Number fields

Henry Twiss

1 Integrality

Let B/A be an extension of rings. We say that $b \in B$ is *integral* over A if β is the root of a monic polynomial $f(x) \in A[x]$. In other words, β satisfies

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_0 = 0,$$

for some $n \geq 1$ and $\alpha_i \in A$ for $0 \leq i \leq n-1$. We say that B is *integral* over A if every element of B is integral over A. The following proposition shows that integral elements form a ring:

Proposition 1.1. *Let B/A be an extension of rings. Then the finitely many elements $\beta_1, \ldots, \beta_n \in B$ are all integral over A if and only if $A[\beta_1, \ldots, \beta_n]$ is a finitely generated A-module. In particular, the elements of B that are integral over A form a ring.*

Proof. First suppose $\beta \in B$ is integral over A. Then there exists a monic polynomial $f(x) \in A[x]$, of say degree $n \geq 1$, such that $f(\beta) = 0$. Now for any $g(x) \in A[x]$, Euclidean division implies

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

with $q(x), r(x) \in A[x]$ and $\deg(r(x)) < n$. Letting

$$r(x) = \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + a_0,$$

with $\alpha_i \in \mathbb{Z}$ for $0 \leq i \leq n-1$, it follows that

$$g(\beta) = r(\beta) = \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta + \alpha_0.$$

As $g(x)$ was arbitrary, we see that $1, \beta, \ldots, \beta^{n-1}$ generates $A[\beta]$ as an A-module. Now suppose $\beta_1, \ldots, \beta_n \in B$ are all integral over A. We will prove that $A[\beta_1, \ldots, \beta_n]$ is finitely generated as an A-module by induction. Our previous work implies the base case. So assume by induction that $R = A[\beta_1, \ldots, \beta_{n-1}]$ is a finitely generated A-module. Then $R[\beta_n] = A[\beta_1, \ldots, \beta_n]$ is a finitely generated R-module and hence a finitely generated $\mathbb{Z}$-module as well by our induction hypothesis. This proves the forward implication of the first statement. For the reverse implication, suppose $A[\beta_1, \ldots, \beta_n]$ is a finitely generated A-module. Let $\omega_1, \ldots, \omega_r$ be a basis of $A[\beta_1, \ldots, \beta_n]$. Then for any $\beta \in A[\beta_1, \ldots, \beta_n]$, we have

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

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

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

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

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

Thus the determinant of the matrix on the left-hand side must be zero. This shows that β is the root of the characteristic polynomial $\det(xI - (\alpha_{i,j})_{i,j})$ which is a monic polynomial with coefficients in A. Hence β is integral over A. As β was arbitrary, this shows that the elements $\beta_1, \ldots, \beta_n$ are all integral over A and that the sum and product of elements that are integral over A are also integral over A. This proves the reverse implication and the second statement completing the proof. $\square$

Integrality is also transitive via the following statement:

Proposition 1.2. *Let $C/B/A$ be an extension of rings. If C is integral over B and B is integral over A then C is integral over A.*

Proof. Let $\gamma \in C$. Since C is integral over B, we have

$$\gamma^n + \beta_{n-1}\gamma^{n-1} + \cdots + \beta_0 = 0,$$

for some $n \geq 1$ and $\beta_i \in B$ for $0 \leq i \leq n-1$. Set $R = A[\beta_0, \ldots, \beta_{n-1}]$. Then $R[\gamma]$ is a finitely generated R-module and since B is integral over A, Proposition 1.1 implies that $R[\gamma]$ is also a finitely generated A-module. Thus γ is integral over A by Proposition 1.1 again. As γ was arbitrary, C is integral over A. $\square$

In light of Proposition 1.2, we define the *integral closure* $\overline{A}$ of A in B by

$$\overline{A} = \{\beta \in B : \beta \text{ is integral over } A\}.$$

Clearly $A \subseteq \overline{A}$. Moreover, we say that A is *integrally closed* in B if $A = \overline{A}$. As $A \subseteq \overline{A} \subseteq \overline{\overline{A}}$, Proposition 1.2 implies that $\overline{A}$ is automatically integrally closed in B. Now suppose A is an integral domain with field of fractions K. Then we call the integral closure $\overline{A}$ of A in K the *normalization* of A and simply say that A is *integrally closed* if A is equal to its normalization. It turns out that every unique factorization domain is integrally closed:

Lemma 1.3. *Let A be a unique factorization domain with field of fractions K. Then A is integrally closed. In particular, every principal ideal domain is integrally closed.*

Proof. Since every principal ideal domain is a unique factorization domain, the second statement follows immediately from the first. To prove the first statement, let $\kappa \in K$ be such that

$$\kappa^n + \alpha_{n-1}\kappa^{n-1} + \cdots + \alpha_0 = 0,$$

for some $n \geq 1$ and $\alpha_i \in A$ for $0 \leq i \leq n-1$. Since A is a unique factorization domain, we may write $\kappa = \frac{\alpha}{\beta}$ for $\alpha, \beta \in A$ with β nonzero and $(\alpha, \beta) = 1$. Multiplying by β^n and isolating the leading term shows that

$$\alpha^n = -(\alpha_{n-1}\beta\alpha^{n-1} + \cdots + \alpha_0\beta^n).$$

As β divides the right-hand side it divides the left-hand side as well. But then $\beta \mid \alpha$ and hence β is a unit in A because $(\alpha, \beta) = 1$. This means $\kappa \in A$ and so A is integrally closed. $\square$

Despite Lemma 1.3, we will often consider the following more general setting: A is an integrally closed integral domain with field of fractions K, L/K is a finite separable extension, and B is the integral closure of A in L. In this setting, the field of fractions of B has a simple description:

Proposition 1.4. *Let A be an integrally closed integral domain with field of fractions K, L/K be a finite separable extension, and B be the integral closure of A in L. Then every $\lambda \in L$ is of the form*

$$\lambda = \frac{\beta}{\alpha},$$

for some $\beta \in B$ and nonzero $\alpha \in A$. In particular, L is the field of fractions of B. Moreover, $\lambda \in L$ is integral over A if and only if the minimal polynomial $m_\lambda(x)$ of λ over K has coefficients in A.

Proof. As L/K is finite, it is necessarily algebraic so that any $\lambda \in L$ satisfies

$$\alpha\lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_0 = 0,$$

with $\alpha_i \in A$ for $0 \leq i \leq n-1$ and nonzero $\alpha \in A$. We claim that $\alpha\lambda$ is integral over A. Indeed, multiplying the previous identity by α^{n-1} yields

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

where $\alpha'_i = \alpha_i\alpha^{n-1-i}$ for $0 \leq i \leq n-1$, and so $\alpha\lambda$ is the root of a monic polynomial with coefficients in A. Then $\alpha\lambda \in B$ and so $\alpha\lambda = \beta$ for some $\beta \in B$ which is equivalent to $\lambda = \frac{\beta}{\alpha}$. As $A \subseteq B$, this also implies that L is the field of fractions of B. For the last statement, suppose $\lambda \in L$. If the minimal polynomial $m_\lambda(x)$ of λ over K has coefficients in A then λ is automatically integral over A (since minimal polynomials are monic). So suppose λ is an integral over A so that λ is a root of a monic polynomial $f(x) \in A[x]$. Then $m_\lambda(x)$ divides $f(x)$ in $A[x]$ and thus all of the roots of $m_\lambda(x)$ are integral over A too. By Vieta's formulas, the coefficients of $m_\kappa(x)$ integral over A as well. But then $m_\kappa(x) \in A[x]$. This completes the proof. $\square$

We are now ready to introduce number fields. A *number field* K is a finite extension of $\mathbb{Q}$. That is, K is a finite dimensional $\mathbb{Q}$-vector space. In particular, $K/\mathbb{Q}$ is a finite separable extension since $\mathbb{Q}$ is perfect so that the primitive element theorem applies. Moreover, $K/\mathbb{Q}$ is Galois if and only if it is normal. We say that the *degree* of K is $[K:\mathbb{Q}]$ which is simply the degree of K as a $\mathbb{Q}$-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*. We define the *ring of integers* $\mathcal{O}_K$ of K to be the integral closure of $\mathbb{Z}$ in K. In other words,

$$\mathcal{O}_K = \{\kappa \in K : \kappa \text{ is integral over } \mathbb{Z}\}.$$

Any $\alpha \in \mathcal{O}_K$ is called an *algebraic integer*. Then α is an algebraic integer if and only if it is the root of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Remark 1.5. By Lemma 1.3, $\mathbb{Z}$ is integrally closed and therefore the ring of integers for the number field $\mathbb{Q}$ is exactly $\mathbb{Z}$.

Let K be a number field of degree n. It follows from Proposition 1.4 that K is the field of fractions of $\mathcal{O}_K$ and every $\kappa \in K$ is of the form

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

for some $\alpha \in \mathcal{O}_K$ and nonzero $a \in \mathbb{Z}$. Moreover, $\kappa \in K$ is an algebraic integers if and only if the minimal polynomial $m_\kappa(x)$ of κ over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

2 Traces and Norms

We will now introduce norms and traces of free modules. Let B/A be an extension of rings such that B is a free A-module of rank n. Then the *trace* and *norm* of B over A, denoted $\mathrm{Tr}_{B/A}$ and $\mathrm{N}_{B/A}$ respectively, are defined by

$$\mathrm{Tr}_{B/A}(\beta) = \mathrm{trace}(T_\beta) \quad \text{and} \quad \mathrm{N}_{B/A}(\beta) = \det(T_\beta),$$

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

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

for all $x \in B$. That is, T_β is the multiplication by β map. Letting $f_\beta(x)$ denote the characteristic polynomial of T_β, we have

$$f_\beta(x) = \det(xI - T_\beta) = x^n - \alpha_{n-1}x^{n-1} + \cdots + (-1)^n\alpha_0,$$

with $\alpha_i \in A$ for $0 \le i \le n-1$. Then the trace and the norm are given by

$$\mathrm{Tr}_{B/A}(\beta) = \alpha_{n-1} \quad \text{and} \quad \mathrm{N}_{B/A}(\beta) = \alpha_0, \tag{1}$$

and therefore take values in A. Moreover, we have

$$\mathrm{Tr}_{B/A}(\alpha\beta) = \alpha\,\mathrm{Tr}_{B/A}(\beta) \quad \text{and} \quad \mathrm{N}_{B/A}(\alpha\beta) = \alpha^n\,\mathrm{N}_{B/A}(\beta),$$

for all $\alpha \in A$ because $T_{\alpha\lambda} = \alpha T_\lambda$. Also note that $T_{\beta+\gamma} = T_\beta + T_\gamma$ and $T_{\beta\gamma} = T_\beta T_\gamma$ for all $\beta, \gamma \in B$. Moreover, recall that the trace and determinant of a linear map are additive and multiplicative respectively with respect to direct sums (since any matrix representation of the linear map becomes block upper triangular). Then if $B = B_1 \oplus B_2$ and $\beta = \beta_1 + \beta_2$ with $\beta_1 \in B_1$ and $\beta_2 \in B_2$, we have

$$\mathrm{Tr}_{B/A}(\beta) = \mathrm{Tr}_{B_1/A}(\beta_1) + \mathrm{Tr}_{B_2/A}(\beta_2) \quad \text{and} \quad \mathrm{N}_{B/A}(\beta) = \mathrm{N}_{B_1/A}(\beta_1)\,\mathrm{N}_{B_2/A}(\beta_2). \tag{2}$$

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, $\mathrm{N}_{L/K}(\lambda) = 0$ if and only if $\lambda = 0$ because otherwise T_λ has inverse $T_{\lambda^{-1}}$ and hence nonzero determinant. Therefore we obtain homomorphisms

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

When L/K is also separable, we can derive alternative descriptions of the trace and norm of L/K. This additional assumption is weak because we are mostly interested in 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/K so that $L = K(\theta)$ and sending θ to one of its conjugate roots in the minimal polynomial $m_\theta(x)$ of θ over K). In other words, there are n elements of $\mathrm{Hom}_K(L, \overline{K})$. Moreover, we prove the following proposition:

Proposition 2.1. *Let L/K be a degree n separable extension and let σ run over the elements of $\mathrm{Hom}_K(L, \overline{K})$. For any $\lambda \in L$, the characteristic polynomial $f_\lambda(x)$ of T_λ over K is a power of the minimal polynomial $m_\lambda(x)$ of λ over K and satisfies*

$$f_\lambda(x) = \prod_\sigma (x - \sigma(\lambda)).$$

We also have

$$\mathrm{Tr}_{L/K}(\lambda) = \sum_\sigma \sigma(\lambda) \quad \textit{and} \quad \mathrm{N}_{L/K}(\lambda) = \prod_\sigma \sigma(\lambda).$$

Moreover, if L/K is Galois and $\lambda_1, \ldots, \lambda_n$ are the conjugates of λ then

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

Proof. Write

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

with $\kappa_i \in K$ for $0 \le i \le m-1$ (necessarily m is the degree of $K(\lambda)/K$) and let d be the degree of $L/K(\lambda)$. We first show that $f_\lambda(x)$ is a power of $m_\lambda(x)$. In particular, we claim

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

To see this, recall that $1, \lambda, \ldots, \lambda^{n-1}$ is a basis of $K(\lambda)/K$. 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 $m_\lambda(x)$ 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 $m_\lambda(x)$ and hence the characteristic polynomial is $m_\lambda(x)$ 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 $m_\lambda(x)$ and there are m elements of $\mathrm{Hom}_K(K(\lambda), \overline{K})$. Then the elements of $\mathrm{Hom}_K(L, \overline{K})$ are partitioned into m many equivalence classes each of size d (because $L/K(\lambda)$ is degree d) where σ and σ' are in the same class if and only if $\sigma(\lambda) = \sigma'(\lambda)$. In particular, a complete set of representatives is given by the τ. But then

$$f_\lambda(x) = m_\lambda(x)^d = \left(\prod_\tau (x - \tau(\lambda))\right)^d = \prod_\sigma (x - \sigma(\lambda)),$$

which proves the first statement. The formulas for the trace and norm follow from Vieta's formulas and Equation (1) which proves the second statement. Now suppose L/K is Galois. Then $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \overline{K})$. Therefore the conjugates of λ are exactly the images of λ under these K-embeddings and the last claim follows. □

As an application of Proposition 2.1, we can show how the field trace and field norm act when A is an integrally closed integral domain with field of fractions K, L/K is a finite separable extension, and B is the integral closure of A in L:

Proposition 2.2. *Let A be an integrally closed integral domain with field of fractions K, L/K be a finite separable extension, and B be the integral closure of A in L. If $\beta \in B$ then the trace and norm of β are in A.*

Proof. By Proposition 1.4, the minimal polynomial $m_\beta(x)$ of β over K has coefficients in A. By Proposition 2.1, the characteristic polynomial $f_\beta(x)$ is a power of $m_\beta(x)$ and hence $f_\beta(x)$ has coefficients in A too. From Equation (1) we conclude that the trace and norm of β are in A. □

We can also classify the units of B in terms of the units of A:

Proposition 2.3. *Let A be an integrally closed integral domain with field of fractions K, L/K be a finite separable extension, and B be the integral closure of A in L. Then $\beta \in B$ is a unit if and only if $\mathrm{N}_{L/K}(\beta) \in A$ is a unit*

Proof. First suppose $\beta \in B$ is a unit. Then $\frac{1}{\beta} \in B$ and so

$$\mathrm{N}_{L/K}(\beta)\,\mathrm{N}_{L/K}\left(\frac{1}{\beta}\right) = \mathrm{N}_{L/K}(1) = 1.$$

By Proposition 2.2, $\mathrm{N}_{L/K}(\beta), \mathrm{N}_{L/K}\left(\frac{1}{\beta}\right) \in A$ and hence $\mathrm{N}_{L/K}(\beta)$ is a unit. Now suppose $\mathrm{N}_{L/K}(\beta) \in A$ is a unit. By Proposition 1.4, the minimal polynomial $m_\beta(x)$ of β over K has coefficients in A. Moreover, Equation (1) and Proposition 2.1 together imply that the constant term is a unit because $\mathrm{N}_{L/K}(\beta)$ is. Letting the degree of $m_\beta(x)$ be m, we have shown that

$$m_\beta(x) = x^m + \alpha_{m-1}x^{m-1} + \cdots + \alpha,$$

with $\alpha_i \in A$ for $1 \le i \le m-1$ and $\alpha \in A$ a unit. Dividing $m_\beta(\beta)$ by β^m, we find that $\frac{1}{\beta}$ is a root of the polynomial

$$f(x) = \alpha x^m + \alpha_1 x^{m-1} + \cdots + 1.$$

Multiplying by $\frac{1}{\alpha}$, it follows that $\frac{1}{\beta}$ is a root of a monic polynomial with coefficients in A. Hence $\frac{1}{\beta} \in B$ and thus β is a unit. □

Having introduced traces and norms, we discuss discriminants of free modules. Let B/A be an extension of rings such that B is a free A-module of rank n. If $\beta_1, \ldots, \beta_n$ is a basis for B, we define its *trace matrix* $\mathrm{Tr}_{B/A}(\beta_1, \ldots, \beta_n)$ by

$$\mathrm{Tr}_{B/A}(\beta_1, \ldots, \beta_n) = \begin{pmatrix} \mathrm{Tr}_{B/A}(\beta_1\beta_1) & \cdots & \mathrm{Tr}_{B/A}(\beta_1\beta_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{B/A}(\beta_n\beta_1) & \cdots & \mathrm{Tr}_{B/A}(\beta_n\beta_n) \end{pmatrix}.$$

The trace matrix will play a prominent role in the theory. Most importantly is the *discriminant* $d_{B/A}(\beta_1, \ldots, \beta_n)$ of $\beta_1, \ldots, \beta_n$ defined by

$$d_{B/A}(\beta_1, \ldots, \beta_n) = \det(\mathrm{Tr}_{B/A}(\beta_1, \ldots, \beta_n)).$$

Equivalently, the discriminant is the determinant of the trace matrix. In particular, the discriminant $d_{B/A}(\beta_1, \ldots, \beta_n)$ is an element of A. It is also independent of the choice of basis up to elements of $(A^*)^2$. For if $\beta_1', \ldots, \beta_n'$ is another basis, we have

$$\beta_i' = \sum_{1 \le j \le m} \alpha_{i,j}\beta_j,$$

with $\alpha_{i,j} \in A$ for $1 \le i, j \le n$. Then $(\alpha_{i,j})_{i,j}$ is the base change matrix from $\beta_1, \ldots, \beta_n$ to $\beta_1', \ldots, \beta_n'$ and so has nonzero determinant. Thus $\det((\alpha_{i,j})_{i,j}) \in A^*$. Moreover,

$$\mathrm{Tr}_{B/A}(\beta_1', \ldots, \beta_n') = (\alpha_{i,j})_{i,j}\,\mathrm{Tr}_{B/A}(\beta_1, \ldots, \beta_n)(\alpha_{i,j})_{i,j}^t,$$

which, upon taking the determinant, shows that

$$d_{B/A}(\beta_1', \dots, \beta_n') = \det((\alpha_{i,j})_{i,j})^2 d_{B/A}(\beta_1, \dots, \beta_n), \tag{3}$$

as claimed. Accordingly, we define the *discriminant* $d_A(B)$ of B/A to be the coset in $A/(A^*)^2$ represented by any discriminant $d_{B/A}(\beta_1, \dots, \beta_n)$. In other words,

$$d_A(B) = d_{B/A}(\beta_1, \dots, \beta_n)(A^*)^2.$$

This is well-defined by Equation (3). In particular, $d_A(B) = 0$ is independent of the choice of representative. The discriminant is also multiplicative with respect to direct sums:

Proposition 2.4. *Let B/A be an extension of rings such that B is a free A-module of rank n. Suppose we have a direct sum decomposition*

$$B = B_1 \oplus B_2,$$

for free A-modules B_1 and B_2 of ranks n_1 and n_2 respectively. Also let $\beta_{1,1}, \dots, \beta_{n_1,1}$ and $\beta_{1,2}, \dots, \beta_{n_2,2}$ be bases of B_1 and B_2 respectively. Then $\beta_{1,1}, \dots, \beta_{n_1,1}, \beta_{1,2}, \dots, \beta_{n_2,2}$ is a basis of B with

$$d_{B/A}(\beta_{1,1}, \dots, \beta_{n_1,1}, \beta_{1,2}, \dots, \beta_{n_2,2}) = d_{B_1/A}(\beta_{1,1}, \dots, \beta_{n_1,1}) d_{B_2/A}(\beta_{1,2}, \dots, \beta_{n_2,2}).$$

Proof. Clearly $\beta_{1,1}, \dots, \beta_{n_1,1}, \beta_{1,2}, \dots, \beta_{n_2,2}$ is a basis for B. We also have $\beta_{i,1}\beta_{j,2} = 0$ for all $1 \le i \le n_1$ and $1 \le j \le n_2$. It follows that $d_{B/A}(\beta_{1,1}, \dots, \beta_{n_1,1}, \beta_{1,2}, \dots, \beta_{n_2,2})$ is the determinant of the block diagonal matrix

$$\begin{pmatrix} \mathrm{Tr}_{B/A}(\beta_{1,1}, \dots, \beta_{n_1,1}) & \\ & \mathrm{Tr}_{B/A}(\beta_{1,2}, \dots, \beta_{n_2,2}) \end{pmatrix}.$$

Moreover, Equation (2) implies

$$\mathrm{Tr}_{B/A}(\beta_1) = \mathrm{Tr}_{B_1/A}(\beta_1) \quad \text{and} \quad \mathrm{Tr}_{B/A}(\beta_2) = \mathrm{Tr}_{B_2/A}(\beta_2)$$

for any $\beta_1 \in B_1$ and $\beta_2 \in B_2$ since multiplication by β_1 and β_2 annihilate B_2 and B_1 respectively. But then the block diagonal matrix above is equal to

$$\begin{pmatrix} \mathrm{Tr}_{B_1/A}(\beta_{1,1}, \dots, \beta_{n_1,1}) & \\ & \mathrm{Tr}_{B_2/A}(\beta_{1,2}, \dots, \beta_{n_2,2}) \end{pmatrix}.$$

The determinant of this matrix is $d_{B_1/A}(\beta_{1,1}, \dots, \beta_{n_1,1}) d_{B_2/A}(\beta_{1,2}, \dots, \beta_{n_2,2})$ which completes the proof. $\square$

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

Lemma 2.5. *Let L/K be a finite separable extension. Then the map*

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

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 of any basis for L/K never vanishes:

Proposition 2.6. *Let L/K be a degree n separable extension and let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K. Then $d_{L/K}(\lambda_1, \ldots, \lambda_n) \neq 0$.*

Proof. Suppose by contradiction that $d_{L/K}(\lambda_1, \ldots, \lambda_n) = 0$. Then the matrix $\mathrm{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ is not invertible. Hence there exists $\kappa_i \in K$ for $1 \leq i \leq n$ such that

$$\mathrm{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n) \begin{pmatrix} \kappa_1 \\ \vdots \\ \kappa_n \end{pmatrix} = \mathbf{0}.$$

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/K, 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 2.5. Hence $d_{L/K}(\lambda_1, \ldots, \lambda_n) \neq 0$ as desired. □

In addition to the discriminant $d_{L/K}(\lambda_1, \ldots, \lambda_n)$ never vanishing, we can also write it in an alternative form. To do this, we define the *embedding matrix* $M(\lambda_1, \ldots, \lambda_n)$ of the basis $\lambda_1, \ldots, \lambda_n$ by

$$M(\lambda_1, \ldots, \lambda_n) = \begin{pmatrix} \sigma_1(\lambda_1) & \cdots & \sigma_1(\lambda_n) \\ \vdots & & \vdots \\ \sigma_n(\lambda_1) & \cdots & \sigma_n(\lambda_n) \end{pmatrix},$$

where $\sigma_1, \ldots, \sigma_n$ are the elements of $\mathrm{Hom}_K(L, \overline{K})$. Then we have the following result:

Proposition 2.7. *Let L/K be a degree n separable extension. Then for any basis $\lambda_1, \dots, \lambda_n$ of L/K, we have*

$$d_{L/K}(\lambda_1, \dots, \lambda_n) = \det(M(\lambda_1, \dots, \lambda_n))^2.$$

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

$$\begin{aligned}
\det(M(\lambda_1, \dots, \lambda_n))^2 &= \det(M(\lambda_1, \dots, \lambda_n)^t M(\lambda_1, \dots, \lambda_n)) \\
&= \det\left(\left(\sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(\lambda_i)\sigma(\lambda_j)\right)_{i,j}\right) \\
&= \det\left(\left(\sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(\lambda_i\lambda_j)\right)_{i,j}\right) \\
&= \det(\mathrm{Tr}_{L/K}(\lambda_1, \dots, \lambda_n)) \\
&= d_{L/K}(\lambda_1, \dots, \lambda_n),
\end{aligned}$$

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

When the degree n separable extension L/K admits a basis of the form $1, \lambda, \dots, \lambda^{n-1}$ (in fact such a basis always exists by choosing λ to be a primitive element for L/K) $d_{L/K}(1, \lambda, \dots, \lambda^{n-1})$ can be easily computed. Indeed, the embedding matrix becomes

$$M(1, \lambda, \dots, \lambda^{n-1}) = \begin{pmatrix} 1 & \sigma_1(\lambda) & \cdots & \sigma_1(\lambda)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \sigma_n(\lambda) & \cdots & \sigma_n(\lambda)^{n-1} \end{pmatrix},$$

which is a Vandermonde matrix. Then

$$d_{L/K}(1, \lambda, \dots, \lambda^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\lambda) - \sigma_j(\lambda))^2, \tag{4}$$

which is the square of the Vandermonde determinant of $M(1, \lambda, \dots, \lambda^{n-1})$, by Proposition 2.7. In any case, discriminants of bases are useful because of the following lemma:

Lemma 2.8. *Let A be an integrally closed integral domain with field of fractions K, L/K be a degree n separable extension, and B be the integral closure of A in L. If $\lambda_1, \dots, \lambda_n$ is a basis for L/K that is contained in B then*

$$d_{L/K}(\lambda_1, \dots, \lambda_n)B \subseteq A\lambda_1 + \cdots + A\lambda_n.$$

Proof. Since $\lambda_1, \ldots, \lambda_n$ is a basis, we may write $\beta = \kappa_1\lambda_1 + \cdots + \kappa_n\lambda_n$ for any $\beta \in B$. Linearity of the trace implies

$$\sum_{1 \le j \le n} \kappa_j \operatorname{Tr}_{L/K}(\lambda_i\lambda_j) = \operatorname{Tr}_{L/K}(\lambda_i\beta),$$

for $1 \le i \le n$. These n equations are equivalent to the identity

$$\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n) \begin{pmatrix} \kappa_1 \\ \vdots \\ \kappa_n \end{pmatrix} = \begin{pmatrix} \operatorname{Tr}_{L/K}(\beta\lambda_1) \\ \vdots \\ \operatorname{Tr}_{L/K}(\beta\lambda_n) \end{pmatrix}.$$

Multiplying on the left by the adjugate $\operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n))$ of $\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ and recalling that a matrix times its adjugate is its determinant times the identity, we see that

$$d_{L/K}(\lambda_1, \ldots, \lambda_n) \begin{pmatrix} \kappa_1 \\ \vdots \\ \kappa_n \end{pmatrix} = \operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)) \begin{pmatrix} \operatorname{Tr}_{L/K}(\beta\lambda_1) \\ \vdots \\ \operatorname{Tr}_{L/K}(\beta\lambda_n) \end{pmatrix}.$$

Since $\lambda_1, \ldots, \lambda_n$ is a basis for L/K that is contained in B, the matrix $\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ has entries in A by Proposition 2.2 and therefore $\operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n))$ does too. Moreover, Proposition 2.2 again implies $\operatorname{Tr}_{L/K}(\beta\lambda_i) \in A$ for all i. So the right-hand side has entires in A and hence the left-hand side must as well. This means $d_{L/K}(\lambda_1, \ldots, \lambda_n)\kappa_i \in A$ for all i. But then

$$d_{L/K}(\lambda_1, \ldots, \lambda_n)B \subseteq A\lambda_1 + \cdots + A\lambda_n,$$

as desired. □

Again suppose A is an integrally closed integral domain with field of fractions K, L/K is a degree n separable extension, and B is the integral closure of A in L. We say that $\beta_1, \ldots, \beta_n$ is an *integral basis* for B/A if $\beta_1, \ldots, \beta_n$ is such that

$$B = A\beta_1 + \cdots + A\beta_n.$$

Equivalently, B is a free A-module of rank n. An integral basis is necessarily a basis for L/K by Proposition 1.4. However, an integral basis need not always exist. For if $\lambda_1, \ldots, \lambda_n$ is a basis of L/K, Proposition 1.4 implies that we can multiply by a nonzero element of A to ensure that this basis is contained in B. However, $\lambda_1, \ldots, \lambda_n$ need not also be a basis of B as an A-module. Nevertheless, if A is a principal ideal domain then we can ensure the existence of an integral basis:

Theorem 2.9. *Let A be a principal ideal domain with field of fractions K, let L/K be a degree n separable extension, and let B be the integral closure of A in L. Then B admits an integral basis over A. Moreover, every finitely generated nonzero B-submodule of L is a free A-module of rank n.*

Proof. A is integrally closed by Lemma 1.3. Let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K. By Proposition 1.4 we may multiply by a nonzero element of A, if necessary, to ensure that this basis belongs to B. Then Lemma 2.8 implies

$$d_{L/K}(\lambda_1, \ldots, \lambda_n)B \subseteq A\lambda_1 + \cdots + A\lambda_n.$$

Since $A\lambda_1 + \cdots + A\lambda_n$ is a free A-module of rank n and A is a principal ideal domain, it follows from the structure theorem of finitely generated modules over principal ideal domains that B is also a free A-module of rank at most n. But any basis for B as an A-module must also be a basis for L/K by Proposition 1.4. Hence the rank is exactly n and B admits an integral basis over A which proves the first statement. Now suppose M is a nonzero B-submodule of L and let $\omega_1, \ldots, \omega_r$ be generators. By Proposition 1.4 again we may multiply by a nonzero element of A, if necessary, to ensure that these generators belong to B. But then

$$d_{L/K}(\omega_1, \ldots, \omega_n)M \subseteq d_{L/K}(\omega_1, \ldots, \omega_n)B.$$

By the structure theorem of finitely generated modules over principal ideal domains again, M is a free A-module of rank at most n. To see that the rank is at least n, let $\alpha \in M$ be nonzero and, as before, let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K that is contained in B. Then $\alpha\lambda_1, \ldots, \alpha\lambda_n$ is a basis for L/K contained in M. Thus the rank of M is at least n, and in particular it must be n. This completes the proof. $\square$

Recall that if L_1/K and L_2/K are finite separable extensions then the composite L of L_1 and L_2 is such that L/K is also a finite separable extension. Integral bases behave well with respect to composite fields provided the fields are linearly disjoint:

Proposition 2.10. *Let A be an integrally closed integral domain with field of fractions K, L_1/K and L_2/K be degree n_1 and n_2 separable extensions respectively, and B_1 and B_2 be the integral closures of A in L_1 and L_2 respectively. Suppose L_1 and L_2 are linearly disjoint over K in $\overline{K}$ and that B_1 and B_2 admit integral bases $\beta_{1,1}, \ldots, \beta_{n_1,1}$ and $\beta_{1,2}, \ldots, \beta_{n_2,2}$ over A with*

$$\alpha_1 d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1}) + \alpha_2 d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2}) = 1,$$

for some $\alpha_1, \alpha_2 \in A$. Let L be the composite of L_1 and L_2 and let B be the integral closure of A in L. Then $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is an integral basis for B over A with

$$\delta_{L/K}(\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}) = d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})^{n_2} d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})^{n_1}.$$

In particular,

$$B = B_1 B_2.$$

Proof. The last statement clearly follows from the first so we will start by proving that $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is an integral basis for B over A. Since L_1 and L_2 are linearly disjoint over K in $\overline{K}$, it must be that $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is a basis for L as a K-vector space. Therefore any $\lambda \in B$ is of the form

$$\lambda = \sum_{\substack{1 \leq i \leq n_1 \\ 1 \leq j \leq n_i}} \kappa_{i,j}\beta_{i,1}\beta_{j,2},$$

for some $\kappa_{i,j} \in K$ for $1 \leq i \leq n_1$ and $1 \leq j \leq n_2$. Then we need to show that $\kappa_{i,j} \in A$ for all i and j. Now let

$$\alpha_{i,2} = \sum_{1 \leq j \leq n_2} \kappa_{i,j}\beta_{j,2} \quad \text{and} \quad \alpha_{j,1} = \sum_{1 \leq i \leq n_1} \kappa_{i,j}\beta_{i,1},$$

for all i and j so that

$$\lambda = \sum_{1 \leq i \leq n_1} \alpha_{i,2}\beta_{i,1} \quad \text{and} \quad \lambda = \sum_{1 \leq j \leq n_2} \alpha_{j,1}\beta_{j,2}.$$

In particular, $\alpha_{i,2} \in L_2$ and $\alpha_{j,1} \in L_1$. By linear disjointness, we have

$$\mathrm{Hom}_K(L, \overline{K}) \cong \mathrm{Hom}_K(L_1, \overline{K}) \times \mathrm{Hom}_K(L_2, \overline{K}).$$

So letting $\sigma_{1,1}, \ldots, \sigma_{n_1,1}$ and $\sigma_{1,2}, \ldots, \sigma_{n_2,2}$ be the elements of $\mathrm{Hom}_K(L_1, \overline{K})$ and $\mathrm{Hom}_K(L_2, \overline{K})$ respectively, $\sigma_{1,1}\sigma_{1,2}, \ldots, \sigma_{n_1,1}\sigma_{n_2,2}$ are the elements of $\mathrm{Hom}_K(L, \overline{K})$. In particular, we may view $\sigma_{1,1}, \ldots, \sigma_{n_1,1}$ and $\sigma_{1,2}, \ldots, \sigma_{n_2,2}$ as elements of $\mathrm{Hom}_K(L, \overline{K})$ that act as the identity on L_2 and L_1 respectively. Then the n_1 and n_2 equations

$$\sum_{1 \leq k \leq n_1} \sigma_{i,1}(\beta_{k,1})\alpha_{k,2} = \sigma_{i,1}(\lambda) \quad \text{and} \quad \sum_{1 \leq k \leq n_2} \sigma_{j,2}(\beta_{k,2})\alpha_{k,1} = \sigma_{j,2}(\lambda),$$

respectively are equivalent to the identities

$$M(\beta_{1,1}, \ldots, \beta_{n_1,1}) \begin{pmatrix} \alpha_{1,2} \\ \vdots \\ \alpha_{n_1,2} \end{pmatrix} = \begin{pmatrix} \sigma_{1,1}(\lambda) \\ \vdots \\ \sigma_{n_1,1}(\lambda) \end{pmatrix} \quad \text{and} \quad M(\beta_{1,2}, \ldots, \beta_{n_2,2}) \begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{n_2,1} \end{pmatrix} = \begin{pmatrix} \sigma_{1,2}(\lambda) \\ \vdots \\ \sigma_{n_2,2}(\lambda) \end{pmatrix},$$

respectively. Multiplying on the left by the adjugates $\mathrm{adj}(M(\beta_{1,1}, \ldots, \beta_{n_1,1}))$ and $\mathrm{adj}(M(\beta_{1,2}, \ldots, \beta_{n_2,2}))$ of $M(\beta_{1,1}, \ldots, \beta_{n_1,1})$ and $M(\beta_{1,2}, \ldots, \beta_{n_2,2})$ respectively and recalling that a matrix times its adjugate is its determinant times the identity, we obtain

$$\det(M(\beta_{1,1}, \ldots, \beta_{n_1,1})) \begin{pmatrix} \alpha_{1,2} \\ \vdots \\ \alpha_{n_1,2} \end{pmatrix} = \mathrm{adj}(M(\beta_{1,1}, \ldots, \beta_{n_1,1})) \begin{pmatrix} \sigma_{1,1}(\lambda) \\ \vdots \\ \sigma_{n_1,1}(\lambda) \end{pmatrix},$$

and

$$\det(M(\beta_{1,2}, \ldots, \beta_{n_2,2})) \begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{n_2,1} \end{pmatrix} = \mathrm{adj}(M(\beta_{1,2}, \ldots, \beta_{n_2,2})) \begin{pmatrix} \sigma_{1,2}(\lambda) \\ \vdots \\ \sigma_{n_2,2}(\lambda) \end{pmatrix}.$$

Since $\lambda \in B$, we have $\sigma_{i,1}(\lambda) \in B$ and $\sigma_{j,2}(\beta) \in B$ for all i and j. Moreover, $M(\beta_{1,1}, \ldots, \beta_{n_1,1})$ and $M(\beta_{1,2}, \ldots, \beta_{n_2,2})$ have entries in B and thus $\mathrm{adj}(M(\beta_{1,1}, \ldots, \beta_{n_1,1}))$ and $\mathrm{adj}(M(\beta_{1,2}, \ldots, \beta_{n_2,2}))$ do too. This means the two right-hand sides have entries in B and so the two left-hand sides must as well. It follows from this fact and Proposition 2.7 that $d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})\alpha_{i,2} \in B$ and $d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})\alpha_{j,1} \in B$ for all i and j. But as $d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})$ and $d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})$ are in A, $\alpha_{i,2} \in L_2$, and $\alpha_{j,1} \in L_1$, we find that $d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})\alpha_{i,2} \in B_2$ and $d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})\alpha_{j,1} \in B_1$. Expanding $\alpha_{i,2}$ and $\alpha_{j,1}$ shows that $d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})\kappa_{i,j} \in A$ and $d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})\kappa_{i,j} \in A$. From the identity

$$k_{i,j} = k_{i,j}(\alpha_1 d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1}) + \alpha_2 d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})),$$

we conclude $k_{i,j}$ is in A as desired. This proves $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is an integral basis for B over A. We will now compute the discriminant of this basis. As $\sigma_{1,1}\sigma_{1,2}, \ldots, \sigma_{n_1,1}\sigma_{n_2,2}$ are the elements of $\mathrm{Hom}_K(L, \overline{K})$, we have

$$M(\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}) = \begin{pmatrix} \sigma_{1,1}(\beta_{1,1})\sigma_{1,2}(\beta_{1,2}) & \cdots & \sigma_{1,1}(\beta_{n_1,1})\sigma_{1,2}(\beta_{n_2,2}) \\ \vdots & & \vdots \\ \sigma_{n_1,1}(\beta_{1,1})\sigma_{n_2,2}(\beta_{1,2}) & \cdots & \sigma_{n_1,1}(\beta_{n_1,1})\sigma_{n_2,2}(\beta_{n_2,2}) \end{pmatrix}.$$

This latter matrix admits the block factorization

$$\begin{pmatrix} M(\beta_{1,1}, \ldots, \beta_{n_1,1}) & & \\ & \ddots & \\ & & M(\beta_{1,1}, \ldots, \beta_{n_1,1}) \end{pmatrix} \begin{pmatrix} I\sigma_{1,2}(\beta_{1,2}) & \cdots & I\sigma_{1,2}(\beta_{n_2,2}) \\ \vdots & & \vdots \\ I\sigma_{n_2,2}(\beta_{1,2}) & \cdots & I\sigma_{n_2,2}(\beta_{n_2,2}) \end{pmatrix},$$

where the second matrix is the Kronecker product $M(\beta_{1,2}, \ldots, \beta_{n_2,2}) \otimes I$. As $M(\beta_{1,2}, \ldots, \beta_{n_2,2}) \otimes I$ is $(I \otimes M(\beta_{1,2}, \ldots, \beta_{n_2,2}))P$ for some permutation matrix P, it takes the form

$$\begin{pmatrix} M(\beta_{1,2}, \ldots, \beta_{n_2,2}) & & \\ & \ddots & \\ & & M(\beta_{1,2}, \ldots, \beta_{n_2,2}) \end{pmatrix} P,$$

with $\det(P) = \pm 1$. Putting these decompositions together and applying Proposition 2.7 shows

$$\delta_{L/K}(\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}) = d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})^{n_2} d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})^{n_1}.$$

This completes the proof. $\square$

It is generally very difficult to write down an integral basis explicitly. However, there is one instance in which this is possible. We say that B is *monogenic* over A if $B = A[\beta]$ for some $\beta \in B$. It follows immediately that $1, \beta, \ldots, \beta^{n-1}$ is an integral basis for B/A since B is of rank n. The discriminant of this basis is then given by Equation (4). In addition, the traces $\mathrm{Tr}_{L/K}$ and $\mathrm{Tr}_{B/A}$ and norms $\mathrm{N}_{L/K}$ and $\mathrm{N}_{B/A}$ agree:

Proposition 2.11. *Let A be an integrally closed integral domain with field of fractions K, L/K be a degree n separable extension, and B be the integral closure of A in L. If B admits an integral basis over A then*

$$\mathrm{Tr}_{L/K}(\beta) = \mathrm{Tr}_{B/A}(\beta) \quad \textit{and} \quad \mathrm{N}_{L/K}(\beta) = \mathrm{N}_{B/A}(\beta),$$

for all $\beta \in B$.

Proof. Let $\beta_1, \dots, \beta_n$ be an integral basis for B/A. Then $\beta_1, \dots, \beta_n$ is also a basis for L/K. It follows that the multiplication by β map in L has the same matrix representation as it does in B. Therefore

$$\mathrm{Tr}_{L/K}(\beta) = \mathrm{Tr}_{B/A}(\beta) \quad \text{and} \quad \mathrm{N}_{L/K}(\beta) = \mathrm{N}_{B/A}(\beta),$$

as desired. $\square$

We now turn to the case of a number field K of degree n. We write $\mathrm{Tr}_K = \mathrm{Tr}_{K/\mathbb{Q}}$ and $\mathrm{N}_K = \mathrm{N}_{K/\mathbb{Q}}$ and call these the *field trace* and *field norm* of K respectively. Moreover, for any $\kappa \in K$ we call $\mathrm{Tr}_K(\kappa)$ and $\mathrm{N}_K(\kappa)$ the *trace* and *norm* of κ respectively. Then from Propositions 2.2 and 2.3 we see that the trace and norm of algebraic integers are themselves integers and $\kappa \in \mathcal{O}_K$ is a unit if and only if $\mathrm{N}_K(\kappa) = \pm 1$ (as these are the only units in $\mathbb{Z}$). Moreover, since $\mathbb{Z}$ is a principal ideal domain Theorem 2.9 implies that $\mathcal{O}_K$ admits an integral basis over $\mathbb{Z}$ of degree n. That is, $\mathcal{O}_K$ is a free abelian group of rank n. Accordingly, we say that $\alpha_1, \dots, \alpha_n$ is an *integral basis* for K if it is an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Accordingly, we define the *discriminant* Δ_K of K to be the discriminant of $\mathcal{O}/\mathcal{o}$. As $(\mathbb{Z}^*)^2 = \{1\}$, Δ_K is a well-defined integer and satisfies

$$\Delta_K = d_{L/K}(\alpha_1, \dots, \alpha_n),$$

for any integral basis $\alpha_1, \dots, \alpha_n$ for K. Moreover, Δ_K is nonzero by Proposition 2.2 and Lemma 2.5 and may very well be negative. In light of Proposition 2.7, we also have

$$|\det(M(\alpha_1, \dots, \alpha_n))| = \sqrt{|\Delta_K|}.$$

Lastly, we say K is *monogenic* if $\mathcal{O}_K$ is monogenic over $\mathbb{Z}$.

3 Dedekind Domains

Let $\mathcal{o}$ be a noetherian integral domain and denote its field of fractions by K. Any nonzero ideal $\mathfrak{a}$ of $\mathcal{o}$ is said to be an *integral ideal* of $\mathcal{o}$. We call any prime integral ideal $\mathfrak{p}$ of $\mathcal{o}$ a *prime* of $\mathcal{o}$ and if $\mathfrak{p}$ is principal with $\mathfrak{p} = \alpha\mathcal{o}$, with $\alpha \in K$ nonzero, we will simply refer to α as the prime instead of $\mathfrak{p}$. In any case, an integral ideal $\mathfrak{a}$ is just a $\mathcal{o}$-submodule of $\mathcal{o}$. Moreover, it is finitely generated since $\mathcal{o}$ is noetherian and is therefore a finitely generated $\mathcal{o}$-submodule of K. More generally, we say $\mathfrak{f}$ is a *fractional ideal* of $\mathcal{o}$ if $\mathfrak{f}$ a nonzero finitely generated $\mathcal{o}$-submodule of K. Moreover, we say that a fractional ideal is *principal* if it is generated by a single element. That is, if $\mathfrak{f} = \kappa\mathcal{o}$ for some nonzero $\kappa \in K$. In particular, all integral ideals are fractional ideals and all principal integral ideals are principal fractional ideals. Now let $\kappa_1, \dots, \kappa_r \in K$ be generators for the fractional ideal $\mathfrak{f}$. Since K is the field of fractions of $\mathcal{o}$, $\kappa_i = \frac{\alpha_i}{\delta_i}$ with $\alpha_i, \delta_i \in \mathcal{o}$ and where δ_i is nonzero for $1 \le i \le r$. Setting $\delta = \delta_1 \cdots \delta_r$, we have that $\delta\kappa_i \in \mathcal{o}$ for all i and hence $\delta\mathfrak{f}$ is an integral ideal. Conversely, if there exists some nonzero $\delta \in \mathcal{o}$ such that $\delta\mathfrak{f} = \mathfrak{a}$ is an integral ideal then $\mathfrak{f}$ is a fractional ideal because $\mathfrak{a}$ is a finitely generated $\mathcal{o}$-submodule of K and hence $\mathfrak{f}$ is too. Thus for any fractional ideal $\mathfrak{f}$, there exists a nonzero $\delta \in \mathcal{O}$ and 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 $\delta = 1$, and fractional ideals need not be a subgroup of $\mathcal{O}$. We will be able to show that an fractional ideal of $\mathcal{O}$ factors into a product of primes provided that $\mathcal{O}$ satisfies a few more restrictive conditions. Accordingly, we say that a ring is a *Dedekind domain* if it satisfies the following properties:

(i) It is an integrally closed integral domain.

(ii) It is noetherian.

(iii) Every nonzero prime ideal is maximal.

In other words, a noetherian integral domain is a Dedekind domain if and only if it is integrally closed and every nonzero prime is maximal.

Remark 3.1. $\mathbb{Z}$ is an integrally closed integral domain by Lemma 1.3. It is also noetherian since $\mathbb{Z}$ is a principal ideal domain. Every prime is of the form $p\mathbb{Z}$ for some prime p and therefore is maximal because $\mathbb{Z}/p\mathbb{Z}$ is a field. It follows that $\mathbb{Z}$ is a Dedekind domain and the primes of $\mathbb{Z}$ are exactly the primes p.

With this setup, property (ii) can be rephrased as saying that every integral ideal is finitely generated while property (iii) is equivalent to the fact that every prime is maximal. One should think of Dedekind domains as generalizations of $\mathbb{Z}$. Note that we have not assumed $\mathcal{O}$ is a principal ideal domain. In fact, the most interesting Dedekind domains are not principal ideal domains. Our primary concern regarding Dedekind domains will be to show that, while there need not be prime factorization of elements, fractional ideals admit a factorization into a product of primes. We first show containment in one direction for integral ideals:

Lemma 3.2. *Let $\mathcal{O}$ be a Dedekind domain. For every integral ideal $\mathfrak{a}$, there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ 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. Assuming otherwise and ordering $\mathcal{S}$ by inclusion, the fact that $\mathcal{O}$ is noetherian implies that there exists a maximal integral ideal $\mathfrak{a} \in \mathcal{S}$. Moreover $\mathfrak{a}$ cannot be prime for otherwise $\mathfrak{a}$ contains a product of primes (namely itself). Since $\mathfrak{a}$ is not prime, there exist $\alpha_1, \alpha_2 \in \mathcal{O}$ with $\alpha_1\alpha_2 \in \mathfrak{a}$ and such that $\alpha_1, \alpha_2 \notin \mathfrak{a}$. Now define integral ideals

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

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

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

and $\alpha_1\alpha_2 \in \mathfrak{a}$. Maximality of $\mathfrak{a}$ implies that there exist primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ 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 $\mathfrak{a} \in \mathcal{S}$. Hence $\mathcal{S}$ is empty as desired. □

In order to obtain the reverse containment in Lemma 3.2, we need to do more work. Precisely, we want to show that every integral ideal factors into a product of primes. Let $\mathfrak{p}$ be a prime. We define $\mathfrak{p}^{-1}$ by

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

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 $\alpha\mathfrak{p}^{-1} \subseteq \mathcal{O}$. 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 3.3. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{p}$ be a prime. Then the following hold:*

(i)

$$\mathcal{O} \subset \mathfrak{p}^{-1}.$$

(ii)

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

Proof. We will prove the latter two statement separately:

(i) Clearly $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ so it suffices to show that $\mathfrak{p}^{-1} - \mathcal{O}$ is nonempty. To this end, let $\alpha \in \mathfrak{p}$ be nonzero. By Lemma 3.2 let $k \geq 1$ be the minimal integer such that there exist primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ with

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

As $\alpha \in \mathfrak{p}$, we have $\alpha\mathcal{O} \subseteq \mathfrak{p}$. 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 $\mathfrak{p}_1 \subseteq \mathfrak{p}$. As primes are maximal since $\mathcal{O}$ is noetherian, we conclude $\mathfrak{p}_1 = \mathfrak{p}$. Moreover, since k is minimal we must have

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

Hence there exists $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_k$ with $\beta \notin \alpha\mathcal{O}$. We will now show that $\beta\alpha^{-1}$ is an element in $\mathfrak{p}^{-1} - \mathcal{O}$. Since $\mathfrak{p}_1 = \mathfrak{p}$, what we have previously shown implies $\beta\mathfrak{p} \subseteq \alpha\mathcal{O}$ and hence $\beta\alpha^{-1}\mathfrak{p} \in \mathcal{O}$ which means $\beta\alpha^{-1} \in \mathfrak{p}^{-1}$. But as $\beta \notin \alpha\mathcal{O}$, we also have $\beta\alpha^{-1} \notin \mathcal{O}$. Hence $\beta\alpha^{-1} \in \mathfrak{p}^{-1} - \mathcal{O}$ which 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 because $\mathcal{O}$ is noetherian, it follows that $\mathfrak{p}^{-1}\mathfrak{p}$ is either $\mathfrak{p}$ or $\mathcal{O}$. So it suffices to show that the first case cannot hold. Assume by contradiction that $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. Let $\omega_1, \ldots, \omega_r$ generate $\mathfrak{p}$ and let $\alpha \in \mathfrak{p}^{-1} - \mathcal{O}$ 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 $\alpha_{i,j} \in \mathcal{O}$ 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 $\mathcal{O}$. As $\mathcal{O}$ is integrally closed, $\alpha \in \mathcal{O}$ which is a contraction. Thus $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$ proving (ii). $\square$

We can now show that every integral ideal factors uniquely into a product of primes (up to reordering of the factors):

Theorem 3.4. *Let $\mathcal{O}$ be a Dedekind domain. Then for every integral ideal $\mathfrak{a}$ there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ 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, let $\mathcal{S}$ be the set of integral ideals that are not a product of primes. We will show that $\mathcal{S}$ is empty. Assuming otherwise and ordering $\mathcal{S}$ by inclusion, the fact that $\mathcal{O}$ is noetherian implies that there exists a maximal integral ideal $\mathfrak{a} \in \mathcal{S}$. Necessarily $\mathfrak{a}$ is not prime and since primes are maximal in $\mathcal{O}$, there is some prime $\mathfrak{p}_1$ for which $\mathfrak{a} \subset \mathfrak{p}_1$. Then by Lemma 3.3 (ii), we have $\mathfrak{p}_1^{-1}\mathfrak{a} \subset \mathcal{O}$ so that $\mathfrak{p}_1^{-1}\mathfrak{a}$ is also an integral ideal. Also, Lemma 3.3 (i) implies that $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}_1^{-1}$. By maximality of $\mathfrak{a}$, $\mathfrak{a}\mathfrak{p}_1^{-1}$ factors into a product of primes. That is, there exist primes $\mathfrak{p}_2, \ldots, \mathfrak{p}_k$ such that

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

Hence

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

so that $\mathfrak{a}$ factors into a product of primes which contradicts the fact that $\mathfrak{a} \in \mathcal{S}$. Hence $\mathcal{S}$ is empty thus proving the existence of such a factorization. Now we prove uniqueness. Suppose that $\mathfrak{a}$ admits factorizations

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

for primes $\mathfrak{p}_i$ and $\mathfrak{q}_j$ with $1 \le i \le k$ and $1 \le j \le \ell$. 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 since primes are maximal in $\mathcal{O}$ we have $\mathfrak{q}_1 = \mathfrak{p}_1$. Then

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

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

As a near immediate corollary of Theorem 3.4, all fractional ideal admits a factorization into a product of primes and their inverses (up to reordering of the factors):

Corollary 3.5. *Let $\mathcal{O}$ be a Dedekind domain. Then for every fractional ideal $\mathfrak{f}$ there exist primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ such that $\mathfrak{f}$ factors as*

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

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

Proof. If $\mathfrak{f}$ is a fractional ideal then there exists a nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$ such that $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$. In particular, $\mathfrak{a}$ and $\delta\mathcal{O}$ are integral ideals such that $\delta\mathcal{O}\mathfrak{f} = \mathfrak{a}$. By Theorem 3.4, $\mathfrak{a}$ and $\delta\mathcal{O}$ admit unique factorizations

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

for some primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_\ell$ up to reordering of the factors. Hence

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

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

By Corollary 3.5, for any fractional ideal $\mathfrak{f}$ there exist distinct prime $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that $\mathfrak{f}$ admits a factorization

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

with $e_i \in \mathbb{Z} - \{0\}$ for all i, called the *prime factorization* of $\mathfrak{f}$ with *prime factors* $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. In particular, the prime factorization of an integral ideal $\mathfrak{a}$ is of the form

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

with $e_i \geq 1$ for all i. Accordingly, for any two integral ideal $\mathfrak{a}$ and $\mathfrak{b}$ we say that $\mathfrak{a}$ *divides* $\mathfrak{b}$ and write $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} \subseteq \mathfrak{a}$. Sometimes this condition is expressed as *to contain is to divide* or *to divide is to contain*. By the prime factorization of fractional ideals, this is equivalent to the fact that every prime power factor of $\mathfrak{a}$ appears in the prime factorization of $\mathfrak{b}$. We also say that $\mathfrak{a}$ *exactly divides* $\mathfrak{b}$ and write $\mathfrak{a} \mid\mid \mathfrak{b}$ if $\mathfrak{a}$ divides $\mathfrak{b}$ but no power of $\mathfrak{a}$ divides $\mathfrak{b}$. This is equivalent to the fact that every prime power factor of $\mathfrak{a}$ appears in the prime factorization of $\mathfrak{b}$ but not for any power of $\mathfrak{a}$. In the case of a prime $\mathfrak{p}$ and an integral ideal $\mathfrak{a}$, $\mathfrak{p} \mid \mathfrak{a}$ if and only if $\mathfrak{p}$ is a prime factor of $\mathfrak{a}$ and $\mathfrak{p}^e \mid\mid \mathfrak{a}$, for some $e \geq 1$, if and only if $\mathfrak{p}^e$ is exactly the power of $\mathfrak{p}$ appearing in the prime factorization of $\mathfrak{a}$. Moreover, if $\mathfrak{a} \mid \mathfrak{p}$ then $\mathfrak{a} = \mathfrak{p}$. The *greatest common divisor* $(\mathfrak{a}, \mathfrak{b})$ of $\mathfrak{a}$ and $\mathfrak{b}$ is defined to be the integral ideal that all other common integral ideal divisors divide. Since to divide is to contain, $(\mathfrak{a}, \mathfrak{b})$ is the smallest ideal that contains both $\mathfrak{a}$ and $\mathfrak{b}$. This is $\mathfrak{a} + \mathfrak{b}$ and so $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$. The *least common multiple* $[\mathfrak{a}, \mathfrak{b}]$ of $\mathfrak{a}$ and $\mathfrak{b}$ is defined to be the integral ideal that divides all other common multiples. Since to divide is to contain, $[\mathfrak{a}, \mathfrak{b}]$ is the largest integral ideal that is contained in both $\mathfrak{a}$ and $\mathfrak{b}$. This is $\mathfrak{a} \cap \mathfrak{b}$ and so $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a} \cap \mathfrak{b}$. Moreover, we say that $\mathfrak{a}$ and $\mathfrak{b}$ are *relatively prime* if $(\mathfrak{a}, \mathfrak{b}) = \mathcal{O}$. In other words, we have

$$\mathfrak{a} + \mathfrak{b} = \mathcal{O}.$$

This is equivalent to the prime factorizations of $\mathfrak{a}$ and $\mathfrak{b}$ containing distinct primes. In particular, distinct primes and their powers are relatively prime. Moreover, if $\mathfrak{a}$ and $\mathfrak{b}$ and relatively prime then we also have

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

The reverse containment is obvious. For the forward containment, since $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$ there exists $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$. Now let $\gamma \in \mathfrak{a} \cap \mathfrak{b}$. Then $\gamma = \gamma\alpha + \gamma\beta$ and hence $\gamma \in \mathfrak{a}\mathfrak{b}$. The reverse containment follows which proves equality. Just as it is common to suppress the fundamental theorem of arithmetic and just state the prime factorization of an integer, we suppress referencing Theorem 3.4 and simply state the prime factorization of a fractional ideal. We can now show that for a Dedekind domain, being a principal ideal domain is equivalent to being a unique factorization domain:

Proposition 3.6. *Let $\mathcal{O}$ be a Dedekind domain. Then $\mathcal{O}$ is a principal ideal domain if and only if it is a unique factorization domain.*

Proof. The forward implication is trivial since every principal ideal domain is a unique factorization domain. For the reverse implication, suppose $\mathcal{O}$ is a unique factorization domain. Since every integral ideal factors into a product of primes by Theorem 3.4 and the product of principal integral ideals is principal, it suffices to show that primes are principal. So let $\mathfrak{p}$ be a prime. Then there exists nonzero $\alpha \in \mathfrak{p}$ and α is not a unit since $\mathfrak{p}$ is prime (primes are necessarily proper). Since $\mathcal{O}$ is a unique factorization domain, we may write

$$\alpha = \mu\rho_1^{e_1} \cdots \rho_r^{e_r},$$

for some unit μ and primes $\rho_i \in \mathcal{O}$ and integers $e_i \geq 1$ for $1 \leq i \leq r$ with $r \geq 1$. Since $\mathfrak{p}$ is prime, it follows that there is some i such that $\rho_i \in \mathfrak{p}$. Without loss of generality, we may assume $\rho_1 \in \mathfrak{p}$. Then the integral ideal $\rho_1\mathcal{O}$ satisfies $\rho_1\mathcal{O} \subseteq \mathfrak{p}$. As ρ_1 is prime and $\mathcal{O}$ is a unique factorization domain, $\rho_1\mathcal{O}$ is a prime and hence maximal since $\mathcal{O}$ is also a Dedekind domain. Thus $\rho_1\mathcal{O} = \mathfrak{p}$ and hence $\mathfrak{p}$ is principal completing the proof. □

With the prime factorization in hand, we will discuss the group structure of the fractional ideals of $\mathcal{O}$. Let $I_{\mathcal{O}}$ denote the set of fractional ideals of $\mathcal{O}$. We call $I_{\mathcal{O}}$ the *ideal group* of $\mathcal{O}$. The following theorem shows that $I_{\mathcal{O}}$ is indeed a group:

Theorem 3.7. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Then $I_{\mathcal{O}}$ is an abelian group with identity $\mathcal{O}$.*

Proof. It is clear that the product of fractional ideals is a fractional ideal. Associativity and commutativity of $I_{\mathcal{O}}$ are also obvious. The identity is $\mathcal{O}$ because every fractional ideal is a finitely generated $\mathcal{O}$-submodule of K. It follows that $\mathfrak{p}^{-1}$ is the inverse of any prime $\mathfrak{p}$ by Lemma 3.3 (ii). Therefore every prime is invertible. If $\mathfrak{a}$ is a integral ideal then it admits a prime factorization $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and then $\mathfrak{b} = \mathfrak{p}_1^{-e_1} \cdots \mathfrak{p}_r^{-e_r}$ is its inverse. Hence every integral ideal is invertible. If $\mathfrak{f}$ is a fractional ideal, there exists a nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$ such that $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ and hence $\mathfrak{f}$ is invertible because δ and $\mathfrak{a}$ are. It follows that every fractional ideal is invertible which completes the proof. □

Now that we have proved that the ideal group $I_{\mathcal{O}}$ of K is indeed a group, we can also deduce the explicit form for the inverse $\mathfrak{f}^{-1}$ of any fractional ideal $\mathfrak{f}$:

Proposition 3.8. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and let $\mathfrak{f}$ be a fractional ideal. Then*

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

In particular, $\mathcal{O} \subseteq \mathfrak{f}$ if and only if $\mathfrak{f}^{-1}$ is an integral ideal.

Proof. Let $\mathfrak{f}$ be a fractional ideal. Then the inverse $\mathfrak{f}^{-1}$ exists by Theorem 3.7. In the case of an integral ideal $\mathfrak{a}$, we have

$$\mathfrak{a}^{-1} = \{\kappa \in K : \kappa\mathfrak{a} \subseteq \mathcal{O}\},$$

by the prime factorization of $\mathfrak{a}$ and the definition of the inverse of a prime. If $\mathfrak{f}$ is a fractional ideal, there exists a nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$ such that $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$. But then $\delta\mathfrak{f} = \mathfrak{a}$ so that

$$\frac{1}{\delta}\mathfrak{f}^{-1} = \{\kappa \in K : \kappa\delta\mathfrak{f} \subseteq \mathcal{O}\},$$

which is equivalent to the first statement. For the second statement, if $\mathcal{O} \subseteq \mathfrak{f}$ then multiplying by $\mathfrak{f}^{-1}$ shows $\mathfrak{f}^{-1} \subseteq \mathcal{O}$ and hence $\mathfrak{f}^{-1}$ is an integral ideal. Running this argument backwards by multiplying by $\mathfrak{f}$ proves the converse. □

We will now discuss applications of the Chinese remainder theorem in the context of integral ideals. With it we can prove some interesting results. First, we recall a useful fact. Suppose $\mathfrak{a}$ is an integral ideal with prime factorization

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

As powers of distinct primes are relatively prime, 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

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

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

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

for all i. We will use the Chinese remainder theorem to prove a few useful lemmas about Dedekind domains. For convenience, if $\mathcal{O}$ is a Dedekind domain with prime $\mathfrak{p}$ we will let $\mathbb{F}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$ be the residue class field of $\mathcal{O}$ by $\mathfrak{p}$ (recall $\mathfrak{p}$ is maximal). The first lemma is an isomorphism between the residue class field and quotients by powers of primes:

Lemma 3.9. *Let $\mathcal{O}$ be a Dedekind domain. Then for any prime $\mathfrak{p}$ and $n \geq 0$, we have an isomorphism*

$$\mathbb{F}_\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}.$$

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

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

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 $\alpha \in \mathcal{O}$ 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 γ be a representative of a coset in $\mathfrak{p}^n/\mathfrak{p}^{n+1}$. As $\beta \in \mathfrak{p}^n$, we have $\beta\mathcal{O} \subseteq \mathfrak{p}^n$. But since $\beta \notin \mathfrak{p}^{n+1}$, we see that $\beta\mathcal{O}\mathfrak{p}^{-n}$ is necessarily an integral ideal relatively prime to $\mathfrak{p}^{n+1}$. As $\mathfrak{p}^{n+1}$ and $\beta\mathcal{O}\mathfrak{p}^{-n}$ are relatively prime, the Chinese remainder theorem implies that we can find a unique $\alpha \in \mathcal{O}$ such that

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

The second condition means $\alpha \in \beta\mathcal{O}\mathfrak{p}^{-n}$. 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 $\alpha \in \beta\mathcal{O}\mathfrak{p}^{-n} \cap \mathfrak{p}^n = \beta\mathcal{O}$ where the equality holds because the intersection of ideals is equal to their product provided the ideals are relatively prime. Thus $\alpha\beta^{-1} \in \mathcal{O}$ and hence

$$\phi(\alpha\beta^{-1}) = \alpha + \mathfrak{p}^{n+1} = \gamma + \mathfrak{p}^{n+1}.$$

This shows ϕ is surjective completing the proof. □

Our second lemma shows that given two integral ideals, we can multiply by a relatively prime integral ideal and produce a principal integral ideal:

Lemma 3.10. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{a}$ and $\mathfrak{b}$ be integral ideals. Then there exists an integral ideal $\mathfrak{c}$ relatively prime to $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{c}$ is principal.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime factors of both $\mathfrak{a}$ and $\mathfrak{b}$ so that

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \quad \text{and} \quad \mathfrak{b} = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_r^{f_r},$$

with $e_i \geq 0$ and $f_i \geq 0$ for all $1 \leq i \leq r$. By the prime factorization of fractional ideals, there exists $\alpha_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ 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 the existence of an $\alpha \in \mathcal{O}$ such that $\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i+1}}$ for all i. But then

$$\alpha \equiv 0 \pmod{\mathfrak{p}_i^{e_i}} \quad \text{and} \quad \alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i+1}},$$

since $\alpha_i \in \mathfrak{p}_i^{e_i}$ for all i. Hence $\alpha \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ and so $\mathfrak{p}_i^{e_i} \mid\mid \alpha\mathcal{O}$ for all i. It follows that $(\alpha\mathcal{O}, \mathfrak{a}\mathfrak{b}) = \mathfrak{a}$. Letting $\mathfrak{c}$ be the integral ideal such that $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{c}$, we have $(\mathfrak{a}\mathfrak{c}, \mathfrak{a}\mathfrak{b}) = \mathfrak{a}$. Thus $(\mathfrak{c}, \mathfrak{b}) = \mathcal{O}$ which is to say that $\mathfrak{c}$ must be relatively prime to $\mathfrak{b}$. ◻

Our last lemma shows that multiplying by fractional ideals does not affect quotients:

Lemma 3.11. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{f}$, $\mathfrak{g}$, $\mathfrak{h}$ be fractional ideals with $\mathfrak{g} \subseteq \mathfrak{f}$. Then we have an isomorphism*

$$\mathfrak{f}/\mathfrak{g} \cong \mathfrak{f}\mathfrak{h}/\mathfrak{g}\mathfrak{h}.$$

In particular,

$$\mathfrak{a}^{-1}/\mathcal{O} \cong \mathcal{O}/\mathfrak{a},$$

for any integral ideal $\mathfrak{a}$.

Proof. We have $\mathfrak{f} = \frac{\mathfrak{a}}{\alpha}$, $\mathfrak{g} = \frac{\mathfrak{b}}{\beta}$, and $\mathfrak{h} = \frac{\mathfrak{c}}{\gamma}$ for nonzero $\alpha, \beta, \gamma \in \mathcal{O}$ and integral ideals $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ with $\mathfrak{b} \subseteq \mathfrak{a}$. In view of the isomorphisms,

$$\mathfrak{f}/\mathfrak{g} \cong \beta\mathfrak{a}/\alpha\mathfrak{b} \quad \text{and} \quad \mathfrak{f}\mathfrak{h}/\mathfrak{g}\mathfrak{h} \cong \beta\mathfrak{a}\mathfrak{c}/\alpha\mathfrak{b}\mathfrak{c},$$

it suffices to show

$$\mathfrak{a}/\mathfrak{b} \cong \mathfrak{a}\mathfrak{c}/\mathfrak{b}\mathfrak{c}.$$

As to contain is to divide, we know $\mathfrak{a} \mid \mathfrak{b}$. Therefore $\mathfrak{b}\mathfrak{a}^{-1}$ is an integral ideal. By Lemma 3.10, there exists an integral ideal $\mathfrak{d}$ relatively prime to $\mathfrak{b}\mathfrak{a}^{-1}$ such that $\mathfrak{c}\mathfrak{d} = \delta\mathcal{O}$ for some $\delta \in \mathcal{O}$. But then $\mathfrak{d} + \mathfrak{b} = \mathcal{O}$ and hence

$$\delta\mathfrak{c}^{-1} + \mathfrak{b}\mathfrak{a}^{-1} = \mathcal{O}.$$

Multiplying by $\mathfrak{a}\mathfrak{c}$ yields

$$\delta\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a}\mathfrak{c}.$$

As $\mathfrak{c}\mathfrak{d} = \delta\mathcal{O}$, we have $\delta\mathcal{O} \subseteq \mathfrak{c}$ so that $\delta \in \mathfrak{c}$. Therefore we may consider the homomorphism

$$\phi : \mathfrak{a} \to \mathfrak{a}\mathfrak{c}/\mathfrak{b}\mathfrak{c} \qquad \alpha \mapsto \alpha\delta + \mathfrak{b}\mathfrak{c}.$$

It is surjective by what we have just proved. Moreover, $\ker\phi = \mathfrak{a} \cap \delta^{-1}\mathfrak{b}\mathfrak{c}$. But observe that

$$\mathfrak{a} \cap \delta^{-1}\mathfrak{b}\mathfrak{c} = \delta^{-1}\mathfrak{a}\mathfrak{c}(\delta\mathfrak{c}^{-1} \cap \mathfrak{b}\mathfrak{a}^{-1}) = \delta^{-1}\mathfrak{a}\mathfrak{c}(\mathfrak{d} \cap \mathfrak{b}\mathfrak{a}^{-1}) = \mathfrak{b},$$

where the last equality follows since $\mathfrak{d}$ and $\mathfrak{b}\mathfrak{a}^{-1}$ are relatively prime so that their intersection is equal to their product. Hence $\ker\phi = \mathfrak{b}$ and the first statement now follows upon applying the first isomorphism theorem. For the second statement, take $\mathfrak{f} = \mathfrak{a}^{-1}$, $\mathfrak{g} = \mathcal{O}$, and $\mathfrak{h} = \mathfrak{a}$ (note that $\mathcal{O} \subseteq \mathfrak{a}^{-1}$ by Proposition 3.8). □

We now state two additional interesting facts about Dedekind domains. The first is that any Dedekind domains with only finitely many primes is a principal ideal domain:

Proposition 3.12. *Let $\mathcal{O}$ be a Dedekind domain. If there are only finitely many primes then $\mathcal{O}$ is a principal ideal domain.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the primes of $\mathcal{O}$. Then for any integral ideal $\mathfrak{a}$, the prime factorization 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 prime factorizations of fractional ideals, there exists $\alpha_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ 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 $\alpha \in \mathcal{O}$ with

$$\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i+1}},$$

for all i. As $\alpha_i \in \mathfrak{p}_i^{e_i}$ for all i, we have that $\alpha \in \mathfrak{a}$ and hence $\alpha\mathcal{O} \subseteq \mathfrak{a}$. But as $\alpha \notin \mathfrak{p}_i^{e_i+1}$ for all i, we see that $\alpha\mathcal{O}\mathfrak{a}^{-1}$ is necessarily an integral ideal relatively prime to all primes of $\mathcal{O}$. This means $\alpha\mathcal{O}\mathfrak{a}^{-1} = \mathcal{O}$ and hence $\mathfrak{a} = \alpha\mathcal{O}$ so that $\mathfrak{a}$ is principal. As $\mathfrak{a}$ was arbitrary, $\mathcal{O}$ is a principal ideal domain. □

The second fact is that any fractional ideal is generated by at most two elements:

Proposition 3.13. *Let $\mathcal{O}$ be a Dedekind domain. Then every fractional ideal 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 $\alpha\mathcal{O}$. As $\alpha\mathcal{O} \subseteq \mathfrak{a}$, 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 prime factorizations of fractional ideals, there exists $\beta_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$ 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 $\beta \in \mathcal{O}$ with

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

for all i. As $\beta_i \in \mathfrak{p}_i^{e_i}$ for all i, we have that $\beta \in \mathfrak{a}$ and hence $\beta\mathcal{O} \subseteq \mathfrak{a}$. But as $\beta \notin \mathfrak{p}_i^{e_i+1}$ for all i, we see that $\beta\mathcal{O}\mathfrak{a}^{-1}$ is necessarily an integral ideal relatively prime to $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and hence to $\alpha\mathcal{O}$. This means

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

and hence

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

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

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

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 $\delta \in \mathcal{O}$ and 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

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

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

Proposition 3.13 shows that while a Dedekind domain $\mathcal{O}$ may not be a principal ideal domain, it is not far off from one since every integral ideal needs at most two generators. We can give a more refined interpretation of this using the ideal group $I_{\mathcal{O}}$. Let $P_{\mathcal{O}}$ denote the subgroup of principal fractional ideals of $I_{\mathcal{O}}$. Since $I_{\mathcal{O}}$ is abelian by Theorem 3.7, $P_{\mathcal{O}}$ is normal. The *ideal class group* $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is defined to be the quotient group

$$\mathrm{Cl}(\mathcal{O}) = I_{\mathcal{O}}/P_{\mathcal{O}},$$

We call an element of $\mathrm{Cl}(\mathcal{O})$ an *ideal class* of $\mathcal{O}$. As every fractional ideal $\mathfrak{f}$ can be expressed as $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$, we have $\delta\mathfrak{f} = \mathfrak{a}$ and hence every ideal class can be represented by an integral ideal $\mathfrak{a}$. The *class number* $h_{\mathcal{O}}$ of $\mathcal{O}$ is defined by

$$h_{\mathcal{O}} = |\,\mathrm{Cl}(\mathcal{O})|.$$

The ideal class group is an object which encodes how much $\mathcal{O}$ fails to be a principal ideal domain (equivalently a unique factorization domain by Proposition 3.6) while the class number $h_{\mathcal{O}}$ is a measure of the degree of failure. For example, $\mathcal{O}$ is a principal ideal domain if and only if $h_{\mathcal{O}} = 1$. Indeed, if $\mathcal{O}$ is a principal ideal domain then every integral ideal is principal and hence every fractional ideal is too (because every fractional ideal is of the form $\frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$). But then $\mathrm{Cl}(\mathcal{O})$ is the trivial group and hence $h_{\mathcal{O}} = 1$. Conversely, if $h_{\mathcal{O}} = 1$ then every integral ideal is principal so that $\mathcal{O}$ is a principal ideal domain.

Remark 3.14. The class number $h_{\mathcal{O}}$ need not be finite for a general Dedekind domain $\mathcal{O}$.

The *unit group* of $\mathcal{O}$ is defined to be $\mathcal{O}^*$. That is, the unit group is the group of units in $\mathcal{O}$. The ideal class group and unit group of $\mathcal{O}$ are related via the following exact sequence:

Proposition 3.15. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Then the sequence*

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \xrightarrow{\ \mathcal{O}\ } I_{\mathcal{O}} \longrightarrow \mathrm{Cl}(\mathcal{O}) \longrightarrow 1,$$

where the middle map takes any $\kappa \in K^*$ to its associated principal fractional ideal $\kappa\mathcal{O}$, is exact.

Proof. The sequence is exact at $\mathcal{O}^*$ because the second map is injective. For exactness at K^*, the image of the second map is contained in the kernel of the third map since $\mathcal{O}$ is the identity in $I_{\mathcal{O}}$ by Theorem 3.7. So suppose $\kappa \in K^*$ is contained in the kernel of the third map. Then $\kappa\mathcal{O} = \mathcal{O}$ which implies $\kappa \in \mathcal{O}^*$ because $1 \in \mathcal{O}$. This proves exactness at K^*. Exactness at $I_{\mathcal{O}}$ follows by the definition of $\mathrm{Cl}(\mathcal{O})$. Lastly, the sequence is exact at $\mathrm{Cl}(\mathcal{O})$ since the fourth map is surjective which completes the proof. □

Thinking of the third map in Proposition 3.15 as passing from numbers in K^* to fractional ideals in $I_{\mathcal{O}}$, exactness means that unit group is measuring the contraction (how many numbers are annihilated) taking place during this process while the class group is measuring the expansion (how many fractional ideal are created).

Remark 3.16. The class number $h_{\mathcal{O}}$ and unit group $\mathcal{O}^*$ of $\mathcal{O}$ are generally two of the most difficult pieces of algebraic data of $\mathcal{O}$ to compute.

We now turn to the case of a number field K for which our developments so far can be refined. However, in order to apply our results on Dedekind domains, we need to show that $\mathcal{O}_K$ is one:

Theorem 3.17. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Since $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, $\mathcal{O}_K$ is automatically an integrally closed integral domain. As $\mathcal{O}_K$ is a free abelian group of finite rank, any ideal is a finitely generated $\mathbb{Z}$-module and hence a finitely generated $\mathcal{O}_K$-module. This proves that $\mathcal{O}_K$ is noetherian. It remains to prove that every prime of $\mathcal{O}_K$ is maximal. Letting $\mathfrak{p}$ be a prime, it suffices to show $\mathcal{O}_K/\mathfrak{p}$ is a field. To this end, consider the homomorphism

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

Then $\ker\phi = \mathfrak{p} \cap \mathbb{Z}$ and we claim $\mathfrak{p} \cap \mathbb{Z}$ is a prime of $\mathbb{Z}$. It is obviously an ideal of $\mathbb{Z}$ and is prime because $\mathfrak{p}$ is. To see that it is nonzero, let $\alpha \in \mathfrak{p}$ be nonzero. As α is an algebraic integer, we have

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

for some $n \geq 1$ and $a_i \in \mathbb{Z}$ for $0 \leq i \leq n-1$. Taking n minimal, we have $a_0 \neq 0$. Isolating a_0 shows that $a_0 \in \mathfrak{p}$ and hence $a_0 \in \mathfrak{p} \cap \mathbb{Z}$. Therefore $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p. Hence $\ker \phi = p\mathbb{Z}$ and by the first isomorphism theorem, ϕ induces an injection $\phi : \mathbb{F}_p \to \mathcal{O}_K/\mathfrak{p}$. As $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, it is obtained from $\mathbb{Z}$ by forming a polynomial ring with algebraic elements in K. The latter injection then shows that $\mathcal{O}_K/\mathfrak{p}$ is obtained from $\mathbb{F}_p$ by adjoining these algebraic elements reduced modulo $\mathfrak{p}$. Their reductions are seen to be algebraic over $\mathbb{F}_p$ by reducing their minimal polynomials over $\mathbb{Q}$, viewed as elements of $\mathcal{o}[x]$, modulo $\mathfrak{p}$ upon recalling that the coefficients of which are in $\mathbb{Z}$ by Proposition 1.4. Hence $\mathcal{O}_K/\mathfrak{p}$ is obtained from $\mathbb{F}_p$ by adjoining algebraic elements to $\mathbb{F}_p$ (since $\mathbb{F}_p[\overline{\alpha}] = \mathbb{F}_p(\overline{\alpha})$ if $\overline{\alpha}$ is algebraic over $\mathbb{F}_p$) and is therefore a field. □

In view of the fact that $\mathcal{O}_K$ is a Dedekind domain by Theorem 3.17, we simplify some terminology. An *integral ideal* of K is simply an integral ideal of $\mathcal{O}_K$, a *prime* of K is a prime of $\mathcal{O}_K$, and a *fractional ideal* of K is a fractional ideal of $\mathcal{O}_K$. The *ideal group* I_K of K is the ideal group of $\mathcal{O}_K$, we write P_K for the subgroup of principal fractional ideals of K, and the *ideal class group* $\mathrm{Cl}(K)$ of K is the ideal class group of $\mathcal{O}_K$. In particular,

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

The *class number* h_K of K is the class number of $\mathcal{O}_K$ and so

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

The *unit group* of K is the unit group of $\mathcal{O}_K$ and we call any element of $\mathcal{O}_K^*$ a *unit* of K (with the understanding that every element of K is invertible in K). It follows from Theorems 3.4 and 3.17 that integral ideals $\mathfrak{a}$ of K admit prime factorizations. One of our core investigations will be to understand how the principal integral ideal $p\mathcal{O}_K$ factors into a product of primes of K for any prime p. Moreover, we will be able to leverage geometric tools to show that the class number h_K is finite and completely describe the unit group $\mathcal{O}_K^*$.

4 Localization

Let $\mathcal{o}$ be a noetherian integral domain with field of fractions K. If $D \subseteq \mathcal{o} - \{0\}$ is a multiplicative subset (recall that necessarily $1 \in D$) then the *localization* $\mathcal{o}D^{-1}$ of $\mathcal{o}$ at D is defined by

$$\mathcal{o}D^{-1} = \left\{ \frac{\alpha}{\delta} \in K : \alpha \in \mathcal{o} \text{ and } \delta \in D \right\}.$$

Moreover, for any subset N of $\mathcal{o}$, we set

$$ND^{-1} = \left\{ \frac{\eta}{\delta} \in K : \eta \in N \text{ and } \delta \in D \right\}.$$

Now $\mathcal{o}D^{-1}$ is clearly a subring of K which is an integral domain and is it formed from $\mathcal{o}$ by making every element of D invertible. It is also noetherian for if $\mathfrak{A}$ is an ideal of $\mathcal{o}D^{-1}$, set $\mathfrak{a} = \mathfrak{A} \cap \mathcal{o}$. Then

$$\mathfrak{A} = \mathfrak{a}D^{-1}.$$

Indeed, the reverse containment is trivial. For the forward containment, if $\frac{\alpha}{\delta} \in \mathfrak{A}$ then $\alpha \in \mathfrak{a}$ because $\delta \in D$ and $\mathfrak{A}$ is an ideal of $\mathcal{O}D^{-1}$. Hence $\frac{\alpha}{\delta} \in \mathfrak{a}D^{-1}$ as desired. Since $\mathcal{O}$ is Dedekind, $\mathfrak{a}$ is a finitely generated $\mathcal{O}$-module and hence $\mathfrak{A}$ is a finitely generated $\mathcal{O}D^{-1}$-module by the identity we have just proved. Thus $\mathcal{O}D^{-1}$ is noetherian. It follows that if $\mathfrak{f}$ is a fractional ideal of $\mathcal{O}$ then $\mathfrak{f}D^{-1}$ is a fractional ideal of $\mathcal{O}D^{-1}$. We call $\mathfrak{f}D^{-1}$ the *localization* of $\mathfrak{f}$ at D. In the case of primes, we have an exact correspondence:

Proposition 4.1. *Let $\mathcal{O}$ be a noetherian integral domain and $D \subseteq \mathcal{O} - \{0\}$ be a multiplicative subset. Then the maps*

$$\mathfrak{q} \mapsto \mathfrak{q}D^{-1} \quad \textit{and} \quad \mathfrak{Q} \mapsto \mathfrak{Q} \cap \mathcal{O}.$$

are inverse inclusion-preserving bijections between the primes $\mathfrak{q}$ of $\mathcal{O}$ disjoint from D and the primes $\mathfrak{Q}$ of $\mathcal{O}D^{-1}$.

Proof. First suppose $\mathfrak{q}$ is a prime of $\mathcal{O}$ that is disjoint from D. We claim that the integral ideal $\mathfrak{q}D^{-1}$ of $\mathcal{O}D^{-1}$ is prime. Indeed, suppose $\frac{\alpha}{\delta}, \frac{\beta}{\gamma} \in \mathcal{O}D^{-1}$ are such that $\frac{\alpha\beta}{\delta\gamma} \in \mathfrak{q}D^{-1}$. Then $\alpha\beta \in \mathfrak{q}$ and thus $\alpha \in \mathfrak{q}$ or $\beta \in \mathfrak{q}$ because $\mathfrak{q}$ is prime. Hence $\frac{\alpha}{\delta} \in \mathfrak{q}D^{-1}$ or $\frac{\beta}{\gamma} \in \mathfrak{q}D^{-1}$ as desired. Also, the prime $\mathfrak{q}D^{-1}$ satisfies

$$\mathfrak{q} = \mathfrak{q}D^{-1} \cap \mathcal{O}.$$

The forward inclusion is obvious. For the reverse inclusion, if $\frac{\alpha}{\delta} \in \mathfrak{q}D^{-1} \cap \mathcal{O}$ then $\alpha \in \mathfrak{q}$ and hence $\frac{\alpha}{\delta} \in \mathfrak{q}$ because $\mathfrak{q}$ is prime and $\delta \notin \mathfrak{q}$ (as $\mathfrak{q}$ is disjoint from D). Now suppose $\mathfrak{Q}$ is a prime of $\mathcal{O}D^{-1}$. We claim that $\mathfrak{Q} \cap \mathcal{O}$ is a prime of $\mathcal{O}$ that is disjoint from D. It is clearly an integral ideal of $\mathcal{O}$ and is prime because $\mathfrak{Q}$ is. If $\mathfrak{Q} \cap \mathcal{O}$ is not disjoint from D then $\delta \in \mathfrak{Q} \cap \mathcal{O}$ with $\delta \in D$. Hence $1 \in \mathfrak{Q} \cap \mathcal{O}$ because $\frac{1}{\delta} \in \mathcal{O}D^{-1}$ and $\mathfrak{Q}$ is an integral ideal of $\mathcal{O}D^{-1}$. This is impossible since $\mathfrak{Q} \cap \mathcal{O}$ is prime (hence proper) and therefore must be disjoint from D. Moreover, the prime $\mathfrak{Q} \cap \mathcal{O}$ satisfies

$$\mathfrak{Q} = (\mathfrak{Q} \cap \mathcal{O})D^{-1}.$$

The reverse inclusion is obvious since $1 \in D$. For the forward inclusion, if $\frac{\alpha}{\delta} \in \mathfrak{Q}$ then $\alpha \in \mathfrak{Q} \cap \mathcal{O}$ and thus $\frac{\alpha}{\delta} \in (\mathfrak{Q} \cap \mathcal{O})D^{-1}$. All of this together shows that the mappings

$$\mathfrak{q} \mapsto \mathfrak{q}D^{-1} \quad \text{and} \quad \mathfrak{Q} \mapsto \mathfrak{Q} \cap \mathcal{O}.$$

are inverse bijections between the primes $\mathfrak{q}$ of $\mathcal{O}$ disjoint from D and the primes $\mathfrak{Q}$ of $\mathcal{O}D^{-1}$. They are clearly inclusion-preserving. □

From Proposition 4.1, the primes of $\mathcal{O}D^{-1}$ are of the form $\mathfrak{p}D^{-1}$ for primes $\mathfrak{p}$ of $\mathcal{O}$ disjoint from D.

Remark 4.2. The bijections in Proposition 4.1 need not hold for all integral ideals.

Localization is most useful when we localize at the compliment of a prime or collection of primes. If $\mathfrak{p}$ is a prime of $\mathcal{o}$ then $\mathcal{o}-\mathfrak{p}\subset\mathcal{o}-\{0\}$ is a multiplicative subset. Indeed, the inclusion is obvious, $1\in\mathcal{o}-\mathfrak{p}$ because $\mathfrak{p}$ is proper and thus does not contain units, and if $\alpha,\beta\in\mathcal{o}-\mathfrak{p}$ we have $\alpha\beta\notin\mathfrak{p}$ because $\mathfrak{p}$ is prime so that $\alpha\beta\in\mathcal{o}-\mathfrak{p}$ and thus $\mathcal{o}-\mathfrak{p}$ is closed under multiplication. We define the *localization* $\mathcal{o}_{\mathfrak{p}}$ of $\mathcal{o}$ at $\mathfrak{p}$ by

$$\mathcal{o}_{\mathfrak{p}}=\mathcal{o}(\mathcal{o}-\mathfrak{p})^{-1}.$$

In other words,

$$\mathcal{o}_{\mathfrak{p}}=\left\{\frac{\alpha}{\delta}\in K:\alpha,\delta\in\mathcal{o}\text{ with }\delta\not\equiv 0 \pmod{\mathfrak{p}}\right\}.$$

Essentially, localizing at a prime $\mathfrak{p}$ removes all of the algebraic information about $\mathcal{o}$ that has nothing to do with $\mathfrak{p}$. If $\mathfrak{f}$ is a fractional ideal of $\mathcal{o}$ then the *localization* $\mathfrak{f}_{\mathfrak{p}}$ of $\mathfrak{f}$ at $\mathfrak{p}$ is defined to be

$$\mathfrak{f}_{\mathfrak{p}}=\mathfrak{f}(\mathcal{o}-\mathfrak{p})^{-1}.$$

More generally, let X be a set of primes in $\mathcal{o}$ and consider

$$\mathcal{o}-\bigcup_{\mathfrak{p}\in X}\mathfrak{p}.$$

Then $\mathcal{o}-\bigcup_{\mathfrak{p}\in X}\mathfrak{p}\subseteq\mathcal{o}-\{0\}$ is a multiplicative subset because

$$\mathcal{o}-\bigcup_{\mathfrak{p}\in X}\mathfrak{p}=\bigcap_{\mathfrak{p}\in X}(\mathcal{o}-\mathfrak{p}),$$

and the $\mathcal{o}-\mathfrak{p}$ are. We define the *localization* $\mathcal{o}(X)$ of $\mathcal{o}$ at X by

$$\mathcal{o}(X)=\mathcal{o}\left(\mathcal{o}-\bigcup_{\mathfrak{p}\in X}\mathfrak{p}\right)^{-1}.$$

Equivalently,

$$\mathcal{o}(X)=\left\{\frac{\alpha}{\delta}\in K:\alpha,\delta\in\mathcal{o}\text{ with }\delta\not\equiv 0 \pmod{\mathfrak{p}}\text{ for some }\mathfrak{p}\in X\right\}.$$

If $\mathfrak{f}$ is a fractional ideal of $\mathcal{o}$ then the *localization* $\mathfrak{f}(X)$ of $\mathfrak{f}$ at X is defined to be

$$\mathfrak{f}(X)=\mathfrak{f}\left(\mathcal{o}-\bigcup_{\mathfrak{p}\in X}\mathfrak{p}\right)^{-1}.$$

Note that if $X=\{\mathfrak{p}\}$ then $\mathcal{o}(X)=\mathcal{o}_{\mathfrak{p}}$ and $\mathfrak{f}(X)=\mathfrak{f}_{\mathfrak{p}}$. In any case, localizing is a useful tool in algebraic investigations and we quickly collect some useful properties. First, localization respects integral closure:

Proposition 4.3. *Let $\mathcal{o}$ be a noetherian integral domain with field of fractions K, L/K be a finite separable extension, and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. Then for any multiplicative set $D\subseteq\mathcal{o}-\{0\}$, $\mathcal{O}D^{-1}$ is the integral closure of $\mathcal{o}D^{-1}$ in L.*

Proof. We need to show that $\mathcal{O}D^{-1} = \overline{\mathcal{o}D^{-1}}$. For the forward inclusion, let $\frac{\alpha}{\delta} \in \mathcal{O}D^{-1}$. As $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in L, α is integral over $\mathcal{o}$ so that

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

for some $n \geq 1$ and $a_i \in \mathcal{o}$ for $0 \leq i \leq n-1$. Diving by δ^n, we obtain

$$\left(\frac{\alpha}{\delta}\right)^n + \frac{a_{n-1}}{\delta}\left(\frac{\alpha}{\delta}\right)^{n-1} + \cdots + \frac{a_0}{\delta^n} = 0.$$

Thus $\frac{\alpha}{\delta}$ is the root of a monic polynomial with coefficients in $\mathcal{o}D^{-1}$. Therefore the forward inclusion holds. For the reverse inclusion, suppose $\lambda \in \overline{\mathcal{o}D^{-1}}$. Then

$$\lambda^n + \frac{a_{n-1}}{\delta_{n-1}}\lambda^{n-1} + \cdots + \frac{a_0}{\delta_0} = 0,$$

for some $n \geq 1$ and $\frac{a_i}{\delta_i} \in \mathcal{o}D^{-1}$ for $0 \leq i \leq n-1$. Letting $\delta = \delta_0 \cdots \delta_{n-1}$ and multiplying by δ^n, we obtain

$$(\lambda\delta)^n + \frac{a_{n-1}\delta}{\delta_{n-1}}(\lambda\delta)^{n-1} + \cdots + \frac{a_0\delta^n}{\delta_0} = 0.$$

It follows that $\lambda\delta$ is the root of a monic polynomial with coefficients in $\mathcal{o}$. As $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in L, we have $\lambda\delta \in \mathcal{o}$ and thus $\lambda \in \mathcal{o}D^{-1}$. This proves the reverse inclusion which means $\mathcal{O}D^{-1}$ is the integral closure of $\mathcal{o}D^{-1}$ in L. □

In the case of Proposition 4.3, we setup some additional notation. Again suppose $\mathcal{o}$ is a noetherian integral domain with field of fractions K, L/K be a finite separable extension, and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. If $\mathfrak{p}$ is a prime of $\mathcal{o}$ and $\mathfrak{F}$ is a fractional ideal of $\mathcal{O}$, the *localization* $\mathfrak{F}_\mathfrak{p}$ of $\mathfrak{F}$ at $\mathfrak{p}$ is defined by

$$\mathfrak{F}_\mathfrak{p} = \mathfrak{F}(\mathcal{o} - \mathfrak{p})^{-1}.$$

More generally, let X be a set of primes of $\mathcal{o}$. Then the *localization* $\mathfrak{F}(X)$ of $\mathfrak{F}$ at X is defined by

$$\mathfrak{F}(X) = \mathfrak{F}\left(\mathcal{o} - \bigcup_{\mathfrak{p} \in X} \mathfrak{p}\right)^{-1}.$$

In particular, Proposition 4.3 shows that $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}(X)$ are the integral closures of $\mathcal{o}_\mathfrak{p}$ and $\mathcal{o}(X)$ respectively. Our second property says intersections of localizations behave with respect to fractional ideals and units:

Proposition 4.4. *Let $\mathcal{o}$ be a noetherian integral domain. Then for every fractional ideal $\mathfrak{f}$ of $\mathcal{o}$, we have*

$$\mathfrak{f} = \bigcap_{\mathfrak{p}} \mathfrak{f}_\mathfrak{p}.$$

In particular,

$$\mathcal{o} = \bigcap_{\mathfrak{p}} \mathcal{o}_\mathfrak{p} \quad \textit{and} \quad \mathcal{o}^* = \bigcap_{\mathfrak{p}} \mathcal{o}_\mathfrak{p}^*.$$

Proof. The first identity follows from the second by multiplying by a fractional ideal $\mathfrak{f}$ of $\mathcal{O}$. As for the second identity, the forward containment is obvious. For the reverse containment, suppose $\frac{\alpha}{\beta} \in \bigcap_{\mathfrak{p} \text{ prime}} \mathcal{O}_{\mathfrak{p}}$ and set

$$\mathfrak{a} = \{\gamma \in \mathcal{O} : \alpha\gamma \in \beta\mathcal{O}\}.$$

Then $\mathfrak{a}$ is clearly an integral ideal of $\mathcal{O}$ as $\beta \in \mathfrak{a}$. It also cannot be contained in any prime $\mathfrak{p}$. Indeed, since $\frac{\alpha}{\beta} \in \mathcal{O}_{\mathfrak{p}}$ we have $\beta \notin \mathfrak{p}$ and so $\beta \in \mathfrak{a} - \mathfrak{p}$. As $\mathcal{O}$ is noetherian (which we recall is equivalent to every nonempty collection of ideals having a maximal element), there exists a maximal integral ideal $\mathfrak{m}$ which is necessarily prime. As $\mathfrak{a}$ is not contained in any prime, $\mathfrak{a}$ is not contained in $\mathfrak{m}$ and thus $\mathfrak{a} = \mathcal{O}$. But then $1 \in \mathfrak{a}$ and so $\alpha \in \beta\mathcal{O}$ implying $\frac{\alpha}{\beta} \in \mathcal{O}$ which proves the reverse containment and the second identity follows. For the third identity, the forward containment is clear. For the reverse containment, suppose $\frac{\alpha}{\beta} \in \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$. We have already showed $\frac{\alpha}{\beta} \in \mathcal{O}$ so it suffices to show $\frac{\alpha}{\beta}$ is a unit. As $\beta \notin \mathfrak{p}$ for any prime $\mathfrak{p}$, it is necessarily not in any maximal integral ideal. Therefore $\beta \in \mathcal{O}^*$ because the complement of the union of all maximal integral ideals is exactly the set of units. Interchanging the roles of α and β shows that $\alpha \in \mathcal{O}^*$ as well. Hence $\frac{\alpha}{\beta} \in \mathcal{O}^*$ which proves the reverse containment and the third equality follows. □

A noetherian integral domain is said to be *local* if it has a unique maximal integral ideal. As we might expect, localizing at a prime will produce a local noetherian integral domain and hence justifies the term localization. We claim that $\mathcal{O}_{\mathfrak{p}}$ is a local noetherian integral domain with maximal integral ideal $\mathfrak{p}_{\mathfrak{p}}$. Indeed, $\mathcal{O}_{\mathfrak{p}}$ is already a noetherian integral domain and it is clear that $\mathfrak{p}_{\mathfrak{p}}$ is an ideal of $\mathcal{O}_{\mathfrak{p}}$. By Proposition 4.1, the map

$$\mathfrak{q} \to \mathfrak{q}_{\mathfrak{p}},$$

is a bijection between the primes of $\mathcal{O}$ contained in $\mathfrak{p}$ the primes of $\mathcal{O}_{\mathfrak{p}}$. As maximal integral ideals are necessarily prime, $\mathfrak{p}_{\mathfrak{p}}$ is the unique maximal integral ideal of $\mathcal{O}_{\mathfrak{p}}$. This implies

$$\mathcal{O}_{\mathfrak{p}}^* = \mathcal{O}_{\mathfrak{p}} - \mathfrak{p}_{\mathfrak{p}},$$

because the complement of the union of all maximal integral ideals is exactly the set of units and $\mathfrak{p}_{\mathfrak{p}}$ is the only one. It follows that $\mathcal{O}_{\mathfrak{p}}^* + \mathfrak{p}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^*$. Indeed, the reverse containment is trivial and the forward containment follows since otherwise $\mathcal{O}_{\mathfrak{p}}^* + \mathfrak{p}_{\mathfrak{p}} \subseteq \mathfrak{p}_{\mathfrak{p}}$ which would imply $\mathcal{O}_{\mathfrak{p}}^* \subseteq \mathfrak{p}_{\mathfrak{p}}$ and this is impossible because $\mathfrak{p}_{\mathfrak{p}}$ is maximal (hence proper). In other words, the sum of a unit of $\mathcal{O}_{\mathfrak{p}}$ and an element of $\mathfrak{p}_{\mathfrak{p}}$ is a unit of $\mathcal{O}_{\mathfrak{p}}$. Also, if $\mathfrak{p}$ itself is maximal we can say more:

Proposition 4.5. *Let $\mathcal{O}$ be a noetherian integral domain and $\mathfrak{p}$ be a prime. Then there is an embedding*

$$\mathcal{O}/\mathfrak{p} \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}},$$

identifying $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$ with the field of fractions of $\mathcal{O}/\mathfrak{p}$. In particular, if $\mathfrak{p}$ is maximal we have

$$\mathcal{O}/\mathfrak{p}^n \cong \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}^n,$$

for all $n \geq 1$.

Proof. Let $n \geq 1$ and consider the homomorphism

$$\phi : \mathcal{O}/\mathfrak{p}^n \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}^n \qquad \alpha + \mathfrak{p}^n \mapsto \alpha + \mathfrak{p}_{\mathfrak{p}}^n.$$

By Proposition 4.1, $\mathfrak{p} = \mathfrak{p}_{\mathfrak{p}} \cap \mathcal{O}$ and therefore this map is an embedding when $n = 1$. As $\mathfrak{p}_{\mathfrak{p}}$ is maximal, $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}$ is a field and thus must be the field of fractions of $\mathcal{O}/\mathfrak{p}$ under this embedding. It remains to prove the last statement so suppose $\mathfrak{p}$ is maximal. We will show ϕ is both injective and surjective which will finish the proof. For injectivity, it suffices to prove $\ker \phi = 0$. So let α be a representative of a coset in $\mathcal{O}/\mathfrak{p}$ such that $\alpha \in \mathfrak{p}_{\mathfrak{p}}^n$. Then $\alpha = \frac{\beta}{\delta}$ with $\beta \in \mathfrak{p}^n$ and $\delta \notin \mathfrak{p}$. Thus β is a representative of the zero coset in $\mathcal{O}/\mathfrak{p}^n$ and so α must be too which implies $\ker \phi = 0$ and injectivity follows. For surjectivity, we first claim that the image of every $\delta \in \mathcal{O} - \mathfrak{p}$ is a unit in $\mathcal{O}/\mathfrak{p}^n$ which equivalent to the fact that $\mathfrak{p}^n + \delta\mathcal{O} = \mathcal{O}$ since there is then a $\gamma \in \mathcal{O}$ such that $\delta - \gamma \in \mathfrak{p}^n$. For $n = 1$, maximality of $\mathfrak{p}$ implies $\mathfrak{p} + \delta\mathcal{O} = \mathcal{O}$. We now argue by induction, so suppose the claim holds for $\mathcal{O}/\mathfrak{p}^{n-1}$. Then $\mathfrak{p}^{n-1} + \delta\mathcal{O} = \mathcal{O}$ whence $\mathfrak{p}^n + \delta\mathfrak{p} = \mathfrak{p}$ and therefore $\mathfrak{p}^n + \delta\mathcal{O} = \mathcal{O}$ by the primality of $\mathfrak{p}$. Now let $\frac{\alpha}{\delta}$ be a representative of a coset in $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}_{\mathfrak{p}}^n$. As $\delta \notin \mathfrak{p}$, what we have just proved shows that the coset represented by δ in $\mathcal{O}/\mathfrak{p}^n$ is invertible. Hence $\frac{\alpha}{\delta}$ represents a coset in $\mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ which proves surjectivity. $\square$

A *discrete valuation ring* is a principal ideal domain with a unique maximal integral ideal (recall that principal ideal domains are necessarily noetherian integral domains). In other words, a discrete valuation ring is a local principal ideal domain and is a particularly simple example of a local noetherian integral domain. As principal ideal domains are integrally closed by Lemma 1.3, discrete valuation rings are necessarily Dedekind domains. In fact, they are Dedekind domains with exactly one prime by Proposition 3.12. If $\mathcal{O}$ is a discrete valuation ring and $\mathfrak{p}$ is its maximal integral ideal (necessarily prime) then $\mathfrak{p}$ is of the form $\mathfrak{p} = \pi\mathcal{O}$ for some prime $\pi \in \mathcal{O}$. We call π a *uniformizer* of $\mathcal{O}$ and it is uniquely defined up to multiplication by units of $\mathcal{O}$. As every element not in $\mathfrak{p}$ is a unit (since $\mathcal{O}$ is local) and $\mathcal{O}$ is a unique factorization domain (because it is a principal ideal domain), it follows that every $\alpha \in \mathcal{O}$ is of the form $\alpha = \varepsilon\pi^n$ for some $\varepsilon \in \mathcal{O}^*$ and $n \geq 0$. In particular, π is the only prime of $\mathcal{O}$ up to multiplication by units and every integral ideal of $\mathcal{O}$ is of the form $\mathfrak{p}^n$ for some $n \geq 0$. As $\mathcal{O}$ is a principal ideal domain, it follows that $\mathfrak{p}$ is also the only prime of $\mathcal{O}$. Thus $\mathfrak{p}$ is both the unique maximal integral ideal and prime $\mathcal{O}$. Moreover, if K is the field of fractions of $\mathcal{O}$ then every nonzero $\kappa \in K$ can be uniquely expressed as

$$\kappa = \varepsilon\pi^n,$$

for some $\varepsilon \in \mathcal{O}^*$ and $n \in \mathbb{Z}$. The *valuation* v associated to $\mathcal{O}$ on K is the function defined by

$$v : K \to \mathbb{Z} \cup \{\infty\} \qquad \kappa \mapsto v(\kappa) = \begin{cases} n & \text{if } \kappa = \varepsilon\pi^n, \\ \infty & \text{if } \kappa = 0. \end{cases}$$

We call $v(\kappa)$ the *valuation* of κ with respect to $\mathcal{O}$. Note that $v(\kappa) = 0$ if and only if κ is a unit in $\mathcal{O}$. If $\kappa \neq 0$ then the $v(\kappa)$ is characterized by the equation

$$\kappa\mathcal{O} = \mathfrak{p}^{v(\kappa)}, \tag{5}$$

since $\kappa = \varepsilon\pi^{v(\kappa)}$. Moreover, if $\kappa = \varepsilon\pi^n$ and $\eta = \delta\pi^m$, we have

$$\kappa\eta = \varepsilon\delta\pi^{n+m} \quad \text{and} \quad \kappa + \eta = (\varepsilon\pi^{n-\min(n,m)} + \delta\pi^{m-\min(n,m)})\pi^{\min(n,m)},$$

where $\varepsilon\pi^{n-\min(n,m)} + \delta\pi^{m-\min(n,m)}$ is a unit of $\mathcal{O}$ because one of the exponents of π is zero so that it is a sum of a unit of $\mathcal{O}$ and an element of $\mathfrak{p}$. Therefore v satisfies the properties

$$v(\kappa\eta) = v(\kappa) + v(\eta) \quad \text{and} \quad v(\kappa + \eta) \geq \min(v(\kappa), v(\eta)). \tag{6}$$

In view of the first identity in Equation (6), v restricted to K^* is a surjective homomorphism. Discrete valuation rings, and hence valuation themselves, arise as as localizations of Dedekind domains at primes. Before we deduce this, we will establish a few facts. The first is that localization respects inversion of fractional ideals:

Proposition 4.6. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and $D \subseteq \mathcal{O} - \{0\}$ be a multiplicative subset. Then for any fractional ideal $\mathfrak{f}$, we have*

$$\mathfrak{f}^{-1}D^{-1} = (\mathfrak{f}D^{-1})^{-1}.$$

Proof. In light of the fact that every fractional ideal $\mathfrak{f}$ is of the form $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$, we have $\mathfrak{f}^{-1} = \delta\mathfrak{a}^{-1}$ and so it suffices to prove the claim for integral ideals. We will show $\mathfrak{a}^{-1}D^{-1} = (\mathfrak{a}D^{-1})^{-1}$. For the forward inclusion, let $\frac{\alpha}{\delta} \in \mathfrak{a}^{-1}D^{-1}$. Since $\alpha \in \mathfrak{a}^{-1}$, Proposition 3.8 implies $\alpha\mathfrak{a} \subseteq \mathcal{O}$ and therefore $\frac{\alpha}{\delta}\mathfrak{a}D^{-1} \subseteq \mathcal{O}D^{-1}$. Invoking Proposition 3.8 again shows $\frac{\alpha}{\delta} \in (\mathfrak{a}D^{-1})^{-1}$ which proves the forward inclusion. For the reverse inclusion, suppose $\kappa \in (\mathfrak{a}D^{-1})^{-1}$. By Proposition 3.8, $\kappa\mathfrak{a}D^{-1} \subseteq \mathcal{O}D^{-1}$ and multiplying by $\mathfrak{a}^{-1}$ shows $\kappa \in \mathfrak{a}^{-1}D^{-1}$ since $\mathfrak{a}$ is an ideal of $\mathcal{O}$. This proves the reverse inclusion. □

Our second fact is that that the localization of a Dedekind domain is again a Dedekind domain:

Proposition 4.7. *Let $\mathcal{O}$ be a Dedekind domain and $D \subseteq \mathcal{O} - \{0\}$ be a multiplicative subset. Then $\mathcal{O}D^{-1}$ is a Dedekind domain.*

Proof. We have seen that $\mathcal{O}D^{-1}$ is a noetherian integral domain since $\mathcal{O}$ is. $\mathcal{O}D^{-1}$ is also integrally closed by Proposition 4.3. It remains to show that every prime of $\mathcal{O}D^{-1}$ is maximal. Letting $\mathfrak{p}D^{-1}$ be such prime, we see that it must be maximal because $\mathfrak{p}$ is and the bijections in Proposition 4.1 are inclusion-preserving. □

As an immediate consequence of Proposition 4.7, the localization $\mathcal{O}_{\mathfrak{p}}$ at any prime $\mathfrak{p}$ is a Dedekind domain if $\mathcal{O}$ is. We can now show that localizing a Dedekind domain at a prime produces a discrete valuation ring. Actually, we will prove the following stronger statement:

Theorem 4.8. *Let $\mathcal{O}$ be a noetherian integral domain. Then $\mathcal{O}$ is a Dedekind domain if and only if $\mathcal{O}_{\mathfrak{p}}$ is a discrete valuation ring for all primes $\mathfrak{p}$.*

Proof. Recall that $\mathcal{O}_\mathfrak{p}$ is local for any prime $\mathfrak{p}$ of $\mathcal{O}$ and so $\mathfrak{p}_\mathfrak{p}$ is the unique maximal integral ideal of $\mathcal{O}_\mathfrak{p}$. For the forward implication, suppose $\mathcal{O}$ is a Dedekind domain. Then $\mathcal{O}_\mathfrak{p}$ is as well by Proposition 4.7. Since primes are maximal in Dedekind domains, $\mathfrak{p}_\mathfrak{p}$ is also the only prime of $\mathcal{O}_\mathfrak{p}$. By uniqueness of prime factorizations of fractional ideals, there exists $\pi \in \mathfrak{p}_\mathfrak{p} - \mathfrak{p}_\mathfrak{p}^2$ and hence $\mathfrak{p}_\mathfrak{p} = \pi\mathcal{O}_\mathfrak{p}$ which further implies $\mathfrak{p}_\mathfrak{p}^n = \pi^n\mathcal{O}_\mathfrak{p}$ for all $n \geq 1$. As these are the only integral ideals of $\mathcal{O}_\mathfrak{p}$, we see that $\mathcal{O}_\mathfrak{p}$ is a principal ideal domain and hence a discrete valuation ring. This proves the forward implication. For the reverse implication, suppose all of the localizations $\mathcal{O}_\mathfrak{p}$ are discrete valuation rings. Then they are principal ideal domains and hence integrally closed by Lemma 1.3. As the intersection of integrally closed rings is clearly integrally closed, it follows from Proposition 4.4 that $\mathcal{O}$ is integrally closed and therefore an integrally closed integral domain by our assumptions. As $\mathcal{O}$ is noetherian by assumption, it remains to show that every prime $\mathfrak{q}$ of $\mathcal{O}$ is maximal. Since $\mathcal{O}$ is noetherian (which we recall is equivalent to every nonempty collection of ideals having a maximal element), $\mathfrak{q} \subseteq \mathfrak{p}$ for some maximal integral ideal $\mathfrak{p}$ which is necessarily prime. Under the inclusion-preserving bijections in Proposition 4.1, we have

$$\mathfrak{q} = \mathfrak{q}_\mathfrak{p} \cap \mathcal{O} = \mathfrak{p}_\mathfrak{p} \cap \mathcal{O} = \mathfrak{p},$$

where the middle equality holds because $\mathfrak{q}_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$ as $\mathcal{O}_\mathfrak{p}$ has a unique prime which is also the unique maximal integral ideal as we have seen. Hence $\mathfrak{q}$ itself must be maximal. □

Proposition 4.4 and Theorem 4.8 together form a powerful simplification tool for Dedekind domains $\mathcal{O}$. For if we want to prove a property about a fractional ideal $\mathfrak{f}$ of $\mathcal{O}$, Proposition 4.4 implies that it suffices to show this property holds for the corresponding fractional ideals $\mathfrak{f}_\mathfrak{p}$ in the localizations $\mathcal{O}_\mathfrak{p}$ at all primes $\mathfrak{p}$ and is preserved under intersections. Moreover, the localizations $\mathcal{O}_\mathfrak{p}$ are discrete valuation rings by Theorem 4.8 in addition to being Dedekind domains by Proposition 4.7. In particular, the localizations $\mathcal{O}_\mathfrak{p}$ are also principal ideal domains. This latter fact is often immensely helpful. In any case, let $v_\mathfrak{p}$ denote the valuation of $\mathcal{O}_\mathfrak{p}$. We call $v_\mathfrak{p}$ the **valuation** associated to the prime $\mathfrak{p}$ of $\mathcal{O}$. These valuations are intimately connected to the prime factorization of principal fractional ideals. Indeed, the prime factorization of fractional ideals implies that for any $\kappa \in K^*$, we have

$$\kappa\mathcal{O} = \prod_{\mathfrak{q} \text{ prime}} \mathfrak{q}^{e_\mathfrak{q}},$$

where the product is taken over all primes $\mathfrak{q}$ of $\mathcal{O}$, $e_\mathfrak{q} \in \mathbb{Z}$ for all $\mathfrak{q}$, and all but finitely many of the $e_\mathfrak{q}$ are zero. We claim that $v_\mathfrak{p}(\kappa) = e_\mathfrak{p}$ for all primes $\mathfrak{p}$. To see this, first observe that if $\mathfrak{p}$ and $\mathfrak{q}$ are distinct primes then we have $\mathfrak{q}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. Indeed, by uniqueness of prime factorizations of fractional ideals choose $\alpha \in \mathfrak{q} - \mathfrak{p}$. Then $\alpha \in \mathfrak{q}_\mathfrak{p} - \mathfrak{p}_\mathfrak{p}$ and hence α is invertible in $\mathcal{O}_\mathfrak{p}$ because $\mathcal{O}_\mathfrak{p}^* = \mathcal{O}_\mathfrak{p} - \mathfrak{p}_\mathfrak{p}$. Therefore $1 \in \mathfrak{q}_\mathfrak{p}$ and so the integral ideal $\mathfrak{q}_\mathfrak{p}$ must be $\mathcal{O}_\mathfrak{p}$. This fact and the prime factorization of $\kappa\mathcal{O}$ together imply

$$\kappa\mathcal{O}_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}^{e_\mathfrak{p}},$$

and we readily see that $v_{\mathfrak{p}}(\kappa) = e_{\mathfrak{p}}$ by Equation (5). In particular, $v_{\mathfrak{p}}(\kappa) = 0$ for all but finitely many primes $\mathfrak{p}$.

Remark 4.9. The valuation $v_{\mathfrak{p}}$ associated to the prime $\mathfrak{p}$ of $\mathcal{O}$ is sometimes called an *exponential valuation.*

Continue to let $\mathcal{O}$ be a Dedekind domain with field of fractions K and let X be a set of all but finitely many primes of $\mathcal{O}$. Then $\mathcal{O}(X)$ is a Dedekind domain by Proposition 4.7 and by Proposition 4.1 the primes $\mathfrak{p}_X$ of $\mathcal{O}(X)$ are of the form $\mathfrak{p}_X = \mathfrak{p}(X)$ for $\mathfrak{p} \in X$. Moreover, $\mathcal{O}$ and $\mathcal{O}(X)$ have the same localizations at $\mathfrak{p}$ and $\mathfrak{p}_X$ respectively. That is,

$$\mathcal{O}_{\mathfrak{p}} = \mathcal{O}(X)_{\mathfrak{p}_X}. \tag{7}$$

Indeed, observe that

$$\mathcal{O}(X)_{\mathfrak{p}_X} = \left\{ \frac{\alpha\gamma}{\beta\delta} \in K : \alpha, \beta, \gamma, \delta \in \mathcal{O} \text{ with } \delta \not\equiv 0 \pmod{\mathfrak{p}} \text{ and } \beta, \gamma \not\equiv 0 \pmod{\mathfrak{q}} \text{ for some } \mathfrak{p}, \mathfrak{q} \in X \right\},$$

which is exactly $\mathcal{O}_{\mathfrak{p}}$. From Equation (7) and the fact that the primes $\mathfrak{p}_X$ are the only primes of $\mathcal{O}(X)$, the prime factorization of a fractional ideal $\mathfrak{f}(X)$ of $\mathcal{O}(X)$, for a fractional ideal $\mathfrak{f}$ of $\mathcal{O}$, is obtained from that of $\mathfrak{f}$ by removing those primes factors corresponding to primes not in X. Also, from Proposition 4.4 and Equation (7) we conclude that the original fractional ideal can be recovered by taking the intersections of $\mathfrak{f}(X)_{\mathfrak{p}}$ for all $\mathfrak{p} \notin X$. Moreover, the ideal class and unit groups of $\mathcal{O}(X)$ are related to those of $\mathcal{O}$ via the following exact sequence:

Proposition 4.10. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and let X be set of all but finitely many primes of $\mathcal{O}$. Then the sequence*

$$1 \longrightarrow \mathcal{O}^* \longrightarrow \mathcal{O}(X)^* \longrightarrow \bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^* \xrightarrow{\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_{\mathfrak{p}}}} \mathrm{Cl}(\mathcal{O}) \xrightarrow{\mathcal{O}(X)} \mathrm{Cl}(\mathcal{O}(X)) \longrightarrow 1,$$

where the fourth map takes the representative $(\kappa_{\mathfrak{p}})_{\mathfrak{p}\notin X}$ of a coset in $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$ to the coset represented by $\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_{\mathfrak{p}}(\kappa_{\mathfrak{p}})}$ in $\mathrm{Cl}(\mathcal{O})$ and the fifth map takes the representative $\mathfrak{a}$ of an ideal class in $\mathrm{Cl}(\mathcal{O})$ to the ideal class represented by $\mathfrak{a}(X)$ in $\mathrm{Cl}(\mathcal{O}(X))$, is exact. Moreover, $K^*/\mathcal{O}_{\mathfrak{p}}^* \cong \mathbb{Z}$ for all primes $\mathfrak{p}$ of $\mathcal{O}$.

Proof. The sequence is exact at $\mathcal{O}^*$ because the second map is injective. For exactness at $\mathcal{O}(X)^*$, it is clear that the image of the second map belongs to the kernel of the third map. So suppose $\alpha \in \mathcal{O}(X)^*$ belongs to the kernel of the third map. Then $\alpha \in \mathcal{O}_{\mathfrak{p}}^*$ for all $\mathfrak{p} \notin X$ and for all $\mathfrak{p} \in X$ as well by Equation (7). It follows from Proposition 4.4 that $\alpha \in \mathcal{O}^*$ so it is in the image of the second map which proves exactness at $\mathcal{O}(X)^*$. For exactness at $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$, from Equation (7) again we see that the image of the third map is contained in the kernel of the fourth. So suppose

$(\kappa_\mathfrak{p})_{\mathfrak{p}\notin X}$ is a representative of a coset in $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_\mathfrak{p}^*$ that is contained in the kernel of the fourth map. Then there is a $\kappa \in K^*$ such that

$$\prod_{\mathfrak{p}\notin X} \mathfrak{p}^{v_\mathfrak{p}(\kappa_\mathfrak{p})} = \kappa\mathcal{O} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(\kappa)}.$$

By the prime factorization of fractional ideals, $v_\mathfrak{p}(\kappa) = 0$ for all $\mathfrak{p} \in X$ and $v_\mathfrak{p}(\kappa) = v_\mathfrak{p}(\kappa_\mathfrak{p})$ for all $\mathfrak{p} \notin X$. As $v_\mathfrak{p}(\kappa) = 0$ for all $\mathfrak{p} \in X$, we have $\kappa \in \mathcal{O}_\mathfrak{p}^*$ for all $\mathfrak{p} \in X$. Because the primes of $\mathcal{O}(X)$ are $\mathfrak{p}_X$ for $\mathfrak{p} \in X$, Equation (7) and Proposition 4.4 together imply that $\bigcap_{\mathfrak{p}\in X} \mathcal{O}_\mathfrak{p}^* = \mathcal{O}(X)^*$ and therefore $\kappa \in \mathcal{O}(X)^*$. As $v_\mathfrak{p}(\kappa) = v_\mathfrak{p}(\kappa_\mathfrak{p})$ for all $\mathfrak{p} \notin X$, we have $\kappa \equiv \kappa_\mathfrak{p} \pmod{\mathcal{O}_\mathfrak{p}^*}$ for all $\mathfrak{p} \notin X$ because they have the same power of a uniformizer for $\mathcal{O}_\mathfrak{p}^*$. We have shown that $\kappa \in \mathcal{O}(X)^*$ and $\kappa \equiv \kappa_\mathfrak{p} \pmod{\mathcal{O}_\mathfrak{p}^*}$ for all $\mathfrak{p} \notin X$ which means κ maps to $(\kappa_\mathfrak{p})_{\mathfrak{p}\notin X}$ under the third map. In other words, $(\kappa_\mathfrak{p})_{\mathfrak{p}\notin X}$ is in the image of the third map proving exactness at $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_\mathfrak{p}^*$. For exactness at $\mathrm{Cl}(\mathcal{O})$, we first show that $\mathfrak{p}(X) = \mathcal{O}(X)$ for any prime $\mathfrak{p} \notin X$. Indeed, by maximality we can choose $\alpha \in \mathfrak{p} - \bigcup_{\mathfrak{q}\in X} \mathfrak{q}$. This fores α to be invertible in $\mathcal{O}(X)$ so that $1 \in \mathfrak{p}(X)$ and hence the ideal $\mathfrak{p}(X)$ must be $\mathcal{O}(X)$. It follows that the image of the fourth map is contained in the kernel of the fifth. Now suppose $\mathfrak{a}$ is an integral ideal representing a class in $\mathrm{Cl}(\mathcal{O})$ that is contained in the kernel of the fifth map. Then there is a $\kappa \in K^*$ such that

$$\mathfrak{a}(X) = \kappa\mathcal{O}(X),$$

In view of Equation (7) and Proposition 4.4 again, taking the intersection with the localizations $\mathcal{O}_\mathfrak{p}$ for all $\mathfrak{p} \notin X$ shows that

$$\mathfrak{a} = \kappa\mathcal{O}.$$

Therefore $(v_\mathfrak{p}(\kappa))_{\mathfrak{p}\notin X}$ is a representative of a coset in $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_\mathfrak{p}^*$ whose image under the fourth map is $\mathfrak{a}$. In other words, $\mathfrak{a}$ is in the image of the third map proving exactness at $\mathrm{Cl}(\mathcal{O})$. Lastly, to show exactness $\mathrm{Cl}(\mathcal{O}(X))$ recall that every ideal class can be represented by an integral ideal and that the primes $\mathfrak{p}_X$ of $\mathcal{O}(X)$ are of the form $\mathfrak{p}_X = \mathfrak{p}(X)$ for $\mathfrak{p} \in X$. Then the fifth map is surjective since the primes of $\mathcal{O}$ and $\mathcal{O}(X)$ generate their corresponding ideal class groups by the prime factorization of fractional ideals. Therefore exactness holds at $\mathrm{Cl}(\mathcal{O}(X))$ which completes exactness of the sequence. The last statement follows from the first isomorphism theorem since the valuation $v_\mathfrak{p}$ restricted to K^* is a surjective homomorphism and the kernel is precisely the set of units of $\mathcal{O}_\mathfrak{p}$. This completes the proof. □

We now turn to the setting of a number field K. We let S denote a finite set of primes of $\mathcal{O}_K$ and let X denote the set of all primes that do not belong to S. The *ring of S-integers* $\mathcal{O}_K^S$ of K is defined by

$$\mathcal{O}_K^S = \mathcal{O}_K(X).$$

We call any $\alpha \in \mathcal{O}_K^S$ an *algebraic S-integer*. The *S-class group* $\mathrm{Cl}^S(K)$ of K is the ideal class group of $\mathcal{O}_K^S$. The *S-class number* h_K^S of K is the class number of $\mathrm{Cl}^S(K)$. The *S-unit group* of K is the unit group $(\mathcal{O}_K^S)^*$ of $\mathcal{O}_K^S$ and we call any element of $(\mathcal{O}_K^S)^*$ an *S-unit* of K.

5 Dedekind Extensions

Having discussed the prime factorization of fractional ideals in Dedekind domains, we now turn to discussing how primes factor when considered in a larger Dedekind domain. Let $\mathcal{o}$ be a Dedekind domain with field of fractions K, L/K be a finite separable extension, and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. We first show that $\mathcal{O}$ is also a Dedekind domain:

Proposition 5.1. *Let $\mathcal{o}$ be a Dedekind domain with field of fractions K, L/K be a finite separable extension, and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. Then $\mathcal{O}$ is a Dedekind domain.*

Proof. $\mathcal{O}$ is an integral domain because it is a subring of L and is integrally closed since it is the integral closure of $\mathcal{o}$. We now show $\mathcal{O}$ is noetherian. Let the degree of L/K be n and let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K. By Proposition 1.4 we may multiply by a nonzero element of $\mathcal{o}$, if necessary, to ensure that this basis is contained in $\mathcal{O}$. Then $d_{L/K}(\lambda_1, \ldots, \lambda_n)$ is nonzero by Proposition 2.6 and Lemma 2.8 implies that

$$d_{L/K}(\lambda_1, \ldots, \lambda_n)\mathcal{O} \subseteq \mathcal{o}\lambda_1 + \cdots + \mathcal{o}\lambda_n.$$

Thus $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module of rank at most n. In particular, every ideal of $\mathcal{O}$ is also a finitely generated $\mathcal{o}$-module and therefore also a finitely generated $\mathcal{O}$-module. It remains to show that every nonzero prime ideal is maximal. Letting $\mathfrak{P}$ be a nonzero prime ideal, it suffices to show $\mathcal{O}/\mathfrak{P}$ is a field. To this end, consider the homomorphism

$$\phi : \mathcal{o} \to \mathcal{O}/\mathfrak{P} \qquad \alpha \mapsto \alpha + \mathfrak{p}.$$

Then $\ker \phi = \mathfrak{P} \cap \mathcal{o}$ and we claim $\mathfrak{P} \cap \mathcal{o}$ is a nonzero prime ideal of $\mathcal{o}$. It is clearly an ideal of $\mathcal{o}$ and is prime because $\mathfrak{P}$ is. To see that it is nonzero, let $\alpha \in \mathfrak{P}$ be nonzero. As α is algebraic over $\mathcal{o}$, we have

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

for some $n \geq 1$ and $a_i \in \mathcal{o}$ for $0 \leq i \leq n-1$. Taking n minimal, we have $a_0 \neq 0$. Isolating a_0 shows that $a_0 \in \mathfrak{P}$ and hence $a_0 \in \mathfrak{P} \cap \mathcal{o}$. Therefore $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$ for some prime $\mathfrak{p}$. Hence $\ker \phi = \mathfrak{p}$ and by the first isomorphism theorem, ϕ induces an injection $\phi : \mathbb{F}_\mathfrak{p} \to \mathcal{O}/\mathfrak{P}$. As $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in L, it is obtained from $\mathcal{o}$ by forming a polynomial ring with algebraic elements in L. The latter injection then shows that $\mathcal{O}/\mathfrak{P}$ is obtained from $\mathbb{F}_\mathfrak{p}$ by adjoining these algebraic elements reduced modulo $\mathfrak{P}$. Their reductions are seen to be algebraic over $\mathbb{F}_\mathfrak{p}$ by reducing their minimal polynomials over K, viewed as elements of $\mathcal{O}[x]$, modulo $\mathfrak{P}$ upon recalling that the coefficients of which are in $\mathcal{o}$ by Proposition 1.4. Hence $\mathcal{O}/\mathfrak{P}$ is obtained from $\mathbb{F}_\mathfrak{p}$ by adjoining algebraic elements to $\mathbb{F}_\mathfrak{p}$ (since $\mathbb{F}_\mathfrak{p}[\overline{\alpha}] = \mathbb{F}_\mathfrak{p}(\overline{\alpha})$ if $\overline{\alpha}$ is algebraic over $\mathbb{F}_\mathfrak{p}$) and is therefore a field. $\square$

Under the assumptions of Proposition 5.1, it follows from Proposition 1.4 that L is the field of fractions of $\mathcal{O}$. We say that a ring extension $\mathcal{O}/\mathcal{o}$ is a *Dedekind extension* of a finite separable extension L/K if $\mathcal{O}$ and $\mathcal{o}$ are Dedekind domains whose field of fractions are L and K respectively and $\mathcal{O}$ is the integral closure of $\mathcal{o}$ in L. This immediately implies

$$\mathcal{O} \cap K = \mathcal{o}.$$

Moreover, if $\mathcal{O}$ is also a free $\mathcal{o}$-module then $\mathcal{O}/\mathcal{o}$ admits an integral basis. In light of Proposition 4.7, $\mathcal{O}D^{-1}/\mathcal{o}D^{-1}$ is also a Dedekind extension of L/K for any multiplicative subset $D \subseteq \mathcal{o} - \{0\}$. We call $\mathcal{O}D^{-1}/\mathcal{o}D^{-1}$ the *localization* of $\mathcal{O}/\mathcal{o}$ at D. In the case $D = \mathcal{o} - \mathfrak{p}$ for a prime $\mathfrak{p}$ of $\mathcal{o}$, we call $\mathcal{O}_{\mathfrak{p}}/\mathcal{o}_{\mathfrak{p}}$ the *localization* of $\mathcal{O}/\mathcal{o}$ at $\mathfrak{p}$. We say that a Dedekind extension $\mathcal{O}/\mathcal{o}$ is *local* if $\mathcal{o}$ is a discrete valuation ring. As $\mathcal{o}$ is a principal ideal domain, Theorem 2.9 implies that $\mathcal{O}/\mathcal{o}$ admits an integral basis if it is local. In addition, as $\mathcal{o}$ has a unique prime we see that $\mathcal{O}$ has finitely many primes since they all must be above the prime of $\mathcal{o}$. By Proposition 3.12 this forces $\mathcal{O}$ to be a principal ideal domain as well. In particular, localizing the Dedekind extension $\mathcal{O}/\mathcal{o}$ at $\mathfrak{p}$ produces the local Dedekind extension $\mathcal{O}_{\mathfrak{p}}/\mathcal{o}_{\mathfrak{p}}$. With this phrasing, the proof of Proposition 5.1 gives the following corollary:

Corollary 5.2. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K. Then $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module of rank at most n and every prime $\mathfrak{P}$ of $\mathcal{O}$ satisfies*

$$\mathfrak{P} \cap \mathcal{o} = \mathfrak{p},$$

for some prime $\mathfrak{p}$ of $\mathcal{o}$. Moreover, $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is a finite extension of degree at most n.

Proof. The first statement was deduced in the proof of Proposition 5.1 along with the fact that there is an injection $\mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{P}}$. From this injection it follows that $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is an extension and since $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module of rank at most n, $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ has degree at most n. □

Continue to let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K. Note that if $\mathfrak{f}$ is a fractional ideal of $\mathcal{o}$ then $\mathfrak{f}\mathcal{O}$ is a fractional ideal of $\mathcal{O}$ because $\mathfrak{f}$ is a finitely generated $\mathcal{o}$-module and hence a finitely generated $\mathcal{O}$-module. In particular, $\mathfrak{a}\mathcal{O}$ is an integral ideal of $\mathcal{O}$ for any integral ideal $\mathfrak{a}$ of $\mathcal{o}$. Now let $\mathfrak{P}$ and $\mathfrak{p}$ be primes of $\mathcal{O}$ and $\mathcal{o}$ respectively. We say that $\mathfrak{P}$ is *above* $\mathfrak{p}$, or equivalently, $\mathfrak{p}$ is *below* $\mathfrak{P}$ if

$$\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}.$$

Then Corollary 5.2 implies that every prime of $\mathcal{O}$ is above exactly one prime of $\mathcal{o}$. If $\mathfrak{P}$ is above $\mathfrak{p}$ then $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}$. Indeed, since $\mathfrak{p} \subseteq \mathfrak{P}$ we have $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$ which is to say that $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}$. This implies that only finitely many primes $\mathfrak{P}$ can lie above a prime $\mathfrak{p}$ and they are exactly the prime factors of $\mathfrak{p}\mathcal{O}$. Moreover, every prime of $\mathcal{o}$ is below at least one prime of $\mathcal{O}$. To see this, it suffices to show that the integral ideal $\mathfrak{p}\mathcal{O}$ satisfies

$$\mathfrak{p}\mathcal{O} \neq \mathcal{O}.$$

By the prime factorization of fractional ideals, choosing $\alpha \in \mathfrak{p} - \mathfrak{p}^2$ we can write $\alpha\mathcal{o} = \mathfrak{p}\mathfrak{a}$ for some integral ideal $\mathfrak{a}$ relatively prime to $\mathfrak{p}$. Then $\mathfrak{a} + \mathfrak{p} = \mathcal{o}$ and so there exist $\beta \in \mathfrak{a}$ and $\gamma \in \mathfrak{p}$ such that $\beta + \gamma = 1$. Then $\beta\mathfrak{p} \subseteq \alpha\mathcal{o}$ and $\beta \notin \mathfrak{p}$ because otherwise $1 \in \mathfrak{p}$ which is absurd since $\mathfrak{p}$ is proper. Now if $\mathfrak{p}\mathcal{O} = \mathcal{O}$, it would follow that $\beta\mathcal{O} \subseteq \alpha\mathcal{O}$ which would imply $\beta = \alpha\delta$ for some $\delta \in \mathcal{O}$. Hence $\delta = \frac{\beta}{\alpha} \in K$ because K is the field of fractions of $\mathcal{o}$. As $\mathcal{O} \cap K = \mathcal{o}$, we also find that $\delta \in \mathcal{o}$. But since $\alpha \in \mathfrak{p}$, it follows that $\beta \in \mathfrak{p}$ which is a contraction. Therefore $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$. In addition, we have

$$\mathfrak{p}\mathcal{O} \cap \mathcal{o} = \mathfrak{p}.$$

The reverse inclusion is obvious. For the forward inclusion, as $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$ there exists a prime factor $\mathfrak{P}$ of $\mathfrak{p}\mathcal{O}$ so that $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$. But then $\mathfrak{P}$ is above $\mathfrak{p}$ so that $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$ and the forward inclusion follows since $\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P}$. We illustrate the relationship between $\mathfrak{P}$ and $\mathfrak{p}$ via the following extension:

$$\begin{array}{c} \mathfrak{P} \subset \mathcal{O} \subseteq L \\ \Big| \\ \mathfrak{p} \subset \mathcal{o} \subseteq K. \end{array}$$

We have the residue class fields $\mathbb{F}_{\mathfrak{P}}$ and $\mathbb{F}_{\mathfrak{p}}$. The former is a finite extension of the latter of degree at most n by Corollary 5.2. Accordingly, we call $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ the *residue class extension* of $\mathcal{O}/\mathcal{o}$ for $\mathfrak{P}$. Actually since Corollary 5.2 implies $\mathcal{O}$ is at finitely generated $\mathcal{o}$-module of rank at most n, the quotient ring $\mathfrak{B}/\mathfrak{A}$ is a $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension at most n for any integral ideals $\mathfrak{A}$ and $\mathfrak{B}$ with $\mathfrak{p} \subseteq \mathfrak{A} \subseteq \mathfrak{B}$. In any case, we define the *inertia degree* $f_{\mathfrak{p}}(\mathfrak{P})$ of $\mathfrak{P}$ relative to $\mathfrak{p}$ by

$$f_{\mathfrak{p}}(\mathfrak{P}) = [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}].$$

That is, $f_{\mathfrak{p}}(\mathfrak{P})$ is the dimension of the residue field $\mathbb{F}_{\mathfrak{P}}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space. The *ramification index* $e_{\mathfrak{p}}(\mathfrak{P})$ is the power of $\mathfrak{P}$ appearing in the prime factorization of $\mathfrak{p}\mathcal{O}$. If $\mathfrak{p}\mathcal{O}$ has prime factors $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ then the prime factorization of $\mathfrak{p}\mathcal{O}$ is

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_{\mathfrak{p}}(\mathfrak{P}_1)} \cdots \mathfrak{P}_r^{e_{\mathfrak{p}}(\mathfrak{P}_r)}.$$

All of this is preserved under localization as the following proposition shows:

Proposition 5.3. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite separable extension L/K and let $D \subseteq \mathcal{o} - \{0\}$ be a multiplicative subset. Then for the Dedekind extension $\mathcal{O}D^{-1}/\mathcal{o}D^{-1}$, $\mathfrak{P}D^{-1}$ is above $\mathfrak{p}D^{-1}$ if and only if $\mathfrak{P}$ is above $\mathfrak{p}$. Moreover, there are isomorphisms*

$$\mathbb{F}_{\mathfrak{P}D^{-1}} \cong \mathbb{F}_{\mathfrak{P}} \quad \textit{and} \quad \mathbb{F}_{\mathfrak{p}D^{-1}} \cong \mathbb{F}_{\mathfrak{p}}.$$

Lastly, we have equalities

$$f_{\mathfrak{p}D^{-1}}(\mathfrak{P}D^{-1}) = f_{\mathfrak{p}}(\mathfrak{P}) \quad \textit{and} \quad e_{\mathfrak{p}D^{-1}}(\mathfrak{P}D^{-1}) = e_{\mathfrak{p}}(\mathfrak{P}).$$

Proof. Note that $\mathfrak{P}$ and $\mathfrak{p}$ are necessarily primes disjoint from D. On the one hand, suppose $\mathfrak{P}$ is above $\mathfrak{p}$. Then $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$ and applying the first bijection in Proposition 4.1 gives

$$\mathfrak{P}D^{-1} \cap \mathcal{o}D^{-1} = \mathfrak{p}D^{-1}.$$

Hence $\mathfrak{P}D^{-1}$ is above $\mathfrak{p}D^{-1}$. On the other hand, suppose $\mathfrak{P}D^{-1}$ is above $\mathfrak{p}D^{-1}$. Then $\mathfrak{P}D^{-1} \cap \mathcal{o}D^{-1} = \mathfrak{p}D^{-1}$ and applying the second bijection in Proposition 4.1 gives

$$\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}.$$

(recall $\mathcal{o} \subseteq \mathcal{O}$) so that $\mathfrak{P}$ is above $\mathfrak{p}$. This proves the first statement. For the second statement, consider the homomorphisms

$$\Phi : \mathbb{F}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}D^{-1}} \qquad \alpha + \mathfrak{P} \mapsto \alpha + \mathfrak{P}D^{-1},$$

and

$$\phi : \mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\mathfrak{p}D^{-1}} \qquad \alpha + \mathfrak{p} \mapsto \alpha + \mathfrak{p}D^{-1}.$$

Let $\frac{\alpha}{\delta}$ be a representative of a coset in $\mathbb{F}_{\mathfrak{P}D^{-1}}$ or $\mathbb{F}_{\mathfrak{p}D^{-1}}$ so that $\alpha \in \mathfrak{P}$ or $\alpha \in \mathfrak{p}$ respectively and $\delta \in D$. By Proposition 4.1, D is disjoint from $\mathfrak{P}$ and $\mathfrak{p}$ and thus elements of D are invertible in $\mathbb{F}_{\mathfrak{P}}$ and $\mathbb{F}_{\mathfrak{p}}$. Then $\frac{\alpha}{\delta}$ represents a coset in $\mathfrak{P}$ or $\mathfrak{p}$ proving surjectivity. For injectivity, suppose α is a representative of a coset in $\mathbb{F}_{\mathfrak{P}}$ or $\mathbb{F}_{\mathfrak{p}}$ that belongs to $\ker \Phi$ or $\ker \phi$ respectively. Then $\alpha \in \mathcal{O} \cap \mathfrak{P}D^{-1}$ or $\alpha \in \mathcal{o} \cap \mathfrak{p}D^{-1}$ which is to say that $\alpha \in \mathfrak{P}$ or $\alpha \in \mathfrak{p}$ by Proposition 4.1. This means α represents the zero class in $\mathbb{F}_{\mathfrak{P}}$ or $\mathbb{F}_{\mathfrak{p}}$ respectively and injectivity follows. Therefore Φ and ϕ are isomorphisms proving the second statement. In fact, these two isomorphisms together give

$$f_{\mathfrak{p}D^{-1}}(\mathfrak{P}D^{-1}) = f_{\mathfrak{p}}(\mathfrak{P}),$$

by the definition of the inertia degrees. Finally, we have

$$e_{\mathfrak{p}D^{-1}}(\mathfrak{P}D^{-1}) = e_{\mathfrak{p}}(\mathfrak{P}),$$

because the first statement implies that the prime factors of $\mathfrak{p}D^{-1}\mathcal{O}$ correspond to those of $\mathfrak{p}\mathcal{O}$ and hence their powers must be the same. □

Let us now introduce towers of Dedekind extensions. We say that $\mathcal{O}'/\mathcal{O}/\mathcal{o}$ is a *tower* of Dedekind extensions for a finite separable tower of extensions $M/L/K$ if $\mathcal{O}'/\mathcal{O}$ and $\mathcal{O}/\mathcal{o}$ are Dedekind extensions for M/L and L/K respectively. Now let $\mathfrak{P}'$, $\mathfrak{P}$, and $\mathfrak{p}$ be primes of $\mathcal{O}'$, $\mathcal{O}$, and $\mathcal{o}$ respectively with $\mathfrak{P}'$ above $\mathfrak{P}$ and $\mathfrak{P}$ above $\mathfrak{p}$. Then we have the residue class field extensions $\mathbb{F}_{\mathfrak{P}'}/\mathbb{F}_{\mathfrak{P}}$ and $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$. Moreover, $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})} \,||\, \mathfrak{p}\mathcal{O}$ and $\mathfrak{P}^{e_{\mathfrak{P}}(\mathfrak{P}')} \,||\, \mathfrak{P}\mathcal{O}'$. Then

$$e_{\mathfrak{p}}(\mathfrak{P}') = e_{\mathfrak{p}}(\mathfrak{P})e_{\mathfrak{P}}(\mathfrak{P}') \quad \text{and} \quad f_{\mathfrak{p}}(\mathfrak{P}') = f_{\mathfrak{p}}(\mathfrak{P})f_{\mathfrak{P}}(\mathfrak{P}'). \tag{8}$$

In other words, the ramification indices and inertia degrees are multiplicative with respect to towers of field extensions. We illustrate this relationship via the following tower of extensions:

$$\begin{array}{c} \mathfrak{P}' \subset \mathcal{O}' \subseteq M \\ \Big| \\ \mathfrak{P} \subset \mathcal{O} \subseteq L \\ \Big| \\ \mathfrak{p} \subset \mathcal{o} \subseteq K. \end{array}$$

The inertia degrees and ramification indices satisfy a simple relationship to the degree of L/K. First, we will prove a useful lemma:

Lemma 5.4. *Let $\mathcal{O}/\wp$ be a Dedekind extension of a degree n separable extension L/K. Suppose $\mathfrak{P}$ is a prime above $\mathfrak{p}$. Then for any $e \geq 1$, we have*

$$\mathcal{O}/\mathfrak{P}^e \cong \bigoplus_{0 \leq i \leq e-1} \mathbb{F}_{\mathfrak{P}}.$$

In particular, the dimension of $\mathcal{O}/\mathfrak{P}^e$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space is $ef_{\mathfrak{p}}(\mathfrak{P})$.

Proof. Consider the descending chain

$$\mathcal{O}/\mathfrak{P}^e \supseteq \mathfrak{P}/\mathfrak{P}^e \supseteq \cdots \supseteq \mathfrak{P}^{e-1}/\mathfrak{P}^e \supseteq \mathfrak{P}^e/\mathfrak{P}^e,$$

of $\mathbb{F}_{\mathfrak{p}}$-vector spaces. By the third isomorphism theorem, these quotients are of the form $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ for $0 \leq i \leq e-1$ and are all isomorphic to $\mathbb{F}_{\mathfrak{P}}$ by Lemma 3.9. Therefore we have a decomposition

$$\mathfrak{P}^i/\mathfrak{P}^e \cong \mathbb{F}_{\mathfrak{P}} \oplus (\mathfrak{P}^{i+1}/\mathfrak{P}^e),$$

for all i. Iteratively applying this isomorphism $e-1$ times gives

$$\mathcal{O}/\mathfrak{P}^e \cong \bigoplus_{0 \leq i \leq e-1} \mathbb{F}_{\mathfrak{P}}.$$

This proves the first statement. Since the dimension of $\mathbb{F}_{\mathfrak{P}}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space is $f_{\mathfrak{p}}(\mathfrak{P})$ by definition, it follows that $\mathcal{O}/\mathfrak{P}^e$ is a $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension $ef_{\mathfrak{p}}(\mathfrak{P})$. This proves the second statement. $\square$

We now describe the relationship between inertia degrees and ramification indices which is known as the *fundamental equality*:

Theorem (Fundamental equality). *Let $\mathcal{O}/\wp$ be a Dedekind extension of a degree n separable extension L/K. Suppose $\mathfrak{p}$ is a prime of $\wp$ and $\mathfrak{p}\mathcal{O}$ has prime factorization*

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_{\mathfrak{p}}(\mathfrak{P}_1)} \cdots \mathfrak{P}_r^{e_{\mathfrak{p}}(\mathfrak{P}_r)}.$$

Then

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

Proof. Since distinct primes are relatively prime, the Chinese remainder theorem implies that

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{1 \leq i \leq r} \mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}.$$

As $\mathcal{O}/\mathfrak{p}\mathcal{O}$ and $\mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}$ are $\mathbb{F}_{\mathfrak{p}}$-vector spaces for all i, it suffices to show $\mathbb{F}_{\mathfrak{P}}$ is of dimension n and $\mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}$ is of dimension $e_{\mathfrak{p}}(\mathfrak{P}_i) f_{\mathfrak{p}}(\mathfrak{P}_i)$ for all i. For $\mathcal{O}/\mathfrak{p}\mathcal{O}$, we already know it is a $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension at most n (since $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module of rank at most n by Corollary 5.2 and $\mathfrak{p} \subseteq \mathfrak{p}\mathcal{O}$). Therefore we must show that the dimension is exactly n. Let $\overline{\lambda_1}, \ldots, \overline{\lambda_m}$ be a basis for $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space and let $\lambda_1, \ldots, \lambda_m$ be any lift of this basis to $\mathcal{O}$. As $m \le n$, it suffices to show $\lambda_1, \ldots, \lambda_m$ spans L/K and hence $m = n$. Let $M = \lambda_1 \mathcal{o} + \cdots + \lambda_m \mathcal{o}$ and set $N = \mathcal{O}/M$. Then $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$ since $\lambda_1, \ldots, \lambda_m$ is a lift a basis for $(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_{\mathfrak{p}}$, and hence $N = \mathfrak{p}N$. As $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module of rank at most n by Corollary 5.2, so is N. So let $\omega_1, \ldots, \omega_r$ be generators. As $N = \mathfrak{p}N$, we have

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

for some $\alpha_{i,j} \in \mathfrak{p}$ for $1 \le i, j \le r$. These r equations are equivalent to the identity

$$((\alpha_{i,j})_{i,j} - I) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \mathbf{0}.$$

Let $d = \det((\alpha_{i,j})_{i,j} - I)$. Then $d \neq 0$ because expanding the determinant shows $d \equiv (-1)^r \pmod{\mathfrak{p}}$ as $\alpha_{i,j} \in \mathfrak{p}$ for all i and j. Multiplying on the left by the adjugate $\mathrm{adj}(\alpha_{i,j})_{i,j} - I)$ of $(\alpha_{i,j})_{i,j} - I$ and recalling that a matrix times its adjugate is its determinant times the identity, we obtain

$$d \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = \mathbf{0}.$$

Hence multiplication by d annihilates N which is to say that $d\mathcal{O} \subseteq M$. Equivalently,

$$d\mathcal{O} \subseteq \lambda_1 \mathcal{o} + \cdots + \lambda_m \mathcal{o}.$$

By Proposition 1.4 and that $d \neq 0$, multiplication by K shows $L = \lambda_1 K + \cdots + \lambda_m K$ (as the reverse containment is trivial). Hence $\lambda_1, \ldots, \lambda_m$ spans L/K so that $m = n$ and $\mathcal{O}/\mathfrak{p}\mathcal{O}$ is a $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension n. For $\mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}$, the dimensionality claim follows from Lemma 5.4. So our dimension computations combine to give

$$n = \sum_{1 \le i \le r} e_{\mathfrak{p}}(\mathfrak{P}_i) f_{\mathfrak{p}}(\mathfrak{P}_i).$$

□

We also classify primes according to extremal cases of the fundamental equality. We say $\mathfrak{p}$ is *inert* in $\mathcal{O}/\mathcal{o}$ if $r = 1$ so that there is a single prime $\mathfrak{P}$ above $\mathfrak{p}$ so that $e_{\mathfrak{p}}(\mathfrak{P}) = 1$ and $f_{\mathfrak{p}}(\mathfrak{P}) = n$ by the fundamental equality. Then

$$\mathfrak{p}\mathcal{O} = \mathfrak{P},$$

which means $\mathfrak{p}\mathcal{O}$ is prime. We say $\mathfrak{p}$ is *totally split* in $\mathcal{O}/\mathcal{o}$ if $r = n$ so that there are primes $\mathfrak{P}_i$ above $\mathfrak{p}$ with $e_{\mathfrak{p}}(\mathfrak{P}_i) = f_{\mathfrak{p}}(\mathfrak{P}_i) = 1$ for $1 \le i \le n$ by the fundamental equality. Hence

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdots \mathfrak{P}_n.$$

In terms of the inertia degrees, being inert or totally split in $\mathcal{O}/\mathcal{o}$ are antithetical properties. In particular, the smaller the inertia degrees are the greater the tendency for $\mathfrak{p}\mathcal{O}$ to factor into distinct primes. Now let us introduce ramification. If $\mathfrak{P}$ is a prime of $\mathcal{O}$ above $\mathfrak{p}$, we say that $\mathfrak{P}$ is *unramified* in $\mathcal{O}/\mathcal{o}$ if $e_{\mathfrak{p}}(\mathfrak{P}) = 1$ and the residue class extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is separable. Otherwise, we say $\mathfrak{P}$ is *ramified* in $\mathcal{O}/\mathcal{o}$. Moreover, we say $\mathfrak{P}$ is *totally ramified* in $\mathcal{O}/\mathcal{o}$ if in addition to being ramified we have $f_{\mathfrak{p}}(\mathfrak{P}) = 1$. Similarly, we say that a prime $\mathfrak{p}$ of $\mathcal{o}$ is *unramified* in $\mathcal{O}/\mathcal{o}$ if every prime $\mathfrak{P}$ above it is unramified and is *ramified* in $\mathcal{O}/\mathcal{o}$ otherwise. The Dedekind extension $\mathcal{O}/\mathcal{o}$ itself is said to be *unramified* if every prime of $\mathcal{o}$ is unramified in $\mathcal{O}/\mathcal{o}$ and is said to be *ramified* otherwise.

Remark 5.5. We will see that it is an exceptional phenomena for a prime $\mathfrak{p}$ of $\mathcal{o}$ to ramify in $\mathcal{O}/\mathcal{o}$. Therefore it is typical that $\mathfrak{p}$ is either inert or totally split in $\mathcal{O}/\mathcal{o}$.

Unfortunately, there is no general way to see how $\mathfrak{p}\mathcal{O}$ factors for an arbitrary Dedekind extension $\mathcal{O}/\mathcal{o}$ of a finite separable extension L/K. However, we can make some progress in this respect. Let θ be a primitive element for L/K so that $L = K(\theta)$. By Proposition 1.4 we can multiply by a nonzero element of $\mathcal{o}$, if necessary, to ensure that $\theta \in \mathcal{O}$ and hence its minimal polynomial $m_\theta(x)$ over K has coefficients in $\mathcal{o}$. We then define the *conductor* $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$ of $\mathcal{O}/\mathcal{o}$ relative to θ by

$$\mathfrak{Q}_{\mathcal{O}/\mathcal{o}} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} \subseteq \mathcal{o}[\theta]\}.$$

This is an integral ideal of $\mathcal{O}$ provided it is nonzero. Since $\mathcal{O}$ is a finitely generated $\mathcal{o}$ module by Corollary 5.2, let $\omega_1, \ldots, \omega_r$ be generators. As L/K is algebraic, θ is algebraic over K and hence $L = K[\theta]$. Then

$$\omega_i = \sum_{1 \le j \le r} \kappa_{i,j}\theta^j,$$

with $\kappa_{i,j} \in K$ for $1 \le i,j \le r$. As K is the field of fractions of $\mathcal{o}$, $\kappa_{i,j} = \frac{\alpha_{i,j}}{\delta_{i,j}}$ with $\alpha_{i,j}, \delta_{i,j} \in \mathcal{o}$ for all i and j. Setting $\delta = \prod_{1 \le i,j \le r} \delta_{i,j}$, we have that δ is a nonzero element of $\mathcal{o}$ (hence $\mathcal{O}$ as well) with $\delta\omega_i \in \mathcal{o}[\theta]$ for all i. As $\omega_1, \ldots, \omega_r$ generate $\mathcal{O}$ as a $\mathcal{o}$-module, it follows that $\delta \in \mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$. Then $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$ is an integral ideal of $\mathcal{O}$ as claimed. The *Dedekind-Kummer theorem* describes the factorization of $\mathfrak{p}\mathcal{O}$ provided it is relatively prime to the conductor $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$:

Theorem (Dedekind-Kummer theorem). *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K, θ be a primitive element of L/K contained in $\mathcal{O}$ with minimal polynomial $m_\theta(x)$ over K, and $\mathfrak{p}$ be a prime of $\mathcal{o}$ such that $\mathfrak{p}\mathcal{O}$ is relatively prime to $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$. Suppose*

$$\overline{m_\theta}(x) = \overline{m_1}(x)^{e_1} \cdots \overline{m_r}(x)^{e_r},$$

is the prime factorization of $\overline{m_\theta}(x)$ in $\mathbb{F}_{\mathfrak{p}}[x]$. Let $m_i(x)$ be any lift of $\overline{m_i}(x)$ to $\mathcal{o}[x]$ and set

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + m_i(\theta)\mathcal{O},$$

for $1 \leq i \leq r$. Then $\mathfrak{P}_i$ is a prime of $\mathcal{O}$ for all i,

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

is the prime factorization of $\mathfrak{p}\mathcal{O}$, and $f_{\mathfrak{p}}(\mathfrak{P}_i) = \deg(\overline{m_i}(x))$ for all i.

Proof. First consider the homomorphism

$$\phi : \mathcal{o}[\theta] \to \mathcal{O}/\mathfrak{p}\mathcal{O} \qquad \alpha \mapsto \alpha + \mathfrak{p}\mathcal{O}.$$

We have $\mathfrak{p}\mathcal{O} + \mathfrak{Q}_{\mathcal{O}/\mathcal{o}} = \mathcal{O}$ because $\mathfrak{p}\mathcal{O}$ is relatively prime to $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$. As $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}} \subseteq \mathcal{o}[\theta]$, it follows that $\mathfrak{p}\mathcal{O} + \mathcal{o}[\theta] = \mathcal{O}$ which shows ϕ is surjective. Now $\ker \phi = \mathcal{o}[\theta] \cap \mathfrak{p}\mathcal{O}$ and we claim $\mathcal{o}[\theta] \cap \mathfrak{p}\mathcal{O} = \mathfrak{p}\mathcal{o}[\theta]$. The reverse inclusion is clear since $\mathfrak{p}$ is an integral ideal of $\mathcal{o}$. For the forward inclusion, intersecting both sides of $\mathfrak{p}\mathcal{O} + \mathfrak{Q}_{\mathcal{O}/\mathcal{o}} = \mathcal{O}$ with $\mathcal{o}$ gives $\mathfrak{p} \cap \mathfrak{Q}_{\mathcal{O}/\mathcal{o}} = \mathcal{o}$ because $\mathfrak{p}\mathcal{O} \cap \mathcal{o} = \mathfrak{p}$. Hence

$$\mathcal{o}[\theta] \cap \mathfrak{p}\mathcal{O} = (\mathfrak{p} \cap \mathfrak{Q}_{\mathcal{O}/\mathcal{o}})(\mathcal{o}[\theta] \cap \mathfrak{p}\mathcal{O}) = (\mathfrak{p}\mathcal{o}[\theta] \cap \mathfrak{p}\mathcal{O}) + (\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}\mathcal{o}[\theta] \cap \mathfrak{Q}_{\mathcal{O}/\mathcal{o}}\mathfrak{p}\mathcal{O}) \subseteq \mathfrak{p}\mathcal{o}[\theta],$$

where the inclusion follows by the definition of the conductor $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$. This proves the reverse inclusion so that $\ker \phi = \mathfrak{p}\mathcal{o}[\theta]$. By first isomorphism theorem, we obtain

$$\mathcal{o}[\theta]/\mathfrak{p}\mathcal{o}[\theta] \cong \mathcal{O}/\mathfrak{p}\mathcal{O}.$$

Since $m_\theta(x)$ is the minimal polynomial for θ over K, we have an isomorphism $\mathcal{o}[x]/m_\theta(x)\mathcal{o}[x] \cong \mathcal{o}[\theta]$ given by evaluation at θ. Then we have the chain of isomorphism

$$\mathcal{o}[\theta]/\mathfrak{p}\mathcal{o}[\theta] \cong (\mathcal{o}[x]/m_\theta(x)\mathcal{o}[x])/(\mathfrak{p}(\mathcal{o}[x]/m_\theta(x)\mathcal{o}[x])) \cong \mathcal{o}[x]/(\mathfrak{p}\mathcal{o}[x]+m_\theta(x)\mathcal{o}[x]) \cong \mathbb{F}_{\mathfrak{p}}[x]/\overline{m_\theta}(x)\mathbb{F}_{\mathfrak{p}}[x],$$

where the second and third isomorphisms follow by taking $\mathcal{o}[x]/(\mathfrak{p}\mathcal{o}[x] + m_\theta(x)\mathcal{o}[x])$ and reducing elements of $\mathcal{o}[x]$ modulo $m_\theta(x)\mathcal{o}[x]$ or their coefficients modulo $\mathfrak{p}$ respectively. Therefore the inverse isomorphism is given by sending any representative $\overline{f}(x)$ of a coset in $\mathbb{F}_{\mathfrak{p}}[x]/\overline{m_\theta}(x)\mathbb{F}_{\mathfrak{p}}[x]$ to a lift $f(x)$ in $\mathcal{o}[x]$ and then to $\overline{f(\theta)}$ by reducing $f(\theta)$ modulo $\mathfrak{p}\mathcal{O}$. Now set $A = \mathbb{F}_{\mathfrak{p}}[x]/\overline{m_\theta}(x)\mathbb{F}_{\mathfrak{p}}[x]$. The Chinese remainder theorem gives an isomorphism

$$A \cong \bigoplus_{1 \leq i \leq r} \mathbb{F}_{\mathfrak{p}}[x]/\overline{m_i}(x)^{e_i}\mathbb{F}_{\mathfrak{p}}[x].$$

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

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

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

$$\pi : \mathcal{O} \to \mathcal{O}/\mathfrak{p}\mathcal{O} \qquad \alpha \mapsto \alpha + \mathfrak{p}\mathcal{O}.$$

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

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_\mathfrak{p}(\mathfrak{P}_1)} \cdots \mathfrak{P}_r^{e_\mathfrak{p}(\mathfrak{P}_r)},$$

for some ramification indices $e_\mathfrak{p}(\mathfrak{P}_i)$. We will be done if we can show $e_\mathfrak{p}(\mathfrak{P}_i) = e_i$ and $f_\mathfrak{p}(\mathfrak{P}_i) = \deg(\overline{m_i}(x))$ for all i. To accomplish this, observe that we have an isomorphism

$$\mathbb{F}_{\mathfrak{P}_i} \cong (\mathcal{O}/\mathfrak{p}\mathcal{O})/(\overline{m_i(\theta)}(\mathcal{O}/\mathfrak{p}\mathcal{O})) \cong \mathbb{F}_\mathfrak{p}[x]/\overline{m_i}(x)\mathbb{F}_\mathfrak{p}[x],$$

where the first isomorphism follow by taking $\mathbb{F}_{\mathfrak{P}_i}$ and reducing $\mathcal{O}$ modulo $\mathfrak{p}$ and the second isomorphism follows from $\mathcal{O}/\mathfrak{p}\mathcal{O} \cong A$ and that the image of the maximal ideal $\overline{m_i(\theta)}(\mathcal{O}/\mathfrak{p}\mathcal{O})$ under this isomorphism is $\overline{m_i}(x)A$. Now $\mathbb{F}_\mathfrak{p}[x]/\overline{m_i}(x)\mathbb{F}_\mathfrak{p}[x]$ is a $\mathbb{F}_\mathfrak{p}$-vector space of degree $\deg(\overline{m_i}(x))$. Hence $f_p(\mathfrak{P}_i) = \deg(\overline{m_i}(x))$ for all i as desired. The ideal $\overline{m_i}(x)^{e_i}A$ under the isomorphism $A \cong \mathcal{O}/\mathfrak{p}\mathcal{O}$ is the ideal $\overline{m_i(\theta)}^{e_i}(\mathcal{O}/\mathfrak{p}\mathcal{O})$. As the image of $\mathfrak{P}_i$ under π is $\overline{m_i(\theta)}(\mathcal{O}/\mathfrak{p}\mathcal{O})$, we have that $\mathfrak{P}_i^{e_i}$ is contained in the preimage of $\overline{m_i(\theta)}^{e_i}(\mathcal{O}/\mathfrak{p}\mathcal{O})$ under π. As $\overline{m_\theta(\theta)}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = 0$, it follows that

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

Since the $\mathfrak{P}_i$ are prime, we have $e_\mathfrak{p}(\mathfrak{P}_i) \le e_i$ for all i. But the fundamental equality then gives

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

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

Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K. The Dedekind-Kummer theorem allows us to compute the prime factorization of $\mathfrak{p}\mathcal{O}$ provided this integral ideal is relatively prime to the conductor $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$. By the prime factorization of fractional ideals, $\mathfrak{Q}_{\mathcal{O}/\mathcal{o}}$ has finitely many prime factors so we only have to avoid finitely many primes of $\mathcal{O}$. In fact, if the conductor is $\mathcal{O}$ then we do not have to avoid any primes at all. This occurs when $\mathcal{O}/\mathcal{o}$ is monogenic. Indeed, Suppose $\mathcal{O} = \mathcal{o}[\alpha]$ for some $\alpha \in \mathcal{O}$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is an integral basis for $\mathcal{O}/\mathcal{o}$ and is necessarily a basis for L/K. But then α is also a primitive element for L/K which implies

$$\mathfrak{Q}_{\mathcal{O}/\mathcal{o}} = \mathcal{O}.$$

We now turn to the setting of a number field K. Every prime $\mathfrak{p}$ of K is above some prime p (recall $\mathbb{Z}$ is a principal ideal domain so we are referring to primes by their generator). Then the residue class extension of $\mathcal{O}_K/\mathbb{Z}$ for $\mathfrak{p}$ is $\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p$. Also, we write $f_p(\mathfrak{p})$ and $e_p(\mathfrak{p})$ for the inertia degree and ramification index of $\mathfrak{p}$ relative to p respectively. Moreover, all of the residue class extensions are separable since $\mathbb{F}_p$ is a perfect field. This implies $\mathfrak{p}$ is ramified in $\mathcal{O}_K/\mathbb{Z}$ if and only if $e_p(\mathfrak{p}) = 1$. If θ is a primitive element for $K/\mathbb{Q}$ contained in $\mathcal{O}_K$, then the *conductor* $\mathfrak{q}_K$ of K relative to θ is the conductor of $\mathcal{O}_K/\mathbb{Z}$ relative to θ. Even though K admits an integral basis, $\mathcal{O}_K$ is not necessarily monogenic so that $\mathfrak{q}_K$ may not be $\mathcal{O}_K$.

6 Galois Extensions

Much more can be said about the ramification of primes in a Dedekind extension $\mathcal{O}/\mathcal{o}$ when the associated extension L/K is Galois. Since L/K is assumed to be finite and separable, this amounts to further assuming L/K is normal. In this case, the elements of the Galois group $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \overline{K})$. Then by Proposition 2.1, we have

$$\mathrm{N}_{L/K}(\lambda) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\lambda) \quad \text{and} \quad \mathrm{Tr}_{L/K}(\lambda) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\lambda),$$

for all $\lambda \in L$. As $\mathcal{o} \subseteq K$, we see that $\mathrm{Gal}(L/K)$ fixes $\mathcal{o}$ pointwise and hence every fractional ideal of $\mathcal{o}$ as well. Now let $\sigma \in \mathrm{Gal}(L/K)$ and $\alpha \in \mathcal{O}$. Then

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

for some $n \geq 1$ and $a_i \in \mathcal{o}$ for $0 \leq i \leq n-1$. Applying σ gives

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_0 = 0,$$

because σ is a K-embedding. This shows $\sigma(\alpha) \in \mathcal{O}$ and therefore the Galois group $\mathrm{Gal}(L/K)$ acts on $\mathcal{O}$. In particular, each automorphism σ of $\mathrm{Gal}(L/K)$ restricts to an automorphism of $\mathcal{O}$ and therefore $\sigma(\mathfrak{P})$ is a prime of $\mathcal{O}$ if $\mathfrak{P}$. Moreover, if $\mathfrak{P}$ is above $\mathfrak{p}$ then so is $\sigma(\mathfrak{P})$. Indeed, just observe that

$$\sigma(\mathfrak{P}) \cap \mathcal{o} = \sigma(\mathfrak{P} \cap \mathcal{o}) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

Accordingly, we say that $\sigma(\mathfrak{P})$ is *conjugate* to $\mathfrak{P}$. It turns out that the Galois group acts transitively on the set of primes above a given prime:

Proposition 6.1. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite Galois extension L/K and let $\mathfrak{p}$ be a prime of $\mathcal{o}$. Then $\mathrm{Gal}(L/K)$ acts transitively on the set of primes above $\mathfrak{p}$. Moreover, if $\mathfrak{p}\mathcal{O}$ has prime factorization*

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_{\mathfrak{p}}(\mathfrak{P}_1)} \cdots \mathfrak{P}_r^{e_{\mathfrak{p}}(\mathfrak{P}_r)},$$

then

$$f_{\mathfrak{p}}(\mathfrak{P}_1) = \cdots = f_{\mathfrak{p}}(\mathfrak{P}_r) \quad \text{and} \quad e_{\mathfrak{p}}(\mathfrak{P}_1) = \cdots = e_{\mathfrak{p}}(\mathfrak{P}_r).$$

Proof. Let $\mathfrak{P}_i$ and $\mathfrak{P}_j$ for $1 \leq i < j \leq r$ be two distinct primes above $\mathfrak{p}$. Assume by contraction that $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$ for any $\sigma \in \mathrm{Gal}(L/K)$. Since distinct primes are relatively prime, the Chinese remainder theorem implies the existence of an $\alpha \in \mathcal{O}$ such that

$$\alpha \equiv 1 \pmod{\sigma(\mathfrak{P}_i)} \quad \text{and} \quad \alpha \equiv 0 \pmod{\mathfrak{P}_j},$$

for all $\sigma \in \mathrm{Gal}(L/K)$. Now recall that $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$ by Proposition 2.1 and $\mathrm{N}_{L/K}(\alpha) \in \mathcal{o}$ by Proposition 2.2. Moreover,

$$\mathfrak{P}_i \cap \mathcal{o} = \mathfrak{p} = \mathfrak{P}_j \cap \mathcal{o}.$$

On the one hand, $\alpha \notin \sigma(\mathfrak{P}_i)$ and hence $\sigma(\alpha) \notin \mathfrak{P}_i$ for all $\sigma \in \mathrm{Gal}(L/K)$ (recall $\mathrm{Gal}(L/K)$ is a group so σ has an inverse σ^{-1}). But then $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{P}_i$ for otherwise $\sigma(\alpha) \in \mathfrak{P}_i$ for some $\sigma \in \mathrm{Gal}(L/K)$ by primality of $\mathfrak{P}_i$. It must be the case that $\mathrm{N}_{L/K}(\alpha) \notin \mathfrak{p}$ because $\mathfrak{P}_i$ is above $\mathfrak{p}$. On the other hand, $\alpha \in \mathfrak{P}_j$ and so $\mathrm{N}_{L/K}(\alpha) \in \mathfrak{P}_j$ since $\sigma(\alpha) \in \mathfrak{P}_j$ when σ is the identity and $\mathfrak{P}_j$ is an integral ideal. But then $\mathrm{N}_{L/K}(\alpha) \in \mathfrak{p}$ because $\mathfrak{P}_j$ is above $\mathfrak{p}$. This gives a contradiction and therefore the action is transitive. We now show that the inertia degrees and ramification indices of $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are equal which will complete the proof. By what we have just proved, there exists a $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Since σ is an automorphism of $\mathcal{O}$, it induces an isomorphism

$$\mathbb{F}_{\mathfrak{P}_i} \cong \mathbb{F}_{\mathfrak{P}_j}.$$

Therefore the inertia degrees of $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are equal. For the ramification indices, recall that σ is an automorphism of $\mathcal{O}$ fixing $\mathcal{o}$, and hence $\mathfrak{p}$ too, pointwise. Thus $\sigma(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$ which implies that $\mathfrak{P}_i^e \mid\mid \mathfrak{p}\mathcal{O}$ if and only if $\mathfrak{P}_j^e \mid\mid \mathfrak{p}\mathcal{O}$. Therefore the ramification indices of $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are equal as well. This completes the proof $\square$

Another way to phrase Proposition 6.1 is that the primes above $\mathfrak{p}$ are all conjugate to each other and their inertia degrees and ramification indices are all equal. We call the common inertia degree f the *inertia degree* of $\mathfrak{p}$ and the common ramification index e the *ramification index* of $\mathfrak{p}$. If there are r primes above $\mathfrak{p}$, the fundamental equality takes the particularly simple form

$$n = ref.$$

Continue to let $\mathfrak{P}$ be a prime above $\mathfrak{p}$. We define the *decomposition group* $D_{\mathfrak{p}}(\mathfrak{P})$ of $\mathfrak{P}$ by

$$D_{\mathfrak{p}}(\mathfrak{P}) = \{\tau \in \mathrm{Gal}(L/K) : \tau(\mathfrak{P}) = \mathfrak{P}\}.$$

Equivalently, $D_{\mathfrak{p}}(\mathfrak{P})$ is the stabilizer subgroup of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$. The associated *decomposition field* $L^{D_{\mathfrak{p}}(\mathfrak{P})}$ of $\mathfrak{P}$ is defined to be

$$L^{D_{\mathfrak{p}}(\mathfrak{P})} = \{\lambda \in L : \tau(\lambda) = \lambda \text{ for all } \tau \in D_{\mathfrak{p}}(\mathfrak{P})\}.$$

In other words, the decomposition field of $\mathfrak{P}$ is the fixed field of L by $D_{\mathfrak{p}}(\mathfrak{P})$. In particular, the fundamental theorem of Galois theory gives

$$\mathrm{Gal}(L/L^{D_{\mathfrak{p}}(\mathfrak{P})}) = D_{\mathfrak{p}}(\mathfrak{P}).$$

We let $\mathcal{O}^D$ denote the integral closure of $\mathcal{o}$ in $L^{D_{\mathfrak{p}}(\mathfrak{P})}$ so that $\mathcal{O}/\mathcal{O}^D/\mathcal{o}$ is a tower of Dedekind extensions. Also, we will write $\mathfrak{P}^D$ for the prime of $L^{D_{\mathfrak{p}}(\mathfrak{P})}$ below $\mathfrak{P}$. Then we can illustrate this relationship via the following tower of extensions:

$$\begin{array}{c} \mathfrak{P} \subset \mathcal{O} \subseteq L \\ \Big| \\ \mathfrak{P}^D \subset \mathcal{O}^D \subseteq L^{D_{\mathfrak{p}}(\mathfrak{P})} \\ \Big| \\ \mathfrak{p} \subset \mathcal{o} \subseteq K. \end{array}$$

Any of the decomposition groups $D_{\mathfrak{p}}(\mathfrak{P})$ encode how $\mathfrak{p}\mathcal{O}$ splits into distinct prime factors in $\mathcal{O}$. Indeed, by the orbit-stabilizer theorem the number of cosets in $\mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\mathfrak{P})$ is equal to the size of the orbit of $\mathfrak{P}$ under the action of $\mathrm{Gal}(L/K)$. As the action is transitive by Proposition 6.1, $\sigma(\mathfrak{P})$ runs over the primes above $\mathfrak{p}$ as σ runs over a complete set of representatives for this coset space. It follows that the number of prime factors of $\mathfrak{p}\mathcal{O}$ is equal to the index $|\mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\mathfrak{P})|$. In particular, $\mathfrak{p}$ is inert in $\mathcal{O}/\mathcal{o}$ if and only if $D_{\mathfrak{p}}(\mathfrak{P}) = \mathrm{Gal}(L/K)$ which is equivalent to $L^{D_{\mathfrak{p}}(\mathfrak{P})} = K$. Antithetically, $\mathfrak{p}$ is totally split in $\mathcal{O}/\mathcal{o}$ if and only if $D_{\mathfrak{p}}(\mathfrak{P}) = \{\mathrm{id}\}$ which is equivalent to $L^{D_{\mathfrak{p}}(\mathfrak{P})} = L$. More generally, the fundamental equality implies $n = ef|\mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\mathfrak{P})|$ which is to say that

$$|D_{\mathfrak{p}}(\mathfrak{P})| = ef. \tag{9}$$

Then $L/L^{D_{\mathfrak{p}}(\mathfrak{P})}$ has degree ef and $L^{D_{\mathfrak{p}}(\mathfrak{P})}/K$ has degree equal to the number of distinct prime factors of $\mathfrak{p}\mathcal{O}$ which is $|\mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\mathfrak{P})|$. If $\mathfrak{p}$ inert in $\mathcal{O}/\mathcal{o}$ then $n = ef$ implying $e = 1$ and $n = f$ as we have seen. If $\mathfrak{p}$ is totally split in $\mathcal{O}/\mathcal{o}$ then $1 = ef$ so that $e = f = 1$ as we have also seen. Moreover, the decomposition group of a conjugate prime $\sigma(\mathfrak{P})$ to $\mathfrak{P}$ is the conjugate of decomposition group of $\mathfrak{P}$ by σ. In other words,

$$D_{\mathfrak{p}}(\sigma(\mathfrak{P})) = \sigma D_{\mathfrak{p}}(\mathfrak{P})\sigma^{-1}.$$

This is simply because $\tau(\mathfrak{P}) = \mathfrak{P}$ if and only if $\sigma\tau\sigma^{-1}(\sigma(\mathfrak{P})) = \sigma(\mathfrak{P})$. Also, the fundamental theorem of Galois theory implies that $D_{\mathfrak{p}}(\sigma(\mathfrak{P}))$ is normal if and only if $L^{D_{\mathfrak{p}}(\sigma(\mathfrak{P}))}/K$ is Galois in which case

$$\mathrm{Gal}(L^{D_{\mathfrak{p}}(\sigma(\mathfrak{P}))}/K) \cong \mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\sigma(\mathfrak{P})).$$

Regardless, Proposition 6.1 shows that the prime factorization of $\mathfrak{p}\mathcal{O}$ takes the form

$$\mathfrak{p}\mathcal{O} = \left(\prod_{\sigma \in \mathrm{Gal}(L/K)/D_{\mathfrak{p}}(\mathfrak{P})} \sigma(\mathfrak{P}) \right)^e.$$

The decomposition field is aptly named because it contains all of the information about the different prime factors that $\mathfrak{p}\mathcal{O}$ splits into in $\mathcal{O}$. In particular, the primes $\mathfrak{P}^D$ are inert in $\mathcal{O}/\mathcal{O}^D$ as the following proposition shows:

Proposition 6.2. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n Galois extension L/K, let $\mathfrak{p}$ be a prime of $\mathcal{o}$ with inertia degree f and ramification index e, and let $\mathfrak{P}$ be a prime of $\mathcal{O}$ above $\mathfrak{p}$. Then the following hold:*

(i) $\mathfrak{P}^D$ *is inert in* $\mathcal{O}/\mathcal{O}^D$.

(ii) $e_{\mathfrak{p}}(\mathfrak{P}^D) = f_{\mathfrak{p}}(\mathfrak{P}^D) = 1$, $e_{\mathfrak{P}^D}(\mathfrak{P}) = e$, *and* $f_{\mathfrak{P}^D}(\mathfrak{P}) = f$.

Proof. We will prove the statements separately:

(i) By the fundamental theorem of Galois theory, $\mathrm{Gal}(L/L^{D_{\mathfrak{p}}(\mathfrak{P})}) = D_{\mathfrak{p}}(\mathfrak{P})$. It follows from Proposition 6.1 that the primes of $\mathcal{O}$ above $\mathfrak{P}^D$ are of the form $\sigma(\mathfrak{P})$ for $\sigma \in D_{\mathfrak{p}}(\mathfrak{P})$. But for these σ we have $\sigma(\mathfrak{P}) = \mathfrak{P}$. Therefore $\mathfrak{P}^D$ is inert $\mathcal{O}/\mathcal{O}^D$. This proves (i).

(ii) Recall $\mathrm{Gal}(L/L^{D_{\mathfrak{p}}(\mathfrak{P})}) = D_{\mathfrak{p}}(\mathfrak{P})$ by the fundamental theorem of Galois theory. On the one hand, since $|\mathrm{Gal}(L/L^{D_{\mathfrak{p}}(\mathfrak{P})})|$ is the degree of $L/L^{D_{\mathfrak{p}}(\mathfrak{P})}$ and $\mathfrak{P}^D$ is inert in $\mathcal{O}/\mathcal{O}^D$, the fundamental equality gives $|D_{\mathfrak{p}}(\mathfrak{P})| = e_{\mathfrak{P}^D}(\mathfrak{P})f_{\mathfrak{P}^D}(\mathfrak{P})$. Then Equation (9) gives
$$ef = e_{\mathfrak{P}^D}(\mathfrak{P})f_{\mathfrak{P}^D}(\mathfrak{P}).$$
On the other hand, as $\mathcal{O}/\mathcal{O}^D/\mathcal{o}$ is a tower of Dedekind extensions, Equation (8) implies $e = e_{\mathfrak{P}^D}(\mathfrak{P})e_{\mathfrak{p}}(\mathfrak{P}^D)$ and $f = f_{\mathfrak{P}^D}(\mathfrak{P})f_{\mathfrak{p}}(\mathfrak{P}^D)$. Thus
$$ef = e_{\mathfrak{P}^D}(\mathfrak{P})e_{\mathfrak{p}}(\mathfrak{P}^D)f_{\mathfrak{P}^D}(\mathfrak{P})f_{\mathfrak{p}}(\mathfrak{P}^D).$$
These two identities together imply $e_{\mathfrak{p}}(\mathfrak{P}^D) = f_{\mathfrak{p}}(\mathfrak{P}^D) = 1$. It follows that $e_{\mathfrak{P}^D}(\mathfrak{P}) = e$ and $f_{\mathfrak{P}^D}(\mathfrak{P}) = f$. This proves (ii). ☐

We can view Proposition 6.2 (i) as a statement that $\mathfrak{p}\mathcal{O}^D$ encodes all of the information about the distinct prime factors $\mathfrak{p}\mathcal{O}$ splits into in $\mathcal{O}$. Moreover, Proposition 6.2 (ii) can be interpreted as the fact that $\mathcal{O}^D/\mathcal{o}$ contains no information about the ramification index or inertia degree of $\mathfrak{p}$ in $\mathcal{O}/\mathcal{o}$. All of that information is contained in $\mathcal{O}/\mathcal{O}^D$ and we need to do more to unpack it. Since any $\tau \in D_{\mathfrak{p}}(\mathfrak{P})$ leaves $\mathcal{O}$ and $\mathfrak{P}$ invariant, it induces an automorphism $\overline{\tau}$ of the residue class field $\mathbb{F}_{\mathfrak{P}}$ defined by
$$\overline{\tau} : \mathbb{F}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}} \qquad \alpha \mapsto \tau(\alpha) + \mathfrak{P}.$$
We then obtain a homomorphism
$$T_{\mathfrak{p}}^{\mathfrak{P}} : D_{\mathfrak{p}}(\mathfrak{P}) \to \mathrm{Aut}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \qquad \tau \mapsto \overline{\tau}.$$
The following proposition shows that the residue class extensions $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ are normal and that $T_{\mathfrak{p}}^{\mathfrak{P}}$ is surjective:

Proposition 6.3. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite Galois extension L/K, let $\mathfrak{p}$ be a prime of $\mathcal{o}$, and let $\mathfrak{P}$ be a prime of $\mathcal{O}$ above $\mathfrak{p}$. Then the residue class extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is normal. Moreover, the homomorphism $T_{\mathfrak{p}}^{\mathfrak{P}}$ is surjective.*

Proof. By Proposition 6.2 (ii), $f_{\mathfrak{p}}(\mathfrak{P}^D) = 1$ so that we have an isomorphism $\mathbb{F}_{\mathfrak{P}^D} \cong \mathbb{F}_{\mathfrak{p}}$. Under this isomorphism we may assume $L^{D_{\mathfrak{p}}(\mathfrak{P})} = K$ which is to say $D_{\mathfrak{p}}(\mathfrak{P}) = \mathrm{Gal}(L/K)$. We will now prove that $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is normal. So let $\alpha \in \mathcal{O}$ and suppose $m_\alpha(x)$ and $m_{\overline{\alpha}}(x)$ are the minimal polynomials of α and $\overline{\alpha}$ over K and $\mathbb{F}_{\mathfrak{p}}$ respectively. Consider the reduction $\overline{m_\alpha}(x)$ of $m_\alpha(x)$, viewed as an element of $\mathcal{O}[x]$, modulo $\mathfrak{P}$ upon recalling that the coefficients of which are in $\mathcal{o}$ by Proposition 1.4. As α is a representative of $\overline{\alpha}$, we find that $\overline{\alpha}$ is a root of $\overline{m_\alpha}(x)$ and thus $m_{\overline{\alpha}}(x)$ divides $\overline{m_\alpha}(x)$ in $\mathbb{F}_{\mathfrak{P}}[x]$. Since L/K is normal (as it is Galois), $m_\alpha(x)$ splits into linear factors over L. These linear factors must also belong to $\mathcal{O}[x]$ since their roots are elements of $\mathcal{O}$ which itself is integrally closed. It follows that $\overline{m_\alpha}(x)$ splits into linear factors over $\mathbb{F}_{\mathfrak{P}}$. As $m_{\overline{\alpha}}(x)$ divides $\overline{m_\alpha}(x)$ in $\mathbb{F}_{\mathfrak{P}}[x]$, the same is true for $m_{\overline{\alpha}}(x)$. Thus $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is normal. We now prove the surjectivity of $T_{\mathfrak{p}}^{\mathfrak{P}}$. Consider the maximal separable subextension of $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$. Since this extension is finite (because the residue class extension is), it is simple by the primitive element theorem. Letting $\theta \in \mathcal{O}$ be such that $\overline{\theta}$ is a primitive element, the maximal separable subextension is of the form $\mathbb{F}_{\mathfrak{p}}(\overline{\theta})/\mathbb{F}_{\mathfrak{p}}$. Now let $\overline{\tau} \in \mathrm{Aut}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. Since $\overline{\tau}$ fixes $\mathbb{F}_{\mathfrak{p}}$ pointwise, $\overline{\tau}(\overline{\theta})$ is a root of $m_{\overline{\theta}}(x)$. As $m_{\overline{\theta}}(x)$ divides $\overline{m_\theta}(x)$ in $\mathbb{F}_{\mathfrak{P}}[x]$, we find that $\overline{\tau}(\overline{\theta})$ is also a root of $\overline{m_\theta}(x)$. Therefore there is a root θ' of $m_\theta(x)$ that is also a representative of $\overline{\tau}(\overline{\theta})$. Because L/K is Galois, we can find $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(\theta) = \theta'$. Moreover, $\tau \in D_{\mathfrak{p}}(\mathfrak{P})$ since $D_{\mathfrak{p}}(\mathfrak{P}) = \mathrm{Gal}(L/K)$. Then $T_{\mathfrak{p}}^{\mathfrak{P}}(\tau) = \overline{\tau}$ because they both take $\overline{\theta}$ to the same element, hence act the same on $\mathbb{F}_{\mathfrak{p}}(\overline{\theta})/\mathbb{F}_{\mathfrak{p}}$, and $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}(\overline{\theta})$ is purely inseparable so that it has trivial automorphism group. This proves $T_{\mathfrak{p}}^{\mathfrak{P}}$ is surjective completing the proof. $\square$

Accordingly, we define the *inertia group* $I_{\mathfrak{p}}(\mathfrak{P})$ of $\mathfrak{P}$ by

$$I_{\mathfrak{p}}(\mathfrak{P}) = \ker T_{\mathfrak{p}}^{\mathfrak{P}}.$$

Then $I_{\mathfrak{p}}(\mathfrak{P})$ is a normal subgroup of $D_{\mathfrak{p}}(\mathfrak{P})$. The associated *inertia field* $L^{I_{\mathfrak{p}}(\mathfrak{P})}$ of $\mathfrak{P}$ is defined to be

$$L^{I_{\mathfrak{p}}(\mathfrak{P})} = \{\lambda \in L : \tau(\lambda) = \lambda \text{ for all } \tau \in I_{\mathfrak{p}}(\mathfrak{P})\}.$$

In other words, the inertia field of $\mathfrak{P}$ is the fixed field of L by $I_{\mathfrak{p}}(\mathfrak{P})$. In particular, the fundamental theorem of Galois theory gives

$$\mathrm{Gal}(L/L^{I_{\mathfrak{p}}(\mathfrak{P})}) = I_{\mathfrak{p}}(\mathfrak{P}).$$

Since $I_{\mathfrak{p}}(\mathfrak{P})$ is a subgroup of $D_{\mathfrak{p}}(\mathfrak{P})$, the fundamental theorem of Galois theory implies that $L^{I_{\mathfrak{p}}(\mathfrak{P})}$ is an intermediate field of $L/L^{D_{\mathfrak{p}}(\mathfrak{P})}$. We let $\mathcal{O}^I$ denote the integral closure of $\mathcal{o}$ in $L^{I_{\mathfrak{p}}(\mathfrak{P})}$ so that $\mathcal{O}/\mathcal{O}^I/\mathcal{O}^D$ is a tower of Dedekind extensions. Also, we will write $\mathfrak{P}^I$ for the prime of $L^{I_{\mathfrak{p}}(\mathfrak{P})}$ below $\mathfrak{P}$. Then we can illustrate this relationship via the following tower of extensions:

$$\begin{array}{c}\mathfrak{P} \subset \mathcal{O} \subseteq L \\ \Big| \\ \mathfrak{P}^I \subset \mathcal{O}^I \subseteq L^{I_\mathfrak{p}(\mathfrak{P})} \\ \Big| \\ \mathfrak{P}^D \subset \mathcal{O}^D \subseteq L^{D_\mathfrak{p}(\mathfrak{P})}.\end{array}$$

The inertia group $I_\mathfrak{p}(\mathfrak{P})$ is closely related to the automorphism group of the residue class extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$. To see this, first recall that $\mathrm{Gal}(L/L^{D_\mathfrak{p}(\mathfrak{P})}) = D_\mathfrak{p}(\mathfrak{P})$ by the fundamental theorem of Galois theory. Then $I_\mathfrak{p}(\mathfrak{P})$ is a normal subgroup of $\mathrm{Gal}(L/L^{D_\mathfrak{p}(\mathfrak{P})})$ and the fundamental theorem of Galois theory again implies $L^{I_\mathfrak{p}(\mathfrak{P})}/L^{D_\mathfrak{p}(\mathfrak{P})}$ is Galois with

$$\mathrm{Gal}(L^{I_\mathfrak{p}(\mathfrak{P})}/L^{D_\mathfrak{p}(\mathfrak{P})}) \cong D_\mathfrak{p}(\mathfrak{P})/I_\mathfrak{p}(\mathfrak{P}).$$

Since $T_\mathfrak{p}^\mathfrak{P}$ is surjective by Proposition 6.3, the first isomorphism theorem induces an isomorphism

$$\mathrm{Gal}(L^{I_\mathfrak{p}(\mathfrak{P})}/L^{D_\mathfrak{p}(\mathfrak{P})}) \cong \mathrm{Aut}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}).$$

Now let e and f be the ramification index and inertia degree of $\mathfrak{p}$ respectively. The inertia group $I_\mathfrak{p}(\mathfrak{P})$ encodes e and f provided the residue class extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is separable. Indeed, Proposition 6.3 implies $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is Galois. Then $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) = \mathrm{Aut}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ and it follows that $|\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})| = f$. Then Equation (9) and our two isomorphisms together give

$$|\mathrm{Gal}(L^{I_\mathfrak{p}(\mathfrak{P})}/L^{D_\mathfrak{p}(\mathfrak{P})})| = f \quad \text{and} \quad |I_\mathfrak{p}(\mathfrak{P})| = e. \tag{10}$$

Then $L^{I_\mathfrak{p}(\mathfrak{P})}/L^{D_\mathfrak{p}(\mathfrak{P})}$ has degree f and $L/L^{I_\mathfrak{p}(\mathfrak{P})}$ has degree e. The decomposition and inertia groups fit into the follow exact sequence

Proposition 6.4. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite Galois extension L/K, let $\mathfrak{p}$ be a prime of $\mathcal{o}$, and let $\mathfrak{P}$ be a prime of $\mathcal{O}$ above $\mathfrak{p}$. Then the sequence*

$$1 \longrightarrow I_\mathfrak{p}(\mathfrak{P}) \longrightarrow D_\mathfrak{p}(\mathfrak{P}) \xrightarrow{T_\mathfrak{p}^\mathfrak{P}} \mathrm{Aut}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) \longrightarrow 1,$$

is exact.

Proof. The sequence is exact at $I_\mathfrak{p}(\mathfrak{P})$ because the second map is injective. Exactness at $D_\mathfrak{p}(\mathfrak{P})$ follows by the definition of $I_\mathfrak{p}(\mathfrak{P})$. Lastly, we have exactness at $\mathrm{Aut}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ since $T_\mathfrak{p}^\mathfrak{P}$ is surjective by Proposition 6.3. □

We can say more when the residue class extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is separable as the following proposition shows:

Proposition 6.5. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite Galois extension L/K, let $\mathfrak{p}$ be a prime of $\mathcal{o}$ with inertia degree f and ramification index e, and let $\mathfrak{P}$ be a prime of $\mathcal{O}$ above $\mathfrak{p}$. Moreover, suppose the residue class extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is separable. Then the following hold:*

(i) $e_{\mathfrak{P}^I}(\mathfrak{P}) = e$ *and* $f_{\mathfrak{P}^I}(\mathfrak{P}) = 1$.

(ii) $e_{\mathfrak{P}^D}(\mathfrak{P}^I) = 1$ *and* $f_{\mathfrak{P}^D}(\mathfrak{P}^I) = f$.

Proof. First observe that $I_{\mathfrak{P}^I}(\mathfrak{P}) = I_{\mathfrak{p}}(\mathfrak{P})$. Indeed, recall that $\mathrm{Gal}(L/L^{I_{\mathfrak{p}}(\mathfrak{P})}) = I_{\mathfrak{p}}(\mathfrak{P})$. Then Proposition 6.1 implies that the primes of $\mathcal{O}$ above $\mathfrak{P}^I$ are of the form $\sigma(\mathfrak{P})$ for $\sigma \in I_{\mathfrak{p}}(\mathfrak{P})$. But for these σ we have $\sigma(\mathfrak{P}) = \mathfrak{P}$. This shows that $\mathfrak{P}^I$ is inert in $\mathcal{O}/\mathcal{O}^I$. Therefore $D_{\mathfrak{P}^I}(\mathfrak{P}) = I_{\mathfrak{p}}(\mathfrak{P})$. Since $\ker T^{\mathfrak{P}}_{\mathfrak{p}} \subseteq \ker T^{\mathfrak{P}}_{\mathfrak{P}^I}$ (because any automorphism that is the identity on $\mathbb{F}_{\mathfrak{P}}$ is also the identity on the subfield $\mathbb{F}_{\mathfrak{P}^I}$), we conclude that $I_{\mathfrak{P}^I}(\mathfrak{P}) = I_{\mathfrak{p}}(\mathfrak{P})$. We now prove the statements:

(i) Since $\mathrm{Gal}(L/L^{I_{\mathfrak{p}}(\mathfrak{P})}) = I_{\mathfrak{p}}(\mathfrak{P})$ and $\mathfrak{P}^I$ is inert in $\mathcal{O}/\mathcal{O}^I$, we have

$$e = e_{\mathfrak{P}^I}(\mathfrak{P}) f_{\mathfrak{P}^I}(\mathfrak{P}),$$

by the fundamental equality and Equation (10). As $I_{\mathfrak{P}^I}(\mathfrak{P}) = I_{\mathfrak{p}}(\mathfrak{P})$, it follows from Proposition 6.3 that $\mathrm{Aut}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{P}^I}) = \{\mathrm{id}\}$. Therefore $e_{\mathfrak{P}^I}(\mathfrak{P}) = e$ and $f_{\mathfrak{P}^I}(\mathfrak{P}) = 1$ proving (i).

(ii) Combining Equation (8) and Proposition 6.2 (ii) together gives

$$e = e_{\mathfrak{P}^D}(\mathfrak{P}^I) e_{\mathfrak{P}^I}(\mathfrak{P}) \quad \text{and} \quad f = f_{\mathfrak{P}^D}(\mathfrak{P}^I) f_{\mathfrak{P}^I}(\mathfrak{P}).$$

Then (i) implies (ii). ∎

In the case the residue class extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is separable, we fit the decomposition and inertia fields into the following tower of extensions:

$$\begin{array}{c}
\mathfrak{P} \subset \mathcal{O} \subseteq L \\
{\scriptstyle e}\Big|{\scriptstyle 1} \\
\mathfrak{P}^I \subset \mathcal{O}^I \subseteq L^{I_{\mathfrak{p}}(\mathfrak{P})} \\
{\scriptstyle 1}\Big|{\scriptstyle f} \\
\mathfrak{P}^D \subset \mathcal{O}^D \subseteq L^{D_{\mathfrak{p}}(\mathfrak{P})} \\
{\scriptstyle 1}\Big|{\scriptstyle 1} \\
\mathfrak{p} \subset \mathcal{o} \subseteq K.
\end{array}$$

The labels on left and right of the extensions represent the corresponding ramification indices and inertia degrees respectively which come from Propositions 6.2 and 6.5. Then we see that the extension $L^{D_{\mathfrak{p}}(\mathfrak{P})}/K$ contains all of the information about the distinct prime factors $\mathfrak{p}\mathcal{O}$ splits into in $\mathcal{O}$, the extension $L^{I_{\mathfrak{p}}(\mathfrak{P})}/L^{D_{\mathfrak{p}}(\mathfrak{P})}$ contains all of the information about the corresponding inertia degrees, and the extension $L/L^{I_{\mathfrak{p}}(\mathfrak{P})}$ contains all of the information about the corresponding ramification indices. In particular, $\mathfrak{p}$ is unramified in $\mathcal{O}/\mathcal{o}$ if and only if $L^{I_{\mathfrak{p}}(\mathfrak{P})} = L$ which is equivalent to $I_{\mathfrak{p}}(\mathfrak{P}) = \{\mathrm{id}\}$.

7 The Different and Discriminant

Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K. It is exceptionally rare for a prime $\mathfrak{p}$ of K to ramify. We will construct two integral ideals, one of $\mathcal{O}$ and the other of $\mathcal{o}$ which will tell us which primes ramify in L or K. These integral ideals are the different and discriminant respectively. To describe them, we will need the concept of lattices in Dedekind domains. We say that $\mathfrak{L}$ is a **$\mathcal{o}$-lattice** if it is a finitely generated $\mathcal{o}$-submodule of L. Moreover, we say that $\mathfrak{L}$ is *complete* if it spans L/K. That is, $\mathfrak{L}$ contains a basis of L/K.

Remark 7.1. A $\mathbb{Z}$-lattice is an integral lattice and a complete $\mathbb{Z}$-lattice is a complete integral lattice.

A $\mathcal{o}$-lattice $\mathfrak{L}$ need not be a fractional ideal of $\mathcal{o}$ since it does not need to be a $\mathcal{O}$-submodule of L. However, every fractional ideal $\mathfrak{F}$ of $\mathcal{O}$ is a complete $\mathcal{o}$-lattice. Indeed, by Corollary 5.2 $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module and so $\mathfrak{F}$ is a finitely generated $\mathcal{o}$-module as well. Moreover, $\mathfrak{F}$ contains a basis of L/K. For if $\lambda_1, \ldots, \lambda_n$ is a basis for L/K we may use Proposition 1.4 to multiply by a nonzero element of $\mathcal{o}$, if necessary, to ensure that this basis is contained in $\mathcal{O}$. Choosing any nonzero $\alpha \in \mathfrak{F}$, $\alpha\lambda_1, \ldots, \alpha\lambda_n$ is a basis for L/K inside $\mathfrak{F}$.

Remark 7.2. A $\mathcal{o}$-lattice $\mathcal{L}$ need not be a free $\mathcal{o}$-submodule of L. Indeed, we are only guaranteed that $\mathcal{L}$ is a finitely generated $\mathcal{o}$-submodule of L not that it is a free finitely generated $\mathcal{o}$-submodule of L.

Recall by Lemma 2.5 that there is a nondegenerate symmetric bilinear form on K given by

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

We call this bilinear form the *trace form* of L/K. The trace form makes L into a nondegenerate inner product space over K and so every basis $\lambda_1, \ldots, \lambda_n$ admits a dual basis $\lambda_1^\vee, \ldots, \lambda_n^\vee$ with respect to $\mathrm{Tr}_{L/K}$ defined by

$$\mathrm{Tr}_{L/K}(\lambda_i\lambda_j^\vee) = \delta_{i,j},$$

for $1 \leq i, j \leq n$. The trace form will allow us to introduce duals. Indeed, if $\mathfrak{F}$ is a fractional ideal $\mathcal{O}$, the *dual* $\mathfrak{F}^\vee$ of $\mathfrak{F}$ is defined by

$$\mathfrak{F}^\vee = \{\lambda \in L : \mathrm{Tr}_{L/K}(\lambda\mathfrak{F}) \subseteq \mathcal{o}\}.$$

We say that $\mathfrak{F}$ is *self-dual* if $\mathfrak{F}^\vee = \mathfrak{F}$. The following proposition shows that the dual $\mathfrak{F}^\vee$ is indeed a fractional ideal:

Proposition 7.3. *Let $\mathcal{O}/\mathscr{o}$ be a Dedekind extension of a degree n separable extension L/K and let $\mathfrak{F}$ be a fractional ideal of $\mathcal{O}$. Then $\mathfrak{F}^\vee$ is also a fractional ideal of $\mathcal{O}$ and*

$$\mathfrak{F}^\vee = \mathfrak{F}^{-1}\mathcal{O}^\vee.$$

Proof. We will first show that $\mathfrak{F}^\vee$ is a finitely generated $\mathscr{o}$-submodule of L. Let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K. Using Proposition 1.4 to multiply by a nonzero element of $\mathscr{o}$, if necessary, we can ensure that this basis is contained in $\mathcal{O}$. Now choose some nonzero $\alpha \in \mathfrak{F} \cap \mathscr{o}$ (such an element exists since every prime $\mathfrak{P}$ of $\mathcal{O}$ is above a prime $\mathfrak{p}$ of $\mathscr{o}$ and $\mathfrak{F}$ is of the form $\mathfrak{F} = \frac{1}{\delta}\mathfrak{A}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{A}$ so that $\mathfrak{A} \subseteq \mathfrak{F}$). Now suppose $\lambda \in \mathfrak{F}^\vee$ and write $\lambda = \kappa_1\lambda_1 + \cdots + \kappa_n\lambda_n$ with $\kappa_i \in K$ for $1 \le i \le n$. Then linearity of the trace implies

$$\sum_{1 \le j \le n} \alpha\kappa_j \operatorname{Tr}_{L/K}(\lambda_i\lambda_j) = \operatorname{Tr}_{L/K}(\alpha\lambda_i\lambda),$$

for $1 \le i \le n$. These n equations are equivalent to the identity

$$\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)\begin{pmatrix}\alpha\kappa_1 \\ \vdots \\ \alpha\kappa_n\end{pmatrix} = \begin{pmatrix}\operatorname{Tr}_{L/K}(\alpha\lambda_1\lambda) \\ \vdots \\ \operatorname{Tr}_{L/K}(\alpha\lambda_n\lambda)\end{pmatrix}.$$

Multiplying on the left by the adjugate $\operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n))$ of $\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ and recalling that a matrix times its adjugate is its determinant times the identity, we see that

$$d_{L/K}(\lambda_1, \ldots, \lambda_n)\begin{pmatrix}\alpha\kappa_1 \\ \vdots \\ \alpha\kappa_n\end{pmatrix} = \operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n))\begin{pmatrix}\operatorname{Tr}_{L/K}(\alpha\lambda_1\lambda) \\ \vdots \\ \operatorname{Tr}_{L/K}(\alpha\lambda_n\lambda)\end{pmatrix}.$$

Since $\lambda_1, \ldots, \lambda_n$ is a basis for L/K that is contained in $\mathcal{O}$, the matrix $\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ has entries in $\mathscr{o}$ by Proposition 2.2 and therefore $\operatorname{adj}(\operatorname{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n))$ does too. As $\alpha\lambda_i \in \mathfrak{F}$ (because $\lambda_j \in \mathcal{O}$ for all j) and $\lambda \in \mathfrak{F}^\vee$, Proposition 2.2 again implies $\operatorname{Tr}_{L/K}(\alpha\lambda_i\lambda) \in \mathscr{o}$ for all i. So the right-hand side has entires in $\mathscr{o}$ and hence the left-hand side must as well. This means $d_{L/K}(\lambda_1, \ldots, \lambda_n)\alpha\kappa_i \in A$ for all i. Since $\lambda \in \mathfrak{F}^\vee$ was arbitrary, we have

$$\alpha d_{L/K}(\lambda_1, \ldots, \lambda_n)\mathfrak{F}^\vee \subseteq \mathcal{O}.$$

As $\mathcal{O}$ is a finitely generated $\mathscr{o}$-module by Corollary 5.2, it follows that $\mathfrak{F}^\vee$ is a finitely generated $\mathscr{o}$-submodule of L. Therefore $\mathfrak{F}^\vee$ is also a finitely generated $\mathcal{O}$-submodule of L if it is preserved under multiplication by $\mathcal{O}$. Let $\alpha \in \mathcal{O}$ and $\beta \in \mathfrak{F}^\vee$. Then we must show $\alpha\beta \in \mathfrak{F}^\vee$. To see this, observe that $\operatorname{Tr}_{L/K}(\alpha\beta\mathfrak{F}) \subseteq \operatorname{Tr}_{L/K}(\beta\mathfrak{F}) \subseteq \mathscr{o}$ by Proposition 2.2 since $\alpha\mathfrak{F} \subseteq \mathfrak{F}$ and $\beta \in \mathfrak{F}^\vee$. Therefore $\alpha\beta \in \mathfrak{F}^\vee$ and hence $\mathfrak{F}^\vee$ is a fractional ideal proving the first statement. To prove the second statement we will show containment in both directions. For the forward containment, first suppose $\alpha \in \mathfrak{F}^\vee$ and $\beta \in \mathfrak{F}$. Then $\mathrm{Tr}_{L/K}(\alpha\beta\mathcal{O}) \subseteq \mathrm{Tr}_{L/K}(\alpha\mathfrak{F}) \subseteq \mathcal{o}$ by Proposition 2.2 since $\beta\mathcal{O} \subseteq \mathfrak{F}$ and $\alpha \in \mathfrak{F}^\vee$. Hence $\alpha\beta \in \mathcal{O}^\vee$ so that $\mathfrak{F}^\vee\mathfrak{F} \subseteq \mathcal{O}^\vee$ and therefore $\mathfrak{F}^\vee \subseteq \mathfrak{F}^{-1}\mathcal{O}^\vee$. This proves the forward containment. For the reverse containment, suppose $\alpha \in \mathfrak{F}^{-1}$ and $\beta \in \mathcal{O}^\vee$. Then $\mathrm{Tr}_{L/K}(\alpha\beta\mathfrak{F}) \subseteq \mathrm{Tr}_{L/K}(\beta\mathcal{O}) \subseteq \mathcal{o}$ by Proposition 2.2 since $\alpha\mathfrak{F} \subseteq \mathcal{O}$ and $\beta \in \mathcal{O}^\vee$. Thus $\alpha\beta \in \mathfrak{F}^\vee$ implying $\mathfrak{F}^{-1}\mathcal{O}^\vee \subseteq \mathfrak{F}^\vee$ and proving the reverse containment. This completes the proof. $\square$

As the dual $\mathfrak{F}^\vee$ is a fractional ideal by Proposition 7.3, it is also a complete $\mathcal{o}$-lattice. As we might hope, localization respects duals:

Proposition 7.4. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and let $D \subseteq \mathcal{o} - \{0\}$ be a multiplicative subset. Then for any fractional ideal $\mathfrak{F}$ of $\mathcal{O}$, we have*

$$(\mathfrak{F}D^{-1})^\vee = (\mathfrak{F}^\vee)D^{-1}.$$

Proof. For the forward containment, suppose $\lambda \in (\mathfrak{F}D^{-1})^\vee$. Then $\mathrm{Tr}_{L/K}(\lambda\mathfrak{F}D^{-1}) \subseteq \mathcal{o}D^{-1}$. As $D \subset K$, linearity of the trace implies $\lambda = \frac{\alpha}{\delta}$ with $\mathrm{Tr}_{L/K}(\alpha\mathfrak{F})\delta \subseteq \mathcal{o}D^{-1}$ so that $\alpha \in \mathfrak{F}^\vee$ and $\delta \in D$. Hence $\lambda \in (\mathfrak{F}^\vee)D^{-1}$ and the forward containment follows. For the reverse containment, suppose $\frac{\alpha}{\delta} \in (\mathfrak{F}^\vee)D^{-1}$. Then $\alpha \in \mathfrak{F}^\vee$ so that $\mathrm{Tr}_{L/K}(\alpha\mathfrak{F}) \subseteq \mathcal{o}$ and $\delta \in D$. As $D \subset K$, linearity of the trace implies $\mathrm{Tr}_{L/K}(\lambda\mathfrak{F}) \subseteq \mathcal{o}D^{-1}$ with $\lambda = \frac{\alpha}{\delta}$. Hence $\frac{\alpha}{\delta} \in (\mathfrak{F}D^{-1})^\vee$ and the reverse containment holds. $\square$

We will now introduce the different and the discriminant. We define the *complement* $\mathfrak{C}_{\mathcal{O}/\mathcal{o}}$ of $\mathcal{O}/\mathcal{o}$ by

$$\mathfrak{C}_{\mathcal{O}/\mathcal{o}} = \mathcal{O}^\vee.$$

This is a fractional ideal by Proposition 7.3. The *different* $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ of $\mathcal{O}/\mathcal{o}$ is defined to be the inverse of the complement $\mathfrak{C}_{\mathcal{O}/\mathcal{o}}$:

$$\mathfrak{D}_{\mathcal{O}/\mathcal{o}} = (\mathcal{O}^\vee)^{-1}.$$

As $\mathcal{O} \subseteq \mathcal{O}^\vee$ by Proposition 2.2, it follows from Proposition 3.8 that $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ is an integral ideal and

$$\mathfrak{D}_{\mathcal{O}/\mathcal{o}} = \{\lambda \in L : \lambda\mathcal{O}^\vee \subseteq \mathcal{O}\}.$$

Also, Lemma 3.11 gives the first isomorphism in the following chain:

$$\mathcal{O}/\mathfrak{D}_{\mathcal{O}/\mathcal{o}} \cong \mathfrak{D}_{\mathcal{O}/\mathcal{o}}^{-1}/\mathcal{O} \cong \mathcal{O}^\vee/\mathcal{O}. \tag{11}$$

From this chain of isomorphisms we find that

$$\mathfrak{D}_{\mathcal{O}/\mathcal{o}} \subseteq \mathcal{O} \subseteq \mathcal{O}^\vee.$$

Therefore the different $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ is a measure of how much $\mathcal{O}$ fails to be self-dual for if $\mathfrak{D}_{\mathcal{O}/\mathcal{o}} = \mathcal{O}^\vee$ then $\mathcal{O}$ must be self-dual. Moreover, by Proposition 7.3 we can express the dual fractional ideal $\mathfrak{F}^\vee$ of a fractional ideal $\mathfrak{F}$ of $\mathcal{o}$ in terms of the different as

$$\mathfrak{F}^\vee = \mathfrak{F}^{-1}\mathfrak{D}_{\mathcal{O}/\mathcal{o}}^{-1}.$$

Now for the discriminant. We define the *discriminant* $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ of $\mathcal{O}/\mathcal{o}$ to be the ideal of $\mathcal{o}$ generated by all discriminants $d_{L/K}(\alpha_1,\ldots,\alpha_n)$ as $\alpha_1,\ldots,\alpha_n$ run over all bases of L/K contained in $\mathcal{O}$. Note that $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ is necessarily an integral ideal. Recall that if $\mathcal{O}/\mathcal{o}$ admits an integral then $\mathcal{O}$ is a free $\mathcal{o}$-module of rank n. In this case, bases of L/K contained in $\mathcal{O}$ are precisely the integral bases of $\mathcal{O}/\mathcal{o}$. Then

$$\mathfrak{d}_{\mathcal{O}/\mathcal{o}} = d_{\mathcal{o}}(\mathcal{O})\mathcal{o},$$

so that the discriminant $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ is generated by the discriminant $d_{\mathcal{o}}(\mathcal{O})$. In particular, $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ is a principal integral ideal if $\mathcal{O}/\mathcal{o}$ admits an integral basis. By Theorem 2.9 this will hold if $\mathcal{o}$ is a principal ideal domain but not necessarily in general. The different and discriminant also respect localization:

Proposition 7.5. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and let $D \subseteq \mathcal{o} - \{0\}$ be a multiplicative subset. Then*

$$\mathfrak{D}_{\mathcal{O}D^{-1}/\mathcal{o}D^{-1}} = \mathfrak{D}_{\mathcal{O}/\mathcal{o}}D^{-1} \quad \textit{and} \quad \mathfrak{d}_{\mathcal{O}D^{-1}/\mathcal{o}D^{-1}} = \mathfrak{d}_{\mathcal{O}/\mathcal{o}}D^{-1}$$

Proof. For the first identity, it is equivalent to show

$$((\mathcal{O}D^{-1})^{\vee})^{-1} = (\mathcal{O}^{\vee})^{-1}D^{-1},$$

by definition of the different. Applying Propositions 4.6 and 7.4, we see that the right-had side is equal to the left-hand side as desired. For the second identity, we will show containment in both directions. For the forward inclusion, suppose $\frac{\alpha_1}{\delta_1},\ldots,\frac{\alpha_n}{\delta_n}$ is a basis of L/K contained in $\mathcal{O}D^{-1}$. Setting $\delta = \delta_1\cdots\delta_n$, we see that $\frac{\alpha_1\delta}{\delta_1},\ldots,\frac{\alpha_n\delta}{\delta_n}$ is a basis of L/K contained in $\mathcal{O}$. As $D \subset K$ and $d_{L/K}\left(\frac{\alpha_1\delta}{\delta_1},\ldots,\frac{\alpha_n\delta}{\delta_n}\right) \in \mathfrak{d}_{\mathcal{O}/\mathcal{o}}$, linearity of the trace implies $d_{L/K}\left(\frac{\alpha_1}{\delta_1},\ldots,\frac{\alpha_n}{\delta_n}\right) \in \mathfrak{d}_{\mathcal{O}/\mathcal{o}}D^{-1}$. This shows the forward containment. For the reverse containment, suppose $\alpha_1,\ldots,\alpha_n$ is a basis of L/K contained in $\mathcal{O}$ and let $\delta \in D^{-1}$. Then $\frac{\alpha_1}{\delta},\ldots,\frac{\alpha_n}{\delta}$ is a basis for L/K contained in $\mathcal{O}D^{-1}$. As $D \subseteq K$ and $d_{L/K}\left(\frac{\alpha_1}{\delta},\ldots,\frac{\alpha_n}{\delta}\right) \in \mathfrak{d}_{\mathcal{O}D^{-1}/\mathcal{o}D^{-1}}$, linearity of the trace again implies $d_{L/K}(\alpha_1\ldots,\alpha_n) \in \mathfrak{d}_{\mathcal{O}D^{-1}/\mathcal{o}D^{-1}}$ proving the reverse containment. $\square$

We want to show that a prime $\mathfrak{P}$ of $\mathcal{O}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if it divides the different $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ provided the residue class extensions are separable. We first require a lemma:

Lemma 7.6. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and let $\mathfrak{A}$ be an integral ideal of $\mathcal{O}$. Then $\mathfrak{A} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ if and only if $\mathrm{Tr}_{L/K}(\mathfrak{A}^{-1}) \subseteq \mathcal{o}$.*

Proof. $\mathfrak{A}$ divides $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ if and only if $\mathfrak{D}_{\mathcal{O}/\mathcal{o}} \subseteq \mathfrak{A}$. This equivalent to $(\mathcal{O}^{\vee})^{-1} \subseteq \mathfrak{A}$ and inverting shows the further equivalence $\mathfrak{A}^{-1} \subseteq \mathcal{O}^{\vee}$. This last containment is equivalent to $\mathrm{Tr}_{L/K}(\mathfrak{A}^{-1}) \subseteq \mathcal{o}$ which completes the proof. $\square$

With Lemma 7.6 in hand, we can now prove our claim:

Theorem 7.7. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and assume that all residue class extensions are separable. Then a prime $\mathfrak{P}$ of $\mathcal{O}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $\mathfrak{P}$ divides $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$. In particular, if $\mathfrak{P}$ is above $\mathfrak{p}$ then the following hold:*

(i) $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ *if and only if* $e_{\mathfrak{p}}(\mathfrak{P}) \equiv 0 \pmod{\mathfrak{p}}$.

(ii) $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})-1} \mid\mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ *if and only if* $e_{\mathfrak{p}}(\mathfrak{P}) \not\equiv 0 \pmod{\mathfrak{p}}$.

Proof. We first show that (i) and (ii) together imply that $\mathfrak{P}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $\mathfrak{P} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$. Since the residue class extensions are separable by assumption, $\mathfrak{P}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $e_{\mathfrak{p}}(\mathfrak{P}) \geq 2$. Therefore (i) and (ii) together show that $\mathfrak{P}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $\mathfrak{P} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ (note that $1 \not\equiv 0 \pmod{\mathfrak{p}}$ for any prime $\mathfrak{p}$). Therefore it remains to prove (i) and (ii). In view of Propositions 5.3 and 7.5, it suffices to assume $\mathcal{O}/\mathcal{o}$ is a local Dedekind extension. Therefore $\mathcal{o}$ is a discrete valuation ring, $\mathcal{O}$ is a principal ideal domain, and $\mathcal{O}/\mathcal{o}$ admits an integral basis $\alpha_1, \ldots, \alpha_n$ making $\mathcal{O}$ a free $\mathcal{o}$-module of rank n. We will first show $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})-1} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ independent of $e_{\mathfrak{p}}(\mathfrak{P})$ modulo $\mathfrak{p}$ (note that this is satisfied by both (i) and (ii)). To this end, write $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})-1}\mathfrak{A}$ for some integral ideal $\mathfrak{A}$ of $\mathcal{O}$ so that $\mathfrak{P} \mid\mid \mathfrak{A}$. By Lemma 7.6, $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})-1} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ if and only if $\mathrm{Tr}_{L/K}(\mathfrak{P}^{1-e_{\mathfrak{p}}(\mathfrak{P})}) \subseteq \mathcal{o}$. Since $\mathfrak{P}^{1-e_{\mathfrak{p}}(\mathfrak{P})} = \mathfrak{p}^{-1}\mathfrak{A}$, linearity of the trace implies that this is equivalent to $\mathrm{Tr}_{L/K}(\mathfrak{A}) \subseteq \mathfrak{p}$. By Proposition 2.11, $\mathrm{Tr}_{K/L}(\mathfrak{A}) = \mathrm{Tr}_{\mathcal{O}/\mathcal{o}}(\mathfrak{A})$ and so it is further equivalent to show

$$\mathrm{Tr}_{\mathcal{O}/\mathcal{o}}(\mathfrak{A}) \subseteq \mathfrak{p},$$

Let $\alpha \in \mathfrak{A}$ and T_α be the multiplication by α map. Then $\mathfrak{p}\mathcal{O}$ is T_α-invariant because it is an ideal of $\mathcal{O}$. This induces a multiplication by $\overline{\alpha}$ map $T_{\overline{\alpha}}$ on $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space. As the classes $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ are a basis for $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space, it follows that

$$\mathrm{Tr}_{\mathcal{O}/\mathcal{o}}(\alpha) \equiv \mathrm{Tr}_{(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_{\mathfrak{p}}}(\overline{\alpha}) \pmod{\mathfrak{p}}.$$

Therefore it is yet further equivalent to show

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_{\mathfrak{p}}}(\overline{\alpha}) \equiv 0 \pmod{\mathfrak{p}},$$

for all $\alpha \in \mathfrak{A}$. To prove this, observe that $\overline{\alpha}$ runs over to the subring $\mathfrak{A}/\mathfrak{p}\mathcal{O}$ of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as α runs over $\mathfrak{A}$. By construction, $\mathfrak{A}$ is divisible by every prime factor of $\mathfrak{p}\mathcal{O}$ and so a power, say k, of $\mathfrak{A}$ is divisible by $\mathfrak{p}\mathcal{O}$. But this means $T_{\overline{\alpha}}^k$ is the zero operator so that it is nilpotent. As nilpotent maps have trace zero, $\mathrm{Tr}_{(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_{\mathfrak{p}}}(\overline{\alpha}) = 0$. But then $\mathrm{Tr}_{\mathcal{O}/\mathcal{o}}(\alpha) \equiv 0 \pmod{p}$ and, as α was arbitrary, the claim is justified. We now prove (i) and (ii):

(i) Begin by writing $\mathfrak{p}\mathcal{O} = \mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}\mathfrak{A}$ for some integral ideal $\mathfrak{A}$ of $\mathcal{O}$ so that $\mathfrak{A}$ is relatively prime to $\mathfrak{P}$. Arguing as before, we find that $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ if and only if

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_{\mathfrak{p}}}(\overline{\alpha}) = 0,$$

for all $\alpha \in \mathfrak{A}$. Since $\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})}$ and $\mathfrak{A}$ are relatively prime, the Chinese remainder theorem implies

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong (\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})}) \oplus (\mathcal{O}/\mathfrak{A}).$$

So there exists $\beta, \gamma \in \mathcal{O}$ such that $\beta \equiv \alpha \pmod{\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})}}$ and $\gamma \equiv \alpha \pmod{\mathfrak{A}}$. Then Equation (2) implies

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{p}\mathcal{O})/\mathbb{F}_\mathfrak{p}}(\overline{\alpha}) = \mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})})/\mathbb{F}_\mathfrak{p}}(\overline{\beta}) + \mathrm{Tr}_{(\mathcal{O}/\mathfrak{A})/\mathbb{F}_\mathfrak{p}}(\overline{\gamma}).$$

As $\alpha \in \mathfrak{A}$, $\overline{\gamma} = 0$ and so $\mathrm{Tr}_{(\mathcal{O}/\mathfrak{A})/\mathbb{F}_\mathfrak{p}}(\overline{\gamma}) = 0$. Therefore it is further equivalent to show

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})})/\mathbb{F}_\mathfrak{p}}(\overline{\beta}) = 0,$$

for all $\beta \in \mathcal{O}$. We will show that this occurs if and only if $e_\mathfrak{p}(\mathfrak{P}) \equiv 0 \pmod{\mathfrak{p}}$. So let $\beta \in \mathcal{O}$. By Lemma 5.4, we have an isomorphism

$$\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})} \cong \bigoplus_{0 \le e \le e_\mathfrak{p}(\mathfrak{P})-1} \mathcal{O}/\mathfrak{P}.$$

Therefore there exists $\beta_e \in \mathcal{O}$ such that $\beta \equiv \beta_e \pmod{\mathfrak{P}}$ for all e. But then $\mathrm{Tr}_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}(\overline{\beta}_e) = \mathrm{Tr}_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}(\overline{\beta})$ for all e, and combining with Equation (2) gives

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})})/\mathbb{F}_\mathfrak{p}}(\overline{\beta}) = e_\mathfrak{p}(\mathfrak{P})\,\mathrm{Tr}_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}(\overline{\beta}),$$

which we recall is an element of $\mathbb{F}_\mathfrak{p}$. As the residue class extensions are assumed to be separable, Lemma 2.5 implies that $\mathrm{Tr}_{\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}}(\overline{\beta})$ cannot be zero for all $\beta \in \mathcal{O}$. So it must be the case that $\mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})})/\mathbb{F}_\mathfrak{p}}(\overline{\beta}) = 0$ for all $\beta \in \mathcal{O}$ if and only if $e_\mathfrak{p}(\mathfrak{P}) \equiv 0 \pmod{\mathfrak{p}}$. This proves (i).

(ii) As we have already shown $\mathfrak{P}^{e_\mathfrak{p}(\mathfrak{P})-1} \mid \mathfrak{D}_{\mathcal{O}/\mathcal{o}}$, (ii) follows from (i). □

Note that Theorem 7.7 does not tell us the degree to which $\mathfrak{P}$ divides $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ in the case $e_\mathfrak{p}(\mathfrak{P}) \equiv 0 \pmod{p}$. It only tells us that the degree is at least $e_\mathfrak{p}(\mathfrak{P})$. Also, only finitely many primes can ramify in L as a corollary of Theorem 7.7:

Corollary 7.8. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite separable extension L/K and assume that all residue class extensions are separable. Then only finitely many primes ramify in L.*

Proof. There are only finitely many prime factors of $\mathfrak{D}_{\mathcal{O}/\mathcal{o}}$ by the prime factorization of fractional ideals. Therefore only finitely many primes can ramify in L by Theorem 7.7. □

Similarly, a prime $\mathfrak{p}$ of $\mathcal{o}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if it divides the discriminant $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ provided the residue class extensions are separable:

Theorem 7.9. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and assume that all residue class extensions are separable. Then a prime $\mathfrak{p}$ of $\mathcal{o}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $\mathfrak{p}$ divides $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$.*

Proof. As the residue class extensions are assumed to be separable, $\mathfrak{p}$ ramifies in $\mathcal{O}/\mathcal{o}$ if and only if $e_{\mathfrak{p}}(\mathfrak{P}) \geq 2$ for some prime $\mathfrak{P}$ above $\mathfrak{p}$. In view of Propositions 5.3 and 7.5, it suffices to assume $\mathcal{O}/\mathcal{o}$ is a local Dedekind extension. Therefore $\mathcal{o}$ is a discrete valuation ring, $\mathcal{O}$ is a principal ideal domain, and $\mathcal{O}/\mathcal{o}$ admits an integral basis $\alpha_1, \ldots, \alpha_n$ making $\mathcal{O}$ a free $\mathcal{o}$-module of rank n. Then, as we have see, $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ is principal and

$$\mathfrak{d}_{\mathcal{O}/\mathcal{o}} = d_{\mathcal{o}}(\mathcal{O})\mathcal{o}.$$

Therefore $\mathfrak{p}$ divides $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ if and only if $d_{\mathcal{o}}(\mathcal{O}) \equiv 0 \pmod{\mathfrak{p}}$. Since $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ is a basis for $\mathcal{O}/\mathfrak{p}\mathcal{O}$ as a $\mathbb{F}_{\mathfrak{p}}$-vector space, it follows that

$$d_{\mathcal{o}}(\mathcal{O}) \equiv d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) \pmod{\mathfrak{p}}.$$

So $\mathfrak{p}$ divides $\mathfrak{d}_{\mathcal{O}/\mathcal{o}}$ if and only if $d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = 0$. Now suppose $\mathfrak{p}\mathcal{O}$ has prime factorization

$$\mathfrak{p}\mathcal{O} = \mathfrak{P}_1^{e_{\mathfrak{p}}(\mathfrak{P}_1)} \cdots \mathfrak{P}_r^{e_{\mathfrak{p}}(\mathfrak{P}_r)}.$$

As the $\mathfrak{P}_1^{e_{\mathfrak{p}}(\mathfrak{P}_1)}, \ldots, \mathfrak{P}_r^{e_{\mathfrak{p}}(\mathfrak{P}_r)}$ are pairwise relatively prime, the Chinese remainder theorem gives

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_{1 \leq i \leq r} \mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}.$$

Then Proposition 2.4 further implies

$$d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = \prod_{1 \leq i \leq r} d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}),$$

Therefore $d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{p}\mathcal{O}) = 0$ if and only if $d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{P}_i^{e_{\mathfrak{p}}(\mathfrak{P}_i)}) = 0$ for some i. We will prove that this occurs if and only if $e_{\mathfrak{p}}(\mathfrak{P}_i) \geq 2$ which will complete the proof because this is exactly when $\mathfrak{p}$ ramifies. So let $\mathfrak{P}$ be above $\mathfrak{p}$ and first suppose $e_{\mathfrak{p}}(\mathfrak{P}) \geq 2$. Then we need to show $d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}) = 0$. By uniqueness of prime factorizations of fractional ideals, there exists $\beta_1 \in \mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})-1} - \mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}$. Then $\beta_1^2 \in \mathfrak{P}^{2(e_{\mathfrak{p}}(\mathfrak{P})-1)} \subseteq \mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}$ because $e_{\mathfrak{p}}(\mathfrak{P}) \geq 2$. By construction, $\overline{\beta_1}$ in $\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}$ is nonzero and such that $\overline{\beta_1}^2 = 0$. Since $\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}$ is a $\mathbb{F}_{\mathfrak{p}}$-vector space of dimension $f_{\mathfrak{p}}(\mathfrak{P})$, there exists a basis of the form $\overline{\beta_1}, \ldots, \overline{\beta_{f_{\mathfrak{p}}(\mathfrak{P})}}$. Now

$$\mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})})/\mathbb{F}_{\mathfrak{p}}}(\overline{\beta_1 \beta_j}) = 0,$$

for $1 \leq j \leq f_{\mathfrak{p}}(\mathfrak{P})$ since $T_{\overline{\beta_1 \beta_j}}$ is nilpotent because $T^2_{\overline{\beta_1 \beta_j}}$ is the zero operator as $\overline{\beta_1}^2 = 0$. But then the first row of $\mathrm{Tr}_{(\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})})/\mathbb{F}_{\mathfrak{p}}}(\overline{\beta_1}, \ldots, \overline{\beta_{f_{\mathfrak{p}}(\mathfrak{P})}})$ is zero and hence $d_{\mathbb{F}_{\mathfrak{p}}}(\mathcal{O}/\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})}) = 0$. Now suppose $e_{\mathfrak{p}}(\mathfrak{P}) = 1$. Then it remains to show $d_{\mathbb{F}_{\mathfrak{p}}}(\mathbb{F}_{\mathfrak{P}}) \neq 0$. Since the residue class extension $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is separable by assumption, Proposition 2.6 implies $d_{\mathbb{F}_{\mathfrak{p}}}(\mathbb{F}_{\mathfrak{P}}) \neq 0$. This completes the proof. $\square$

As a corollary of Theorem 7.9 we see that only finitely many primes can ramify in K:

Corollary 7.10. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a degree n separable extension L/K and assume that all residue class extensions are separable. Then only finitely many primes ramify in K.*

Proof. There are only finitely many prime factors of $\mathfrak{d}_{\mathcal{O}/o}$ by the prime factorization of fractional ideals. Therefore only finitely many primes can ramify in K by Theorem 7.9. $\square$

Now consider the case of a number field K of degree n. The *complement* $\mathfrak{C}_K$ of K is the complement of $\mathcal{O}_K/\mathbb{Z}$, the *different* $\mathfrak{D}_K$ of K is the different of $\mathcal{O}_K/\mathbb{Z}$, and the *discriminant* $\mathfrak{d}_K$ of K is the discriminant of $\mathcal{O}_K/\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, the $\mathfrak{d}_K$ is related to the discriminant Δ_K by

$$\mathfrak{d}_K = \Delta_K \mathcal{O}_K.$$

As all of the residue class extensions are separable, it follows from Theorems 7.7 and 7.9 that a prime of K ramifies in $\mathcal{O}_K/\mathbb{Z}$ if and only if it divides $\mathfrak{D}_K$ and a prime of $\mathbb{Q}$ ramifies in $\mathcal{O}_K/\mathbb{Z}$ if and only if it divides $|\Delta_K|$. Moreover, finitely many primes of K and $\mathbb{Q}$ ramify by Corollaries 7.8 and 7.10.

8 The Ideal Norm

Let $\mathcal{O}/o$ be a Dedekind extension of a degree n extension L/K. If $\mathfrak{P}$ a prime of L is above the prime $\mathfrak{p}$ of K, we define the *norm* $\mathrm{N}_{\mathcal{O}/o}(\mathfrak{P})$ of $\mathfrak{P}$ by

$$\mathrm{N}_{\mathcal{O}/o}(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{p}}(\mathfrak{P})}.$$

Setting $\mathrm{N}_{\mathcal{O}/o}(\mathcal{O}) = o$, we extend this multiplicatively to all fractional ideals of $\mathcal{O}$. This induces a homomorphism

$$\mathrm{N}_{\mathcal{O}/o} : I_{\mathcal{O}} \to I_o \qquad \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \mapsto \mathfrak{p}_1^{e_1 f_{\mathfrak{p}_1}(\mathfrak{P}_1)} \cdots \mathfrak{p}_r^{e_r f_{\mathfrak{p}_r}(\mathfrak{P}_r)},$$

called the *ideal norm* of $\mathcal{O}/o$. It follows from the fundamental equality and multiplicatively of the ideal norm that

$$\mathrm{N}_{\mathcal{O}/o}(\mathfrak{f}\mathcal{O}) = \mathfrak{f}^n,$$

for any fractional ideal $\mathfrak{f}$ of o.

Remark 8.1. The ideal norm can be though of as an almost inverse to the mapping that sends a fractional ideal $\mathfrak{f}$ of o to the fractional ideal $\mathfrak{f}\mathcal{O}$ of $\mathcal{O}$.

In the case of a degree n number field K, the *ideal norm* N_K of K is the ideal norm of $\mathcal{O}_K/\mathbb{Z}$. As $\mathbb{Z}$ is a principal ideal domain, every fractional ideal is principal. Therefore, $\mathrm{N}_K(\mathfrak{f})$ is generated by an $r_{\mathfrak{f}} \in \mathbb{Q}^*$ for every fractional ideal $\mathfrak{f}$ of $\mathcal{O}_K$. We define the *norm* $\mathrm{N}_K(\mathfrak{f})$ of $\mathfrak{f}$ by

$$\mathrm{N}_K(\mathfrak{f}) = |r_{\mathfrak{f}}|.$$

Since the ideal norm is multiplicative, we obtain a homomorphism

$$\mathrm{N}_K : I_K \to \mathbb{Q}^* \qquad \mathfrak{f} \mapsto |r_{\mathfrak{f}}|,$$

called the *norm* of K. For an integral ideal $\mathfrak{a}$, there is a simple relationship between the norm $\mathfrak{a}$ and the quotient $\mathcal{O}_K/\mathfrak{a}$:

Proposition 8.2. *Let K be a number field of degree n. Then for any integral ideal $\mathfrak{a}$, we have*

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

Moreover, any $\alpha \in \mathcal{O}_K$ satisfies

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

Proof. Since K admits an integral basis, $\mathcal{O}_K$ is a free abelian group of rank n as is any fractional ideal. In particular, $|\mathcal{O}_K/\mathfrak{a}|$ is finite. As the Chinese remainder theorem implies

$$|\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{b}|,$$

whenever $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, it suffices to prove the claim in the case of a prime power. So let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ above p and $e \geq 1$. On the one hand, $\mathrm{N}_K(\mathfrak{p}^e) = p^{ef_p(\mathfrak{p})}$ by definition of the norm. On the other hand, Lemma 5.4 implies $\mathcal{O}_K/\mathfrak{p}^e$ is an $\mathbb{F}_p$-vector space of dimension $ef_p(\mathfrak{p})$ so that $|\mathcal{O}_K/\mathfrak{p}^e| = p^{ef_p(\mathfrak{p})}$. Together, we have

$$\mathrm{N}_K(\mathfrak{p}^e) = |\mathcal{O}_K/\mathfrak{p}^e|,$$

and the first statement follows. For the second statement, we just have to show that $|\,\mathrm{N}_K(\alpha)| = |\mathcal{O}_K/\alpha\mathcal{O}_K|$. To this end, let $\alpha_1, \ldots, \alpha_n$ be an integral basis for K. Writing

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

with $a_i \in \mathbb{Z}$, we see that $a_1\alpha_1, \ldots, a_n\alpha_n$ is a basis for $\alpha\mathcal{O}_K$. In particular, the base change matrix from $\alpha_1, \ldots, \alpha_n$ to this basis is a diagonal matrix with the a_i on the diagonal. Then on the one hand, we have $|\mathcal{O}_K/\alpha\mathcal{O}_K| = |a_1 \cdots a_n|$ by **??** again. On the other hand, the multiplication by α map in terms of the basis $a_1\alpha_1, \ldots, a_n\alpha_n$ has matrix representation

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

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

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

as desired. □

As a consequence of Proposition 8.2 and Lagrange's theorem, $\mathrm{N}_K(\mathfrak{a}) \in \mathfrak{a}$ for any integral ideal $\mathfrak{a}$ and therefore for every fractional ideal as well (recall every such fractional ideal is of the form $\frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathbb{Z}$ and integral ideal $\mathfrak{a}$). Computing the norm of the discriminant Δ_K is also an easy matter:

Proposition 8.3. *Let K be a number field of degree n. Then*

$$\mathrm{N}_K(\mathfrak{D}_K) = |\Delta_K|.$$

Proof. From Equation (11) we have an isomorphism

$$\mathcal{O}_K/\mathfrak{D}_K \cong \mathcal{O}_K^\vee/\mathcal{O}_K.$$

Therefore $\mathrm{N}_K(\mathfrak{D}_K) = |\mathcal{O}_K^\vee/\mathcal{O}_K|$ by Proposition 8.2. Now let $\alpha_1, \ldots, \alpha_n$ be an integral basis for $\mathcal{O}_K$. Then the dual basis $\alpha_1^\vee, \ldots, \alpha_n^\vee$ is a basis for $\mathcal{O}_K^\vee$ and we have

$$\alpha_i^\vee = \sum_{1\le j\le n} \mathrm{Tr}_K(\alpha_i\alpha_j)\alpha_j.$$

But then the base change matrix from $\alpha_1, \ldots, \alpha_n$ to $\alpha_1^\vee, \ldots, \alpha_n^\vee$ is $\mathrm{Tr}_K(\alpha_1, \ldots, \alpha_n)$. The claim follows by **??** and the definition of Δ_K. $\square$

We can now compute the norm of a dual ideal:

Corollary 8.4. *Let K be a number field and $\mathfrak{f}$ be a fractional ideal. Then*

$$\mathrm{N}_K(\mathfrak{f}^\vee) = \frac{\mathrm{N}_K(\mathfrak{f}^{-1})}{|\Delta_K|}.$$

Proof. This follows immediately from $\mathfrak{f}^\vee = \mathfrak{f}^{-1}\mathfrak{D}_K^{-1}$, multiplicativity of the norm, and Proposition 8.3. $\square$

Lastly, let $a_K(m)$ denote the number of integral ideals of norm m. Because the ideal norm is multiplicative so is $a_K(m)$. Moreover, we have the following result:

Proposition 8.5. *Let K be a number field of degree n. Then $a_K(m) \le \sigma_0(m)^n$.*

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

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

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

$$e_1 f_p(\mathfrak{p}_1) + \cdots + e_n f_p(\mathfrak{p}_n) = k,$$

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. $\square$

As a consequence of **??**, we have the slightly weaker estimate $a_K(n) \ll_\varepsilon n^\varepsilon$.

9 Minkowski Space

Let K be number field of degree n and let $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Then either σ is real or complex and if it is complex it has a paired $\mathbb{Q}$-embedding $\overline{\sigma} \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ given by the conjugate of σ. Accordingly, let r_1 and $2r_2$ be the number of real and complex $\mathbb{Q}$-embeddings of K into $\overline{\mathbb{Q}}$ respectively. We call the pair (r_1, r_2) the *signature* of K and it satisfies the relation

$$n = r_1 + 2r_2.$$

Setting

$$K_{\mathbb{C}} = \mathbb{C}^n,$$

we see that $K_{\mathbb{C}}$ is a $\mathbb{C}$-algebra and also a complex Hilbert space with respect to $\langle \cdot, \cdot \rangle_{K_{\mathbb{C}}}$ which we take to be the standard complex inner product. We denote the associated Lebesgue measure by $d\lambda_{K_{\mathbb{C}}}$. We define the *canonical embedding* j of K to be the $\mathbb{Q}$-embedding

$$j : K \to K_{\mathbb{C}} \qquad \kappa \mapsto (\sigma(\kappa))_{\sigma},$$

where σ runs over $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Consider the conjugation map

$$F : \mathbb{C} \to \mathbb{C} \qquad z \mapsto \overline{z}.$$

This induces an automorphism

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}} \qquad (z_{\sigma})_{\sigma} \mapsto (\overline{z_{\overline{\sigma}}})_{\sigma},$$

that is clearly an involution. The inner product $\langle \cdot, \cdot \rangle_{K_{\mathbb{C}}}$ is also F-equivariant since any $\mathbf{z}, \mathbf{w} \in K_{\mathbb{C}}$ satisfy

$$\langle F(\mathbf{z}), F(\mathbf{z}) \rangle_{K_{\mathbb{C}}} = \langle (\overline{z_{\overline{\sigma}}})_{\sigma}, (\overline{w_{\overline{\sigma}}})_{\sigma} \rangle_{K_{\mathbb{C}}} = \sum_{\sigma} \overline{z_{\overline{\sigma}} w_{\overline{\sigma}}} = \overline{\sum_{\sigma} z_{\sigma} w_{\sigma}} = F(\langle \mathbf{z}, \mathbf{w} \rangle_{K_{\mathbb{C}}}),$$

where in the third equality we have used the fact that the complex $\mathbb{Q}$-embeddings of K into $\overline{\mathbb{Q}}$ come in conjugate pairs. On $K_{\mathbb{C}}$ we also have linear maps

$$\mathrm{Tr}_{K_{\mathbb{C}}}((z_{\sigma})_{\sigma}) = \sum_{\sigma} z_{\sigma} \quad \text{and} \quad \mathrm{N}_{K_{\mathbb{C}}}((z_{\sigma})_{\sigma}) = \prod_{\sigma} z_{\sigma},$$

and clearly induce homomorphisms

$$\mathrm{Tr}_{K_{\mathbb{C}}} : K_{\mathbb{C}} \to \mathbb{C} \quad \text{and} \quad \mathrm{N}_{K_{\mathbb{C}}} : K_{\mathbb{C}}^* \to \mathbb{C}^*.$$

The composition of j with $\mathrm{Tr}_{K_{\mathbb{C}}}$ and $\mathrm{N}_{K_{\mathbb{C}}}$ are Tr_K and N_K respectively since

$$\mathrm{Tr}_{K_{\mathbb{C}}}(j(\kappa)) = \sum_{\sigma} \sigma(\kappa) = \mathrm{Tr}_K(\kappa) \quad \text{and} \quad \mathrm{N}_{K_{\mathbb{C}}}(j(\kappa)) = \prod_{\sigma} \sigma(\kappa) = \mathrm{N}_K(\kappa),$$

where the last equality in each chain follow by Proposition 2.1. We now define the *Minkowski space* $K_{\mathbb{R}}$ of K by

$$K_{\mathbb{R}} = \{(z_{\sigma})_{\sigma} \in K_{\mathbb{C}} : F((z_{\sigma})_{\sigma}) = (z_{\sigma})_{\sigma}\}.$$

In other words, $K_{\mathbb{R}}$ consists of all of the F-invariant points of $K_{\mathbb{C}}$. That is, $\mathbf{z} \in K_{\mathbb{R}}$ if and only if $F(\mathbf{z}) = \mathbf{z}$ or equivalently $z_{\overline{\sigma}} = \overline{z_{\sigma}}$ for all σ. In particular, $j(K) \subset K_{\mathbb{R}}$ because $\overline{\sigma}(\kappa) = \overline{\sigma(\kappa)}$ by definition of $\overline{\sigma}$. We denote the restriction of the inner product $\langle \cdot, \cdot \rangle_{K_{\mathbb{C}}}$ on $K_{\mathbb{C}}$ to $K_{\mathbb{R}}$ by $\langle \cdot, \cdot \rangle_{K_{\mathbb{R}}}$. Note that $K_{\mathbb{R}}$ is an $\mathbb{R}$-algebra. Moreover, the inner product $\langle \cdot, \cdot \rangle_{K_{\mathbb{R}}}$ turns $K_{\mathbb{R}}$ into a real Hilbert space. Indeed, for any $\mathbf{z}, \mathbf{w} \in K_{\mathbb{R}}$ the conjugate symmetry and F-equivariance of the inner product together give

$$\overline{\langle \mathbf{z}, \mathbf{w} \rangle} = F(\langle \mathbf{w}, \mathbf{z} \rangle) = \langle F(\mathbf{z}), F(\mathbf{w}) \rangle = \langle \mathbf{z}, \mathbf{w} \rangle,$$

so that $\langle \mathbf{z}, \mathbf{w} \rangle \in \mathbb{R}$ is real. Accordingly, we call $\langle \cdot, \cdot \rangle_{K_{\mathbb{R}}}$ the *Minkowski inner product.* We denote the restriction of the Lebesgue measure $d\lambda_{\mathbb{C}}$ to $K_{\mathbb{R}}$ by $d\lambda_{K_{\mathbb{R}}}$ which is also the Lebesgue measure associated to $\langle \cdot, \cdot \rangle_{K_{\mathbb{R}}}$. We call $d\lambda_{K_{\mathbb{R}}}$ the *Minkowski measure.* Lastly, we denote the restrictions of $\mathrm{Tr}_{K_{\mathbb{C}}}$ and $\mathrm{N}_{K_{\mathbb{C}}}$ to $K_{\mathbb{R}}$ by $\mathrm{Tr}_{K_{\mathbb{R}}}$ and $\mathrm{N}_{K_{\mathbb{R}}}$ respectively and call these maps the *Minkowski trace* and *Minkowski norm* respectively. We also have homomorphisms

$$\mathrm{Tr}_{K_{\mathbb{R}}} : K_{\mathbb{R}} \to \mathbb{R} \quad \text{and} \quad \mathrm{N}_{K_{\mathbb{R}}} : K_{\mathbb{R}}^* \to \mathbb{R}^*,$$

$\mathbf{z} \in K_{\mathbb{R}}$ if and only if $z_{\overline{\sigma}} = \overline{z_{\sigma}}$ for all σ. As $j(K) \subset K_{\mathbb{R}}$, the compositions of j with the Minkowski trace and Minkowski norm are the field trace and field norm respectively. We can now give a more explicit description of $K_{\mathbb{R}}$ and to do this we setup some notation. Let ρ run over the real $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ and let τ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. For any $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, let $N_{\sigma} = 1, 2$ according to if σ is real or complex respectively. So $N_{\rho} = 1$ and $N_{\tau} = 2$. As $K_{\mathbb{R}}$ consists of exactly the F-invariant points of $K_{\mathbb{C}}$, we have

$$K_{\mathbb{R}} = \{(z_{\sigma})_{\sigma} \in K_{\mathbb{C}} : z_{\rho} \in \mathbb{R} \text{ and } z_{\overline{\tau}} = \overline{z_{\tau}} \text{ for all } \rho \text{ and } \tau\}.$$

We now describe an explicit isomorphism from the Minkowski space and $\mathbb{R}^n$:

Proposition 9.1. *Let K be a number field of degree n and signature (r_1, r_2). Also let σ run over $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, ρ run over all such real $\mathbb{Q}$-embeddings, and τ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings. Then there is an isomorphism*

$$K_{\mathbb{R}} \to \mathbb{R}^n \qquad z_{\sigma} \mapsto x_{\sigma} = \begin{cases} z_{\sigma} & \text{if } \sigma = \rho, \\ \mathrm{Re}(z_{\sigma}) & \text{if } \sigma = \tau, \\ \mathrm{Im}(z_{\sigma}) & \text{if } \sigma = \overline{\tau}. \end{cases}$$

In particular, $K_{\mathbb{R}}$ is a n-dimensional real vector space. Moreover, the inner product $\langle \cdot, \cdot \rangle$ on $\mathbb{R}^n$ induced by the Minkowski inner product is given by

$$\langle \mathbf{x}, \mathbf{x}' \rangle = \sum_{\sigma} N_{\sigma} x_{\sigma} x'_{\sigma},$$

for any $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^n$.

Proof. This map is an isomorphism since it is invertible and linear in each component. Since there are n elements of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, we see that $K_{\mathbb{R}}$ is an n-dimensional real vector space. We will now prove the statement about the inner product. Let $(z_\sigma)_\sigma$ and $(z'_\sigma)_\sigma$ be elements of $K_{\mathbb{R}}$ and let $(x_\sigma)_\sigma$ and $(x'_\sigma)_\sigma$ be the corresponding elements in $\mathbb{R}^n$. If $\sigma = \rho$ then

$$x_\rho = z_\rho \quad \text{and} \quad x'_\rho = z'_\rho,$$

and thus

$$x_\rho x'_\rho = z_\rho \overline{z'_\rho}.$$

If $\sigma = \tau$ then

$$x_\tau = \mathrm{Re}(z_\tau), \quad x_{\overline{\tau}} = \mathrm{Im}(z_\tau), \quad x'_\tau = \mathrm{Re}(z'_\tau), \text{and} \quad x'_{\overline{\tau}} = \mathrm{Im}(z'_\tau),$$

and hence

$$2(x_\tau x'_\tau + x_{\overline{\tau}} x'_{\overline{\tau}}) = 2(\mathrm{Re}(z_\tau)\mathrm{Re}(z'_\tau) + \mathrm{Im}(z_\tau)\mathrm{Im}(z'_\tau)) = 2\mathrm{Re}(z_\tau \overline{z'_\tau}) = z_\tau \overline{z'_\tau} + z_{\overline{\tau}} \overline{z'_{\overline{\tau}}}.$$

This proves the claim about the inner product. □

Define the *Minkowski embedding* σ_K of K by

$$\sigma_K : K \to \mathbb{R}^n \qquad \kappa \mapsto (\rho_1(\kappa), \ldots, \rho_{r_1}(k), \mathrm{Re}(\tau_1(\kappa)), \mathrm{Im}(\tau_1(\kappa)), \ldots, \mathrm{Re}(\tau_{r_2}(\kappa)), \mathrm{Im}(\tau_{r_2}(\kappa))),$$

where $\rho_1, \ldots, \rho_{r_1}$ are the real $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ and $\tau_1, \ldots, \tau_{r_2}$ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. The Minkowski embedding σ_K is then a $\mathbb{Q}$-embedding of K into $\mathbb{R}^n$ since it is the composition of the canonical embedding j (whose image under K is in $K_{\mathbb{R}}$ as we have noted) and the isomorphism established by Proposition 9.1. It is also independent of the choice of representatives $\tau_1, \ldots, \tau_{r_2}$ since the complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ occur in conjugate pairs. As j is a $\mathbb{Q}$-embedding and any fractional ideal $\mathfrak{f}$ is a complete lattice, $j(\mathfrak{f})$ is a complete lattice in $K_{\mathbb{R}}$. We now determine the covolume of $j(\mathfrak{f})$:

Proposition 9.2. *Let K be a number field with signature (r_1, r_2). Then $V_{j(\mathfrak{f})}$ is the absolute value of the determinant of any embedding matrix for $\mathfrak{f}$. In particular,*

$$V_{j(\mathfrak{f})} = \mathrm{N}_K(\mathfrak{f})\sqrt{|\Delta_K|},$$

and

$$V_{j(\mathcal{O}_K)} = \sqrt{|\Delta_K|}.$$

Proof. The last statement follows from the first two by taking $\mathfrak{f} = \mathcal{O}_K$ so it suffices to prove the first two statements. Let $\kappa_1, \ldots, \kappa_n$ be a basis for $\mathfrak{f}$ and let $\sigma_1, \ldots, \sigma_n$ be the elements of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Then the associated generator matrix P for $j(\mathfrak{f})$ is given by

$$P = \begin{pmatrix} \sigma_1(\kappa_1) & \cdots & \sigma_1(\kappa_n) \\ \vdots & & \vdots \\ \sigma_n(\kappa_1) & \cdots & \sigma_n(\kappa_n) \end{pmatrix} = M(\kappa_1, \ldots, \kappa_n),$$

which is an embedding matrix for $\mathfrak{f}$. Hence

$$V_{j(\mathfrak{f})} = |\det(M(\kappa_1, \ldots, \kappa_n))|,$$

proving the first statement. We will be done if we can show

$$|\det(M(\kappa_1, \ldots, \kappa_n))| = \mathrm{N}_K(\mathfrak{f})|\det(M(\alpha_1, \ldots, \alpha_n))|,$$

for any integral basis $\alpha_1, \ldots, \alpha_n$ since $|\det(M(\alpha_1, \ldots, \alpha_n))| = \sqrt{|\Delta_K|}$ (as we have seen). As $\mathfrak{f}$ is a fractional ideal, there exists a nonzero $\delta \in \mathcal{O}_K$ and an integral ideal $\mathfrak{a}$ such that

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

Then $\delta\kappa_1, \ldots, \delta\kappa_n$ is a basis for $\mathfrak{a}$. By Proposition 8.2 and **??**, we have

$$|\det(M(\delta\kappa_1, \ldots, \delta\kappa_n))| = \mathrm{N}_K(\mathfrak{a})|\det(M(\alpha_1, \ldots, \alpha_n))|,$$

since they together show that $\mathrm{N}_K(\mathfrak{a})$ is the absolute value of the determinant of the base change matrix from $\kappa_1, \ldots, \kappa_n$ to $\delta\kappa_1, \ldots, \delta\kappa_n$. Similarly,

$$|\det(M(\delta\kappa_1, \ldots, \delta\kappa_n))| = |\mathrm{N}_K(\delta)||\det(M(\kappa_1, \ldots, \kappa_n))|,$$

since Proposition 8.2 and **??** together show that $|\mathrm{N}_K(\delta)|$ is the absolute value of the determinant of the base change matrix from $\kappa_1, \ldots, \kappa_n$ to $\delta\kappa_1, \ldots, \delta\kappa_n$. As $\mathrm{N}_K(\mathfrak{f}) = \frac{\mathrm{N}_K(\mathfrak{a})}{|\mathrm{N}_K(\delta)|}$ by multiplicativity of the norm and Proposition 8.2, these two identities for $|\det(M(\delta\kappa_1, \ldots, \delta\kappa_n))|$ together imply the claim. $\square$

Now as σ_K is also a $\mathbb{Q}$-embedding, $\sigma_K(\mathfrak{f})$ is a complete lattice in $\mathbb{R}^n$. As a corollary of Proposition 9.2, we can determine the covolume of $\sigma_K(\mathfrak{f})$:

Corollary 9.3. *Let K be a number field with signature (r_1, r_2). Then*

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

In particular,

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

Proof. The second statement follows from the first by taking $\mathfrak{f} = \mathcal{O}_K$ so it suffices to prove the first statement. Let $\kappa_1, \ldots, \kappa_n$ be a basis for $\mathfrak{f}$, $\rho_1, \ldots, \rho_{r_1}$ be the real $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, and $\tau_1, \ldots, \tau_{r_2}$ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Then the associated generator matrix P for $\sigma_K(\mathfrak{f})$ is

$$P = \begin{pmatrix} \rho_1(\kappa_1) & \cdots & \rho_{r_1}(\kappa_1) & \mathrm{Re}(\tau_1(\kappa_1)) & \mathrm{Im}(\tau_1(\kappa_1)) & \cdots & \mathrm{Re}(\tau_{r_2}(\kappa_1)) & \mathrm{Im}(\tau_{r_2}(\kappa_1)) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \rho_1(\kappa_n) & \cdots & \rho_{r_1}(\kappa_n) & \mathrm{Re}(\tau_1(\kappa_n)) & \mathrm{Im}(\tau_1(\kappa_n)) & \cdots & \mathrm{Re}(\tau_{r_2}(\kappa_n)) & \mathrm{Im}(\tau_{r_2}(\kappa_n)) \end{pmatrix}^t.$$

By Proposition 9.2 we are done if the absolute value of the determinant of this matrix is 2^{-r_2} times the determinate of an embedding matrix for $\mathfrak{f}$. To show this, 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

$$P' = \begin{pmatrix} \rho_1(\kappa_1) & \cdots & \rho_{r_1}(\kappa_1) & \tau_1(\kappa_1) & \frac{\tau_1(\kappa_1)-\overline{\tau_1}(\kappa_1)}{2i} & \cdots & \tau_{r_2}(\kappa_1) & \frac{\tau_{r_2}(\kappa_1)-\overline{\tau_{r_2}}(\kappa_1)}{2i} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \rho_1(\kappa_n) & \cdots & \rho_{r_1}(\kappa_n) & \tau_1(\kappa_n) & \frac{\tau_1(\kappa_n)-\overline{\tau_1}(\kappa_n)}{2i} & \cdots & \tau_{r_2}(\kappa_n) & \frac{\tau_{r_2}(\kappa_n)-\overline{\tau_{r_2}}(\kappa_n)}{2i} \end{pmatrix}^t.$$

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

$$P'' = \begin{pmatrix} \rho_1(\kappa_1) & \cdots & \rho_{r_1}(\kappa_1) & \tau_1(\kappa_1) & \overline{\tau_1}(\kappa_1) & \cdots & \tau_{r_2}(\kappa_1) & \overline{\tau_{r_2}}(\kappa_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \rho_1(\kappa_n) & \cdots & \rho_{r_1}(\kappa_n) & \tau_1(\kappa_n) & \overline{\tau_1}(\kappa_n) & \cdots & \tau_{r_2}(\kappa_n) & \overline{\tau_{r_2}}(\kappa_n) \end{pmatrix}^t.$$

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,

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

Since the complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ occur in conjugate pairs and $\kappa_1, \ldots, \kappa_n$ is a basis for K, we see that $P'' = M(\kappa_1, \ldots, \kappa_n)$ is an embedding matrix for $\mathfrak{f}$. $\square$

10 Finiteness of the Class Number

Recall that the class number h_K is a measure of how much the ring of integers $\mathcal{O}_K$ fails to be a principal ideal domain. From Remark 3.14, the class number of an arbitrary Dedekind domain need not be finite. However, we will show that the class number h_K for a number field K is always finite and thus $\mathcal{O}_K$ only has finite failure from being a principal ideal domain:

Theorem 10.1. *Let K be a number field of degree n and signature (r_1, r_2). Also, let $X \subseteq \mathbb{R}^n$ be a compact convex symmetric set and set $M = \max_{\mathbf{x}\in X}\left(\prod_{1\le i\le n}|x_i|\right)$. Then every ideal class contains an integral ideal $\mathfrak{a}$ satisfying*

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

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

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

for any $n \geq 1$. Then by construction,

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

By Minkowski's lattice point theorem, there exists a nonzero $\alpha \in \mathfrak{f}^{-1}$ such that $\sigma_K(\alpha) \in \sigma_K(\mathfrak{f}^{-1})$ and $\sigma_K(\alpha) \in \lambda X$. 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 σ run over $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. Since the norm is multiplicative, we have

$$\mathrm{N}_K(\alpha\mathfrak{f}) = |\,\mathrm{N}_K(\alpha)|\,\mathrm{N}_K(\mathfrak{f}) = \left|\prod_{\sigma} \sigma(\alpha)\right| \mathrm{N}_K(\mathfrak{f}) \leq \lambda^n M \,\mathrm{N}_K(\mathfrak{f}),$$

where in the first equality we have applied multiplicativity of the norm and Proposition 8.2, in the second we have used Proposition 2.1, and the inequality follows since $\sigma_K(\alpha) \in \lambda X$. This inequality, our choice of λ^n, and Corollary 9.3 together give

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

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 for $\mathrm{Cl}(K)$ consisting of integral ideals of bounded norm. Since the norm is multiplicative, 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 10.1 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 10.2. *Suppose n is a positive integer and write $n = r_1 + 2r_2$ for some non-negative integers r_1 and r_2. Let $X \subset \mathbb{R}^n$ to be the compact convex symmetric set given by*

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

Then

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

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

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

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 $u_j \mapsto \frac{u_j}{2}$ for all j and using the fact that the integrand is symmetric in the x_i for all i gives

$$\mathrm{Vol}(X) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \int_{X''} u_1 \cdots u_{r_2}\, dx_1 \cdots dx_{r_1}\, du_1 \cdots du_{r_2}, \tag{12}$$

where

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

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 $x_i \mapsto tx_i$ and $u_j \mapsto tu_j$ for all i and j gives

$$I_{\ell,k}(t) = t^{\ell+2k} I_{\ell,k}(1). \tag{13}$$

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 Fubini–Tonelli theorem and Equation (13) 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

$$I_{\ell,k}(1) = \frac{1}{(\ell+2k)\cdots(2k+1)} I_{0,k}(1). \tag{14}$$

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 Fubini–Tonelli theorem, Equation (13), and **??**, gives

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

Repeating this procedure $k-1$ times results in

$$I_{0,k}(1) = \frac{1}{k!}, \tag{15}$$

since $I_{0,0}(1) = 1$. Combining Equations (13) to (15) 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 (12) we obtain

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

as desired. □

Observe that the set X in Lemma 10.2 just consists of those points in $\mathbb{R}^n$ whose induced norm corresponding to the induced Minkowski inner product is at most n (recall Proposition 9.1). We can now obtain an explicit bound in Theorem 10.1 known as the *Minkowski bound*:

Theorem (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*

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

Proof. Let X be given by

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

Then Theorem 10.1 and Lemma 10.2 together show that every ideal class contains an integral ideal $\mathfrak{a}$ such that

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

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

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

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

As a corollary we can obtain a lower bound for the discriminant of a number field and show that every number field K, other than $\mathbb{Q}$, has at least one ramified prime in $\mathcal{O}_K/\mathbb{Z}$:

Corollary 10.3. *Let K be a number field of degree n. Then*

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

In particular, there is at least one ramified prime in $\mathcal{O}_K/\mathbb{Z}$ provided the degree of K is at least 2.

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 the Minkowski bound. Now suppose $n \ge 2$. 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 $n^n \ge n!$ for all $n \ge 1$ (which easily follows by induction), $\left(\frac{\pi}{4}\right)^{\frac{n}{2}} \frac{n^n}{n!}$ is an increasing function in n. Therefore $|\Delta_K| \ge 2$ for all $n \ge 2$ so that $|\Delta_K|$ has a prime divisor. This means at least one prime of K ramifies in $\mathcal{O}_K/\mathbb{Z}$. $\square$

Generally speaking, the class number h_K is one of the most difficult pieces of arithmetic data about K to compute. For example, it is still unknown if there are infinitely many number fields of class number 1, that is, number fields such that their ring of integers are principal ideal domains.

11 Dirichlet's Unit Theorem

Let K be a number field of signature (r_1, r_2). We define the *rank* r_K of K to be

$$r_K = r_1 + r_2 - 1.$$

This will be an important in the following. Another very important piece of arithmetic data about K is the structure of the unit group $\mathcal{O}_K^*$. Note that $\mathcal{O}_K^*$ is closed under conjugation because $\mathrm{N}_K(\alpha) = \mathrm{N}_K(\overline{\alpha})$ as a consequence of Proposition 2.1. Moreover, since the norm of a unit is ± 1, we can express the unit group as

$$\mathcal{O}_K^* = \{\varepsilon \in \mathcal{O}_K : \mathrm{N}_K(\varepsilon) = \pm 1\}.$$

Our main goal will be to describe the group structure of $\mathcal{O}_K^*$ completely. Let Ω denote the group of all roots of unity. We will set $\mu(K) = \mathcal{O}_K^* \cap \Omega$ so that $\mu(K)$ is the subgroup of $\mathcal{O}_K^*$ consisting of all of the roots of unity in K. Clearly $\{\pm 1\} \subseteq \mu(K)$. In fact, $\mu(K)$ is finite since any root of unity in K is a root of $x^n - 1$ and thus an n-th root of unity. We set

$$w_K = |\mu(K)|.$$

Our goal will be to show that $\mathcal{O}_K^*$ is a direct product of $\mu(K)$ and a free abelian group of rank r_K. Determining that the rank of the free group is exactly r_K will be the most difficult part of the proof. We will require a map on K^* that transitions between the field trace and the field norm. Let $\rho_1, \ldots, \rho_{r_1}$ be the real $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$ and $\tau_1, \ldots, \tau_{r_2}$ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings of $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$. First consider the map

$$\ell : K_{\mathbb{R}}^* \to \mathbb{R}^{r_K+1} \qquad (z_\sigma)_\sigma \mapsto (\log|z_{\rho_1}|, \ldots, \log|z_{\rho_{r_1}}|, 2\log|z_{\tau_1}|, \ldots, 2\log|z_{\tau_{r_2}}|).$$

This map is independent of the choice of representatives $\tau_1, \ldots, \tau_{r_2}$ because $z_{\overline{\tau}} = \overline{z_\tau}$ for $\mathbf{z} \in K_{\mathbb{R}}$. We define the *logarithmic embedding* $\log_K$ of K by

$$\log_K : K^* \to \mathbb{R}^{r_K+1} \qquad \kappa \mapsto (\log|\rho_1(\kappa)|, \ldots, \log|\rho_{r_1}(\kappa)|, 2\log|\tau_1(\kappa)|, \ldots, 2\log|\tau_{r_2}(\kappa)|).$$

Then $\log_K$ is just the restriction of j to K^* composed with ℓ. Since ℓ is a homomorphism and j is a $\mathbb{Q}$-embedding, $\log_K$ is a homomorphism. We distinguish the subsets

$$S = \{\mathbf{x} \in \mathbb{R}_+^{r_K+1} : \mathrm{N}_{\mathbb{R}^{r_K+1}/\mathbb{R}}(\mathbf{x}) = 1\} \quad \text{and} \quad H = \{\mathbf{x} \in \mathbb{R}^{r_K+1} : \mathrm{Tr}_{\mathbb{R}^{r_K+1}/\mathbb{R}}(\mathbf{x}) = 0\},$$

called the *norm-one hypersurface* and *trace-zero hyperplane* of $\mathbb{R}^{r_K+1}$ respectively. Note that H is an r_K-dimensional subspace of $\mathbb{R}^{r_K+1}$. We will also make use of the subset

$$U = \{\mathbf{z} \in K_{\mathbb{R}} : \mathrm{N}_{K_{\mathbb{R}}}(\mathbf{z}) = \pm 1\}.$$

Let λ denote the restriction of $\log_K$ to $\mathcal{O}_K^*$ and set

$$\Lambda = \log_K(\mathcal{O}_K^*),$$

so that Λ is the image of λ. We call Λ the *unit lattice* of K. It is not immediately obvious that Λ is a lattice, but we will show this and more. Observe that ℓ takes U into H since $\mathrm{Tr}_{\mathbb{R}^{r_K+1}/\mathbb{R}}(\ell(\mathbf{z})) = \log|\,\mathrm{N}_{K_{\mathbb{R}}}(\mathbf{z})| = 1$. In particular, $\Lambda \subset H$ since $j(\mathcal{O}_K^*) \subset U$. All of this data can be collected into the following commutative diagram:

$$
\begin{tikzcd}
\mathcal{O}_K^* \arrow[r, "j"] \arrow[d] \arrow[rr, bend left, "\log_K"] & U \arrow[r, "\ell"] \arrow[d] & H \arrow[d] \\
K^* \arrow[r, "j"] \arrow[d, "\mathrm{N}"] & K_{\mathbb{R}}^* \arrow[r, "\ell"] \arrow[d, "\mathrm{N}_{K_{\mathbb{R}}}"] & \mathbb{R}^{r_K+1} \arrow[d, "\mathrm{Tr}_{\mathbb{R}^{r_K+1}/\mathbb{R}}"] \\
\mathbb{Q}^* \arrow[r] & \mathbb{R}^* \arrow[r, "\log|\,|"] & \mathbb{R}.
\end{tikzcd}
$$

We first show that the logarithmic embedding fits into an exact sequence:

Proposition 11.1. *Let K be a number field. Then the sequence*

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\ \lambda\ } \Lambda \longrightarrow 0,$$

is exact.

Proof. Exactness of this sequence means that $\mu(K)$ is the kernel of λ. If $\omega \in \mu(K)$ then $|\omega| = 1$ and it follows that $\lambda(\omega) = 0$. Therefore $\ker \lambda$ contains $\mu(K)$. To see that this is all of $\ker \lambda$, suppose $\varepsilon \in \mathcal{O}_K^*$ is such that $\lambda(\varepsilon) = 0$. But then every component of $j(\varepsilon)$ is has absolute value 1 and therefore belongs to a bounded subset of the Minkowski space $K_{\mathbb{R}}$. Since $\mathcal{O}_K^*$ is a subgroup of $\mathcal{O}_K$ and $j(\mathcal{O}_K)$ is a complete lattice in $K_{\mathbb{R}}$ (as we have already remarked), $j(\mathcal{O}_K^*)$ is a lattice in $K_{\mathbb{R}}$. But then $j(\varepsilon)$ belongs to a discrete set by **??**. Together, $j(\varepsilon)$ belongs to a discrete and bounded set and hence is necessarily finite. Since j is a $\mathbb{Q}$-embedding, it follows that the subgroup $\ker \lambda$ of $\mathcal{O}_K^*$ contains finitely many elements and hence only roots of unity because $\ker \lambda \subset K \subset \mathbb{C}$. Thus $\ker \lambda = \mu(K)$. □

Our aim now is to show that the unit lattice Λ is a a free abelian group of rank r_K. For this, we will require a lemma:

Lemma 11.2. *Let K be a number field. There are finitely many elements in $\mathcal{O}_K$ of a given norm up to multiplication by units.*

Proof. Recall that the norm of an algebraic integer is an integer and that the elements of norm ± 1 are exactly the units of K. Therefore it suffices to prove the claim for norm $n \geq 2$ (the norm is only zero for zero itself). Further recall that $\mathcal{O}_K / n\mathcal{O}_K$ is finite (with $\mathrm{N}_K(n\mathcal{O}_K)$ many elements). Therefore, it suffices to show that in each coset there is at most one element of norm n up to multiplication by units. To show this, suppose α and β are two representatives in the same coset and are of norm n. Writing $\alpha = \beta + n\gamma$ for some $n\gamma \in n\mathcal{O}_K$, we have

$$\frac{\alpha}{\beta} = 1 + \frac{n}{\beta}\gamma = 1 + \frac{\mathrm{N}_K(\beta)}{\beta}\gamma,$$

which is an element of $\mathcal{O}_K$ because $\frac{\mathrm{N}_K(\beta)}{\beta}$ is since $\mathrm{N}_K(\beta) \in \beta\mathcal{O}_K$ as any integral ideal contains it norm. Hence $\frac{\alpha}{\beta} \in \mathcal{O}_K$, and interchanging the roles of α and β shows that $\frac{\beta}{\alpha} \in \mathcal{O}_K$ too. But then $\frac{\alpha}{\beta}$ is a unit in $\mathcal{O}_K$ and thus α and β differ up to multiplication by a unit. $\square$

Recall that $\Lambda \subset H$. We will show Λ is a lattice in H, actually a complete lattice, and compute its rank as a free abelian group:

Theorem 11.3. *Let K be a number field of degree n and signature (r_1, r_2). Then the unit lattice Λ is a complete lattice in the trace-zero hyperplane H of $\mathbb{R}^{r_K+1}$. In particular, Λ is a free abelian group of rank r_K.*

Proof. Throughout, let σ run over $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})$, ρ run over all such real $\mathbb{Q}$-embeddings, and τ run over a complete set of representatives for the pairs of complex $\mathbb{Q}$-embeddings. We first prove Λ is a lattice in H. Since λ is a homomorphism (because $\log_K$ is), Λ is a subgroup of H. So by **??**, Λ is a lattice if and only if it is discrete. In particular, we will show that for any $c > 0$, the bounded region

$$X = \{\mathbf{x} \in \mathbb{R}^{r_K+1} : |x_\rho| \leq c \text{ and } |x_\tau| \leq 2c \text{ for all } \rho \text{ and } \tau\},$$

contains only finitely many points of Λ. The preimage of X under ℓ is

$$\ell^{-1}(X) = \{\mathbf{z} \in K_{\mathbb{R}} : e^{-c} \leq |z_\sigma| \leq e^c \text{ for all } \sigma\},$$

and hence it contains finitely many points of $j(\mathcal{O}_K^*)$ because this is a subset of the lattice $j(\mathcal{O}_K)$. It follows that X contains finitely many points of Λ (as the preimage of $\mathbf{x}$ in $\mathbb{R}^n$ under ℓ contains 2^n points of $K_{\mathbb{R}}$) so that Λ is discrete and thus a lattice. We will now show that Λ is a complete lattice in H and since H is an r_K-dimensional real vector space, this will also prove the claim about the rank of Λ. By **??** it suffices to show that there is a bounded subset M of the trace-zero hyperplane H whose translates by Λ cover H. Actually, since ℓ is surjective it suffices to construct a bounded subset T of U such that

$$U = \bigcup_{\varepsilon \in \mathcal{O}_K^*} j(\varepsilon)T.$$

Indeed, if such T exists then any $\mathbf{z} \in T$ satisfies $|\mathrm{N}_{K_{\mathbb{R}}}(\mathbf{z})| = \prod_\sigma |z_\sigma| = 1$ and hence each z_σ is bounded above and away from zero because T is bounded. Setting $M = \ell(T)$, it follows that M is also bounded (because $\log|z|$ is continuous) and

$$H = \bigcup_\lambda (M + \lambda).$$

It now suffices to construct such a subset T. For every σ, fix constants $c_\sigma > 0$ satisfying

$$c_\sigma = c_{\overline{\sigma}} \quad \text{and} \quad \prod_\sigma c_\sigma > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|D_K|},$$

and set $C = \prod_\sigma c_\sigma$. Now consider the bounded subset

$$Z = \{\mathbf{z} \in K_\mathbb{R} : |z_\sigma| < c_\sigma \text{ for all } \sigma\}.$$

For any $\mathbf{w} \in U$, we have

$$\mathbf{w}Z = \{\mathbf{z} \in K_\mathbb{R} : |z_\sigma| < |w_\sigma| c_\sigma \text{ for all } \sigma\},$$

and $\prod_\sigma |w_\sigma| c_\sigma = \mathrm{N}_{K_\mathbb{R}}(\mathbf{w})C = C$ so that $\mathbf{w}Z$ is also bounded. By Proposition 9.1, the volume of $\mathbf{w}Z$ is 2^{r_2} times the volume of

$$X = \{\mathbf{x} \in \mathbb{R}^n : |x_\rho| < c_\rho \text{ and } x_\tau^2 + x_{\overline{\tau}}^2 < c_\tau^2 \text{ for all } \rho \text{ and } \tau\},$$

which is $\prod_\rho (2c_\rho) \prod_\tau (\pi c_\tau^2) = C 2^{r_1} \pi^{r_2}$ because X is the product of r_1 many intervals each of length $2c_\rho$ and r_2 many disks each of of radius c_τ. Thus $\mathrm{Vol}(\mathbf{w}Z) = C 2^{r_K+1} \pi^{r_2}$. By Proposition 9.2, $V_{j(\mathcal{O}_K)} = \sqrt{|D_K|}$ and our choice of C gives

$$\mathrm{Vol}(\mathbf{w}Z) > 2^n V_{j(\mathcal{O}_K)}.$$

Since $j(\mathcal{O}_K)$ is a complete lattice in $K_\mathbb{R}$, Minkowski's lattice point theorem implies that there exists some nonzero $\alpha \in \mathcal{O}_K$ such that $j(\alpha) \in \mathbf{w}Z$. Now by Lemma 11.2, there exist finitely many nonzero elements $\alpha_1, \ldots, \alpha_m$ of $\mathcal{O}_K$ such that every $\alpha \in \mathcal{O}_K$ with $0 < \mathrm{N}_K(\alpha) \le C$ is equal to α_i for some $1 \le i \le m$ by multiplying by a unit. Set

$$T = U \cap \left(\bigcup_{1 \le i \le m} j(\alpha_i)^{-1} Z \right).$$

Then T is a bounded subset of U since Z is a bounded subset of $K_\mathbb{R}$ (and thus the $j(\alpha_i)^{-1}Z$ are too). We now claim that

$$U = \bigcup_{\varepsilon \in \mathcal{O}_K^*} j(\varepsilon)T.$$

Indeed, since $\mathbf{w}^{-1} \in U$ for any $\mathbf{w} \in U$ we have shown implies that there exists a nonzero $\alpha \in \mathcal{O}_K$ such that $j(\alpha) \in \mathbf{w}^{-1}Z$. Hence $j(\alpha) = \mathbf{w}^{-1}\mathbf{z}$ for some $\mathbf{z} \in Z$. But as

$$|\mathrm{N}_K(\alpha)| = |\mathrm{N}_{K_\mathbb{R}}(j(\alpha))| = |\mathrm{N}_{K_\mathbb{R}}(\mathbf{w}^{-1}\mathbf{z})| = |\mathrm{N}_{K_\mathbb{R}}(\mathbf{z})| < C,$$

it follows that there exists an α_i and $\varepsilon \in \mathcal{O}_K^*$ such that $\alpha_i = \alpha\varepsilon$. Writing $\mathbf{w} = j(\alpha)^{-1}\mathbf{z}$ (recall that $K_\mathbb{R}$ is commutative), we have

$$\mathbf{w} = j(\alpha)^{-1}\mathbf{z} = j(\alpha_i \varepsilon^{-1})^{-1}\mathbf{z} = j(\varepsilon) j(\alpha_i)^{-1}\mathbf{z},$$

where the last equality holds because j is a $\mathbb{Q}$-embedding. As $\mathbf{w}, j(\varepsilon) \in U$, we see that $j(\alpha_i)^{-1}\mathbf{z} \in U$ and thus $j(\alpha_i)^{-1}\mathbf{z} \in T$. But then $\mathbf{w} \in j(\varepsilon)T \subset U$ as desired. $\square$

By Theorem 11.3, there exist elements $\varepsilon_1, \ldots, \varepsilon_{r_K}$ of $\mathcal{O}_K^*$ such that $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r_K})$ is a basis for the unit lattice Λ by taking the preimage under j of any basis for Λ. We say that $\varepsilon_1, \ldots, \varepsilon_{r_K}$ are a *system of fundamental units* of K and we call any such element a *fundamental unit* for K. The structure theorem for $\mathcal{O}_K^*$ known as *Dirichlet's unit theorem* says that $\mathcal{O}_K^*$ is a product of a root of unity in K and powers of fundamental units:

Theorem (Dirichlet's unit theorem). *Let K be a number field of signature (r_1, r_2). Then*

$$\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r_K}.$$

In particular, if $\varepsilon_1, \ldots, \varepsilon_{r_K}$ is a system of fundamental units for K then any unit ε of K is of the form

$$\varepsilon = \omega \varepsilon_1^{\nu_1} \cdots \varepsilon_{r_K}^{\nu_{r_K}},$$

for some $\omega \in \mu(K)$ and $\nu_i \in \mathbb{Z}$ for $1 \leq i \leq r_K$.

Proof. By Proposition 11.1 we have an exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\lambda} \Lambda \longrightarrow 0,$$

and by Theorem 11.3 we know that Λ is a free abelian group of rank r_K. Let $\varepsilon_1, \ldots, \varepsilon_{r_K}$ be a system of fundamental units for K and let E be the subgroup of $\mathcal{O}_K^*$ generated by them. Then λ induces an isomorphism between E and Λ so that $\mu(K) \cap E = \{1\}$ because the sequence is exact. As $\mu(K)$ and E are subgroups, $\mu(K) \cap E = \{1\}$ implies $\mathcal{O}_K^* \cong \mu(K) \times E$. Since $E \cong \mathbb{Z}^{r_K}$ (because $\Lambda \cong \mathbb{Z}^{r_K}$), we have $\mathcal{O}_K^* \cong \mu(K) \times \mathbb{Z}^{r_K}$. Moreover, from the isomorphism $E \cong \mathbb{Z}^{r_K}$ we see that any element of E is of the form $\varepsilon_1^{\nu_1} \cdots \varepsilon_{r_K}^{\nu_{r_K}}$ with $\nu_i \in \mathbb{Z}$ for $1 \leq i \leq r_K$. This completes the proof. $\square$

Note that Dirichlet's unit theorem also implies that Λ is a complete lattice in H (by the definition of λ). In other words, we may reference this result instead of Theorem 11.3. We will now discuss the covolume V_Λ of Λ. Let $\varepsilon_1, \ldots, \varepsilon_{r_K}$ be a system of fundamental units for K. Then $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r_K})$ is a basis for Λ. Setting

$$\lambda_0 = \frac{1}{\sqrt{r_K + 1}} \mathbf{1},$$

we see that λ_0 is a unit vector in $\mathbb{R}^{r_K+1}$ since $\|\mathbf{1}\| = r_K + 1$ and is orthogonal to H because $\mathrm{Tr}_{\mathbb{R}^{r_K+1}/\mathbb{R}}(\lambda_0) = \sqrt{r_K + 1}$ is nonzero. As λ_0 is orthogonal to $\Lambda \subset H$, we see that $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r_K})$ is a basis for the complete lattice $\Lambda' = \mathbb{Z}\lambda_0 + \Lambda$ in $\mathbb{R}^{r_K+1}$. Since λ_0 is a unit vector, the volume of the fundamental domain for Λ' in $\mathbb{R}^{r_K+1}$ is equal to the volume of the fundamental domain for Λ in $\mathbb{H}$. By **??**, the corresponding covolumes are equal which is to say $V_\Lambda = V_{\Lambda'}$. So it suffices to compute $V_{\Lambda'}$. The generator matrix P for Λ' associated to the basis $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r_K})$ is given by

$$P = \begin{pmatrix} \frac{1}{\sqrt{r_K+1}} & \lambda(\varepsilon_1)_1 & \cdots & \lambda(\varepsilon_{r_K})_1 \\ \vdots & \vdots & & \vdots \\ \frac{1}{\sqrt{r_K+1}} & \lambda(\varepsilon_1)_{r_K+1} & \cdots & \lambda(\varepsilon_{r_K})_{r_K+1} \end{pmatrix}.$$

Adding all of the rows to a fixed row results in

$$P' = \begin{pmatrix} \frac{1}{\sqrt{r_K+1}} & \lambda(\varepsilon_1)_1 & \cdots & \lambda(\varepsilon_{r_K})_1 \\ \vdots & \vdots & & \vdots \\ \sqrt{r_K + 1} & 0 & & 0 \\ \vdots & \vdots & & \vdots \\ \frac{1}{\sqrt{r_K+1}} & \lambda(\varepsilon_1)_{r_K+1} & \cdots & \lambda(\varepsilon_{r_K})_{r_K+1} \end{pmatrix},$$

because $\lambda(\varepsilon) \in H$ for all $\varepsilon \in \mathcal{O}_K^*$. As P' differs from P be row addition, their determinants are the same. Cofactor expanding along the row with all zeros except the first entry, and that this row is arbitrary, shows

$$V_\Lambda = \sqrt{r_K + 1} R_K, \tag{16}$$

where R_K is the absolute value of the determinant of any rank r_K minor of

$$\begin{pmatrix} \lambda(\varepsilon_1)_1 & \cdots & \lambda(\varepsilon_{r_K})_1 \\ \vdots & & \vdots \\ \lambda(\varepsilon_1)_{r_K+1} & \cdots & \lambda(\varepsilon_{r_K})_{r_K+1} \end{pmatrix}.$$

We call R_K the *regulator* of K. Since V_Λ is independent of the choice of basis, the regulator R_K is independent of any choice of a system of fundamental units for K. Moreover, since H is a real inner product space we see that the regulator is roughly a measure of the density of the fundamental units in K (recall **??**). The smaller the regulator the more dense the fundamental units are.