Chapter 1

Elementary Number Theory

1.1. The Unique Factorization of Integers

In this section, we will state some properties of $\mathbb{Z}$, the set of integers.

Lemma 1.1.1. *If a and b are relatively prime, then we can find integers x and y such that $ax+by = 1$.*

By Lemma 1.1.1, we can easily derive the following.

Proposition 1.1.2. *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

We have the *Fundamental Theorem of Arithmetic*.

Theorem 1.1.3. *$\mathbb{Z}$ has unique factorization.*

The existence part of Theorem 1.1.3 can be proved by the fact that every positive integer greater than 1 has a prime divisor and the uniqueness part can be proved by using Proposition 1.1.2

Definition 1.1.4. For any integer n, we define $\phi(n)$ to be the number of integers less than n which are co-prime to n. This is known as the *Euler $\phi-$function*

By interpreting $\phi(n)/n$ as the probability that a random number chosen from $1, \ldots, n$ is co-prime to n, we have that

$$\frac{\phi(n)}{n} = \prod_{p|n}(1 - \frac{1}{p}).$$

For a prime number p, we have $\phi(p) = p - 1$. *Fermat's Little Theorem* says that if $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. This can be proved by using induction and the fact that the *binomial coefficient* $\binom{p}{k}$, for $k \leq p-1$ is divisible by p. However, by using elementary group theory, the following proposition which is due to Euler, generalizes Fermat's Little Theorem

Proposition 1.1.5. *Given a, $n \in \mathbb{Z}$, $a^{\phi(n)} \equiv 1 \pmod{n}$ when $\gcd(a, n) = 1$.*

Consider prime of the form $a^n - 1$. If n has a factor, say k, then $a^k - 1 \mid a^n - 1$. If $a > 2$, then $a^n - 1$ is divisible by $a - 1$ and is therefore not prime. Therefore if $a^n - 1$ is a prime, then $a = 2$ and n is a prime. Numbers of this form are called *Mersenne numbers*.

On the other hand, consider primes of the form 2^n+1. If n has an odd factor, say $n=rs$ with r odd, then $2^{rs}+1$ is divisible by 2^s+1 and is therefore not prime. Hence, we have the following definition.

Definition 1.1.6. We call integers of the form $F_n = 2^{2^n}+1$, the *Fermat numbers*

Fermat made the conjecture that these numbers are all primes. Indeed, $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, and $F_4=65537$ are all primes, but unfortunately, F_5 is divisible by 641. It is unknown if F_n represents infinitely many primes. It is also unknown if F_n is infinitely often composite.

1.2. The ABC Conjecture

Given a nature number n, let $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$. Define the *radical* of n, denoted $\mathrm{rad}(n)$, to be the product $p_1\cdots p_k$.

In 1980, Masser and Oesterlé formulated the following conjecture. Suppose that we have three mutually co-prime integers A, B and C satisfying $A+B=C$. Given any $\varepsilon>0$, it is conjectured that there is a constant $\kappa(\varepsilon)$ such that

$$\max(|A|,|B|,|C|) \le \kappa(\varepsilon)(\mathrm{rad}(ABC))^{1+\varepsilon}.$$

This is called the *ABC Conjecture*.

Proposition 1.2.1. *Assuming the ABC Conjecture, if $xyz\neq 0$ and $x^n+y^n=z^n$ for three mutually co-prime integers x, y and z, then n is bounded.*

A nature number n is called *squarefull*, if n has no squarefree part (*i.e.* if $p\,|\,n$ then $p^2\,|\,n$). Erdös conjectured that we cannot have three consecutive squarefull natural numbers. Assuming that the Erdös conjecture is true, we can show that there are infinitely many primes p such that $2^{p-1}\not\equiv 1 \pmod{p^2}$.

Exercise

(1) Let $a_1,\ldots,a_n$ for $n\ge 2$ be nonzero integers. Suppose that there is a prime p and positive integer h such that $p^h\,|\,a_i$ for some i and p^h does not divide a_j for all $j\neq i$. Then show that

$$S=\frac{1}{a_1}+\cdots+\frac{1}{a_n}$$

is not an integer.

(2) Show that $n\,|\,\phi(a^n-1)$ for any $a>n$.

(3) Show that $n\not| 2^n-1$ for any nature number $n>1$.

(4) Let $\pi(x)$ be the number of primes less than or equal to x
   (a) Show that $p_k<2^{2^k}$, where p_k denotes the k-th prime.
   (b) Prove that $\pi(x)\ge \ln(\ln x)$.

(5) Prove *Wilson's Theorem*. Thus $(p-1)!\equiv -1 \pmod{p}$ if and only if p is a prime. Use Wilson's theorem to prove that for a prime p, $x^2\equiv -1 \pmod{p}$ is solvable if and only if $p=2$ or $p\equiv 1 \pmod{4}$.

(6) Prove that if $f(x)\in\mathbb{Z}[x]$, then $f(x)\equiv 0 \pmod{p}$ is solvable for infinitely many primes p.

(7) Let q be prime. Show that there are infinitely many primes p so that $p\equiv 1 \pmod{q}$. (Hint: Consider the polynomial $f(x)=(x^q-1)/(x-1)=1+x+\cdots+x^{q-1}$.)

(8) Prove that if p is an odd prime, any prime divisor of $2^p - 1$ is of the form $2kp + 1$, with k a positive integer.

(9) Let $F_n = 2^{2^n} + 1$ be the Fermat numbers.
   (a) Show that F_n divides $F_m - 2$ if $n < m$, and from this deduce that F_n and F_m are relatively prime if $m \neq n$.
   (b) Prove that every divisor of F_n is of the form $2^{n+1}k + 1$.
   (c) Show that there are infinitely many primes p such that $p \equiv 1 \pmod{2^r}$ for any given r.

(10) Let p be an odd prime and let d be the order of 2 modulo p (*i.e.* d is the least positive integer such that $2^d \equiv 1 \pmod{p}$.)
   (a) Suppose that $2^n \equiv 1 \pmod{p}$ and $2^n \not\equiv 1 \pmod{p^2}$. Show that $2^d \not\equiv 1 \pmod{p^2}$.
   (b) Suppose that $2^n \equiv 1 \pmod{p}$ and $2^n \not\equiv 1 \pmod{p^2}$. Show that $2^{p-1} \not\equiv 1 \pmod{p^2}$.
   (c) Assuming the ABC conjecture, show that there are infinitely many prime p such that $2^{p-1} \not\equiv 1 \pmod{p^2}$.

(11) Assuming the ABC conjecture, prove that there are only finitely many n such that $n - 1$, n and $n + 1$ are squarefull.

Chapter 2

Euclidean Rings

2.1. Unique Factorization Domain

In this chapter R is a commutative ring with identity 1. If a, $b \in R$, we will write $a \mid b$ (a divides b), if there exists some $c \in R$ such that $ac = b$. Any divisor of 1 is called a *unit*. We will say that a and b are *associate* and write $a \sim b$, if there exists a unit $u \in R$ such that $a = bu$. It is easy to verify that $\sim$ is an equivalent relation.

Definition 2.1.1. We say that $\pi \in R$ is *irreducible* if for any factorization $\pi = ab$, one of a or b is a unit. We say that $\tau \in R$ is a *prime* if $\tau \mid ab$ implies that $\tau \mid a$ or $\tau \mid b$.

We remark that in general, an irreducible element is not necessary a prime.

Definition 2.1.2. Suppose that there is a map $N : R \to \mathbb{N}$ such that:

(1) $N(ab) = N(a)N(b)$;

(2) $N(a) = 1$ if and only if a is a unit.

Then we call such a map a *norm map* with $N(a)$ the *norm* of a.

Proposition 2.1.3. *Suppose that R is an integral domain with a norm map. Then R can be written as a product of irreducible elements.*

Definition 2.1.4. We say that R, an integral domain, is a *unique factorization domain* if:

(1) every element of R can be written as a product of irreducibles;

(2) if $a = \pi_1 \cdots \pi_r = \tau_1 \cdots \tau_s$ with π_i and τ_j irreducibles, then $r = s$ and after a suitable permutation, $\pi_i \sim \tau_i$.

Example 2.1.5. Let $R = \mathbb{Z}[\sqrt{-5}]$. Then $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible in R and they are not associate. Observe that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, so that R is not a unique factorization domain.

Definition 2.1.6. An ideal $I \subseteq R$ is called *principal* if it can be generated by a single element of R. A domain R is then called a *principle ideal domain*, if every ideal of R is principle.

Theorem 2.1.7. *If R is a principle ideal domain, then R is a unique factorization domain.*

The proof of Theorem 2.1.7 is similar to the proof Theorem 1.1.3. We first prove that every element of R can be written as a product of irreducibles for the existence and then prove that an irreducible element is a prime for the uniqueness.

Now, we describe an important class of principle ideal domains:

Definition 2.1.8. If R is a domain with a map $\psi : R \to \mathbb{N}$ and given $a, b \in R$, there exist $q, r \in R$ such that $a = bq + r$ with $r = 0$ or $\psi(r) < \psi(b)$, then we call R an *Euclidean domain.*

Theorem 2.1.9. *If R is an Euclidean domain, then it is a principle ideal domain.*

Definition 2.1.10. Let R be a unique factorization domain and $f(x) \in R[x]$. Then we define the *content* of f to be the greatest common divisor of the coefficients of f, denoted by $\mathcal{C}(f)$.

Let R be a unique factorization domain and let K be its field of fraction. The following result, called *Gauss' Lemma*, allows us to relate the factorization of polynomials in $R[x]$ with that in $K[x]$.

Lemma 2.1.11 (Gauss' Lemma)**.** *Let R be a unique factorization domain. Then, for $f(x)$ and $g(x) \in R[x]$, we have $\mathcal{C}(f \cdot g) = \mathcal{C}(f)\mathcal{C}(g)$.*

Because for a field K, $K[x]$ is an Euclidean domain, we have the following.

Theorem 2.1.12. *If R is a unique factorization domain, then $R[x]$ is a unique factorization domain.*

2.2. Gaussian Integers and Eisenstein Integers

Let $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}, i = \sqrt{-1}\}$. This ring is often called the ring of *Gaussian integers*. It can be shown that $\mathbb{Z}[i]$ is an Euclidean domain and the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Let $\rho = (-1 + \sqrt{-3})/2$. Notice that $\rho^2 + \rho + 1 = 0$ and notice that $\rho^2 = \overline{\rho}$. The set $\mathbb{Z}[\rho] = \{a + b\rho \,|\, a, b \in \mathbb{Z}\}$ is a ring which is called the ring of *Eisenstein integers*. Notice that $\mathbb{Z}[\rho]$ is closed under complex conjugation. $\mathbb{Z}[\rho]$ is also an Euclidean domain and the only units in $\mathbb{Z}[\rho]$ are ± 1, $\pm\rho$ and $\pm\rho^2$.

Example 2.2.1. We have $(x-\rho)(x-\rho^2) = x^2+x+1$, so that $3 = (1-\rho)(1-\rho^2) = (1+\rho)(1-\rho)^2 = -\rho^2(1-\rho)^2$. Because $1 - \rho$ is irreducible, we have a factorization of 3.

We can use the unique factorization property of $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ to solve certain Diophantine equations for integers. For instance, we can apply the arithmetic of $\mathbb{Z}[i]$ to show that the equation $y^2 + 1 = x^3$ has no integer solutions with $xy \neq 0$.

Exercise

(1) Let D be squarefree. Consider $R = \mathbb{Z}[\sqrt{D}]$. Show that every element of R can be written as a product of irreducible elements

(2) Find all the prime elements of the ring $\mathbb{Z}[i]$.

(3) Show that a positive integer a is a sum of two squares if and only if $a = b^2c$ where c is not divisible by any prime $p \equiv 3 \pmod 4$.

(4) Show that $\mathbb{Z}[\rho]/(1 - \rho)$ has order 3.

(5) Consider the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\}$.
   (a) Show that $\mathbb{Z}[\sqrt{2}]$ is Euclidean.

(b) Let $\epsilon = 1 + \sqrt{2}$. Write $\epsilon^n = u_n + v_n\sqrt{2}$. Show that $u_n^2 - 2v_n^2 = \pm 1$.
(c) Show that there is no unit η in $\mathbb{Z}[\sqrt{2}]$ such that $1 < \eta < \varepsilon$. Deduce that every unit of $\mathbb{Z}[\sqrt{2}]$ is of the form $\pm\varepsilon^n$ for $n \in \mathbb{Z}$.

(6) Prove that $\mathbb{Z}[\sqrt{-10}]$ is not a unique factorization domain.

(7) Show that $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$ is Euclidean.

(8) Show that for considering the norm map, $\mathbb{Z}[(1 + \sqrt{-19})/2]$ is not Euclidean.

(9) Prove that $\mathbb{Z}[\sqrt{6}]$ is Euclidean.

(10) Show that there are only finitely many rings $\mathbb{Z}[\sqrt{d}]$ with $d \equiv 2$ or $d \equiv 3 \pmod 4$ which are norm Euclidean.

Chapter 3

Algebraic Numbers and Integers

3.1. Basic Concepts

a number $\alpha \in \mathbb{C}$ is called an *algebraic number* if there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. If $f(x)$ is a monic polynomial with coefficients in $\mathbb{Z}$, we say that α is an *algebraic integer*. Clearly all algebraic integers are algebraic numbers. However, the converse is false.

Example 3.1.1. $\sqrt{2}/3$ is a root of $f(x) = 9x^2 - 2$, so it is an algebraic number. Because there is no monic polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(\sqrt{2}/3) = 0$, $\sqrt{2}/3$ is not an algebraic integer.

Proposition 3.1.2. *Let α be an algebraic number. There exists a unique polynomial $p(x) \in \mathbb{Q}[x]$ which is monic, irreducible and of smallest degree such that $p(\alpha) = 0$. Furthermore, if $f(x) \in \mathbb{Q}[x]$ and $f(\alpha) = 0$, then $p(x) \mid f(x)$ in $\mathbb{Q}[x]$.*

The degree of $p(x)$ is called the *degree* of α and is denoted $\deg(\alpha)$; $p(x)$ is called the *minimal polynomial* of α.

The set of algebraic numbers is countable. Since the set of complex numbers, $\mathbb{C}$, is uncountable, it follows that there exist complex numbers which are not algebraic. These numbers are called *transcendental* and the set of transcendental numbers is uncountable.

3.2. Liouville's Theorem and Generalizations

In 1853, Liouville showed that algebraic numbers cannot be too well approximated by rational numbers.

Theorem 3.2.1 (Liouville)**.** *Given a real algebraic number α of degree $n \neq 1$, there is a constant $c = c(\alpha)$ such that for all rational numbers p/q, $(p, q) = 1$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$$

holds.

Using Theorem 3.2.1, we can give specific examples of transcendental numbers. For instance, we can show that

$$\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

In 1909, Thue was able to improve Liouville's inequality.

Theorem 3.2.2 (Thue)**.** *If α is algebraic of degree n, then there exists a constant $c(\alpha)$ so that for all $p/q \in \mathbb{Q}$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{n/2+1}}.$$

Theorem 3.2.2 has immediate Diophantine applications.

Proposition 3.2.3. *Let $f(x, y)$ be an irreducible polynomial of degree $n \geq 3$. For any fixed $m \in \mathbb{Z}^*$, $f(x, y)$ has only finitely many solutions.*

Over a long series of improvements upon Liouvilles's Theorem, in 1955, Roth was able to improve the inequality.

Theorem 3.2.4 (Roth)**.** *Given an algebraic number α, for any $\varepsilon > 0$, there exists a constant $c(\alpha, \varepsilon)$ so that for all $p/q \in \mathbb{Q}$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

This improved inequality gives us a new family of transcendental numbers. For example, $\sum_{n=1}^{\infty} 2^{-3^n}$ is transcendental.

3.3. Algebraic Number Fields

A field $K \subset \mathbb{C}$ is called an *algebraic number field* if its dimension over $\mathbb{Q}$ is finite. The dimension of K over $\mathbb{Q}$ is called the *degree* of K and is denoted $[K : \mathbb{Q}]$.

Let α be an algebraic number of degree n and define $\mathbb{Q}[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{Q}[x]\}$, a subring of $\mathbb{C}$. Then $\mathbb{Q}[\alpha]$ is an algebraic number filed of degree n over $\mathbb{Q}$. From now on, we will denote $\mathbb{Q}[\alpha]$ by $\mathbb{Q}(\alpha)$.

Let α and β be algebraic numbers. $\mathbb{Q}(\alpha, \beta)$ is a field since it is the intersection of the subfields of $\mathbb{C}$ containing $\mathbb{Q}$, α and β. The intersection of a finite number of subfields in a fixed field is again a field.

Proposition 3.3.1. *If α and β are algebraic numbers, then there exists an algebraic number θ such that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$.*

Proposition 3.3.1 can be generalized quite easily using induction: for a finite set of algebraic numbers $\alpha_1, \ldots, \alpha_n$, there exists an algebraic number θ such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\theta)$. Therefore, any algebraic number field K is $\mathbb{Q}(\theta)$ for some algebraic number θ.

The roots of minimal polynomial $p(x)$ of α are called the *conjugates* of α. Since, $p(x)$ has no repeated roots, if n is the degree of $p(x)$, then α has n conjugates. If $\theta = \theta^{(1)}$ and $\theta^{(2)}, \ldots, \theta^{(n)}$ are the conjugates of θ, then $\mathbb{Q}(\theta^{(i)})$ for $i = 2, \ldots, n$ is called a *conjugate field* to $\mathbb{Q}(\theta)$. Further, the maps $\theta \mapsto \theta^{(i)}$ are monomorphisms of $\mathbb{Q}(\theta) \to \mathbb{Q}(\theta^{(i)})$ which is referred to as *embeddings* of $\mathbb{Q}(\theta)$ to $\mathbb{C}$. we can partition the conjugates of θ into real roots and nonreal roots (called complex roots).

K is called a *normal extension* of $\mathbb{Q}$ if all the conjugate fields of K are identical to K. We also define the *normal closure* of any field K as the extension $\widetilde{K}$ of smallest degree containing all the conjugate fields of K.

Using Galois Theory, Liouville's theorem also holds for α where α is a complex algebraic number of degree $n \geq 2$.

The following theorem gives several characterizations of algebraic integers.

Theorem 3.3.2. *The following statements are equivalent:*

(1) *α is an algebraic integer.*

(2) *The minimal polynomial of α is monic over $\mathbb{Z}$*

(3) *$\mathbb{Z}[\alpha]$ is a finite generated $\mathbb{Z}$-module.*

(4) *There exists a finitely generated $\mathbb{Z}$-submodule $M \neq \{0\}$ of $\mathbb{C}$ such that $\alpha M \subseteq M$.*

Part (c) and (d) of Theorem 3.3.2 are the most useful because they supply us with an immediate tool to test whether a given number is an algebraic integer or not.

Proposition 3.3.3. *Let K be an algebraic number field. Let $\mathcal{O}_K$ be the set of all algebraic integers in K. Then $\mathcal{O}_K$ is a ring.*

Exercise

(1) Show that if $r \in \mathbb{Q}$ is an algebraic integer, then $r \in \mathbb{Z}$.

(2) Find the minimal polynomial of $\sqrt{n}$ where n is a squarefree integer.

(3) Show that

$$\sum_{n=0}^{\infty} \frac{1}{a^{n!}}$$

is transcendental for $a \in \mathbb{Z}$ and $a \geq 2$.

(4) Show that

$$\sum_{n=0}^{\infty} \frac{1}{a^{f(n)}}$$

is transcendental for $a \in \mathbb{Z}$ and $a \geq 2$ when

$$\lim_{n \to \infty} \frac{f(n+1)}{f(n)} > 2$$

.

(5) Show that there are only finitely many integral solutions to the equation $x^3 + 3x^2y + xy^2 + y^3 = m$.

(6) Let α be an algebraic number. Show that there exists $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

(7) Let $K = \mathbb{Q}(\theta)$ be of degree n over $\mathbb{Q}$. Let $\omega_1, \ldots, \omega_n$ be a basis of K as a vector space over $\mathbb{Q}$. Show that the matrix (a_{ij}) is invertible, where $a_{ij} = w_i^{(j)}$.

(8) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and assume that $p \,|\, a_i$ for $i = 0, \ldots, k-1$ and $p^2 \nmid a_0$. Show that $f(x)$ has an irreducible factor of degree at least k.

(9) Prove that $f(x) = x^6 + 7x^5 - 12x^3 + 6x + 8$ is irreducible over $\mathbb{Q}$.

(10) Let ζ_m be a primitive m-th root of unity. Show that

$$\prod_{0\le i\ne j\le m-1} (\zeta_m^i - \zeta_m^j) = (-1)^{m-1} m^m.$$

(11) Let

$$\phi_m(x) = \prod_{1\le i\le m,\ (i,m)=1} (x - \zeta_m^i)$$

denote the m-th cyclotomic polynomial.

(a) Prove that

$$x^m - 1 = \prod_{d|m} \phi_d(x).$$

(b) Let I be a subset of the positive integers smaller than m which are co-prime to m. Suppose that

$$f(x) = \prod_{i\in I} (x - \zeta_m^i) \in \mathbb{Z}[x].$$

Show that if $f(\zeta_m) = 0$ and $f(\zeta_m^p) \ne 0$ for some prime p, then $p \,|\, m$.

(c) Show that $\phi_m(x) \in \mathbb{Z}[x]$ and is irreducible in $\mathbb{Q}[x]$.

(12) Let a be a squarefree and greater than 1 and let p be a prime. Show that the normal closure of $\mathbb{Q}(a^{1/p})$ is $\mathbb{Q}(a^{1/p}, \zeta_p)$.

Chapter 4

Integral Bases

In this chapter, we look more closely at the algebraic structure of $\mathcal{O}_K$, the ring of integers of an algebraic number field K. In particular, we show that $\mathcal{O}_K$ is always a finitely $\mathbb{Z}$-module admitting a $\mathbb{Q}$-basis for K as a generating set (where K is viewed as a $\mathbb{Q}$-vector space). We will also define an important invariant of a number field called the discriminant which arises in many calculations within the number field.

4.1. The Norm and the Trace

Recall that if K is an algebraic number field, then K can be viewed as a finite dimensional vector space over $\mathbb{Q}$. If $\alpha \in K$, the map from K to K defined by $\Phi_\alpha : v \mapsto \alpha v$ gives a linear operator on K. We define the *trace* of α by $\mathrm{Tr}_K(\alpha) := \mathrm{Tr}(\Phi_\alpha)$ and the *norm* of α by $\mathrm{N}_K(\alpha) := \det(\Phi_\alpha)$. Thus, we choose any $\mathbb{Q}$-basis $\omega_1, \omega_2, \ldots, \omega_n$ of K and write $\alpha\omega_i = \sum_{j=1}^n a_{ij}\omega_j$ for all $1 \leq i \leq n$, so $\mathrm{Tr}_K(\alpha) = \sum_{i=1}^n a_{ii}$ and $\mathrm{N}_K(\alpha) = \det(a_{ij})$.

Lemma 4.1.1. *If K is an algebraic number field of degree n over $\mathbb{Q}$ and $\alpha \in \mathcal{O}_K$ its ring of integers, then $\mathrm{Tr}_K(\alpha)$ and $\mathrm{N}_K(\alpha)$ are in $\mathbb{Z}$.*

Given an algebraic number field K and $\omega_1, \omega_2, \ldots, \omega_n$ a $\mathbb{Q}$-basis for K, consider the correspondence from K to $M_n(\mathbb{Q})$ (the space of $n \times n$ matrix over $\mathbb{Q}$) given by $\alpha \mapsto (a_{ij})$ where $\alpha\omega_i = \sum_{j=1}^n a_{ij}w_j$. This is readily seen to give a homomorphism from K to $M_n(\mathbb{Q})$. From this we can deduce that $\mathrm{Tr}_K(\cdot)$ is in fact a $\mathbb{Q}$-linear map from K to $\mathbb{Q}$.

Lemma 4.1.2. *The bilinear pairing given by $B(x, y) : K \times K \to \mathbb{Q}$ such that $(x, y) \mapsto \mathrm{Tr}_K(xy)$ is nondegenerate.*

We remark that the definition of nondegeneracy above is independent of the choice of basis.

4.2. Existence of an Integral Basis

Let K be an algebraic number field of degree n over $\mathbb{Q}$ and $\mathcal{O}_K$ its ring of integers. We say that $\omega_1, \omega_2, \ldots, \omega_n$ is an *integral basis* for $\mathcal{O}_K$ if $\omega_i \in \mathcal{O}_K$ for all i and $\mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$. In general, we say that a $\mathbb{Z}$-module M has an integral basis if there exists $\alpha_1, \alpha_2, \ldots, \alpha_m \in M$ such that $M = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_m$, for some positive integer m, and $\alpha_1, \ldots, \alpha_m$ are linearly independent over $\mathbb{Z}$.

For a module M with submodule N, we can define the *index* of N in M to be the number of elements in M/N and denote this by $[M : N]$.

Lemma 4.2.1. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a set of generators for a finitely generated $\mathbb{Z}$-module M and let N be a submodule.*

(1) *There exist $\beta_1, \beta_2, \ldots, \beta_m$ in N with $m \leq n$ such that $N = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots \mathbb{Z}\beta_m$ and $\beta_i = \sum_{j \geq i} p_{ij}\alpha_j$ with $1 \leq i \leq m$ and $p_{ij} \in \mathbb{Z}$.*

(2) *If $m = n$, then $[M : N] = p_{11}p_{22}\cdots p_{nn}$.*

In Exercise 2, we ask you to prove that there exist $w_1, w_2 \ldots, w_n \in K$ such that $\mathcal{O}_K \subseteq \mathbb{Z}w_1 + \mathbb{Z}w_2 + \cdots + \mathbb{Z}w_n$. Applying Lemma 4.2.1, we have the following.

Theorem 4.2.2. *$\mathcal{O}_k$ has an integral basis.*

For example, let $K = \mathbb{Q}(\sqrt{D})$ with D a squarefree integer. If $D \equiv 1 \pmod 4$, then we can choose 1, $(1 + \sqrt{D})/2$ as an integral basis. If $D \equiv 2, 3 \pmod 4$, then we can choose 1, $\sqrt{D}$ as an integral basis.

We are justified now in making the following definition.

Definition 4.2.3. If K is an algebraic number field of degree n over $\mathbb{Q}$ and $\mathcal{O}_K$ its ring of integers, define the *discriminant* of K as $d_K := \det(\omega_i^{(j)})^2$, where $\omega_1, \omega_2, \ldots, \omega_n$ is an integral basis for $\mathcal{O}_K$.

Note that the discriminant is independent of the choice of integral basis.

We can generalize the notion of a discriminant for arbitrary elements of K. Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K. For $a_1, a_2, \ldots, a_n \in K$, we can define $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = \det(\sigma_i(a_j))^2$.

We denote $d_{K/\mathbb{Q}}(1, a, a^2, \ldots, a^{n-1})$ by $d_{K/\mathbb{Q}}(a)$. If α is an algebraic integer with minimal polynomial $f(x)$. Then we have

$$d_{K/\mathbb{Q}}(\alpha) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\alpha^{(i)}).$$

Definition 4.2.4. Suppose α is an algebraic integer of degree n, generating a field K. We define the *index* of α to be the index of $\mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$ in $\mathcal{O}_K$.

Suppose that the minimal polynomial of α is an Eisenstein polynomial with respect to a prime number p. We can show that the index of α is not divisible by p.

4.3. Ideals in $\mathcal{O}_K$

At this point, we have shown that $\mathcal{O}_K$ is indeed much like $\mathbb{Z}$ in its algebraic structure. It turns out that we are only halfway to the final step in our generalization of an integer in a number field. We may think of the ideals in $\mathcal{O}_K$ as the most general integers in K, and we remark that when this set of ideals is endowed with the usual operations of ideal addition and multiplication, we recover an arithmetic most like that of $\mathbb{Z}$.

Because for a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we have $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$, it implies that the index of $\mathfrak{a}$ in $\mathcal{O}_K$ must be finite. By Lemma 4.2.1, $\mathfrak{a}$ has an integral basis.

We define the *norm* of a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ to be its index in $\mathcal{O}_K$. We will denote the norm of $\mathfrak{a}$ by $N(\mathfrak{a})$.

Exercise

(1) Determine the algebraic integers of $K = \mathbb{Q}(\sqrt{-5})$.

(2) Show that there exist $w_1, w_2 \ldots, w_n \in K$ such that $\mathcal{O}_K \subseteq \mathbb{Z}w_1 + \mathbb{Z}w_2 + \cdots + \mathbb{Z}w_n$.

(3) Let K be an algebraic number field of finite degree over $\mathbb{Q}$. Show that $d_K \equiv 0$ or $1 \pmod 4$.

(4) Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the embeddings of K. For $a_1, a_2, \ldots, a_n \in K$, define $d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = \det(\sigma_i(a_j))^2$.
   (a) Show that
   $$d_{K/\mathbb{Q}}(1, a, \ldots, a^{n-1}) = \prod_{i>j} \big(\sigma_i(a) - \sigma_j(a)\big)^2.$$
   (b) Suppose that $u_i = \sum_{j=1}^n a_{ij} v_j$ with $a_{ij} \in \mathbb{Q}$, $v_j \in K$. Show that
   $$d_{K/\mathbb{Q}}(u_1, u_2, \ldots, u_n) = \big(\det(a_{ij})\big)^2 d_{K/\mathbb{Q}}(v_1, v_2, \ldots, v_n).$$
   (c) Let $a_1, a_2, \ldots, a_n$ be linearly independent over $\mathbb{Q}$. Let $N = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_n$ and $m = [\mathcal{O}_K : N]$. Prove that
   $$d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n) = m^2 d_K.$$
   (d) Let $\mathfrak{a}$ be an integral ideal with basis $\alpha_1, \ldots, \alpha_n$. Show that
   $$|\det(\alpha_i^{(j)})|^2 = N(\mathfrak{a})^2 d_K.$$
   (e) Let K be an algebraic number field. Suppose that $\theta \in \mathcal{O}_K$ is such that $d_{K/\mathbb{Q}}(\theta)$ is squarefree. Show that $\mathcal{O}_K = \mathbb{Z}[\theta]$.
   (f) Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{Z}$ be the minimal polynomial of θ. Let $K = \mathbb{Q}(\theta)$. If for each prime p such that $p \,|\, d_{K/\mathbb{Q}}(\theta)$ we have $f(x)$ Eisensteinian with respect to p, show that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

(5) Let $K = \mathbb{Q}(\alpha)$ where $\alpha = r^{1/3}$, $r = ab^2 \in \mathbb{Z}$, where ab is squarefree. Suppose that $3 \nmid b$. Find an integral basis for $\mathcal{O}_K$.

(6) Let $K = \mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 2\theta - 8 = 0$
   (a) Show that $f(x) = x^3 - x^2 - 2x - 8$ is irreducible over $\mathbb{Q}$.
   (b) Consider $\beta = (\theta^2 + \theta)/2$. Show that β is an algebraic integer.
   (c) Show that $d_{K/\mathbb{Q}}(1, \theta, \beta) = -503$ and $d_{K/\mathbb{Q}}(\theta) = -4 \cdot 503$. Deduce that $1, \theta, \beta$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$.
   (d) Show that every integer x of K has an even discriminant.
   (e) Deduce that $\mathcal{O}_K$ is not of the form $\mathbb{Z}[\alpha]$.

(7) Let $m = p^a$ with p prime and let $K = \mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of 1.
   (a) Show that $(1 - \zeta_m)^{\phi(m)} = p\,\mathcal{O}_K$.
   (b) Show that
   $$d_{K/\mathbb{Q}}(\zeta_m) = \frac{(-1)^{\frac{\phi(m)}{2}} m^{\phi(m)}}{p^{\frac{m}{p}}}.$$
   (c) Show that $\{1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}\}$ is an integral basis for $\mathcal{O}_K$. Deduce that $d_K = d_{K/\mathbb{Q}}(\zeta_m)$.
   (d) Show that $\mathbb{Z}[\zeta_m + \zeta_m^{-1}]$ is the ring of integers of $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

(8) Suppose that K is a number field with r_1 real embeddings and $2r_2$ complex embeddings so that $r_1 + 2r_2 = [K : \mathbb{Q}]$. Show that d_K has sign $(-1)^{r_2}$.

(9) Show that only finitely many imaginary quadratic fields are Euclidean.

(10) Let K and L be algebraic number fields of degree m and n, respectively, over $\mathbb{Q}$. Let $d = \gcd(d_K, d_L)$.
   (a) Show that if $[KL : \mathbb{Q}] = mn$, then $d\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$.
   (b) Suppose $d = 1$. Show that $d_{KL} = d_K^n d_L^m$.
   (c) Let $K = \mathbb{Q}(\sqrt{2})$ and $L = \mathbb{Q}(\sqrt{-3})$. Find an integral basis for $\mathcal{O}_{KL}$.
   (d) Let ζ_m be a primitive m-th root of 1 and let $K = \mathbb{Q}(\zeta_m)$. Show that $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ and

$$d_K = \frac{(-1)^{\frac{\phi(m)}{2}} m^{\phi(m)}}{\prod_{p \mid m} p^{\frac{\phi(m)}{p-1}}}.$$

(11) Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let $a_1, a_2, \ldots, a_n \in \mathcal{O}_K$ be linearly independent over $\mathbb{Q}$ and set

$$\triangle = d_{K/\mathbb{Q}}(a_1, a_2, \ldots, a_n).$$

   (a) Show that if $\alpha \in \mathcal{O}_K$, then $\triangle\alpha \in \mathbb{Z}[a_1, \ldots, a_n]$.
   (b) For each $i \in \{1, \ldots, n\}$, choose the least natural number d_{ii} so that for some $d_{ij} \in \mathbb{Z}$, the number

$$w_i = \triangle^{-1} \sum_{j=1}^{i} d_{ij} a_j \in \mathcal{O}_K.$$

   Show that $w_1, \ldots, w_n$ is an integral basis of $\mathcal{O}_K$.
   (c) Show that there is an integral basis $w_1, \ldots, w_n$ of $\mathcal{O}_K$ such that for $j = 1, \ldots, n$, $a_j = c_{j1}w_1 + \cdots + c_{jj}w_j$ for some $c_{ij} \in \mathbb{Z}$.
   (d) If $\mathbb{Q} \subseteq K \subseteq L$ and K, L are algebraic number fields, show that $d_K \mid d_L$.

Chapter 5

Dedekind Domains

The notion of a Dedekind domain is the concept we need in order to establish the unique factorization of ideals as a product of prime ideals. We will also meet the fundamental idea of a Noetherian ring. It turns out that Dedekind domains can be studied in the wider context of Noetherian rings.

5.1. Characterizing Dedekind Domains

Let R be a commutative ring with identity. If $\mathfrak{p}$ is a prime ideal containing the product $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_r$ of r ideals of R, then $\mathfrak{a}_i \subseteq \mathfrak{p}$ for some i.

We know that a finite integral domain is a field. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Since every nonzero ideal in $\mathcal{O}_K$ has finite index in $\mathcal{O}_K$, we have that $\mathcal{O}_K/\mathfrak{p}$ is a finite field for every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Hence, every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Definition 5.1.1. For any field containing R, we say that $\alpha \in L$ is *integral over* R if α satisfies a monic polynomial equation $f(\alpha) = 0$ with $f(x) \in R[x]$. R is said to be *integrally closed* if every element in the quotient field of R which is integral over R, already lies in R

The following theorem and its proof were exactly the same as Theorem 3.3.2, with $\mathcal{O}_K$ replacing $\mathbb{Z}$.

Theorem 5.1.2. *Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. The following statements are equivalent:*

(1) $\alpha \in \mathcal{O}_K$

(2) $\mathcal{O}_K[\alpha]$ *is a finite generated $\mathcal{O}_K$-module.*

(3) *There exists a finitely generated $\mathcal{O}_K$-submodule $M \neq \{0\}$ of $\mathbb{C}$ such that $\alpha M \subseteq M$.*

By Theorem 5.1.2, we have the following important result.

Theorem 5.1.3. *Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is integrally closed.*

Definition 5.1.4. A ring is called *Noetherian* if every ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ of ideals terminates, *i.e.*, if there exists n such that $\mathfrak{a}_n = \mathfrak{a}_{n+k}$ for all $k \geq 0$.

Lemma 5.1.5. *For any commutative ring R with identity, the following are equivalent:*

(1) *R is Noetherian;*

(2) *every nonempty set of ideals contains a maximal element; and*

(3) *every ideal of R is finitely generated.*

If $\mathfrak{a} \subsetneq \mathfrak{b}$ are ideals of $\mathcal{O}_K$, then we have that $N(\mathfrak{a}) > N(\mathfrak{b})$. Since $N(\mathfrak{a})$ is a positive integer for every ideal $\mathfrak{a}$ in $\mathcal{O}_K$, this shows that $\mathcal{O}_K$ is Noetherian.

Thus, we have proved that:

(1) $\mathcal{O}_K$ is integrally closed;

(2) every nonzero prime ideal of $\mathcal{O}_K$ is maximal; and

(3) $\mathcal{O}_K$ is Noetherian.

A commutative integral domain which satisfies these three conditions is called a *Dedekind domain*. We have thus seen that $\mathcal{O}_K$ is a Dedekind domain.

5.2. Fractional Ideals and Unique Factorization

A *fractional ideal* $\mathcal{A}$ of $\mathcal{O}_K$ is an $\mathcal{O}_K$-module contained in K such that there exists $m \in \mathbb{Z}$ with $m\mathcal{A} \subseteq \mathcal{O}_K$. Of course, any ideal of $\mathcal{O}_K$ is a fractional ideal by taking $m = 1$.

It is easy tocheck that any fractional ideal is finitely generated as an $\mathcal{O}_K$-module and the sum and product of two fractional ideals are again fractional ideals.

To show that every ideal can be written as a product of prime ideals uniquely, we need the following lemmas.

Lemma 5.2.1. *Any proper ideal of $\mathcal{O}_K$ contains a product of nonzero prime ideals.*

Lemma 5.2.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. There exists $z \in K \setminus \mathcal{O}_K$, such that $z\mathfrak{p} \subseteq \mathcal{O}_K$.*

Let $\mathfrak{p}$ be a prime ideal. Define

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

Lemma 5.2.2 implies, in particular, that $\mathfrak{p}^{-1} \neq \mathcal{O}_K$.

Lemma 5.2.3. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}^{-1}$ is a fractional ideal and $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.*

Theorem 5.2.4. *Any ideal of $\mathcal{O}_K$ can be written as a product of prime ideals uniquely.*

For $\mathfrak{a}$ and $\mathfrak{b}$ ideals of $\mathcal{O}_K$, we say $\mathfrak{a}$ divides $\mathfrak{b}$ (denoted $\mathfrak{a} \mid \mathfrak{b}$), if $\mathfrak{a} \supseteq \mathfrak{b}$.

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, the ideal $\mathfrak{d}$ satisfying:

(1) $\mathfrak{d} \mid \mathfrak{a}$ and $\mathfrak{d} \mid \mathfrak{b}$; and

(2) if $\mathfrak{e} \mid \mathfrak{a}$ and $\mathfrak{e} \mid \mathfrak{b}$ then $\mathfrak{e} \mid \mathfrak{d}$

is called the *great common divisor* of $\mathfrak{a}$ and $\mathfrak{b}$ and denoted by $\gcd(\mathfrak{a}, \mathfrak{b})$.

Similarly, the ideal $\mathfrak{m}$ satisfying:

(1) $\mathfrak{a} \mid \mathfrak{m}$ and $\mathfrak{b} \mid \mathfrak{m}$; and

(2) if $\mathfrak{a} \mid \mathfrak{n}$ and $\mathfrak{b} \mid \mathfrak{n}$ then $\mathfrak{m} \mid \mathfrak{n}$

is called the *least common multiple* of $\mathfrak{a}$ and $\mathfrak{b}$ and denoted by $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b})$.

Theorem 5.2.5 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals so that $\gcd(\mathfrak{a}, \mathfrak{b}) = 1$. Given $a, b \in \mathcal{O}_K$, we can solve $x \equiv a \pmod{\mathfrak{a}}$ and $x \equiv b \pmod{\mathfrak{b}}$. Furthermore, let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ be r distinct prime ideals in $\mathcal{O}_K$. Given $a_i \in \mathcal{O}_K$, $e_i \in \mathbb{Z}^+$, there exist x such that $x \equiv a_i \pmod{\mathfrak{p}_i^{r_1}}$ for all $i = 1, \ldots, r$.*

Definition 5.2.6. Given a prime ideal $\mathfrak{p}$. We define the order of $\mathfrak{a}$ in $\mathfrak{p}$ by $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = t$ if $\mathfrak{p}^t \mid \mathfrak{a}$ and $\mathfrak{p}^{t+1} \nmid \mathfrak{a}$.

It easy to show that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{ab}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$, by unique factorization of ideals.

Proposition 5.2.7. *Let $\mathfrak{p}$, $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ be prime ideals in $\mathcal{O}_K$. We have that*

(1) *$\mathcal{O}_K/\mathfrak{p} \simeq \mathfrak{p}^{e-1}/\mathfrak{p}^e$ and $N(\mathfrak{p}^e) = (N(\mathfrak{p}))^e$, for every integer $e \geq 1$.*
(2) *If $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, then $N(a) = \prod_{i=1}^r N(\mathfrak{p}_i^{e_1})$.*