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 α, β aren't units, each factor is > 1, hence $p = x^2 + y^2 = x'^2 + y'^2$. $\square$

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. $\square$

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 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 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 $\mathrm{cl}_K = I_K/P_K$ 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 1.11. $|\mathrm{cl}_K| < \infty$.

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 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 $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_1 X + a_0 \in A[X]$ 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 $b_1 b_2$ 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 $b^m = -\sum_{i=0}^{m-1} a_i b^i$, 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 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 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 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.

Theorem 2.6. *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. $\square$

Definition 2.7. 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 2.8. $\mathcal{O}_{A,B}$ 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 2.6 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 2.9. *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

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

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 $\operatorname{mod} \pi$, we see that $\pi \mid a^n$; i.e. $\pi \mid a$, contradicting the coprime assumption. $\square$

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.

$$\begin{array}{ccc} L & \hookleftarrow & B \\ | & & | \\ K & \hookleftarrow & A \end{array}$$

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

Lemma 2.10. *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

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

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

Lemma 2.11. *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 $\mu \in A[X]$. $\square$