A PRIMER ON NUMBER FIELDS

HENRY TWISS

Abstract. Introductory analytic number theory is done over $\mathbb{Q}$. The associated set of integers $\mathbb{Z}$ is a ring inside $\mathbb{Q}$. Moreover, the fundamental theorem of arithmetic tells us that prime factorization exists in $\mathbb{Z}$. That is, every integer is uniquely a product of primes (up to reordering of the factors). The study of number fields is concerned with finite extensions of $\mathbb{Q}$ where there might no longer be prime factorization. In the following, we discuss the structure of number fields, their associated ring of integers, and the properties of prime factorization.

1. Numbers Fields & Algebraic Integers

A **number field** K is a finite extension of $\mathbb{Q}$. That is, K is a finite dimensional vector space over $\mathbb{Q}$. In particular, $K/\mathbb{Q}$ is a finite separable extension, so that the primitive element theorem applies, and is Galois if and only if $K/\mathbb{Q}$ is normal. We say that the **degree** of K is $[K : \mathbb{Q}]$ which is the dimension of this vector space. If K is of degree 2, 3, etc. then we say it is **quadratic**, **cubic**, etc. Any $\kappa \in K$ is called an **algebraic number**. Moreover, we say that κ is an **algebraic integer** if it is the root of a monic polynomial $f(x) \in \mathbb{Z}[x]$. If $K = \mathbb{Q}$, it is clear that any integer is an algebraic integer (n is the root of $x - n$.). Moreover, any rational root of a monic polynomial must be an integer by the rational root theorem. In other words, if $f(x) \in \mathbb{Z}[x]$ is monic and $q \in \mathbb{Q}$ is a root of $f(x)$ then $q \in \mathbb{Z}$. Therefore for the number field $\mathbb{Q}$, the algebraic integers are exactly the integers $\mathbb{Z}$. Our first goal in studying number fields is to discuss the algebraic integers. Accordingly, we define the **ring of integers** $\mathcal{O}_K$ of K by

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

From what we have just shown above, $\mathbb{Z} \subseteq \mathcal{O}_K$. For a general number field K, $\mathcal{O}_K$ can be strictly larger than $\mathbb{Z}$. The ring of integers $\mathcal{O}_K$ is the analog of $\mathbb{Z}$ in $\mathbb{Q}$ but for K. Our primarily goals will be to show that $\mathcal{O}_K$ is a ring and more precisely a free abelian group of rank equal to the degree of K. The following proposition shows that $\mathcal{O}_K$ is indeed a ring:

Proposition 1.1. *Let K be a number field. Then the finitely many elements $\kappa_1, \ldots, \kappa_n \in B$ are all algebraic integers if and only if $\mathbb{Z}[\kappa_1, \ldots, \kappa_n]$ is a finitely generated $\mathbb{Z}$-module. In particular, $\mathcal{O}_K$ is a ring.*

Proof. First suppose $\kappa \in K$ is an algebraic integer. Then there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$, of say degree $n \geq 1$, such that $f(\kappa) = 0$. Now for any $g(x) \in \mathbb{Z}[x]$, Euclidean division implies

$$g(x) = q(x)f(x) + r(x),$$

with $q(x), r(x) \in \mathbb{Z}[x]$ and $\deg(r(x)) < n$. Letting $r(x) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $a_i \in \mathbb{Z}$ for $0 \leq i \leq n-1$, it follows that

$$g(\kappa) = r(\kappa) = a_{n-1}\kappa^{n-1} + \cdots + a_1\kappa + a_0.$$

As $g(x)$ was arbitrary, we see that $\{1, \kappa, \ldots, \kappa^{n-1}\}$ is a generating set for $\mathbb{Z}[\kappa]$ as a $\mathbb{Z}$-module. Now suppose $\kappa_1, \ldots, \kappa_n \in K$ are all algebraic integers. We will prove that $\mathbb{Z}[\kappa_1, \ldots, \kappa_n]$ is finitely generated as an $\mathbb{Z}$-module by induction. Our previous work implies the base case. So assume by induction that $R = \mathbb{Z}[\kappa_1, \ldots, \kappa_{n-1}]$ is a finitely generated $\mathbb{Z}$-module. Then $R[\kappa_n] = A[\kappa_1, \ldots, \kappa_n]$ is a finitely generated R-module and hence a finitely generated $\mathbb{Z}$-module as well by our induction hypothesis. Now suppose

Date: 2024.

$A[\kappa_1, \ldots, \kappa_n]$ is a finitely generated $\mathbb{Z}$-module. Let $\{\omega_1, \ldots, \omega_r\}$ be a basis for $A[\kappa_1, \ldots, \kappa_n]$. Then for any $\kappa \in A[\kappa_1, \ldots, \kappa_n]$, we have

$$\kappa\omega_i = \sum_{1 \le j \le r} a_{i,j}\omega_j,$$

with $a_{i,j} \in \mathbb{Z}$ for $1 \le i, j \le r$.We can rewrite this as,

$$(\kappa - a_{i,i})\omega_i - \sum_{\substack{1 \le j \le r \\ j \ne i}} a_{i,j}\omega_j = 0,$$

for all i. These r equations are equivalent to the identity

$$\begin{pmatrix} k - a_{1,1} & a_{1,2} & \cdots & -a_{1,r} \\ -a_{2,1} & \kappa - a_{2,2} & & \\ \vdots & & \ddots & \\ -a_{r,1} & & & \kappa - a_{r,r} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_r \end{pmatrix} = \mathbf{0}.$$

Thus the determinant of the matrix on the left-hand side must be zero. This shows that κ is the root of the characteristic polynomial $\det(xI - (a_{i,j}))$ which is a monic polynomial with coefficients in $\mathbb{Z}$. Hence κ is an algebraic integer. As κ was arbitrary, this shows that the elements $\kappa_1, \ldots, \kappa_n$ are all algebraic integers and that the sum and product of algebraic integers are algebraic integers. It follows that $\mathcal{O}_K$ is a ring. □

We can also show that K is the field of fractions of $\mathcal{O}_K$. Actually, the following proposition proves this and more:

Proposition 1.2. *Let K be a number field. Then every $\kappa \in K$ is of the form*

$$\kappa = \frac{\alpha}{a},$$

for some $\alpha \in \mathcal{O}_K$ and nonzero $a \in \mathbb{Z}$. In particular, K is the field of fractions of $\mathcal{O}_K$. Moreover, $\kappa \in K$ is an algebraic integer if and only if the minimal polynomial of κ has coefficients in $\mathbb{Z}$.

Proof. As $K/\mathbb{Q}$ is finite, it is necessarily algebraic so that any $\kappa \in K$ satisfies

$$a\kappa^n + a_{n-1}\kappa^{n-1} + \cdots + a_0 = 0,$$

with $a_i \in \mathbb{Z}$ for $0 \le i \le n-1$ and $a \ne 0$. We claim that $a\kappa$ is an algebraic integer. Indeed, multiplying the previous identity by a^{n-1} yields

$$(a\kappa)^n + a'_{n-1}(a\kappa)^{n-1} + \cdots + a'_0 = 0,$$

where $a'_i = a_i a^{n-1-i}$ for $0 \le i \le n-1$, and so $a\kappa$ is the root of a monic polynomial with coefficients in $\mathbb{Z}$. Then $a\kappa \in \mathcal{O}_K$ and so $a\kappa = \alpha$ for some $\alpha \in \mathcal{O}_K$ which is equivalent to $\kappa = \frac{\alpha}{a}$. As $\mathbb{Z} \subseteq \mathcal{O}_K$, this also implies that K is the field of fractions of $\mathcal{O}_K$. For the last statement, suppose $\kappa \in K$. If the minimal polynomial of κ has integer coefficients then κ is automatically an algebraic integer (since the minimal polynomial is monic). So suppose κ is an algebraic integer so that κ is a root of a monic polynomial $f(x) \in \mathbb{Z}[x]$. If $m_\kappa(x) \in \mathbb{Q}[x]$ is the minimal polynomial of κ, then $m_\kappa(x)$ divides $f(x)$ and thus all of the roots of $m_\kappa(x)$ algebraic integers too. By Vieta's formulas, the coefficients of $m_\kappa(x)$ algebraic integers as well. But then $m_\kappa(x) \in \mathbb{Z}[x]$. This completes the proof. □

2. Traces & Norms

We will now require norms and traces of free algebras over fields. Let K be a field and let R be a free K-algebra of rank n. Then the **trace** and **norm** of R, denoted $\mathrm{Tr}_{R/K}$ and $\mathrm{N}_{R/K}$ respectively, are defined by

$$\mathrm{Tr}_{R/K}(\rho) = \mathrm{trace}(T_\rho) \quad \text{and} \quad \mathrm{N}_{R/K}(\rho) = \det(T_\rho),$$

for any $\rho \in R$, where $T_\rho : R \to R$ is the linear operator defined by

$$T_\rho(x) = \rho x,$$

for all $x \in R$. That is, T_ρ is the multiplication by ρ map. Letting $f_\rho(t)$ denote the characteristic polynomial of T_ρ, we have

$$f_\rho(t) = \det(tI - T_\rho) = t^n - \kappa_{n-1}t^{n-1} + \cdots + (-1)^n\kappa_0,$$

with $\kappa_i \in K$ for $0 \leq i \leq n-1$. Then the trace and the norm are given by

$$\mathrm{Tr}_{R/K}(\rho) = \kappa_{n-1} \quad \text{and} \quad \mathrm{N}_{R/K}(\rho) = \kappa_0, \tag{1}$$

and therefore take values in K. Moreover, we have

$$\mathrm{Tr}_{R/K}(\kappa\rho) = \kappa\,\mathrm{Tr}_{R/K}(\rho) \quad \text{and} \quad \mathrm{N}_{R/K}(\kappa\rho) = \kappa^m\,\mathrm{N}_{R/K}(\rho),$$

for all $\kappa \in K$ because $T_{\kappa\lambda} = \kappa T_\lambda$. As $T_{\lambda+\nu} = T_\lambda + T_\nu$ and $T_{\lambda\nu} = T_\lambda T_\nu$, we obtain homomorphisms

$$\mathrm{Tr}_{R/K} : R \to K \quad \text{and} \quad \mathrm{N}_{R/K} : R \to K.$$

In the case of a degree n extension L/K, we call $\mathrm{Tr}_{L/K}$ and $\mathrm{N}_{L/K}$ the **trace** and **norm** of L/K. Moreover, $\mathrm{N}(\lambda) = 0$ if and only if $\lambda = 0$ because otherwise T_λ has inverse $T_{\lambda^{-1}}$ and hence nonzero determinant. Therefore we obtain homomorphisms

$$\mathrm{Tr}_{L/K} : L \to K \quad \text{and} \quad \mathrm{N}_{L/K} : L^* \to K^*.$$

In the specialized setting $K/\mathbb{Q}$ for a number field K, we write $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}}$ and $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$. Moreover, for any $\kappa \in K$ we call $\mathrm{Tr}(\kappa)$ and $\mathrm{N}(\kappa)$ the **trace** and **norm** of κ respectively. More generally, when L/K is separable, we can derive alternative descriptions of the trace and norm of L/K. This additional assumption is weak because the only situations we will be interested in are finite extensions of $\mathbb{Q}$ and $\mathbb{F}_p$ which are always separable (because both $\mathbb{Q}$ and $\mathbb{F}_p$ are perfect). In any case, to do this we need to work in the algebraic closure $\overline{K}$ of K. As L/K is a degree n separable extension, there are exactly n distinct K-embeddings $\sigma_1, \ldots, \sigma_n$ of L into $\overline{K}$ (each given by letting θ be a primitive element for L so that $L = K[\theta]$ and sending θ to one of its conjugate roots in the minimal polynomial $m_\theta(x)$ of θ). Clearly $\sigma_1, \ldots, \sigma_n$ send $\mathcal{O}_K$ to itself and fix $\mathcal{O}_K$ pointwise. Moreover, we prove the following proposition:

Proposition 2.1. *Let L/K be a degree n separable extension and let $\sigma_1, \ldots, \sigma_n$ denote the K-embeddings of L in $\overline{K}$. For any $\lambda \in L$, the characteristic polynomial $f_\lambda(t)$ of T_λ is a power of the minimal polynomial of λ and satisfies*

$$f_\lambda(t) = \prod_{1 \leq i \leq n} (t - \sigma_i(\lambda)).$$

In particular,

$$\mathrm{Tr}_{L/K}(\lambda) = \sum_{1 \leq i \leq n} \sigma_i(\lambda) \quad \textit{and} \quad \mathrm{N}_{L/K}(\lambda) = \prod_{1 \leq i \leq n} \sigma_i(\lambda).$$

Proof. Let

$$m_\lambda(t) = t^m + \kappa_{m-1}t^{m-1} + \cdots + \kappa_0,$$

with $\kappa_i \in K$ for $0 \leq i \leq n-1$, be the minimal polynomial of λ (necessarily m is the degree of $K(\lambda)/K$). Let d be the degree of $L/K(\lambda)$. We first show that $f_\lambda(t)$ is a power of $m_\lambda(t)$. Precisely, we claim that

$$f_\lambda(t) = m_\lambda(t)^d.$$

To see this, recall that $\{1, \lambda, \ldots, \lambda^{n-1}\}$ is a basis for $K(\lambda)/K$. If $\{\alpha_1, \ldots, \alpha_d\}$ is a basis for $L/K(\lambda)$, then

$$\{\alpha_1, \alpha_1\lambda, \ldots, \alpha_1\lambda^{m-1}, \ldots, \alpha_d, \alpha_d\lambda, \ldots, \alpha_d\lambda^{m-1}\},$$

is a basis for L/K. Because the minimal polynomial $m_\lambda(t)$ gives the linear relation

$$\lambda^m = -\kappa_0 - k_1\lambda - \cdots - \kappa_{m-1}\lambda^{m-1},$$

the matrix of T_λ is block diagonal with d blocks each of the form

$$\begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -\kappa_0 & -\kappa_1 & \cdots & -\kappa_{m-1} \end{pmatrix}.$$

This is the companion matrix to $m_\lambda(t)$ and hence the characteristic polynomial is $m_\lambda(t)$ as well. Our claim follows since the matrix of T_λ is block diagonal. Since λ is algebraic over K of degree m, $K(\lambda)$ is the splitting field of $m_\lambda(t)$ and there are m distinct K-embeddings of $K(\lambda)$ into $\overline{L}$. Denote these m embeddings by $\tau_1, \ldots, \tau_m$. Then the embeddings $\sigma_1, \ldots, \sigma_n$ are partitioned into m many equivalence classes each of size d (because $L/K(\lambda)$ is degree d) where σ_i and σ_j are in the same class if and only if $\sigma_i(\lambda) = \sigma_j(\lambda)$. In particular, a complete set of representatives is $\{\tau_1, \ldots, \tau_m\}$. But then

$$f_\lambda(t) = m_\lambda(t)^d = \left(\prod_{1 \le i \le m} (t - \tau_i(\lambda)) \right)^d = \prod_{1 \le i \le n} (t - \sigma_i(\lambda)).$$

This proves the first statement. The formulas for the trace and norm follow from Vieta's formulas and Equation (1). □

As a corollary of Proposition 2.1, we can show how the trace and norm act on algebraic integers for the extension $K/\mathbb{Q}$:

Corollary 2.1. *Let K be a number field. If $\kappa \in K$ is an algebraic integer, then the trace and norm of κ are integers.*

Proof. By Proposition 1.2, if κ is an algebraic integer then its minimal polynomial $m_\kappa(t)$ has integer coefficients. By Proposition 2.1 the characteristic polynomial $f_\kappa(t)$ is a power of $m_\kappa(t)$. Hence $f_\kappa(t)$ has integer coefficients. From Equation (1) we conclude that the trace and norm of κ are integers. □

We can also classify the units in $\mathcal{O}_K$ according to their norm:

Corollary 2.2. *Let K be a number field. Then $\alpha \in \mathcal{O}_K$ is a unit if and only if its norm is ± 1.*

Proof. Let $\alpha \in \mathcal{O}_K$. First suppose α is a unit in $\mathcal{O}_K$. Then $\frac{1}{\alpha} \in \mathcal{O}_K$ and so

$$\mathrm{N}(\alpha)\,\mathrm{N}\left(\frac{1}{\alpha}\right) = \mathrm{N}(1) = 1.$$

By Corollary 2.1, the norm of α and $\frac{1}{\alpha}$ are both integers. Hence they must be ± 1 and thus the norm of α is ± 1. Now suppose the norm of α is ± 1. By Proposition 1.2, its minimal polynomial $m_\alpha(t)$ has integer coefficients. Moreover, Equation (1) and Proposition 2.1 together imply that the constant term is ± 1. Letting the degree of $m_\alpha(t)$ be m, we have shown that

$$m_\alpha(t) = t^m + a_{m-1}t^{m-1} + \cdots \pm 1,$$

with $a_i \in \mathbb{Z}$ for $1 \le i \le m-1$. Dividing $m_\alpha(\alpha)$ by α^m, we find that $\frac{1}{\alpha}$ is a root of the polynomial

$$f(x) = \pm t^m + a_1 t^{m-1} + \cdots + 1.$$

Multiplying by -1 if necessary, it follows that $\frac{1}{\alpha}$ is a root of a monic polynomial with coefficients in $\mathbb{Z}$. Hence $\frac{1}{\alpha} \in \mathcal{O}_K$ and thus α is a unit in $\mathcal{O}_K$. □

We can now prove a structure theorem for the ring of integers $\mathcal{O}_K$ of a number field K. We show that the ring of integers is a free abelian group with rank equal to the degree of K which clearly is a generalization of the structure of $\mathbb{Z}$ for for the number field $\mathbb{Q}$:

Theorem 2.1. *Let K be a number field of degree n. Then $\mathcal{O}_K$ is a free abelian group of rank n. In particular, $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module.*

Proof. Let $\{\kappa_1, \ldots, \kappa_n\}$ be a basis for K. By Proposition 1.2, we have $\kappa_i = \frac{\alpha_i}{a_i}$ with $\alpha_i \in \mathcal{O}_K$ and $a_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Hence $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K as well. In particular, any element $\alpha \in \mathcal{O}_K$ can be expressed as

$$\alpha = \sum_{1 \leq i \leq n} q_i(\alpha)\alpha_i,$$

with $q_i(\alpha) \in \mathbb{Q}$. We now show that the denominators of the $q_i(\alpha)$ are uniformly bounded for all $1 \leq i \leq n$ and all α. Assume this is not the case. Then there is a sequence $(\beta_j)_{j \geq 1}$ of nonzero elements in $\mathcal{O}_K$ where

$$\beta_j = \sum_{1 \leq i \leq n} q_i(\beta_j)\alpha_i,$$

is such that the greatest denominator of $q_i(\beta_j)$ for $1 \leq i \leq n$ tends to infinity as $j \to \infty$. In terms of the basis $\{\alpha_1, \ldots, \alpha_n\}$, $\mathrm{N}(\beta_j)$ is the determinant of an $n \times n$ matrix with coefficients in $\mathbb{Q}[q_i(\beta_j)]_{1 \leq i \leq n}$. In particular, it is a homogenous polynomial of degree n in the $q_i(\beta_j)$ for $1 \leq i \leq n$ with coefficients in $\mathbb{Q}$ determined by the basis $\{\alpha_1, \ldots, \alpha_n\}$. But $\mathrm{N}(\beta_j)$ is an integer by Corollary 2.1. It is also nonzero because β_j is nonzero. Hence $|\mathrm{N}(\beta_j)| \geq 1$ and thus, by what we have just shown, the greatest denominator of $q_i(\beta_j)$ for $1 \leq i \leq n$ must be bounded as $j \to \infty$. This gives a contradiction. Hence there is an integer $M \geq 1$ such that $Mq_i(\alpha) \in \mathbb{Z}$ for all $1 \leq i \leq n$ and $\alpha \in \mathcal{O}_K$. Therefore

$$\mathcal{O}_K \subseteq \frac{1}{M} \bigoplus_{1 \leq i \leq n} \mathbb{Z}\alpha_i.$$

As the group on the right-hand side is a free abelian group so is $\mathcal{O}_K$. Moreover, as $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K we see that $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent over $\mathbb{Z}$ as well. This means that the rank of $\mathcal{O}_K$ must be n. The last statement is now clear. □

In accordance with Theorem 2.1, we say that $\{\alpha_1, \ldots, \alpha_n\}$ is an **integral basis** for K if $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K and $\mathcal{O}_K$ can be expressed as

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

That is, every $\alpha \in \mathcal{O}_K$ is a unique integer linear combination of the α_i. An integral basis for K always exists by Theorem 2.1. In the special case $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, we say K is **monogenic**. By Theorem 2.1, we see that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is an integral basis for K. Lastly, we can show that algebraic integers satisfy a slightly weaker condition:

Proposition 2.2. *Let K be a number field. Then $\kappa \in K$ is an algebraic integer if and only if κ is the root of a monic polynomial with coefficients in $\mathcal{O}_K$.*

Proof. If $\kappa \in K$ is an algebraic integer, then κ is the root of a monic polynomial with coefficients in $\mathbb{Z}$ and hence in $\mathcal{O}_K$ as well. So suppose $\kappa \in K$ is the root of a monic polynomial $f(x) \in \mathcal{O}_K$. Let $f(x)$ have degree n and write

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0,$$

with $\alpha_i \in \mathcal{O}_K$ for $0 \leq i \leq n-1$. As $f(\kappa) = 0$, we have

$$\kappa^n = -\alpha_{n-1}\kappa^{n-1} - \cdots - \alpha_0,$$

and hence $\mathcal{O}_K[\kappa]$ is a finitely generated $\mathbb{Z}$-module because $\mathcal{O}_K$ is by Theorem 2.1. As $\mathbb{Z}[\kappa] \subseteq \mathcal{O}_K[\kappa]$, we see that $\mathbb{Z}[\kappa]$ must also be a finitely generated $\mathbb{Z}$-module. Hence κ is an algebraic integer by Proposition 1.1. □

3. Discriminants

We will now discuss discriminants of free modules over fields. Let K be a field and R be a free K-algebra of rank n. If $\{\rho_1, \dots, \rho_n\}$ is a basis for R, we set

$$\operatorname{disc}_{R/K}(\rho_1, \dots, \rho_n) = \det((\operatorname{Tr}_{R/K}(\rho_i \rho_j))_{i,j}).$$

In particular, $\operatorname{disc}_{R/K}(\rho_1, \dots, \rho_n)$ is an element of K. It is also independent of the choice of basis up to elements of $(K^*)^2$. Indeed, if $\{\rho'_1, \dots, \rho'_n\}$ is another basis then we have

$$\rho'_i = \sum_{1 \le j \le m} \kappa_{i,j} \rho_j,$$

with $\kappa_{i,j} \in K$ for $1 \le i, j \le n$. Then $(\kappa_{i,j})_{i,j}$ is the base change matrix from $\{\rho_1, \dots, \rho_n\}$ to $\{\rho'_1, \dots, \rho'_n\}$ and so it has nonzero determinant. Thus $\det((\kappa_{i,j})_{i,j}) \in K^*$. Moreover, we have

$$(\operatorname{Tr}_{R/K}(\rho'_i \rho'_j))_{i,j} = (\kappa_{i,j})_{i,j} (\operatorname{Tr}_{R/K}(\rho_i \rho_j))_{i,j} (\kappa_{i,j})^t_{i,j},$$

which, upon taking the determinant, shows that

$$\operatorname{disc}_{R/K}(\rho'_1, \dots, \rho'_n) = \det((\kappa_{i,j})_{i,j})^2 \operatorname{disc}_{R/K}(\rho_1, \dots, \rho_n), \tag{2}$$

as claimed. We define the **discriminant** $\operatorname{disc}_K(R)$ of R by

$$\operatorname{disc}_K(R) = \operatorname{disc}_{R/K}(\rho_1, \dots, \rho_n) \pmod{(K^*)^2}.$$

for any basis $\{\rho_1, \dots, \rho_n\}$ of R. By what we have shown, $\operatorname{disc}_K(R)$ is well-defined. The discriminant is also multiplicative with respect to direct sums:

Proposition 3.1. *Let K be a field and R be a free K-algebra of rank n. Suppose we have a direct sum decomposition*

$$R = R_1 \oplus R_2,$$

for free K-algebras R_1 and R_2 of ranks n_1 and n_2 respectively. Also let $\{\eta_1, \dots, \eta_{n_1}\}$ and $\{\gamma_1, \dots, \gamma_{n_2}\}$ be bases of R_1 and R_2 respectively. Then

$$\operatorname{disc}_{R/K}(\eta_1, \dots, \eta_{n_1}, \gamma_1, \dots, \gamma_{n_2}) = \operatorname{disc}_{R/K}(\eta_1, \dots, \eta_{n_1}) \operatorname{disc}_R(\gamma_1, \dots, \gamma_{n_2}).$$

In particular,

$$\operatorname{disc}_K(R) = \operatorname{disc}_K(R_1) \operatorname{disc}_K(R_2).$$

Proof. The second statement follows immediately from the first. To prove the first statement, write

$$\operatorname{disc}_{R/K}(\eta_1, \dots, \eta_{n_1}) = \det((\operatorname{Tr}_{R/K}(\eta_i \eta_j))_{i,j}) \quad \text{and} \quad \operatorname{disc}_R(\gamma_1, \dots, \gamma_{n_2}) = \det((\operatorname{Tr}_{R/K}(\gamma_k \gamma_\ell))_{k,\ell}).$$

As R is the direct sum of R_1 and R_2 as K-modules, we have $\eta_i \gamma_k = 0$ for all $1 \le i \le n_1$ and $1 \le k \le n_2$. It follows that $\operatorname{disc}_{R/K}(\eta_1, \dots, \eta_{n_1}, \gamma_1, \dots, \gamma_{n_2})$ is the determinant of the block diagonal matrix

$$\begin{pmatrix} (\operatorname{Tr}_{R/K}(\eta_i \eta_j))_{i,j} & \\ & (\operatorname{Tr}_{R/K}(\gamma_k \gamma_\ell))_{k,\ell} \end{pmatrix}.$$

Moreover, we have

$$\operatorname{Tr}_{R/K}(\rho_1) = \operatorname{Tr}_{R_1/K}(\rho_1) \quad \text{and} \quad \operatorname{Tr}_{R/K}(\rho_2) = \operatorname{Tr}_{R_2/K}(\rho_2)$$

for any $\rho_1 \in R_1$ and $\rho_2 \in R_2$. Indeed, multiplication by ρ_1 and ρ_2 annihilate R_2 and R_1 respectively. But then

$$\begin{pmatrix} (\operatorname{Tr}_{R/K}(\eta_i \eta_j))_{i,j} & \\ & (\operatorname{Tr}_{R/K}(\gamma_k \gamma_\ell))_{k,\ell} \end{pmatrix} = \begin{pmatrix} (\operatorname{Tr}_{R_1/K}(\eta_i \eta_j))_{i,j} & \\ & (\operatorname{Tr}_{R_2/K}(\gamma_k \gamma_\ell))_{k,\ell} \end{pmatrix}.$$

The determinant of the matrix on right-hand side is $\operatorname{disc}_{R/K}(\eta_1, \dots, \eta_{n_1}) \operatorname{disc}_R(\gamma_1, \dots, \gamma_{n_2})$. This completes the proof. □

We now specialize to the setting of a degree n separable extension L/K. It turns out that the discriminant is nonzero. To see this, we require a lemma:

Lemma 3.1. *Let L/K be a finite separable extension. Then the map*

$$L \times L \to K \qquad (\lambda, \eta) \to \mathrm{Tr}_{L/K}(\lambda\eta),$$

is a nondegenerate symmetric bilinear form.

Proof. From the definition of the trace, it is clear that the map is a symmetric bilinear form. To see that is is nondegenerate, suppose L/K is degree n. Then for any nonzero $\lambda \in L$, Proposition 2.1 implies that

$$\mathrm{Tr}_{L/K}(\lambda\lambda^{-1}) = \mathrm{Tr}_{L/K}(1) = n.$$

Hence the symmetric bilinear form is nondegenerate. □

We can now show that the discriminant is never zero:

Proposition 3.2. *Let L/K be a degree n separable extension and let $\{\lambda_1, \ldots, \lambda_n\}$ be a basis for L. Then we have that $\mathrm{disc}_K(\lambda_1, \ldots, \lambda_n) \neq 0$. In particular, $\mathrm{disc}_K(L) \neq 0$.*

Proof. The second statement follows immediately from the first. To prove the first statement, suppose to the contrary that $\mathrm{disc}_K(\lambda_1, \ldots, \lambda_n) = 0$. Then the matrix $(\mathrm{Tr}_{L/K}(\lambda_i\lambda_j))_{i,j}$ is not invertible. Hence there exists a nonzero column vector $(\kappa_1, \ldots, \kappa_n)^t$ with $\kappa_i \in K$ for $1 \leq i \leq n$ such that

$$(\mathrm{Tr}_{L/K}(\lambda_i\lambda_j))_{i,j}(\kappa_1, \ldots, \kappa_n)^t = \mathbf{0}.$$

This is equivalent to the n equations

$$\sum_{1 \leq j \leq n} \kappa_j \,\mathrm{Tr}_{L/K}(\lambda_i\lambda_j) = 0,$$

for all i. Setting

$$\lambda = \sum_{1 \leq j \leq n} \kappa_j\lambda_j,$$

linearity of the trace implies that these n equations are equivalent to the fact that $\mathrm{Tr}_{L/K}(\lambda\lambda_i) = 0$ for all i. As $\{\lambda_1, \ldots, \lambda_n\}$ is a basis for L, it follows that $\lambda \in L$ is a nonzero element for which $\mathrm{Tr}_{L/K}(\lambda\eta) = 0$ for all $\eta \in L$. This is impossible by Lemma 3.1. Hence $\mathrm{disc}_K(\lambda_1, \ldots, \lambda_n) \neq 0$. □

In addition to $\mathrm{disc}_K(\lambda_1, \ldots, \lambda_n)$ never vanishing, we can also write it in an alternative form. To do this, for any basis $\{\lambda_1, \ldots, \lambda_n\}$ of L we define the associated **embedding matrix** $M(\lambda_1, \ldots, \lambda_n)$ by

$$M(\lambda_1, \ldots, \lambda_n) = (\sigma_i(\lambda_j))_{i,j}.$$

Then we have the following result:

Proposition 3.3. *Let L/K be a degree n separable extension. Then for any basis $\{\lambda_1, \ldots, \lambda_n\}$ of L, we have*

$$\mathrm{disc}_K(\lambda_1, \ldots, \lambda_n) = \det(M(\lambda_1, \ldots, \lambda_n))^2.$$

Proof. Recalling that the (i, j)-entry of $M(\lambda_1, \ldots, \lambda_n)^t M(\lambda_1, \ldots, \lambda_n)$ is the dot product of the i-th and j-th columns of $M(\lambda_1, \ldots, \lambda_n)$, we have

$$\begin{aligned}
\det(M(\lambda_1, \ldots, \lambda_n))^2 &= \det(M(\lambda_1, \ldots, \lambda_n)^t M(\lambda 1, \ldots, \lambda_n)) \\
&= \det\left(\left(\sum_{1 \leq k \leq n} \sigma_k(\lambda_i)\sigma_k(\lambda_j)\right)_{i,j}\right) \\
&= \det\left(\left(\sum_{1 \leq k \leq n} \sigma_k(\lambda_i\lambda_j)\right)_{i,j}\right) \\
&= \det((\mathrm{Tr}_{L/K}(\lambda_i\lambda_j))_{i,j}) \\
&= \mathrm{disc}_{L/K}(\lambda_1, \ldots, \lambda_n),
\end{aligned}$$

where the second to last equality follows by Proposition 2.1, as desired. □

In the specialized case $K/\mathbb{Q}$ for a number field K, we define the **discriminant** Δ_K of K by

$$\Delta_K = \operatorname{disc}_K(\alpha_1, \ldots, \alpha_n),$$

for any integral basis $\{\alpha_1, \ldots, \alpha_n\}$. As Δ_K is not defined modulo $(K^*)^2$, we need to show that Δ_K is independent of the choice of integral basis and hence well-defined. Indeed, if $\{\alpha_1', \ldots, \alpha_n'\}$ is another integral basis then the base change matrix, as well as its inverse, both have integer entries (because integral bases are bases for $\mathcal{O}_K$ as a $\mathbb{Z}$-module). This implies that the determinant of the base change matrix is ± 1 and so Equation (2) shows that Δ_K is independent of the choice of integral basis. Moreover, Δ_K is nonzero by Proposition 3.2 and

$$\Delta_K = \det(M(\alpha_1, \ldots, \alpha_n))^2,$$

by Proposition 3.3.

4. Integral & Fractional Ideals

For the number field $\mathbb{Q}$, its ring of integers $\mathbb{Z}$ is a unique factorization domain. Indeed, this is just a restatement of the fundamental theorem of arithmetic. Unfortunately, for a general number field K its ring of integers $\mathcal{O}_K$ need not be a unique factorization domain. However, the integral ideals of $\mathcal{O}_K$ do factor into a unique product of prime integral ideals (this is trivial for a unique factorization domain). Our main goal is to prove this. We first introduce some notation. Any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is said to be an **integral ideal** of K. As $\mathcal{O}_K$ is a free abelian group of rank n by Theorem 2.1 and $\alpha\mathcal{O}_K \subseteq \mathfrak{a}$ for any nonzero $\alpha \in \mathfrak{a}$, we see that $\mathfrak{a}$ is also a free abelian group of rank n as well. We first show that the quotient ring by an integral ideal is finite:

Proposition 4.1. *Let K be a number field. Then $\mathcal{O}_K/\mathfrak{a}$ is finite for any integral ideal $\mathfrak{a}$ and*

$$|\mathcal{O}_K/\mathfrak{a}| = |\det(A)|,$$

where A is any base change matrix from a basis of $\mathcal{O}_K$ to a basis of $\mathfrak{a}$. In particular, for any $\alpha \in \mathcal{O}_K$,

$$|\mathcal{O}_K/\alpha\mathcal{O}_K| = |\operatorname{N}(\alpha)|.$$

Proof. Let the degree of K be n and $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K. Since $\mathfrak{a}$ is a a free abelian group of rank n, there exists a basis $\{\kappa_1, \ldots, \kappa_n\}$. Now write

$$\kappa_i = \sum_{1 \leq j \leq n} a_{i,j}\alpha_j,$$

with $a_{i,j} \in \mathbb{Z}$ for $1 \leq i, j \leq n$. Then $A = (a_{i,j})_{i,j}$ is the base change matrix from $\{\alpha_1, \ldots, \alpha_n\}$ to $\{\kappa_1, \ldots, \kappa_n\}$. Putting A in Smith normal form and letting D be the associated diagonal matrix, we see that there exist bases of $\mathcal{O}_K$ and $\mathfrak{a}$ such that the base change matrix is D and $|\det(A)| = |\det(D)|$ (because A has integer entries and hence the invertible matrices in the Smith normal form have determinant ± 1). Letting $a_1, \ldots, a_n$ be the invariant factors, this shows that

$$\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_n\mathbb{Z}.$$

Thus $|\mathcal{O}_K/\alpha\mathcal{O}_K| = |a_1 \cdots a_n| = |\det(D)| = |\det(A)|$ is finite. This proves the first statement. For the second statement, letting

$$\alpha = \sum_{1 \leq i \leq n} a_i\alpha_i,$$

with $a_i \in \mathbb{Z}$, we see that $\{a_1\alpha_1, \ldots, a_n\alpha_n\}$ is a basis for $\alpha\mathcal{O}_K$. Then on the one hand, what we have just proved shows that $|\mathcal{O}_K/\alpha\mathcal{O}_K| = |a_1 \cdots a_n|$. On the other hand, in terms of the basis $\{a_1\alpha_1, \ldots, a_n\alpha_n\}$ we

have

$$T_\alpha = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},$$

and so $\mathrm{N}(\alpha) = a_1 \cdots a_n$. Hence

$$|\mathcal{O}_K/\alpha\mathcal{O}_K| = |\,\mathrm{N}(\alpha)|,$$

as desired. □

For an integral ideal $\mathfrak{a}$, we define its **norm** $\mathrm{N}(\mathfrak{a})$ by

$$\mathrm{N}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

By Proposition 4.1, the norm is finite, necessarily a positive integer, and for every $\alpha \in \mathcal{O}_K$ we have

$$\mathrm{N}(\alpha\mathcal{O}_K) = |\,\mathrm{N}(\alpha)|.$$

We can now show that every prime integral ideal is maximal:

Proposition 4.2. *Let K be a number field. Every prime integral ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is maximal.*

Proof. Recall that an ideal is maximal if and only if the quotient ring is a field. Therefore it suffices to show that $\mathcal{O}_K/\mathfrak{p}$ is a field. Let $\alpha \in \mathcal{O}_K/\mathfrak{p}$ be nonzero. We will show that α is invertible in $\mathcal{O}_K/\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. Therefore the multiplication map

$$\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p} \qquad x \mapsto \alpha x,$$

is injective. By Proposition 4.1, $\mathcal{O}_K/\mathfrak{p}$ is finite and therefore this map must be a bijection. But this means that α has an inverse in $\mathcal{O}_K/\mathfrak{p}$. Hence $\mathcal{O}_K/\mathfrak{p}$ is a field. □

As prime integral ideals are maximal by Proposition 4.2 and distinct maximal ideals are relatively prime, we see that distinct prime integral ideals $\mathfrak{p}$ and $\mathfrak{q}$ are relatively prime. In particular, their powers are relatively prime as well (which follows by induction). We will now being working to show that every integral ideal factors uniquely into a product of prime integral ideals. First we show containment in one direction:

Lemma 4.1. *Let K be a number field. For every integral ideal $\mathfrak{a}$, there exist prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that*

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{a}.$$

Proof. Let $\mathcal{S}$ be the set of integral ideals which do not contain a product of prime integral. Then it suffices to show $\mathcal{S}$ is empty. Assume otherwise so that there is an integral ideal $\mathfrak{a} \in \mathcal{S}$. Then $\mathfrak{a}$ cannot be prime for otherwise $\mathfrak{a}$ contains a product of prime integral ideals (namely itself). Since $\mathfrak{a}$ is not prime, there exist $\alpha_1, \alpha_2 \in \mathcal{O}_K$ with $\alpha_1\alpha_2 \in \mathfrak{a}$ and such that $\alpha_1, \alpha_2 \notin \mathfrak{a}$. Now define integral ideals

$$\mathfrak{b}_1 = \mathfrak{a} + \alpha_1\mathcal{O}_K \quad \text{and} \quad \mathfrak{b}_2 = \mathfrak{a} + \alpha_2\mathcal{O}_K.$$

Note that $\mathfrak{b}_1$ and $\mathfrak{b}_2$ strictly contain $\mathfrak{a}$ because $\alpha_1, \alpha_2 \notin \mathfrak{a}$. Moreover, $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$ because

$$\mathfrak{b}_1\mathfrak{b}_2 = (\mathfrak{a} + \alpha_1\mathcal{O}_K)(\mathfrak{a} + \alpha_2\mathcal{O}_K) = \mathfrak{a}^2 + \alpha_1\mathcal{O}_K + \alpha_2\mathcal{O}_K + \alpha_1\alpha_2\mathcal{O}_K,$$

and $\alpha_1\alpha_2 \in \mathfrak{a}$. We now show that either $\mathfrak{b}_1$ or $\mathfrak{b}_2$ belongs to $\mathcal{S}$. Suppose otherwise. Then there exist prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \mathfrak{b}_1 \quad \text{and} \quad \mathfrak{q}_1 \cdots \mathfrak{q}_\ell \subseteq \mathfrak{b}_2.$$

But then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k\mathfrak{q}_1 \cdots \mathfrak{q}_\ell \subseteq \beta_1\beta_2 \subseteq \mathfrak{a},$$

which contradicts the fact that $\mathfrak{a}$ is in $\mathcal{S}$. Hence $\mathfrak{b}_1$ or $\mathfrak{b}_2$ belongs to $\mathcal{S}$. In total, we have shown that if $\mathfrak{a} \in \mathcal{S}$, then there exists an integral ideal $\mathfrak{a}_1 \in \mathcal{S}$ strictly larger than $\mathfrak{a}$. Thus we obtain a strictly increasing infinite sequence of integral ideals in $\mathcal{S}$:

$$\mathfrak{a} \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots .$$

Taking the norm, we obtain a strictly decreasing sequence of positive integers:

$$\mathrm{N}(\mathfrak{a}) > \mathrm{N}(\mathfrak{a}_1) > \mathrm{N}(\mathfrak{a}_2) > \cdots .$$

This is impossible since the norm of an integral ideal is a positive integer. Hence $\mathcal{S}$ is empty and the claim follows. □

In order to obtain the reverse containment in Lemma 4.1, we need to do more work. Precisely, we want to show that every integral ideal factors into a product of prime integral ideals. To accomplish this, we will construct a group containing the ideals. Unfortunately, ideals are not invertible and so we need to work in a slightly more general setting. First observe that an integral ideal $\mathfrak{a}$ is just an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$. Moreover, it is a finitely generated $\mathcal{O}_K$-submodule of K by Theorem 2.1. We say $\mathfrak{f}$ is a **fractional ideal** of K if $\mathfrak{f}$ a nonzero finitely generated $\mathcal{O}_K$-submodule of K. In particular, all integral ideals are fractional ideals. Now let $\kappa_1, \ldots, \kappa_r \in K$ be generators for the fractional ideal $\mathfrak{f}$. Since K is the field of fractions of $\mathcal{O}_K$ by Proposition 1.2, $\kappa_i = \frac{\alpha_i}{\delta_i}$ with $\alpha_i, \delta_i \in \mathcal{O}_K$ and where δ_i is nonzero for $1 \leq i \leq r$. Setting $\delta = \delta_1 \cdots \delta_r$, we have that $\delta\kappa_i \in \mathcal{O}_K$ for all i and hence $\delta\mathfrak{f}$ is an integral ideal. Conversely, if there exists some nonzero $\delta \in \mathcal{O}_K$ such that $\delta\mathfrak{f}$ is an integral ideal then $\mathfrak{f}$ is a fractional ideal because $\mathfrak{a}$ is a finitely generated $\mathcal{O}_K$-submodule of K and hence $\mathfrak{f}$ is too. Thus for any fractional ideal $\mathfrak{f}$, there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}.$$

Every fractional ideal is of this form and integral ideals are precisely those for which $\delta = 1$. In particular, since $\mathfrak{a}$ is a free abelian group of rank n, we see that $\mathfrak{f}$ is a free abelian group of rank n as well. Now let $\mathfrak{p}$ be a prime integral ideal. We define $\mathfrak{p}^{-1}$ by

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

It turns out that $\mathfrak{p}^{-1}$ is a fractional ideal. Indeed, since $\mathfrak{p}$ is an integral ideal there exists a nonzero $\alpha \in \mathfrak{p}$. By definition of $\mathfrak{p}^{-1}$, we have that $\alpha\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Hence $\alpha\mathfrak{p}^{-1}$ is an integral ideal and therefore $\mathfrak{p}^{-1}$ is a fractional ideal. Unlike integral ideals, $1 \in \mathfrak{p}^{-1}$ so that $\mathfrak{p}^{-1}$ contains units. The following proposition proves a stronger version of this and more:

Lemma 4.2. *Let K be a number field and $\mathfrak{p}$ be a prime integral ideal. Then the following hold:*

(i)
$$\mathcal{O}_K \subset \mathfrak{p}^{-1}.$$

(ii)
$$\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K.$$

Proof. We will prove the latter two statement separately:

(i) Clearly $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$ so it suffices to show that $\mathfrak{p}^{-1}$ contains a nonzero element which is not an algebraic integer. Again, let $\alpha \in \mathfrak{p}$ be nonzero. By Lemma 4.1 let $k \geq 1$ be the minimal integer such that there exist prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ with

$$\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq \alpha\mathcal{O}_K.$$

As $\alpha \in \mathfrak{p}$, we have $\alpha\mathcal{O}_K \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, there must be some i with $1 \leq i \leq k$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. Without loss of generality, we may assume $\mathfrak{p}_1 \subseteq \mathfrak{p}$. But by Proposition 4.2 prime integral ideals are maximal and thus $\mathfrak{p}_1 = \mathfrak{p}$. Moreover, since k is minimal we must have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_k \not\subseteq \alpha\mathcal{O}_K.$$

Hence there exists a nonzero $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_k$ with $\beta \notin \alpha\mathcal{O}_K$. We will now show that $\beta\alpha^{-1}$ is a nonzero element in $\mathfrak{p}^{-1}$ that is not an algebraic integer. Clearly $\beta\alpha^{-1}$ is nonzero. Since $\mathfrak{p}_1 = \mathfrak{p}$, what we have previously shown implies $\beta\mathfrak{p} \subseteq \alpha\mathcal{O}_K$ and hence $\beta\alpha^{-1}\mathfrak{p} \in \mathcal{O}_K$ which means $\beta\alpha^{-1} \in \mathfrak{p}^{-1}$. But as $\beta \notin \alpha\mathcal{O}_K$, we also have $\beta\alpha^{-1} \notin \mathcal{O}_K$ so that $\beta\alpha^{-1}$ is not an algebraic integer. This proves (i).

(ii) By (i) and the definition of $\mathfrak{p}^{-1}$, we have $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p} \subseteq \mathcal{O}$. Since $\mathfrak{p}$ is maximal by Proposition 4.2, it follows that $\mathfrak{p}^{-1}\mathfrak{p}$ is either $\mathfrak{p}$ or $\mathcal{O}_K$. So it suffices to show that the first case cannot hold. Assume by contradiction that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Let $\{\omega_1, \ldots, \omega_r\}$ be a set of generators for $\mathfrak{p}$ and let $\alpha \in \mathfrak{p}^{-1}$ be a nonzero element that is not an algebraic integer which exists by (i). Then $\alpha\omega_i \in \mathfrak{p}^{-1}\mathfrak{p}$ for $1 \leq i \leq r$ and hence $\alpha\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. By our assumption, this further implies that $\alpha\mathfrak{p} \subseteq \mathfrak{p}$. But then

$$\alpha\omega_i = \sum_{1 \leq j \leq r} \alpha_{i,j}\omega_j,$$

with $\alpha_{i,j} \in \mathcal{O}_K$ for $1 \leq i, j \leq r$. We can rewrite this as,

$$(\alpha - \alpha_{i,i})\omega_i - \sum_{\substack{1 \leq j \leq r \\ j \neq i}} \alpha_{i,j}\omega_j = 0,$$

for all i. These r equations are equivalent to the identity

$$\begin{pmatrix} \alpha - \alpha_{1,1} & \alpha_{1,2} & \cdots & -\alpha_{1,r} \\ -\alpha_{2,1} & \alpha - \alpha_{2,2} & & \\ \vdots & & \ddots & \\ -\alpha_{r,1} & & & \alpha - \alpha_{r,r} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_r \end{pmatrix} = \mathbf{0}.$$

Thus the determinant of the matrix on the left-hand side must be zero. But this means α is a root of the characteristic polynomial $\det(xI - (\alpha_{i,j}))$ which is a monic polynomial with coefficients $\mathcal{O}_K$. By Proposition 2.2, α is an algebraic integer which is a contradiction. Thus $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$.

□

Let I_K denote the collection of fractional ideals of K. We call I_K the **ideal group** of K. The following theorem shows that I_K is indeed a group:

Theorem 4.1. *Let K be a number field. Then I_K is an abelian group with identity $\mathcal{O}_K$.*

Proof. Since fractional ideals are finitely generated $\mathcal{O}_K$-submodules of K, the product of fractional ideals is a fractional ideal. It is also clear that I_K is abelian if it is a group. Moreover, $\mathcal{O}_K$ is the identity since every every fractional ideal is a finitely generated $\mathcal{O}_K$-submodule of K. It now suffices to show that every fractional ideal $\mathfrak{f}$ has an inverse in I_K. By Lemma 4.2 (ii), the prime integral ideal $\mathfrak{p}$ has inverse $\mathfrak{p}^{-1}$. We now show that any integral ideal that is not prime has an inverse. Suppose by contradiction that $\mathfrak{a}$ is such an integral ideal with $N(\mathfrak{a})$ minimal. By Proposition 4.2, there exists a prime integral ideal $\mathfrak{p}$ such that $\mathfrak{a} \subset \mathfrak{p}$. This fact together with Lemma 4.2 (i) implies that

$$\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K.$$

We now claim $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$. If not, $\mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$. Let $\{\omega_1, \ldots, \omega_r\}$ be a set of generators for $\mathfrak{a}$. By Lemma 4.2, let $\alpha \in \mathfrak{p}^{-1}$ be a nonzero element that is not an algebraic integer. Then $\alpha\omega_i \in \mathfrak{p}^{-1}\mathfrak{a}$ for $1 \leq i \leq r$ and hence $\alpha\mathfrak{a} \subseteq \mathfrak{p}^{-1}\mathfrak{a}$. By our assumption, this further implies that $\alpha\mathfrak{p} \subseteq \mathfrak{a}$. But then

$$\alpha\omega_i = \sum_{1 \leq j \leq r} \alpha_{i,j}\omega_j,$$

with $\alpha_{i,j} \in \mathcal{O}_K$ for $1 \leq i, j \leq r$. We can rewrite this as,

$$(\alpha - \alpha_{i,i})\omega_i - \sum_{\substack{1 \leq j \leq r \\ j \neq i}} \alpha_{i,j}\omega_j = 0,$$

for all i. These r equations are equivalent to the identity

$$\begin{pmatrix} \alpha - \alpha_{1,1} & \alpha_{1,2} & \cdots & -\alpha_{1,r} \\ -\alpha_{2,1} & \alpha - \alpha_{2,2} & & \\ \vdots & & \ddots & \\ -\alpha_{r,1} & & & \alpha - \alpha_{r,r} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_r \end{pmatrix} = \mathbf{0}.$$

Thus the determinant of the matrix on the left-hand side must be zero. But this means α is a root of the characteristic polynomial $\det(xI - (\alpha_{i,j}))$ which is a monic polynomial with coefficients $\mathcal{O}_K$. By Proposition 2.2, α is an algebraic integer which is a contradiction. Thus $\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a}$. But then $\mathrm{N}(\mathfrak{p}^{-1}\mathfrak{a}) < \mathrm{N}(\mathfrak{a})$ and by the minimality of $\mathrm{N}(\mathfrak{a})$ it follows that the fractional ideal $\mathfrak{p}^{-1}\mathfrak{a}$ is invertible. Let $\mathfrak{b}$ be its inverse. Then $\mathfrak{b}\mathfrak{p}^{-1}\mathfrak{a} = \mathcal{O}_K$ and thus $\mathfrak{a}$ is invertible with inverse $\mathfrak{b}\mathfrak{p}^{-1}$. This is a contradiction, so we conclude that every integral ideal is invertible. We now show that every fractional ideal $\mathfrak{f}$ is invertible. Since $\mathfrak{f}$ is a fractional ideal, there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}.$$

As $\mathfrak{a}$ is invertible, $\delta\mathfrak{a}^{-1}$ is the inverse of $\mathfrak{f}$. This completes the proof. □

Now that we have proved that the ideal group I_K of K is indeed a group, we can shown that every integral ideal factors uniquely into a product of prime integral ideals (up to reordering of the factors):

Theorem 4.2. *Let K be a number field. Then for every integral ideal $\mathfrak{a}$ there exist prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that $\mathfrak{a}$ factors as*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k.$$

Moreover, this factorization is unique up to reordering of the factors.

Proof. We first prove existence and then uniqueness. For existence, suppose to the contrary that $\mathfrak{a}$ is an integral ideal that does not factor into a product of prime integral ideals and $\mathfrak{a}$ is maximal among all such integral ideals. Necessarily $\mathfrak{a}$ is not prime and by Proposition 4.2 there is some prime integral idea $\mathfrak{p}_1$ for which $\mathfrak{a} \subset \mathfrak{p}_1$. Then by Lemma 4.2 (ii), we have $\mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathcal{O}_K$ so that $\mathfrak{p}_1^{-1}\mathfrak{a}$ is also an integral ideal. Also, Lemma 4.2 (i) implies $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}_1^{-1}$. Actually, $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}_1^{-1}$ for otherwise $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_1^{-1}$ and hence $\mathfrak{p}_1^{-1} = O_K$ which is impossible because $\mathfrak{p}_1$ is proper. By maximality, $\mathfrak{a}\mathfrak{p}_1^{-1}$ factors into a product of prime integral ideals. That is, there exist prime integral ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_k$ such that

$$\mathfrak{a}\mathfrak{p}_1^{-1} = \mathfrak{p}_2, \ldots, \mathfrak{p}_k.$$

Hence

$$\mathfrak{a} = \mathfrak{p}_1, \ldots, \mathfrak{p}_k,$$

so that $\mathfrak{a}$ factors into a product of prime integral ideals which is a contradiction. This proves existence of such a factorization. Now we prove uniqueness. Suppose that $\mathfrak{a}$ admits factorizations

$$\mathfrak{a} = \mathfrak{p}_1, \ldots, \mathfrak{p}_k \quad \text{and} \quad \mathfrak{a} = \mathfrak{q}_1, \ldots, \mathfrak{q}_\ell,$$

for prime integral ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ with $1 \leq i \leq k$ and $1 \leq j \leq \ell$. Since $\mathfrak{p}_1$ is prime, there is some j for which $\mathfrak{q}_j \subseteq \mathfrak{p}_1$. Without loss of generality, we may assume $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$ and Proposition 4.2 we have that $\mathfrak{q}_1 = \mathfrak{p}_1$. Then

$$\mathfrak{p}_2, \ldots, \mathfrak{p}_k = \mathfrak{q}_2, \ldots, \mathfrak{q}_\ell.$$

Repeating this process, we see that $k = \ell$ and $\mathfrak{q}_i = \mathfrak{p}_i$ for all i. This proves uniqueness of the factorization. □

By Theorem 4.2, for any integral ideal $\mathfrak{a}$ there exist distinct prime integral ideal $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{a}$ admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

with $e_i \geq 1$ for all i, called the **prime factorization** of $\mathfrak{a}$ with **prime factors** $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Just as it is common to suppress the fundamental theorem of arithmetic and just state the prime factorization of an integer, we suppress Theorem 4.2 and state the prime factorization of an integral ideal. Also, as a near immediate corollary of Theorem 4.2, all fractional ideal admits a factorization into a product of prime integral ideals and their inverses (up to reordering of the factors):

Corollary 4.1. *Let K be a number field. Then for every fractional ideal $\mathfrak{f}$ there exist prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ such that $\mathfrak{f}$ factors as*

$$\mathfrak{f} = \mathfrak{p}_1 \cdots \mathfrak{p}_k \mathfrak{q}_1^{-1}, \ldots, \mathfrak{q}_\ell^{-1}.$$

Moreover, this factorization is unique up to reordering of the factors.

Proof. If $\mathfrak{f}$ is a fractional ideal, then there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}.$$

In particular, $\mathfrak{a}$ and $\delta\mathcal{O}_K$ are integral ideals such that $\delta\mathcal{O}_K\mathfrak{f} = \mathfrak{a}$. By Theorem 4.2, $\mathfrak{a}$ and $\delta\mathcal{O}_K$ admit unique factorizations

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k \quad \text{and} \quad \delta\mathcal{O}_K = \mathfrak{q}_1, \ldots, \mathfrak{q}_\ell,$$

up to reordering of the factors. Hence

$$\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell\mathfrak{f} = \mathfrak{p}_1 \cdots \mathfrak{p}_k,$$

which is equivalent to the factorization for $\mathfrak{f}$. □

With the Chinese remainder theorem, we can now derive some useful consequences of the unique factorization of integral ideals. Indeed, suppose $\mathfrak{a}$ is an integral ideal with prime factorization

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Then the integral ideals $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_r^{e_r}$ are pairwise relatively prime so that the Chinese remainder theorem gives an isomorphism

$$\mathcal{O}_K/\mathfrak{a} \cong \bigoplus_{1 \leq i \leq r} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

In particular, for any $\alpha_i \in \mathcal{O}_K$ for all i, there exists a unique $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i}},$$

for all i. We can now show that any fractional ideal is generated by at most two elements:

Corollary 4.2. *Let K be a number field. Then any fractional ideal $\mathfrak{f}$ is generated by at most two elements.*

Proof. We first prove the claim for an integral ideal $\mathfrak{a}$. Let $\alpha \in \mathfrak{a}$ be nonzero and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime factors of $\alpha\mathcal{O}_K$. As $\alpha\mathcal{O}_K \subseteq \mathfrak{a}$, the prime factorization of $\mathfrak{a}$ is

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

with $e_i \geq 0$ for $1 \leq i \leq r$. By uniqueness of the prime factorization of integral ideals, $\mathfrak{p}_i^{e_i+1} \subset \mathfrak{p}_i^{e_i}$ for all i. Thus there exist nonzero $\beta_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ for all i. Since $\mathfrak{p}_1^{e_1+1}, \ldots, \mathfrak{p}_r^{e_r+1}$ are pairwise relatively prime, the Chinese remainder theorem implies that there exists $\beta \in \mathcal{O}_K$ with

$$b \equiv \beta_i \pmod{\mathfrak{p}_i^{e_i+1}},$$

for all i. As $\beta_i \in \mathfrak{p}_i^{e_i}$ for all i, we have $\beta \in \mathfrak{a}$ and hence $\beta\mathcal{O}_K \subseteq \mathfrak{a}$. But as $\beta \notin \mathfrak{p}_i^{e_i+1}$ for all i, we see that $\beta\mathcal{O}_K\mathfrak{a}^{-1}$ is necessarily an integral ideal relatively prime to $\alpha\mathcal{O}_K$. This means

$$\beta\mathcal{O}_K\mathfrak{a}^{-1} + \alpha\mathcal{O}_K = \mathcal{O}_K,$$

and hence

$$\beta\mathcal{O}_K + \alpha\mathfrak{a} = \mathfrak{a}.$$

But as $\alpha, \beta \in \mathfrak{a}$, we have $\beta\mathcal{O}_K + \alpha\mathfrak{a} \subseteq \beta\mathcal{O}_K + \alpha\mathcal{O}_K \subseteq \mathfrak{a}$ and so

$$\beta\mathcal{O}_K + \alpha\mathcal{O}_K = \mathfrak{a}.$$

This shows that $\mathfrak{a}$ is generated by at most two elements. Now suppose $\mathfrak{f}$ is a fractional ideal. Then there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}.$$

Since $\mathfrak{a}$ is generated by at most two elements, say α and β, we have

$$\mathfrak{f} = \frac{\alpha}{\delta}\mathcal{O}_K + \frac{\beta}{\delta}\mathcal{O}_K,$$

and so $\mathfrak{f}$ is also generated by at most two elements as well. □

Corollary 4.2 shows that while the the ring of integers $\mathcal{O}_K$ of K may not be a principal ideal domain, it is not far off from one since we every integral ideal needs at most two generators. We will give a more refined interpretation of this when discussing quotients of the ideal group I_K. For now, we deduce some more properties of the norm of integral ideals and extend this notion to fractional ideals as well. We will need a useful proposition:

Proposition 4.3. *Let K be a number field. Then for any prime integral ideal $\mathfrak{p}$ and $n \geq 0$,*

$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1},$$

as $\mathcal{O}_K$-modules.

Proof. By the uniqueness of the factorization of integral ideals, there exists $\beta \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$. Now consider the homomorphism

$$\phi : \mathcal{O}_K \to \mathfrak{p}^n/\mathfrak{p}^{n+1} \qquad \alpha \to \alpha\beta \pmod{\mathfrak{p}^{n+1}}.$$

By the first isomorphism theorem, it suffices to show $\ker\phi = \mathfrak{p}$ and that ϕ is surjective. Let us first show $\ker\phi = \mathfrak{p}$. As $\beta \in \mathfrak{p}^n$, it is obvious that $\mathfrak{p} \subseteq \ker\phi$. Conversely, suppose $\alpha \in \mathcal{O}_K$ is such that $\phi(\alpha) = 0$. Then $\alpha\beta \in \mathfrak{p}^{n+1}$, and as $\beta \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$ we must have $\alpha \in \mathfrak{p}$. It follows that $\ker\phi = \mathfrak{p}$. We now show that ϕ is surjective. Let $\gamma \in \mathfrak{p}^n$ be a representative of a class in $\mathfrak{p}^n/\mathfrak{p}^{n+1}$. As $\beta \in \mathfrak{p}^n$, we have $\beta\mathcal{O}_K \subseteq \mathfrak{p}^n$. But since $\beta \notin \mathfrak{p}^{n+1}$, we see that $\beta\mathcal{O}_K\mathfrak{p}^{-n}$ is necessarily an integral ideal relatively prime to $\mathfrak{p}^{n+1}$. As $\mathfrak{p}^{n+1}$ and $\beta\mathcal{O}_K\mathfrak{p}^{-n}$ are relatively prime, the Chinese remainder theorem implies that we can find a unique $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv \gamma \pmod{\mathfrak{p}^{n+1}} \quad \text{and} \quad \alpha \equiv 0 \pmod{\beta\mathcal{O}_K\mathfrak{p}^{-n}}.$$

The second condition implies $\alpha \in \beta\mathcal{O}_K\mathfrak{p}^{-n}$. As $\gamma \in \mathfrak{p}^n$ and α and γ differ by an element in $\mathfrak{p}^{n+1} \subset \mathfrak{p}^n$, we have that $\alpha \in \beta\mathcal{O}_K\mathfrak{p}^{-n} \cap \mathfrak{p}^n = \beta\mathcal{O}_K$ where the equality holds because the intersection of ideals is equal to their product if the ideals are relatively prime. Thus $\frac{\alpha}{\beta} \in \mathcal{O}_K$ and hence

$$\phi\left(\frac{\alpha}{\beta}\right) = \alpha \equiv \gamma \pmod{\mathfrak{p}^{n+1}}.$$

This shows ϕ is surjective completing the proof. □

Now we can show that the norm of an integral ideal is completely multiplicative:

Proposition 4.4. *Let K be a number field and let $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals. Then*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b}).$$

Proof. First suppose $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime. Then the Chinese remainder theorem implies

$$\mathcal{O}_K/\mathfrak{ab} \cong \mathcal{O}_K/\mathfrak{a} \oplus \mathcal{O}_K/\mathfrak{b},$$

and hence $|\mathcal{O}_K/\mathfrak{ab}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{b}|$ so that $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b})$. It now suffices to show $\mathrm{N}(\mathfrak{p}^n) = \mathrm{N}(\mathfrak{p})^n$ for all prime integral ideals $\mathfrak{p}$ and $n \geq 0$. We will prove this by induction. The base case is clear so assume that the claim holds for $n-1$. By the third isomorphism theorem, we have

$$\mathcal{O}_K/\mathfrak{p}^{n-1} \cong (\mathcal{O}_K/\mathfrak{p}^n)/(\mathfrak{p}^{n-1}/\mathfrak{p}^n).$$

Using Proposition 4.3, it follows that

$$|\mathcal{O}_K/\mathfrak{p}^{n-1}| = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathfrak{p}^{n-1}/\mathfrak{p}^n|} = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathcal{O}_K/\mathfrak{p}|}.$$

Thus $\mathrm{N}(\mathfrak{p}^n) = \mathrm{N}(\mathfrak{p}^{n-1})\,\mathrm{N}(\mathfrak{p})$ and our induction hypothesis implies $\mathrm{N}(\mathfrak{p}^n) = \mathrm{N}(\mathfrak{p})^n$ as desired. □

Note that by Proposition 4.4, the norm is a homomorphism from the set of integral ideals into $\mathbb{Z}_{\geq 1}$. As last we can extend the norm to fractional ideals. Let $\mathfrak{f}$ be a fractional ideal. By Corollary 4.1, there exist unique integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that

$$\mathfrak{f} = \mathfrak{a}\mathfrak{b}^{-1}.$$

For any fractional ideal $\mathfrak{f}$, we define its **norm** $\mathrm{N}(\mathfrak{f})$ by

$$\mathrm{N}(\mathfrak{f}) = \frac{\mathrm{N}(\mathfrak{a})}{\mathrm{N}(\mathfrak{b})}.$$

Then we have a homomorphism

$$\mathrm{N} : I_K \to \mathbb{Q}^* \qquad \mathfrak{f} \mapsto \mathrm{N}(\mathfrak{f}).$$

5. Ramification

We now discuss the factorization of prime integral ideals in number fields. First, we need to introduce the concept of prime integral ideals above primes. Let K be a number field and let $\mathfrak{p}$ be a prime integral ideal. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime integral ideal of $\mathbb{Q}$. Indeed, it is clear that $\mathfrak{p} \cap \mathbb{Z}$ is an integral ideal of $\mathbb{Q}$. It is proper because $1 \notin \mathfrak{p} \cap \mathbb{Z}$ as $\mathfrak{p}$ does not contain units. It is nonzero because $\mathcal{O}_K/\mathfrak{p}$ is a finite field by Proposition 4.2 and thus has characteristic dividing $\mathrm{N}(\mathfrak{p})$ by definition of the norm so that $\mathrm{N}(\mathfrak{p}) \in \mathfrak{p}$. But as $\mathrm{N}(\mathfrak{p})$ is also a positive integer, $\mathrm{N}(\mathfrak{p}) \in \mathfrak{p} \cap \mathbb{Z}$. To show that $\mathfrak{p} \cap \mathbb{Z}$ is prime, suppose a and b are integers such that $ab \in \mathfrak{p} \cap \mathbb{Z}$. Then $ab \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. But then $a \in \mathfrak{p} \cap \mathbb{Z}$ or $b \in \mathfrak{p} \cap \mathbb{Z}$ as desired. We have now shown that $\mathfrak{p} \cap \mathbb{Z}$ is a prime integral ideal of $\mathbb{Q}$. Hence

$$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z},$$

for some prime integer p. Accordingly, we say that $\mathfrak{p}$ is **above** p, or equivalently, p is **below** $\mathfrak{p}$. Moreover, if $\mathfrak{p}$ is above p, then $\mathfrak{p}$ must be a prime factor of $p\mathcal{O}_K$. Indeed, $p\mathbb{Z} \subseteq \mathfrak{p}$ so that $p\mathcal{O}_K \subseteq \mathfrak{p}$ and then the fact $\mathfrak{p}$ is prime implies that some prime factor of $p\mathcal{O}_K$ is contained in $\mathfrak{p}$. Since prime integral ideals are maximal by Proposition 4.2, this prime factor must be $\mathfrak{p}$ itself. We illustrate these relations by the extension

$$\begin{array}{ccccc} \mathfrak{p} & \subset & \mathcal{O}_K & \subset & K \\ & & \big| & & \\ p\mathbb{Z} & \subset & \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Since $\mathfrak{p}$ and $p\mathbb{Z}$ are maximal in $\mathcal{O}_K$ and $\mathbb{Z}$ respectively (by Proposition 4.2), we have the residue fields $\mathcal{O}_K/\mathfrak{p}$ and $\mathbb{F}_p$. It turns out that $\mathcal{O}_K/\mathfrak{p}$ is a finite dimensional vector space over $\mathbb{F}_p$. To see this, consider the homomorphism

$$\phi : \mathbb{Z} \to \mathcal{O}_K/\mathfrak{p} \qquad a \to a \pmod{\mathfrak{p}}.$$

Now $\ker\phi = \mathfrak{p} \cap \mathbb{Z}$ and hence $\ker\phi = p\mathbb{Z}$ since $\mathfrak{p}$ is above p. By the first isomorphism theorem, ϕ induces an injection $\phi : \mathbb{F}_p \to \mathcal{O}_K/\mathfrak{p}$. By Proposition 4.1, $\mathcal{O}_K/\mathfrak{p}$ is finite and thus a finite field containing $\mathbb{F}_p$. Necessarily $\mathcal{O}_K/\mathfrak{p}$ is a finite dimensional vector space over $\mathbb{F}_p$. Accordingly, we define the **inertia degree** $f_\mathfrak{p}$ of $\mathfrak{p}$ by

$$f_\mathfrak{p} = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p].$$

That is, $f_\mathfrak{p}$ is the dimension of the residue field $\mathcal{O}_K/\mathfrak{p}$ as a vector space over $\mathbb{F}_p$. Then we have

$$\mathrm{N}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_p|^{f_\mathfrak{p}} = p^{f_\mathfrak{p}}.$$

In particular, the norm of a prime integral ideal is a power of the prime below it. As we have already noted, $\mathfrak{p}$ is a prime factor of $p\mathcal{O}_K$. The **ramification index** $e_\mathfrak{p}$ of $\mathfrak{p}$ is the positive integer such that $p\mathcal{O}_K\mathfrak{p}^{-e_\mathfrak{p}}$ is relatively prime to $\mathfrak{p}$. If $p\mathcal{O}_K$ has prime factors $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, then the prime factorization of $p\mathcal{O}_K$ is

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_r^{e_{\mathfrak{p}_r}}.$$

We say that p is **ramified** if $e_{\mathfrak{p}_i} \geq 2$ for some i and **unramified** otherwise. In particular,

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

if and only if p is unramified. We also say p is **split** if $p\mathcal{O}_K$ is not prime. The degree of a number field is connected to the inertia degree and ramification index via the following proposition:

Proposition 5.1. *Let K be a number field of degree n and let p be a prime. Suppose $p\mathcal{O}_K$ has prime factorization*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_r^{e_{\mathfrak{p}_r}}.$$

Then

$$n = \sum_{1 \leq i \leq r} e_{\mathfrak{p}_i} f_{\mathfrak{p}_i}.$$

Proof. Since p is an integer and K is of degree n, on the one hand

$$\mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(p) = p^n.$$

On the other hand, complete multiplicativity of the norm by Proposition 4.4 implies

$$\mathrm{N}(p\mathcal{O}_K) = \mathrm{N}(\mathfrak{p}_1)^{e_{\mathfrak{p}_1}} \cdots \mathrm{N}(\mathfrak{p}_r)^{e_{\mathfrak{p}_r}} = p^{e_{\mathfrak{p}_1} f_{\mathfrak{p}_1}} \cdots p^{e_{\mathfrak{p}_r} f_{\mathfrak{p}_r}}.$$

Thus

$$p^n = p^{e_{\mathfrak{p}_1} f_{\mathfrak{p}_1}} \cdots p^{e_{\mathfrak{p}_r} f_{\mathfrak{p}_r}},$$

and the claim follows upon comparing exponents. □

We now describe some special cases of how $p\mathcal{O}_K$ may factor. If $r = n$, we say p is **totally split** and so $e_\mathfrak{p} = f_\mathfrak{p} = 1$ for all $\mathfrak{p}$ above p by Proposition 5.1. Equivalently, p is totally split if and only if the number of prime integral ideal above p is equal to the degree of K. If $r = 1$, then there is exactly one prime integral ideal $\mathfrak{p}$ above p and so

$$p\mathcal{O}_K = \mathfrak{p}^{e_\mathfrak{p}}.$$

If $e_\mathfrak{p} = 1$, so that p does not ramify, we say p is **inert** and so $f_\mathfrak{p} = n$ by Proposition 5.1. Thus p is inert if and only if $p\mathcal{O}_K$ is prime. If $e_\mathfrak{p} \geq 2$, then p ramifies and we say p is **totally ramified** if $e_\mathfrak{p} = n$ so that $f_\mathfrak{p} = 1$ by Proposition 5.1. Equivalently, p is totally ramified if and only if it is the power of a prime integral ideal with power equal to the degree of K. The ramification of primes is intimately connected to the discriminant of a number field as the following theorem shows:

Theorem 5.1. *Let K be a number field. Then p is ramified if and only if p divides $|\Delta_K|$.*

Proof. Let p be a prime and suppose $p\mathcal{O}_K$ has prime factorization

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_r^{e_{\mathfrak{p}_r}},$$

Now let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis for K and let $\overline{\alpha} \in \mathcal{O}_K/p\mathcal{O}_K$ denote the reduction of $\alpha \in \mathcal{O}_K$ modulo p. Then $\{\overline{\alpha_1}, \ldots, \overline{\alpha_n}\}$ is a basis for $\mathcal{O}_K/p\mathcal{O}_K$ as a vector space over $\mathbb{F}_p$. Moreover, the matrix for $T_{\overline{\alpha}}$ is obtained from T_α by reducing the coefficients modulo p. These two facts together give

$$\Delta_K = \operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) \equiv \operatorname{disc}_{(\mathcal{O}_K/p\mathbb{Z})/\mathbb{F}_p}(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) \pmod{p}.$$

Recall that $\operatorname{disc}_{(\mathcal{O}_K/p\mathbb{Z})/\mathbb{F}_p}(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ is an element of $\mathbb{F}_p$. Then as $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K)$ is equivalent to $\operatorname{disc}_{(\mathcal{O}_K/p\mathbb{Z})/\mathbb{F}_p}(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ up to elements of $(\mathbb{F}_p^*)^2$, it must be the case that p divides $|\Delta_K|$ if and only if $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/p\mathcal{O}_K) = 0$. By the Chinese remainder theorem,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \bigoplus_{1 \le i \le r} \mathcal{O}_K/\mathfrak{p}_i^{e_{\mathfrak{p}_i}},$$

and so Proposition 3.1 further implies

$$\Delta_K = \prod_{1 \le i \le r} \operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_i^{e_{\mathfrak{p}_i}}).$$

Hence p divides $|\Delta_K|$ if and only if $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_i^{e_{\mathfrak{p}_i}}) = 0$ for some i. It is now sufficient to show that $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}) = 0$ for any prime integral ideal $\mathfrak{p}$ above p if and only if $e_\mathfrak{p} \ge 2$. First suppose $e_\mathfrak{p} \ge 2$. We will prove $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}) = 0$. By the uniqueness of the factorization of integral ideals, there exists a nonzero $\alpha_1 \in \mathfrak{p}^{e_\mathfrak{p}-1} - \mathfrak{p}^{e_\mathfrak{p}}$. Then $\alpha_1^2 \in \mathfrak{p}^{2(e_\mathfrak{p}-1)} \subseteq \mathfrak{p}^{e_\mathfrak{p}}$ because $e_\mathfrak{p} \ge 2$. By construction, $\overline{\alpha_1} \in \mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}$ is nonzero and such that $\overline{\alpha_1}^2 = 0$. Since $\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}$ is an n dimensional vector space over $\mathbb{F}_p$, there exists a basis of the form $\{\overline{\alpha_1}, \ldots, \overline{\alpha_m}\}$. Now

$$\operatorname{Tr}_{(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}})/\mathbb{F}_p}(\overline{\alpha_1\alpha_j}) = 0,$$

for $1 \le j \le n$ because $T^2_{\overline{\alpha_1\alpha_i}}$ is the zero operator (as $\overline{\alpha_1}^2 = 0$) and hence all of its eigenvalues are zero. But then the first row of $(\operatorname{Tr}_{(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}})/\mathbb{F}_p}(\overline{\alpha_i\alpha_j}))_{i,j}$ is zero and hence $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}) = 0$. Now suppose $e_\mathfrak{p} = 1$. We will prove $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}) \ne 0$. Recall that $\mathcal{O}_K/\mathfrak{p}$ is a field and a vector space over $\mathbb{F}_p$ of dimension $f_\mathfrak{p}$. Thus $(\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p$ it is a finite separable extension. Hence $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$ is nonzero by Proposition 3.2. We have now shown that $\operatorname{disc}_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}^{e_\mathfrak{p}}) = 0$ if and only if $e_\mathfrak{p} \ge 2$ which completes the proof. □

As an immediate corollary, we see that only finitely many primes can ramify:

Corollary 5.1. *Let K be a number field. Then finitely many primes ramify in K.*

Proof. There are only finitely many prime divisors of $|\Delta_K|$. Hence finitely many primes ramify by Theorem 5.1. □

There is no general way to see how a prime p factors for an arbitrary number field K. However, in the case that the ring of integers is monogenic we can describe the factorization explicitly via the **Dedekind-Kummer theorem**:

Theorem 5.2 (Dedekind-Kummer theorem)**.** *Let K be a monogenic number field where $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for $\alpha \in \mathcal{O}_K$ and let p be a prime. Let $m_\alpha(x)$ be the minimal polynomial for α and let $\overline{m_\alpha}(x)$ be its reduction modulo p. Also let*

$$\overline{m_\alpha}(x) = \overline{m_r}(x)^{e_r} \cdots \overline{m_r}(x)^{e_r}$$

with $\overline{m_i}(x) \in \mathbb{F}_p[x]$ and $e_i \ge 0$, be the prime factorization of $\overline{m_\alpha}(x)$ in $\mathbb{F}_p[x]$. Let $m_i(x) \in \mathbb{Z}[x]$ be any lift of $\overline{m_i}(x)$ and set

$$\mathfrak{p}_i = p\mathcal{O}_K + m_i(\alpha)\mathcal{O}_K,$$

for all i. Then $\mathfrak{p}_i$ is a prime integral ideal for all i and

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

is the prime factorization of $p\mathcal{O}_K$.

Proof. Since $m_\alpha(x)$ is the minimal polynomial for α, we have an isomorphism $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/m_\alpha(x)\mathbb{Z}[x]$ where the inverse isomorphism is given by evaluation at α. Then we have the chain of isomorphism

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}[x]/m_\alpha(x)\mathbb{Z}[x])/(p(\mathbb{Z}[x]/m_\alpha(x)\mathbb{Z}[x])) \cong \mathbb{Z}[x]/(p\mathbb{Z}[x] + m_\alpha(x)\mathbb{Z}[x]) \cong \mathbb{F}_p[x]/\overline{m_\alpha}(x)\mathbb{F}_p[x],$$

where the second and third isomorphisms follow by taking $\mathbb{Z}[x]/(p\mathbb{Z}[x] + m_\alpha(x)\mathbb{Z}[x])$ and reducing $\mathbb{Z}[x]$ modulo $m_\alpha(x)$ or p respectively. Therefore the inverse isomorphism is given by sending any representative $\overline{f}(x)$ of a class in $\mathbb{F}_p[x]/\overline{m_\alpha}(x)\mathbb{F}_p[x]$ to a lift $f(x) \in \mathbb{Z}[x]$ and then to $\overline{f(\alpha)}$ where $\overline{f(\alpha)}$ is $f(\alpha)$ modulo $p\mathcal{O}_K$. Now set $A = \mathbb{F}_p[x]/\overline{m_\alpha}(x)\mathbb{F}_p[x]$. Then the Chinese remainder theorem gives an isomorphism

$$A \cong \bigoplus_{1\le i\le r} \mathbb{F}_p[x]/\overline{m_i}(x)^{e_i}\mathbb{F}_p[x].$$

As $\overline{m_i}(x)$ is irreducible, $\overline{m_i}(x)\mathbb{F}_p[x]$ is maximal and hence $\mathbb{F}_p[x]/\overline{m_i}(x)\mathbb{F}_p[x]$ is a field. By the third isomorphism theorem, $\overline{m_i}(x)\mathbb{F}_p[x]/\overline{m_i}(x)^{e_i}\mathbb{F}_p[x]$ is a maximal ideal of $\mathbb{F}_p[x]/\overline{m_i}(x)^{e_i}\mathbb{F}_p[x]$. It follows that the maximal ideals of A are precisely $\overline{m_i}(x)A$ and we have an isomorphism

$$A/\overline{m_i}(x)A \cong \mathbb{F}_p[x]/\overline{m_i}(x)\mathbb{F}_p[x],$$

for all i. Via the isomorphism $\mathcal{O}_K/p\mathcal{O}_K \cong A$ described above, the maximal ideals of $\mathcal{O}_K/p\mathcal{O}_K$ are exactly $\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)$. We now show that the $\mathfrak{p}_i$ are prime. To see this, consider the surjective homomorphism

$$\pi : \mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K \qquad \alpha \to \alpha \pmod{p\mathcal{O}_K}.$$

Then the image of $\mathfrak{p}_i$ under π is $\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)$. As this ideal is maximal and hence prime, the preimage $\mathfrak{p}_i$ is prime too. Moreover, the $\mathfrak{p}_i$ are all distinct since the $\overline{m_i(\alpha)}\mathcal{O}_K/p\mathcal{O}_K$ are which are all distinct because the $\overline{m_i}(x)A$ are (using the isomorphism $\mathcal{O}_K/p\mathcal{O}_K \cong A$). In particular, they are also relatively prime. By construction, $\mathfrak{p}_i \subseteq p\mathcal{O}_K$ so that the $\mathfrak{p}_i$ are prime factors of $p\mathcal{O}_K$. These are the only prime factors of $p\mathcal{O}_K$ because the image of any prime integral ideal under π and contained in $p\mathcal{O}_K$ must be a maximal ideal of $\mathcal{O}_K/p\mathcal{O}_K$, by Proposition 4.2 and the fourth isomorphism theorem, and every maximal ideal is one of the $\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)$. Together, all of this means that $p\mathcal{O}_K$ admits the prime factorization

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdots \mathfrak{p}_r^{e_{\mathfrak{p}_r}},$$

for some ramification indices $e_{\mathfrak{p}_i}$ for all i. We will be done if we can show that the ramification indices satisfy $e_{\mathfrak{p}_i} = e_i$. To accomplish this, observe that we have an isomorphism

$$\mathcal{O}_K/\mathfrak{p}_i \cong (\mathcal{O}_K/p\mathcal{O}_K)/(\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)) \cong \mathbb{F}_p[x]/\overline{m_i}(x)\mathbb{F}_p[x],$$

where the first isomorphism follow by taking $\mathcal{O}_K/\mathfrak{p}_i$ and reducing $\mathcal{O}_K$ modulo p and the second isomorphism follows from $\mathcal{O}_K/p\mathcal{O}_K \cong A$ and that the image of the maximal ideal $\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)$ under this isomorphisms is $\overline{m_i}(x)A$. Now $\mathbb{F}_p[x]/\overline{m_i}(x)\mathbb{F}_p[x]$ is a vector space over $\mathbb{F}_p$ (as it contains $\mathbb{F}_p$) of degree $\deg(\overline{m_i}(x))$. Hence the inertia degree $f_{\mathfrak{p}_i}$ of $\mathfrak{p}_i$ satisfies $f_{\mathfrak{p}_i} = \deg(\overline{m_i}(x))$. The ideal $\overline{m_i}(x)^{e_i}A$ under the isomorphism $A \cong \mathcal{O}_K/p\mathcal{O}_K$ is the ideal $\overline{m_i(\alpha)}^{e_i}(\mathcal{O}_K/p\mathcal{O}_K)$. As the image of $\mathfrak{p}_i$ under π is $\overline{m_i(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K)$, we have that $\mathfrak{p}_i^{e_i}$ is contained in the preimage of $\overline{m_i(\alpha)}^{e_i}(\mathcal{O}_K/p\mathcal{O}_K)$ under π. As $\overline{m_\alpha(\alpha)}(\mathcal{O}_K/p\mathcal{O}_K) = 0$ is the zero ideal, it follows that

$$p\mathcal{O}_K = \pi^{-1}(0) \supseteq \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Since the $\mathfrak{p}_i$ are prime, we have $e_{\mathfrak{p}_i} \le e_i$ for all i. By Proposition 5.1 then gives

$$n = \sum_{1\le i\le r} e_{\mathfrak{p}_i} f_{\mathfrak{p}_i} \le \sum_{1\le i\le r} e_i f_{\mathfrak{p}_i} \le \sum_{1\le i\le r} e_i \deg(\overline{m_i}(x)) \le n,$$

where the last equality follows by the prime factorization of $\overline{m_\alpha}(x)$ and that $\deg(\overline{m_\alpha}(x)) = \deg(m_\alpha(x))$ because $m_\alpha(x)$ is monic. This shows that $e_{\mathfrak{p}_i} = e_i$ for all i which completes the proof. □

Lastly, we want to show that the number of integral ideals of a given norm is relatively small. Indeed, let $a_K(m)$ denote the number of integral ideals of norm m. Because the norm is multiplicative so is $a_K(m)$. Moreover, we have the following result:

Proposition 5.2. *Let K be a number field of degree n. Then $a_K(m) \leq \sigma_0(m)^n$.*

Proof. Let $\mathfrak{a}$ be an integral ideal of norm m. First suppose $m = p^k$ for some prime p and $k \geq 0$. As there are at most n prime integral ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ above p with inertia degrees $f_{\mathfrak{p}_1}, \ldots, f_{\mathfrak{p}_1}$ respectively, we have

$$\mathrm{N}(\mathfrak{a}) = p^{e_1 f_{\mathfrak{p}_1}} \cdots p^{e_n f_{\mathfrak{p}_n}},$$

for some integers $0 \leq e_i \leq k$ for $1 \leq i \leq n$. Therefore the number of possibilities is equivalent to the number of solutions

$$e_1 f_{\mathfrak{p}_1} + \cdots + e_n f_{\mathfrak{p}_n} = k,$$

which is at most $\sigma_0(p^k)^n = (k+1)^n$. This proves the claim in the case m is a prime power. By multiplicativity of $a_K(m)$ and the divisor function, it follows that the number of integral ideals of norm m is at most $\sigma_0(m)^n$ as desired. □

6. Lattices

Before we can continue with the study of number fields, we need to make a detour and discuss some geometry of lattices. This is essential because it will provide us with a geometric interpretation for how the ring of integers $\mathcal{O}_K$ sits inside the number field K. We say that $\Lambda \subset \mathbb{R}^n$ is a **lattice** if Λ is a free abelian group of rank n. In particular, any lattice Λ is of the form

$$\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n,$$

for some basis $\{v_1, \ldots, v_n\}$. Notice that Λ acts on $\mathbb{R}^n$ by automorphisms given by translation. That is, we have a group action

$$\Lambda \times \mathbb{R}^n \to \mathbb{R}^n \qquad (\lambda, x) \to \lambda + x.$$

Moreover, Λ acts properly discontinuously on $\mathbb{R}^n$. To see this, let $x \in \mathbb{R}^n$ and let δ_x be such that $0 < \delta_x < \min_{1 \leq i \leq n}(x - v_i)$. Then taking U_x to be the ball of radius δ_x about x, the intersection $\lambda + U_x \cap U_x$ is empty unless $\lambda = 0$. As Λ is also discrete, it follows that $\mathbb{R}^n/\Lambda$ is also connected Hausdorff (recall that $\mathbb{R}^n$ is connected Hausdorff). In particular, $\mathbb{R}^n/\Lambda$ admits a fundamental domain

$$\mathcal{P} = \{t_1 v_1 + \cdots + t_n v_n \in \mathbb{R}^n : 0 \leq t_i \leq 1 \text{ for } 1 \leq i \leq n\}.$$

Indeed, since Λ acts by translations, it is obvious that $\mathcal{P}$ is a fundamental domain for $\mathbb{R}^n/\Lambda$. Moreover, any translation of $\mathcal{P}$ by an element of Λ is also a fundamental domain. Recall that the volume $\mathrm{Vol}(X)$ of a measurable subset $X \subseteq \mathbb{R}^n$ is defined as

$$\mathrm{Vol}(X) = \int_X dx_1 \cdots dx_n.$$

Then we define the **volume** V_Λ of Λ by

$$V_\Lambda = \mathrm{Vol}(\mathcal{P}).$$

That is, the volume of Λ is the volume of the fundamental domain $\mathcal{P}$. Since the measures dx_i for $1 \leq i \leq n$ are translation invariant, V_Λ is independent of the choice of fundamental domain. If Λ is given by the basis $\{v_1, \ldots, v_n\}$, we write

$$v_i = \sum_{1 \leq i \leq n} v_{i,j} e_j,$$

where the e_i are the standard basis vectors, and define the **generator matrix** P of Λ by

$$P = \begin{pmatrix} v_{1,1} & \cdots & v_{1,n} \\ \vdots & & \vdots \\ v_{n,1} & \cdots & v_{n,n} \end{pmatrix}.$$

The following proposition shows that the volume of Λ is essentially given by the determinant of the generator matrix:

Proposition 6.1. *Let Λ be a lattice in $\mathbb{R}^n$ and P be its generator matrix. Then*

$$V_\Lambda = |\det(P)|.$$

Proof. Making the change of variables $x_i \to t_i$ for $1 \leq i \leq n$ where

$$x_1 e_1 + \cdots + x_n e_n = t_1 v_1 + \cdots + t_n v_n,$$

the corresponding Jacobian matrix is P because this is the base change matrix from the standard basis to the basis $\{v_1, \ldots, v_n\}$. Then

$$V_\Lambda = \int_{\mathcal{P}} dx_1 \cdots dx_n = |\det(P)| \int_{[0,1]^n} dt_1 \cdots dt_n = |\det(P)|,$$

as claimed. □

The crucial result we require is **Minkowski's lattice point theorem** which states that, under some mild conditions, a set of sufficiently large volume contains a nonzero point of a lattice:

Theorem 6.1 (Minkowski's lattice point theorem)**.** *Let Λ be a lattice in $\mathbb{R}^n$. Suppose $X \subset \mathbb{R}^n$ is a compact convex symmetric set. If*

$$\mathrm{Vol}(X) \geq 2^n V_\Lambda,$$

then there exists a nonzero $\lambda \in L$ with $\lambda \in X$

Proof. We will prove the claim depending on if the inequality is strict or not. First suppose $\mathrm{Vol}(X) > 2^n V_\Lambda$. Consider the linear map

$$\phi : \frac{1}{2}X \to \mathbb{R}^n/\Lambda \qquad \frac{1}{2}x \mapsto \frac{1}{2}x \pmod{\Lambda}.$$

If ϕ were injective, then

$$\mathrm{Vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\mathrm{Vol}(X) \leq V_\Lambda,$$

so that $\mathrm{Vol}(X) \leq 2^n V_\Lambda$. This is a contradiction, so ϕ cannot be injective. Hence there exists distinct $x_1, x_2 \in \frac{1}{2}X$ such that $\phi(x_1) = \phi(x_2)$. Thus $2x_1, 2x_2 \in X$. In particular, since X is symmetric we must have $-2x_2 \in X$. But then the fact that X is convex implies that

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

Note that $x_1 - x_2 \in \Lambda$ because $\phi(x_1) = \phi(x_2)$ and ϕ is linear. Then $\lambda = x_1 - x_2$ is a nonzero element of Λ with $\lambda \in X$. Now suppose $\mathrm{Vol}(X) = 2^n V_\Lambda$. Then for any $\varepsilon > 0$, we have

$$\mathrm{Vol}((1+\varepsilon)X) = (1+\varepsilon)^n \mathrm{Vol}(X) = (1+\varepsilon)^n 2^n V_\Lambda > 2^n V_\Lambda.$$

So what we have just proved shows that there exists a nonzero $\lambda_\varepsilon \in \Lambda$ with $\lambda_\varepsilon \in (1+\varepsilon)X$. In particular, if $\varepsilon \leq 1$ then $\lambda_\varepsilon \in 2X \cap \Lambda$. The set $2X \cap \Lambda$ is compact and discrete, because X is compact and Λ is discrete, and therefore is finite. But as this holds for all $\varepsilon \leq 1$, the sequence $(\lambda_{\frac{1}{n}})_{n \geq 1}$ belongs to the finite set $2X \cap \Lambda$ and so must converge to a point λ. Since Λ is discrete and the $\lambda_{\frac{1}{n}}$ are nonzero so too is λ. As

$$\lambda \in \bigcap_{n \geq 1} \left(1 + \frac{1}{n}\right) X,$$

and X is closed, $\lambda \in X$ as well. Thus we have found a nonzero $\lambda \in L$ with $\lambda \in X$ and we are done. □

We will now work in the setting of number fields. Let K be number field of degree n and let $\sigma_1, \dots, \sigma_n$ be the n distinct $\mathbb{Q}$-embeddings of K into $\overline{\mathbb{Q}}$. In particular, these embeddings are $\mathbb{Q}$-embeddings of K into $\mathbb{C}$. Let r_1 and $2r_2$ be the number of real and complex embeddings respectively (the complex embeddings occur in pairs of two because if σ is a complex embedding then so is its conjugate $\overline{\sigma}$). We call the pair (r_1, r_2) the **signature** of K. In particular,

$$n = r_1 + 2r_2.$$

Choose one representative for each pair of complex embeddings and fix and ordering of $r_1 + r_2$ distinct $\mathbb{Q}$-embedding where $\sigma_1, \dots, \sigma_{r_1+r_2}$ is such that $\sigma_1, \dots, \sigma_{r_1}$ are the real embeddings and $\sigma_{r_1+1}, \dots, \sigma_{r_2}$ are the representative complex embeddings. We define the **canonical embedding** σ of K with resect to $\sigma_1, \dots, \sigma_{r_1+r_2}$ by

$$\sigma : K \to \mathbb{R}^n \qquad \kappa \to (\sigma_1(\kappa), \dots, \sigma_{r_1}(\kappa), \mathrm{Re}(\sigma_{r_1+1}(\kappa)), \mathrm{Im}(\sigma_{r_1+1}(\kappa)), \dots, \mathrm{Re}(\sigma_{r_1+r_2}(\kappa)), \mathrm{Im}(\sigma_{r_1+r_2}(\kappa))).$$

Since $\mathcal{O}_K$ is a free abelian group of rank n by Theorem 2.1, so is $\sigma(\mathcal{O}_K)$. Moreover, as $\mathcal{O}_K$ admits an integral basis for K, we see that $\sigma(\mathcal{O}_K)$ contains a basis of $\mathbb{R}^n$. It follows that $\sigma(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$. Actually, this holds for any fractional ideal $\mathfrak{f}$. As $\mathfrak{f}$ is a free abelian group of rank n, so is $\sigma(\mathfrak{f})$. Letting $\alpha \in \mathfrak{f}$ be nonzero, $\alpha\mathcal{O}_K \subseteq \mathfrak{f}$ and hence $\mathfrak{f}$ contains a basis for K since $\mathcal{O}_K$ admits an integral basis. Therefore $\sigma(\mathfrak{f})$ contains a basis for $\mathbb{R}^n$ and hence $\sigma(\mathfrak{f})$ is a lattice in $\mathbb{R}^n$. We now determine the volume of $\sigma(\mathfrak{f})$ for any fractional ideal $\mathfrak{f}$:

Proposition 6.2. *Let K be a number field with signature (r_1, r_2) and canonical embedding σ. Then*

$$V_{\sigma(\mathcal{O}_K)} = \frac{\sqrt{|\Delta_K|}}{2^{r_2}}.$$

Moreover, for any fractional ideal $\mathfrak{f}$ we have

$$V_{\sigma(\mathfrak{f})} = \mathrm{N}(\mathfrak{f})\frac{\sqrt{|\Delta_K|}}{2^{r_2}}.$$

Proof. Let $\mathfrak{f}$ be a fractional ideal with basis $\{\kappa_1, \dots, \kappa_n\}$. Then the generator matrix P for $\sigma(\mathfrak{f})$ is

$$P = \begin{pmatrix} \sigma_1(\kappa_1) & \cdots & \sigma_{r_1}(\kappa_1) & \mathrm{Re}(\sigma_{r_1+1}(\kappa_1)) & \mathrm{Im}(\sigma_{r_1+1}(\kappa_1)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\kappa_1)) & \mathrm{Im}(\sigma_{r_1+r_2}(\kappa_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\kappa_n) & \cdots & \sigma_{r_1}(\kappa_n) & \mathrm{Re}(\sigma_{r_1+1}(\kappa_n)) & \mathrm{Im}(\sigma_{r_1+1}(\kappa_n)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\kappa_n)) & \mathrm{Im}(\sigma_{r_1+r_2}(\kappa_n)) \end{pmatrix}^t.$$

To compute this determinant, first add an i multiple of the imaginary columns to their corresponding real columns and then apply the identity $\mathrm{Im}(z) = \frac{z-\overline{z}}{2i}$ to the imaginary columns to obtain

$$P' = \begin{pmatrix} \sigma_1(\kappa_1) & \cdots & \sigma_{r_1}(\kappa_1) & \sigma_{r_1+1}(\kappa_1) & \frac{\sigma_{r_1+1}(\kappa_1)-\overline{\sigma_{r_1+1}(\kappa_1)}}{2i} & \cdots & \sigma_{r_1+r_2}(\kappa_1) & \frac{\sigma_{r_1+r_2}(\kappa_1)-\overline{\sigma_{r_1+r_2}(\kappa_1)}}{2i} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\kappa_n) & \cdots & \sigma_{r_1}(\kappa_n) & \sigma_{r_1+1}(\kappa_n) & \frac{\sigma_{r_1+1}(\kappa_n)-\overline{\sigma_{r_1+1}(\kappa_n)}}{2i} & \cdots & \sigma_{r_1+r_2}(\kappa_n) & \frac{\sigma_{r_1+r_2}(\kappa_n)-\overline{\sigma_{r_1+r_2}(\kappa_n)}}{2i} \end{pmatrix}^t.$$

Since P' differs from P by column addition, their determinants are the same. Now multiply the imaginary columns of P' by $-2i$ and then adding the corresponding columns to annihilate the negative terms, we get

$$P'' = \begin{pmatrix} \sigma_1(\kappa_1) & \cdots & \sigma_{r_1}(\kappa_1) & \sigma_{r_1+1}(\kappa_1) & \overline{\sigma_{r_1+1}(\kappa_1)} & \cdots & \sigma_{r_1+r_2}(\kappa_1) & \overline{\sigma_{r_1+r_2}(\kappa_1)} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(\kappa_n) & \cdots & \sigma_{r_1}(\kappa_n) & \sigma_{r_1+1}(\kappa_n) & \overline{\sigma_{r_1+1}(\kappa_n)} & \cdots & \sigma_{r_1+r_2}(\kappa_n) & \overline{\sigma_{r_1+r_2}(\kappa_n)} \end{pmatrix}^t.$$

As P'' differs from P' by column addition and column scaling of which there were r_2 many of factor $-2i$, the determinant of P'' is $(-2i)^{-r_2}$ that of P'. Altogether,

$$|\det(P)| = |\det(P')| = |(-2i)^{-r_2}\det(P'')| = 2^{-r_2}|\det(P'')|.$$

Since the complex embeddings occur in conjugate pairs and $\{\kappa_1, \dots, \kappa_n\}$ is also a basis for K, we see that $P'' = M(\kappa_1, \dots, \kappa_n)$ is the embedding matrix of the basis. Then Proposition 6.1 gives

$$V_{\mathfrak{f}} = \frac{|M(\kappa_1, \dots, \kappa_n)|}{2^{r_2}}.$$

In the case of $\mathcal{O}_K$ and an integral basis $\{\alpha_1, \dots, \alpha_n\}$, we get

$$V_{\sigma(\mathcal{O}_K)} = \frac{\sqrt{|\Delta_K|}}{2^{r_2}},$$

which proves the first statement. It now suffices to show that

$$M(\kappa_1, \dots, \kappa_n) = \mathrm{N}(\mathfrak{f}) M(\alpha_1, \dots, \alpha_n).$$

Since the σ_i are embeddings, this will follow if the absolute value of the determinant of the base change matrix from $\{\alpha_1, \dots, \alpha_n\}$ to $\{\kappa_1, \dots, \kappa_n\}$ is $\mathrm{N}(\mathfrak{f})$. To see this, recall that since $\mathfrak{f}$ is fractional there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

$$\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}.$$

Then $\{\delta\kappa_1, \dots, \delta\kappa_n\}$ is a basis for $\mathfrak{a}$. Now write

$$\delta\kappa_i = \sum_{1 \le i \le n} a_{i,j}\alpha_j,$$

with $a_{i,j} \in \mathbb{Z}$ for $1 \le i, j \le n$. Then $(a_{i,j})_{i,j}$ is the base change matrix from $\{\alpha_1, \dots, \alpha_n\}$ to $\{\delta\kappa_1, \dots, \delta\kappa_n\}$. By Proposition 4.1, it follows that $\mathrm{N}(\mathfrak{a}) = \mathrm{N}(\mathfrak{f})|\,\mathrm{N}(\delta)|$ is the absolute value of determinant of $(a_{i,j})_{i,j}$. By Proposition 4.1 again, the absolute value of the determinant of the base change matrix from $\{\kappa_1, \dots, \kappa_n\}$ to $\{\delta\kappa_1, \dots, \delta\kappa_n\}$ is $|\,\mathrm{N}(\delta)|$. Combining these two facts, $\mathrm{N}(\mathfrak{f})$ is the absolute value of determinant of the base change matrix from $\{\alpha_1, \dots, \alpha_n\}$ to $\{\kappa_1, \dots, \kappa_n\}$ completing the proof. □

7. The Ideal Class Group

Let K be a number field. Recall that the ideal group I_K is the group of fractional ideals of K. We let P_K denote the subgroup of I_K of principal ideals $\alpha\mathcal{O}_K$ for nonzero $\alpha \in K$. Since I_K is abelian, P_K is normal. The **ideal class group** $\mathrm{Cl}(K)$ of K is defined to be the quotient group

$$\mathrm{Cl}(K) = I_K/P_K,$$

of fractional ideals modulo principal ideals. We call an element of $\mathrm{Cl}(K)$ an **ideal class** of K. The **class number** h_K of K is defined by

$$h_K = |\,\mathrm{Cl}(K)|.$$

That is, the class number is the size of the ideal class group. The class number is a measure of how much the ring of integers $\mathcal{O}_K$ fails to be a principal ideal domain. Indeed, if $\mathcal{O}_K$ is a principal ideal domain then every integral ideal is principal and hence every fractional ideal is too (because every fractional ideal $\mathfrak{f}$ is of the form $\frac{1}{\alpha}\mathfrak{a}$ for some integral ideal $\mathfrak{a}$ and nonzero $\alpha \in \mathcal{O}_K$). But then $\mathrm{Cl}(K)$ is the trivial group an hence $h_K = 1$. Conversely, if $h_K = 1$ then every fractional ideal is principal and hence every integral ideal is too so that $\mathcal{O}_K$ is a principal ideal domain. In short, $\mathcal{O}_K$ is a principal ideal domain if and only if $h_K = 1$. Our primary goal is to show that the class number is finite:

Theorem 7.1. *Let K be a number field of degree n and signature (r_1, r_2). Let $X \subseteq \mathbb{R}^n$ be a compact convex symmetric set and set $M = \max_{x \in X}\left(\prod_{1 \le i \le n} |x_i|\right)$ where $x = (x_1, \dots, x_n)$. Then every ideal class contains an integral ideal $\mathfrak{a}$ satisfying*

$$\mathrm{N}(\mathfrak{a}) \le \frac{2^{r_1+r_2}M}{\mathrm{Vol}(X)}\sqrt{|\Delta_K|}.$$

Moreover, the ideal class group $\mathrm{Cl}(K)$ is finite so that the class number h_K is too.

Proof. Let $\mathfrak{f}$ be a fractional ideal, and set

$$\lambda^n = 2^n \frac{V_{\sigma(\mathfrak{f}^{-1})}}{\mathrm{Vol}(X)}.$$

Then by construction,

$$\mathrm{Vol}(\lambda X) = \lambda^n \,\mathrm{Vol}(X) = 2^n V_{\sigma(\mathfrak{f}^{-1})}.$$

By Minkowski's lattice point theorem, there exists a nonzero $\alpha \in \mathfrak{f}^{-1}$ such that $\sigma(\alpha) \in \sigma(\mathfrak{f}^{-1})$ and $\sigma(\alpha) \in \lambda X$. Since $\alpha \in \mathfrak{f}^{-1}$, $\alpha\mathfrak{f} \subseteq \mathcal{O}_K$ so that $\alpha\mathfrak{f}$ is an integral ideal in the same ideal class as $\mathfrak{f}$. Now let $\sigma_1, \ldots, \sigma_n$ be the n distinct $\mathbb{Q}$-embeddings of K into $\overline{K}$. Since the norm is completely multiplicative by Proposition 4.4, we have

$$\mathrm{N}(\alpha\mathfrak{f}) = |\,\mathrm{N}(\alpha)|\,\mathrm{N}(\mathfrak{f}) = \left|\prod_{1\le i\le n} \sigma_i(\alpha)\right| \mathrm{N}(\mathfrak{f}) \le \lambda^n M\,\mathrm{N}(\mathfrak{f}),$$

where in the first equality we have applied Proposition 4.1, in the second we have used Proposition 2.1, and the inequality follows since $\sigma(\alpha) \in \lambda X$. This inequality, our choice of λ^n, and Proposition 6.2 together give

$$\mathrm{N}(\alpha\mathfrak{f}) \le \lambda^n M\,\mathrm{N}(\mathfrak{f}) = 2^n M N(\mathfrak{f}) \frac{V_{\sigma(\mathfrak{f}^{-1})}}{\mathrm{Vol}(X)} = 2^n M \frac{\sqrt{|\Delta_K|}}{2^{r_2}\,\mathrm{Vol}(X)} = \frac{2^{r_1+r_2} M}{\mathrm{Vol}(X)} \sqrt{|\Delta_K|},$$

which proves the first statement since the fractional ideal $\mathfrak{f}$ was arbitrary. We now prove that the class group is finite. By what we have just proved, we can find a complete set of representatives of $\mathrm{Cl}(K)$ consisting of integral ideals of bounded norm. Since the norm is multiplicative by Proposition 4.4, the prime factors of these representatives have bounded norm as well. As we have seen, the norm of a prime integral ideal is exactly the prime p below it. Thus the norms of these prime factors are bounded primes p. As there are finitely many prime integral ideals above any prime p (because $p\mathcal{O}_K$ factors into a product of prime integral ideals and these are exactly the prime integral ideals above p), it follows that these representatives have finitely many prime factors. Altogether this means that there are finitely many representatives. Hence $\mathrm{Cl}(K)$ is finite and so the class number h_K is too. □

We would like to obtain an explicit bound in Theorem 7.1 by making a choice for the set X. To obtain a bound that is not too large, we need to ensure that the volume of X is large while the constant M is small. The following lemma dictates our choice of X and computes its volume:

Lemma 7.1. *Suppose n is a positive integer and write $n = r_1 + 2r_2$ for some nonnegative integers r_1 and r_2. Let $X \subset \mathbb{R}^n$ to be the compact convex symmetric set given by*

$$X = \left\{ x \in \mathbb{R}^n : \sum_{1\le i\le r_1} |x_i| + 2 \sum_{\substack{1\le j\le r_2 \\ j\equiv 1 \pmod 2}} \sqrt{x_{r_1+j}^2 + x_{r_1+j+1}^2} \le n \right\}.$$

Then

$$\mathrm{Vol}(X) = \frac{n^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}.$$

Proof. Making the change of variables $x_{r_1+j} \to u_j \sin(\theta_j)$ and $x_{r_1+j+1} \to u_j \cos(\theta_j)$ for all j gives

$$\mathrm{Vol}(X) = \int_{X'} u_1 \cdots u_{r_2}\, dx_1 \cdots dx_{r_1}\, du_1\theta_1 \cdots du_{r_2}\theta_{r_2},$$

where X' is the region

$$X' = \left\{ (x_1, \ldots, x_{r_1}, u_1, \theta_1, \ldots, u_{r_2}, \theta_{r_2}) : \sum_{1\le i\le r_1} |x_i| + 2 \sum_{1\le j\le r_2} u_j \le n \right\}.$$

Since the integrand is independent of the θ_j, we have

$$\mathrm{Vol}(X) = (2\pi)^{r_2} \int_{X'} u_1 \cdots u_{r_2}\, dx_1 \cdots dx_{r_1}\, du_1 \cdots du_{r_2}.$$

Making the change of variables $u_j \to \frac{u_j}{2}$ for all j and using the fact that the integrand is symmetric in the x_i for all i gives

$$\mathrm{Vol}(X) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \int_{X''} u_1 \cdots u_{r_2}\, dx_1 \cdots dx_{r_1}\, du_1 \cdots du_{r_2}, \tag{3}$$

where X'' is the region

$$X'' = \left\{ (x_1, \ldots, x_{r_1}, u_1, \ldots, u_{r_2}) : \sum_{1 \le i \le r_1} x_i + \sum_{1 \le j \le r_2} u_j \le n \right\}.$$

To compute the remaining integral, for nonnegative integers ℓ and k and $t \ge 0$, we let

$$X''_{\ell,k}(t) = \left\{ (x_1, \ldots, x_\ell, u_1, \ldots, u_k) : \sum_{1 \le i \le \ell} x_i + \sum_{1 \le j \le k} u_j \le t \right\},$$

and set

$$I_{\ell,k}(t) = \int_{X''_{\ell,k}(t)} u_1 \cdots u_\ell\, dx_1 \cdots dx_n\, du_1 \cdots du_k.$$

Then we have to compute $I_{r_1,r_2}(n)$. To this end, the change of variables $x_i \to t x_i$ and $u_j \to t u_j$ for all i and j gives

$$I_{\ell,k}(t) = t^{\ell+2k} I_{\ell,k}(1). \tag{4}$$

Now note that the condition

$$\sum_{1 \le i \le \ell} x_i + \sum_{1 \le j \le k} u_j \le t,$$

is equivalent to

$$\sum_{1 \le i \le \ell-1} x_i + \sum_{1 \le j \le k} u_j \le t - x_i.$$

This fact together with the dominated convergence theorem and Equation (4) gives

$$I_{\ell,k}(1) = \int_0^1 I_{\ell-1,k}(1 - x_\ell)\, dx_\ell = \int_0^1 (1 - x_\ell)^{\ell-1+2k} I_{\ell-1,k}(1)\, dx_\ell = \frac{1}{\ell + 2k} I_{\ell-1,k}(1).$$

Repeating this procedure $\ell - 1$ times results in

$$I_{\ell,k}(1) = \frac{1}{(\ell + 2k) \cdots (2k + 1)} I_{0,k}(1). \tag{5}$$

Similarly, the condition

$$\sum_{1 \le j \le k} u_j \le t,$$

is equivalent to

$$\sum_{1 \le j \le k-1} u_j \le t - u_k.$$

This fact together with the dominated convergence theorem, Equation (4) and the definition of the beta function, together give

$$I_{0,k}(1) = \int_0^1 u_k I_{0,k-1}(1 - u_k)\, du_k = \int_0^1 u_k (1 - u_k)^{2k-2} I_{0,k-1}(1)\, du_k = B(1, 2k-1) I_{0,k-1}(1) = \frac{1}{2k} I_{0,k-1}(1).$$

Repeating this procedure $k-1$ times results in

$$I_{0,k}(1) = \frac{1}{k!}, \tag{6}$$

since $I_{0,0}(1) = 1$. Combining Equations (4) to (6) we find that

$$I_{\ell,k}(t) = t^{\ell+2k}\frac{1}{(\ell+2k)!}.$$

In particular, $I_{r_1,r_2}(n) = \frac{n^n}{n!}$ and from Equation (3) we obtain

$$\mathrm{Vol}(X) = \frac{n^n}{n!}2^{r_1}\left(\frac{\pi}{2}\right)^{r_2},$$

as desired. □

We can now obtain an explicit bound in Theorem 7.1 known as the **Minkowski bound**:

Theorem 7.2 (Minkowski bound)**.** *Let K be a number field of degree n and signature (r_1, r_2). Then every ideal class contains an integral ideal $\mathfrak{a}$ satisfying*

$$\mathrm{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\Delta_K|}.$$

Proof. Choose X in Theorem 7.1 to be

$$X = \left\{ x \in \mathbb{R}^n : \sum_{1\leq i\leq r_1} |x_i| + 2\sum_{\substack{1\leq j\leq r_2 \\ j\equiv 1 \pmod 2}} \sqrt{x_{r_1+j}^2 + x_{r_1+j+1}^2} \leq n \right\},$$

where $x = (x_1, \ldots, x_n)$. Then Lemma 7.1 gives

$$\mathrm{N}(\mathfrak{a}) \leq M\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\Delta_K|},$$

where $M = \max_{x\in X}\left(\prod_{1\leq\ell\leq n}|x_\ell|\right)$. But for all $x \in X$, the arithmetic geometric inequality gives

$$\left(\prod_{1\leq\ell\leq n}|x_\ell|\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{1\leq\ell\leq n}|x_\ell| \leq 1,$$

where the second inequality holds by the definition of X. Hence $M \leq 1$ and this completes the proof. □

As a corollary we can obtain a lower bound for the discriminant of a number field and show that every number field other than $\mathbb{Q}$ has a ramified prime:

Corollary 7.1. *Let K be a number field of degree n. Then*

$$|\Delta_K| \geq \left(\frac{\pi}{4}\right)^{\frac{n}{2}}\frac{n^n}{n!}.$$

In particular, every number field of degree at least 2 contains at least one ramified prime.

Proof. Since the norm of every integral ideal is at least 1, $\pi < 4$, and r_2 is at most n, the desired inequality follows immediately from Minkowski's bound. Now suppose $n \geq 2$. In the case $n = 2$, the lower bound is larger than 1 so that $|\Delta_K|$ is at least 2 for every quadratic number field. As $n^n \geq n!$ for all $n \geq 1$ (which easily follows by induction), $\left(\frac{\pi}{4}\right)^{\frac{n}{2}}\frac{n^n}{n!}$ is an increasing function in n. Therefore $|\Delta_K| \geq 2$ for all $n \geq 2$ so that $|\Delta_K|$ has a prime divisor. Then Theorem 5.1 implies that at least one prime is ramified in K. □

8. Quadratic Number Fields

We will now classify and discuss the structure of quadratic number fields. We first show that quadratic number fields are exactly those where we adjoint the square-root of a fundamental discriminant:

Proposition 8.1. *Every quadratic number field K is of the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d other than 0 or 1.*

Proof. Suppose K is a quadratic number field. In particular, $K/\mathbb{Q}$ is separable so by the primitive element theorem there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. The minimal polynomial $m_\theta(x)$ of θ is of the form

$$m_\theta(x) = x^2 + ax + b,$$

for $a, b \in \mathbb{Q}$. Then the quadratic formula gives

$$\theta = -\frac{a}{2} \pm \frac{\sqrt{q}}{2},$$

where $q = a^2 - 4b \in \mathbb{Q}$. Clearly $q \neq 0$ and $q \neq 1$ for otherwise $\theta \in \mathbb{Q}$. It follows that $K = \mathbb{Q}(\sqrt{q})$. Write $q = \frac{n}{m}$ for relatively prime $n, m \in \mathbb{Z}$ and set $d = m^2 q = nm \in \mathbb{Z}$. Then d is square-free, $d \neq 0$, and $d \neq 1$. Moreover, $\sqrt{d} = m\sqrt{q}$ so that $K = \mathbb{Q}(\sqrt{d})$. □

From Proposition 8.1, we see that the d for a quadratic number field $\mathbb{Q}(\sqrt{d})$ satisfies $d \equiv 1, 2, 3 \pmod 4$ (otherwise d is not square-free). Moreover, any element of a quadratic number field is of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ and for some square-free d other than 0 or 1. We say that a quadratic number field $\mathbb{Q}(\sqrt{d})$ is **real** if $d > 0$ and **imaginary** if $d < 0$. Now $\mathbb{Q}(\sqrt{d})$ is real or imaginary according to if $\sqrt{d}$ is real or purely imaginary so that the two $\mathbb{Q}$-embeddings σ_1 and σ_2 of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{C}$ are

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d} \quad \text{and} \quad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d},$$

because the roots of the minimal polynomial for $\sqrt{d}$ are $\pm\sqrt{d}$. In particular, the signature is $(2, 0)$ or $(0, 1)$ according to if $\mathbb{Q}(\sqrt{d})$ is real or imaginary. In either case, Proposition 2.1 shows that the norm and trace of $\kappa = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ are given by

$$\mathrm{Tr}(\kappa) = 2a \quad \text{and} \quad \mathrm{N}(\kappa) = a^2 - b^2 d.$$

We will now begin describing the ring of integers, discriminant, and the factorization of primes in $\mathbb{Q}(\sqrt{d})$. For simplicity, we write $\mathcal{O}_d = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and $\Delta_d = \Delta_{\mathbb{Q}(\sqrt{d})}$. The ring of integers has a particularly simple description since it is monogenic as the following proposition shows:

Proposition 8.2. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then $\mathbb{Q}(\sqrt{d})$ is monogenic and*

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

Proof. Let $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ be an algebraic integer. If $b = 0$, then $\alpha \in \mathbb{Q}$ and since the only elements of $\mathbb{Q}$ that are algebraic integers are the integers themselves we must have that α is an integer. Now suppose $b \neq 0$. Then the minimal polynomial of α is

$$m_\alpha(x) = x^2 + 2ax + (a^2 - b^2 d) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})).$$

As α is an algebraic integer, $2a \in \mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$ (note that these are the trace and norm of α respectively). In particular, $(2a)^2 + (2b)^2 d \in \mathbb{Z}$ and hence $(2b)^2 \in \mathbb{Z}$ is as well. But as $b \in \mathbb{Q}$, it must be the case that $2b \in \mathbb{Z}$. If $2a = n + 1$ is odd then n is even. We compute

$$a^2 - b^2 d = \left(\frac{n+1}{2}\right)^2 - b^2 d = \frac{n^2 + 2n + 1 + 4b^2 d}{4},$$

and since the right-hand side must be an integer $b \notin \mathbb{Z}$. For if $b \in \mathbb{Z}$, the numerator of the right-hand side is equivalent to 1 modulo 4 because n is even. As $2b \in \mathbb{Z}$ it follows that $2b$ must be odd so set $2b = m + 1$ with m even. Again, we compute

$$a^2 - b^2 d = \left(\frac{n+1}{2}\right)^2 - \left(\frac{m+1}{2}\right)^2 d = \frac{n^2 + 2n + 1 - d(m^2 + 2m + 1)}{4},$$

and since the right-hand side must be an integer the numerator must be divisible by 4. As n and m are even, this is equivalent to $d \equiv 1 \pmod 4$. So we have shown $2a$ or $2b$ is odd if and only if $d \equiv 1 \pmod 4$. Thus if $d \equiv 1 \pmod 4$, we have $a = \frac{a'}{2}$ and $b = \frac{b'}{2}$ for some $a', b' \in \mathbb{Z}$ and hence $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Otherwise, $d \equiv 2, 3 \pmod 4$ (because d is square-free) so that $2a$ and $2b$ are both even, $a, b \in \mathbb{Z}$, and therefore $\alpha \in \mathbb{Z}[\sqrt{d}]$. We have now shown that $\mathcal{O}_d \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and $\mathcal{O}_d \subseteq \mathbb{Z}[\sqrt{d}]$ according to if $d \equiv 1 \pmod 4$ or $d \equiv 2, 3 \pmod 4$ respectively. For the reverse containment, just note that $\sqrt{d}$ is an algebraic integer since its minimal polynomial $m_{\sqrt{d}}(x)$ is

$$m_{\sqrt{d}}(x) = x^2 \pm d,$$

according to if $d < 0$ or $d > 0$. The reverse containment now follows by Proposition 1.1 and that all integers are algebraic integers. □

It follows from Proposition 8.2 that

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\} \quad \text{and} \quad \{1, \sqrt{d}\},$$

are integral bases for $\mathcal{O}_d$ according to if $d \equiv 1 \pmod 4$ or $d \equiv 2, 3 \pmod 4$ respectively. Let us now show that the discriminants quadratic number fields are exactly the fundamental discriminants D other than 1:

Proposition 8.3. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic number field. Then*

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

In particular, the discriminants quadratic number fields are exactly the fundamental discriminants other than 1.

Proof. Let σ_1 and σ_2 be the two $\mathbb{Q}$-embeddings of $\mathbb{Q}(\sqrt{d})$ into $\mathbb{C}$ where σ_1 is the identity and σ_2 is given by sending $\sqrt{d}$ to its conjugate. If $d \equiv 1 \pmod 4$, an integral basis for $\mathcal{O}_d$ is $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$. In this case, the embedding matrix is

$$M\left(1, \frac{1+\sqrt{d}}{2}\right) = \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix},$$

and thus $\Delta_d = d$. If $d \equiv 2, 3 \pmod 4$, an integral basis for $\mathcal{O}_d$ is $\left\{1, \sqrt{d}\right\}$. In this case, the embedding matrix is

$$M(1, \sqrt{d}) = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix},$$

and hence $\Delta_d = 4d$. This proves the first statement and the second statement is clear since d is square-free and not 0 or 1. □

We will now discuss the factorization of a prime p in a quadratic number field $\mathbb{Q}(\sqrt{d})$. Since $\mathbb{Q}(\sqrt{d})$ is a degree 2 extension, Proposition 5.1 implies that p is ramified if and only if it is totally ramified and if p is split but not ramified then it is totally split. In other words, there are three possible cases for how $p\mathcal{O}_d$ factors:

$$p\mathcal{O}_d = \mathfrak{p}, \quad p\mathcal{O}_d = \mathfrak{p}^2, \quad \text{and} \quad p\mathcal{O}_d = \mathfrak{p}\mathfrak{q},$$

according to if p is inert, totally ramified, or totally split. Since $\mathbb{Q}(\sqrt{d})$ is monogenic by Proposition 8.2, we can describe the factorization using the Dedekind-Kummer theorem and connect it to the quadratic character χ_{Δ_d} given by the fundamental discriminant Δ_d:

Proposition 8.4. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic number field and let χ_{Δ_d} be the quadratic character given by the fundamental discriminant Δ_d. Then for any prime p, we have*

$$\chi_{\Delta_d}(p) = \begin{cases} 1 & \text{if } p \text{ is split,} \\ -1 & \text{if } p \text{ is inert,} \\ 0 & \text{if } p \text{ is ramified.} \end{cases}$$

Proof. By Theorem 5.1, p is ramified if and only if p divides $|\Delta_d|$ but this is exactly when $\chi_{\Delta_d}(p) = 0$. Therefore it suffices to prove the cases when p is split and inert. First suppose $d \equiv 1 \pmod 4$ so that $\mathcal{O}_d = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ and $\Delta_d = d$ by Propositions 8.2 and 8.3. The minimal polynomial $m_{\frac{1+\sqrt{d}}{2}}(x)$ for $\frac{1+\sqrt{d}}{2}$ is

$$m_{\frac{1+\sqrt{d}}{2}}(x) = x^2 - x + \frac{1-d}{4},$$

where $\frac{1-d}{4} \in \mathbb{Z}$ because $d \equiv 1 \pmod 4$. The reduction of $m_{\frac{1+\sqrt{d}}{2}}(x)$ modulo p is either irreducible, factors into two distinct linear factors, or is a square, and Dedekind-Kummer theorem implies that this is equivalent to p being inert, split, or ramified accordingly because the prime factorization is unique. First suppose $p \neq 2$. Then from the quadratic formula, $m_{\frac{1+\sqrt{d}}{2}}(x)$ reduces modulo p as

$$m_{\frac{1+\sqrt{d}}{2}}(x) \equiv \left(x - \frac{1+\sqrt{d}}{2}\right)\left(x - \frac{1-\sqrt{d}}{2}\right) \pmod p,$$

if and only if the roots $\frac{1\pm\sqrt{d}}{2}$ are elements of $\mathbb{F}_p$ and is otherwise irreducible. As $p \neq 2$, these factors are distinct. Moreover, $\frac{1\pm\sqrt{d}}{2}$ is an element of $\mathbb{F}_p$ if and only if d is a square modulo p and hence p is split or inert according to if $\chi_d(p) = \pm 1$. Now suppose $p = 2$. Since $m_{\frac{1+\sqrt{d}}{2}}(x)$ has a nonzero linear term with an odd coefficient, it reduces modulo 2 as

$$m_{\frac{1+\sqrt{d}}{2}}(x) \equiv x(x-1) \pmod 2,$$

if and only if $\frac{1-d}{4} \equiv 0 \pmod 2$ and is otherwise irreducible. Clearly these factors are distinct. Now observe $\frac{1-d}{4} \equiv 0 \pmod 2$ is equivalent to $d \equiv 1 \pmod 8$ provided $d > 0$ and $d \equiv 7 \pmod 8$ provided $d < 0$ and thus p is split or inert according to if $\chi_d(2) = \pm 1$. This completes the argument in the case $d \equiv 1 \pmod 4$. Now suppose $d \equiv 2, 3 \pmod 4$ so that $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ and $\Delta_d = 4d$ by Propositions 8.2 and 8.3. The minimal polynomial $m_{\sqrt{d}}(x)$ for $\sqrt{d}$ is

$$m_{\sqrt{d}}(x) = x^2 - d.$$

As $\Delta_d = 4d$, we see that 2 is ramified and therefore we may assume $p \neq 2$. Similarly, the reduction of $m_{\sqrt{d}}(x)$ modulo p is either irreducible, factors into two distinct linear factors, or is a square, and Dedekind-Kummer theorem implies that this is equivalent to p being inert, split, or ramified accordingly because the prime factorization is unique. As $p \neq 2$, the quadratic formula implies that $m_{\sqrt{d}}(x)$ reduces modulo p as

$$m_{\sqrt{d}}(x) \equiv (x - \sqrt{d})(x + \sqrt{d}) \pmod p,$$

if and only if the roots $\pm\sqrt{d}$ are elements of $\mathbb{F}_p$. As $p \neq 2$, these factors are distinct. Moreover, $\sqrt{d}$ is an element of $\mathbb{F}_p$ if and only if d and hence $4d$ are squares modulo p so that p is split or inert according to if $\chi_{4d}(p) = \pm 1$. This completes the verification in the case $d \equiv 2, 3 \pmod 4$. □

From Proposition 8.4, we see that the factorization of primes in $\mathbb{Q}(\sqrt{d})$ is controlled by the quadratic character χ_{Δ_d} attached to the fundamental discriminant Δ_d. In other words, the factorization of p depends completely upon if Δ_d is a square modulo p.