrak{p}$, so $0 < r < n$ would yield a non-trivial factorization of f by Hensel's Lemma. □

Theorem 8.44. *Let K be complete w.r.t. $|\cdot|$. Let L/K be a finite field extension, $n := [L : K]$. Then $|\cdot|$ has a unique extension to L given by $|\alpha|_L := \sqrt[n]{|\mathrm{N}_{L/K}(\alpha)|}$. In addition, L is complete w.r.t. $|\cdot|_L$.*

Proof. (for non-archimedean values) We claim that $\mathcal{O}_L = \{x \in L \mid \mathrm{N}_{L/K}(x) \in \mathcal{O}\}$, where "$\subseteq$" is clear. For the other direction, let $f = \sum_i a_i X^i$ be the minimal polynomial of x. Then $\mathrm{N}_{L/K}(x)$ is a power of a_0, hence $a_0 \in \mathcal{O}$, so $f \in \mathcal{O}[X]$ by the previous corollary.

To show that $|\cdot|_L$ is a value, we only have to check the triangle inequality, everything else is clear. Let $\alpha, \beta \in L$ with $|\alpha|_L \leq |\beta|_L$. Dividing by $|\beta|_L$, it is enough to show $|\frac{\alpha}{\beta} + 1|_L \leq 1$. By the claim at the start of the proof, this is equivalent to showing $\frac{\alpha}{\beta} \in \mathcal{O} \Rightarrow \frac{\alpha}{\beta} + 1 \in \mathcal{O}$, which is clearly true.

□