Lecture Notes for

Algebraic Number Theory

Lecturer
Mahesh Kakde

Notes typed by
Sayan Das

2025
NPTEL, IISc

Contents

Syllabus

Week 1. — Study of number fields, definition of the ring of integers. Definition of norm and trace.

Week 2. — Definition of absolute and relative discriminant. Computation of discriminant. Computation of the ring of integers.

Week 3. — Definition and properties of Dedekind domains. Proof that the ring of integers is a Dedekind domain. Factorisation of extension of prime ideals in a finite extension of number fields.

Week 4. — Embeddings of a number field in complex numbers. A result from geometry of numbers. Finiteness of class groups.

Week 5. — Computation of class groups, including several examples. Applications to Diophantine equations of computations of class groups.

Week 6. — Dirichlet's unit theorem.

Week 7. — Extension and norm of ideals in field extensions. Maps between class groups of extensions. Decomposition subgroups, inertia subgroups, Frobenius elements etc. Localisation, residue field.

Week 8. — Valuations in a number fields. Local fields. Hensel's lemma and applications.

Week 9. — Field extensions of local fields, ramification, different, inertia subgroups etc.

Week 10. — Study of special number fields. Imaginary quadratic fields, real quadratic fields, cubic fields, cyclotomic fields.

Week 11. — Definition of ray class field as a generalisation of ideal class group. Some statements from class field theory without proofs.

Week 12. — Definition of zeta functions and L-functions. Statements of their analytic properties without proofs. Dirichlet Class number formula.

Chapter 1.

The ring of algebraic integers

1

1.1. Overview and motivation

Aim. — Number theory is a study of *Diophantine equations*, i.e., polynomial equations $p(X_1, \ldots, X_n) = 0$ with coefficients in $\mathbb{Z}$ (respectively, in $\mathbb{Q}$) and one seeks solutions $(x_1, \ldots, x_n)$ with the x_i's in $\mathbb{Z}$ (respectively, in $\mathbb{Q}$). One can replace $\mathbb{Z}$ (respectively, $\mathbb{Q}$) by more general rings A (respectively, fields K).

1.1.1. Remark. — The use of $\mathbb{Z}$ to denote integers derives from the German word *Zahlen*. Rationals are *quotients* of integers, hence $\mathbb{Q}$. In French, rings are called *anneaux* hence A. Finally, K comes from the German word *Körper* for field.

1.1.2. Example. — *Pythagorean triplets* $x^2 + y^2 = z^2$, or the question: when does a right triangle have integer sides ?

$(3, 4, 5)$ is a solution, as is $(6, 8, 10)$ or $(3k, 4k, 5k)$ for any integer k.

1.1.3. Question. — For any Diophantine equation we may have the following questions:

1. Is there a solution ?
2. If yes, how many solutions are there ? (finitely many, infinitely many or upto a certain modulus)
3. If the question above can be answered, can we find all such solutions ?

1.1.4. Example. — Consider $x^2 + y^2 = 3z^2$. Of course $(0, 0, 0)$ is a solution trivially, we call it the *trivial solution*. We are interested in *nontrivial solutions* which is what we shall mean by a *solution*. Is there a solution ? In fact there are no solutions and we don't even need any algebraic machinery in this case.

Consider the equation modulo 3, i.e. $x^2 + y^2 \equiv 0 \pmod 3$. The only solutions then are $x \equiv 0$ and $y \equiv 0 \pmod 3$. Thus $x = 3a,\ y = 3b$ for some $a, b \in \mathbb{Z}$. Plugging these values in the equation,

$$\begin{aligned} & 9a^2 + 9b^2 = 3z^2 \\ \implies & 3a^2 + 3b^2 = z^2 \implies 3 \mid z^2 \implies 3 \mid z \\ \implies & \exists c \in \mathbb{Z} : z = 3c \implies \boxed{3a^2 + 3b^2 = 9c^2}. \end{aligned}$$

If (x, y, z) is a solution and $d = \gcd(x, y, z)$ then $(x/d, y/d, z/d)$ is also a solution with $\gcd(x/d, y/d, z/d) = 1$ and we call such solutions with gcd $= 1$ *primitive solutions*. We can assume (x, y, z) is a primitive solution, but we proved that 3 divides each of x, y, z which is absurd as $\gcd(x, y, z) = 1$. Hence, no solutions.

In many cases it is easy to prove that there's no solution, in many cases it is however not easy to do so. A famous example is:

1.1.5. Example (Fermat's Last Theorem)**.** — $x^n + y^n = z^n,\ n \geqslant 3$. In 1995, Andrew Wiles proved that there are no solutions with $xyz \neq 0$

1.1.6. Example (Catalan's conjecture)**.** — $x^n + 1 = y^m$. No solution in positive integers other than $2^3 + 1 = 3^2$. Proven by Preda Mihailescu in 2002.

1.1.7. Example (Euler's conjecture)**.** — $A_1^N + A_2^N + \cdots + A_{N-1}^N = A_N^N$. Euler conjectured that there were no solutions but this was disproven by Noam Elkies with the following counterexample: $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$.

In algebraic number theory we are concerned not just with Diophantine equations and integers but also field extensions of the rationals and other extended number systems.

1.1.8. Definition. — A *field* is a triple $(K, +, \cdot)$ such that

1. $(K, +)$ is an abelian group.
2. $(K \setminus \{0\}, \cdot)$ is an abelian group.
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in K$.

Usually, we only use K to denote the field as the operations $+$ and $\cdot$ are clear.

1.1.9. Example. — We have $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ where p is prime. Analoguous to the construction of the field $\mathbb{C}$ from $\mathbb{R}$ or the ring of *Gaussian integers* $\mathbb{Z}[i]$ from $\mathbb{Z}$ we have the field of *Gaussian numbers* $\mathbb{Q}(i)$ from $\mathbb{Q} = \{a + ib \mid a, b \in \mathbb{Q},\ i^2 = -1\}$.

1.1.10. Definition. — The *characteristic* of a field K is the smallest positive integer n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$ and is denoted $\operatorname{char}(K) = n$. If such an n doesn't exist then we say that K has characteristic 0, $\operatorname{char}(K) = 0$.

1.1.11. Example. — $\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = \operatorname{char}(\mathbb{Q}(i)) = 0$.
$\operatorname{char}(\mathbb{Z}/p\mathbb{Z}) = p > 0$. (positive characteristic)

The main objects of study in this course will be *number fields*. *Number fields* are finite field extensions of rational numbers. Every number field K can be represented as all polynomials in an *algebraic number* α,

$$K = \mathbb{Q}(\alpha) = \left\{ \sum_{k=0}^{n} a_k \alpha^k \;\middle|\; a_k \in \mathbb{Q} \right\}.$$

The main objects that we study in *algebraic number theory* are number fields, rings of integers of number fields, unit groups, ideal class groups, norms, traces, discriminants, prime ideals, Hilbert and other class fields and associated reciprocity laws, zeta and L-functions, and algorithms for computing each of the above. We must emphasise, however, that algebraic number theory is really the *theory of algebraic numbers* more than an *algebraic theory of numbers*. Even though the majority of the tools used in this subject are taken from (commutative) ring theory and Galois theory, the nature of number theory is such that it draws upon almost all branches of mathematics; so one mustn't be surprised to see the use of analytic techniques even in *algebraic* number theory.

1.1.12. Example. — $\mathbb{Q}(i)$ is a number field and degree of $\mathbb{Q}(i)$ over $\mathbb{Q}$ is 2 ($[\mathbb{Q}(i):\mathbb{Q}]=2$). But $\mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ are not number fields.

One possible generalisation of Gaussian numbers can be as follows: define $\zeta_n := e^{2i\pi/n}$, so $\zeta_4 = i$ and ζ_n is a *primitive nth root of unity*, $\zeta_n^n = 1$. Then the field

$$\mathbb{Q}(\zeta_n) = \left\{ \sum_{k=0}^{n} a_k \zeta_n^k \;\middle|\; a_k \in \mathbb{Q} \right\}$$

is a number field of degree $\phi(n) = \#\{\text{positive integers coprime to } n\}$ (Euler's totient function). The number field $\mathbb{Q}(\zeta_n)$ is called a *cyclotomic field* because, geometrically, ζ_n is a point on the unit circle in the complex plane, cutting the circle into exactly n parts (in Greek *cyclo-* means circle and *-tomy* means cutting).

Revisiting Fermat's Last Theorem. — Let us revisit the equation of Fermat's Last Theorem,

$$x^n + y^n = z^n \implies y^n = z^n - x^n = \prod_{k=0}^{n-1} \left(z - \zeta_n^k x\right) \tag{1.1.1}$$

where the factorisation occurs in $\mathbb{Q}(\zeta_n)$. So we have a product of n numbers as an nth power. We may assume (x, y, z) is a primitive solution ($\gcd(x, y, z) = 1$) and hope that the factors on the RHS of

$$y^n = \prod_{k=0}^{n-1} \left(z - \zeta_n^k\right)$$

are 'coprime' in some sense. Now if the product of coprime integers is an nth power y^n then each of these integers should be an nth power. So we may hope that each of the n product terms on the RHS are themselves nth powers and then work from that to get a contradiction. In fact, this is how several mathematicians tried to prove Fermat's Last Theorem in the 19th century, including Lamé and Cauchy. However, this approach doesn't quite work.

Firstly, we should define what we even mean by an integer in a number field like $\mathbb{Q}(\zeta_n)$. This can be done and that led to many developments in algebraic number theory during this time in an attempt to prove Fermat's conjecture using number fields. However, this also led to the main reason why this approach falls apart - the *failure of unique factorisation* in number fields. In particular, Kummer showed that

1.1.13. Theorem. — *If p is an odd prime and 'unique factorisation' holds in $\mathbb{Z}[\zeta_p]$ then $x^p + y^p = z^p$ has no solutions with $xyz \neq 0$.*

Unfortunately, it was Kummer himself who showed that unique factorisation doesn't always hold in this ring $\mathbb{Z}[\zeta_p]$. Kummer did a lot of work in this direction and his notions were further refined by Kronecker and Dedekind. The failure of unique factorisation led to the notion of ideals, and in particular the *ideal class group* which will be a major object of study in this course.

Nevertheless, this approach of using bigger and bigger extensions of number systems beyond the usual rational numbers to solve Diopantine equations has been extremely fruitful.

Around 1955, Yutaka Taniyama and Goro Shimura made the following famous conjecture:

1.1.14. Conjecture (Taniyama-Shimura)**.** — Every elliptic curve E over $\mathbb{Q}$ is modular.

In 1985, assuming towards a contradiction that there was some solution to Fermat's last theorem (the Frey curve), Gerhard Frey showed that he could create an unusual elliptic curve which appeared not to be modular. If the curve were not modular, then this amounted to showing that if Fermat's last theorem were false, then the Taniyama-Shimura conjecture would also be false. Furthermore, if the Taniyama-Shimura conjecture were true, then so would be Fermat's last theorem. The conjecture that Frey's curve was not modular became known as the *ε-conjecture*, and was proven by Ken Ribet in 1986. Serre and Ribet showed that the ε-conjecture (now Ribet's theorem) combined with Conjecture 1.1.14 for semistable elliptic curves was enough to prove Fermat's last theorem. Finally, from 1993 to 1994, Andrew Wiles (with help from his student Richard Taylor in correcting a flaw) provided a proof of Conjecture 1.1.14 for semistable elliptic curves.

Some other applications of algebraic number theory. —

1. **Integer factorisation:** the *general number field sieve* is the most efficient classical algorithm known for factoring integers larger than 10^{100}. In December 2003, the number field sieve was used to factor the RSA-576 $10000 challenge.

2. **Primality test:** In 2002, Manindra Agrawal and his students Nitin Saxena and Neeraj Kayal from IIT Kanpur found the first ever deterministic polynomial-time (in the number of digits) primality test called the *AKS primality test*. Their methods involve arithmetic in quotients of $(\mathbb{Z}/n\mathbb{Z})[x]$, which are best understood in the context of algebraic number theory. For example, Hendrik Lenstra, Daniel J. Bernstein et al have done that and improved the algorithm significantly.

3. **Deeper perspective on number theoretic questions:**
   a) Pell's equation $x^2 - dy^2 = 1 \implies$ Units in real quadratic fields $\implies$ Unit groups in number fields.
   b) Diophantine equations $\implies$ For which n does $x^n + y^n = z^n$ have a solution in $\mathbb{Q}(\sqrt{2})$.
   c) Integer factorisation $\implies$ Factorisation of ideals.
   d) Riemann hypothesis $\implies$ Generalised Riemann hypothesis.
   e) Deeper proof of Gauss' quadratic reciprocity law in terms of arithmetic of cyclotomic fields, which leads to *class field theory*.
   f) The computation of class numbers of number fields is quite difficult; remarkably, it is possible to compute the class number of an infinite tower of cyclotomic fields, which leads to *Iwasawa theory*.

4. **'Algebraic number theory is arithmetic geometry in one-dimension':** arithmetic geometry is 'higher-dimensional algebraic number theory' in the sense that it studies polynomials with several variables lying in arithmetically interesting rings such as the integers or number fields. For instance, the *Weil conjectures* are a deep result in higher-dimensional number theory both motivated by and informed by higher-dimensional complex geometry. A famous major triumph of arithmetic geometry is *Gerd Faltings' proof of Mordell's conjecture*.

1.1.15. Theorem (Faltings). — *Let X be a plane algebraic curve over a number field K. Assume that the manifold $X(\mathbb{C})$ of complex solutions to X has genus at least 2 (i.e., $X(\mathbb{C})$ is topologically a donut with two holes). Then the set $X(K)$ of points on X with coordinates in K is finite.*

For example, Theorem 1.1.15 implies that for any $n \geqslant 4$ and any number field K, there are only finitely many solutions in K to $x^n + y^n = 1$. Apart from the Weil conjectures, a famous open problem in arithmetic geometry is the *Birch and Swinnerton-Dyer conjecture*, which gives a deep conjectural criterion for exactly when $X(K)$ should be infinite when $X(\mathbb{C})$ is a torus.

1.2. Algebraic numbers and number fields K

1.2.1. Definition (Field extension). — If F is a field then a **field extension** (or simply *extension*) of F is a field K containing F as a subfield, denoted K/F (read "K over F").

If K/F is an extension then K is an F-vector space. We say that K/F is a *finite extension* if K is a finite dimensional F-vector space. Otherwise, K/F is an *infinite extension.*

The *degree* of K/F, denoted $[K : F]$, is defined as the dimension of K as an F-vector space. Thus, $[K : F] := \dim_F(K)$.

1.2.2. Example. — Consider the following examples of field extensions:

1. F/F is the only extension of degree 1 for any field F.
2. $\mathbb{C}/\mathbb{R}$ is an extension of degree 2.
3. $\mathbb{R}/\mathbb{Q}$ is an extension of infinite degree.

Our aim is to study finite extensions of rational numbers.

1.2.3. Definition (Number field). — A **number field** K is a finite extension $K/\mathbb{Q}$ of $\mathbb{Q}$.

1.2.4. Definition (Algebraic over K). — Let L/K be an extension. We say that $\alpha \in L$ is **algebraic over K** if there exists a nonzero polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$. Otherwise, α is **transcendental over K**.

1.2.5. Lemma. — *If L/K is a finite extension then every $\alpha \in L$ is algebraic over K.*

1.2.6. Remark. — In particular, this implies that every element of a number field is algebraic over $\mathbb{Q}$. We therefore call the elements of a number field **algebraic numbers**. Two different algebraic closures are isomorphic but the isomorphism isn't unique so we fix an algebraic closure. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Every number field will be a subset of $\overline{\mathbb{Q}}$.

1.3. Number rings $\mathcal{O}_K$

1.3.1. Definition (Algebraic integer)**.** — Let K be a number field. We say that $\alpha \in K$ is an **algebraic integer** if there exists a monic polynomial $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

1.3.2. Proposition. — *Let K be a number field and $\alpha \in K$. The following are equivalent:*

1. *$\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.*
2. *α is an algebraic integer.*
3. *The monic minimal polynomial of α over $\mathbb{Q}$ is contained in $\mathbb{Z}[X]$.*

1.3.3. Definition/Proposition (Number ring)**.** —

$$\mathcal{O}_K := \{\alpha \in K : \alpha \text{ is an algebraic integer}\} \subseteq K.$$

Then $\mathcal{O}_K$ is a subring of K. This ring $\mathcal{O}_K$ is called the **ring of algebraic integers** in K, or a **number ring**.

$$\begin{array}{ccc} K & \supseteq & \mathcal{O}_K \\ | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} \end{array}$$

We'll:

1. Prove $\mathcal{O}_K$ is a Dedekind domain.
2. Prove ideal class group is finite.
3. Show $\mathcal{O}_K^\times$ (its group of units) is a finitely generated $\mathbb{Z}$-module.
4. Find integral basis of $\mathcal{O}_K$, ideal class group of $\mathcal{O}_K$, etc.

1.3.4. Definition (Integrality)**.** — Let A_2 be a ring and $A_1 \subseteq A_2$ a subring. Then $\alpha \in A_2$ is said to be **integral over A_1** if there exists a monic polynomial $f(X) \in A_1[X]$ such that $f(\alpha) = 0$.

The **integral closure** of A_1 in A_2 is the set of all $\alpha \in A_2$ that are integral over A_1. We say that A_1 is **integrally closed in A_2** if A_1 equals its integral closure in A_2.

1.3.5. Lemma. — *$\mathcal{O}_K$ is integrally closed in K.*

1.4. Lattices

Let K be a number field of degree n, $[K : \mathbb{Q}] = n$. After fixing a $\mathbb{Q}$-basis of K, we get $K \cong \mathbb{Q}^n$ as vector spaces.

$$\mathcal{O}_K \subseteq K \cong \mathbb{Q}^n.$$

1.4.1. Proposition*. — *After identifying K with $\mathbb{Q}^n$, we get $\mathcal{O}_K$ as a **lattice** in $\mathbb{Q}^n$.*

Norms and traces. —

1.4.2. Definition (Norm and trace)**.** — Let L/K be a finite extension and for any $y \in L$ define the K-linear map $L \to L$ given by $x \mapsto yx$. If $\{x_1, \dots, x_n\}$ is a K-basis of L, then for some $a_{ij} \in K$

$$yx_i = \sum_{j=1}^{n} a_{ij} x_j. \tag{1.4.1}$$

We get the matrix $A \in K^{n\times n}$ and the *characteristic polynomial* of y is $F(X) = \det(XI - A)$ which is independent of the choice of K-basis of L. We then define the *norm* and *trace* of $y \in L/K$ as, respectively,

$$\mathrm{Tr}_{L/K}(y) = \mathrm{Tr}(A), \quad \mathrm{N}_{L/K}(y) = \det(A). \tag{1.4.2}$$

1.4.3. Proposition. — *If $y_1, y_2 \in L$ then*

$$\mathrm{Tr}_{L/K}(y_1 + y_2) = \mathrm{Tr}_{L/K}(y_1) + \mathrm{Tr}_{L/K}(y_2), \quad \mathrm{N}_{L/K}(y_1 y_2) = \mathrm{N}_{L/K}(y_1)\,\mathrm{N}_{L/K}(y_2). \tag{1.4.3}$$

1.4.4. Proposition. — *If L/K and M/L are finite extensions and, for a fixed $y \in L$, $F_y(X)$ and $f_y(X)$ are characteristic polynomials of y wrt M/K and L/K respectively, then*

$$F(X) = f(X)^{[M:L]}. \tag{1.4.4}$$

1.4.5. Proposition. — *Let L/K be a finite separable extension and $y \in L$. Consider $K(y) \subseteq L$. Let $\{\sigma_1, \dots, \sigma_m\}$ be the embeddings of $K(y)$ in $\overline{K}$. Then*

$$\mathrm{Tr}_{L/K}(y) = [L : K(y)] \sum_{i=1}^{m} \sigma_i(y), \quad \mathrm{N}_{L/K}(y) = \left(\prod_{i=1}^{m} \sigma_i(y) \right)^{[L:K(y)]}. \tag{1.4.5}$$

Some notions on torsion. —

1.4.6. Lemma. — *Let G be a finitely generated torsion-free*[1] *abelian group. Let $\{x_1, \dots, x_n\}$ be a set of generators of G and assume n is the smallest possible number. Then $\sum a_i x_i = 0$ in G for $a_i \in \mathbb{Z}$ implies that $a_i = 0$ for all i.*

1.4.7. Definition (Minimal basis)**.** — Let G be a finitely generated torsion-free abelian group. A **minimal basis** of G is a generating set with as few elements as possible.

1.4.8. Lemma. — *Let G be a finitely generated torsion-free abelian group. Let H be a subgroup of G. There exists a minimal basis $\{x_1, \dots, x_n\}$ of G and integers $m_1, \dots, m_r$ for $r \leqslant n$ such that*

1. *$m_i \geqslant 0$, $m_i \mid m_{i+1}$ for all $1 \leqslant i \leqslant r-1$.*
2. *$\{m_i x_i \mid 1 \leqslant i \leqslant r\}$ is a minimal basis for H.*

Further if $[G : H] < \infty$ then $r = n$.

Let us consider $V = \mathbb{Q}^n$ or $\mathbb{R}^n$, with $K = \mathbb{Q}$ or $\mathbb{R}$ respectively.

[1] A group G is *torsion-free* if there is no $x \in G : x \neq 0$ and $nx = 0$ for some positive integer n.

1.4.9. Definition/Proposition (Lattice)**.** — A lattice Λ in V is a $\mathbb{Z}$-module contained in V satisfying any 2 of the following three:

1. Λ spans V as a K-vector space.
2. Λ is discrete in V.
3. Λ is a free $\mathbb{Z}$-module of rank n.

Moreover, any 2 of the above implies the 3rd.

1.5. Properties of $\mathcal{O}_K$

Recall the proposition made earlier Proposition* 1.4.1:

1.5.1. Proposition. — *If a number field K of degree n is identified with $\mathbb{Q}^n$, then the image of $\mathcal{O}_K$ in $\mathbb{Q}^n$ is a lattice.*

1.5.2. Corollary. — *If K is a number field of degree n, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

1.5.3. Lemma. — *$V = \sigma(k) \otimes_{\mathbb{Q}} \mathbb{R}$ is a vector space over R of dimension $n = [K : \mathbb{Q}]$.*

1.5.4. Lemma. — *$\sigma(\mathcal{O}_K)$ is discrete in $\mathbb{C}^n$.*

1.5.5. Remark. — This shows that $V \cong \mathbb{R}^n$.

1.6. Discriminant

Geometric intuition. —

1.6.1. Question. — What is the 'shape' of $\sigma(\mathcal{O}_K) \cong \mathcal{O}_K$ in V ?
What is the 'volume' of $\mathbb{R}^n/\mathcal{O}_K$?

1. **Approach 1:** Look at measures on $\mathbb{R}^n$. We won't do it measure theoretically in this course, but this is a possible approach.
2. **Approach 2:** Define $M = (\sigma_i(\alpha_j))_{1 \leqslant i,j \leqslant n}$ where $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. From this, we can define a very important invariant quantity - the (absolute) **discriminant** of K, as
$$d_K = \det(M)^2 = \det(M^T M).$$

1.6.2. Definition/Lemma (Integral basis)**.** — Let $\{\beta_1, \ldots, \beta_n\}$ be any $\mathbb{Q}$-basis of K. We define $\Delta^2(\beta_1, \ldots, \beta_n) = \det(\sigma_i(\beta_j))^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i \beta_j)) \in \mathbb{Q}$.
If $\{\beta_1, \ldots, \beta_n\} \subseteq \mathcal{O}_K$ then $\mathbb{Z}$-span of $\{\beta_1, \ldots, \beta_n\}$ is a subgroup of $\mathcal{O}_K$,
$$\Lambda = \mathbb{Z}\beta_1 + \cdots \mathbb{Z}\beta_n \subseteq \mathcal{O}_K. \tag{1.6.1}$$
Let $m = [\mathcal{O}_K : \Lambda]$, then $\Delta^2(\beta_1, \ldots, \beta_n) = m^2 d_K$. We call $\{\beta_1, \ldots, \beta_n\}$ an **integral basis** if it is simultaneously a basis for $K/\mathbb{Q}$ and $\mathcal{O}_K$ over $\mathbb{Z}$,
$$\mathcal{O}_K = \left\{ \sum_{i=1}^{n} c_i \beta_i \;\middle|\; c_i \in \mathbb{Z} \right\} = \bigoplus_{i=1}^{n} \mathbb{Z}\beta_i. \tag{1.6.2}$$

1.6.3. Definition/Proposition (Absolute discriminant)**.** — Given a number field K with ring of integers $\mathcal{O}_K$ and degree $[K:\mathbb{Q}] = n$, the **discriminant** or **absolute discriminant** of K is defined, for an integral basis $\{\alpha_1, \ldots, \alpha_n\}$ of $\mathcal{O}_K$, as

$$d_K = \left(\det(\sigma_i(\alpha_j))_{1\leqslant i,j\leqslant n}\right)^2 = \det(M)^2 = \det(M^T M) \tag{1.6.3}$$

where $\{\sigma_1, \ldots, \sigma_n\}$ are embeddings of K in $\mathbb{C}$. Further,

1. d_K is independent of the choice of integral basis.
2. $d_K \neq 0$.
3. $d_K = \mathrm{Tr}_{K/\mathbb{Q}}\left((\alpha_i\alpha_j)_{1\leqslant i,j\leqslant n}\right)$.
4. $d_K \in \mathbb{Z}$.

Proof. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are two integral bases for $\mathcal{O}_K$, then there exists an invertible change-of-basis matrix $C = (c_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$\beta_j = \sum_{k=1}^{n} c_{jk}\alpha_k \quad \forall j.$$

Now $C \in \mathrm{GL}_n(\mathbb{Z}) \implies \det(C) = \pm 1$. Let $M' = (\sigma_i(\beta_j))_{1\leqslant i,j\leqslant n}$. Observe that

$$\sigma_i(\beta_j) = \sum_{k=1}^{n} c_{jk}\sigma_i(\alpha_k)$$

so that $M' = MC \implies \det(M') = \det(M)\det(C) = \pm\det(M)$.

Hence $\det(M')^2 = \det(M)^2 = d_K$ is independent of choice of integral basis and so the aboslute discriminant is well-defined. □

1.6.4. Corollary. — *Let $\{\beta_1, \ldots, \beta_n\} \subseteq \mathcal{O}_K$ such that $\{\beta_1, \ldots, \beta_n\}$ spans $K/\mathbb{Q}$. If $\Delta^2(\beta_1, \ldots, \beta_n)$ is square-free then $\{\beta_1, \ldots, \beta_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.*

1.6.5. Theorem. — *Let $K/\mathbb{Q}$ be a quadratic extension, i.e. $K = \mathbb{Q}(\sqrt{d})$ with d square-free. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 2, 3 \pmod 4 \end{cases} \tag{1.6.4}$$

and

$$d_K = \begin{cases} d, & \text{if } d \equiv 1 \pmod 4 \\ 4d, & \text{if } d \equiv 2, 3 \pmod 4. \end{cases} \tag{1.6.5}$$

Proof. $d \equiv 2, 3 \pmod 4 \implies \{1, \sqrt{d}\}$ is an integral basis of $\mathcal{O}_K$. So $d_K = \Delta^2(1, \sqrt{d}) = 4d$.

$d \equiv 1 \pmod 4 \implies \left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis of $\mathcal{O}_K$. So $d_K = \Delta^2\left(1, \frac{1+\sqrt{d}}{2}\right) = d$. □

1.6.6. Theorem (Stickelberger)**.** — *For any number field K, $d_K \equiv 0$ or $1 \pmod 4$.*

Chapter 2.

Ideals and factorisation

2.1. Dedekind domains

2.1.1. Definition (Dedekind domain)**.** — A **Dedekind domain** is an integral domain D such that

1. D is Noetherian and integrally closed in the quotient field $Q(D)$ of D.
2. Every nonzero prime ideal in D is a maximal ideal.

2.1.2. Theorem. — *If a ring A is PID then A is Dedekind.*

2.1.3. Definition (Fractional ideal)**.** — A fractional ideal of a Dedekind domain D is a D-submodule of $K = Q(D)$ that is finitely generated.

2.1.4. Lemma. — *Every nonzero fractional ideal of a Dedekind domain D has an inverse.*

2.1.5. Theorem. — *Let D be a Dedekind domain. Then the set $I(D)$ of nonzero fractional ideals in D forms a group under multiplication.*

2.2. Unique factorisation of ideals

2.2.1. Theorem. — *Let D be a Dedekind domain. Every nonzero ideal in D can be written as a product of prime ideals in a unique way (upto reordering).*

2.2.2. Example. — In $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Then

$$6\mathcal{O}_K = (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5})(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$$

is the prime ideal factorisation of $6\mathcal{O}_K$.

2.2.3. Theorem (Chinese Remainder Theorem)**.** — *Let D be a Dedekind domain. Let $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_m^{n_m}$ be a nonzero ideal of D, with $\mathfrak{p}_i \neq \mathfrak{p}_j \ \forall i \neq j$ and $n_i \geqslant 1$. Then*

$$D/\mathfrak{a} \xrightarrow{\cong} \prod_{i=1}^{m} D/\mathfrak{p}_i^{n_i}. \tag{2.2.1}$$

2.3. $\mathcal{O}_K$ as a Dedekind domain

2.3.1. Theorem (Hilbert Basis Theorem)**.** — *If A is a Noetherian ring then $A[X]$ is a Noetherian ring.*

2.3.2. Lemma. — *$\mathcal{O}_K$ is Noetherian.*

2.3.3. Lemma. — *Every nonzero prime ideal in $\mathcal{O}_K$ is maximal.*

2.3.4. Corollary. — *$\mathcal{O}_K$ is a Dedekind domain.*

2.3.5. Definition (Norm of an ideal)**.** — Let $\mathfrak{a}$ be a nonzero ideal on $\mathcal{O}_K$. We define

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

with $\mathrm{N}((0)) = 0$.

Chapter 3.

The ideal class group 3

3.1. Ideal class group of a number field

3.1.1. Lemma. — *Let A be a Dedekind domain and $\mathfrak{p}$ be a nonzero prime ideal. Then $A/\mathfrak{p} \cong \mathfrak{p}^{n-1}/\mathfrak{p}^n$ for $n \geqslant 1$ as A-modules.*

3.1.2. Lemma. — *Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of $\mathcal{O}_K$. Then* $\mathrm{N}(\mathfrak{ab}) = (\mathrm{N}(\mathfrak{a}))(\mathrm{N}(\mathfrak{b}))$.

Notion of primes lying above and below. — Let L/K be a finite extension of number fields and let $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_K$. Consider the 'extension of $\mathfrak{p}$ to $\mathcal{O}_L$.' $\mathfrak{p}\mathcal{O}_L =$ ideal generated by $\mathfrak{p}$ in $\mathcal{O}_L$.

$$\begin{array}{lll} L & \supseteq \mathcal{O}_L & \\ | & | & \\ K & \supseteq \mathcal{O}_K & \supseteq \mathfrak{p} \end{array}$$

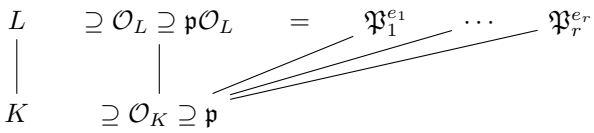
$\mathfrak{p}\mathcal{O}_L$ is a nonzero ideal of $\mathcal{O}_L$.

3.1.3. Warning. — $\mathfrak{p}\mathcal{O}_L$ need not be a prime ideal in $\mathcal{O}_L$.

As $\mathcal{O}_L$ is a Dedekind domain, $\mathfrak{p}\mathcal{O}_L$ has a prime factorisation in $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \tag{3.1.1}$$

where the $\mathfrak{P}_i$'s are prime ideals in $\mathcal{O}_L$.



3.1.4. Definition (Primes lying above, primes lying below and ramification index)**.** — Each prime $\mathfrak{P}_i$ is said to be **above** $\mathfrak{p}$, denoted $\mathfrak{P}_i/\mathfrak{p}$. We also say that $\mathfrak{p}$ is **below** $\mathfrak{P}_i$.

In (3.1.1), e_i is called the **ramification index** of $\mathfrak{P}_i$ in L/K.

3.1.5. Definition/Lemma (Residue fields and residue degree)**.** — $\mathcal{O}_L/\mathfrak{P}_i$ is a finite extension of $\mathcal{O}_K/\mathfrak{p}$. We call the fields

$$k_{\mathfrak{P}_i} = \mathcal{O}_L/\mathfrak{P}_i, k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$$

residue fields and $f_i = [k_{\mathfrak{P}_i} : k_{\mathfrak{p}}]$ is **residue degree** of $\mathfrak{P}_i$.

3.1.6. Theorem. — *Let L/K be a finite extension of number fields with $n = [L : K]$. Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a nonzero prime ideal and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. Then $n = \sum_{1 \leqslant i \leqslant r} e_i f_i$.*

3.2. Integral ideal in an ideal class

3.3. Finiteness of ideal class group

3.4. Geometry of numbers

Chapter 4.

4 Dirichlet's Unit Theorem and change of fields

4.1. Dirichlet's Unit Theorem

4.1.1. Theorem. — *Let K be a number field. Then*

$$\mathcal{O}_K^\times = \{x \in \mathcal{O}_K \mid \exists y \in \mathcal{O}_K \text{ with } xy = 1\} \subseteq \left\{x \in \mathcal{O}_K \mid \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1\right\}$$

is a finitely generated abelian group (finitely generated $\mathbb{Z}$-module). Further,

$$\mathrm{rank}_{\mathbb{Z}}\left(\mathcal{O}_K^\times / \mathrm{Tor}\right) = r_1 + r_2 - 1$$

where

$$\mathrm{Tor} = \mathrm{Tor}\left(\mathcal{O}_K^\times\right) = \{x \in \mathcal{O}_K^\times \mid \exists n \geqslant 1 \text{ with } x^n = 1\}.$$

4.2. Relative extension

Chapter 5.

5 Decomposition groups, the Artin map and theory of valuations

Chapter 6.

6 Local fields

Chapter 7.

7 Field extensions, ramification and the different ideal

Chapter 8.

8 Quadratic fields and binary quadratic forms

8.1. Ramification and the different ideal

8.2. Quadratic fields

8.3. Binary quadratic forms

8.3.1. Definition. — The discriminant of a binary quadratic form $f(X,Y) = aX^2 + bXY + cY^2$ is $\Delta = b^2 - 4ac$.

Chapter 9.

9 Ideal class group for imaginary quadratic fields and binary quadratic forms

9.1. Reduced binary quadratic forms

9.1.1. Definition (Reduced binary quadratic form)**.** — A binary quadratic form $f(X,Y) = aX^2 + bXY + cY^2$ is **reduced** if

1. $a > 0$
2. $|b| \leqslant a \leqslant c$
3. If $|b| = a$ or $a = c$ then $b \geqslant 0$.

In particular it is useful to assume WLOG that $a < c$ and $|b| \leqslant a \leqslant \sqrt{\frac{|\Delta|}{3}}$.

9.2. Class group of imaginary quadratic fields and binary quadratic forms

9.3. Computation of class group of imaginary quadratic fields using binary quadratic forms

9.4. Order 2 elements in class group of imaginary quadratic fields

9.4.1. Theorem. — *Let $K = \mathbb{Q}(\sqrt{m})$ with $m < 0$ and suppose t distinct primes divide d_K. Then there are exactly 2^{t-1} elements of order 2 in the ideal class group $\mathrm{Cl}(K)$.*

Chapter 10.

Special fields

10

10.1. Pure cubic fields

10.1.1. Theorem. — *Consider a pure cubic number field K, i.e. $K = \mathbb{Q}(\sqrt[3]{m})$ with m square-free and cube-free. Let $\alpha = \sqrt[3]{m}$. Then*

$$m \equiv \begin{cases} \pm 1 \pmod 9 & \implies \{1, \alpha, (1 \pm \alpha + \alpha^2)/3\} \text{ is an integral basis.} \\ \text{otherwise} & \implies \{1, \alpha, \alpha^2\} \text{ is an integral basis.} \end{cases} \tag{10.1.1}$$

10.2. Pell's equation

Chapter 11.

11 Biquadratic and cyclotomic fields

Chapter 12.

12 Computation of ideal class groups

12.1. General procedure

Recall the Minkowski bound for a number field K. — Given a number field K, with r_1 real places, r_2 complex places, degree $n = [K : \mathbb{Q}] = r_1 + 2r_2$ and discriminant d_K. Then every ideal class in $\mathrm{Cl}(K)$ contains an integral ideal $\mathfrak{a}$ such that

$$\boxed{\mathrm{N}(\mathfrak{a}) \leqslant \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}.} \tag{12.1.1}$$

Steps for computing the ideal class group of a number field K. —

1. Compute the Minkowski bound m_K for K.
2. Factorise all primes $p \leqslant m_K$ in $\mathbb{Q}$ in the number field K, $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.
3. The ideal class group $\mathrm{Cl}(K)$ is generated by all these $\mathfrak{p}_i$'s.

12.2. Quadratic case

Real quadratic case. — If K is real quadratic then $r_1 = 2, r_2 = 0, n = 2$. Then Minkowski bound is $\boxed{m_K = (1/2)\sqrt{d_K}.}$ Furthermore, the class group of K is trivial i.e.

$$\mathrm{Cl}(K) = \{1\} \iff m_K < 2 \iff d_K < 16.$$

12.2.1. Conjecture (Gauss)**.** — There are infinitely many real quadratic fields K such that $\mathrm{Cl}(K) = \{1\}$.

Imaginary quadratic case. — If K is imaginary quadratic then $r_1 = 0, r_2 = 1, n = 2$. Then Minkowski bound is $\boxed{m_K = (2/\pi)\sqrt{|d_K|}.}$ So we have

$$\mathrm{Cl}(K) = \{1\} \iff m_K < 2 \iff |d_K| < \pi^2 < 11.$$

12.2.2. Theorem (Heegner–Stark-Baker; conjectured by Gauss)**.** — *The class group* $\mathrm{Cl}(K) = \{1\}$ *for* $K = \mathbb{Q}(\sqrt{d_K}), d_K < 0 \iff d_K = -3, -4, -7, -8, -11, -19, -43, -67, -163$. *These numbers are called* ***Heegner numbers****.*

12.2.3. Theorem (Davenport-Heilbronn)**.** — *If* $d_K < 0$ *then* $\mathrm{Cl}(K) \to \infty$ *as* $|d_K| \to \infty$.

12.3. Cubic case

We'll first consider $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(X) = X^3 + X + 3$. We'll first note that f is irreducible over $\mathbb{Z}$ (and hence over $\mathbb{Q}$), as

$$f(X) \equiv X^3 + X + 1 \pmod 2$$

which has no roots in $\mathbb{F}_2$. Hence, f is irreducible (mod 2 as well).

As α is a root of f, $\{1, \alpha, \alpha^2\}$ is a $\mathbb{Q}$-basis of $K = \mathbb{Q}(\alpha)$. The discriminant for a general cubic polynomial $aX^3 + bX^2 + cX + d$ is given by

$$\boxed{\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.}$$

So $\Delta^2(1, \alpha, \alpha^2)$

$$= 18(1)(0)(1)(3) - 4(0)^3(3) + (0)^2(1)^2 - 4(1)(1)^3 - 27(1)^2(3)^2 = -247.$$

Now $m^2 d_K = \Delta^2(1, \alpha, \alpha^2) = -247$ where $m = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. As $-247 = -13 \cdot 19$ is square-free, it follows that $m = 1$ and $\{1, \alpha, \alpha^2\}$ is an integral basis of K. Hence, $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Now, in general, the sign of d_K is $(-1)^{r_2}$, and as $d_K = -247 < 0$, r_2 must be odd. As $r_1 + 2r_2 = 3$, we must have $r_1 = r_2 = 1$. Thus, the Minkowski bound is

$$\frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{247} = \frac{24\sqrt{247}}{27\pi} < 5. \tag{12.3.1}$$

So we look at primes lying above 2 and 3. We already showed that f is irreducible mod 2 so (2) is prime. Now,

$$f(X) \equiv X^3 + X \equiv X(X^2 + 1) \pmod 3.$$

Here, $X^2 + 1$ is irreducible over $\mathbb{F}_3$ because $-1 \notin (\mathbb{F}_3)^2$. So we get that $(3) = \mathfrak{p}_3\mathfrak{p}_9$ where $\mathfrak{p}_3 = (3, \alpha)$ and $\mathfrak{p}_9 = (3, \alpha^2 + 1)$. But from the relation $\alpha^3 + \alpha + 3 = 0$ we get that

$$3 = -\alpha(\alpha^2 + 1) \in (\alpha) \cap (\alpha^2 + 1).$$

Hence, $\mathfrak{p}_3 = (\alpha), \mathfrak{p}_9 = (\alpha^2 + 1)$ are principal so $[\mathfrak{p}_3] = [\mathfrak{p}_9] = 1$ in $\mathrm{Cl}(K)$. Hence, class group $\mathrm{Cl}(K)$ is generated by the classes of $\mathfrak{p}_3$ and $\mathfrak{p}_9$ both of which are principal. Therefore, $\mathrm{Cl}(K) = \{1\}$ and the class number is 1.