# Algebraic Number Theory

read by Prof. Dr. Werner Bley

notes by Stefan Albrecht

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

## Contents

# 1 Motivation

Lecture 1
Oct 15, 2025

**Theorem 1.1** (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 $\alpha, \beta$ aren't units, each factor is $> 1$, hence $p = x^2 + y^2 = x'^2 + y'^2$. □

**Definition 1.2.** A finite extension $K$ of $\mathbb{Q}$ is called a *number field*.

**Example 1.3.** $\mathbb{Q}(i)$ 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 1.4.** 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 1.5.**
(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 1.6.** *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 $\bmod p$.

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 1.1 and 1.6 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 1.7** (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 1.8.** 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 $\alpha$. 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 $\alpha$. $\sigma$ 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 $\alpha_i$ is a conjugate of $\alpha$, so is $\overline{\alpha_i}$.

**Example 1.9.** 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 1.10.** 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 $\operatorname{cl}_K = I_K/P_K$ is called the *ideal class group*

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

**Theorem 1.11.** $|\operatorname{cl}_K| < \infty$.

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 1.12.** 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 1.13.** 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 1.14.** *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 $(*)$.*

# 2 Integrality

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

**Definition 2.1.** 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 2.2.** 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 2.3.** *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 2.4, this implies that $\det(bE - M)\omega_i = 0$ for all $i = 1, \ldots, r$, hence $\det(bE - M) = 0$ since the $\omega_i$ 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 2.4.** *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 2.5.** $K = \mathbb{Q}(\sqrt{2}) \supseteq \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. 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 $\omega_i$ 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 2.3.

**Proposition 2.6.** *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 2.7.** *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 2.3, hence finitely generated. Again by theorem 2.3, we are done. □

**Definition 2.8.** 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 2.3, 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 2.9.** $\mathcal{O}_{A,B}$ 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 2.7 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 2.10.** *Let $R$ be a UFD and $K = \mathrm{Quot}(R)$. 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

$$X^n + c_{n-1}X^{n-1} + \ldots + c_1X + c_0 = 0 \qquad \text{with } c_i \in R$$

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

$$a^n + c_{n-1}ba^{n-1} + \ldots + c_1ab^{n-1} + c_0b^n = 0.$$

Suppose $b \notin R^\times$, then there exists a prime element $\pi \in R$ dividing $b$. Looking at the equation $\bmod \pi$, 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 $K = \mathrm{Quot}(A)$. 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 2.11.** *In the above situation, $L = \mathrm{Quot}(B)$. 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

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + \ldots + a_1a_n^{n-2}(a_n\beta) + a_0a_n^{n-1} = 0.$$

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

**Lemma 2.12.** *One has $\beta \in B$ if and only if its minimal polynomial $\mu = \mathrm{mipo}_{\beta,K}$ 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 $\mu$ (in some algebraic closure of $K$) are integral over $A$. Since the coefficients of $\mu$ are the elementary symmetric functions in its zeroes, the coefficients of $\mu$ 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 2.13.** We define $\mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(T_x)$ and $\mathrm{N}_{L/K}(x) := \det(T_x)$.

**Lemma 2.14.** *(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 $a_1 = \mathrm{Tr}_{L/K}(x)$ and $a_n = \mathrm{N}_{L/K}(x)$.*

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

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

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

**Theorem 2.15.** *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)* $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$

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

*Proof.* (ii) and (iii) follow from (i) using lemma 2.14(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 $\sigma$, 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 $\mu_x$ w.r.t. the basis $1, x, \ldots, x^{n-1}$. □

**Example 2.16.** (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 $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = 2a$ and $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d$.

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

(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 $\alpha$ has no $t^2$-term.

**Corollary 2.17.** *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 $\omega = (\omega_1, \ldots, \omega_m)^t$ be a $L$-basis of $M$. Then $\widehat{\sigma}_i(\omega_1), \ldots, \widehat{\sigma}_i(\omega_m)$ 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 $\alpha_1, \ldots, \alpha_n$ be $[L : K]$-many elements of $L$.

**Definition 2.18.** The discriminant of $\alpha_1, \ldots, \alpha_n$ is defined as

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

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

**Lemma 2.19.** *(i) $d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{1 \le i,j \le n}$.*

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

*Proof.* One calculates

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

and takes determinants for the first part. For the second, the matrix in the definition 2.18 of $d$ is the Vandermonde matrix of the $\theta_i$. □

**Theorem 2.20.** *Let $L/K$ be a finite separable field extension of degree $n$. Let $\alpha_1, \ldots, \alpha_n \in L$. Then*

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

*(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 $\det(M) = d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j}(\theta_i - \theta_j)^2 \neq 0$ by lemma 2.19.

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

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

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

Lecture 4
Oct 24, 2025

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 $L$.

**Lemma 2.21.** *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 2.22.** 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 1.7, since there is one real and one pair of complex embeddings.

**Lemma 2.23.** *Let $\alpha_1, \ldots, \alpha_n \in B$ be a $K$-basis of $L$. Let $d = d_{L/K}(\alpha_1, \ldots, \alpha_n) \in A$. Then*

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

*Proof.* Let $B \ni \alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$ 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 $(a_1, \ldots, a_n)$ is a solution of

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

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 $d(a_1, \ldots, a_n) \in A^n$ □

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 2.24.** *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 $\omega_1, \ldots, \omega_n \in B$ such that $B = A\omega_1 \oplus \ldots \oplus A\omega_n$.*

*Proof.* Let $\alpha_1, \ldots, \alpha_n \in B$ be a $K$-basis of $L$. Let $\mu_1, \ldots, \mu_r \in M \subseteq L$ be a $B$-generating system of $M$. Let $0 \neq a \in A$ such that $a\mu_i \in B$ (possible by lemma 2.11). Let $d = d_{L/K}(\alpha_1, \ldots, \alpha_n)$, which is nonzero by theorem 2.20. Then $daM \subseteq dB \subseteq A\alpha_1 \oplus \ldots \oplus A\alpha_n \cong A^n$ by lemma 2.23. It follows that $daM \cong A^m$ with $m \leq n$, hence also $M \cong A^m$.

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

**Example 2.25.**
(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 2.26.** Let $L/K/\mathbb{Q}$ be number fields. Then $\mathcal{O}_K$ is in general not a PID, so theorem 2.24 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 2.27.** Let $L/\mathbb{Q}$ be a number field. Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$ be an integral basis, i.e. $\mathcal{O}_L = \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_n$. Then $d_L = d_{L/\mathbb{Q}} := d_{L/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$ 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 $d_L(M) = d_{L/\mathbb{Q}}(M) := d(m_1, \ldots, m_n)$ for some integral basis $m_1, \ldots, m_n$ of $M$.

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

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

**Example 2.28.** $L = \mathbb{Q}(\sqrt{d})$, $d \equiv 2, 3 \bmod 4$. 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 2.29.**
(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 $d_{L/K} := (d_{L/K}(\alpha_1, \dots, \alpha_n))$ for an integral basis $\alpha_i$ is well-defined.

Now assume $\mathcal{O}_K$ is arbitrary. As in remark 2.26, 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.

**Theorem 2.30.** *Let $L/\mathbb{Q}$ be a number field. Let $0 \neq \mathfrak{a} \subseteq \mathfrak{a}'$ be $\mathcal{O}_L$-submodules of $L$. Then* Lecture 5 Oct 29, 2025

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

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

*Proof.* Let $\alpha'_1, \dots, \alpha'_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}'$ and $\alpha_1, \dots, \alpha_n$ 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 2.31.** *Let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$. If $d_L(\alpha_1, \dots, \alpha_n)$ is squarefree, then $\alpha_1, \dots, \alpha_n$ is an integral basis.*

**Remark 2.32.** This is not a necessary condition: In example 2.28 we saw $4 \mid d_{\mathbb{Q}(\sqrt{d})}$ for $d \equiv 2, 3 \bmod 4$.

**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 2.33.** *The following are equivalent:*

*(i) $M$ is Noetherian*

*(ii) Each ascending chain $M_1 \subseteq M_2 \subseteq \dots$ 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 2.34.** *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 2.24, hence in particular finitely generated. Thus $\mathcal{O}_K$ is noetherian. $\mathcal{O}_K$ is integrally closed by definition and transitivity 2.7.

Finally, for $0 \neq \mathfrak{p}$ prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain which is finite by theorem 2.30, hence a field. Therefore, $\mathfrak{p}$ is maximal. □

**Definition 2.35.** A noetherian, integrally closed integral domain of dimension 1 is called a *Dedekind* domain.

**Example 2.36.** By theorem 2.34, $\mathcal{O}_K$ 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 2.37.** 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 2.38.** *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 $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$ with pairwise distinct primes $\mathfrak{p}_j$, then also $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cap \dots \cap \mathfrak{p}_s^{e_s}$*

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

*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 2.33 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 2.40.** *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* $0 \neq \mathfrak{a} \subseteq O$ *one has* $\mathfrak{a}\mathfrak{p}^{-1} \supsetneq \mathfrak{a}$.

*Proof.* Everything is clear but the strictness of the final inclusion. □

Now we can return to the proof of theorem 2.38. 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 2.33 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 2.40, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$ 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. □