Classical Algebraic and Analytic Number Theory

Henry Twiss

2025

Contents

Part I

Multiplicative Number Theory

Chapter 1

Arithmetic Functions

1.1 Multiplicative and Additive Functions

Any function

$$f : \mathbb{Z}_{\geq 1} \to \mathbb{C},$$

is said to be **arithmetic**. That is, arithmetic functions are maps from the positive integers to the complex numbers. If an arithmetic function f satisfies

$$f(nm) = f(n)f(m) \quad \text{or} \quad f(nm) = f(n) + f(m),$$

whenever n and m are relatively prime, we say f is **multiplicative** or **additive** respectively. If either condition holds for all n and m then we say f is **completely multiplicative** or **completely additive**. If f is additive or multiplicative then f is uniquely determined by its values on prime powers and if f is completely additive or completely multiplicative then it is uniquely determined by its values on primes. Moreover, we have

$$f(1) = 1 \quad \text{or} \quad f(1) = 0,$$

according to if f is multiplicative or additive. Most important arithmetic functions are either multiplicative or additive. Below is a list of the most important arithmetic functions (some of these functions are restrictions of common functions but we define them here as arithmetic functions for completeness):

(i) The **constant function**: The function $\mathbf{1}(n)$. This function is neither additive nor multiplicative.

(ii) The **indicator function**: The function $\varepsilon(n)$ defined by

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

This function is completely multiplicative.

(iii) The **identity function**: The function $\mathrm{id}(n)$. This function is completely multiplicative.

(iv) The **logarithm**: The function $\log(n)$. This function is completely additive.

(v) The **Möbius function**: The function $\mu(n)$ defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n \text{ is square-free with an even number of prime factors,} \\ -1 & \text{if } n \text{ is square-free with an odd number of prime factors,} \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

This function is multiplicative.

(vi) The **characteristic function of square-free integers**: The square of the Möbius function $\mu^2(n)$. This function is multiplicative.

(vii) **Liouville's function**: The function $\lambda(n)$ defined by

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is composed of } k \text{ not necessarily distinct prime factors.} \end{cases}$$

This function is completely multiplicative.

(viii) **Euler's totient function**: The function $\varphi(n)$ defined by

$$\varphi(n) = \sum_{\substack{a \pmod n \\ (a,n)=1}} 1.$$

This function is multiplicative.

(ix) The **divisor function**: The function $\sigma_0(n)$ defined by

$$\sigma_0(n) = \sum_{d|n} 1.$$

This function is multiplicative.

(x) The **sum of divisors function**: The function $\sigma_1(n)$ defined by

$$\sigma_1(n) = \sum_{d|n} d.$$

This function is multiplicative.

(xi) The **generalized sum of divisors function**: The function $\sigma_s(n)$ defined by

$$\sigma_s(n) = \sum_{d|n} d^s,$$

for any $s \in \mathbb{C}$. This function is multiplicative.

(xii) The **number of distinct prime factors function**: The function $\omega(n)$ defined by

$$\omega(n) = \sum_{p|n} 1.$$

This function is additive.

(xiii) The **total number of prime divisors function**: The function $\Omega(n)$ defined by

$$\Omega(n) = \sum_{p^m|n} 1.$$

This function is completely additive.

(xiv) The **von Mangoldt function**: The function $\Lambda(n)$ defined by

$$\Lambda(n) = \begin{cases} 0 & \text{if } n \text{ is not a prime power,} \\ \log(p) & \text{if } n = p^m \text{ for some prime } p \text{ and positive integer } m. \end{cases}$$

This function is neither additive or multiplicative.

1.2 Dirichlet Convolution and Möbius Inversion

If f and g are two arithmetic functions then we can define a new arithmetic function $f * g$ called their **Dirichlet convolution** defined by

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

As the sum is over all divisors, Dirichlet convolution is a symmetric operation. Dirichlet convolution preserves multiplicative functions.

Proposition 1.2.1. *If f and g are multiplicative arithmetic functions then so is their Dirichlet convolution $f * g$.*

Proof. Let n and m be relatively prime positive integers. Every divisor d of nm is of the form $d = d'd''$ with d' a divisor of n, d'' a divisor of m, and d' and d'' relatively prime. A short computation shows

$$\sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) = \left(\sum_{d'|n} f(d') g\left(\frac{n}{d'}\right)\right) \left(\sum_{d''|m} f(d'') g\left(\frac{m}{d''}\right)\right),$$

which is equivalent to the claim. □

This result makes the set of multiplicative functions into a commutative semigroup under Dirichlet convolution. It is actually a commutative monoid since the indicator function ε acts as an identity. This means

$$f * \varepsilon = f.$$

A certain case of interest for Dirichlet convolution is when the Möbius function is convolved with the constant function.

Proposition 1.2.2. *We have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \geq 2. \end{cases}$$

In particular,

$$\mu * \mathbf{1} = \varepsilon.$$

Proof. The first statement is equivalent to the second, so it suffices to prove the first. The sum $\sum_{d|n} \mu(d)$ is multiplicative by Proposition 1.2.1 so we may assume $n = p^r$ is a nonnegative power of a prime. When $r = 0$, $d = 1$ and the sum is 1. When $r \geq 1$, d runs over $1, p, \ldots, p^r$. Every value is zero except $\mu(1) = 1$ and $\mu(p) = -1$. This proves that the sum is zero. □

With this result we can prove **Möbius inversion**:

Theorem (Möbius inversion). *If f and g are arithmetic functions, then*

$$g(n) = \sum_{d|n} f(d) \quad \text{if and only if} \quad f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

In particular,

$$g = f * \mathbf{1} \quad \text{if and only if} \quad f = g * \mu.$$

Proof. As the first statement is equivalent to the second, we will prove the second statement. Convolving $g = f * \mathbf{1}$ with μ gives $f = g * \mu$ in view of Proposition 1.2.2. This proves the forward implication. The reverse implication follows by convolving $f = g * \mu$ with $\mathbf{1}$ and arguing analogously. □

Chapter 2

Todo: [Ditributions and Asymptotics]

Chapter 3

Dirichlet Characters and Exponential Sums

3.1 Dirichlet Characters

Let m be a positive integer. A multiplicative homomorphism

$$\chi : \mathbb{Z} \to \mathbb{C},$$

is said to be a **Dirichlet character** modulo m if it is m-periodic and such that $\chi(a) = 0$ if and only if $(a, m) > 1$. We call m the **modulus** of χ. A Dirichlet character is necessarily a completely multiplicative arithmetic function when restricted to the positive integers.

We say a Dirichlet character χ is **principal** if it only takes values 0 or 1. There is always a unique principal Dirichlet character modulo m, denoted $\chi_{m,0}$, defined by

$$\chi_{m,0}(a) = \begin{cases} 1 & (a, m) = 1, \\ 0 & (a, m) > 1. \end{cases}$$

When the modulus is 1, the principal Dirichlet character is identically 1 and we call this the **trivial Dirichlet character**. This is the only Dirichlet character modulo 1.

By Euler's little theorem, $a^{\varphi(m)} \equiv 1 \pmod{m}$ whenever $(a, m) = 1$. This forces $\chi(a)^{\varphi(m)} = 1$ and so the nonzero values of any Dirichlet character modulo m are $\varphi(m)$-th roots of unity. This implies that there are only finitely many Dirichlet characters of any fixed modulus. Given two Dirichlet character χ and ψ modulo m, the functions

$$\chi\psi : \mathbb{Z} \to \mathbb{C} \quad \text{and} \quad \overline{\chi} : \mathbb{Z} \to \mathbb{C},$$

are also Dirichlet characters modulo m. This turns the set of such Dirichlet characters into an abelian group denote by X_m where the identity is the principal Dirichlet character modulo m and the inverse is given by the conjugate as the nonzero values of Dirichlet characters are roots of unity.

This is all strikingly similar to characters on $(\mathbb{Z}/m\mathbb{Z})^*$ and there is indeed a connection. By the multiplicativity and m-periodicity of χ, it induces a character of

$(\mathbb{Z}/m\mathbb{Z})^*$. Conversely, if we are given a character on $(\mathbb{Z}/m\mathbb{Z})^*$ we can extend it to a Dirichlet character χ by defining it to be m-periodic with $\chi(a) = 0$ if $(a, m) > 1$. We call this extension a **zero extension**. This argument shows that Dirichlet characters modulo m are exactly the zero extensions of characters on $(\mathbb{Z}/m\mathbb{Z})^*$. As abelian groups are isomorphic to their character groups, we deduce that the group of Dirichlet characters modulo m is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$. Therefore there are $\varphi(m)$ Dirichlet characters modulo m and we identify them with the characters on $(\mathbb{Z}/m\mathbb{Z})^*$. Just as for characters of abelian groups, we have orthogonality relations called the **Dirichlet orthogonality relations**.

Proposition (Dirichlet orthogonality relations). *Let χ and ψ be Dirichlet characters modulo m and let $a, b \in (\mathbb{Z}/m\mathbb{Z})^*$. Then*

$$\sum_{a \pmod m} (\chi\overline{\psi})(a) = \varphi(m)\delta_{\chi,\psi} \quad \textit{and} \quad \sum_{\chi \pmod m} \chi(a\bar{b}) = \varphi(m)\delta_{a,b}.$$

In particular,

$$\sum_{a \pmod m} \chi(a) = \varphi(m)\delta_{\chi,\chi_{m,0}} \quad \textit{and} \quad \sum_{\chi \pmod m} \chi(a) = \varphi(m)\delta_{a,1}.$$

Proof. If $\chi = \psi$ then the first sum is clearly $\phi(m)$. If not, let $b \in (\mathbb{Z}/m\mathbb{Z})^*$ be such that $(\chi\overline{\psi})(b) \neq 1$. A short computation shows

$$(\chi\overline{\psi})(b) \sum_{a \pmod m} (\chi\overline{\psi})(a) = \sum_{a \pmod m} (\chi\overline{\psi})(a),$$

in which case the sum vanishes. This proves the first identity. For the second, if $a = b$ then the second sum is clearly $\varphi(m)$. If $a \neq b$, we claim that there exists a Dirichlet character ψ modulo m with $\psi(a\bar{b}) \neq 1$. Set $g = a\bar{b}$. The cyclic subgroup $\langle g \rangle$ of $(\mathbb{Z}/m\mathbb{Z})^*$ has some order $d > 1$. Consider the homomorphism

$$\psi_d : \langle g \rangle \to \mathbb{C} \qquad g^k \mapsto e^{\frac{2\pi i k}{d}}.$$

By the structure theorem for finite abelian groups, $(\mathbb{Z}/m\mathbb{Z})^* \cong \langle g \rangle \times H$ for some subgroup H. Whence we define a Dirichlet character ψ modulo m by

$$\psi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C} \qquad g^k h \mapsto e^{\frac{2\pi i k}{d}}.$$

This ψ is the desired Dirichlet character, A short computation shows

$$\psi(a\bar{b}) \sum_{\chi \pmod m} \chi(a\bar{b}) = \sum_{\chi \pmod m} \chi(a\bar{b}),$$

in which case the sum vanishes. This proves the second identity and the first statement in its entirety. The second statement follows from the first upon taking $\psi = \chi_{m,0}$ and $b = 1$ respectively. $\square$

It it possible for Dirichlet characters of a fixed modulus to arise from Dirichlet characters of a smaller modulus. Suppose χ and χ^* are Dirichlet characters modulo m and d respectively with $d \mid m$. We say χ is induced **induced** from χ^* if

$$\chi(a) = \begin{cases} \chi^*(a) & \text{if } (a,m) = 1, \\ 0 & \text{if } (a,m) > 1. \end{cases}$$

This means χ is a Dirichlet character whose values are given by those of χ^*. Necessarily χ is d-periodic and its nonzero values are $\varphi(d)$-th roots of unity. We say a Dirichlet character is **primitive** if it is not induced by any Dirichlet character other than itself and **imprimitive** otherwise. The principal Dirichlet characters are precisely those induced from the trivial Dirichlet character and the only primitive one is the trivial Dirichlet character itself. Moreover, a Dirichlet character is primitive if and only if its conjugate is. Our primary aim will be to show that every Dirichlet character is induced from a unique primitive Dirichlet character.

Theorem 3.1.1. *Suppose χ is a Dirichlet character modulo m. There exists a unique primitive Dirichlet character $\widetilde{\chi}$ such that χ is induced from $\widetilde{\chi}$.*

Proof. Let q be the positive integer given by

$$q = \min\{d \mid m : \chi(a) = \chi(b) \text{ for all } a \equiv b \pmod{d} \text{ with } (ab, m) = 1\},$$

and let $\widetilde{\chi} : \mathbb{Z} \to \mathbb{C}$ be defined by

$$\widetilde{\chi}(a) = \begin{cases} \chi(a) & \text{if } (a,q) = 1, \\ 0 & \text{if } (a,q) > 1. \end{cases}$$

The definition of q implies $\widetilde{\chi}$ is well-defined and hence q-periodic. In fact, $\widetilde{\chi}$ is a Dirichlet character modulo q and minimality forces $\widetilde{\chi}$ to be primitive. By construction χ is indued from $\widetilde{\chi}$ and this proves existence. Now suppose $\widetilde{\chi}_1$ and $\widetilde{\chi}_2$ are two primitive Dirichlet characters modulo q_1 and q_2 respectively both of which induce χ. Then $\widetilde{\chi}_1(a) = \widetilde{\chi}_2(a)$ whenever $(a,m) = 1$. Setting $q = (q_1, q_2)$, we also have $\widetilde{\chi}_1(a) = \widetilde{\chi}_2(a)$ whenever $(a,q) = 1$. Hence $\widetilde{\chi}_1$ and $\widetilde{\chi}_2$ are both induced from the same Dirichlet character modulo q. Primitivity implies $q_1 = q_2$ and $\widetilde{\chi}_1 = \widetilde{\chi}_2$. This proves uniqueness. □

In light of this result, we define the **conductor** q of a Dirichlet character χ modulo m to be the modulus of the unique primitive Dirichlet character $\widetilde{\chi}$ inducing χ. By the proof, the conductor is given by

$$q = \min\{d \mid m : \chi(a) = \chi(b) \text{ for all } a \equiv b \pmod{d} \text{ with } (ab, m) = 1\}.$$

Also observe that χ is q-periodic, q is the minimal period of χ, and the nonzero values of χ are $\varphi(q)$-th roots of unity. Moreover,

$$\chi = \widetilde{\chi}\chi_{\frac{m}{q},0},$$

and χ is primitive if and only if its conductor and modulus are equal.

As not every Dirichlet character of a fixed modulus is primitive, it is natural to ask how many primitive Dirichlet characters there are for a given modulus. Let $N(m)$ be the number of primitive Dirichlet characters modulo m. Then $N(m)$ is easily determined via Möbius inversion.

Proposition 3.1.2. *For any positive integer m, we have*

$$\phi(m) = \sum_{d|m} N(d),$$

where $N(d)$ be the number of primitive Dirichlet characters modulo d. In particular, $N(m)$ is given by

$$N(m) = \sum_{d|m} \phi(d)\mu\left(\frac{m}{d}\right)$$

Proof. To prove the first formula, the right-hand side counts the number of Dirichlet characters modulo m since every such Dirichlet character is induced from a unique primitive Dirichlet character whose modulus divides m by Theorem 3.1.1. The left hand side also counts the number of Dirichlet characters modulo m as are $\phi(m)$ many. This proves the first formula. The second follows by Möbius inversion. □

Primitive Dirichlet characters also behave well with respect to multiplication if the conductors are relatively prime as the following proposition shows:

Proposition 3.1.3. *Suppose χ_1 and χ_2 are Dirichlet characters modulo m_1 and m_2 respectively with $(m_1, m_2) = 1$. Set $\chi = \chi_1\chi_2$. Then χ is a primitive if and only if χ_1 and χ_2 both are.*

Proof. By construction, χ is a Dirichlet character modulo m_1m_2. Let q_1 and q_2 be the conductors of χ_1 and χ_2 respectively and let q be the conductor of χ. Then χ is q_1q_2-periodic and $q \mid q_1q_2$.

For the forward implication, suppose χ is primitive so that $q = m_1m_2$ whence $m_1m_2 \mid q_1q_2$. This forces $m_1 = q_1$ and $m_2 = q_2$ proving χ_1 and χ_2 are both primitive. For the reverse implication, suppose χ_1 and χ_2 are both primitive so that $q_1 = m_1$ and $q_2 = m_2$. Then $(q_1, q_1) = 1$ and the Chinese remainder theorem implies that χ is q_1-periodic on those integers that are congruent to 1 modulo q_2 and q_2-periodic on those integers that are congruent to 1 modulo q_1. This forces $q_1 \mid q$ and $q_2 \mid q$ which together imply $q = q_1q_2$ and thus χ is primitive. □

We would now like to distinguish Dirichlet characters based on their nonzero values. We say χ is **real** if it is real-valued. This means the nonzero values of χ are 1 or -1 since they are the only real roots of unity. We say χ is **complex** if it is not real. More commonly, we distinguish Dirichlet characters by the roots of unity that their nonzero values take. We say χ is of **order** n if the nonzero values of χ are all n-th roots of unity. In the cases of small order we will often use the latin derived

names **quadratic**, **cubic**, etc. To connect these two naming conventions observe that a nontrivial Dirichlet character is quadratic if and only if it is real and an other nontrivial Dirichlet character is necessarily complex. Also note that quadratic Dirichlet characters are their own conjugates.

We will also distinguish Dirichlet characters by their parity. By multiplicativity, we must have $\chi(-1) = \pm 1$. Accordingly, we say χ is **even** if $\chi(-1) = 1$ and **odd** if $\chi(-1) = -1$. Then even Dirichlet characters are even functions while odd Dirichlet characters are odd functions. Note that conjugate and induced Dirichlet characters necessarily have the same parity. The parity is also expressed via the formula

$$\frac{\chi(1) - \chi(-1)}{2} = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ 1 & \text{if } \chi \text{ is odd.} \end{cases}$$

3.2 Quadratic Dirichlet Characters

Quadratic Dirichlet characters deserve special attention as it is possible to classify all of them explicitly. This is due to the fact that they arise from Jacobi and Kronecker symbols. For a positive odd integer m, define

$$\chi_m(a) = \left(\frac{a}{m}\right).$$

By definition of the Jacobi symbol, χ_m becomes a quadratic Dirichlet character modulo m. Unfortunately, the quadratic Dirichlet characters constructed in this manner do not exhaust all possible examples. To accomplish this we need to use Kronecker symbols. An integer D is said to be a **fundamental discriminant** if it is of the form

$$D = \begin{cases} d & \text{if } D \equiv 1 \pmod 4, \\ 4d & \text{if } D \equiv 8, 12 \pmod{16}, \end{cases}$$

for some square-free integer d. Necessarily $d \equiv 1 \pmod 4$ or $d \equiv 2, 3 \pmod 4$ respectively and thus is nonzero. We define $\chi_D : \mathbb{Z} \to \mathbb{C}$ by

$$\chi_D(a) = \left(\frac{D}{a}\right).$$

It turns out that χ_D defines a primitive quadratic Dirichlet character modulo $|D|$, provided $D \neq 1$, and exhausts all such possibilities.

Theorem 3.2.1. *If D is a fundamental discriminant and $D \neq 1$ then χ_D is a primitive quadratic Dirichlet character of conductor $|D|$. Moreover, all primitive quadratic Dirichlet characters are of this form.*

Proof. We first show that χ_D is a primitive quadratic Dirichlet character modulo $|D|$. If $D \equiv 1 \pmod 4$, the sign in quadratic reciprocity is always 1. Then

$$\chi_D(a) = \left(\frac{a}{|D|}\right),$$

which is a Dirichlet character modulo $|D|$. If $D \equiv 12 \pmod{16}$ then $\frac{D}{4} \equiv 3 \pmod{4}$ and the sign in quadratic reciprocity is $\left(\frac{-1}{a}\right)$ which is the primitive quadratic Dirichlet character modulo 4 as there are only two such Dirichlet characters and $\left(\frac{-1}{a}\right)$ is not principal. Whence

$$\chi_D(a) = \left(\frac{-1}{a}\right)\left(\frac{a}{\left|\frac{D}{4}\right|}\right),$$

which is a Dirichlet character modulo $|D|$. If $D \equiv 8 \pmod{16}$ first observe that $\left(\frac{D}{a}\right) = \left(\frac{8}{a}\right)\left(\frac{\frac{D}{8}}{a}\right)$ where $\left(\frac{8}{a}\right)$ is one of the two primitive quadratic Dirichlet character modulo 8 (the other is $\left(\frac{-8}{a}\right)$). As $\frac{D}{8} \equiv 1, 3 \pmod{4}$, the sign in quadratic reciprocity is either 1 or $\left(\frac{-1}{a}\right)$ according to these two cases. Thus

$$\chi_D(a) = \left(\frac{8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) \quad \text{or} \quad \chi_D(a) = \left(\frac{-8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right),$$

according to if $\frac{D}{8} \equiv 1, 3 \pmod{4}$ respectively, and in either case is a Dirichlet character modulo $|D|$. We can compactly express all of these cases as follows:

$$\chi_D(a) = \begin{cases} \left(\frac{a}{|D|}\right) & \text{if } D \equiv 1 \pmod{4}, \\ \left(\frac{-1}{a}\right)\left(\frac{a}{\left|\frac{D}{4}\right|}\right) & \text{if } \frac{D}{4} \equiv 3 \pmod{4}, \\ \left(\frac{8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) & \text{if } \frac{D}{8} \equiv 1 \pmod{4}, \\ \left(\frac{-8}{a}\right)\left(\frac{a}{\left|\frac{D}{8}\right|}\right) & \text{if } \frac{D}{8} \equiv 3 \pmod{4}. \end{cases}$$

This proves χ_D is a Dirichlet characters modulo $|D|$. It is not hard to see that χ_D is primitive. Indeed, we have already mentioned that the characters $\left(\frac{-1}{a}\right)$, $\left(\frac{8}{a}\right)$, and $\left(\frac{-8}{a}\right)$ are all primitive. Since D, $\frac{D}{4}$, and $\frac{D}{8}$ are square-free according to their equivalences modulo 4 and $D \neq 1$, it suffices to show that χ_p is primitive for all primes p with $p \neq 2$ by Proposition 3.1.3. This is immediate since p is prime and χ_p is not principal.

We now show that every primitive quadratic Dirichlet character is of the form χ_D for some fundamental discriminant D. By Proposition 3.1.3 again, it suffices to consider primitive quadratic Dirichlet character modulo a prime power p^m.

First suppose $p \neq 2$. Then $(\mathbb{Z}/p^m\mathbb{Z})^*$ is cyclic, generated by say g, and every $a \in (\mathbb{Z}/p^m\mathbb{Z})^*$ is of the form $a = g^\nu$ for some $\nu \in (\mathbb{Z}/\varphi(p^m)\mathbb{Z})$. It follows that every corresponding Dirichlet character χ is of the form

$$\chi(a) = e^{\frac{2\pi i k \nu}{\varphi(p^m)}},$$

for an integer k modulo $\varphi(p^m)$. Moreover, χ is primitive if and only if $k \not\equiv 0 \pmod{p}$ for otherwise χ is a Dirichlet character modulo p^{m-1}. Similarly, χ is quadratic if and only if $k \equiv \frac{\varphi(p^m)}{2} \pmod{\varphi(p^m)}$. Such a k exists and is unique because $p \neq 2$. We also see that if χ is quadratic then it is imprimitive unless $m = 1$ for then $\varphi(p) = p - 1$ which is not a multiple of p. To summarized, there is a unique quadratic Dirichlet

character modulo p^m and it is primitive if and only if $m = 1$. Necessarily, this unique primitive quadratic Dirichlet character modulo p is given by χ_D for the fundamental discriminant $D = p$ if $p \equiv 1 \pmod 4$ and $D = -p$ if $p \equiv 3 \pmod 4$.

Now suppose $p = 2$ so that $p^m = 2^m$. If $m = 1$ then $\varphi(2) = 1$ and there are no primitive quadratic Dirichlet characters as the only Dirichlet character is principal. If $m = 2$ then $\varphi(4) = 2$ so that there are two Dirichlet characters. They are both quadratic but only one is primitive namely the aforementioned $\left(\frac{-1}{a}\right)$. This primitive quadratic Dirichlet character is given by χ_D for the fundamental discriminant $D = -4$. For $m \geq 3$ there is an isomorphism $(\mathbb{Z}/2^m\mathbb{Z})^* \cong C_2 \times C_{2^{m-2}}$ where C_2 and $C_{2^{m-2}}$ are the cyclic groups of order 2 and 2^{m-2} respectively. Therefore every $a \in (\mathbb{Z}/2^m\mathbb{Z})^*$ is of the form $a = (-1)^\mu 5^\nu$ for some $\mu \in \mathbb{Z}/2\mathbb{Z}$ and $\nu \in \mathbb{Z}/2^{m-2}\mathbb{Z}$. Then every corresponding Dirichlet character χ is of the form

$$\chi(a) = e^{\frac{2\pi i j \mu}{2}} e^{\frac{2\pi i k \nu}{2^{m-2}}},$$

for integers j modulo 2 and k modulo 2^{m-2}. Similarly to the case for $p \neq 2$, χ is primitive if and only if $k \not\equiv 0 \pmod{2^{m-2}}$. Moreover, χ is quadratic if and only if $k \equiv 0 \pmod{2^{m-3}}$. These congruences together imply that a primitive quadratic Dirichlet character exists if and only if $m = 3$. In this case there are four Dirichlet characters. They are all quadratic but only two are primitive, namely the aforementioned $\left(\frac{8}{a}\right)$ and $\left(\frac{-8}{a}\right)$. These two primitive quadratic Dirichlet characters are given by χ_D for the fundamental discriminants $D = 8$ and $D = -8$ respectively. □

It follows from Theorem 3.2.1 that all quadratic Dirichlet characters are induced from some χ_D including $D = 1$ since this corresponds to the trivial Dirichlet character. In particular, so too are the quadratic Dirichlet characters given by Jacobi symbols.

3.3 Ramanujan and Gauss Sums

For integers b and m with m positive, the **Ramanujan sum** $r(b, m)$ is defined by

$$r(b, m) = \sum_{\substack{a \pmod m \\ (a,m)=1}} e^{\frac{2\pi i a b}{m}}.$$

The Ramanujan sum is a finite sum of m-th roots of unity. When $b \mid m$ the summands are all 1 and the Ramanujan sum has the simple evaluation

$$r(b, m) = \varphi(m).$$

For a general idex the Ramanujan sums can be computed explicitly by means of the Möbius function.

Proposition 3.3.1. *For integers b and m with m positive, we have*

$$r(b, m) = \sum_{d \mid (b,m)} d\mu\left(\frac{m}{d}\right).$$

Proof. The identity is obvious if $m = 1$ since the Ramanujan sum is 1. So assume $m > 1$. Every a modulo m is of the form $a = a'd$ for some divisor d of m and a' modulo $\frac{m}{d}$ with $\left(a', \frac{m}{d}\right) = 1$. So summing $r(b,d)$ over the divisors d of m gives

$$\sum_{d|m} r(b,d) = \sum_{a \pmod m} e^{\frac{2\pi iab}{m}},$$

If $m \mid b$ the latter sum is m while if $m \nmid b$ the sum vanishes as it is the sum of all m-th roots of unity. Thus

$$\sum_{d|m} r(b,d) = \begin{cases} m & \text{if } m \mid b, \\ 0 & \text{if } m \nmid b. \end{cases}$$

Now apply Möbius inversion. □

More general Ramanujan sums can be constructed by introducing a Dirichlet character. Let χ be a Dirichlet character modulo m. For any integer b, the **Ramanujan sum** $\tau(n,\chi)$ associated to χ is given by

$$\tau(b,\chi) = \sum_{a \pmod m} \chi(a) e^{\frac{2\pi iab}{m}}.$$

This generalizes the previous Ramanujan sum as

$$r(b,m) = \tau(b, \chi_{m,0}).$$

When $b \mid m$ the summands are all 1 and the Dirichlet orthogonality relations imply

$$\tau(b,\chi) = \varphi(m)\delta_{\chi,\chi_{m,0}}.$$

When $b = 1$ we simply write $\tau(\chi) = \tau(1,\chi)$ and call $\tau(\chi)$ the **Gauss sum** associated to χ. The following proposition develops the basic properties of these Ramanujan sums:

Proposition 3.3.2. *Let χ and ψ be nontrivial Dirichlet characters modulo m and n respectively and let b be an integer. Then the following properties hold:*

(i) $\overline{\tau(b,\overline{\chi})} = \chi(-1)\tau(b,\chi)$.

(ii) If $(b,m) = 1$ *then* $\tau(b,\chi) = \overline{\chi}(b)\tau(\chi)$.

(iii) If $(b,m) > 1$ *and* χ *is primitive then* $\tau(b,\chi) = 0$.

(iv) If $(m,n) = 1$ *then* $\tau(b,\chi\psi) = \chi(n)\psi(m)\tau(b,\chi)\tau(b,\psi)$.

(v) If $\widetilde{\chi}$ *is the primitive Dirichlet character of conductor q inducing χ, then*

$$\tau(\chi) = \mu\left(\frac{m}{q}\right)\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

Proof. We will prove the properties separately.

(i) This follows by direct computation.

(ii) This follows by direct computation.

(iii) Let c be an integer with $(c, m) = 1$ and satisfying $\chi(c) \neq 1$. Such a c exists because otherwise χ the principal Dirichlet character modulo m and thus imprimitive. A short computation shows

$$\chi(c)\tau(b, \chi) = \tau(b, \chi),$$

whence $\tau(b, \chi) = 0$.

(iv) Since $(m, n) = 1$, the Chinese remainder theorem implies that any a modulo mn is of the form $a = a'n + a''m$ with a' modulo m and a'' modulo n. Whence

$$(\chi\psi)(a) = \chi(a'n)\psi(a''m).$$

Using this fact, a short computation shows

$$\sum_{a \pmod{mn}} (\chi\psi)(a)e^{\frac{2\pi iab}{mn}} = \chi(n)\psi(m) \cdot \left(\sum_{a' \pmod{m}} \chi(a')e^{\frac{2\pi iab}{m}} \right) \left(\sum_{a'' \pmod{n}} \psi(a'')e^{\frac{2\pi ia''b}{n}} \right),$$

which is equivalent to the claim.

(v) First consider the case when $\left(\frac{m}{q}, q\right) = 1$. In view of $\chi = \widetilde{\chi}\chi_{\frac{m}{q},0}$, we use (iv) to obtain

$$\tau(\chi) = \tau(\chi_{\frac{m}{q},0})\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

As $\tau(\chi_{\frac{m}{q},0}) = r\left(1, \frac{m}{q}\right)$, we use Proposition 3.3.1 to compute $\tau(\chi_{\frac{m}{q},0}) = \mu\left(\frac{m}{q}\right)$. Whence

$$\tau(\chi) = \mu\left(\frac{m}{q}\right)\widetilde{\chi}\left(\frac{m}{q}\right)\tau(\widetilde{\chi}).$$

Now suppose $\left(\frac{m}{q}, q\right) > 1$. In this case the right-hand side is zero because $\widetilde{\chi}\left(\frac{m}{q}\right) = 0$. So we must show $\tau(\chi) = 0$. Now there exists a prime p with $p \mid \frac{m}{q}$ and $p \mid q$. For any a modulo m write $a = a'\frac{m}{p} + a''$ with a' modulo p and a'' modulo $\frac{m}{p}$. Moreover, as $p \mid \frac{m}{q}$ we know $q \mid \frac{m}{p}$. These two facts and a short computation together show

$$\tau(\chi) = \left(\sum_{a' \pmod{p}} e^{\frac{2\pi ia'}{p}} \right) \left(\sum_{a'' \pmod{\frac{m}{p}}} \widetilde{\chi}(a'')e^{\frac{2\pi ia''}{m}} \right).$$

The first sum vanishes since it is the sum of all p-th roots of unity. This proves $\tau(\chi) = 0$. □

These properties help to reduce the evaluation of Ramanujan and Gauss sums. However, even evaluating Gauss sums for arbitrary primitive Dirichlet characters is a very difficult problem much of which is still open. Yet it is not difficult to determine the modulus of the Gauss sum when χ is primitive.

Theorem 3.3.3. *Let χ be a primitive Dirichlet character of conductor q. Then*

$$|\tau(\chi)| = \sqrt{q}.$$

Proof. If χ is the trivial Dirichlet character the claim is obvious since the Gauss sum is 1. So assume χ is nontrivial whence $q > 1$. Consider instead $|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)}$. Expanding the Gauss sum $\overline{\tau(\chi)}$ and invoking Proposition 3.3.2 (ii), a short computation shows

$$|\tau(\chi)|^2 = \sum_{a \pmod q} \tau(a, \chi) e^{-\frac{2\pi i a}{q}}.$$

Upon expanding the Ramanujan sum, another short computation gives

$$|\tau(\chi)|^2 = \sum_{a' \pmod q} \chi(a') \left(\sum_{a \pmod q} e^{\frac{2\pi i a(a'-1)}{q}} \right).$$

If $a' \equiv 1 \pmod q$ the inner sum is q and otherwise vanishes as it is the sum of all q-th roots of unity. It follows that the double sum is q whence $|\tau(\chi)|^2 = q$. This is equivalent to the claim. □

As an almost immediate corollary, we deduce a useful expression for primitive Dirichlet characters as exponential sums.

Corollary 3.3.4. *Let χ be a primitive Dirichlet character of conductor q. Then for any integer b, we have*

$$\tau(b, \chi) = \overline{\chi}(b)\tau(\chi).$$

In particular,

$$\chi(b) = \frac{1}{\tau(\overline{\chi})} \sum_{a \pmod q} \overline{\chi}(a) e^{\frac{2\pi i a b}{q}}.$$

Proof. For the first statement, the identity is obvious if χ is the trivial character as the Ramanujan sum is 1. So assume χ is nontrivial. If $(b, q) = 1$ then this is exactly Proposition 3.3.2 (ii). If $(b, q) > 1$ then the identity follows from Proposition 3.3.2 (iii) and that $\overline{\chi}(b) = 0$. This proves the first statement in full. For the second statement, observe that $\tau(\chi) \neq 0$ by Theorem 3.3.3. The second identity follows upon replacing χ with $\overline{\chi}$, dividing by $\tau(\chi)$, and expanding the Ramanujan sum. □

For a Dirichlet character χ modulo m, we define the **epsilon factor** ε_χ by

$$\varepsilon_\chi = \frac{\tau(\chi)}{\sqrt{m}}.$$

When χ is primitive, the epsilon factor lies on the unit circle by Theorem 3.3.3. The question of the evaluation of Gauss sums, and hence Ramanujan sums, boils down to determining what value the epsilon factor is. This is the real difficultly in evaluating Gauss sums. However, when χ is primitive there is a simple relationship between the epsilon factors ε_χ and $\varepsilon_{\overline{\chi}}$:

Proposition 3.3.5. *Let χ be a primitive Dirichlet character of conductor q. Then*

$$\varepsilon_\chi \varepsilon_{\overline{\chi}} = \chi(-1).$$

Proof. If χ is trivial this is obvious since both epsilon factors are 1. So assume χ is nontrivial. On the one hand, $\varepsilon_{\overline{\chi}}$ lies on the unit circle so that

$$\varepsilon_{\overline{\chi}}^{-1} = \frac{\overline{\tau(\chi)}}{\sqrt{q}}.$$

On the other hand, Proposition 3.3.2 (i) implies

$$\varepsilon_\chi = \chi(-1)\frac{\overline{\tau(\chi)}}{\sqrt{q}}.$$

Combining these identities gives the result. □

3.4 Quadratic Gauss Sums

Our primary aim will be to evaluate the epsilon factor of the Gauss sum for quadratic Dirichlet characters defined by Jacobi symbols. To accomplish this we will study and auxiliary exponential sum. For integers b and m with m positive, the **quadratic Gauss sum** $g(b, m)$ is defined by

$$g(b, m) = \sum_{a \pmod m} e^{\frac{2\pi i a^2 b}{m}}.$$

When $b \mid m$ the summands are all 1 and the quadratic Gauss sum evaluates to

$$g(b, m) = m.$$

If $b = 1$ we write $g(m) = g(1, m)$. It turns out that for square-free m the Ramanujan sum attached to the quadratic Dirichlet character modulo m given by the Jacobi symbol is precisely the quadratic Gauss sum. This takes some work to prove. The first step is to reduce to the case when $(b, m) = 1$.

Proposition 3.4.1. *Let b and m be integers with m positive. Then*

$$g(b, m) = (b, m) g\left(\frac{b}{(b, m)}, \frac{m}{(b, m)}\right).$$

Proof. Any a modulo m is of the form $a = a'\frac{m}{(b,m)} + a''$ with a' modulo (b,m) and a'' modulo $\frac{m}{(b,m)}$. A short computation shows

$$\sum_{a \pmod m} e^{\frac{2\pi i a^2 b}{m}} = (b,m) \sum_{a'' \pmod{\frac{m}{(b,m)}}} e^{\frac{2\pi i (a'')^2 \frac{b}{(b,m)}}{\frac{m}{(b,m)}}}.$$

The remaining sum is exactly $g\left(\frac{b}{(b,m)}, \frac{m}{(b,m)}\right)$ and the desired identity follows. □

The second step is to deduce an equivalent formulation of the Ramanujan sum associated to quadratic Dirichlet characters given by Jacobi symbols. This will imply equivalence between the aforementioned exponential sums when the modulus is an odd prime.

Proposition 3.4.2. *Let b and m be integers with m positive, odd, and such that $(b,m) = 1$. Let χ_m be the quadratic Dirichlet character modulo m given by the Jacobi symbol. Then*

$$\tau(b, \chi_m) = \sum_{a \pmod m} \left(1 + \left(\frac{a}{m}\right)\right) e^{\frac{2\pi i a b}{m}}.$$

When $m = p$ is prime,

$$\tau(b, \chi_p) = g(b,p).$$

Proof. The first statement is obvious when $m = 1$ since the Ramanujan sum is 1. So assume $m > 1$. Now write the sum as

$$\sum_{a \pmod m} e^{\frac{2\pi i a b}{m}} + \sum_{a \pmod m} \left(\frac{a}{m}\right) e^{\frac{2\pi i a b}{m}}.$$

The first sum vanishes as it is the sum of all m-th roots of unity. This proves the first identity. Now let $m = p$ be an odd prime. Then

$$1 + \left(\frac{a}{p}\right) = \begin{cases} 2 & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } a \text{ is not quadratic residue modulo } p, \\ 1 & \text{if } p \mid a. \end{cases}$$

Moreover, when a is a quadratic residue modulo p there exists an a' modulo p with $a \equiv (a')^2 \pmod p$. As there are $\frac{p-1}{2}$ such residues, the first statement implies

$$\tau(b, \chi_p) = 1 + \sum_{\substack{a' \pmod p \\ a' \nmid 0}} e^{\frac{2\pi i (a')^2 b}{p}}.$$

This is exactly $g(b,p)$ which proves the second statement. □

The third step is to generalize the second statement in Proposition 3.4.2 for square-free m. To accomplish this we will need to develop some properties of quadratic Gauss sums.

Proposition 3.4.3. *Let b, m, and n be integers with m and n positive and let p be an odd prime Then the following properties hold:*

(i) If $(b,p)=1$ then $g(b,p^r)=pg(b,p^{r-2})$ provided $r\geq 2$.

(ii) If $(m,n)=1$ and $(b,mn)=1$ then $g(b,mn)=g(bn,m)g(bm,n)$.

(iii) If m is odd and $(b,m)=1$ then $g(b,m)=\left(\frac{b}{m}\right)g(m)$ where $\left(\frac{b}{m}\right)$ is the Jacobi symbol.

Proof. We will prove the properties separately.

(i) Every a modulo p satisfies $(a,p)=1$ or is a multiple of p. Whence

$$g(b,p^r)=\sum_{\substack{a \pmod{p^r}\\(a,p)=1}} e^{\frac{2\pi i a^2 b}{p^r}}+\sum_{a \pmod{p^{r-1}}} e^{\frac{2\pi i a^2 b}{p^{r-2}}},$$

since every a modulo p satisfies $(a,p)=1$ or not. Every a modulo p^{r-1} is of the form $a=a'p^{r-2}+a''$ with a' modulo p and a'' modulo p^{r-2}. A short computation shows

$$\sum_{a \pmod{p^{r-1}}} e^{\frac{2\pi i a^2 b}{p^{r-2}}}=p\sum_{a'' \pmod{p}} e^{\frac{2\pi i (a'')^2 b}{p^{r-2}}}.$$

The remaining sum is exactly $g(b,p^{r-2})$. So it suffices to show that the first sum vanishes. This sum is exactly $r(b,p^r)$ and Proposition 3.3.1 implies $r(b,p^r)=\mu(p^r)$ which is zero as $r\geq 2$.

(ii) Since $(m,n)=1$, the Chinese remainder theorem implies that any a modulo mn is of the form $a=a'n+a''m$ with a' modulo m and a'' modulo n. Whence

$$\left(\sum_{a' \pmod{m}} e^{\frac{2\pi i (a')^2 bn}{m}}\right)\left(\sum_{a'' \pmod{n}} e^{\frac{2\pi i (a'')^2 bm}{n}}\right)=\sum_{a \pmod{mn}} e^{\frac{2\pi i a^2 b}{mn}}.$$

This is equivalent to the claim.

(iii) The claim is obvious if $m=1$ because the quadratic Gauss sum is 1. So assume $m>1$. By multiplicativity of the Jacobi symbol and (ii), it suffices to prove the claim when $m=p^r$ is an odd prime power. The case when $r=1$ follows from Proposition 3.4.2, Proposition 3.3.2 (ii), and that quadratic Dirichlet characters are their own conjugates. The case when $r\geq 2$ follows by induction using (i). □

At last we can prove our Ramanujan and quadratic Gauss sums agree.

Theorem 3.4.4. *Suppose m is a square-free positive odd integer and let χ_m be the quadratic Dirichlet character modulo m given by the Jacobi symbol. Then for any integer b with $(b,m)=1$, we have*

$$\tau(b,\chi_m)=g(b,m).$$

Proof. The claim is obvious if $m = 1$ because the Ramanujan and Gauss sums are both 1. So suppose $m > 1$. It suffices to assume $b = 1$ by Proposition 3.3.2 (ii), Proposition 3.4.3 (iii), and that quadratic Dirichlet characters are their own conjugates. Let $m = p_1 p_2 \cdots p_k$ be the prime decomposition of m. Repeated application of Proposition 3.3.2 (iv) shows

$$\tau(\chi) = \left(\prod_{i<j} \chi_{p_j}(p_i) \chi_{p_i}(p_j) \right) \left(\prod_i \tau(\chi_{p_i}) \right).$$

By Proposition 3.4.2, we may write

$$\left(\prod_{i<j} \chi_{p_j}(p_i) \chi_{p_i}(p_j) \right) \left(\prod_i \tau(\chi_{p_i}) \right) = \left(\prod_{i<j} \left(\frac{p_i}{p_j} \right) \left(\frac{p_j}{p_i} \right) \right) \left(\prod_i g(p_i) \right).$$

Repeated application of Proposition 3.4.3 (ii) gives

$$\left(\prod_{i<j} \left(\frac{p_i}{p_j} \right) \left(\frac{p_j}{p_i} \right) \right) \left(\prod_i g(p_i) \right) = g(m).$$

This completes the proof. □

The properties in Proposition 3.4.3 help to reduce the evaluation of quadratic Gauss sums. Thankfully, it is possible to completely evaluate quadratic Gauss sums when $b = 1$ and therefore even some Ramanujan sums. As with the Gauss sum, we first deduce a fact about the modulus.

Theorem 3.4.5. *Let m be a positive odd integer. Then*

$$|g(m)| = \sqrt{m}.$$

Proof. The claim is obvious if $m = 1$ because the quadratic Gauss sum is 1. So assume $m > 1$. By Proposition 3.4.3 (ii) and (iii), it suffices to prove the claim when $m = p^r$ is an odd prime power. The case when $r = 1$ follows from Theorems 3.3.3 and 3.4.4. The case when $r \geq 2$ is proved by induction and Proposition 3.4.3 (i). □

For any integer m, we define the **epsilon factor** ε_m by

$$\varepsilon_m = \frac{g(m)}{\sqrt{m}}.$$

Theorem 3.4.5 says that this value lies on the unit circle when m is odd. This evaluation of these epsilon factors was completely resolved by Gauss in 1808. Modern proofs use analytic techniques by expressing $g(m)$ in a form where Poisson summation can be applied.

Theorem 3.4.6. *Let $m \geq 1$. Then*

$$\varepsilon_m = \begin{cases} (1+i) & \text{if } m \equiv 0 \pmod 4, \\ 1 & \text{if } m \equiv 1 \pmod 4, \\ 0 & \text{if } m \equiv 2 \pmod 4, \\ i & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Proof. The aim is to express $g(m)$ as a periodic sum over $\mathbb{Z}$ whose summands are compactly supported functions of bounded variation. For then we can apply Poisson summation to evaluate the sum in an alternative manner. To this end, consider the function

$$f(x) = \begin{cases} e^{\frac{2\pi i x^2}{m}} & \text{if } x \in [0, m], \\ 0 & \text{if } x \notin [0, m]. \end{cases}$$

Then $f(x)$ is of bounded variation with compact support and has jump discontinuities only at $x = 0$ and $x = m$. Therefore Poisson summation applies where $f(n)$ is understood to be the average of the left-hand and right-hand limits at points of discontinuity and the sums are ordered symmetrically with respect to the size of the index. On the one hand, this means

$$\sum_{n \in \mathbb{Z}} f(n) = g(m).$$

On the other hand, Poisson summation gives

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{t \in \mathbb{Z}} \sqrt{m} e^{-\frac{2\pi i t^2 m}{4}} \int_{\frac{t\sqrt{m}}{2}}^{\sqrt{m} + \frac{t\sqrt{m}}{2}} e^{2\pi i x^2} \, dx.$$

As $t \equiv 0, 1 \pmod 4$ according to if t is even or odd, the subsums according to this parity are

$$\sqrt{m} \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx \quad \text{and} \quad \sqrt{m} e^{-\frac{2\pi i m}{4}} \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx,$$

respectively. As the sum is ordered with respect to this parity, we have

$$\sum_{n \in \mathbb{Z}} f(n) = \sqrt{m} \left(1 + e^{-\frac{2\pi i m}{4}}\right) \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx.$$

Equating our two expressions gives

$$g(m) = \sqrt{m} \left(1 + e^{-\frac{2\pi i m}{4}}\right) \int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx.$$

To compute the remaining integral we take $m = 1$. As the Gauss sum is 1 and $e^{-\frac{2\pi i}{4}} = -i$, we find that

$$\int_{-\infty}^{\infty} e^{2\pi i x^2} \, dx = \frac{1}{1-i}.$$

Therefore

$$\varepsilon_m = \frac{1 + e^{-\frac{2\pi i m}{4}}}{1 - i} = \begin{cases} (1+i) & \text{if } m \equiv 0 \pmod 4, \\ 1 & \text{if } m \equiv 1 \pmod 4, \\ 0 & \text{if } m \equiv 2 \pmod 4, \\ i & \text{if } m \equiv 3 \pmod 4, \end{cases}$$

as desired. □

As an immediate corollary, we can evaluate the epsilon factor ε_{χ_p} for the quadratic Dirichlet character χ_p modulo p given by the Jacobi symbol when p is an odd prime.

Corollary 3.4.7. *Let p be an odd prime and χ_p be the quadratic Dirichlet character modulo p given by the Jacobi symbol. Then*

$$\varepsilon_{\chi_p} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. The claim follows immediately from Theorem 3.4.6 and Proposition 3.4.2. □

Part II

Algebraic Number Theory

Chapter 4

Algebraic Integers

Throughout, all rings will be understood to be commutative and with unity.

4.1 Integrality

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

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

for some positive integer n and $\alpha_i \in A$. We say that B is *integral* over A if every element of B is integral over A. As we may expect, the set of integral elements form a ring.

Proposition 4.1.1. *Let B/A be a ring extension. Then $\beta_1, \ldots, \beta_n \in B$ 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. We will prove the forward implication by induction. First suppose $\beta \in B$ is integral over A. Then there exists a monic polynomial $f(x) \in A[x]$ of say degree n such that $f(\beta) = 0$. Let $g(x) \in A[x]$ and write

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

with $q(x), r(x) \in A[x]$ where the degree of $r(x)$ is strictly less than n. Then $g(\beta) = r(\beta)$. Letting

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

with $\alpha_i \in A$, it follows that

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

As $g(x)$ was arbitrary, we see that $1, \beta, \ldots, \beta^{n-1}$ generate $A[\beta]$ as an A-module. Now assume by induction $R = A[\beta_1, \ldots, \beta_{n-1}]$ 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

A-module. 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 and let $\omega_1, \ldots, \omega_r$ be generators. Then for any $\beta \in A[\beta_1, \ldots, \beta_n]$, we have

$$\beta\omega_i = \sum_j \alpha_{i,j}\omega_j,$$

with $\alpha_{i,j} \in A$. These r equations are equivalent to the identity

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

The determinant of the matrix on the left-hand side must be zero. This shows that β is the root of the characteristic polynomial $\det(xI - (\alpha_{i,j}))$ which is a monic polynomial with coefficients in A. Hence β is integral over A. As β was arbitrary, 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. □

Integrality is also transitive.

Proposition 4.1.2. *Let $C/B/A$ be a ring extension. 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 positive integer n and $\beta_i \in B$. Set $R = A[\beta_0, \ldots, \beta_{n-1}]$. Then $R[\gamma]$ is a finitely generated R-module. As B is integral over A, Proposition 4.1.1 implies that $R[\gamma]$ is also a finitely generated A-module whence γ is integral over A. As γ was arbitrary, this proves C is integral over A. □

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

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

Then $\overline{A}$ is a subring of B by Proposition 4.1.1. 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 4.1.2 implies that $\overline{A}$ is automatically integrally closed in B. It will often be more fruitful to work with the integral closure rather than a generic ring.

There is a particular situation of integrally closed rings which is deserving of additional interest. Suppose A is an integral domain with field of fractions K. 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 4.1.3. *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. Let $\kappa \in K$ be such that

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

for some positive integer n and $\alpha_i \in A$. 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

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

As β divides the right-hand side it divides the left-hand side as well. But then β is a unit in A since $(\alpha, \beta) = 1$. This means $\kappa \in A$ whence A is integrally closed. This proves the first statement. The second statement is immediate since every principal ideal domain is a unique factorization domain. □

We will often consider the more refined setting where A is integrally closed 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, L is the field of fractions of B and the elements of L which are integral over A have a simple description.

Proposition 4.1.4. *Let A be integrally closed 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 and B is integrally closed. 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

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

for some positive integer n and $\alpha, \alpha_i \in A$ with α nonzero. 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 $\alpha'_i = \alpha_i\alpha^{n-1-i}$. Whence $\alpha\lambda$ is integral over A and thus $\alpha\lambda \in B$. Then $\alpha\lambda = \beta$ for some $\beta \in B$ which is equivalent to $\lambda = \frac{\beta}{\alpha}$. It follows at once that L is the field of fractions of B. As B is a subring of a field it is an integral domain. It is also integrally closed since B is the integral closure of A in L. Whence B is integrally closed. It remains to prove the last statement. For the forward implication, suppose λ is integral over A. Then λ is a root of a monic polynomial $f(x) \in A[x]$. As $m_\lambda(x)$ divides $f(x)$ in $A[x]$, all of the roots of $m_\lambda(x)$ are integral over A too. By Vieta's formulas, the coefficients of $m_\lambda(x)$ integral over A as well whence $m_\lambda(x) \in A[x]$. For the reverse implication, if the minimal polynomial $m_\lambda(x)$ of λ over K has coefficients in A then λ is automatically integral over A. □

Number fields are a particular instance of the aforementioned setting. 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 whence 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. In the cases of small degrees we will often use the latin derived names **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**. Note that α is an algebraic integer if and only if it is the root of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Remark 4.1.5. By Lemma 4.1.3, $\mathbb{Z}$ is integrally closed and therefore the ring of integers of $\mathbb{Q}$ is exactly $\mathbb{Z}$.

It follows from Proposition 4.1.4 that every $\kappa \in K$ is of the form

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

for some algebraic integer α and nonzero integer a. In particular, K is the field of fractions of $\mathcal{O}_K$ and $\mathcal{O}_K$ is integrally closed. Moreover, κ is an algebraic integer if and only if the minimal polynomial $m_\kappa(x)$ of κ over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

4.2 Traces and Norms

Let B/A be a ring extension such that B is a free A-module of rank n. Recall that by fixing a basis for B/A, there is an isomorphism

$$\mathrm{End}_A(B) \cong \mathrm{Mat}_n(A)$$

This permits us to view A-linear operators from B to itself as $n \times n$ matrices with coefficients in A. To any $\beta \in B$, we associate the A-linear operator T_β defined by

$$T_\beta : B \to B \qquad x \mapsto \beta x.$$

This is simply multiplication by β. The trace and determinant of T_β are deserving of special interest. For instance, let $f_\beta(x)$ denote the characteristic polynomial of T_β so that

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

with $\alpha_i \in A$. Then the trace and determinant have the alternative representations

$$\mathrm{trace}(T_\beta) = \alpha_{n-1} \quad \text{and} \quad \det(T_\beta) = \alpha_0,$$

We define the **trace** and **norm** of B over A, denoted $\mathrm{Tr}_{B/A}$ and $\mathrm{N}_{B/A}$, by

$$\mathrm{Tr}_{B/A} : B \to A \qquad \beta \mapsto \mathrm{trace}(T_\beta) \quad \text{and} \quad \mathrm{N}_{B/A} : B \to A \qquad \beta \mapsto \det(T_\beta)$$

Our primary aim will be to develop a sufficient understanding of the trace and norm. The trace is additive while the norm is multiplicative because they correspond to the trace and determinant of matrices. Whence

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

for all $\beta, \beta' \in B$. In fact, we have the additional relations

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

for all $\alpha \in A$ by scalar multiplication of matrices. The trace and norm also behave well with respect to direct sums. If $B = B_1 \oplus B_2$ and we have a decomposition $\beta = \beta_1 + \beta_2$ with $\beta_1 \in B_1$ and $\beta_2 \in B_2$ then

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

because the corresponding matrix for β is block diagonal.

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. For any $\lambda \in L$, the **trace** and **norm** of λ are $\mathrm{Tr}_{L/K}(\lambda)$ and $\mathrm{N}_{L/K}(\lambda)$. In this case, $\mathrm{N}_{L/K}(\lambda) = 0$ if and only if $\lambda = 0$ because otherwise T_λ has inverse $T_{\lambda^{-1}}$ and hence a 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 as these fields 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 $\overline{K}$. That is, there are n elements of $\mathrm{Hom}_K(L, \overline{K})$. These K-embeddings are constructed by letting θ be a primitive element for L/K and sending θ to one of its conjugate roots in the minimal polynomial $m_\theta(x)$ of θ over K. These K-embeddings are deeply connected to the trace and norm.

Proposition 4.2.1. *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

$$\mathrm{Tr}_{L/K}(\lambda) = \sum_i \lambda_i \quad \textit{and} \quad \mathrm{N}_{L/K}(\lambda) = \prod_i \lambda_i.$$

Proof. Let m and d be the degrees of $K(\lambda)/K$ and $L/K(\lambda)$ respectively. Write

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

with $\kappa_i \in K$. We claim

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

Indeed, recall that $1, \lambda, \ldots, \lambda^{m-1}$ 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. The matrix of T_λ with respect to this basis 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 matrix is the companion matrix to $m_\lambda(x)$ and hence the characteristic polynomial is $m_\lambda(x)$ as well. Our claim follows since the characteristic polynomial of a block diagonal matrix is the product of the characteristic polynomials of the blocks. 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 where two K-embeddings are equivalent if and only if they take the same value at λ. If τ runs over the elements of $\mathrm{Hom}_K(K(\lambda), \overline{K})$, then this a complete set of representatives. As

$$m_\lambda(x) = \prod_\tau (x - \tau(\lambda))$$

it follows that

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

The formulas for the trace and norm follow from Vieta's formulas applied to this product for $f_\lambda(x)$. Now suppose L/K is Galois. Then $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}(L/K)$. Therefore the conjugates of λ are exactly the images of λ under these K-embeddings and the last statement follows. □

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

Proposition 4.2.2. *Let A be integrally closed 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 4.1.4, the minimal polynomial $m_\beta(x)$ of β over K has coefficients in A. By Proposition 4.2.1, the characteristic polynomial $f_\beta(x)$ is a power of $m_\beta(x)$ and hence $f_\beta(x)$ has coefficients in A too. Whence trace and norm of β are in A as they are coefficients of $f_\beta(x)$ up to sign. □

In this setting it is also easy to classify the units of B in terms of the units of A.

Proposition 4.2.3. *Let A be integrally closed 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. For the forward implication, if $\beta \in B$ is a unit then $\frac{1}{\beta} \in B$. Whence

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

By Proposition 4.2.2, both of the norms on the left-hand side are in A. This proves $\mathrm{N}_{L/K}(\beta) \in A$ is a unit. For the reverse implication, we know by assumption that β is nonzero. Also, Proposition 4.1.4 implies that the minimal polynomial $m_\beta(x)$ of β over K has coefficients in A. The constant term is a unit since it is $\mathrm{N}_{L/K}(\beta)$ up to sign. 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 $\alpha, \alpha_i \in A$ where α is a unit. Dividing this relation by $\alpha\beta^m$, we find that $\frac{1}{\beta}$ is a root of the monic polynomial

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

whose coefficients are in A. Hence $\frac{1}{\beta} \in B$ and thus β is a unit. □

Having introduced traces and norms, we turn to discussing discriminants of free modules. Let B/A be a ring extension such that B is a free A-module of rank n. If $\beta_1, \ldots, \beta_n$ is a basis for B/A, 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 **discriminant** $d_{B/A}(\beta_1, \ldots, \beta_n)$ of $\beta_1, \ldots, \beta_n$ is defined to be the determinant of the trace matrix. That is,

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

In particular, the discriminant $d_{B/A}(\beta_1, \ldots, \beta_n)$ is an element of A since the entries of the trace matrix are. 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 for B/A, we have

$$\beta_i' = \sum_j \alpha_{i,j}\beta_j,$$

with $\alpha_{i,j} \in A$. Then $(\alpha_{i,j})$ is the base change matrix from $\beta_1, \ldots, \beta_n$ to $\beta'_1, \ldots, \beta'_n$ and so has nonzero determinant. Thus $\det((\alpha_{i,j})) \in A^*$. Moreover,

$$\mathrm{Tr}_{B/A}(\beta'_1, \ldots, \beta'_n) = (\alpha_{i,j}) \, \mathrm{Tr}_{B/A}(\beta_1, \ldots, \beta_n)(\alpha_{i,j})^t,$$

which, upon taking the determinant, shows

$$d_{B/A}(\beta'_1, \ldots, \beta'_n) = \det((\alpha_{i,j}))^2 d_{B/A}(\beta_1, \ldots, \beta_n).$$

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

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

In particular, $d_A(B) = 0$ is independent of the choice of representative. The discriminant is also multiplicative with respect to direct sums.

Proposition 4.2.4. *Let B/A be a ring extension 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 with bases $\beta_{1,1}, \ldots, \beta_{n_1,1}$ and $\beta_{1,2}, \ldots, \beta_{n_2,2}$ over A respectively. Then $\beta_{1,1}, \ldots, \beta_{n_1,1}, \beta_{1,2}, \ldots, \beta_{n_2,2}$ is a basis of B over A and

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

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

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

Recall that

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

for any $\beta_1 \in B_1$ and $\beta_2 \in B_2$. Whence the block diagonal matrix above is

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

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

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 will require some work. First, we define the **trace form** of L/K to be the map

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

In other words, this is just the trace of L/K considered as a pairing. Clearly this is a symmetric bilinear form. In fact, the trace form is also nondegenerate as Proposition 4.2.1 implies

$$\mathrm{Tr}_{L/K}(1) = n,$$

and we can pair any $\lambda \in L$ with its inverse. Using the trace form, we can show that the discriminant of any basis for L/K is nonzero.

Proposition 4.2.5. *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 trace matrix $\mathrm{Tr}_{L/K}(\lambda_1, \ldots, \lambda_n)$ is not invertible. Therefore

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

for some $\kappa_i \in K$ not all of which are zero. Then the element

$$\lambda = \sum_j \kappa_j \lambda_j.$$

is nonzero. Moreover, the previous identity is equivalent to the fact that $\mathrm{Tr}_{L/K}(\lambda\lambda_i) = 0$. As $\lambda_1, \ldots, \lambda_n$ is a basis for L/K, it follows that the trace form is degenerate which is a contradiction. Hence $d_{L/K}(\lambda_1, \ldots, \lambda_n) \neq 0$. □

In addition to the discriminant $d_{L/K}(\lambda_1, \ldots, \lambda_n)$ being nonzero, we can also write it in a more useful 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 $\mathrm{Hom}_K(L, \overline{K})$. The discriminant turns out to be the square of the determinant of the embedding matrix.

Proposition 4.2.6. *Let L/K be a degree n separable extension. Then for any basis $\lambda_1, \ldots, \lambda_n$ of L/K, we have*

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

Proof. Recall that the ij-entry of $M(\lambda_1, \ldots, \lambda_n)^t M(\lambda_1, \ldots, \lambda_n)$ is the dot product of the i-th and j-th columns of $M(\lambda_1, \ldots, \lambda_n)$. Then a straightforward computation shows

$$\det(M(\lambda_1, \ldots, \lambda_n)^t M(\lambda_1, \ldots, \lambda_n)) = \det\left(\left(\sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(\lambda_i \lambda_j) \right)_{i,j} \right).$$

By Proposition 4.2.1, this identity is equivalent to the claim. □

In general, it is difficult to compute the discriminant of a basis for L/K. However, if the basis is of the form $1, \lambda, \ldots, \lambda^{n-1}$ (take $\lambda = \theta$ for a primitive element θ of L/K), then the discriminant of this basis can be easily computed. Indeed, the embedding matrix becomes

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

which is a Vandermonde matrix. By Proposition 4.2.6, we have

$$d_{L/K}(1, \lambda, \ldots, \lambda^{n-1}) = \prod_{i \leq j} (\sigma_i(\lambda) - \sigma_j(\lambda))^2, \tag{4.1}$$

which is the square of the Vandermonde determinant of $M(1, \lambda, \ldots, \lambda^{n-1})$.

Let us now consider the situation when A is integrally closed with field of fractions K, L/K be a degree n separable extension, and B is the integral closure of A in L. The discriminant relates containment of B relative to A when the underlying basis is contained in B.

Lemma 4.2.7. *Let A be integrally closed with field of fractions K, L/K be a degree n separable extension, and B be the integral closure of A in L. If $\lambda_1, \ldots, \lambda_n$ is a basis for L/K that is contained in B then*

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

Proof. Let $\beta \in B$ and write $\beta = \kappa_1 \lambda_1 + \cdots + \kappa_n \lambda_n$ for some $\kappa_i \in K$. Linearity of the trace implies

$$\sum_j \kappa_j \operatorname{Tr}_{L/K}(\lambda_i \lambda_j) = \operatorname{Tr}_{L/K}(\lambda_i \beta),$$

These n equations are equivalent to the identity

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

By Proposition 4.2.2, the trace matrix and the column vector on the right-hand side have entries in A. Cramer's rule then implies $d_{L/K}(\lambda_1, \ldots, \lambda_n)\kappa_i \in A$. As β was arbitrary, this means

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

In this situation, we say that $\beta_1, \ldots, \beta_n$ is an **integral basis** for B/A if

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

Equivalently, B is a free A-module of rank n. An integral basis is necessarily a basis for L/K by Proposition 4.1.4. However, an integral basis need not always exist. For

if $\lambda_1, \ldots, \lambda_n$ is a basis of L/K, Proposition 4.1.4 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 over A. Nevertheless, if A is a principal ideal domain then we can ensure the existence of an integral basis.

Theorem 4.2.8. *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/A admits an integral basis. Moreover, every finitely generated nonzero B-submodule of L is a free A-module of rank n.*

Proof. Let $\lambda_1, \ldots, \lambda_n$ be a basis for L/K. From Lemma 4.1.3 we see that A is integrally closed. Then by Proposition 4.1.4, we may multiply by a nonzero element of A, if necessary, to ensure that this basis belongs to B. Then Lemma 4.2.7 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/A must also be a basis for L/K by Proposition 4.1.4. 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 4.1.4 again we may multiply by a nonzero element of A, if necessary, to ensure that these generators belong to B. 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 proves the second statement. □

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 4.2.9. *Let A be integrally closed with field of fractions K, L_1/K and L_2/K be degree n_1 and n_2 separable extensions, 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/A and B_2/A admit integral bases $\beta_{1,1}, \ldots, \beta_{n_1,1}$ and $\beta_{1,2}, \ldots, \beta_{n_2,2}$ 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/A and

$$B = B_1 B_2.$$

In particular,

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

Proof. We will start by proving $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is an integral basis for B/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/K. Therefore any $\beta \in B$ is of the form

$$\beta = \sum_{i,j} \kappa_{i,j}\beta_{i,1}\beta_{j,2},$$

for some $\kappa_{i,j} \in K$. We need to show that $\kappa_{i,j} \in A$. To this end, let

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

so that

$$\beta = \sum_{i} \alpha_{i,2}\beta_{i,1} \quad \text{and} \quad \beta = \sum_{j} \alpha_{j,1}\beta_{j,2}.$$

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

$$\sum_{i} \sigma_{i,1}(\beta_{i,1})\alpha_{i,2} = \sigma_{i,1}(\beta) \quad \text{and} \quad \sum_{j} \sigma_{j,2}(\beta_{j,2})\alpha_{j,1} = \sigma_{j,2}(\beta),$$

are equivalent to the identities

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

and

$$M(\beta_{1,2}, \ldots, \beta_{n_2,2}) \begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{n_2,1} \end{pmatrix} = \begin{pmatrix} \sigma_{1,2}(\beta) \\ \vdots \\ \sigma_{n_2,2}(\beta) \end{pmatrix},$$

respectively. The embedding matrices and column vectors on the right-hand sides all have entries in B. Cramer's rule together with Proposition 4.2.6 imply that $d_{L_1/K}(\beta_{1,1}, \ldots, \beta_{n_1,1})\alpha_{i,2} \in B$ and $d_{L_2/K}(\beta_{1,2}, \ldots, \beta_{n_2,2})\alpha_{j,1} \in B$. As $B_1 = L_1 \cap B$ and $B_2 = L_2 \cap B$, we have $\alpha_{i,2} \in B_2$ and $\alpha_{j,1} \in B_1$. Expanding $\alpha_{i,2}$ and $\alpha_{j,1}$ show 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 $k_{i,j} \in A$. This proves $\beta_{1,1}\beta_{1,2}, \ldots, \beta_{n_1,1}\beta_{n_2,2}$ is an integral basis for B/A. The fact that

$$B = B_1 B_2,$$

follows at once. It remains to prove the discriminant formula which will be achieved by decomposing the embedding matrix into blocks. Recall that $\sigma_{1,1}\sigma_{1,2}, \ldots, \sigma_{n_1,1}\sigma_{n_2,2}$ 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 left-hand side 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 this Kronecker product can be expressed as $(I \otimes M(\beta_{1,2}, \ldots, \beta_{n_2,2}))P$ 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 4.2.6 shows

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

This proves the discriminant formula. □

It is generally a difficult problem to write down an integral basis explicitly. However, there is one instance in which this is possible. We say that B/A is **monogenic** 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. The discriminant of this basis is then given by Equation (4.1).

Regardless of if B/A is monogenic or not, if an integral basis exists then the traces $\mathrm{Tr}_{L/K}$ and $\mathrm{Tr}_{B/A}$ and norms $\mathrm{N}_{L/K}$ and $\mathrm{N}_{B/A}$ agree.

Proposition 4.2.10. *Let A be integrally closed 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 $\beta_1, \ldots, \beta_n$ be an integral basis for B/A. Then $\beta_1, \ldots, \beta_n$ 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. Whence

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

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 **trace** and **norm** of K. Moreover, for any $\kappa \in K$ we call $\mathrm{Tr}_K(\kappa)$ and $\mathrm{N}_K(\kappa)$ the **trace** and **norm** of κ. Observe from Propositions 4.2.2 and 4.2.3 that the trace and norm of algebraic integers are themselves integers and $\kappa \in \mathcal{O}_K$ is a unit if and only if $\mathrm{N}_K(\kappa) = \pm 1$. We also call the nondegenerate symmetric bilinear form

$$\mathrm{Tr}_{K/\mathbb{Q}} : K \times K \to \mathbb{Q} \qquad (\kappa, \lambda) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\kappa\lambda),$$

the **trace form** of K. Moreover, since $\mathbb{Z}$ is a principal ideal domain Theorem 4.2.8 implies that $\mathcal{O}_K/\mathbb{Z}$ admits an integral basis. Whence $\mathcal{O}_K$ is a free abelian group of rank n. Accordingly, we say that $\alpha_1, \ldots, \alpha_n$ is an **integral basis** for K if it is an integral basis for $\mathcal{O}_K/\mathbb{Z}$. Accordingly, we define the **discriminant** Δ_K of K to be the discriminant of $\mathcal{O}_K/\mathbb{Z}$. As $(\mathbb{Z}^*)^2 = \{1\}$, Δ_K is an integer and satisfies

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

for any integral basis $\alpha_1, \ldots, \alpha_n$ for K. Moreover, Δ_K is nonzero since the trace form is nondegenerate and may very well be negative. In light of Proposition 4.2.6, we also have

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

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

4.3 Dedekind Domains

Let $\mathcal{O}$ be an integral domain with field of fractions 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 $\mathcal{O}$. If $\mathfrak{p}$ is principal with $\mathfrak{p} = \alpha\mathcal{O}$ for some nonzero $\alpha \in K$ we will also refer to α as the prime instead of $\mathfrak{p}$. In any case, an integral ideal is just a $\mathcal{O}$-submodule of $\mathcal{O}$. More generally, we say $\mathfrak{f}$ is a **fractional ideal** of $\mathcal{O}$ if it is $\mathcal{O}$-submodule of K such that there is a nonzero $\delta \in \mathcal{O}$ with $\delta\mathfrak{f} \in \mathcal{O}$. This simply means $\delta\mathfrak{f}$ is an integral ideal. Conversely, if $\mathfrak{a}$ is an integral ideal and $\delta \in \mathcal{O}$ is nonzero then

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

is a fractional ideal. So every fractional ideal is of this form. The fractional ideal $\mathfrak{f}$ is said to be **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 by taking $\delta = 1$ and all principal integral ideals are principal fractional ideals.

We will need to consider a more restrictive setting in order to develop a useful theory of integral and fractional ideals. This will allow for integral ideals to factor uniquely into a product of primes and for the fractional ideals to form a group in which $\mathcal{O}$ will act as the identity. This will essentially permit us to treat integral ideas as we would integers. Accordingly, an integral domain $\mathcal{O}$ is said to be a **Dedekind domain** if the following properties are satisfied:

(i) $\mathcal{O}$ is integrally closed.

(ii) $\mathcal{O}$ is noetherian.

(iii) Every prime of $\mathcal{O}$ is maximal.

Observe that $\wr$ being noetherian forces every integral ideal $\mathfrak{a}$ to be a finitely generated $\mathcal{O}$-module. In fact, as 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 $\mathfrak{a}$, $\mathfrak{f}$ is a finitely generated $\mathcal{O}$-submodule of K.

Remark 4.3.1. As $\mathbb{Z}$ is a principal ideal domain which is integrally closed by Remark 4.1.5, $\mathbb{Z}$ is a Dedekind domain. The primes of $\mathbb{Z}$ are exactly the primes p.

In view of principal ideal domains being integrally closed by Lemma 4.1.3, they are Dedekind domains. In fact, Dedekind domains should be thought of as generalizations of principal ideal domains. As $\mathbb{Z}$ is a prototypical example of a principal ideal domain, a Dedekind domain $\mathcal{O}$ should be thought of as a generalization of $\mathbb{Z}$. In fact, we will show that being a principal ideal domain is equivalent to being a unique factorization domain for $\mathcal{O}$. So if $\mathcal{O}$ is not a principal ideal domain then unique factorization fails. However, it will be possible to remedy most of this as one of our primary aims is to prove that integral ideals factor uniquely into a product of primes. This clearly generalizes unique factorization in $\mathbb{Z}$ which will be enough. To this end, we first show containment in one direction for integral ideals.

Lemma 4.3.2. *Let $\mathcal{O}$ be a Dedekind domain. For every integral ideal $\mathfrak{a}$ of $\mathcal{O}$, there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of $\mathcal{O}$ 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 primes. It suffices to show $\mathcal{S}$ is empty. Assuming otherwise and ordering $\mathcal{S}$ by inclusion, there exists a maximal element $\mathfrak{a} \in \mathcal{S}$ as $\mathcal{O}$ is noetherian. Moreover $\mathfrak{a}$ cannot be prime. Then there exist $\alpha_1, \alpha_2 \in \mathcal{O}$ with $\alpha_1\alpha_2 \in \mathfrak{a}$ and such that $\alpha_1, \alpha_2 \notin \mathfrak{a}$. 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 $\mathfrak{a}$. Moreover, $\mathfrak{b}_1\mathfrak{b}_2 \subseteq \mathfrak{a}$ because

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

Maximality of $\mathfrak{a}$ implies that there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ such that

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

But then

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

which contradicts the fact that $\mathfrak{a} \in \mathcal{S}$. Hence $\mathcal{S}$ is empty. □

More work will be necessary obtain reverse containment. To this end, we being by constructing a fractional ideal associated to every prime which will turn out to be the inverse. Let $\mathfrak{p}$ be a prime. We define $\mathfrak{p}^{-1}$ by

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

Then $\mathfrak{p}^{-1}$ is a fractional ideal. Indeed, since $\mathfrak{p}$ is an integral ideal there exists a nonzero $\alpha \in \mathfrak{p}$. The definition of $\mathfrak{p}^{-1}$ implies $\alpha\mathfrak{p}^{-1} \subseteq \mathcal{O}$. 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.

Lemma 4.3.3. *Let $\mathcal{O}$ be a Dedekind domain and $\mathfrak{p}$ be a prime of $\mathcal{O}$. Then*

$$\mathcal{O} \subset \mathfrak{p}^{-1} \quad \textit{and} \quad \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}.$$

Proof. We will first prove the containment. As $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, it suffices to show $\mathfrak{p}^{-1} - \mathcal{O}$ is nonempty. To this end, let $\alpha \in \mathfrak{p}$ be nonzero. By Lemma 4.3.2 let k be the smallest positive integer such that there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ with

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

As $\alpha\mathcal{O} \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is prime, there must be some $\mathfrak{p}_i$ 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 in $\mathcal{O}$, we conclude $\mathfrak{p}_1 = \mathfrak{p}$. Minimality of k forces

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

Hence there exists $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_k$ with $\beta \notin \alpha\mathcal{O}$. We claim $\beta\alpha^{-1} \in \mathfrak{p}^{-1} - \mathcal{O}$. Since $\mathfrak{p}_1 = \mathfrak{p}$, what we have previously shown implies $\beta\mathfrak{p} \subseteq \alpha\mathcal{O}$ whence $\beta\alpha^{-1}\mathfrak{p} \in \mathcal{O}$ 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 $\beta\alpha^{-1} \in \mathfrak{p}^{-1} - \mathcal{O}$ as desired.

Now let us prove the identity. Observe that

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

Since $\mathfrak{p}$ is maximal, 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 $\omega_1, \ldots, \omega_r$ be generators of $\mathfrak{p}$ and let $\alpha \in \mathfrak{p}^{-1} - \mathcal{O}$. Then $\alpha\omega_i \in \mathfrak{p}^{-1}\mathfrak{p}$ whence $\alpha\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$ and $\alpha\mathfrak{p} \subseteq \mathfrak{p}$. But then

$$\alpha\omega_i = \sum_j \alpha_{i,j}\omega_j,$$

with $\alpha_{i,j} \in \mathcal{O}$. 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 $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. □

We can now show that every integral ideal factors uniquely into a product of primes.

Theorem 4.3.4. *Let $\mathcal{O}$ be a Dedekind domain. Then for every integral ideal $\mathfrak{a}$ of $\mathcal{O}$ there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of $\mathcal{O}$ 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, there exists a maximal element $\mathfrak{a} \in \mathcal{S}$ as $\mathcal{O}$ is noetherian. Necessarily $\mathfrak{a}$ is not prime. Since primes are maximal in $\mathcal{O}$, there is some prime $\mathfrak{p}_1$ for which $\mathfrak{a} \subset \mathfrak{p}_1$. Then Lemma 4.3.3 implies

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}_1^{-1} \subset \mathcal{O}.$$

In particular, $\mathfrak{a}\mathfrak{p}_1^{-1}$ is an integral ideal. 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

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

which is a contradiction. Therefore $\mathcal{S}$ is empty thus proving the existence of such a factorization.

Now we prove uniqueness. Suppose $\mathfrak{a}$ admits factorizations

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

for primes $\mathfrak{p}_i$ and $\mathfrak{q}_j$. 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

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

Repeating this process, we see that the factorizations are the same. This proves uniqueness of the factorization. □

As a near immediate corollary, fractional ideal admits analogous factorizations.

Corollary 4.3.5. *Let $\mathcal{O}$ be a Dedekind domain. Then for every fractional ideal $\mathfrak{f}$ of $\mathcal{O}$ there exist primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell$ of $\mathcal{O}$ such that $\mathfrak{f}$ factors as*

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

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

Proof. Write $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$. By Theorem 4.3.4, $\mathfrak{a}$ and $\delta\mathcal{O}$ admit unique factorizations

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

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

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

So for any fractional ideal $\mathfrak{f}$ there exist distinct prime $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{f}$ admits a factorization

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

for some nonzero integers e_i. This is called the **prime factorization** of $\mathfrak{f}$ with **prime factors** $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. In particular, the prime factorization of an integral ideal $\mathfrak{a}$ is of the form

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

for some positive integers e_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 $\mathfrak{a} \,||\, \mathfrak{b}$ 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 $\mathfrak{p}^e \,||\, \mathfrak{a}$ for some positive integer e 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 $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a} \cap \mathfrak{b}$. Lastly, we say that $\mathfrak{a}$ and $\mathfrak{b}$ are **relatively prime** if $(\mathfrak{a}, \mathfrak{b}) = \mathcal{O}$. In other words, $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal which is to say

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

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. As these integral ideals are comaximal, we also have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. In terms of the least common multiple, this means $[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a}\mathfrak{b}$.

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 4.3.4 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 4.3.6. *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 immediate as every principal ideal domain is a unique factorization domain. For the reverse implication, suppose $\mathcal{O}$ is a unique factorization domain. As every integral ideal factors into a product of primes by Theorem 4.3.4 and the product of principal integral ideals is principal, it suffices to show that primes are principal. Let $\mathfrak{p}$ be a prime. Then there exists nonzero $\alpha \in \mathfrak{p}$ and α is not a unit since $\mathfrak{p}$ a proper ideal. Since $\mathcal{O}$ is a unique factorization domain, let $\alpha = \varepsilon\rho_1^{e_1} \cdots \rho_r^{e_r}$ be the prime factorization of α. 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, $\rho_1\mathcal{O}$ is a prime and hence maximal since prime ideals are maximal in $\mathcal{O}$. Whence $\rho_1\mathcal{O} = \mathfrak{p}$ proving $\mathfrak{p}$ is principal. □

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 $\mathcal{O}$. This is indeed a group as the following theorem demonstrates:

Theorem 4.3.7. *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. By Lemma 4.3.3, we see that $\mathfrak{p}^{-1}$ is the inverse of any prime $\mathfrak{p}$. Therefore every prime is invertible. If $\mathfrak{f}$ is a fractional ideal it admits a prime factorization $\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and then $\mathfrak{f}^{-1} = \mathfrak{p}_1^{-e_1} \cdots \mathfrak{p}_r^{-e_r}$ is its inverse. This completes the proof. □

It is possible to deduce an explicit description for the inverse $\mathfrak{f}^{-1}$ of any fractional ideal $\mathfrak{f}$.

Proposition 4.3.8. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and let $\mathfrak{f}$ be a fractional ideal of $\mathcal{O}$. 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 4.3.7. 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 $\mathfrak{p}^{-1}$ for a prime $\mathfrak{p}$. Write $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$. Whence

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

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

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. Whence they are pairwise comaximal so that the Chinese remainder theorem gives an isomorphism

$$\mathcal{o}/\mathfrak{a} \cong \bigoplus_i \mathcal{o}/\mathfrak{p}_i^{e_i}.$$

In particular, for any choice of $\alpha_i \in \mathcal{o}$ there exists a $\alpha \in \mathcal{o}$ such that

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

We will use the Chinese remainder theorem to prove a few useful lemmas about Dedekind domains. If $\mathcal{o}$ is a Dedekind domain with prime $\mathfrak{p}$, we call $\mathbb{F}_\mathfrak{p} = \mathcal{o}/\mathfrak{p}$ the **residue class field** of $\mathcal{o}$ by $\mathfrak{p}$. This is field as primes are maximal in Dedekind domains. Our first lemma is an isomorphism between the residue class field and quotients by powers of a prime.

Lemma 4.3.9. *Let $\mathcal{o}$ be a Dedekind domain. Then for any prime $\mathfrak{p}$ of $\mathcal{o}$ and non-negative integer n, 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 $\beta \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$. 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 $\alpha \in \ker\phi$. Then $\alpha\beta \in \mathfrak{p}^{n+1}$ and as $\beta \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$, we must have $\alpha \in \mathfrak{p}$. Whence $\ker\phi = \mathfrak{p}$. 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 $\beta\mathcal{o} \subseteq \mathfrak{p}^n$. Since $\beta \notin \mathfrak{p}^{n+1}$, it must be the case that $\beta\mathcal{o}\mathfrak{p}^{-n}$ is an integral ideal relatively prime to $\mathfrak{p}^{n+1}$. By the Chinese remainder theorem, we can find a $\alpha \in \mathcal{o}$ 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 congruence means $\alpha \in \beta\mathcal{o}\mathfrak{p}^{-n}$ whence $\alpha \in \beta\mathcal{o}$ by relative primality of the aforementioned integral ideals. Thus $\alpha\beta^{-1} \in \mathcal{o}$ and the first congruence implies

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

This shows ϕ is surjective. $\square$

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

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

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

for some nonnegative integers e_i and f_i. By the prime factorization of fractional ideals, there exists $\alpha_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$. As $\mathfrak{p}_1^{e_1+1}, \ldots, \mathfrak{p}_r^{e_r+1}$ are pairwise relatively prime, the Chinese remainder theorem implies the existence of an $\alpha \in \mathcal{O}$ such that $\alpha \equiv \alpha_i \pmod{\mathfrak{p}_i^{e_i+1}}$. But then

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

Whence $\mathfrak{p}_i^{e_i} \mid\mid \alpha\mathcal{O}$. It follows that $(\alpha\mathcal{O}, \mathfrak{ab}) = \mathfrak{a}$. Then there exists an integral ideal $\mathfrak{c}$ such that $\alpha\mathcal{O} = \mathfrak{ac}$ and necessarily $(\mathfrak{ac}, \mathfrak{ab}) = \mathfrak{a}$. 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 4.3.11. *Let $\mathcal{O}$ be a Dedekind domain where $\mathfrak{f}$, $\mathfrak{g}$, and $\mathfrak{h}$ be fractional ideals of $\mathcal{O}$ with $\mathfrak{g} \subseteq \mathfrak{f}$. Then we have an isomorphism*

$$\mathfrak{f}/\mathfrak{g} \cong \mathfrak{fh}/\mathfrak{gh}.$$

In particular,

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

for any integral ideal $\mathfrak{a}$ of $\mathcal{O}$.

Proof. Write $\mathfrak{f} = \frac{1}{\alpha}\mathfrak{a}$, $\mathfrak{g} = \frac{1}{\beta}\mathfrak{b}$, and $\mathfrak{h} = \frac{1}{\gamma}\mathfrak{c}$ for some 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,

$$\mathfrak{f}/\mathfrak{g} \cong \beta\mathfrak{a}/\alpha\mathfrak{b} \quad \text{and} \quad \mathfrak{fh}/\mathfrak{gh} \cong \beta\mathfrak{ac}/\alpha\mathfrak{bc},$$

it suffices to show

$$\mathfrak{a}/\mathfrak{b} \cong \mathfrak{ac}/\mathfrak{bc}.$$

Consider the homomorphism

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

By the first isomorphism theorem, it suffices to show $\ker \phi = \mathfrak{b}$ and that ϕ is surjective. To this end, we know $\mathfrak{a} \mid \mathfrak{b}$ since to contain is to divide. Therefore $\mathfrak{ba}^{-1}$ is an integral

ideal and Lemma 4.3.10 implies the existence of an integral ideal $\mathfrak{d}$ relatively prime to $\mathfrak{b}\mathfrak{a}^{-1}$ such that $\mathfrak{c}\mathfrak{d} = \delta\mathcal{O}$ for some nonzero $\delta \in \mathcal{O}$. Whence

$$\mathfrak{d} + \mathfrak{b}\mathfrak{a}^{-1} = \mathcal{O} \quad \text{and} \quad \mathfrak{d} \cap \mathfrak{b}\mathfrak{a}^{-1} = \mathfrak{d}\mathfrak{a}^{-1}.$$

Writing $\mathfrak{d} = \delta\mathfrak{c}^{-1}$, a short computation shows that these identities imply

$$\delta\mathfrak{a} + \mathfrak{b}\mathfrak{c} = \mathfrak{a}\mathfrak{c} \quad \text{and} \quad \mathfrak{a} \cap \delta^{-1}\mathfrak{b}\mathfrak{c} = \mathfrak{b}.$$

As $\ker\phi = \mathfrak{a} \cap \delta^{-1}\mathfrak{b}\mathfrak{c}$, the second identity shows $\ker\phi = \mathfrak{b}$. Surjectivity follows from the first identity. This proves the first statement. For the second statement, take $\mathfrak{f} = \mathfrak{a}^{-1}$, $\mathfrak{g} = \mathcal{O}$, and $\mathfrak{h} = \mathfrak{a}$. □

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 4.3.12. *Let $\mathcal{O}$ be a Dedekind domain. If there are only finitely many primes of $\mathcal{O}$ 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 $\mathfrak{a}$, Lemma 4.3.10 implies the existence of an integral ideal $\mathfrak{b}$ relatively prime to $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ such that $\mathfrak{a}\mathfrak{b} = \alpha\mathcal{O}$ for some nonzero $\alpha \in \mathcal{O}$. As $\mathfrak{b}$ is relatively prime to all of the primes of $\mathcal{O}$ we must have $\mathfrak{b} = \mathcal{O}$. Then $\mathfrak{a} = \alpha\mathcal{O}$. As $\mathfrak{a}$ was arbitrary, $\mathcal{O}$ is a principal ideal domain. □

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

Proposition 4.3.13. *Let $\mathcal{O}$ be a Dedekind domain. Then every fractional ideal $\mathfrak{f}$ of $\mathcal{O}$ is generated by at most two elements.*

Proof. Writing $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$, it suffices to prove the claim $\mathfrak{a}$. Let $\alpha \in \mathfrak{a}$ be nonzero. By Lemma 4.3.10, there exists an integral ideal $\mathfrak{b}$ relatively prime to $\alpha\mathcal{O}$ such that $\mathfrak{a}\mathfrak{b} = \beta\mathcal{O}$ for some nonzero $\beta \in \mathcal{O}$. Whence

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

Upon multiplying by $\mathfrak{a}$, a short computation shows

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

Therefore $\mathfrak{a}$ is generated by at most two elements. □

This result 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 the degree to which $\mathcal{O}$ fails to be a principal ideal domain 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 4.3.7, $P_{\mathcal{O}}$ is normal. The **ideal class group** $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is defined to be the quotient group

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

An element of $\mathrm{Cl}(\mathcal{O})$ is called 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 it follows that every ideal class can be represented by an integral ideal. The **class number** $h_{\mathcal{O}}$ of $\mathcal{O}$ is defined by

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

The ideal class group encodes how much $\mathcal{O}$ fails to be a principal ideal domain and the class number is a measure of the degree of failure. Indeed, $\mathcal{O}$ is a principal ideal domain if and only if $h_{\mathcal{O}} = 1$.

Remark 4.3.14. 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 $\mathcal{O}$ fit into an exact sequence.

Proposition 4.3.15. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. Then the sequence*

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

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

Proof. As the second map is injective and the fourth map is surjective, the sequence is exact at $\mathcal{O}^*$ and $\mathrm{Cl}(\mathcal{O})$. So it suffices to prove exactness at K^* and $I_{\mathcal{O}}$. For exactness at K^*, recall from Theorem 4.3.7 that $\mathcal{O}$ is the identity of $I_{\mathcal{O}}$. A principal integral ideal is $\mathcal{O}$ if and only if it is generated by a unit in $\mathcal{O}$ and exactness at K^* follows. We have exactness at $I_{\mathcal{O}}$ because the principal fractional ideals represent the identity class of $\mathrm{Cl}(\mathcal{O})$ and these are generated by elements of K^*. □

Thinking of the third map in this exact sequence 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 ideals are created).

Remark 4.3.16. The class number $h_{\mathcal{O}}$ and unit group $\mathcal{O}^*$ are 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 4.3.17. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is already integrally closed. As $\mathcal{O}_K/\mathbb{Z}$ admits an integral basis, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of finite rank. Whence any ideal is a finitely generated $\mathbb{Z}$-module and hence a finitely generated $\mathcal{O}_K$-module. This proves $\mathcal{O}_K$ is noetherian. It remains to prove that every prime $\mathfrak{p}$ of $\mathcal{O}_K$ is maximal. This is equivalent to showing $\mathcal{O}_K/\mathfrak{p}$ 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 positive integer n and $a_i \in \mathbb{Z}$. Taking n minimal ensures $a_0 \neq 0$. Isolating a_0 shows $a_0 \in \mathfrak{p}$ and hence $a_0 \in \mathfrak{p} \cap \mathbb{Z}$. Therefore $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p. Then $\ker \phi = p\mathbb{Z}$, and by the first isomorphism theorem, ϕ induces an injection $\phi : \mathbb{F}_p \to \mathcal{O}_K/\mathfrak{p}$. Whence $\mathcal{O}_K/\mathfrak{p}$ is a finite dimensional $\mathbb{F}_p$-vector space as $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of finite rank. By primality of $\mathfrak{p}$, $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain and thus must be a field. □

In view of the fact that $\mathcal{O}_K$ is a Dedekind domain, 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 Theorem 4.3.4 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. We will also leverage geometric ideas to show that the class number is finite and completely describe the unit group.

4.4 Localization

Let $\mathcal{o}$ be an integral domain with field of fractions K. A subset D of $\mathcal{o}$ is said to be **multiplicative** if it is closed under multiplication, $1 \in D$, and $0 \notin D$. The set $\mathcal{o} - \{0\}$ is always multiplicative but more interesting examples are when we consider strict subsets. In any case, we define the **localization** $\mathcal{o}D^{-1}$ of $\mathcal{o}$ at D by

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

Clearly $\mathcal{O}D^{-1}$ is a subring of K which is an integral domain and is obtained from $\mathcal{O}$ by making the elements of D invertible. More generally, for any fractional ideal $\mathfrak{f}$ of $\mathcal{O}$, the **localization** $\mathfrak{f}D^{-1}$ of $\mathfrak{f}$ at D is defined by

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

In particular, $\mathfrak{a}D^{-1}$ is an integral ideal of $\mathcal{O}D^{-1}$ if $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$. Writing $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$, it follows that $\mathfrak{f}D^{-1}$ is a fractional ideal of $\mathcal{O}D^{-1}$.

In the case of primes, we have an exact correspondence between those of $\mathcal{O}$ disjoint from D and those of $\mathcal{O}D^{-1}$.

Proposition 4.4.1. *Let $\mathcal{O}$ be an integral domain and D be a multiplicative subset of $\mathcal{O}$. 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. Then the integral ideal $\mathfrak{q}D^{-1}$ of $\mathcal{O}D^{-1}$ is prime because $\mathfrak{q}$ is. Also, the prime $\mathfrak{q}D^{-1}$ satisfies

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

because $\mathfrak{q}$ is disjoint from D. Now suppose $\mathfrak{Q}$ is a prime of $\mathcal{O}D^{-1}$. Then the integral ideal $\mathfrak{Q} \cap \mathcal{O}$ of $\mathcal{O}$ is prime because $\mathfrak{Q}$ is. Also, $\mathfrak{Q} \cap \mathcal{O}$ is disjoint from D for otherwise it contains a unit which is a contradiction as prime ideals are proper. Moreover, the prime $\mathfrak{Q} \cap \mathcal{O}$ satisfies

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

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. □

It follows from this result that 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. Often, D is chosen so that it is the compliment of a prime $\mathfrak{p}$. Indeed, $\mathcal{O} - \mathfrak{p}$ is a multiplicative subset precisely because $\mathfrak{p}$ is prime. In fact, let X be a set of primes of $\mathcal{O}$ and consider

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

Then $\mathcal{O} - \bigcup_{\mathfrak{p} \in X} \mathfrak{p}$ is a multiplicative subset because of the identity

$$\mathcal{O} - \bigcup_{\mathfrak{p} \in X} \mathfrak{p} = \bigcap_{\mathfrak{p} \in X} (\mathcal{O} - \mathfrak{p}).$$

In any case, we define the **localization** $\mathcal{o}_\mathfrak{p}$ of $\mathcal{o}$ at $\mathfrak{p}$ by

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

Localizing at a prime $\mathfrak{p}$ should be thought of as removing all of the algebraic information about $\mathcal{o}$ that has nothing to do with $\mathfrak{p}$. More generally, 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

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

In both of these constructions we have localized at a single prime. It is possible to localize at more than one prime. Let X be a set of primes in $\mathcal{o}$. We define the **localization** $\mathcal{o}(X)$ of $\mathcal{o}$ at X by

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

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

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

If X consists of a single prime $\mathfrak{p}$ then $\mathcal{o}(X) = \mathcal{o}_\mathfrak{p}$ and $\mathfrak{f}(X) = \mathfrak{f}_\mathfrak{p}$.

In order for localization to be a useful tool in algebraic investigations, it must behave well with respect to what we have already developed. To this end, we will collect some useful properties about localization. Our first property says that intersections of localizations behave well with respect to fractional ideals and units.

Proposition 4.4.2. *Let $\mathcal{o}$ be an integral domain with field of fractions K. Then for every fractional ideal $\mathfrak{f}$ of $\mathcal{o}$, we have*

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

In particular,

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

Proof. For the first identity, the forward containment is obvious. For the reverse containment, suppose $\frac{\eta}{\delta} \in \bigcap_\mathfrak{p} \mathcal{o}_\mathfrak{p}$ and set

$$\mathfrak{a} = \{\alpha \in \mathcal{o} : \eta\alpha \in \delta\mathcal{o}\}.$$

Then $\mathfrak{a}$ is an integral ideal of $\mathcal{o}$ and contains δ. As δ is not contained in any prime of $\mathcal{o}$, it follows that $\mathfrak{a}$ cannot be contained in any prime of $\mathcal{o}$. By Zorn's lemma every proper ideal is contained in a maximal ideal which is necessarily prime. Whence $\mathfrak{a}$ is not proper and so $\mathfrak{a} = \mathcal{o}$. In particular, $1 \in \mathfrak{a}$. Therefore $\eta \in \delta\mathcal{o}$ which implies

$\frac{\alpha}{\beta} \in \mathcal{O}$ proving the reverse containment. The second identity follows from the first upon multiplying by $\mathfrak{f}$. This proves the first statement in full.

For the second statement, the forward containment is clear. For the reverse containment, suppose $\frac{\eta}{\delta} \in \bigcap_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}^*$. We have already showed $\frac{\eta}{\delta} \in \mathcal{O}$ so it suffices to show $\frac{\eta}{\delta}$ is a unit. As δ is not contained in any prime of $\mathcal{O}$, it cannot be contained in any maximal ideal as maximal ideals are prime. This means δ is a unit. Interchanging the roles of η and δ shows that η is a unit as well. Hence $\frac{\eta}{\delta}$ is a unit and the reverse containment follows. □

Our second property is that localization behaves well with respect to the inverse of fractional ideals. Of course, this assumes $\mathcal{O}$ is a Dedekind domain.

Proposition 4.4.3. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and D be a multiplicative subset of $\mathcal{O}$. Then for any fractional ideal $\mathfrak{f}$ of $\mathcal{O}$, we have*

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

Proof. As $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some nonzero $\delta \in \mathcal{O}$ and integral ideal $\mathfrak{a}$, it suffices to prove the claim for the integral ideal $\mathfrak{a}$. We will show

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

By Proposition 4.3.8, these sets can be explicitly described as

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

and

$$(\mathfrak{a}D^{-1})^{-1} = \{\kappa \in K : \kappa\mathfrak{a}D^{-1} \subseteq \mathcal{O}D^{-1}\}.$$

Whence they are the same and the identity follows. □

Our third property is that that the localization of a Dedekind domain is again a Dedekind domain.

Proposition 4.4.4. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and D be a multiplicative subset of $\mathcal{O}$. Then $\mathcal{O}D^{-1}$ is a Dedekind domain.*

Proof. To prove $\mathcal{O}D^{-1}$ is integrally closed, let $\kappa \in K$ be integral over $\mathcal{O}D^{-1}$. Then

$$\kappa^n + \frac{\eta_{n-1}}{\delta_{n-1}}\kappa^{n-1} + \cdots + \frac{\eta_0}{\delta_0} = 0,$$

for some positive integer n and $\frac{\eta_i}{\delta_i} \in \mathcal{O}D^{-1}$. Letting $\delta = \delta_0 \cdots \delta_{n-1}$ and multiplying by δ^n shows that

$$(\kappa\delta)^n + \frac{\eta_{n-1}\delta}{\delta_{n-1}}(\kappa\delta)^{n-1} + \cdots + \frac{\eta_0\delta^n}{\delta_0} = 0.$$

Whence $\kappa\delta$ is the root of a monic polynomial with coefficients in $\mathcal{O}$. As $\mathcal{O}$ is integrally closed, $\kappa\delta \in \mathcal{O}$ and therefore $\kappa \in \mathcal{O}D^{-1}$. This proves $\mathcal{O}D^{-1}$ is integrally closed. To show it is noetherian, let $\mathfrak{A}$ be an ideal of $\mathcal{O}D^{-1}$ and set $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}$. Then

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

Since $\mathcal{O}$ is a Dedekind domain, $\mathfrak{a}$ 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. Hence $\mathcal{O}D^{-1}$ is noetherian. It remains to show that every prime of $\mathcal{O}D^{-1}$ is maximal. By Proposition 4.4.1, every prime is of the form $\mathfrak{p}D^{-1}$ for some prime $\mathfrak{p}$ of $\mathcal{O}$. But then $\mathfrak{p}D^{-1}$ is maximal because $\mathfrak{p}$ is and the bijections in Proposition 4.4.1 are inclusion-preserving.□

As an immediate consequence of this result is that the localizations $\mathcal{O}_\mathfrak{p}$ and $\mathcal{O}(X)$ are Dedekind domains if $\mathcal{O}$ is.

Returning to the general setting, an integral domain $\mathcal{O}$ is said to be a **local** if it has a unique maximal ideal. As may be expected, the resulting integral domain after localizing at a prime will be local. In particular, $\mathcal{O}_\mathfrak{p}$ is local where the maximal ideal is $\mathfrak{p}_\mathfrak{p}$. Indeed, recall from Proposition 4.4.1 that the map

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

is an inclusion-preserving bijection between the primes of $\mathcal{O}$ contained in $\mathfrak{p}$ the primes of $\mathcal{O}_\mathfrak{p}$. As maximal ideals are prime, $\mathfrak{p}_\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}_\mathfrak{p}$. As for consequences, we have

$$\mathcal{O}_\mathfrak{p}^* = \mathcal{O}_\mathfrak{p} - \mathfrak{p}_\mathfrak{p} \quad \text{and} \quad \mathcal{O}_\mathfrak{p}^* + \mathfrak{p}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^*.$$

In other words, the units of $\mathcal{O}_\mathfrak{p}$ are precisely the elements not in $\mathfrak{p}_\mathfrak{p}$ and the sum of a unit of $\mathcal{O}_\mathfrak{p}$ and an element of $\mathfrak{p}_\mathfrak{p}$ is again a unit of $\mathcal{O}_\mathfrak{p}$. If $\mathfrak{p}$ itself is maximal we can say more.

Proposition 4.4.5. *Let $\mathcal{O}$ be an integral domain and $\mathfrak{p}$ be a prime of $\mathcal{O}$. 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 an isomorphism

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

for any positive integer n.

Proof. Consider the homomorphism

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

We have $\ker\phi = \mathfrak{p}_\mathfrak{p}^n \cap \mathcal{O}$. By Proposition 4.4.1, $\mathfrak{p} = \mathfrak{p}_\mathfrak{p} \cap \mathcal{O}$ and the first isomorphism theorem induces the desired 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. It suffices to prove $\ker\phi = \mathfrak{p}^n$ and that ϕ is surjective for then the first isomorphism theorem completes the proof. Now $\ker\phi = \mathfrak{p}^n$ if and only if $\mathfrak{p}^n = \mathfrak{p}_\mathfrak{p}^n \cap \mathcal{O}$. This latter identity follows by induction and the aforementioned fact $\mathfrak{p} = \mathfrak{p}_\mathfrak{p} \cap \mathcal{O}$. For surjectivity, let $\frac{\alpha}{\delta}$ be a representative of a coset in $\mathcal{O}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^n$. As $\delta \notin \mathfrak{p}$ and $\mathfrak{p}$ is maximal, δ is a representative of an invertible element in the field $\mathcal{O}/\mathfrak{p}$. Whence there exists an $\varepsilon \in \mathcal{O}$ such that

$$\delta\varepsilon \equiv 1 \mod \mathfrak{p}.$$

Whence there is a $\rho \in \mathfrak{p}$ such that $\frac{1}{\delta} = \frac{\varepsilon}{1+\rho}$. Moreover, as $\mathfrak{p}$ is maximal $1+\rho$ is a unit in $\mathcal{O}$. Then $\frac{\alpha}{\delta} = \frac{\alpha\varepsilon}{1+\rho}$ is an element of $\mathcal{O}$ proving surjectivity. □

We wil now restrict to principal ideal domains rather than integral domains. An integral domain $\mathcal{O}$ is said to be a **discrete valuation ring** if it is a principal ideal domain with a unique maximal ideal. Equivalently, $\mathcal{O}$ is a local principal ideal domain or a Dedekind domain with exactly one prime.

Let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}$. In particular, $\mathfrak{p}$ is prime and 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 a unit. On the one hand, $\mathcal{O}$ is local so every element not in $\mathfrak{p}$ is a unit. On the other hand, $\mathcal{O}$ is a principal ideal domain so that π is the only prime of $\mathcal{O}$. Since $\mathcal{O}$ is necessarily a unique factorization domain, these facts together imply that every $\alpha \in \mathcal{O}$ is of the form

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

for some nonnegative integer n and unit ε. Moreover, α generates the integral ideal $\mathfrak{p}^n$ and every integral ideal is of this form. If K is the field of fractions of $\mathcal{O}$, it follows that every nonzero $\kappa \in K$ can be uniquely expressed as

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

for some integer n and unit ε. The most important data of a discrete valuation ring is its valuation. 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 $\kappa \in \mathcal{O}$ then the $v(\kappa)$ is characterized by the equation

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

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. These identities imply that v satisfies the properties

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

The first of which shows that

$$v : K^* \to \mathbb{Z},$$

is a surjective homomorphism.

If $\mathcal{O}$ is a Dedekind domain then it is local if and only if it is a discrete valuation ring. Indeed, any Dedekind domain with finitely many primes is a principal ideal domain by Proposition 4.3.12. This will allow us to establish a connection between Dedekind domains and discrete valuation rings. In particular, a noetherian integral domain is a Dedekind domain if and only if its localization at any prime is a discrete valuation ring.

Theorem 4.4.6. *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. For the forward implication, suppose $\mathcal{O}$ is a Dedekind domain and let $\mathfrak{p}$ be a prime. Then $\mathcal{O}_\mathfrak{p}$ is a local Dedekind domain and hence a discrete valuation ring as we have seen. This proves the forward implication. For the reverse implication, suppose $\mathcal{O}$ is a noetherian integral domain and $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring for all primes $\mathfrak{p}$. As $\mathcal{O}_\mathfrak{p}$ is a principal ideal domain, $\mathcal{O}_\mathfrak{p}$ is integrally closed by Lemma 4.1.3. Then Proposition 4.4.2 implies $\mathcal{O}$ is integrally closed too. As $\mathcal{O}$ is noetherian by assumption, it remains to show that every prime is maximal. So let $\mathfrak{q}$ be prime. By Zorn's lemma, $\mathfrak{q}$ is contained in some maximal ideal $\mathfrak{p}$. As maximal ideals are prime, the inclusion-preserving bijections in Proposition 4.4.1 show that $\mathfrak{q}_\mathfrak{p}$ and $\mathfrak{p}_\mathfrak{p}$ are primes of $\mathcal{O}_\mathfrak{p}$. As $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring it is a Dedekind domain with exactly one prime. Whence $\mathfrak{q}_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$ and the aforementioned inclusion-preserving bijections imply that $\mathfrak{q} = \mathfrak{p}$. Hence $\mathfrak{q}$ is maximal. This proves the reverse implication. □

Remark 4.4.7. Theorem 4.4.6 and Proposition 4.4.2 together provide a powerful simplification tool for studying a Dedekind domains $\mathcal{O}$. For if we want to prove a property about a fractional ideal $\mathfrak{f}$ of $\mathcal{O}$, Proposition 4.4.2 reduces to showing that the desired property holds for the fractional ideals $\mathfrak{f}_\mathfrak{p}$ corresponding to the localizations $\mathcal{O}_\mathfrak{p}$ at all primes $\mathfrak{p}$ and is preserved under intersection. But by Theorem 4.4.6, the localizations $\mathcal{O}_\mathfrak{p}$ are Dedekind domains with exactly one prime and hence principal ideal domains.

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 prime factorizations. Indeed, the prime factorization of fractional ideals implies that for any $\kappa \in K^*$, we have

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

for some integers $e_\mathfrak{q}$ all but finitely many of which are zero. We claim that $v_\mathfrak{p}(\kappa) = e_\mathfrak{p}$. To see this, first observe that if $\mathfrak{p}$ and $\mathfrak{q}$ are distinct primes then $\mathfrak{q}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. Indeed, as these primes are distinct choose $\alpha \in \mathfrak{q} - \mathfrak{p}$. Then $\alpha \in \mathfrak{q}_\mathfrak{p} - \mathfrak{p}_\mathfrak{p}$ by primality of $\mathfrak{p}$. As $\mathcal{O}_\mathfrak{p}$ is local, α must be a unit whence $\mathfrak{q}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. This forces

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

and we readily see that $v_\mathfrak{p}(\kappa) = e_\mathfrak{p}$. In particular, $v_\mathfrak{p}(\kappa) = 0$ for all but finitely many primes $\mathfrak{p}$. In view of these properties, $v_\mathfrak{p}$ is also 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 4.4.4 and by Proposition 4.4.1 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 because the only elements which are not inverted are those of $\mathfrak{p}$. In particular, this means

$$\mathcal{O}_\mathfrak{p} = \mathcal{O}(X)_{\mathfrak{p}_X} \quad \text{and} \quad \mathfrak{f}_\mathfrak{p} = \mathfrak{f}(X)_{\mathfrak{p}_X}. \tag{4.2}$$

The relationship between $\mathcal{O}$ and $\mathcal{O}(X)$ can be expressed via an exact sequence.

Proposition 4.4.8. *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 the sequence*

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

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 ideal class 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. As the second map is injective and the fifth map is surjective, we must show exactness at $\mathcal{O}(X)^*$, $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$, and $\mathrm{Cl}(\mathcal{O})$. For exactness at $\mathcal{O}(X)^*$, $\alpha \in \mathcal{O}(X)^*$ represents the zero coset in under the third map $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$ if and only if $\alpha \in \mathcal{O}_{\mathfrak{p}}^*$ for all $\mathfrak{p} \notin X$. But Equation (4.2) implies $\alpha \in \mathcal{O}_{\mathfrak{p}}^*$ for all primes $\mathfrak{p} \in X$. Whence α represents the zero coset if and only if $\alpha \in \mathcal{O}^*$ by Proposition 4.4.2 proving exactness at $\mathcal{O}(X)^*$. For exactness at $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$, a representative $(\kappa_{\mathfrak{p}})_{\mathfrak{p}\notin X}$ of a coset in $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$ represents the principal class in $\mathrm{Cl}(\mathcal{O})$ under the fourth map if and only if there is a $\kappa \in K^*$ such that

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

By the prime factorization of fractional ideals, $v_{\mathfrak{p}}(\kappa) = v_{\mathfrak{p}}(\kappa_{\mathfrak{p}})$. In particular, $v_{\mathfrak{p}}(\kappa) = 0$ 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 these primes as well. Because the primes of $\mathcal{O}(X)$ are $\mathfrak{p}_X$ for $\mathfrak{p} \in X$, Equation (4.2) and Proposition 4.4.2 together imply $\kappa \in \mathcal{O}(X)^*$. Exactness at $\bigoplus_{\mathfrak{p}\notin X} K^*/\mathcal{O}_{\mathfrak{p}}^*$ follows. For exactness at $\mathrm{Cl}(\mathcal{O})$, an integral ideal $\mathfrak{a}$ representing a class in $\mathrm{Cl}(\mathcal{O})$ represents the principal class under the fifth map if and only if there is a $\kappa \in K^*$ such that

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

In view of Equation (4.2) and Proposition 4.4.2 again, taking the intersection with the localizations at $\mathfrak{p}_X$ for all $\mathfrak{p} \notin X$ shows

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

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 $\mathfrak{a}$ proving exactness at $\mathrm{Cl}(\mathcal{O})$.

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. 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.

4.5 Todo: [Dedekind Extensions]

Let $\mathcal{o}$ be integrally closed with field of fractions K, L/K be a finite separable extension, and $\mathcal{O}$ be the integral closure of $\mathcal{o}$ in L. It turns out that $\mathcal{O}$ will be Dedekind whenever $\mathcal{o}$ is and the argument is similar to that of Theorem 4.3.17.

Proposition 4.5.1. *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 integrally closed as it is the integral closure of $\mathcal{o}$. To show $\mathcal{O}$ is noetherian, let the degree of L/K be n and $\lambda_1, \dots, \lambda_n$ be a basis for L/K. By Proposition 4.1.4 we may multiply by a nonzero element of $\mathcal{o}$, if necessary, to ensure that this basis belongs to $\mathcal{O}$. Being a basis, we find that $d_{L/K}(\lambda_1, \dots, \lambda_n)$ is nonzero by Proposition 4.2.5. As this basis is contained $\mathcal{O}$, Lemma 4.2.7 implies

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

Thus $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module. In particular, every ideal of $\mathcal{O}$ is also a finitely generated $\mathcal{o}$-module and therefore also a finitely generated $\mathcal{O}$-module. Whence $\mathcal{O}$ is noetherian. It remains to show that every prime of $\mathcal{O}$ is maximal. This is equivalent to showing $\mathcal{O}/\mathfrak{P}$ 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 prime 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 $\lambda \in \mathfrak{P}$ be nonzero. As λ is integral over $\mathcal{o}$, we have

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

for some positive integer n and $\alpha_i \in \mathcal{o}$. Taking n minimal ensures $\alpha_0 \neq 0$. Isolating α_0 shows $\alpha_0 \in \mathfrak{P}$ whence $\alpha_0 \in \mathfrak{P} \cap \mathcal{o}$. Therefore $\mathfrak{P} \cap \mathcal{o} = \mathfrak{p}$ for some prime $\mathfrak{p}$. This means $\ker \phi = \mathfrak{p}$, and by the first isomorphism theorem, ϕ induces an injection $\phi : \mathbb{F}_\mathfrak{p} \to \mathcal{O}/\mathfrak{P}$. Therefore $\mathcal{O}/\mathfrak{P}$ is a finite dimensional $\mathbb{F}_\mathfrak{p}$-vector space as $\mathcal{O}$ is a free $\mathcal{o}$-module of finite rank. By primality of $\mathfrak{P}$, $\mathcal{O}/\mathfrak{P}$ is a finite integral domain and thus must be a field. This proves the first statement and the second is equivalent. □

Accordingly, a ring extension $\mathcal{O}/\mathcal{o}$ is said to be 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 $\mathfrak{o}$ in L. These Dedekind domains are related via the identity

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

With this phrasing, the proof of Proposition 4.5.1 gives another important result.

Corollary 4.5.2. *Let $\mathcal{O}/\mathfrak{o}$ be a Dedekind extension of a degree n separable extension L/K. Then $\mathcal{O}$ is a finitely generated $\mathfrak{o}$-module of rank at most n and every prime $\mathfrak{P}$ of $\mathcal{O}$ satisfies*

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

for some prime $\mathfrak{p}$ of $\mathfrak{o}$. 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 4.5.1 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 a field extension and since $\mathcal{O}$ is a finitely generated $\mathfrak{o}$-module of rank at most n, $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ has degree at most n. □

In view of this result, if $\mathfrak{f}$ is a fractional ideal of $\mathfrak{o}$ then $\mathfrak{f}\mathcal{O}$ is a fractional ideal of $\mathcal{O}$ because $\mathfrak{f}$ is a finitely generated $\mathfrak{o}$-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 $\mathfrak{o}$.

We can say more in the case of primes. Suppose $\mathfrak{P}$ and $\mathfrak{p}$ are primes of $\mathcal{O}$ and $\mathfrak{o}$ respectively. We say that $\mathfrak{P}$ is **above** $\mathfrak{p}$, or equivalently, $\mathfrak{p}$ is **below** $\mathfrak{P}$ if

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

Corollary 4.5.2 implies that every prime of $\mathcal{O}$ is above exactly one prime of $\mathfrak{o}$. 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 $\mathfrak{o}$ is below at least one prime of $\mathcal{O}$. This is equivalent to the fact that any integral ideal of the form $\mathfrak{p}\mathcal{O}$ satisfies

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

Indeed, by the prime factorization of fractional ideals, choose $\alpha \in \mathfrak{p} - \mathfrak{p}^2$ so that $\alpha\mathfrak{o} = \mathfrak{p}\mathfrak{a}$ for some integral ideal $\mathfrak{a}$ relatively prime to $\mathfrak{p}$. Then $\mathfrak{a} + \mathfrak{p} = \mathfrak{o}$ so there exist $\beta \in \mathfrak{a}$ and $\gamma \in \mathfrak{p}$ with $\beta + \gamma = 1$. It follows that $\beta\mathfrak{p} \subseteq \alpha\mathfrak{o}$ and $\beta \notin \mathfrak{p}$. 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 $\delta \in \mathcal{O}$. Then $\alpha\delta + \gamma = 1$ whence $1 \in \mathfrak{p}$ contradicting the fact that $\mathfrak{p}$ is proper. Equivalently, $\mathfrak{p}\mathcal{O}$ has at least one prime factor $\mathfrak{P}$. This also implies

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

as the prime $\mathfrak{P}$ is above $\mathfrak{p}$ and $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}$. We illustrate the relationship between $\mathfrak{P}$ and $\mathfrak{p}$ via the following extension:

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

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

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

Something can also be said about 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 4.5.2. Accordingly, we call $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ the **residue class extension** of $\mathcal{O}/\mathcal{o}$ for $\mathfrak{P}$. 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. More generally, recall from Corollary 4.5.2 that $\mathcal{O}$ is at finitely generated $\mathcal{o}$-module of rank at most n. Therefore 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 $\mathfrak{p} \subseteq \mathfrak{A} \subseteq \mathfrak{B}$. We obtain the residue class field $\mathbb{F}_{\mathfrak{P}}$ when $\mathfrak{A} = \mathfrak{P}$ and $\mathfrak{B} = \mathcal{O}$.

Todo: [xxx]

All of this is preserved under localization.

In light of this result, $\mathcal{O}D^{-1}/\mathcal{o}D^{-1}$ is also a Dedekind extension of L/K for any multiplicative subset D of $\mathcal{o}$. We call $\mathcal{O}D^{-1}/\mathcal{o}D^{-1}$ the **localization** of $\mathcal{O}/\mathcal{o}$ at D. In the case of localizing at 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 $\mathfrak{p}$. The Dedekind extension $\mathcal{O}/\mathcal{o}$ is said to be **local** if $\mathcal{o}$ is local. Equivalently, $\mathcal{o}$ is a discrete valuation ring because it is a Dedekind domain. Whence $\mathcal{o}$ is a principal ideal domain and Theorem 4.2.8 implies that $\mathcal{O}/\mathcal{o}$ admits an integral basis. 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 4.3.12 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 $\mathcal{O}_{\mathfrak{p}}/\mathcal{o}_{\mathfrak{p}}$.

Todo: [xxx]

Proposition 4.5.3. *Let $\mathcal{O}/\mathcal{o}$ be a Dedekind extension of a finite separable extension L/K and let D be a multiplicative subset of $\mathcal{o}$. 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 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 4.4.1 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 4.4.1 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 4.4.1, 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 4.4.1. 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, $\mathfrak{P}^{e_{\mathfrak{p}}(\mathfrak{P})} \mid\mid \mathfrak{p}\mathcal{O}$ and $\mathfrak{P}'^{e_{\mathfrak{P}}(\mathfrak{P}')} \mid\mid \mathfrak{P}\mathcal{O}'$. Then

$$e_{\mathfrak{p}}(\mathfrak{P}') = e_{\mathfrak{p}}(\mathfrak{P})e_{\mathfrak{P}}(\mathfrak{P}') \quad \text{and} \quad f_{\mathfrak{p}}(\mathfrak{P}') = f_{\mathfrak{p}}(\mathfrak{P})f_{\mathfrak{P}}(\mathfrak{P}'). \tag{4.3}$$

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:

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

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

Lemma 4.5.4. *Let $\mathcal{O}/\mathfrak{o}$ 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 4.3.9. 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. □

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

Theorem (Fundamental equality). *Let $\mathcal{O}/\mathfrak{o}$ be a Dedekind extension of a degree n separable extension L/K. Suppose $\mathfrak{p}$ is a prime of $\mathfrak{o}$ 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 4.5.2 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 $m \leq n$, 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 4.5.2, so is N. So let $\omega_1, \ldots, \omega_r$ be generators. As $N = \mathfrak{p}N$, we have

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

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

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

Let $d = \det((\alpha_{i,j}) - I)$. 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 $(\mathrm{adj}(\alpha_{i,j}) - I)$ of $(\alpha_{i,j}) - I$ 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 4.1.4 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 4.5.4. So our dimension computations combine to give

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

□

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 $1 \leq i \leq n$ 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 4.5.5. 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 4.1.4 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 4.5.2, let $\omega_1, \ldots, \omega_r$ be generators. As L/K is algebraic, θ is algebraic over K and hence $L = K[\theta]$. Then

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

with $\kappa_{i,j} \in K$ for $1 \leq i, j \leq r$. 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 $\delta = \prod_{1 \leq i,j \leq r} \delta_{i,j}$, 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 $\mathcal{O}/o$ 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 o such that $\mathfrak{p}\mathcal{O}$ is relatively prime to $\mathfrak{Q}_{\mathcal{O}/o}$. 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 $o[x]$ 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

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

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

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

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

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

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

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

where the second and third isomorphisms follow by taking $o[x]/(\mathfrak{p}o[x] + m_\theta(x)o[x])$ and reducing elements of $o[x]$ modulo $m_\theta(x)o[x]$ 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 $o[x]$ 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 $e_\mathfrak{p}(\mathfrak{P}_i) \leq e_i$ for all i. But the fundamental equality then gives

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

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 $\mathcal{O}/o$ 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 $\mathfrak{Q}_{\mathcal{O}/o}$. By the prime factorization of fractional ideals, $\mathfrak{Q}_{\mathcal{O}/o}$ 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 $\mathcal{O}/o$ is monogenic. Indeed, Suppose $\mathcal{O} = o[\alpha]$ for some $\alpha \in \mathcal{O}$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is an integral basis for $\mathcal{O}/o$ and is necessarily a basis for L/K. But then α is also a primitive element for L/K which implies

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

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 $\mathcal{O}_K$.

Chapter 5

Todo: [Ramification]

Chapter 6

Todo: [Geometry of Numbers]

Part III

Analytic Number Theory

Chapter 7

Dirichlet Series

Throughout, $s = \sigma + it$ and $s_0 = \sigma_0 + it_0$ will stand for complex variables with σ, σ_0, t, and t_0 real.

7.1 Convergence Properties

A **Dirichlet series** $D(s)$ is a sum of the form

$$D(s) = \sum_{n \geq 1} \frac{a(n)}{n^s},$$

with $a(n) \in \mathbb{C}$. Our first aim is to understand where Dirichlet series converge and where they converge absolutely. It does not take much for $D(s)$ to converge uniformly in a sector.

Theorem 7.1.1. *Suppose $D(s)$ is a Dirichlet series that converges at $s_0 = \sigma_0 + it_0$. Then for any $H > 0$, $D(s)$ converges uniformly in the sector*

$$\{s \in \mathbb{C} : \sigma \geq \sigma_0 \text{ and } |t - t_0| \leq H(\sigma - \sigma_0)\}.$$

In particular, $D(s)$ converges in the half-plane $\sigma > \sigma_0$.

Proof. Write $R(u) = \sum_{n \geq u} \frac{a(n)}{n^{s_0}}$ for the tail of $D(s_0)$ so that

$$\frac{a(n)}{n^{s_0}} = (R(n) - R(n+1)).$$

Then for positive integers N and M with $M \leq N$, summation by parts implies

$$\sum_{M \leq n \leq N} \frac{a(n)}{n^s} = R(M)M^{s_0-s} - R(N+1)(N+1)^{s_0-s} - \sum_{M \leq n \leq N} R(n+1)(n^{s_0-s} - (n+1)^{s_0-s}).$$

We will express the sum on the right-hand side as an integral. To do this, observe that

$$n^{s_0-s} - (n+1)^{s_0-s} = -(s_0 - s) \int_n^{n+1} u^{s_0-s-1}\, du.$$

As $R(u)$ is constant on the interval $(n, n+1]$ a short computation shows

$$\sum_{M \le n \le N} R(n+1)(n^{s_0-s} - (n+1)^{s_0-s}) = -(s_0 - s)\int_M^{N+1} R(u)u^{s_0-s-1}\,du,$$

Whence

$$\sum_{M \le n \le N} \frac{a(n)}{n^s} = R(M)M^{s_0-s} - R(N+1)(N+1)^{s_0-s} + (s_0 - s)\int_M^{N+1} R(u)u^{s_0-s-1}\,du.$$

As $D(s)$ converges at $s = s_0$, we can choose M sufficiently large such that $|R(u)| < \varepsilon$ for all $u \ge M$. It follows that $|R(u)u^{s_0-s}| < \varepsilon$ for all such u provided s in the desired sector. For such s, we have

$$|s - s_0| \le (\sigma - \sigma_0) + |t - t_0| \le (H+1)(\sigma - \sigma_0).$$

These estimates together imply

$$\sum_{M \le n \le N} \frac{a(n)}{n^s} = O\left(2\varepsilon + \varepsilon(H+1)(\sigma - \sigma_0)\int_M^{N+1} u^{\sigma_0-\sigma-1}\,du\right).$$

Since the integral is $O\left(\frac{1}{\sigma-\sigma_0}\right)$, the sum is $o(1)$ for s in the desired sector. The first statement follows by uniform Cauchy's criterion. Taking the limit as $H \to \infty$ proves the second statement. □

We will want to keep track of where Dirichlet series converge absolutely. Let σ_c be the infimum of all σ for which $D(s)$ converges. We call σ_c the **abscissa of convergence** of $D(s)$. Similarly, let σ_a be the infimum of all σ for which $D(s)$ converges absolutely. We call σ_a the **abscissa of absolute convergence** of $D(s)$. As the summands of $D(s)$ are holomorphic, the convergence is locally absolutely uniform for $\sigma > \sigma_a$ (actually uniform in sectors) and so $D(s)$ is holomorphic in this half-plane.

The abscissas σ_c and σ_a act as the boundaries of convergence and absolute convergence respectively. Anything can happen on the lines $\sigma = \sigma_c$ and $\sigma = \sigma_a$, but to the right of them we have convergence and absolute convergence of $D(s)$ respectively. It turns out that σ_a is never far from σ_c provided σ_c is finite.

Theorem 7.1.2. *If $D(s)$ is a Dirichlet series with finite abscissa of convergence σ_c then*

$$\sigma_c \le \sigma_a \le \sigma_c + 1.$$

Proof. The first inequality is clear since absolute convergence implies convergence. For the second inequality, the terms $a(n)n^{-(\sigma_c+\varepsilon)}$ tend to zero as $n \to \infty$ because $D(s)$ converges at $s = \sigma_c + \varepsilon$. Therefore $a(n) \ll_\varepsilon n^{\sigma_c+\varepsilon}$ and so $D(s)$ is absolutely convergent at $s = \sigma_c + 1 + 2\varepsilon$. This means $\sigma_a \le \sigma_c + 1 + 2\varepsilon$. Taking the limit as $\varepsilon \to 0$ gives the second inequality. □

We now turn to the question of uniqueness of Dirichlet series. In particular, we would like to show that Dirichlet series are uniquely determined by their coefficient as this would allow us compare coefficient analogous to that of Taylor series. This is indeed possible.

Proposition 7.1.3. *Suppose $D(s)$ is a Dirichlet series with finite abscissa of convergence σ_c such that*

$$D(s) = \sum_{n\geq 1} \frac{a(n)}{n^s} \quad \textit{and} \quad D(s) = \sum_{n\geq 1} \frac{b(n)}{n^s}.$$

Then $a(n) = b(n)$ for all n.

Proof. Set $c(n) = a(n) - b(n)$. Then it suffices to prove $c(n) = 0$ for all n and we will do so by induction. Take $\sigma \geq \sigma_a$ so that $D(s)$ converges absolutely. Letting $\sigma \to \infty$, the dominated convergence theorem implies

$$\lim_{\sigma\to\infty} D(\sigma) = a(1) \quad \text{and} \quad \lim_{\sigma\to\infty} D(\sigma) = b(1).$$

Whence $c(1) = 0$. Assume by induction that $c(n) = 0$ for $n \leq N$ and consider the Dirichlet series

$$\sum_{n\geq 1} \frac{c(n)}{n^s}.$$

Its abscissa of absolute convergence is σ_a. As

$$\sum_{n>N} \frac{c(n)}{n^s} = 0,$$

by assumption, it follows that

$$c(N+1) = -\sum_{n>N} c(n) \left(\frac{N}{n}\right)^{\sigma}.$$

Letting $\sigma \to \infty$, the dominated convergence theorem implies

$$\lim_{\sigma\to\infty} \left(-\sum_{n>N} c(n) \left(\frac{N}{n}\right)^{\sigma} \right) = 0.$$

Hence $c(N+1) = 0$ which completes the proof. □

We will now introduce several resulting concerning the growth and average growth of the coefficients of a Dirichlet series. For legibility, it will be useful to introduce some notation. If $D(s)$ is a Dirichlet series with coefficients $a(n)$ then for $X > 0$, we set

$$A(X) = \sum_{n\leq X} a(n) \quad \text{and} \quad |A|(X) = \sum_{n\leq X} |a(n)|.$$

These are the partial sums of the coefficients $a(n)$ and their absolute values up to X respectively. Many of our results will be in terms of these sums. Our first result shows that the coefficients of a Dirichlet series grown at most polynomially provided the Dirichlet series converges absolutely at some point.

Proposition 7.1.4. *Suppose $D(s)$ is a Dirichlet series with coefficients $a(n)$ that converges absolutely at $s = \alpha$ for some real α. Then*

$$a(n) \ll_\varepsilon n^{\alpha+\varepsilon}.$$

In particular, if $D(s)$ has finite abscissa of absolute convergence σ_a then

$$a(n) \ll_\varepsilon n^{\sigma_a+\varepsilon}.$$

Proof. Necessarily $\sigma_a \leq \alpha$ and so $D(s)$ converges absolutely in the half-plane $\sigma > \alpha$. Write

$$|a(n)| \leq n^{\alpha+\varepsilon} \sum_{n\geq 1} \frac{|a(n)|}{n^{\alpha+\varepsilon}}.$$

The sum is $O_\varepsilon(1)$ because $D(s)$ is absolutely convergent for $\sigma > \alpha$. The first estimate follows at once. The second is immediate from the first and the definition of the abscissa of absolute convergence. □

It is natural to be curious about the converse, namely, is it possible to determine an upper bound on the abscissa of absolute convergence if we know a polynomial bound for the coefficients. This is indeed possible.

Proposition 7.1.5. *Suppose $D(s)$ is a Dirichlet series whose coefficients satisfy the estimate $a(n) \ll_\alpha n^\alpha$ for some real α. Then the abscissa of absolute convergence satisfies $\sigma_a \leq \alpha + 1$.*

Proof. Let $\sigma > \alpha + 1$. It suffices to show convergence of the series

$$\sum_{n\geq 1} \frac{|a(n)|}{n^\sigma}.$$

As

$$\sum_{n\geq 1} \frac{|a(n)|}{n^\sigma} \ll_\alpha \sum_{n\geq 1} \frac{1}{n^{\sigma-\alpha}},$$

and the latter series converges, the proof is complete. □

Let us now turn to the same questions but using averages of the coefficients. Our first result is analogous to Proposition 7.1.4.

Proposition 7.1.6. *Suppose $D(s)$ is a Dirichlet series with coefficients $a(n)$ that converges absolutely at $s = \alpha$ for some real α. Then*

$$A(X) \ll X^{\alpha+\varepsilon} \quad \textit{and} \quad |A|(X) \ll X^{\alpha+\varepsilon}.$$

In particular,

$$A(X) \ll_\varepsilon X^{\sigma_a+\varepsilon} \quad \textit{and} \quad |A|(X) \ll_\varepsilon X^{\sigma_a+\varepsilon}.$$

Proof. Necessarily $\sigma_a \leq \alpha$ and so $D(s)$ converges absolutely in the half-plane $\sigma > \alpha$. Write

$$\sum_{n \leq X} |a(n)| \leq X^{\alpha+\varepsilon} \sum_{n \geq 1} \frac{|a(n)|}{n^{\alpha+\varepsilon}}.$$

The sum is $O_\varepsilon(1)$ because $D(s)$ is absolutely convergent for $\sigma > \alpha$. As $A(x) \ll |A|(x)$, the first statement follows at once. The second is immediate from the first and the definition of the abscissa of absolute convergence. □

It turns out that if $A(X)$ is bounded then σ_c is negative.

Proposition 7.1.7. *Suppose $D(s)$ is a Dirichlet series and that $A(X) \ll 1$. Then $\sigma_c \leq 0$.*

Proof. Let $\sigma > 0$. Abel summation gives

$$\sum_{n \leq X} \frac{a(n)}{n^s} = \frac{A(X)}{X^s} + \int_1^X A(u) u^{-(s-1)} \, du.$$

As $A(X) \ll 1$, take the limit as $X \to \infty$ to obtain

$$D(s) = s \int_1^\infty A(u) u^{-(s+1)} \, du.$$

This expresses $D(s)$ as an integral. Direct evaluation shows that the integral is finite. Therefore $D(s)$ converges for $\sigma > 0$ which means $\sigma_c \leq 0$. □

Unfortunately, it is not often the case that $A(X)$ is bounded as this is quite a strong condition for most Dirichlet series. Fortunately, we can still obtain nice result analogous to that of Proposition 7.1.5 if we assume $|A|(X)$ grows at most polynomially.

Proposition 7.1.8. *Suppose $D(s)$ is a Dirichlet series such that $|A|(X) \ll_\alpha X^\alpha$ for some $\alpha \geq 0$. Then the abscissa of absolute convergence satisfies $\sigma_a \leq \alpha$.*

Proof. Let $\sigma > \alpha$. It suffices to show convergence of the series

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma}.$$

Abel summation gives

$$\sum_{n \leq X} \frac{|a(n)|}{n^\sigma} = \frac{|A|(X)}{X^\sigma} + \sigma \int_1^X |A|(u) u^{-(\sigma+1)} \, du.$$

In view of the bound $|A|(X) \ll_\alpha X^\alpha$, take the limit as $X \to \infty$ to obtain

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma} = \sigma \int_1^\infty |A|(u) u^{-(\sigma+1)} \, du.$$

Direct evaluation shows that the integral is bounded. Therefore our series is bounded and hence must converge. □

Unfortunately, Proposition 7.1.8 does not immediately imply a sharper upper bound for the abscissa of absolute convergence than that of Proposition 7.1.5. This is because if $a(n) \ll_\alpha n^\alpha$ then the trivial bounds for $A(X)$ and $|A(X)|$ are

$$A(X) \ll_\alpha X^{\alpha+1} \quad \text{and} \quad |A|(X) \ll_\alpha X^{\alpha+1}.$$

In particular, using the second bound in Proposition 7.1.8 will give $\sigma_a \leq \alpha + 1$. So if we want to obtain sharper upper bounds for the abscissa of absolute convergence then we must improve the polynomial bound for the coefficients directly. Unfortunately, this is often a daunting task in practice especially if the Dirichlet series is connected to a deep algebraic or arithmetic object. However, if we assume that the coefficients are nonnegative then **Landau's theorem** provides a way of locating the abscissa of absolute convergence exactly:

Theorem (Landau's theorem). *Suppose $D(s)$ is a Dirichlet series with nonnegative coefficients $a(n)$ and finite abscissa of absolute convergence σ_a. Then σ_a is a singularity of $D(s)$.*

Proof. Replacing $a(n)$ by $a(n)n^{-\sigma_a}$, if necessary, we may assume $\sigma_a = 0$. Now suppose to the contrary that $D(s)$ was holomorphic at $s = 0$. Then $D(s)$ is holomorphic in the domain

$$\mathcal{D} = \{s \in \mathbb{C} : \sigma_a > 0\} \cup \{s \in \mathbb{C} : |s| < \delta\},$$

for some $\delta > 0$. Let $P(s)$ be the power series expansion of $D(s)$ at $s = 1$. Then

$$P(s) = \sum_{k \geq 0} \frac{c_k}{k!}(s-1)^k,$$

where

$$c_k = \sum_{n \geq 1} \frac{a(n)(-\log(n))^k}{n},$$

upon differentiating $D(s)$ termwise. The radius of convergence of $P(s)$ is the distance from $s = 1$ to the nearest singularity of $P(s)$. Since $P(s)$ is holomorphic on $\mathcal{D}$, the closest possible singularities are at $s = \pm i\delta$. Therefore, the radius of convergence is at least $\sqrt{1+\delta^2}$. Write $\sqrt{1+\delta^2} = 1 + \delta'$ for some $\delta' > 0$. Then for $|s-1| < 1 + \delta'$, $P(s)$ is holomorphic and can be expressed as

$$P(s) = \sum_{k \geq 0} \frac{(s-1)^k}{k!} \sum_{n \geq 1} \frac{a(n)(-\log(n))^k}{n}.$$

Now choose s in this region to be real with with $-\delta' < s < 1$. Then this double sum is a sum of positive terms by assumption of the $a(n)$ being nonnegative. As $P(s)$ is necessarily absolutely convergent, interchanging the sums and a short computation shows

$$P(s) = D(s).$$

As $-\delta' < s < 1$ and $D(s)$ has nonnegative coefficients, it converges absolutely for some $s < 0$. This contradicts $\sigma_a = 0$. □

There is a very important distinction in Landau's theorem that abscissa of absolute convergence is a singularity and not just a point where the Dirichlet series does not converge. Indeed, this means that if $D(s)$ could be analytically continued to a region containing $\sigma = \sigma_a$ then the continuation must have a pole at $s = \sigma_a$. In particular, the abscissa of absolute convergence would then be a pole with the largest possible real part. This signals that the singularity is an inherent property of the analytic continuation and not one of the representation of the function as a Dirichlet series.

7.2 Euler Products

Generally speaking, if the coefficients $a(n)$ are chosen at random, $D(s)$ is not guaranteed to good properties outside of absolute convergence in some half-plane (provided it converges at a point). However, many Dirichlet series of interest will have coefficients that are multiplicative. These Dirichlet series admits product expressions.

Proposition 7.2.1. *Suppose $D(s)$ is a Dirichlet series with finite abscissa of absolute convergence σ_a and whose coefficients $a(n)$ are multiplicative. Then*

$$D(s) = \prod_p \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right),$$

for $\sigma > \sigma_a$. If the prime power coefficients satisfy

$$a(p^k) = \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

for some $\alpha_1(p), \ldots, \alpha_d(p) \in \mathbb{C}$ and positive integer d, then the product takes the form

$$D(s) = \prod_p (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1}.$$

Proof. Let $\sigma > \sigma_a$ and consider the series

$$\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}}.$$

This series converges absolutely because $D(s)$ does. Now let N be a positive integer. By absolute convergence and the fundamental theorem of arithmetic,

$$\prod_{p \leq N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right) = \sum_{n \leq N} \frac{a(n)}{n^s} + \sum_{n > N}^{*} \frac{a(n)}{n^s},$$

where the $*$ indicates that we are summing over only those additional terms $\frac{a(n)}{n^s}$ that appear in the expanded product. As $N \to \infty$, the first sum on the right-hand side tends to $D(s)$ and the second sum tends to zero because it is part of the tail of $D(s)$.

This proves that the product converges and is equal to $D(s)$. If the prime power coefficients are of the form

$$a(p^k) = \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

then

$$\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} = (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1},$$

from which the product formula follows. □

The representation

$$D(s) = \prod_p \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right),$$

the called the **Euler product** of $D(s)$. By Proposition 7.2.1, multiplicativity of the coefficients is enough to ensure that the Euler product exists and is equal to the Dirichlet series in the half-plane of absolute convergence. If the Euler product takes the form

$$D(s) = \prod_p (1 - \alpha_1(p)p^{-s})^{-1} \cdots (1 - \alpha_d(p)p^{-s})^{-1},$$

then it is said to be of **degree** d. The special case of complete multiplicative coefficients corresponds to degree 1 Euler products as

$$D(s) = \prod_p (1 - a(p)p^{-s})^{-1}.$$

The condition

$$a(p^k) = \sum_{1 \leq j_1 \leq \cdots \leq j_k \leq d} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p),$$

guarantees that the Dirichlet series has an Euler product of degree d.

Remark 7.2.2. Replacing $D(s)$ with its absolute series in Proposition 7.2.1 shows that

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma} = \prod_p \left(\sum_{k \geq 0} \frac{|a(p^k)|}{p^{k\sigma}} \right)$$

for $\sigma > \sigma_a$. Under the stronger assumption of an Euler product of degree d this identity becomes

$$\sum_{n \geq 1} \frac{|a(n)|}{n^\sigma} = \prod_p (1 - |\alpha_1(p)|p^{-\sigma})^{-1} \cdots (1 - |\alpha_d(p)|p^{-\sigma})^{-1}.$$

Either of these equalities is stronger than mere absolute convergence of the infinite product since each factor is replaced with its absolute series not just the absolute value of the series. In particular, this implies that the Euler product converges locally absolutely uniformly in the same region that the Dirichlet series does.

If $D(s)$ admits a Euler product, we write $D^{(N)}(s)$ to denote the Dirichlet series with the factors $p \mid N$ in the Euler product removed. This means

$$D^{(N)}(s) = D(s) \prod_{p|N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right).$$

Dually, we let $D_{(N)}(s)$ denote the Dirichlet series consisting only of the factors $p \mid N$ in the Euler product. This means

$$D_{(N)}(s) = \prod_{p|N} \left(\sum_{k \geq 0} \frac{a(p^k)}{p^{ks}} \right).$$

With this notation, we have the relationship

$$D(s) = D^{(N)}(s) D_{(N)}(s).$$

7.3 Dirichlet Convolution

We now turn to discussing how Dirichlet series behave with respect to products. Let $D_f(s)$ and $D_g(s)$ be the Dirichlet series defined by

$$D_f(s) = \sum_{n \geq 1} \frac{f(n)}{n^s} \quad \text{and} \quad D_g(s) = \sum_{n \geq 1} \frac{g(n)}{n^s},$$

for some arithmetic functions f and g. Let $f * g$ be the Dirichlet convolution of f and g. A short computation shows

$$D_f(s) D_g(s) = D_{f*g}(s).$$

In other words, $D_f(s)D_g(s)$ is again a Dirichlet series whose coefficients are given by the Dirichlet convolution of f and g. This relation also shows that $D_{f*g}(s)$ converges absolutely wherever both $D_f(s)$ and $D_g(s)$ do. Since Dirichlet convolution preserves multiplicativity, $D_{f*g}(s)$ will have multiplicative coefficients if both $D_f(s)$ and $D_g(s)$ do. Moreover, from the Möbius inversion formula we immediately find that

$$D_g(s) = D_{f*\mathbf{1}}(s),$$

if and only if

$$D_f(s) = D_{g*\mu}(s).$$

These identities can be used to compute the Dirichlet series for many types of arithmetic functions.

7.4 Perron Formulas

With Mellin inversion, it is possible to relate the sums of coefficients of a Dirichlet series to an integral of its associated Dirichlet series. Such formulas are desirable because they allow for the examination of these sums by methods in complex analysis. First, we setup some general notation. Let $D(s)$ be a Dirichlet series with coefficients $a(n)$. For $X > 0$, we set

$$A^*(X) = \sum_{n \leq X}^{*} a(n),$$

where the $*$ indicates that the last term is multiplied by $\frac{1}{2}$ if X is an integer. This slight modification of $A(X)$ accounts for the fact that Mellin inversion returns the average at a jump discontinuity. We would like to relate $A^*(X)$ to the inverse Mellin transform of $D(s)$. We will prove several variants of this basic idea. The first being **(classical) Perron's formula** which is a consequence of Abel summation and Mellin inversion applied to Dirichlet series.

Theorem (Perron's formula, classical). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$, we have*

$$A^*(X) = \frac{1}{2\pi i} \int_{(c)} D(s) X^s \frac{ds}{s}.$$

Proof. Let $\sigma > \sigma_a$. By Proposition 7.1.6, $A(X) \ll_\varepsilon X^{\sigma_a + \varepsilon}$. Taking ε sufficiently small, we find that $A(X)X^{-s} \to 0$ as $X \to \infty$. Abel summation then gives

$$D(s) = s \int_1^\infty A(u) u^{-(s+1)} \, du. \tag{7.1}$$

As $A(u) = 0$ in the interval $[0, 1)$, we can write the previous identity in the form

$$\frac{D(s)}{s} = \int_0^\infty A(u) u^{-(s+1)} \, du.$$

Mellin inversion immediately gives the result. □

In the proof of classical Perron's formula, we obtained a useful integral representation for a Dirichlet series. We collect this in the following corollary:

Corollary 7.4.1. *Let $D(s)$ be a Dirichlet series with finite and nonnegative abscissa of absolute convergence σ_a. Then for $\sigma > \sigma_a$, we have*

$$D(s) = s \int_1^\infty A(u) u^{-(s+1)} \, du.$$

Proof. The identity is Equation (7.1). □

Classical Perron's formula is not always useful in applications because often it is necessary to estimate the integral of the Dirichlet series. As the integral need not be absolutely bounded, this would require nontrivial estimates for the Dirichlet series in vertical strips. Fortunately, there are two ways to correct for this defect each of which leads to a different variant of Perron's formula. The first is to truncate the integral while the latter is to introduce a smoothing function. In the former case, a careful estimation of the error term is often necessary while the latter case requires estimates for the smoothing function. Both variants can be equally useful and the choice of which to use is often dependent upon what methods are available in the current setting.

Let us first focus on the truncated variant. To state it, we will need to setup some notation and prove a lemma. For $c > 0$ and $T > 0$, consider the integrals

$$\delta(y) = \frac{1}{2\pi i}\int_{(c)} y^s \frac{ds}{s} \quad \text{and} \quad I(y,T) = \frac{1}{2\pi i}\int_{c-iT}^{c+iT} y^s \frac{ds}{s},$$

defined for $y > 0$. Note that $I(y,T)$ is just $d(y)$ truncated outside height T. The lemma we require gives an explicit evaluation of $\delta(y)$ and gives an approximation for the error between $\delta(y)$ and its truncation $I(y,T)$. The proof is quite laborious but standard.

Lemma 7.4.2. *We have*

$$\delta(y) = \begin{cases} 0 & \text{if } y < 1, \\ \frac{1}{2} & \text{if } y = 1, \\ 1 & \text{if } y > 1. \end{cases}$$

Moreover,

$$I(y,T) - \delta(y) = \begin{cases} O\left(y^c \min\left(1, \frac{1}{T\log(y)}\right)\right) & \text{if } y \neq 1, \\ O\left(\frac{c}{T}\right) & \text{if } y = 1. \end{cases}$$

Proof. Since $I(y,T) \to \delta(y)$ as $T \to \infty$, it suffices to estimate $I(y,T)$ and then take the limit as $T \to \infty$. First consider the case $y = 1$. A short computation shows

$$I(1,T) = \frac{1}{\pi}\tan^{-1}\left(\frac{T}{c}\right).$$

Truncate the Laurent series of the inverse tangent after the first term to write $\tan^{-1}(t) = \frac{\pi}{2} + O\left(\frac{1}{t}\right)$. Then

$$I(1,T) = \frac{1}{2} + O\left(\frac{c}{T}\right),$$

and we see that $\delta(y) = \frac{1}{2}$. This proves everything when $y = 1$. Now suppose $y < 1$ and let $d > c$. Let $\eta = \sum_{1\leq i\leq 4}\eta_i$ be the rectangular contour in Figure 7.1 where the horizontal lines are along $t = \pm T$ and the vertical lines are along $\sigma = c$ and $\sigma = d$. Consider

$$\frac{1}{2\pi i}\int_{\eta} y^s \frac{ds}{s}.$$

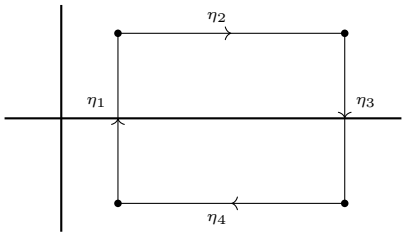

Figure 7.1: A rectangular contour.

We will evaluate this integral in the limit as $d \to \infty$. The contour does not enclose the only pole of the integrand which is at $s = 0$. So on the one hand, the residue theorem gives

$$\frac{1}{2\pi i} \int_{\eta} y^s \, \frac{ds}{s} = 0.$$

On the other hand, the integral is a sum along all four contours. Observe that

$$\frac{1}{2\pi i} \int_{\eta_1} y^s \, \frac{ds}{s} = I(y, T).$$

For the integrals over η_2 and η_4, the parameterizations $s \mapsto \sigma \pm iT$ show

$$\frac{1}{2\pi i} \int_{\eta_2} y^s \, \frac{ds}{s} + \frac{1}{2\pi i} \int_{\eta_4} y^s \, \frac{ds}{s} = O\left(\frac{y^c}{\log(y) T} \right),$$

as $y < 1$. For the integral over η_3, the parameterization $s \mapsto d + it$ shows

$$\frac{1}{2\pi i} \int_{\eta_3} y^s \, \frac{ds}{s} = O\left(y^d \log(T) \right).$$

Whence

$$I(y, T) = O\left(\frac{y^c}{\log(y) T} \right),$$

upon taking the limit as $d \to \infty$ since $y < 1$. It follows that $\delta(y) = 0$. We now obtain another estimate for $I(y, T)$ this time using a modified contour. Let $\eta = \eta_1 + \eta_2$ be the semicircular contour in Figure 7.2 where the vertical line is along $\sigma = c$ with endpoints at $s = c \pm iT$.

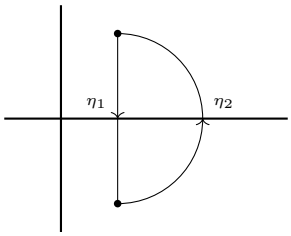

Figure 7.2: A semicircular contour.

As before, the residue theorem gives

$$\frac{1}{2\pi i}\int_{\eta} y^s \frac{ds}{s} = 0.$$

However, now

$$\frac{1}{2\pi i}\int_{\eta_1} y^s \frac{ds}{s} = -I(y,T).$$

The parameterization $s \mapsto \sqrt{(c^2+T^2)}e^{i\theta}$ shows that

$$\frac{1}{2\pi i}\int_{\eta_2} y^s \frac{ds}{s} = O(y^c).$$

Whence

$$I(y,T) = O(y^c).$$

Combining these two estimates for $I(y,T)$ proves everything when $y < 1$. Now suppose $y > 1$ and let $d < 0$. We argue as in the case $y < 1$ except we use the the rectangular contour in Figure 7.3.

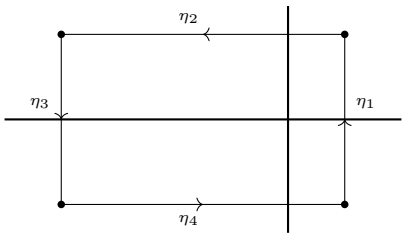

Figure 7.3: A rectangular contour.

This time the the contour encloses the simple pole of the integrand at $s = 0$ whose residue is 1. Arguing analogously, we find

$$I(y,T) = 1 + O\left(\frac{y^c}{\log(y)T}\right),$$

and so $\delta(y) = 1$.

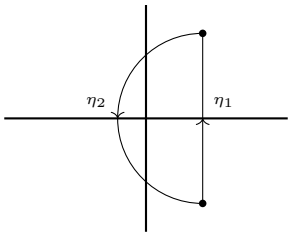

Figure 7.4: A semicircular contour.

We now modify the contour by using the semicircular one in Figure 7.4. Again, the contour encloses the simple pole of the integrand at $s = 0$ whose residue is 1. Arguing analogously, we obtain

$$I(y, T) = 1 + O(y^c).$$

Combining these two estimates for $I(y, T)$ proves everything when $y < 1$ and completes the proof. □

This result will provide the estimate we need to prove (truncated) **Perron's formula**:

Theorem (Perron's formula, truncated). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$ and $T > 0$, we have*

$$\begin{aligned} A^*(X) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} D(s) X^s \frac{ds}{s} \\ + O\left(X^c \sum_{\substack{n \geq 1 \\ n \neq X}} \frac{|a(n)|}{n^c} \min\left(1, \frac{1}{T\left|\log\left(\frac{X}{n}\right)\right|}\right) + \delta_X |a(X)| \frac{c}{T} \right), \end{aligned}$$

where $\delta_X = 1, 0$ according to if X is an integer or not.

Proof. By Lemma 7.4.2, we may write

$$A^*(X) = \sum_{n \geq 1} a(n) \delta\left(\frac{X}{n}\right),$$

and

$$\delta(y) = I(y, T) - \begin{cases} O\left(y^c \min\left(1, \frac{1}{T \log(y)}\right)\right) & \text{if } y \neq 1, \\ O\left(\frac{c}{T}\right) & \text{if } y = 1. \end{cases}$$

Substituting the second identity into the first and combining the O-estimates gives

$$\begin{aligned} A^*(X) = \sum_{n \geq 1} a(n) \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{X^s}{n^s} \frac{ds}{s} \\ + O\left(X^c \sum_{\substack{n \geq 1 \\ n \neq X}} \frac{|a(n)|}{n^c} \min\left(1, \frac{1}{T\left|\log\left(\frac{X}{n}\right)\right|}\right) + \delta_X |a(X)| \frac{c}{T} \right). \end{aligned}$$

As $D(s)$ converges absolutely, we may interchange the sum and the integral. The statement follows. □

Since the integral in truncated Perron's formula is over a finite vertical line, the integral is automatically absolutely bounded. There is also a mor crude variant of truncated Perron's formula that follows as a corollary:

Corollary 7.4.3. *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Then for any $c > \sigma_a$ and $0 < T < X^c$, we have*

$$A^*(X) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} D(s) X^s \frac{ds}{s} + O_c\left(\frac{X^c}{T}\right),$$

Proof. For $0 < T < X^c$, we have

$$\min\left(1, \frac{1}{T \log\left(\frac{X}{n}\right)}\right) \ll \frac{X^c}{T}.$$

Also, Proposition 7.1.4 guarantees $a(X) \ll X^c$. These estimates and that $D(s)$ is absolutely convergent at $s = c$ together imply that error term in truncated Perron's formula is $O_c\left(\frac{X^c}{T}\right)$. The claim follows. □

Having discussed truncated Perron's formula, we turn to the variant where we instead introduce a smoothing function. We call $\psi(y)$ a **smooth weight** if it is a positive bump function whose support is bounded away from zero. For any $X > 0$, we set

$$A_\psi(X) = \sum_{n \geq 1} a(n) \psi\left(\frac{n}{X}\right),$$

We distinguish between two cases. The first is when we choose $\psi(y)$ to assign weight 1 or 0 to the coefficients and we obtain sums such as

$$\sum_{\frac{X}{2} \leq n < X} a(n) \quad \text{or} \quad \sum_{X \leq n < X+Y} a(n).$$

Sums of this type are called **unweighted**. As an example of an unweighted sum, suppose $\psi(y)$ is a smooth weight that is identically 1 on $\left[\frac{1}{2}, 1\right]$ and supported in $\left[\frac{1}{2} - \frac{1}{X}, 1 + \frac{1}{X}\right]$. Then

$$A_\psi(X) = \sum_{\frac{X}{2} \leq n \leq X} a(n).$$

In the second case, we want $\psi(y)$ to dampen the coefficients with a weight other than 1 or 0. Sums of this type are called **weighted**. In either case, the Mellin transform $\Psi(s)$ of $\psi(y)$ is given by

$$\Psi(s) = \int_0^\infty \psi(y) y^s \frac{dy}{y}.$$

As $\psi(y)$ has compact support, the integral defining $\Psi(s)$ is a locally absolutely uniformly bounded on $\mathbb{C}$. In particular, $\Psi(s)$ is holomorphic and Mellin inversion implies that $\psi(y)$ is the Mellin inverse of $\Psi(s)$. As for nice properties, $\Psi(s)$ exhibit rapid decay.

Proposition 7.4.4. *Suppose $\psi(y)$ is smooth weight and let $\Psi(s)$ be its Mellin transform. Then for bounded σ, we have*

$$\Psi(s) \ll (|s| + 1)^{-N},$$

for any positive integer N.

Proof. Consider

$$\Psi(s) = \int_0^\infty \psi(y) y^s \frac{dy}{y}.$$

Since $\psi(y)$ is compactly supported, integration by parts yields

$$\Psi(s) = \frac{1}{s} \int_0^\infty \psi'(y) y^{s+1} \frac{dy}{y}.$$

Repeated integration by parts gives

$$\Psi(s) = \frac{1}{s(s+1)\cdots(s+N-1)} \int_0^\infty \psi^{(N)}(y) y^{s+N} \frac{dy}{y}.$$

Therefore

$$\Psi(s) \ll (|s|+1)^{-N} \int_0^\infty \psi^{(N)}(y) y^{\sigma+N} \frac{dy}{y}.$$

Now $\psi^{(N)}(y)$ is compactly supported in the same region as $\psi(y)$. In particular, $\psi^{(N)}(y)$ has compact support away from zero. Therefore

$$\int_0^\infty \psi^{(N)}(y) y^{\sigma+N} \frac{dy}{y} \ll 1,$$

and the estimate follows. □

The following result is (smoothed) **Perron's formula**:

Theorem (Perron's formula, smoothed). *Let $D(s)$ be a Dirichlet series with coefficient $a(n)$ and finite and nonnegative abscissa of absolute convergence σ_a. Let $\psi(y)$ be a smooth weight and let $\Psi(s)$ be its Mellin transform. Then for any $c > \sigma_a$, we have*

$$A_\psi(X) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) X^s \, ds.$$

In particular,

$$\sum_{n\geq 1} a(n)\psi(n) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) \, ds.$$

Proof. By Mellin inversion, we may write

$$A_\psi(X) = \sum_{n\geq 1} \frac{a(n)}{2\pi i} \int_{(c)} \Psi(s) \left(\frac{n}{X}\right)^{-s} ds.$$

We may interchange the sum and integral by the absolute convergence of $D(s)$ and Proposition 7.4.4. This gives

$$A_\psi(X) = \frac{1}{2\pi i} \int_{(c)} D(s)\Psi(s) X^s \, ds,$$

which is the first statement. For the second, take $X = 1$. □

The integral in smoothed Perron's formula is absolutely bounded (this permitted the interchange of the sum and integral). In practice, this means that the integral can be estimated directly and we do not need to truncate. The compensation for this is that we have introduced a weighting factor to the sum of coefficients.

Chapter 8

Analytic L-functions

Throughout, $s = \sigma + it$ and $u = \tau + ir$ will stand for complex variables with σ, τ, t, and r real. We also write

$$(u)_k = u(u+1)\cdots(u+(k-1)),$$

for the Pochhammer symbol.

8.1 Analytic Data

An **analytic L-function** $L(s)$ is a Dirichlet series

$$L(s) = \sum_{n\geq 1} \frac{a_L(n)}{n^s},$$

with coefficients $a_L(n) \in \mathbb{C}$ such that $a_L(1) = 1$ and satisfying the following properties:

Analyticity: There exists a nonnegative integer m_L such that the Dirichlet series of $L(s)$ is absolutely convergent for $\sigma > 1$ and admits meromorphic continuation to $\mathbb{C}$ with at most a pole at $s = 1$ of order m_L. Moreover, $(s-1)^{m_L}L(s)$ is order 1.

Functional Equation: There is a positive integer q_L, called the **conductor** of $L(s)$, a positive integer d_L called the **degree** of $L(s)$, complex numbers $(\mu_j)_{1\leq j\leq d_L}$ called the **gamma parameters** of $L(s)$ that are either real or occur in conjugate pairs and satisfy $\mathrm{Re}(\mu_j) \geq 0$, and a complex number ε_L called the **root number** of $L(s)$ with $|\varepsilon_L| = 1$, all of which determine functions

$$\Lambda(s,L) = q_L^{\frac{s}{2}}\gamma_L(s)L(s) \quad \text{and} \quad \gamma_L(s) = \pi^{-\frac{d_L s}{2}}\prod_j \Gamma\left(\frac{s+\mu_j}{2}\right),$$

called the **completion** of $L(s)$ and the **gamma factor** of $L(s)$ respectively, satisfying

$$\Lambda(s,L) = \varepsilon_L\overline{\Lambda(1-\overline{s},L)}.$$

This is called the **functional equation** of $L(s)$. The tuple $(\varepsilon_L, q_L, \mu_1, \ldots, \mu_{d_L})$ is called the **functional equation data** of $L(s)$.

Euler product: For every prime p, there exist complex numbers $(\alpha_j(p))_{1\leq j\leq d_L}$ called the **Euler parameters** of $L(s)$ at p satisfying $|\alpha_j(p)| \leq p^\theta$ for some $0 \leq \theta < 1$ and are such that $L(s)$ admits the Euler product

$$L(s) = \prod_p (1-\alpha_1(p)p^{-s})^{-1}\cdots(1-\alpha_{d_L}(p)p^{-s})^{-1},$$

for $\sigma > 1$. The polynomial L_p defined by

$$L_p(T) = (1-\alpha_1(p)T)\cdots(1-\alpha_{d_L}(p)T),$$

is called the **Euler factor** of $L(s)$ at p. If $p \nmid q_L$ then L_p is of degree d_L while if $p \mid q_L$ then L_p is of degree less than d_L.

An analytic L-function is said to be **Selberg class** if it satisfies the following additional property:

Ramanujan bound: We may take $\theta = 0$ so that $|\alpha_j(p)| \leq 1$.

Some comments on the definition of analytic L-functions are in order.

(i) As the Dirichlet series of $L(s)$ converges absolutely for $\sigma > 1$ its converges locally absolutely uniformly in this half-plane and therefore defines a holomorphic function there. Moreover, the Euler product necessarily converges locally absolutely uniformly in the same half-plane and hence defines a holomorphic function there as well which agrees with the Dirichlet series.

(ii) The bound $\mathrm{Re}(\mu_j) \geq 0$ ensures that the gamma factor is holomorphic in the half-plane $\sigma > 0$. As this factor is then guaranteed to be finite and nonzero at $s = 1$, the completion possesses a pole at $s = 1$ of order r. By the functional equation, the completion also has a pole at $s = 0$ of the same order.

(iii) If we merely assume $(s-1)^{m_L}L(s)$ is finite order then the functional equation forces the order to be 1. This can be deduced by considering the entire function

$$s^{m_L}(s-1)^{m_L}\Lambda(s, L),$$

and applying the Phragmén-Lindelöf convexity principle in vertical strips.

(iv) The condition that the root number satisfies $|\varepsilon_L| = 1$ isn't strictly necessary. For applying the functional equation twice shows $|\varepsilon_L|^2 = 1$.

(v) As the gamma function is conjugation-equivariant and the gamma parameters are real or occur in conjugate pairs, the gamma factor is also conjugation-equivariant. This means that we can write the functional equation in the form

$$q_L^{\frac{s}{2}}\gamma_L(s)L(s) = \varepsilon_L q_L^{\frac{1-s}{2}}\gamma_L(1-s)\overline{L(1-\overline{s})}.$$

(vi) The Euler product implies that the coefficients $a_L(n)$ are multiplicative and are determined on prime powers by

$$a_L(p^k) = \sum_{1 \le j_1 \le \cdots \le j_k \le d_L} \alpha_{j_1}(p) \cdots \alpha_{j_k}(p).$$

In other words, $a_L(p^k)$ is the complete symmetric polynomial of degree k in the Euler parameters at p. If the Ramanujan bound holds, then it follows that $a_L(n) \ll \sigma_{d_L}(n)$. This implies the slightly weaker, but more practical, estimate $a_L(n) \ll_\varepsilon n^\varepsilon$.

It it clear from the definition that analytic L-functions are closed under multiplication and that the degree is additive. Moreover, this closure respects Selberg class L-functions. This makes the set of analytic L-functions into a graded commutative semigroup where the grading is induced by degree. It follows that there exist irreducible elements with respect to the grading and we say that an analytic L-function is **primitive** if it such an irreducible. Clearly any analytic L-function of degree 1 is primitive. Moreover, every analytic L-function factors into a product of primitive L-functions. Such a factorization is only conjectured to be unique for Selberg class L-functions. A sufficient condition would be **Selberg's orthogonality conjecture**.

Conjecture (Selberg's orthogonality conjecture). *For any two primitive Selberg class L-functions $L_1(s)$ and $L_2(s)$, we have*

$$\sum_{p \le x} \frac{a_{L_1}(p)\overline{a_{L_2}(p)}}{p} = \delta_{L_1,L_2} \log\log(x) + O(1).$$

Indeed, we have the following result:

Proposition 8.1.1. *Assume Selberg's orthogonality conjecture. Then every Selberg class L-function factors uniquely into a product of primitive Selberg class L-functions.*

Proof. If the factorization into primitive unity L-functions were not unique, then we would have distinct factorizations satisfying

$$L_1(s) \cdots L_n(s) = M_1(s) \cdots M_m(s),$$

for some primitive Selberg class L-functions L_i and M_j. By uniqueness of coefficients of Dirichlet series, compare the p-th coefficient to see that

$$\sum_i a_{L_i}(p) = \sum_j a_{M_j}(p).$$

Now consider

$$\sum_{p<x} \frac{1}{p} \left(\sum_i a_{L_i}(p) \right) \left(\sum_j \overline{a_{M_j}(p)} \right) = \sum_{i,j} \sum_{p<x} \frac{a_{L_i}(p)\overline{a_{M_j}(p)}}{p}.$$

Selberg's orthogonality conjecture implies

$$O(1) = c \log\log(x) + O(1),$$

for some positive integer c since the factorizations are distinct. This is impossible. □

To an analytic L-function $L(s)$, we associate its **analytic conductor** $\mathfrak{q}(s,L)$ defined by

$$\mathfrak{q}(s,L) = q_L \mathfrak{q}_\infty(s,L),$$

where

$$\mathfrak{q}_\infty(s,L) = \prod_j (|s+\mu_j|+3).$$

The choice of 3 in $|s+\mu_j|+3$ is a matter of convenience as could use any positive constant. In particular, it is useful when taking logarithms as $\log(|s+\mu_j|+3) \geq 1$. For legibility, we will also write

$$\mathfrak{q}(t,L) = \mathfrak{q}\left(\frac{1}{2}+it, L\right) \quad \text{and} \quad \mathfrak{q}_\infty(t,L) = \mathfrak{q}_\infty\left(\frac{1}{2}+it, L\right).$$

as well as

$$\mathfrak{q}(L) = \mathfrak{q}\left(\frac{1}{2}, L\right) \quad \text{and} \quad \mathfrak{q}_\infty(L) = \mathfrak{q}_\infty\left(\frac{1}{2}, L\right),$$

Estimates for the analytic conductor follow from those of the gamma function. Recall from Stirling's formula that

$$\Gamma(s) \ll_\varepsilon (|t|+3)^{\sigma-\frac{1}{2}} e^{-\frac{\pi}{2}|t|} \quad \text{and} \quad \frac{1}{\Gamma(s)} \ll (|t|+3)^{\frac{1}{2}-\sigma} e^{\frac{\pi}{2}|t|}, \tag{8.1}$$

for bounded σ provided that in the former estimate s is at least distance ε away from the poles of the gamma function. Hence

$$\frac{\Gamma(1-s)}{\Gamma(s)} \ll_\varepsilon (|t|+3)^{1-2\sigma},$$

for bounded σ provided s is at least distance ε away from the poles of $\Gamma(1-s)$. Then the estimates

$$\frac{\gamma_L(1-s)}{\gamma_L(s)} \ll_\varepsilon \mathfrak{q}_\infty(s,L)^{\frac{1}{2}-\sigma} \quad \text{and} \quad q_L^{\frac{1}{2}-s}\frac{\gamma_L(1-s)}{\gamma_L(s)} \ll_\varepsilon \mathfrak{q}(s,L)^{\frac{1}{2}-\sigma}, \tag{8.2}$$

hold for bounded σ provided s is at least distance ε away from the poles of $\gamma_L(1-s)$. An associated estimate can be obtain for the logarithmic derivative of the analytic conductor. Recall from the logarithm of Stirling's formula that

$$\frac{\Gamma'}{\Gamma}(s) \ll \log(|s|+3),$$

provided σ is bounded and s is at least distance ε away from the poles of the gamma function. Then the estimates

$$\frac{\gamma_L'}{\gamma_L}(s) \ll_\varepsilon \log \mathfrak{q}_\infty(s,L) \quad \text{and} \quad \log q_L + \frac{\gamma_L'}{\gamma_L}(s) \ll_\varepsilon \log \mathfrak{q}(s,L), \tag{8.3}$$

hold for bounded σ provided s is at least distance ε away from the poles of the gamma factor.

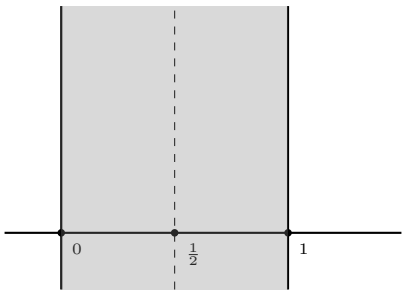

Figure 8.1: The critical strip.

The **critical strip** of an analytic L-function is the vertical strip left invariant by the transformation $s \mapsto 1 - s$. This region can also be described as

$$\left\{ s \in \mathbb{C} : \left| \sigma - \frac{1}{2} \right| \leq \frac{1}{2} \right\}.$$

The **critical line** is the vertical line left invariant by the transformation $s \mapsto 1 - s$ which is also given by $\sigma = \frac{1}{2}$. The critical line bisects the critical strip vertically. The **central point** is the fixed point of the transformation $s \mapsto 1 - s$, in other words, the point $s = \frac{1}{2}$. Clearly the central point is also the center of the critical line. The critical strip, critical line, and central point are all displayed in Figure 8.1.

In the half-plane $\sigma > 1$ we may study the analytic properties of $L(s)$ via its Dirichlet series. Using the functional equation, we may write

$$L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)} \overline{L(1-\overline{s})}.$$

This permits the study of $L(s)$ in the half-plane $\sigma < 0$ by using the Dirichlet series of $\overline{L(1-\overline{s})}$ and the the functional equation data. The interior of the critical strip is exactly the region where we cannot use either of these methods to study the analytic properties of $L(s)$. Of course, anything may be possible on the boundary lines $\sigma = 0$ and $\sigma = 1$ (for example Landau's theorem).

8.2 The Approximate Functional Equation

Despite not being able to study an analytic L-function $L(s)$ in the critical strip by means of Dirichlet series, there is formula which acts as a compromise between the functional equation and the Dirichlet series. This formula is known as the approximate functional equation. The usefulness comes from the fact that the approximate functional equation is valid inside of the critical strip and therefore can be used to obtain analytic properties about $L(s)$ in that region. We will first derive a preliminary result showing $L(s)$ has at most polynomial growth.

Proposition 8.2.1. *Let $L(s)$ be an analytic L-function with σ bounded and σ at least distance ε away from the possible pole at $s = 1$. Then there is a positive constant A such that*

$$L(s) \ll_\varepsilon (|t| + 3)^A.$$

Proof. Observe that $(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{m_L}$ on the vertical line $\sigma = \max(1+\varepsilon, \sigma_2)$. Now suppose $\sigma = \min(-\varepsilon, \sigma_1)$. On this vertical line, the functional equation and Equation (8.2) together show

$$L(s) \ll_\varepsilon \mathfrak{q}(s,L)^{\frac{1}{2}-\sigma}\overline{L(1-\overline{s})}.$$

Hence there exists a positive constant A'' with

$$(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{A''},$$

on the vertical line $\sigma = \min(-\varepsilon, \sigma_1)$. As $(s-1)^{m_L}L(s)$ is entire and of order 1, we can apply the Phragmén-Lindelöf convexity principle to $(s-1)^{m_L}L(s)$ the vertical strip $\min(-\varepsilon, \sigma_1) \leq \sigma \leq \max(1+\varepsilon, \sigma_2)$. Whence there is a positive constant A' such that

$$(s-1)^{m_L}L(s) \ll_\varepsilon (|t|+3)^{A'},$$

provided σ is bounded. Assuming s is at least distance ε away from the possible pole at $s=1$, diving by $(s-1)^{m_L}$ completes the proof. □

We are almost ready to prove the approximate function equation for an analytic L-function $L(s)$. The formula itself consists of two sums representing the Dirichlet series at s and a dualized Dirichlet series at $1-s$ as well as a potential residue term. The dual sum comes equip with a term containing the data of the functional equation. Both sums will also be dampened by a smooth cutoff function. In the statement of the approximate function equation, we will make use of a test function $\Phi(u)$. We require $\Phi(u)$ be an even holomorphic function bounded in the vertical strip $|\tau| < a+1$ for some $a > 1$ and such that $\Phi(0) = 1$. For s in the critical strip, we let $V_s(y)$ be the inverse Mellin transform

$$V_s(y) = \frac{1}{2\pi i}\int_{(a)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)y^{-u}\frac{du}{u},$$

defined for $y > 0$. For legibility, we will write

$$V_t(y) = V_{\frac{1}{2}+it}(y).$$

Stirling's formula implies

$$\frac{\Gamma(s+u)}{\Gamma(s)} \ll_\varepsilon \frac{(|t+r|+3)^{\sigma+\tau-\frac{1}{2}}}{(|t|+3)^{\sigma-\frac{1}{2}}}e^{-\frac{\pi}{2}(|t+r|-|t|)},$$

for s in the critical strip and bounded τ provided $s+u$ is at least distance ε away from the poles of the gamma function. Whence

$$\frac{\gamma_L(s+u)}{\gamma_L(s)} \ll_\varepsilon \frac{\mathfrak{q}_\infty(s+u)^{\frac{\sigma+\tau}{2}-\frac{1}{4}}}{\mathfrak{q}_\infty(s)^{\frac{\sigma}{2}-\frac{1}{4}}}e^{-d_L\frac{\pi}{2}(|t+r|-|t|)}, \tag{8.4}$$

for s in the critical strip and bounded τ provided $s+u$ is at least distance ε away from the poles of the gamma factor. Since $\Phi(u)$ is bounded in the vertical strip $|\tau| < a+1$,

the integrand exhibits exponential decay. Therefore the integral is locally absolutely uniformly bounded and hence $V_s(y)$ is smooth. The function $V_s(y)$ is the smooth cutoff function mentioned previously. We will also let $\varepsilon_L(s)$ be given by

$$\varepsilon_L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)}.$$

For legibility, we let

$$\varepsilon_L(t) = \varepsilon_L\left(\frac{1}{2}+it\right).$$

This term appears as a factor in the dual sum accounting for the functional equation data. We now prove the **approximate function equation**:

Theorem (Approximate functional equation). *Suppose $L(s)$ is an analytic L-function, $\Phi(u)$ is an even holomorphic function bounded in the vertical strip $|\tau| < a+1$ for some $a > 1$ and such that $\Phi(0) = 1$, and let $X > 0$. Then for s in the critical strip, we have*

$$L(s) = \sum_{n\geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L}X}\right) + \varepsilon_L(s) \sum_{n\geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_{1-s}\left(\frac{nX}{\sqrt{q_L}}\right) + \frac{R(s,X,L)}{q_L^{\frac{s}{2}}\gamma_L(s)},$$

where $R(s,X,L)$ is given by

$$R(s,X,L) = \operatorname*{Res}_{u=1-s} \frac{\Lambda(s+u,L)\Phi(u)X^u}{u} + \operatorname*{Res}_{u=-s} \frac{\Lambda(s+u,L)\Phi(u)X^u}{u}.$$

Proof. Consider the integral

$$\frac{1}{2\pi i}\int_{(a)} \Lambda(s+u,L)\Phi(u)X^u \frac{du}{u}.$$

Stirling's formula shows that $\gamma_L(s+u)$ exhibits exponential decay while $L(s+u)$ has at most polynomial growth by Proposition 8.2.1. Since $\Phi(u)$ is bounded in the vertical strip $|\tau| < a+1$, it follows that the integrand exhibits exponential decay. Therefore the integral is locally absolutely uniformly bounded. We will evaluate the integral in two ways. On the one hand, we can expand $L(s+u)$ inside the integrand as a Dirichlet series and by absolute boundedness of the integral we may interchange the sum and integral. A short computation shows that this is

$$q_L^{\frac{s}{2}}\gamma_L(s) \sum_{n\geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L}X}\right).$$

On the other hand, we can shift the line of integration to $(-a)$. In doing so we pass by a simple pole at $u = 0$ and possible poles at $u = 1-s$ and $u = -s$ giving

$$\frac{1}{2\pi i}\int_{(-a)} \Lambda(s+u,L)\Phi(u)X^u \frac{du}{u} + \Lambda(s,L) + R(s,X,L).$$

Apply the functional equation and perform the change of variables $u \mapsto -u$ to rewrite this as

$$-\varepsilon_L \frac{1}{2\pi i} \int_{(a)} \overline{\Lambda(1-\overline{s+u}, L)} \Phi(u) X^{-u} \frac{du}{u} + \Lambda(s, L) + R(s, X, L).$$

Analogous to the above, we can now expand $\overline{L(1-\overline{s+u})}$ inside the integrand as a Dirichlet series and by absolute boundedness of the integral we may interchange the sum and integral. A short computation shows that our previous expression becomes

$$-\varepsilon_L q_L^{\frac{1-s}{2}} \gamma_L(1-s) \sum_{n \geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_s\left(\frac{nX}{\sqrt{q_L}}\right) + \Lambda(s, L) + R(s, X, L).$$

Equating these two evaluations and isolating the completion gives

$$\begin{aligned}\Lambda(s, L) = q_L^{\frac{s}{2}} \gamma_L(s) \sum_{n \geq 1} \frac{a_L(n)}{n^s} V_s\left(\frac{n}{\sqrt{q_L} X}\right) \\ + \varepsilon_L q_L^{\frac{1-s}{2}} \gamma_L(1-s) \sum_{n \geq 1} \frac{\overline{a_L(n)}}{n^{1-s}} V_{1-s}\left(\frac{nX}{\sqrt{q_L}}\right) + R(s, X, L).\end{aligned}$$

Diving by $q_L^{\frac{s}{2}} \gamma_L(s)$ completes the proof. □

Let us now show how $V_s(y)$ has the effect of dampening the two dual sums appearing on the right-hand side of the approximate functional equation. In practice, it is common to choose $\Phi(u)$ such that it has exponential decay and we can make the vertical strip on which it is bounded arbitrarily wide. For example, let

$$\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right),$$

for some positive integer M. Clearly $\Phi(u)$ is an even holomorphic function in the vertical strip $|\tau| < (2M-1)+1$ and satisfies $\Phi(0) = 1$. In view of the identity $\cos(u) = \frac{e^{iu}+e^{-iu}}{2}$, we find that

$$\cos^{-4d_L M}\left(\frac{\pi u}{4M}\right) \ll_\varepsilon e^{-d_L \pi |r|}, \tag{8.5}$$

for $|\tau| < (2M-1)+1$ provided u is at least distance ε away from the poles of $\Phi(u)$. Therefore $\Phi(u)$ admits exponential decay. For this choice of $\Phi(u)$, $V_s(y)$ and its derivatives will possess rapid decay.

Proposition 8.2.2. *Let $L(s)$ be an analytic L-function, set $\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right)$ for some positive integer M, and let $V_s(y)$ be the inverse Mellin transform defined by*

$$V_s(y) = \frac{1}{2\pi i} \int_{(2M-1)} \frac{\gamma_L(s+u)}{\gamma_L(s)} \Phi(u) y^{-u} \frac{du}{u}.$$

Then for s in the critical strip, any nonnegative integer k, and positive integer N with $N < 2M$, $V_s(y)$ satisfies the estimates

$$(-y)^k V_s^{(k)}(y) = \begin{cases} \delta_{k,0} + O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^N\right) & \text{if } y \ll \sqrt{\mathfrak{q}_\infty(s,L)}, \\ O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}\right) & \text{if } y \gg \sqrt{\mathfrak{q}_\infty(s,L)}. \end{cases}$$

In particular,

$$(-y)^k V_s^{(k)}(y) \ll_\varepsilon \left(1 + \frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}.$$

Proof. As we have already seen, the integrand defining $V_s(y)$ admits exponential decay. This permits us to differentiate under the integral sign and shift the line of integration. The former shows

$$(-y)^k V_s^{(k)}(y) = \frac{1}{2\pi i}\int_{(2M-1)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

Shifting to $(-N)$, we pass by a simple pole at $u = 0$ of residue 1 if and only if $k = 0$. This gives

$$(-y)^k V_s^{(k)}(y) = \delta_{k,0} + \frac{1}{2\pi i}\int_{(-N)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

This integrand also exhibits exponential decay since the Pochhammer symbol grows polynomially. Therefore the integral is dominated by the contribution when $u \ll 1$ and the Equations (8.4) and (8.5) together show

$$(-y)^k V_s^{(k)}(y) = \delta_{k,0} + O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^N\right).$$

If we instead shift to (N), we do not pass by any poles and obtain

$$(-y)^k V_s^{(k)}(y) = \frac{1}{2\pi i}\int_{(N)} \frac{\gamma_L(s+u)}{\gamma_L(s)}\Phi(u)(u)_k y^{-u}\frac{du}{u}.$$

An analogous argument to estimate the remaining integral shows

$$(-y)^k V_s^{(k)}(y) = O_\varepsilon\left(\left(\frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}\right).$$

From these O-estimates we obtain nontrivial bounds in the ranges $y \ll \sqrt{\mathfrak{q}_\infty(s,L)}$ and $y \gg \sqrt{\mathfrak{q}_\infty(s,L)}$ respectively. Combining both of these estimates produces the bound

$$(-y)^k V_s^{(k)}(y) \ll_\varepsilon \left(1 + \frac{y}{\sqrt{\mathfrak{q}_\infty(s,L)}}\right)^{-N}.$$

□

With our choice of $\Phi(u)$, this result shows that $V_s(y)$ is essentially 1 up to some admissible error for $y \ll \sqrt{\mathfrak{q}_\infty(s, L)}$ and exhibits rapid decay thereafter as we can take M (and hence N) to be arbitrarily large.

In a similar spirit to the approximate functional equation, a useful summation formula can be derived from the functional equation. Let $\psi(y)$ be a smooth weight where $\Psi(s)$ is its Mellin transform. Then we will let $\psi(y, L)$ be the inverse Mellin transform

$$\psi(y, L) = \frac{1}{2\pi i} \int_{(a)} q_L^s \frac{\gamma_L(s)}{\gamma_L(1-s)} y^{-s} \Psi(1-s)\, ds,$$

defined for $y > 0$ where $a > 1$. By our choice of $\psi(y)$, its inverse Mellin transform $\Psi(s)$ has rapid decay. Since $L(s)$ has at most polynomial growth by Proposition 8.2.1, the integrand has rapid decay as well. Therefore the integral is locally absolutely uniformly bounded and hence $\psi(y, L)$ is smooth for $y > 0$. Our result is the following:

Theorem 8.2.3. *Let $L(s)$ be an analytic L-function and let $\psi(y)$ be a smooth weight where $\Psi(s)$ is its Mellin transform. Then*

$$\sum_{n \geq 1} a_L(n)\psi(n) = \frac{\varepsilon_L}{\sqrt{q_L}} \sum_{n \geq 1} \overline{a_L(n)}\psi(n, L) + R(L)\Psi(1),$$

where $R(L)$ is given by

$$R(L) = \operatorname*{Res}_{s=1} L(s).$$

Proof. Smoothed Perron's formula implies

$$\sum_{n \geq 1} a_L(n)\psi(n) = \frac{1}{2\pi i} \int_{(a)} L(s)\Psi(s)\, ds.$$

By our choice of $\psi(y)$, its inverse Mellin transform $\Psi(s)$ has rapid decay. Since $L(s)$ has at most polynomial growth by Proposition 8.2.1, the integrand has rapid decay as well. Therefore the integral is locally absolutely uniformly bounded which permits us to shift the line of integration. Shifting to $(1-a)$, we pass by a potential pole at $s = 1$ and obtain

$$\sum_{n \geq 1} a_L(n)\psi(n) = \frac{1}{2\pi i} \int_{(1-a)} L(s)\Psi(s)\, ds + R(L)\Psi(1).$$

Apply the functional equation to rewrite this equality in the form

$$\sum_{n \geq 1} a_L(n)\psi(n) = \frac{1}{2\pi i} \int_{(1-a)} \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)} \overline{L(1-\overline{s})}\Psi(s)\, ds + R(L)\Psi(1).$$

Performing the change of variables $s \mapsto 1 - s$ in this latter integral gives

$$\sum_{n \geq 1} a_L(n)\psi(n) = \frac{1}{2\pi i} \int_{(a)} \varepsilon_L q_L^{s-\frac{1}{2}} \frac{\gamma_L(s)}{\gamma_L(1-s)} \overline{L(\overline{s})}\Psi(1-s)\, ds + R(L)\Psi(1).$$

The proof is complete upon expanding $\overline{L(\overline{s})}$ as a Dirichlet series, interchanging the sum and integral by absolute boundedness of the integral, and factoring out $\frac{\varepsilon_L}{\sqrt{q_L}}$. $\square$

8.3 The Riemann Hypothesis and Nontrivial Zeros

The zeros of an L-functions $L(s)$ has interesting behavior. From the Euler product we immediately see that $L(s)$ has no zeros in the half-plane $\sigma > 1$. We can use the functional equation to determine the zeros for $\sigma < 0$. Indeed, write the functional equation in the form

$$L(s) = \varepsilon_L q_L^{\frac{1}{2}-s} \frac{\gamma_L(1-s)}{\gamma_L(s)} \overline{L(1-\overline{s})}.$$

So for $\sigma < 0$, we see that $\overline{L(1-\overline{s})}$ is nonzero. Moreover, $\gamma_L(1-s)$ is as well. Together this means that for $\sigma < 0$ the poles of $\gamma_L(s)$ are zeros of $L(s)$. Such a zero is called a **trivial zero** of $L(s)$. From the definition of the gamma factor, they are all simple and of the form $s = -(\mu_j + 2n)$ for some gamma parameter μ_j and some nonnegative integer n.

Any other zero of $L(s)$ is called a **nontrivial zero** and it necessarily lies inside of the critical strip. Let ρ be a nontrivial zero of $L(s)$. Then the functional equation implies that $1 - \overline{\rho}$ is also a nontrivial zero of $L(s)$. This means that nontrivial zeros occur in pairs

$$\rho \quad \text{and} \quad 1 - \overline{\rho}.$$

It is possible to say more when $L(s)$ takes real values for $s > 1$. For in this case, the Schwarz reflection principle implies $L(\overline{s}) = \overline{L(s)}$ and that $L(s)$ takes real values on the entire real axis save for the possible pole at $s = 1$. It follows from the functional equation that $\overline{\rho}$ and $1 - \rho$ are also nontrivial zeros. Therefore the nontrivial zeros of $L(s)$ come in sets of four

$$\rho, \quad \overline{\rho}, \quad 1 - \rho, \quad \text{and} \quad 1 - \overline{\rho}.$$

See Figure 8.2 for an example of this symmetry.

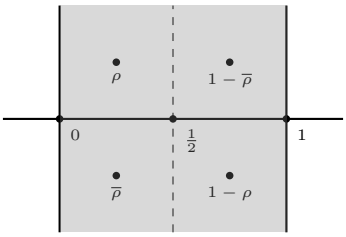

Figure 8.2: Symmetric nontrivial zeros.

The **Riemann hypothesis** for $L(s)$ says that this symmetry should be as simple as possible.

Conjecture (Riemann hypothesis, $L(s)$). *The nontrivial zeros of the analytic L-function $L(s)$ all lie on the vertical line $\sigma = \frac{1}{2}$.*

While stated as a conjecture, we not expect the Riemann hypothesis to hold for just any analytic L-function. We do however expect it to hold for Selberg class L-functions. In particular, the **Selberg class Riemann hypothesis** says that this symmetry should hold for any Selberg class L-function:

Conjecture (Selberg class Riemann hypothesis). *The nontrivial zeros of any Selberg class L-function $L(s)$ lie on the vertical line $\sigma = \frac{1}{2}$.*

So far, the Riemann hypothesis remains completely out of reach for any analytic L-function and thus the Selberg class Riemann hypothesis does as well.

8.4 The Lindelöf Hypothesis and Estimates on the Critical Line

Instead of asking about the zeros of an analytic L-function $L(s)$ on the critical line we can ask about its growth there. Let us begin this investigation by deriving an upper bound for $L(s)$ on the critical line using the Phragmén-Lindelöf convexity principle. This amounts to a more refined version of the argument used in Proposition 8.2.1 for the critical strip.

Theorem 8.4.1. *Let $L(s)$ be an analytic L-function. Then for $-\varepsilon \leq \sigma \leq 1+\varepsilon$, we have*

$$L(s) \ll_\varepsilon \mathfrak{q}(s, L)^{\frac{1-\sigma}{2}+\varepsilon},$$

provided s is at least distance ε away from the possible pole at $s = 1$.

Proof. Since $(s-1)^{r_L} L(s)$ is entire and of order 1, we will apply the Phragmén-Lindelöf convexity principle just outside the edges of the critical strip. Just past the right edge along the vertical line $\sigma = 1+\varepsilon$, we have

$$(s-1)^{r_L} L(s) \ll_\varepsilon (s-1)^{r_L}.$$

Just past the left edge along the vertical line $\sigma = -\varepsilon$, the functional equation and Equation (8.2) together imply the bound

$$(s-1)^{r_L} L(s) \ll_\varepsilon (s-1)^{r_L} \mathfrak{q}(s, L)^{\frac{1}{2}+\varepsilon}.$$

By the Phragmén-Lindelöf convexity principle, we obtain

$$(s-1)^{r_L} L(s) \ll_\varepsilon (s-1)^{r_L} \mathfrak{q}(s, L)^{\frac{1-\sigma}{2}+\varepsilon},$$

provided $-\varepsilon \leq \sigma \leq 1+\varepsilon$. Assuming s is at least distance ε away from the possible pole at $s = 1$, dividing by $(s-1)^{r_L}$ completes the proof. □

At the critical line this theorem produces the bound

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t, L\right)^{\frac{1}{4}+\varepsilon}.$$

This is known as the **convexity bound** for $L(s)$. The **Lindelöf hypothesis** for $L(s)$ says that the exponent can be reduced to ε:

Conjecture (Lindelöf hypothesis, $L(s)$). *The analytic L-function $L(s)$ satisfies*

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^\varepsilon.$$

Unlike the Riemann hypothesis, the Lindelöf hypothesis is expected to hold for any analytic L-function. In any case, the **Selberg class Lindelöf hypothesis** says that the exponent can be reduced to ε for any Selberg class L-function:

Conjecture (Selberg class Lindelöf hypothesis). *Any Selberg class L-function $L(s)$ satisfies*

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^\varepsilon.$$

Like the Riemann hypothesis, we have been unable to prove the Lindelöf hypothesis for any analytic L-function. However, in practice the Lindelöf hypothesis is more tractable. Generally speaking, any improvement upon the exponent in the convexity bound in any aspect of the analytic conductor is called a **subconvexity estimate** (or a **convexity breaking bound**). In the uniform case, we would like to prove bounds of the form

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^{\delta+\varepsilon},$$

for some $0 \leq \delta \leq \frac{1}{4}$. The convexity bound says that we may take $\delta = \frac{1}{4}$ while the Lindelöf hypothesis for $L(s)$ implies that we may take $\delta = 0$. Any uniform subconvexity estimate would give a δ strictly less than $\frac{1}{4}$. Subconvexity estimates are viewed with great interest. This is primarily because of their connection to the Lindelöf hypothesis, but also because any improvement upon the convexity bound in any aspect of the analytic conductor often has drastic consequences in applications.

Remark 8.4.2. Some subconvexity bounds are deserving of names. The cases $\delta = \frac{3}{16}$ and $\delta = \frac{1}{6}$ are referred to as the **Burgess bound** and **Weyl bound** respectively.

With a little more work, we can obtain a a similar bound for the derivatives of analytic L-functions. First observe that Theorem 8.4.1 gives the estimate

$$L(s) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^{\frac{1}{4}+\varepsilon},$$

in the vertical strip $\left|\sigma - \frac{1}{2}\right| \leq \frac{\varepsilon}{2}$. This is just slightly stronger than the convexity bound. By Cauchy's integral formula, we may write

$$L^{(k)}\left(\frac{1}{2}+it\right) = \frac{k!}{2\pi i}\int_\eta \frac{L(s)}{(s-\frac{1}{2}-it)^{k+1}}\,ds,$$

where η is the circle about $\frac{1}{2}+it$ of radius $\frac{\varepsilon}{2}$. The parameterization $u \mapsto \frac{1}{2}+it+\frac{\varepsilon}{2}e^{i\theta}$ for η shows that

$$L^{(k)}\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}\left(t,L\right)^{\frac{1}{4}+\varepsilon}.$$

This is known as the **convexity bound** for $L^{(k)}(s)$.

We now turn to the question of how to obtain estimates on the critical line. There are many methods one can apply often depending upon the particular analytic L-function of interest. Here we will provide a method that works in vast generality and reduces the estimation of $L\left(\frac{1}{2}+it\right)$ to that of estimating smoothed finite sums of coefficients. To achieve this we need to establish the existence of certain bump functions. We say that a function $\omega(y)$ is a **smooth dyadic weight** if it is a positive bump function supported in $[1-\delta, 2+\delta]$ and such that

$$\sum_{k\in\mathbb{Z}} \omega\left(\frac{y}{2^k}\right) = 1,$$

for all positive y. This last condition means $\left(\omega\left(\frac{y}{2^k}\right)\right)_{k\in\mathbb{Z}}$ is a partition of unity on $(0,\infty)$. To see that dyadic weights exist, let $\psi(y)$ be a smooth weight that is identically 1 on $[1,2]$ and supported in $[1-\delta, 2+\delta]$. Write

$$\sigma(y) = \sum_{k\in\mathbb{Z}} \psi\left(\frac{y}{2^k}\right).$$

Then $\sigma(y)$ is finite as finitely many of its summands are nonzero since any positive y satisfies $2^k \leq y < 2^{k+1}$ for some unique integer k. This forces $\sigma(y)$ to be smooth and bounded. It is also bounded away from zero as $\sigma(y) \geq 1$ because $\psi(y)$ is identically 1 on $[1,2]$. Then we may take

$$\omega(y) = \frac{\psi(y)}{\sigma(y)}.$$

This shows that smooth dyadic weights exist. For any $t \in \mathbb{R}$ and $X > 0$, set

$$A_\omega(t, X, L) = \sum_{n\geq 1} a_L(n) n^{-it} \omega\left(\frac{n}{X}\right).$$

and write

$$A_\omega(X, L) = A_\omega(0, X, L).$$

Our result estimates $L(s)$ at $s = \frac{1}{2}+it$ in terms of $A_\omega(t, X, L)$.

Theorem 8.4.3. *Let $L(s)$ be an analytic L-function and let $\omega(y)$ be a smooth dyadic weight. Then*

$$L\left(\frac{1}{2}+it\right) \ll_\varepsilon \mathfrak{q}(t, L)^\varepsilon \sup_{X \ll \sqrt{\mathfrak{q}(t,L)}} \left(\frac{|A_\omega(t, X, L)|}{\sqrt{X}}\right).$$

Proof. Take $s = \frac{1}{2}+it$, $X = 1$, and $\Phi(u) = \cos^{-4d_L M}\left(\frac{\pi u}{4M}\right)$ for some large positive integer M in the approximate functional equation. This permits us to write

$$L\left(\frac{1}{2}+it\right) = \sum_{n\geq 1} \frac{a_L(n) n^{-it}}{\sqrt{n}} V_t\left(\frac{n}{\sqrt{q_L}}\right) + \varepsilon_L(t) \sum_{n\geq 1} \frac{\overline{a_L(n)} n^{it}}{\sqrt{n}} V_t\left(\frac{n}{\sqrt{q_L}}\right) + \frac{R\left(\frac{1}{2}+it, 1, L\right)}{q_L^{\frac{1}{4}+i\frac{t}{2}} \gamma_L\left(\frac{1}{2}+it\right)}.$$

Equation (8.2) implies $\varepsilon_L(t) \ll 1$ while Equations (8.1) and (8.5) together imply that the residue term exhibits exponential decay. This implies that right-hand side of the approximate functional equation is

$$O\left(\sum_{n\geq 1}\frac{a_L(n)n^{-it}}{\sqrt{n}}V_t\left(\frac{n}{\sqrt{q_L}}\right)\right)+O\left(\sum_{n\geq 1}\frac{\overline{a_L(n)}n^{it}}{\sqrt{n}}V_{-t}\left(\frac{n}{\sqrt{q_L}}\right)\right)+O(e^{-|t|}).$$

We now turn to estimating the remaining sums which will be accomplished by applying the smooth dyadic weight. Consider the first sum. By our choice of $\Phi(u)$, the estimates in Proposition 8.2.2 are valid which implies that the summands exhibit rapid decay for $n \gg \sqrt{\mathfrak{q}(t,L)}$. Whence the sum is say

$$\sum_{n\ll\sqrt{\mathfrak{q}(t,L)}}\frac{a_L(n)n^{-it}}{\sqrt{n}}V_t\left(\frac{n}{\sqrt{q_L}}\right)+O_\varepsilon\left(\mathfrak{q}(t,L)^\varepsilon\right)$$

Now write

$$V_s(y)=\sum_{k\in\mathbb{Z}}\omega\left(\frac{y}{2^k}\right)V_s(y).$$

Apply this identity to the sum and interchange the resulting two sums by local finiteness to obtain

$$\sum_{k\in\mathbb{Z}}\sum_{n\ll\sqrt{\mathfrak{q}(t,L)}}\frac{a_L(n)n^{-it}}{\sqrt{n}}\omega\left(\frac{n}{2^k\sqrt{q_L}}\right)V_t\left(\frac{n}{\sqrt{q_L}}\right).$$

By compact support of the smooth dyadic weight, for each k the inner sum over n is supported on the dyadic block $n \asymp X_k$ where $X_k = 2^k\sqrt{q_L}$. As $n \ll \sqrt{\mathfrak{q}(t,L)}$, the summands which contribute must satisfy $k \ll \log \mathfrak{q}_\infty(t,L)$. Therefore our double sum can be expressed as

$$\sum_{k\ll\log\mathfrak{q}_\infty(t,L)}\sum_{n\asymp X_k}\frac{a_L(n)n^{-it}}{\sqrt{n}}\omega\left(\frac{n}{X_k}\right)V_t\left(\frac{n}{\sqrt{q_L}}\right).$$

Let $V_k(y)=\frac{1}{\sqrt{y}}V_t\left(\frac{y}{\sqrt{q_L}}\right)$. By Abel summation, the inner sum is O of

$$\sup_{n\asymp X_k}|A_\omega(X_k,t,L)|\,|V_k(n)|+\int_{u\asymp X_k}|A_\omega(u,t,L)||V_k'(u)|\,du.$$

In view of Proposition 8.2.2, we have the estimates

$$V_k(y)=O\left(\frac{1}{\sqrt{y}}\right)\quad\text{and}\quad V_k'(y)=O\left(\frac{1}{y^{\frac{3}{2}}}\right),$$

for $y \ll \sqrt{\mathfrak{q}(t,L)}$. Whence our previous expression is O of

$$\sup_{X\asymp X_k}\left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right).$$

As there are $O_\varepsilon\left(\mathfrak{q}\left(t,L\right)^\varepsilon\right)$ many such k, the bound above implies that our sum is O_ε of

$$\mathfrak{q}\left(t,L\right)^\varepsilon \sup_{X\ll\sqrt{\mathfrak{q}(t,L)}}\left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right).$$

The estimate for the second sum is treated analogously. Thus

$$L\left(\frac{1}{2}+it\right)\ll_\varepsilon \mathfrak{q}\left(t,L\right)^\varepsilon \sup_{X\ll\sqrt{\mathfrak{q}(t,L)}}\left(\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\right),$$

upon absorbing smaller order error terms. □

As any useful estimate for the sum $A_\omega(t,X,L)$ will be in terms of powers of X, the supremum in Theorem 8.4.4 will automatically pick out the largest possible bound when X is the square root of the analytic conductor. This means that the savings of $\sqrt{X}$ in the denominator is essentially as large as possible. For example, we obtain the convexity bound as an application. Since the Dirichlet series of $L(s)$ is absolutely convergent for $\sigma<1$, we have a bound of shape

$$\sum_{n\leq X}|a_L(n)|\ll_\varepsilon X^{1+\varepsilon}.$$

Then $A_\omega(t,X,L)\ll_\varepsilon X^{1+\varepsilon}$ as well and we obtain

$$\sup_{X\ll\sqrt{\mathfrak{q}(t,L)}}\frac{|A_\omega(t,X,L)|}{\sqrt{X}}\ll_\varepsilon \mathfrak{q}\left(t,L\right)^{\frac{1}{4}+\varepsilon}, \tag{8.6}$$

which gives the convexity bound. As we believe $L(s)$ satisfies the Lindelöf hypothesis, we should expect lots of cancellation in the sum $A_\omega(t,X,L)$. In fact, the expected cancellation should be $O\left(\mathfrak{q}\left(t,L\right)^{\frac{1}{4}}\right)$ in light of the aforementioned bound. This means we expect $A_\omega(t,X,L)$ to exhibit square-root cancellation in the sense

$$A_\omega(t,X,L)\ll_\varepsilon X^{\frac{1}{2}+\varepsilon}.$$

As the coefficients $a_L(n)$ may very well be real, the expected cancellation must come from the terms $n^{-it}=e^{-it\log(n)}$ which acts on the coefficients $a_L(n)$ by rotation. In effect, we should think of the terms $a_L(n)n^{-it}$ as modeling identically distributed random variables.

The case when $t=0$ is deserving of unique importance. In this case, we are estimating the value of $L(s)$ at the central point. The value of $L(s)$ at the central point is called the **central value** of $L(s)$. Many important properties about $L(s)$ can be connected to its central value. Any argument used to estimate the central value of an L-function is called a **central value estimate**. Taking $t=0$ in Theorem 8.4.3 gives a way to obtain central value estimates.

Theorem 8.4.4. *Let $L(s)$ be an analytic L-function and let $\omega(y)$ be a smooth dyadic weight. Then*

$$L\left(\frac{1}{2}\right)\ll_\varepsilon \mathfrak{q}\left(L\right)^\varepsilon \max_{X\ll\sqrt{\mathfrak{q}(L)}}\left(\frac{|A_\omega(X,L)|}{\sqrt{X}}\right).$$

Proof. Take $t=0$ in Theorem 8.4.3. □

8.5 Logarithmic Derivatives

Recall that $L(s)$ nonzero in the half-plane $\sigma > 1$. As this region is simply connected, there exists a unique holomorphic logarithm $\log L(s)$ there. By absolute convergence of the Euler product, we may write

$$\log L(s) = -\sum_p \sum_j \log(1 - \alpha_j(p)p^{-s}).$$

Moreover, the bound $|\alpha_j(p)| \leq p^\theta$ ensures that $|\alpha_j(p)p^{-s}| < 1$ in this half-plane. Therefore the Taylor series of the logarithm is valid in this region and we may further write

$$\log L(s) = \sum_p \sum_j \sum_{k \geq 1} \frac{\alpha_j(p)^k}{kp^{ks}}.$$

While this triple sum converges for $\sigma > 1$, the bound $|\alpha_j(p)p^{-s}| < p^{\theta-\sigma}$ only guarantees absolutely convergence for $\sigma > 1 + \theta$. It is in this half-plane that we may differentiate termwise. A short computation shows

$$\frac{L'}{L}(s) = -\sum_{n \geq 1} \frac{\Lambda_L(n)}{n^s},$$

where

$$\Lambda_L(n) = \begin{cases} \sum_j \alpha_j(p)^k \log(p) & \text{if } n = p^k, \\ 0 & \text{otherwise.} \end{cases}$$

We call $\Lambda_L(n)$ the **Von Mangoldt coefficients** of $L(s)$.

There is an incredibly useful formula for the logarithmic derivative of $L(s)$ which is often the starting point for deeper analytic investigations. To deduce it, we require a more complete understanding of the completion $\Lambda(s, L)$. First observe that the zeros ρ of $\Lambda(s, L)$ are contained within the critical strip. Indeed, by our earlier discussion of zeros, $\Lambda(s, L)$ is nonzero for $\sigma > 1$ and the functional equation implies that $\Lambda(s, L)$ is nonzero for $\sigma < 0$ too. This means that the zeros of $\Lambda(s, L)$ are exactly nontrivial zeros of $L(s)$. Now let us setup some notation. We define $\xi(s, L)$ by

$$\xi(s, L) = (s(1 - s))^{r_L} \Lambda(s, L).$$

Then $\xi(s, L)$ is just $\Lambda(s, L)$ with the potential poles at $s = 0$ and $s = 1$ removed. This means $\xi(s, L)$ is entire. The functional equation also implies

$$\xi(s, L) = \varepsilon_L \overline{\xi(1 - \overline{s}, L)}.$$

Our result will compute the Hadamard factorization of $\xi(s, L)$ and taking its logarithmic derivative will give a formula relating the logarithmic derivative of $L(s)$ to the zeros of $L(s)$.

Proposition 8.5.1. *For any analytic L-function $L(s)$, there exist constants A_L and B_L such that*

$$\xi(s,L) = e^{A_L + B_L s} \prod_{\rho \neq 0,1} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

and hence the sum

$$\sum_{\rho \neq 0,1} \frac{1}{|\rho|^{1+\varepsilon}},$$

is convergent provided the product and sum are both counted with multiplicity and ordered with respect to the size of the ordinate. Moreover,

$$-\frac{L'}{L}(s) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) - B_L - \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Proof. Recall that $\xi(s,L)$ is entire and its zeros are exactly the nontrivial zeros of $L(s)$. We claim $\xi(s,L)$ is of order 1. This follows from Stirling's formula and that $(s-1)^{r_L} L(s)$ is of order 1. Then the Hadamard factorization theorem implies

$$\xi(s,L) = e^{A_L + B_L s} \prod_{\rho \neq 0,1} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}},$$

for some constants A_L and B_L and that the desired sum converges. This proves the first statement. We will compute the logarithmic derivative of $\xi(s,L)$ in two ways to prove the second statement. On the one hand, taking the logarithmic derivative of the definition of $\xi(s,L)$ yields

$$\frac{\xi'}{\xi}(s,L) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) + \frac{L'}{L}(s).$$

On the other hand, taking the logarithmic derivative of the Hadamard factorization gives

$$\frac{\xi'}{\xi}(s,L) = B_L + \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Equating these expressions to obtain

$$B_L + \sum_{\rho \neq 0,1} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) = \frac{r_L}{s} + \frac{r_L}{s-1} + \frac{1}{2}\log q_L + \frac{\gamma_L'}{\gamma_L}(s) + \frac{L'}{L}(s).$$

This is equivalent to the second statement. □

Explicit evaluation of the constants A_L and B_L can be challenging and heavily depend upon the particular L-function under investigation. However, useful estimates are not too difficult to obtain and this is often sufficient for applications.

Chapter 9

Todo: [Moments]

Chapter 10

Todo: [Analytic Theory of the Riemann Zeta Function]

Chapter 11

Todo: [Analytic Theory of Dirichlet L-functions]

Chapter 12

Todo: [Analytic Theory of Dedekind Zeta Functions]

Part IV

Appendices

Index