Number Theory

February 15, 2023

Contents

Part I
Algebraic Number Theory

1 Ideal Factorization

Definition 1.1. For ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a commutative ring, write $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ for an ideal $\mathfrak{c}$.

If $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{a} \supset \mathfrak{b}$. The converse may fail in some rings, but in the ring of integers of a number field it will turn out that containment implies divisibility.

Theorem 1.1. *In any commutative ring A, an ideal $\mathfrak{p}$ is prime if and only if for all ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A,*

$$\mathfrak{p} \supset \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \supset \mathfrak{a} \text{ or } \mathfrak{p} \supset \mathfrak{b}. \tag{1}$$

Proof. Suppose $\mathfrak{p} \supset \mathfrak{a}\mathfrak{b}$ and $\mathfrak{p} \not\supset \mathfrak{a}$. Choose $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}$. For every element $y \in \mathfrak{b}$, $xy \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$, we must have $y \in \mathfrak{p}$, for every $y \in \mathfrak{b}$. So $\mathfrak{p} \supset \mathfrak{b}$. Conversely, suppose $\mathfrak{p}$ is an ideal in A which satisfies the property (1) for all ideals $\mathfrak{a}$ and $\mathfrak{b}$ in A. If $xy \in \mathfrak{p}$ for some $x, y \in A$, then $\mathfrak{p} \supset (xy) = (x)(y)$, and so $\mathfrak{p}$ contains either (x) or (y), which means either x or y is in $\mathfrak{p}$. □

Corollary 1. *Let K be a number field. In $\mathcal{O}_K$, if $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where all the ideals are nonzero and prime, then for some i, $\mathfrak{p} = \mathfrak{p}_i$..*

Proof. By Theorem 1.1, $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Since nonzero prime ideals in $\mathcal{O}_K$ are maximal, $\mathfrak{p} = \mathfrak{p}_\mathrm{i}$. □

Definition 1.2. A **fractional ideal** I in K is a nonzero $\mathcal{O}_K$-submodule of K such that for some $d \in \mathcal{O}_K \setminus \{0\}$, $dI \subset \mathcal{O}_K$. Such a d is called a **common denominator** for I.

Theorem 1.2. *The following properties of an $\mathcal{O}_K$-submodule of K are equivalent:*

1. *I is a fractional ideal.*
2. *$dI \subset \mathcal{O}_K$ for some $d \in \mathbb{Z} \setminus \{0\}$.*
3. *$I = x\mathfrak{a}$ for some $x \in K^\times$ and some nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$.*
4. *I is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.*

Proof. $(1 \Rightarrow 2)$: Since I is a fractional ideal, there is a $c \in \mathcal{O}_K \setminus \{0\}$ such that $cI \subset \mathcal{O}_K$. Set $d = N_{K/\mathbb{Q}}(c) \in \mathbb{Z} \setminus \{0\}$. Since $c \mid d$, we also have $dI \subset \mathcal{O}_K$. $(2 \Rightarrow 3)$: dI is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$, thus it must be some nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$. Set $x = \frac{1}{d}$. Then $x\mathfrak{a} = \frac{1}{d}(dI) = I$. $(3 \Rightarrow 4)$: Since $\mathcal{O}_K$ is noetherian, $\mathfrak{a}$ is finitely generated, which implies I is finitely generated too. $(4 \Rightarrow 1)$: Write $I = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n})$ where $a_i, b_i \in \mathcal{O}_K$ for $1 \le i \le n$. Set $d = b_1 \cdots b_n$. Then $dI \subset \mathcal{O}_K$. □

Definition 1.3. For a fractional ideal I in $\mathcal{O}_K$, set

$$\tilde{I} = \{x \in K \mid xI \subset \mathcal{O}_K\} = \mathcal{O}_K :_K I$$

$\tilde{I}$ is a fractional ideal in K. To see this, choose any $y \in I$, then $y\tilde{I} \subset \mathcal{O}_K$, so $\tilde{I} \subset (1/y)\mathcal{O}_K$. Therefore $\tilde{I}$ is a submodule of a finite free $\mathbb{Z}$-module, so $\tilde{I}$ is a finitely generated $\mathbb{Z}$-module, hence finitely generated as an $\mathcal{O}_K$-module too.

Proposition 1.1. $\tilde{I} \cong Hom_{\mathcal{O}_K}(I, \mathcal{O}_K)$

Proof. Suppose $c \in \tilde{I}$. Then multiplication by c is an $\mathcal{O}_K$-linear map from I to $\mathcal{O}_K$. Conversely, suppose$\varphi \in Hom_{\mathcal{O}_K}(I, \mathcal{O}_K)$. We need to show that φ has the form $\varphi(x) = cx$ for some $c \in K$ and for all $x \in I$. In other words, we need to show that $\varphi(x)/x$ is independent of x:

$$\frac{\varphi(x)}{x} \stackrel{?}{=} \frac{\varphi(y)}{y} \iff y\varphi(x) \stackrel{?}{=} x\varphi(y) \qquad \forall x, y \in I.$$

We can't pull in the x and y inside φ yet since x and y may not lie in $\mathcal{O}_K$. Since I is a fractional ideal though, we know that there exists a nonzero $d \in \mathcal{O}_K$ such that $dx, dy \in \mathcal{O}_K$. Choose such a d. Then since I is torsion-free, we have

$$y\varphi(x) - x\varphi(y) \stackrel{?}{=} 0 \iff d(y\varphi(x) - x\varphi(y)) \stackrel{?}{=} 0 \iff \varphi(dyx) - \varphi(dxy) \stackrel{\checkmark}{=} 0 \qquad \forall x, y \in I.$$

□

Theorem 1.3. *Let I be a fractional ideal in the number field K. If I admits a fractional ideal inverse then the inverse must be $\tilde{I}$.*

Proof. Let J be a multiplicative inverse of I. Certainly we have $J \subset \tilde{I}$ since for each $j \in J$, $jI \subset \mathcal{O}_K$. Conversely, since $IJ = \mathcal{O}_K$, we have $i_1 j_1 + \cdots + i_n j_n = 1$ where $i_1, \ldots, i_n \in I$ and $j_1, \ldots j_n \in J$. Then given $x \in \tilde{I}$, we have $(xi_1)j_1 + \cdots (xi_n)j_n = x$, where $xi_1, \ldots xi_n \in \mathcal{O}_K$, and so $x \in J$. □

Proposition 1.2. *Let A be a Noetherian ring and let $\mathfrak{a}$ be a nonzero ideal in A. Then $\mathfrak{a}$ contains a product of prime ideals.*

Proof. Assume for a contradiction that $\mathfrak{a}$ does not contain a product of prime ideals. Let $\mathcal{S}$ denote the set of all nonzero ideals in A which do not contain a product of prime ideals. Note that $\mathcal{S}$ is nonempty since $\mathfrak{a} \in \mathcal{S}$ and note that $A \notin \mathcal{S}$ since every ring contains a prime ideal (let alone a product of prime ideals). Since A is a Noetherian ring, we see that $\mathcal{S}$ has a maximal element. Choose $\mathfrak{b} \in \mathcal{S}$ to be such a maximal element. Now $\mathfrak{b}$ cannot be a prime ideal since it would then contain itself as a prime ideal. In particular, there exists $a, b \in A$ such that $ab \in \mathfrak{b}$ and neither a nor b is in $\mathfrak{b}$. By maximality of $\mathfrak{b}$, we see that $\mathfrak{b} + \langle a \rangle \notin \mathcal{S}$ and $\mathfrak{b} + \langle b \rangle \notin \mathcal{S}$. In particular, both $\mathfrak{b} + \langle a \rangle$ and $\mathfrak{b} + \langle b \rangle$ contains a product of prime ideals respectively, say

$$\mathfrak{b} + \langle a \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_m \quad \text{and} \quad \mathfrak{b} + \langle b \rangle = \mathfrak{q}_1 \cdots \mathfrak{q}_n.$$

Then observe that

$$\begin{aligned} \mathfrak{p}_1 \cdots \mathfrak{p}_m \mathfrak{q}_1 \cdots \mathfrak{q}_n &= (\mathfrak{b} + \langle a \rangle)(\mathfrak{b} + \langle b \rangle) \\ &= \mathfrak{b}^2 + \mathfrak{b}\langle b \rangle + \langle a \rangle \mathfrak{b} + \langle ab \rangle \\ &\subseteq \mathfrak{b}. \end{aligned}$$

This contradicts the fact that $\mathfrak{b} \in \mathcal{S}$. □

Lemma 1.4. *Every nonzero ideal in $\mathcal{O}_K$ contains a product of prime ideals.*

Proof. First, we show that every nonzero ideal of $\mathcal{O}_K$ has finite index (this requires knowledge of finitely generated modules over PID's). Suppose $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$. Choose a nonzero element $a \in \mathfrak{a}$. Then we have inclusions

$$a\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$$

$\mathcal{O}_K$ and $a\mathcal{O}_K$ are both free $\mathbb{Z}$-modules of rank n, so $\mathfrak{a}$ must be free of rank n as well. If $\{e_1, \ldots, e_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, and $\{f_1, \ldots, f_n\}$ is a $\mathbb{Z}$-basis of $\mathfrak{a}$, where $f_i = \sum a_{ji} e_j$, then

$$|\mathcal{O}_K / \mathfrak{a}| = \det(a_{ji})$$

which is clearly finite. Now assume the lemma is false and let $\mathfrak{a}$ be a nonzero ideal of least index which does not contain a product of primes. Then $\mathfrak{a} \neq \mathcal{O}_K$ since $\mathcal{O}_K$ contains nonzero prime ideals, so $[\mathcal{O}_K : \mathfrak{a}] \geq 2$. Since $\mathfrak{a}$ is not a prime ideal, there exists $x, y \in \mathcal{O}_K$ such that $xy \in \mathfrak{a}$ and neither x nor y is in $\mathfrak{a}$. Then $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ have smaller indexes than $\mathfrak{a}$, and thus must each contain primes, say $\mathfrak{a} + (x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and $\mathfrak{a} + (y) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_k$. So

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_k \subset (\mathfrak{a} + (x))(\mathfrak{a} + (y)) = \mathfrak{a}^2 + \mathfrak{a}(y) + \mathfrak{a}(x) + (xy) \subset \mathfrak{a}$$

Which is a contradiction. □

We can't say for sure yet that every nonzero ideal in $\mathcal{O}_K$ is equal to a product of primes. We can only say it contains a product of primes.

Theorem 1.5. *For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the fractional ideal $\tilde{\mathfrak{p}}$ satisfies the following properties*

1. *$\mathcal{O}_K \subset \tilde{\mathfrak{p}}$ and the containment is strict.*
2. *$\mathfrak{p}\tilde{\mathfrak{p}} = \mathcal{O}_K$.*

Proof. We construct an $\alpha \in \tilde{\mathfrak{p}}$ such that $\alpha \notin \mathcal{O}_K$ as follows: Choose any $x \in \mathfrak{p}$. By Lemma 1.1, $(x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some nonzero prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ of $\mathcal{O}_K$. Choose r to be minimal. Since $\mathfrak{p} \supset (x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{p}$ must be equal to one of the $\mathfrak{p}_1, \ldots \mathfrak{p}_r$. Without loss of generality $\mathfrak{p} = \mathfrak{p}_1$. If $r = 1$, then $\mathfrak{p} = (x)$. In which case $(1/x)\mathfrak{p} \subset \mathcal{O}_K$, so $\alpha = 1/x$ works. So assume $r \geq 2$. Since r is minimal, there exists a $y \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $y \notin (x)$. Then $\alpha = y/x$ works since $(y/x)\mathfrak{p} \subset (1/x)\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset \mathcal{O}_K$ and $y/x \notin \mathcal{O}_K$.

Now we show the second part (which is more interesting) follows from the first part. Given $\alpha \in \tilde{\mathfrak{p}}$ such that $\alpha \notin \mathcal{O}_K$, we claim $\tilde{\mathfrak{p}} = \mathcal{O}_K + \alpha\mathcal{O}_K$. We have $\mathfrak{p}\tilde{\mathfrak{p}} = \mathfrak{p}\mathcal{O}_K + \alpha\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K$. Since $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_K + \alpha\mathfrak{p}\mathcal{O}_K \subset \mathcal{O}_K$ and $\mathfrak{p}$ is maximal, we must have $\mathfrak{p}\mathcal{O}_K + \alpha\mathfrak{p}\mathcal{O}_K = \mathfrak{p}$ or $\mathfrak{p}\mathcal{O}_K + \alpha\mathfrak{p}\mathcal{O}_K = \mathcal{O}_K$. If $\mathfrak{p}\mathcal{O}_K + \alpha\mathfrak{p}\mathcal{O}_K = \mathfrak{p}$, then $\alpha\mathfrak{p} \subset \mathfrak{p}$, but this would mean α is integral over $\mathbb{Z}$, and hence $\alpha \in \mathcal{O}_K$, which is a contradiction.

□

Remark 1. In the proof above, we used the fact that if $\alpha\mathfrak{p} \subset \mathfrak{p}$, then $\alpha \in \mathcal{O}_K$. In fact, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{O}_K$ is the set $\{\alpha \in K \mid \alpha\mathfrak{p} \subset \mathfrak{p}\}$. This is the key step to the proof above. Later on, when we study orders, we will see that the proof that the above proof almost carries over. Given an order $\mathcal{O}$, there will be a special ideal $\mathfrak{c}$ of $\mathcal{O}$, called the conductor, which has the following property: For any prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathfrak{p}$ is relatively prime to the conductor, then $\mathcal{O}$ is the set $\{\alpha \in K \mid \alpha\mathfrak{p} \subset \mathfrak{p}\}$. It will then follow that every prime ideal $\mathfrak{p}$ of $\mathcal{O}$ which is relatively prime to the conductor $\mathfrak{c}$, is invertible.

We are now ready to prove the main theorem:

Theorem 1.6. *Every nonzero proper ideal of $\mathcal{O}_K$ is uniquely a product of nonzero prime ideals in $\mathcal{O}_K$.*

Proof. First, we prove existence. We will prove by induction on $r \geq 1$ that if a nonzero proper ideal $\mathfrak{a} \subset \mathcal{O}_K$ contains a product of r nonzero prime ideals then it equals a product of nonzero prime ideals. In the case $r = 1$, we have the inclusions

$$\mathfrak{p} \subset \mathfrak{a} \subset \mathcal{O}_K.$$

If $\mathfrak{a}$ is a proper ideal in $\mathcal{O}_K$, then $\mathfrak{a} = \mathfrak{p}$ since prime ideals are maximal in $\mathcal{O}_K$. Now assume the result is true for r and suppose

$$\mathfrak{a} \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_{r+1}.$$

Since $\mathfrak{a}$ is a proper ideal, it is contained in some prime $\mathfrak{p}$, and by the usual argument, we conclude $\mathfrak{p} = \mathfrak{p}_i$ for some $1 \leq i \leq r + 1$. Without loss of generality, $\mathfrak{p} = \mathfrak{p}_1$. Now apply $\mathfrak{p}^{-1}$ to the inclusion of ideals given by

$$\mathfrak{p} \supset \mathfrak{a} \supset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_{r+1}$$

to obtain the inclusion of ideals given by

$$\mathcal{O}_K \supset \mathfrak{p}^{-1}\mathfrak{a} \supset \mathfrak{p}_2 \cdots \mathfrak{p}_{r+1}$$

This tells us that $\mathfrak{p}^{-1}\mathfrak{a}$ is an ideal in $\mathcal{O}_K$ which contains a product of r nonzero prime ideals. Therefore by induction, $\mathfrak{p}^{-1}\mathfrak{a}$ is equal to a product of nonzero prime ideals, hence $\mathfrak{a}$ is a product of nonzero prime ideals. This proves existence. To prove uniqueness, suppose for some ideal $\mathfrak{a} \subset \mathcal{O}_K$ we have

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \qquad \text{for prime ideals } \mathfrak{p}_1, \ldots, \mathfrak{p}_r \text{ and } \mathfrak{q}_1, \ldots, \mathfrak{q}_s.$$

We can cancel any common prime ideals on both sides and thus may suppose $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j. Since $\mathfrak{p}_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, $\mathfrak{p}_1$ is equal to some $\mathfrak{q}_j$, which is a contradiction.

□

1.1 Analogues in $F[X]$

Many properties of $\mathbb{Z}$ can be carried over to $F[x]$, where F is a field. Both $\mathbb{Z}$ and $F[x]$ have division with remainder, and thus are PID's. The table below indicates some further similarities.

$\mathbb{Z}$	$F[x]$
Prime	Irreducible
± 1	$F^\times$
Positive	Monic
$\mathbb{Q}$	$F(x)$

Analogies are even strongest when F is a finite field, but here we allow any F. We want to adapt the methods from number fields to the "function field" case: if K is a finite extension of $F(x)$, does the integral closure of $F[x]$ in K have unique factorization of ideals? A key idea running through the proofs in this section was induction on the index of nonzero ideals in a ring of integers. We can't directly use this idea for the integral closure of $F[x]$ in K, since ideals in $F[x]$ don't have finite index if F is an infinite field. For example, representatives in $\mathbb{Q}[x]/(x^3-2)$ are $a + bx + cx^2$ with rational a, b, c and there are infinitely many of these. However, there is something finite about this example: it is finite dimensional over $\mathbb{Q}$ with dimension 3. More generally, if $f(x)$ has degree $d \geq 0$ in $F[x]$ then $F[x]/(f(x))$ has dimension d as an F-vector space (with basis $\{1, x, x^2, \ldots, x^{d-1}\}$). So if we count dimension over F rather than count index in $F[x]$, then $F[x]/(f(x))$ has a finiteness property we can take advantage of.

Let $K/F(x)$ be a finite separable extension of degree n and let A be the integral closure of $F[x]$ in K. This is an analogue of the ring of integers of a number field. For any $\alpha \in A$, $\mathrm{Tr}_{K/F(x)}(\alpha)$ and $\mathrm{N}_{K/F(x)}(\alpha)$ are in $F[x]$. More generally, the characteristic polynomial $\chi_{K/F(x),\alpha}(t)$ is in $F[x][t]$.

Example 1.1. Suppose $K = \mathbb{C}(x)$, $B = \mathbb{C}[x]$, and $y = \sqrt{x^3+1}$, then $K(y)/K$ is a finite separable extension of degree 2. Indeed, the minimal polynomial for y is given by $\pi(t) = t^2 - (x^3+1)$, which is irreducible and separable of degree 2. The integral closure of B in $K(y)$ is $B[y]$. Given $\alpha \in B[y]$, write$\alpha = f(x) + g(x)y$. The matrix representation of the multiplication by α is given by

$$[m_\alpha] = \begin{pmatrix} f(x) & g(x)(x^3+1) \\ g(x) & f(x) \end{pmatrix}$$

So $\mathrm{Tr}_{K(y)/K}(\alpha) = 2f(x)$ and $\mathrm{N}_{K(y)/K}(\alpha) = f(x)^2 - g(x)^2(x^3+1)$.

Theorem 1.7. *With the notation as above, A is a finite free $F[x]$-module of rank n, any nonzero ideal $\mathfrak{a}$ in A is a finite free $F[x]$-module of rank n, and $A/\mathfrak{a}$ is finite dimensional over F.*

Proof. The proof that a ring of integers is a finite free $\mathbb{Z}$-module uses the nonvanishing of discriminants and the fact that $\mathbb{Z}$ is a PID. Specifically, if $\{\alpha_1, \ldots \alpha_n\}$ is a $\mathbb{Q}$-basis of K consisting entirely of algebraic integers, then we can squeeze $\mathcal{O}_K$ in between two $\mathbb{Z}$-modules of rank n

$$\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \subset \mathcal{O}_K \subset \frac{1}{\Delta}(\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n)$$

where $\Delta = \mathrm{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$, hence $\mathcal{O}_K$ must be a free $\mathbb{Z}$-module of rank n. Let's discuss why

$$\mathcal{O}_K \subset \frac{1}{\Delta}(\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n)$$

since it is such a nice proof. Given $\alpha \in \mathcal{O}_K$, write

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \qquad \text{where } a_i \in \mathbb{Q} \text{ for } 1 \leq i \leq n.$$

We want to show that $\Delta a_i \in \mathbb{Z}$ for all $1 \leq i \leq n$. The key is to use the elements $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$.

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}$$

By Cramer's rule,

$$a_i = \frac{\gamma_i}{\delta} \tag{2}$$

where $\gamma_i \in \mathcal{O}_K^\times$ is the determinant of the matrix $M \in \mathrm{GL}_n(\mathcal{O}_K)$, obtained by replacing the i'th column of matrix $(\sigma_i(\alpha_j))$ with the column vector (α_i), and $\delta \in \mathcal{O}_K^\times$ is the determinant of the matrix $(\sigma_i(\alpha_j))$. Thus, $\delta^2 = \Delta$Multiply both sides of equation (2) by Δ to obtain

$$\Delta a_i = \delta\gamma_i \tag{3}$$

The left side of equation (3) is rational number, while the right side of equation (3) is an algebraic integer. Therefore since $\mathcal{O}_K^\times \cap \mathbb{Q} = \mathbb{Z}$, we have $\Delta a_i \in \mathbb{Z}$. Since $F[x]$, like $\mathbb{Z}$, is a PID, and $K/F(x)$ is a separable extension, the proof that a ring of integers is a finite free $\mathbb{Z}$-module carries over to show A is a finite free $F[x]$-module. If $K/F(x)$ were an inseparable extension, then $\Delta = 0$ since there would be a repeated row in the matrix $(\sigma_i(\alpha_j))$. Similarly the proof which shows every nonzero ideal in $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n carries over to show every nonzero ideal in A is a free $F[x]$-module of rank n. From the structure of finitely generated modules over a PID, given a nonzero ideal $\mathfrak{a}$ of A, there is an $F[x]$-basis $y_1, \dots y_n$ of A and nonzero $f_1, \dots, f_n$ in $F[x]$ such that $f_1 y_1, \dots, f_n y_n$ is an $F[x]$-basis of $\mathfrak{a}$, so

$$A/\mathfrak{a} = (\bigoplus_{i=1}^n F[x]y_i)/(\bigoplus_{i=1}^n F[x]f_i y_i) \cong \bigoplus_{i=1}^n (F[x]/(f_i))\overline{y}_i$$

Each $F[x]/(f_i)$ has finite dimension over F and there are finitely many of these, so $A/\mathfrak{a}$ is finite dimensional over F. $\square$

Corollary 2. *Every nonzero prime ideal in A is a maximal ideal.*

Proof. For any nonzero prime ideal $\mathfrak{p}$ of A, $A/\mathfrak{p}$ is a domain that is finite-dimensional over F. A domain that is finite-dimensional over a field is itself a field, so $\mathfrak{p}$ is maximal. $\square$

Define a fractional A-ideal I to be a nonzero A-module in K with a common denominator: $aI \subset A$ for some nonzero $a \in A$. All of the theorems in the previous section carry over to fractional A-ideals in K. For instance, fractional A-ideals are precisely the nonzero finitely generated A-modules in K and each is a free $F[x]$-module of rank $n = [K : F(X)]$.

1.2 Totally ramified primes and Eisenstein polynomials

Let p be a prime and let $f(T)$ be a monic polynomial in $\mathbb{Z}[T]$ and expressed as

$$f = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0.$$

We say f is **p-Eisenstein** if $p \mid c_i$ for all i and $p^2 \nmid c_0$. Now suppose α is a root of f. Note that since f is monic and irreducible (Eisenstein's criterion), we see that f is the minimal polynomial of α over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_K$ be the corresponding ring of integers (that is, the integral closure of $\mathbb{Z}$ in K). Our goal in this subsection is to show that $p \nmid [\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$.

Lemma 1.8. *For $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}$, if*

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K, \tag{4}$$

then $a_i \equiv 0 \bmod p\mathbb{Z}$ for all i.

Proof. Assume for $j \in \{0, 1, \dots, n-1\}$ that $a_i \equiv 0 \bmod p\mathbb{Z}$ for $i < j$ (this is an empty condition if $j = 0$). We will prove $a_j \equiv 0 \bmod p\mathbb{Z}$. Since $a_i \equiv 0 \bmod p\mathbb{Z}$ for $i < j$, (4) implies

$$a_j\alpha^j + a_{j+1}\alpha^{j+1} + \cdots + a_{n-1}\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K.$$

Multiply through this congruence by α^{n-1-j}, making all but the first term $a_j\alpha^{n-1}$ a multiple of α^n. Since α is the root of an Eisenstein polynomial at p, we have $\alpha^n \equiv 0 \bmod p\mathcal{O}_K$, so

$$a_j\alpha^{n-1} \equiv 0 \bmod p\mathcal{O}_K.$$

Write this congruence as an equation, say $a_j\alpha^{n-1} = p\gamma$ with $\gamma \in \mathcal{O}_K$. Now take norms of both sides down to $\mathbb{Z}$:

$$(-1)^{n-1}a_j^n c_0^{n-1} = p^n \mathrm{N}_{K/\mathbb{Q}}(\gamma).$$

The right side is an integral multiple of p^n. On the left side, c_0^{n-1} (the norm of α^{n-1} up to a sign) is divisible by p exactly once (Eisenstein condition!). It follows that $p \mid a_j$. Thus $a_i \equiv 0 \bmod p\mathbb{Z}$ for $i < j+1$. Repeat this for $j = 1, 1, \dots, n-1$ to get $p \mid a_i$ for all i. $\square$

Lemma 1.9. *For $r_0, r_1, \dots, r_{n-1} \in \mathbb{Q}$, if*

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} \in \mathcal{O}_K, \tag{5}$$

then r_i has no p in its denominator for all i.

Proof. Assume some r_i has a p in its denominator. Let d be the least common denominator of the r_i's, so $p \mid d$. Write $r_i = a_i/d$ where $a_i \in \mathbb{Z}$, so some a_i is not divisible by p (otherwise d, being divisible by p, would not be the least common denominator). Then (5) implies

$$\frac{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}}{d} \in \mathcal{O}_K.$$

Multiply through by the integer d to get

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in d\mathcal{O}_K \subseteq p\mathcal{O}_K.$$

Then Lemma (1.8) tells us $a_i \in p\mathbb{Z}$ for every i. This is a contradiction. $\square$

Theorem 1.10. *We have $p \nmid [\mathcal{O}_K \colon \mathbb{Z}[\alpha]]$.*

Proof. Assume for a contradiction that $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then $\mathcal{O}_K/\mathbb{Z}[\alpha]$, viewed as a finite abelian group, has an element of order p: there is some $\gamma \in \mathcal{O}_K$ such that $\gamma \notin \mathbb{Z}[\alpha]$ but $p\gamma \in \mathbb{Z}[\alpha]$. Using the basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ for $K/\mathbb{Q}$, write

$$\gamma = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$$

with $r_i \in \mathbb{Q}$. Since $\gamma \notin \mathbb{Z}[\alpha]$, some r_i is not in $\mathbb{Z}$. Since $p\gamma \in \mathbb{Z}[\alpha]$ we have $pr_i \in \mathbb{Z}$. Hence r_i has a p in its denominator, which contradicts Lemma (1.9). $\square$

Example 1.2. We show the ring of algebraic integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$. Let $\mathcal{O}$ be the full ring of algebraic integers of $\mathbb{Q}(\sqrt[3]{2})$, so $\mathbb{Z}[\sqrt[3]{2}] \subseteq \mathcal{O}$ and

$$\operatorname{disc} \mathbb{Z}[\sqrt[3]{2}] = [\mathcal{O} : \mathbb{Z}[\sqrt[3]{2}]]^2 \operatorname{disc} \mathcal{O}$$

By an explicit calculation, $\operatorname{disc} \mathbb{Z}[\sqrt[3]{2}] = -2^2 3^3$, so 2 and 3 are the only primes that could divide $[\mathcal{O} : \mathbb{Z}[\sqrt[3]{2}]]$. Since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $T^3 - 2$, which is 2-Eisenstein, we see that 2 does not divide $[\mathcal{O} \colon \mathbb{Z}[\sqrt[3]{2}]]$ by Theorem (1.10). The minimal polynomial of $1 + \sqrt[3]{2}$ over $\mathbb{Q}$ is given by

$$(T-1)^3 - 2 = T^3 - 3T^2 + 3T - 3,$$

which is 3-Eisenstein, so 3 does not divide $[\mathcal{O} \colon \mathbb{Z}[1 + \sqrt[3]{2}]]$. The ring $\mathbb{Z}[1 + \sqrt[3]{2}]$ equals $\mathbb{Z}[\sqrt[3]{2}]$, so $[\mathcal{O} : \mathbb{Z}[\sqrt[3]{2}]]$ is not divisible by 3. Therefore this index is 1, and so $\mathcal{O} = \mathbb{Z}[\sqrt[3]{2}]$.

1.3 Eisenstein Polynomials in $\mathcal{O}_K[T]$

So far we've been discussing Eisenstein polynomials in $\mathbb{Z}[T]$. Let's generalize the concept to polynomials over other rings of integers.

Definition 1.4. Let K be a number field. A monic polynomial

$$f(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1 T + c_0 \in \mathcal{O}_K[T]$$

is called **Eisenstein** at the nonzero prime ideal $\mathfrak{p}$ when $c_i \equiv 0 \bmod \mathfrak{p}$ for all i and $c_0 \not\equiv 0 \bmod \mathfrak{p}^2$.

Theorem 1.11. *Any Eisenstein polynomial in $\mathcal{O}_K[T]$ is irreducible in $K[T]$.*

Proof. Let $f(T) \in \mathcal{O}_K[T]$ be Eisenstein at some prime ideal. If $f(T)$ is reducible in $K[T]$ then $f(T) = g(T)h(T)$ for some nonconstant $g(T)$ and $h(T)$ in $K[T]$.

We first show that g and h can be chosen in $\mathcal{O}_K[T]$. As f is monic, we can assume g and h are monic by rescaling if necessary. Every root of g or h is an algebraic integer (since their roots are roots of $f(T)$, so they're integral over $\mathcal{O}_K$ and thus also over $\mathbb{Z}$). Because g and h are monic, their coefficients are polynomials in their roots with $\mathbb{Z}$-coefficients, hence their coefficients are algebraic integers. Thus g and h both lie in $\mathcal{O}_K[T]$.

Let $n = \deg f$, $r = \deg g$, and $s = \deg h$. All of these degrees are positive. Let $\mathfrak{p}$ be a prime at which f is Eisenstein. Reduce the equation $f = gh$ in $\mathcal{O}_K[T]$ modulo $\mathfrak{p}$ to get $\overline{f} = \overline{g}\overline{h}$ in $(\mathcal{O}_K/\mathfrak{p})[T]$. As f, g, and h are all monic, their reductions modulo $\mathfrak{p}$ have the same degree as the original polynomials (n, r, and s respectively). Since f is Eisenstein at $\mathfrak{p}$, we have $\overline{f} = T^n$. Therefore, by unique factorization in $(\mathcal{O}_K/\mathfrak{p})[T]$, we see that $\overline{g}$ and $\overline{h}$ are powers of T too, so $\overline{g} = T^r$ and $\overline{h} = T^s$. But, because r and s are positive, we conclude that g and h each have constant term in $\mathfrak{p}$. Then the constant term of f is

$$\begin{aligned} f(0) &= g(0)h(0) \\ &\in \mathfrak{p}^2. \end{aligned}$$

This contradicts the definition of an Eisenstein polynomial. □

2 Class Group Calculations

Let K be a number field. Recall Minkowski's bound tells us that any ideal class contains an integral ideal with norm bounded above by

$$\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_K|}$$

where r_2 is the number of conjugate pairs of complex embeddings, $n = r_1 + 2r_2$ is the degree of the number field, r_1 is the number of real embeddings, and Δ_K is the discriminant of the field K (i.e. the determinant of the trace pairing matrix $(\mathrm{Tr}_{K/\mathbb{Q}}(e_i e_j))$ where the e_i form a $\mathbb{Z}$-basis of $\mathcal{O}_K$). We will use this bound to calculate the class group for various K:

Example 2.1. Suppose $K = \mathbb{Q}(\sqrt{-65})$. We will show its class group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The Minkowski bound is roughly 10.26, so we should factor 2, 3, 5, and 7 in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-65}]$. From the following table, we see that the class group is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$, and $[\mathfrak{p}_5]$.

p	$T^2 + 65 \bmod p$	(p)
2	$(T+1)^2$	$\mathfrak{p}_2^2$
3	$(T+1)(T+2)$	$\mathfrak{p}_3\mathfrak{p}_3'$
5	T^2	$\mathfrak{p}_5^2$
7	T^2+2	(7)

where

$$\begin{aligned} \mathfrak{p}_2 &= \langle 2, \sqrt{-65}+1 \rangle \\ \mathfrak{p}_3 &= \langle 3, \sqrt{-65}+1 \rangle \\ \mathfrak{p}_3' &= \langle 3, \sqrt{-65}+2 \rangle \\ \mathfrak{p}_5 &= \langle 5, \sqrt{-65} \rangle. \end{aligned}$$

Note that the table already tells us that $[\mathfrak{p}_2]^2 = 1 = [\mathfrak{p}_5]^2$ and $[\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$. In order to find more relations, we factor

$$\mathrm{N}(a + \sqrt{-65}) = a^2 + 65$$

for small a, looking for only factors of 2, 3, 5, in the table below:

a	a^2+65
1	$2 \cdot 3 \cdot 11$
2	$3 \cdot 23$
3	$2 \cdot 37$
4	3^4
5	$2 \cdot 3^2 \cdot 5$

Since $\langle 4 + \sqrt{-65} \rangle$ is not divisible by $\langle 3 \rangle$, we see that the ideal $\langle 4 + \sqrt{-65} \rangle$ is divisible by only one of the prime factors of $\langle 3 \rangle$. In particular, $\langle 4 + \sqrt{-65} \rangle$ is divisible by $\mathfrak{p}_3$ since $4 + \sqrt{-65} \equiv 0 \bmod \mathfrak{p}_3$. Thus we see that

$$\langle 4 + \sqrt{-65} \rangle = \mathfrak{p}_3^4.$$

A similar argument shows that

$$\langle 5 + \sqrt{-65} \rangle = \mathfrak{p}_2 \mathfrak{p}_3'^2 \mathfrak{p}_5$$

which tells us that $[\mathfrak{p}_5] = [\mathfrak{p}_2][\mathfrak{p}_3]^2$. Finally, note that the ideal $\mathfrak{p}_2$ is non-principal since there is no integral solution to the equation $2 = x^2 + 65y^2$. Similarly, the only integral solution to $9 = x^2 + 65y^2$ is $x = \pm 3$ and $y = 0$, so if $\mathfrak{p}_3^2$ were principal then $\mathfrak{p}_3^2 = \langle 3 \rangle = \mathfrak{p}_3 \mathfrak{p}_3'$ and that is false ($\mathfrak{p}_3 \neq \mathfrak{p}_3'$). Can $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2]$? If so, then $\mathfrak{p}_3^2 \mathfrak{p}_2$ is principal. But $18 = x^2 + 65y^2$ has no integral solution.

Ideal Class Group Motivation

Let R be an integral domain. Recall that R is a **Unique Factorization Domain (UFD)** if every nonzero nonunit element $r \in R$ has the following two properties

1. r can be written as a product of irreducibles $r = p_1 p_2 \cdots p_m$ where $p_1, p_2, \ldots, p_m$ are irreducible elements in R (repetitions of the p_i are allowed).
2. This decomposition is unique up to associates, i.e. if $r = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_\ell$ where p_i and q_j are all irreducible elements in R, then $m = \ell$ and (perhaps after reordering the factors) $p_i = u_i q_i$ where u_i is a unit in R and $1 \leq i \leq m$.

Let's demonstrate the usefulness of UFD's. First we need a theorem.

Theorem 2.1. *Let R be a ring with unique factorization. If $a, b, c \in R$ are nonzero, $ab = c^n$, and a and b are relatively prime, then there are units u and v in R, as well as elements a' and b' in R, such that $a = ua'^n$ and $b = vb'^n$.*

Proof. Decompose a, b and c into irreducibles and collect together any irreducible factors which are equal up to unit multiple. This lets us write

$$a = up_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \quad b = vp_1'^{f_1} p_2'^{f_2} \cdots p_s'^{f_s}, \quad c = wq_1^{g_1} q_2^{g_2} \cdots q_t^{g_t},$$

where p_i, p_j', and q_k are all irreducibles and u, v and w are units. Since a and b are relatively prime, no p_i and p_j' are unit multiples. We have

$$ab = uvp_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} p_1'^{f_1} p_2'^{f_2} \cdots p_s'^{f_s} \quad \text{and} \quad c^n = w^n q_1^{ng_1} q_2^{ng_2} \cdots q_t^{ng_t}.$$

Comparing the irreducible factorizations of ab and c^n shows from unique factorization that each p_i and p_j' has multiplicity divisible by n: each e_i and f_j is some ng_k. (Here is where we need relatively primality of a and b). Since all the e_i's are divisible by n, a is u times an nth power. Similarly, b is v times an nth power. □

Example 2.2. Consider the equation $X^3 = Y^2 + 4$. Using unique factorization in $\mathbb{Z}[i]$, we can show that the only integral solutions to this equation are $(5, \pm 11)$ or $(2, \pm 2)$. To show this, first re-express the equation as

$$X^3 = (Y + 2i)(Y - 2i). \tag{6}$$

Assume x and y are two integers which satisfy 6). We can view the equation $x^3 = (y + 2i)(y - 2i)$ as an equation in $\mathbb{Z}[i]$, which is a UFD. Using Theorem (2.1), we conlude that $y + 2i = u\alpha^3$ for some $\alpha \in \mathbb{Z}[i]$. The only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$. In each case, we can swallow them into the cubed power: $-\alpha^3 = (-\alpha)^3$, $i\alpha^3 = (-i\alpha)^3$, etc..), So we may assume that $y + 2i = \alpha^3$ for some $\alpha \in \mathbb{Z}[i]$. Write $\alpha = a + bi$, then

$$\begin{aligned} y + 2i &= (a + bi)^3 \\ &= (a^3 - 3ab^2) + (3a^2b - b^3)i, \end{aligned}$$

and therefore

$$y = a^3 - 3ab^2 \quad \text{and} \quad 2 = \left(3a^2 - b^2\right) b$$

The second of these equations forces $b \in \{1, -1, 2, -2\}$. Checking case by case

$b = 1$	$3a^2 - 1 = 2$	$a = \pm 1$ and $y = \pm 2$
$b = -1$	$3a^2 - 1 = -2$	No Solution
$b = 2$	$3a^2 - 4 = 1$	No Solution
$b = -2$	$3a^2 - 4 = -1$	$a = \pm 1$ and $y = \pm 11$

In summary, we've shown that if $x^3 = y^2 + 4$, then y must either be ± 2 or ± 11.

In Algebraic Number Theory, we come across many instances of integral domains which fail to be a UFD. For instance, consider the ring $R = \mathbb{Z}[\sqrt{-5}]$. In this ring, we have two irreducible factorizations of 6:

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

and there do not exist units u and v such that $2 = u(1 + \sqrt{-5})$ or $2 = v(1 + \sqrt{-5})$ (the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1). Therefore $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

On the other hand, it's easy to show that $\mathbb{Z}[i]$ is a UFD. Here's a consequence of this: Consider the equation $X^3 = Y^2 + 4$. Using unique factorization in $\mathbb{Z}[i]$, we can show that the only integral solutions to this equation are

$$(x, y) = (5, \pm 11) \quad \text{or} \quad (x, y) = (2, \pm 2)$$

To show this, first re-express the equation as

$$X^3 = (Y + 2i)(Y - 2i). \tag{7}$$

Now assume x and y are two integers which satisfy 7). We can view the equation $x^3 = (y + 2i)(y - 2i)$ as in equation in $\mathbb{Z}[i]$. We want to conlude from this that $y + 2i = \alpha^3$ for some $\alpha \in \mathbb{Z}[i]$, but we need to justify this. Let's express both sides as a product of primes in $\mathbb{Z}[i]$

$$\left(\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}\mathfrak{p}_5^{e_5}\mathfrak{p}'^{e'_5}_5 \cdots\right)^3 = \left(\mathfrak{p}_2^{f_2}\mathfrak{p}_3^{f_3}\mathfrak{p}_5^{f_5}\mathfrak{p}'^{f'_5}_5 \cdots\right)\left(\mathfrak{p}_2^{f_2}\mathfrak{p}_3^{f_3}\mathfrak{p}_5^{f'_5}\mathfrak{p}'^{f_5}_5 \cdots\right) = \left(\mathfrak{p}_2^{2f_2}\mathfrak{p}_3^{2f_3}\mathfrak{p}_5^{f'_5+f_5}\mathfrak{p}'^{f'_5+f_5}_5 \cdots\right)$$

Now let's show that f_i and f'_i can't both be nonzero, where i runs through the primes that split. If $\pi | y + 2i$ and $\pi | y - 2i$, then $\pi | (y + 2i) - (y - 2i) = 4i$; so $\pi | 2$, which means $(\pi) = (1 + i) = \mathfrak{p}_2$. So without loss of generality, assume f'_i is zero. We also get from this $f_j = 0$, where j runs through the inert primes. This is already obvious here though. So the factorization of $y + 2i$ really looks like this $\left(\mathfrak{p}_2^{f_2}\mathfrak{p}_5^{f_5} \cdots\right)$. Now we are led to the equations

Ramified	Split	Inert
$2f_2 = 3e_2$	$f_i = 3e_i$	$f_j = 0$

Thus, $3 | f_i$ for all primes i. Now we can conclude $y + 2i = \alpha^3$. This is where finiteness of the number of solutions comes in. Write $\alpha = a + bi$, then

$$y + 2i = (a + bi)^3 = (a^3 - 3ab^2) + (3ab^2 - b^3)i$$

Therefore

$$y = a^3 - 3ab^2 \qquad 2 = \left(3a^2 - b^2\right) b$$

The second of these equations forces $b \in \{1, -1, 2, -2\}$. Checking case by case

$b = 1$	$3a^2 - 1 = 2$	$a = \pm 1$ and $y = \pm 2$
$b = -1$	$3a^2 - 1 = -2$	No Solution
$b = 2$	$3a^2 - 4 = 1$	No Solution
$b = -2$	$3a^2 - 4 = -1$	$a = \pm 1$ and $y = \pm 11$

Example 2.3. Consider the equation $x^3 = y^2 + 20$. We will show the only integral solutions to this equation are

$$(x, y) = (6, \pm 14)$$

As before, re-express the equation as

$$x^3 = (y + 2\sqrt{-5})(y - 2\sqrt{-5})$$

Again, we want to conlude from this that $y + 2\sqrt{-5} = u \cdot \alpha^3$ for some unit u and $\alpha \in \mathbb{Z}[\sqrt{-5}]$, but we need to be more careful this time. First, if $y + 2\sqrt{-5} \in \mathfrak{p}$ and $y - 2\sqrt{-5} \in \mathfrak{p}$, then $4\sqrt{-5} \in \mathfrak{p}$, which implies $\mathfrak{p} = (2, 1 + \sqrt{-5})$ or $\mathfrak{p} = (\sqrt{-5})$. We are led to the equations

Ramified	Split	Inert
$2f_2 = 3e_2$ and $2f_5 = 3e_5$	$f_i = 3e_i$	$f_j = 0$

Thus, $3 | f_i$ for all primes i, but we can't conclude yet that $y + 2\sqrt{-5} = u \cdot \alpha^3$ for some unit u and $\alpha \in \mathbb{Z}[\sqrt{-5}]$. We can only conclude the ideal equation $(y + 2\sqrt{-5}) = \mathfrak{a}^3$, for some ideal $\mathfrak{a}$. If $\mathfrak{a}^3 = (\alpha)$, then we can conclude that $y + 2\sqrt{-5} = u \cdot \alpha^3$. Because the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2, $\mathfrak{a}^3 \sim 1$, so $\mathfrak{a}^3 = (\alpha)$. Since the units of $\mathbb{Z}[\sqrt{-5}]$ are just $\{\pm 1\}$, we get $y + 2\sqrt{-5} = \pm\alpha^3 = (\pm\alpha)^3$.

Example 2.4. Consider the equation $x^3 = y^2 + 26$. Doing everything as before, let's jump to the equation $y + \sqrt{-26} = \left(a + b\sqrt{-26}\right)^3$. So we have

$$y + \sqrt{-26} = (a + b\sqrt{-26})^3 = (a^3 - 3 \cdot 26ab^2) + (3ab - 26b^2)b\sqrt{-26}$$

Therefore

$$y = a^3 - 3 \cdot 26ab^2 \qquad 1 = (3ab - 26b^2)b$$

The second of these equations forces $b \in \{1, -1\}$. Checking case by case

$b = 1$	$3a^2 - 26 = 1$	$a = \pm 3$ and $y = \pm 207$
$b = -1$	$3a^2 - 26 = -1$	No Solution

Thus, $(35, \pm 207)$ is a solution to the equation $x^3 = y^2 + 26$. Are these the only solutions? No! $(3,1)$ is another solution! How did we miss it? Proceeding as we did in the two examples above, we get everything up to the conclusion that $\left(y + \sqrt{-26}\right) = \mathfrak{a}^3$. However we cannot conclude that for all y, $y + \sqrt{-26} = \alpha^3$ for some element α. The reason is because $\mathbb{Z}[\sqrt{-26}]$ has class number 6. The solution $(3,1)$ represents a "nontrivial" solution. We have

$$3^3 = \left(1 + \sqrt{-26}\right)\left(1 - \sqrt{-26}\right)$$

But $1 + \sqrt{-26}$ is not a cube. However, $\left(1 + \sqrt{-26}\right) = \mathfrak{p}_3^3$, where $\mathfrak{p}_3 = \left(3, 1 + \sqrt{-26}\right)$.

Let's now shift our focus to a different kind of Dedekind domain, one with more geometric flavor. Consider the quadratic extension $\mathbb{C}(T, \sqrt{T^3+1})/\mathbb{C}(T)$. The table below compares this quadratic extension with the quadratic extension $\mathbb{Q}(\sqrt{-26})/\mathbb{Q}$.

Field of Functions	Integral Closure	How Primes Split
$\mathbb{Q}(\sqrt{-26})$	$\mathbb{Z}[\sqrt{-26}]$	$(3) = (3, 1+\sqrt{-26})(3, 1-\sqrt{-26})$
$\mathbb{C}(T, \sqrt{T^3+1})$	$\mathbb{C}[T, \sqrt{T^3+1}]$	$(T) = (T, \sqrt{T^3+1}-1)(T, \sqrt{T^3+1}+1)$

$\mathbb{Q}(\sqrt{-26})$ is called an algebraic number field, whereas $\mathbb{C}(T, \sqrt{T^3+1})$ is called an algebraic function field. The algebraic function field setting is more geometric for the following reasons

- There is a one-to-one correspondence between points in $\{\alpha \mid \alpha \in \mathbb{C}\}$ and nonzero prime ideals in $\mathbb{C}[T]$: $\alpha \mapsto (T - \alpha)$.
- There is a one-to-one correspondence between points in $\{(\alpha, \beta) \in \mathbb{C} \times \mathbb{C} \mid \beta^2 = \alpha^3 + 1\}$ and nonzero prime ideals in $\mathbb{C}[T, \sqrt{T^3+1}]$: $(\alpha, \beta) \mapsto (T - \alpha, \sqrt{T^3+1} - \beta)$.

Another useful aspect in the algebraic function field case is that we can change the field $\mathbb{C}$ to $\mathbb{F}_p$, which makes the analogy even stronger.

Example 2.5. Let x, y, z be homogenous coordinates in $\mathbb{P}^2$. For the cubic curve $\mathrm{V}(y^2z - x^3 - xz^2)$, let's write the divisor $div\left(\frac{y}{z}\right)$ and $div\left(\frac{x}{z}\right)$. For $div\left(\frac{y}{z}\right)$, setting $y = 0$ reduces the equation $y^2z - x^3 - xz^2 = 0$ to $-x(x+iz)(x-iz) = 0$, which has solutions $(0:0:1)$, $(-i:0:1)$, and $(i:0:1)$. Setting $z = 0$ reduces the equation to $y^2z - x^3 - xz^2 = 0$ to $-x^3 = 0$, which has solution $(0:1:0)$ with multiplicity 3. Thus,

$$div\left(\frac{y}{z}\right) = (0:0:1) + (-i:0:1) + (i:0:1) - 3(0:1:0)$$

For $div\left(\frac{x}{z}\right)$, setting $x = 0$ reduces the equation $y^2z - x^3 - xz^2 = 0$ to $y^2z = 0$, which has solutions $(0:0:1)$ with multiplicity 2 and $(0:1:0)$. Setting $z = 0$ reduces the equation to $y^2z - x^3 - xz^2 = 0$ to $-x^3 = 0$, which has solution $(0:1:0)$ with multiplicity 3. Thus,

$$div\left(\frac{x}{z}\right) = 2(0:0:1) - 2(0:1:0)$$

For $div\left(\frac{x-z}{z}\right)$, setting $x = z$ reduces the equation $y^2z - x^3 - xz^2 = 0$ to $z(y - \sqrt{2}z)(y + \sqrt{2}z) = 0$, which has solutions $(0:1:0)$,$(1:\sqrt{2}:1)$, and $(1:-\sqrt{2}:1)$. Setting $z = 0$ reduces the equation to $y^2z - x^3 - xz^2 = 0$ to $-x^3 = 0$, which has solution $(0:1:0)$ with multiplicity 3. Thus,

$$div\left(\frac{x-z}{z}\right) = (1:\sqrt{2}:1) + (1:-\sqrt{2}:1) - 2(0:1:0)$$

3 Ideal classes and matrix conjugation over $\mathbb{Z}$

In this presentation, we will describe a relationship between conjugacy classes of matrices with integer coefficients and $\mathcal{O}$-ideal classes of fractional $\mathcal{O}$-ideals where $\mathcal{O}$ is an order in a number field K. This presentation was inspired by Keith Conrad's expository notes **[?]**.

3.0.1 Conjugacy Classes of Matrices in $\mathrm{M}_n(\mathbb{Z})$

Let A and B be matrices in $\mathrm{M}_n(\mathbb{Z})$. We say A is **conjugate** to B, denoted by $A \sim_{\mathrm{c}} B$, if there exists a $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAU^{-1} = B$. It is straightforward to check that $\sim_{\mathrm{c}}$ is an equivalence relation. We will denote by $[A]_{\mathrm{c}}$ to be the equivalence class which is represented by the matrix $A \in \mathrm{M}_n(\mathbb{Z})$. We call these equivalence classes **conjugacy classes**. We denote by $\mathrm{C}_{\mathrm{GL}_n(\mathbb{Z})}(\mathbb{Z})$ to be set of all conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$. Recall the characteristic polynomial of a matrix $A \in \mathrm{M}_n(\mathbb{Z})$ is defined by

$$\chi_A(T) = \det(T\mathrm{I}_n - A).$$

If $A \sim_{\mathrm{c}} B$, then there exists $U \in \mathrm{GL}_n(\mathbb{Z})$ such that $UAU^{-1} = B$, and hence

$$\begin{aligned}
\chi_B(T) &= \det(T\mathrm{I}_n - B) \\
&= \det(T\mathrm{I}_n - UAU^{-1}) \\
&= \det(U(T\mathrm{I}_n - A)U^{-1}) \\
&= \det(U)\det(T\mathrm{I}_n - A)\det(U^{-1}) \\
&= \det(T\mathrm{I}_n - A) \\
&= \chi_A(T).
\end{aligned}$$

Therefore it makes sense to assign a characteristic polynomial to a conjugacy class of matrices in $\mathrm{M}_n(\mathbb{Z})$. For any monic polynomial $f(T) \in \mathbb{Z}[T]$ of degree n, we will denote by $\mathrm{C}_n(\mathbb{Z}, f)$ to be the set of all conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial f.

3.0.2 Fractional $\mathcal{O}$-Ideals

Let $\mathcal{O}$ be an order in a number field K. That is, $\mathcal{O}$ is a subring of K that is finitely generated as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of K. A typical example of an order is $\mathbb{Z}[\alpha]$ in $\mathbb{Q}(\alpha)$ where α is an algebraic integer over $\mathbb{Q}$. A **fractional $\mathcal{O}$-ideal** is a nonzero finitely generated $\mathcal{O}$-module in K. Let I an J be two fractional $\mathcal{O}$-ideals. We say I and J are **equivalent**, denoted $I \sim J$, if $I = xJ$ for some $x \in K^\times$. It is straightforward to check that this is an equivalence relation. We will denote by $[I]$ to be the equivalence class which is represented by the $\mathcal{O}$-fractional ideal I. We call these equivalence classes **$\mathcal{O}$-ideal classes**. We denote by $\mathrm{Cl}(\mathcal{O})$ to be the set of all $\mathcal{O}$-ideal classes. In fact, it is easy to show that $\mathrm{Cl}(\mathcal{O})$ is none other than the set of isomorphism classes of $\mathcal{O}$-fractional ideals. That is, the relation $I \sim J$ is equivalent to saying I is isomorphic to J as $\mathcal{O}$-modules. Indeed, if $I \sim J$, then $I = xJ$ for some $x \in K^\times$. Then the multiplication by x map $\mathrm{m}_x \colon I \to J$, given by

$$\mathrm{m}_x(y) = xy$$

for all $y \in I$ is an $\mathcal{O}$-module isomorphism from I to J. Conversely, if $\varphi \colon I \to J$ is an $\mathcal{O}$-module isomorphism, then we claim that $\varphi(y)/y = \varphi(z)/z$ for all nonzero $y, z \in I$. To see this, first choose a nonzero $\gamma \in \mathcal{O}$ such that $\gamma y, \gamma z \in \mathcal{O}$ (such a choice is possible since I is a fractional $\mathcal{O}$-ideal). Then observe that

$$\begin{aligned}
\gamma\left(\frac{\varphi(y)}{y} - \frac{\varphi(z)}{z}\right) &= \gamma\left(\frac{z\varphi(y) - y\varphi(z)}{yz}\right) \\
&= \frac{\gamma z\varphi(y) - \gamma y\varphi(z)}{yz} \\
&= \frac{\varphi(\gamma zy) - \varphi(\gamma yz)}{yz} \\
&= 0.
\end{aligned}$$

This implies $\varphi(y)/y = \varphi(z)/z$ since $\mathcal{O}$ is an integral domain. Now write $x = \varphi(y)/y$ for some nonzero $y \in I$. Then for any nonzero $z \in I$, we have

$$\begin{aligned}
\varphi(z) &= \frac{\varphi(z)}{z} z \\
&= \frac{\varphi(y)}{y} z \\
&= xz \\
&= \mathrm{m}_x(z),
\end{aligned}$$

and since clearly $\varphi(0) = \mathrm{m}_x(0)$, we see that $\varphi = \mathrm{m}_x$. Thus $I \sim J$.

3.1 Main Theorem

Theorem 3.1. *Let $f(T) \in \mathbb{Z}[T]$ be a monic irreducible polynomial of degree n and let α be a root of $f(T)$. Then we have a bijection*

$$\mathrm{C}_n(\mathbb{Z}, f) \cong \mathrm{Cl}(\mathbb{Z}[\alpha]).$$

Proof. We define $\Psi \colon \mathrm{Cl}(\mathbb{Z}[\alpha]) \to \mathrm{C}_n(\mathbb{Z}, f)$ as follows: let $\mathfrak{a}$ be a $\mathbb{Z}[\alpha]$-fractional ideal. From the structure of finitely-generated torsion-free modules over $\mathbb{Z}$, we know that $\mathfrak{a}$ is a finitely-generated free $\mathbb{Z}$-module of rank n. Choose an ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, say $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$. Let $\mathrm{m}_\alpha \colon \mathfrak{a} \to \mathfrak{a}$ be the multiplication by α map, given by

$$\mathrm{m}_\alpha(x) = \alpha x$$

for all $x \in \mathfrak{a}$ and let $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} \in \mathrm{M}_n(\mathbb{Z})$ denote the matrix representation of m_α with respect to the basis $\mathbf{a}$. That is, the (i, j)'th entry in $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$ is given by $a_{ji} \in \mathbb{Z}$ where

$$\mathrm{m}_\alpha(\alpha_i) = \sum_{j=1}^{n} a_{ji}\alpha_j.$$

If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is another ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, then the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ is given by $[1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}} \in \mathrm{GL}_n(\mathbb{Z})$, and we have

$$\begin{aligned}
[1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}\left([1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}\right)^{-1} &= [1_{\mathfrak{a}}]_{\mathbf{a}'}^{\mathbf{a}}[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}[1_{\mathfrak{a}}]_{\mathbf{a}}^{\mathbf{a}'} \\
&= [1_{\mathfrak{a}} \circ \mathrm{m}_\alpha \circ 1_{\mathfrak{a}}]_{\mathbf{a}}^{\mathbf{a}}. \\
&= [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}
\end{aligned}$$

Thus changing the basis from $\mathbf{a}$ to $\mathbf{a}'$ corresponds to conjugating the matrix $[\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}$ to $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$.

We are now ready to define Ψ. We set

$$\Psi([\mathfrak{a}]) = [[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}]_{\mathrm{C}}. \tag{8}$$

We must check that (8) is in fact well-defined. Our construction of Ψ involved two choices. One choice that we made was in the choice of a basis for $\mathfrak{a}$ as free $\mathbb{Z}$-module (where we chose $\mathbf{a}$). By what was mentioned above, changing this basis to another basis would result in a matrix which is conjugate to $[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$ and hence would result in the same conjugacy class $[[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}]_{\mathrm{C}}$. The other choice that we made was in the choice of a representative of the $\mathbb{Z}[\alpha]$-ideal class $[\mathfrak{a}]$ (where we chose $\mathfrak{a}$) So let $\mathfrak{b}$ be another another coset representative of the coset $[\mathfrak{a}]$, so $\mathfrak{b} \sim \mathfrak{a}$. Choose $x \in \mathbb{Q}(\alpha)^\times$ such that $\mathfrak{b} = x\mathfrak{a}$. Then observe that $x\mathbf{a}$ is a basis for $\mathfrak{b}$ as a free $\mathbb{Z}$-module! Indeed, it clearly spans $\mathfrak{b}$ as a $\mathbb{Z}$-module since $\mathfrak{b} = x\mathfrak{a}$. Also, it is $\mathbb{Z}$-linearly independent since it is $\mathbb{Q}$-linearly independent (since multiplication by x is a $\mathbb{Q}$-isomorphism). Furthermore, it is easy to check that since $\mathrm{m}_x\mathrm{m}_\alpha = \mathrm{m}_\alpha\mathrm{m}_x$, we have

$$\begin{aligned}
[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} &= [\mathrm{m}_\alpha]_{x\mathbf{a}}^{x\mathbf{a}} \\
&= [\mathrm{m}_\alpha]_{\mathbf{b}}^{\mathbf{b}}.
\end{aligned}$$

Thus (8) is well-defined.

Now we show that Ψ is injective. Let $[\mathfrak{a}]$ and $[\mathfrak{a}']$ be two fractional $\mathcal{O}$-ideals and let $\mathbf{a}$ and $\mathbf{a}'$ be ordered bases for $\mathfrak{a}$ and $\mathfrak{a}'$ as free $\mathbb{Z}$-modules respectively. Suppose $\Psi([\mathfrak{a}]) = \Psi([\mathfrak{a}'])$, that is suppose

$$U[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} U^{-1} = [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}$$

for some $U \in \mathrm{GL}_n(\mathbb{Z})$. Let $[\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. That is $[\cdot]_{\mathbf{a}}$ is the unique $\mathbb{Z}$-linear map which sends α_i to e_i for all $1 \leq i \leq n$, where $\mathbf{e} = (e_1, \dots, e_n)$ is the standard ordered column basis for $\mathbb{Z}^n$ as a free $\mathbb{Z}$-module. Similarly, let $[\cdot]_{\mathbf{a}'} \colon \mathfrak{a}' \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. Then observe that $[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathfrak{a}'$ gives us an isomorphism of $\mathfrak{a}$ and $\mathfrak{a}'$ as $\mathbb{Z}$-modules. In fact, this is a $\mathbb{Z}[\alpha]$-isomorphism since it commutes with m_α. Indeed, we have

$$\begin{aligned}
[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \mathrm{m}_\alpha &= [\cdot]_{\mathbf{a}'}^{-1} U [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} [\cdot]_{\mathbf{a}} \\
&= [\cdot]_{\mathbf{a}'}^{-1} [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'} U [\cdot]_{\mathbf{a}} \\
&= \mathrm{m}_\alpha [\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}}.
\end{aligned}$$

Isomorphic fractional $\mathbb{Z}[\alpha]$-ideals are scalar multiples of each other, so $\mathfrak{a}' = x\mathfrak{a}$ for some $x \in \mathbb{Q}(\alpha)^\times$. In particular, $[\mathfrak{a}] = [\mathfrak{a}']$. Thus Ψ is injective.

Now let us show that Ψ is surjective. Let $A = (a_{ij})$ be in $\mathrm{M}_n(\mathbb{Z})$ such that $\chi_A(T) = f(T)$. We will find a $\mathbb{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ and a ordered basis $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ of $\mathfrak{a}$ as a free $\mathbb{Z}$-module such that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. First, we make $\mathbb{Q}^n$ into a $\mathbb{Q}(\alpha)$-vector space as follows: Let $x \in \mathbb{Q}(\alpha)$ and let $v \in \mathbb{Q}^n$. Choose $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$ (such a choice is possible since $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$). We define scalar multiplication of $\mathbb{Q}(\alpha)$ on $\mathbb{Q}^n$ by

$$x \cdot v = g(A)v. \tag{9}$$

We need to check that (9) is well-defined. In our construction of (9), we made a choice, namely $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$, so suppose $h(T) \in \mathbb{Q}[T]$ such that $h(\alpha) = x$. Then $(g - h)(\alpha) = 0$ and this implies $f \mid (g - h)$ (since f is the minimal polynomial of α over $\mathbb{Q}$ since it is monic and irreducible with root α) and therefore $g(A) = h(A)$ as matrices, so $g(A)v = h(A)v$ for all $v \in \mathbb{Q}^n$. Thus (9) is well-defined. It is straightforward to check that (9) gives $\mathbb{Q}^n$ a $\mathbb{Q}(\alpha)$-vector space structure. By restricting scalars, (9) also gives $\mathbb{Q}^n$ a $\mathbb{Z}[\alpha]$-module structure. In fact, if $v \in \mathbb{Z}^n$, then $\alpha \cdot v = Av$ is in $\mathbb{Z}^n$ since A has integral entries, so $\mathbb{Z}^n$ is a $\mathbb{Z}[\alpha]$-submodule of $\mathbb{Q}^n$. Treating $\mathbb{Q}^n$ as both a $\mathbb{Q}$-vector space and as a $\mathbb{Q}(\alpha)$-vector space, we have

$$\begin{aligned}
n &= \dim_{\mathbb{Q}}(\mathbb{Q}^n) \\
&= [\mathbb{Q}(\alpha) : \mathbb{Q}] \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \\
&= n \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n),
\end{aligned}$$

so $\mathbb{Q}^n$ is 1-dimensional as a $\mathbb{Q}(\alpha)$-vector space. In particular, this means that for any nonzero $v_0 \in \mathbb{Q}^n$, the $\mathbb{Q}(\alpha)$-linear map $\varphi_{v_0} \colon \mathbb{Q}(\alpha) \to \mathbb{Q}^n$ given by

$$\varphi_{v_0}(x) = x \cdot v_0$$

for all $x \in \mathbb{Q}(\alpha)$ is an isomorphism of 1-dimensional $\mathbb{Q}(\alpha)$-vector spaces. Thus, letting $\mathbf{e} = (e_1, \dots, e_n)$ denote the standard ordered column basis for $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space, there exists unique $\alpha_i \in \mathbb{Q}(\alpha)$ such that $\varphi_{v_0}(\alpha_i) = e_i$ for all $1 \leq i \leq n$. In particular, $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ is an ordered basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space. Let

$$\mathfrak{a} = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i.$$

Observe that $\mathfrak{a}$ is a $\mathbb{Z}[\alpha]$-fractional ideal. Indeed, it suffices to show that $\alpha\alpha_i \in \mathfrak{a}$ for all $1 \leq i \leq n$, and this follows from the fact that

$$\begin{aligned}
\varphi_{v_0}\left(\alpha\alpha_i - \sum_{j=1}^{n} a_{ji}\alpha_i\right) &= \alpha \cdot \varphi_{v_0}(\alpha_i) - \sum_{j=1}^{n} a_{ji}\varphi_{v_0}(\alpha_i) \\
&= \alpha \cdot e_i - \sum_{j=1}^{n} a_{ji} e_i \\
&= Ae_i - Ae_i \\
&= 0,
\end{aligned}$$

which implies

$$\alpha\alpha_i = \sum_{j=1}^{n} a_{ji}\alpha_i \tag{10}$$

since φ_{v_0} is injective. In fact, (10) also shows that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. So we have realized A as a matrix representation for m_α on a fractional $\mathbb{Z}[\alpha]$-ideal $\mathfrak{a}$. Thus Ψ is onto. $\square$

3.2 Example

Example 3.1. Let $f(T) = T^2 + 5$. We will count $\#\mathrm{C}_2(\mathbb{Z}, f)$ and we will find a coset representative for each conjugacy class in $\mathrm{C}_2(\mathbb{Z}, f)$. Note that f is a monic irreducible polynomial over $\mathbb{Z}$ and $\sqrt{-5}$ is a root of f. The ring $\mathbb{Z}[\sqrt{-5}]$ has class number 2, and so by Theorem (4.1), we see that $\#\mathrm{C}_2(\mathbb{Z}, f) = 2$. The ideal classes in $\mathbb{Z}[\sqrt{-5}]$ can be represented by $\mathbb{Z}[\sqrt{-5}] = \langle 1 \rangle$ and $\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-5} \rangle$. An ordered basis for $\mathbb{Z}[\sqrt{-5}]$ is given by $\mathbf{a}_1 = (1, \sqrt{-5})$ and an ordered basis for $\mathfrak{p}_2$ is given by $\mathbf{a}_2 = (2, 1 + \sqrt{-5})$. We calculate

$$\begin{aligned}
\sqrt{-5} \cdot 1 &= 0 \cdot 1 + 1 \cdot \sqrt{-5} \\
\sqrt{-5} \cdot \sqrt{-5} &= -5 \cdot 1 + 0 \cdot \sqrt{-5}.
\end{aligned}$$

Therefore $[\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_1}_{\mathbf{a}_1} = \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$. Similarly, we calculate

$$\begin{aligned} \sqrt{-5} \cdot 2 &= -1 \cdot 2 + 2 \cdot (1 + \sqrt{-5}) \\ \sqrt{-5} \cdot (1 + \sqrt{-5}) &= -3 \cdot 2 + 1 \cdot (1 + \sqrt{-5}). \end{aligned}$$

Therefore $[\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_2}_{\mathbf{a}_2} = \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. Thus if $A \in \mathrm{M}_2(\mathbb{Z})$ has characteristic polynomial $f(T)$, then $A \sim_{\mathrm{c}} \left(\begin{smallmatrix} 0 & -5 \\ 1 & 0 \end{smallmatrix}\right)$ or $A \sim_{\mathrm{c}} \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. Now let $\mathfrak{p}_7 = \langle 7, 3 + \sqrt{-5} \rangle$. Then $\mathfrak{p}_7 \sim \mathfrak{p}_2$ since

$$\mathfrak{p}_7 = \left(\frac{3 - \sqrt{-5}}{2} \right) \mathfrak{p}_2$$

An ordered basis for $\mathfrak{p}_7$ is given by $\mathbf{a}_7 = (7, 3 - \sqrt{-5})$. By a straightforward calculation, we have $[\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_7}_{\mathbf{a}_7} = \left(\begin{smallmatrix} 3 & 2 \\ -7 & -3 \end{smallmatrix}\right)$. Thus $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right) \sim_{\mathrm{c}} \left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$. To find the matrix which conjugates $\left(\begin{smallmatrix} -3 & -2 \\ 7 & 3 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -1 & -3 \\ 2 & 1 \end{smallmatrix}\right)$ we first change the ordered $\mathbb{Z}$-basis $\mathbf{a}_2$ of $\mathfrak{p}_2$ to the ordered $\mathbb{Z}$-basis $\mathbf{a}_2' = (2, 3 + \sqrt{-5})$. The change of basis matrix from $\mathbf{a}_2$ to $\mathbf{a}_2'$ is given by $[1_{\mathfrak{p}_2}]^{\mathbf{a}_2}_{\mathbf{a}_2'} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Similarly, we change the ordered $\mathbb{Z}$-basis $\mathbf{a}_7$ of $\mathfrak{p}_7$ to the ordered $\mathbb{Z}$-basis $\mathbf{a}_7' = (3 - \sqrt{-5}, 7)$. The change of basis matrix from $\mathbf{a}_7$ to $\mathbf{a}_7'$ is given by $[1_{\mathfrak{p}_7}]^{\mathbf{a}_7}_{\mathbf{a}_7'} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Next we observe that

$$\begin{aligned} \left(\frac{3 - \sqrt{-5}}{2} \right) \mathbf{a}_2' &= \left(\frac{3 - \sqrt{-5}}{2} \right) \left(2, 3 + \sqrt{-5} \right) \\ &= (3 - \sqrt{-5}, 7) \\ &= \mathbf{a}_7'. \end{aligned}$$

Therefore we have

$$\begin{aligned} \begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix} &= [\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_2}_{\mathbf{a}_2} \\ &= [1_{\mathfrak{p}_2}]^{\mathbf{a}_2}_{\mathbf{a}_2'} [\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_2'}_{\mathbf{a}_2'} [1_{\mathfrak{p}_2}]^{\mathbf{a}_2'}_{\mathbf{a}_2} \\ &= [1_{\mathfrak{p}_2}]^{\mathbf{a}_2}_{\mathbf{a}_2'} [\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_7'}_{\mathbf{a}_7'} [1_{\mathfrak{p}_2}]^{\mathbf{a}_2'}_{\mathbf{a}_2} \\ &= [1_{\mathfrak{p}_2}]^{\mathbf{a}_2}_{\mathbf{a}_2'} [1_{\mathfrak{p}_7}]^{\mathbf{a}_7'}_{\mathbf{a}_7} [\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_7}_{\mathbf{a}_7} [1_{\mathfrak{p}_7}]^{\mathbf{a}_7}_{\mathbf{a}_7'} [1_{\mathfrak{p}_2}]^{\mathbf{a}_2'}_{\mathbf{a}_2} \\ &= \left([1_{\mathfrak{p}_2}]^{\mathbf{a}_2}_{\mathbf{a}_2'} [1_{\mathfrak{p}_7}]^{\mathbf{a}_7'}_{\mathbf{a}_7} \right) [\mathrm{m}_{\sqrt{-5}}]^{\mathbf{a}_7}_{\mathbf{a}_7} \left([1_{\mathfrak{p}_7}]^{\mathbf{a}_2}_{\mathbf{a}_2'} [1_{\mathfrak{p}_2}]^{\mathbf{a}_7'}_{\mathbf{a}_7} \right)^{-1}. \\ &= \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right) \begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix} \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right)^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1}. \end{aligned}$$

The table below summarizes our calculations

Fractional Ideal	$[\mathrm{m}_{\sqrt{-5}}]$	Ordered $\mathbb{Z}$-Basis	$\sim$
$\langle 1 \rangle = \mathbb{Z}[\sqrt{-5}]$	$\begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$	$\mathbf{a}_1 = (1, \sqrt{-5})$	$\langle 1 \rangle = \langle 1 \rangle$
$\mathfrak{p}_2 = \langle 2, 1 + \sqrt{-5} \rangle$	$\begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}$	$\mathbf{a}_2 = (2, 1 + \sqrt{-5})$	$\mathfrak{p}_2 = \left(\frac{2}{3 - \sqrt{-5}} \right) \mathfrak{p}_7$
$\mathfrak{p}_7 = \langle 7, 3 - \sqrt{-5} \rangle$	$\begin{pmatrix} 3 & 2 \\ -7 & -3 \end{pmatrix}$	$\mathbf{a}_7 = (7, 3 + \sqrt{-5})$	$\mathfrak{p}_7 = \left(\frac{3 - \sqrt{-5}}{2} \right) \mathfrak{p}_2$

4 Generalizations

We now would like to generalize our results in Theorem (4.1). Let us consider the following example. Let $f(T) = T^2 + 2$. Then f is monic irreducible polynomial over $\mathbb{Q}$ and $\sqrt{-2}$ is a root of f. We compute a table similar to the one in Example (3.1):

Fractional Ideal	$[\mathrm{m}_{\sqrt{-2}}]$	Ordered $\mathbb{Z}$-Basis
$\mathbb{Z}[\sqrt{-2}]$	$\begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$	$\mathbf{a} = \{1, \sqrt{-2}\}$
$\mathbb{Z}[\sqrt{-2}]$	$\begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$	$\overline{\mathbf{a}} = (1, -\sqrt{-2})$

Now $\mathbb{Z}[\sqrt{-2}]$ has class number 1, so Theorem (4.1) tells us that the matrices $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ are conjugate. However, more specifically, when we say conjugate, we mean they $\mathrm{GL}_2(\mathbb{Z})$-conjugate. In fact, the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ conjugates $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$. Indeed, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

However note that $\det \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) = -1$, and so $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \notin \mathrm{SL}_2(\mathbb{Z})$. It's natural wonder if $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ are $\mathrm{SL}_2(\mathbb{Z})$-conjugate. It turns out that they are not even conjugate by an element of $\mathrm{SL}_2(\mathbb{Q})$. However, they are $\mathrm{SL}_2(\mathbb{Z}[\mathrm{i}])$-conjugate. The matrix $\left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}[i])$ conjugates $\left(\begin{smallmatrix} 0 & 2 \\ -1 & 0 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} 0 & -2 \\ 1 & 0 \end{smallmatrix}\right)$. Indeed, we have

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^{-1} = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}.$$

4.1 $\mathrm{SL}_n(\mathbb{Z})$-Conjugacy Classes of Matrices in $\mathrm{M}_n(\mathbb{Z})$

To improve Theorem (4.1), we introduce the following notation. We denote by $\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ to be the set of all $\mathrm{SL}_n(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$. Similarly, if $f(T) \in \mathbb{Z}[T]$ is a nonzero monic polynomial, then we denote by $\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ to be the set of all $\mathrm{SL}_n(\mathbb{Z})$-conjugacy classes of matrices in $\mathrm{M}_n(\mathbb{Z})$ with characteristic polynomial f.

4.1.1 Orientations

Let V be a nonzero $\mathbb{R}$-vector space with n and let $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ be an ordered basis of V. This gives rise to a nonzero vector

$$\wedge(\mathbf{a}) = \alpha_1 \wedge \cdots \wedge \alpha_n \in \Lambda^n(V)$$

in the line $\Lambda^n(V)$. If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is a second ordered basis, then $\wedge(\mathbf{a}')$ is another nonzero vector in the same line $\Lambda^n(V)$, so $\wedge(\mathbf{a}') = c \wedge (\mathbf{a})$ for a unique $c \in \mathbb{R}^\times$. Concretely, if $T_{\mathbf{a},\mathbf{a}'} \colon V \to V$ is the unique linear automorphism satisfying $\alpha_i' = T(\alpha_i)$ for all i (it is the "change of basis matrix" from $\mathbf{a}'$-coordinates to $\mathbf{a}$-coordinates), then $c = \det T_{\mathbf{a},\mathbf{a}'}$ and $1/c = \det T^{-1}_{\mathbf{a}',\mathbf{a}}$. Hence $c > 0$ if and only if $\wedge(\mathbf{a})$ and $\wedge(\mathbf{a}')$ lie in the same connected component of $\Lambda^n(V)\backslash\{0\}$.

Definition 4.1. An **orientation** μ on V is a choice of connected component of $\Lambda^n(V)\backslash\{0\}$, called the **positive component** with respect to μ. An **oriented vector space** is a nonzero vector space V equipped with a choice of orientation μ.

Definition 4.2. Let V be a $\mathbb{Q}$-vector space and let $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ and $\mathbf{a}' = (\alpha_1', \dots, \alpha_n)$ be two ordered bases of V. We say $\mathbf{a}$ and $\mathbf{a}'$ are **similarly oriented**, denoted $\mathbf{a} \sim_+ \mathbf{a}'$, if the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ has positive determinant, that is if

$$\det[1_V]^{\mathbf{a}}_{\mathbf{a}'} > 0.$$

It is straightforward to check that $\sim_+$ is an equivalence relation. Indeed, reflexivity and symmetry of $\sim_+$ are clear. For transitivity, suppose $\mathbf{a} \sim_+ \mathbf{a}'$ and $\mathbf{a}' \sim_+ \mathbf{a}''$. Then

$$\begin{aligned}\det[1_V]^{\mathbf{a}}_{\mathbf{a}''} &= \det\left([1_V]^{\mathbf{a}}_{\mathbf{a}'}[1_V]^{\mathbf{a}'}_{\mathbf{a}''}\right)\\ &= \det[1_V]^{\mathbf{a}}_{\mathbf{a}'}\det[1_V]^{\mathbf{a}'}_{\mathbf{a}''}\\ &> 0\end{aligned}$$

implies $\mathbf{a} \sim_+ \mathbf{a}''$. We shall denote by $[\mathbf{a}]_{\mathrm{o}}$ to by the $\sim_+$-equivalence class which is represented by the ordered basis $\mathbf{a}$. Clearly, there are just two $\sim_{\mathrm{o}}$-equivalence classes. An oriented $\mathbb{Q}$-vector space (V, μ_+) is a $\mathbb{Q}$-vector space V equipped with the choice of a $\sim_{\mathrm{o}}$-equivalence class, which we shall call the **positive orientation**. We shall also denote this equivalence class by μ_+. In this case, the other $\sim_{\mathrm{o}}$-equivalence class will be denoted by μ_-. Note that if $[\mathbf{a}]_{\mathrm{o}} = \mu_+$, then $[-\mathbf{a}]_{\mathrm{o}} = \mu_-$. If an ordered basis represents μ_+, then we say it is **positively oriented**. If an ordered basis represents μ_-, then we say it is **negatively oriented**. If (V, μ_+) and (W, ν_+) are two oriented n-dimensional $\mathbb{Q}$-vector spaces and $T \colon V \to W$ is a linear isomorphism, then we say T is **orientation-preserving** if $\det[T]^{\mathbf{b}}_{\mathbf{a}} > 0$, where $\mathbf{a}$ represents μ_+ and $\mathbf{b}$ represents ν_+.

4.1.2 Generalized Theorem

Theorem 4.1. *Let $f(T) \in \mathbb{Z}[T]$ be a monic irreducible polynomial of degree n and let α be a root of $f(T)$. Then we have a bijection*

$$\mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f) \cong \mathrm{Cl}_+(\mathbb{Z}[\alpha]).$$

Proof. We define $\Psi \colon \mathrm{Cl}_+(\mathbb{Z}[\alpha]) \to \mathrm{C}_{\mathrm{SL}_n(\mathbb{Z})}(\mathbb{Z}, f)$ as follows: let $\mathfrak{a}$ be a $\mathbb{Z}[\alpha]$-fractional ideal. From the structure of finitely-generated torsion-free modules over $\mathbb{Z}$, we know that $\mathfrak{a}$ is a finitely-generated free $\mathbb{Z}$-module of rank n. Choose a positive ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, say $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$. Let $\mathrm{m}_\alpha \colon \mathfrak{a} \to \mathfrak{a}$ be the multiplication by α map and let $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}} \in \mathrm{M}_n(\mathbb{Z})$ denote the matrix representation of m_α with respect to $\mathbf{a}$. If $\mathbf{a}' = (\alpha_1', \dots, \alpha_n')$ is another positive ordered basis of $\mathfrak{a}$ as a free $\mathbb{Z}$-module, then the change of basis matrix from $\mathbf{a}$ to $\mathbf{a}'$ is given by $[1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'} \in \mathrm{SL}_n(\mathbb{Z})$ since both $\mathbf{a}$ and $\mathbf{a}'$ are positive, and hence $\det[1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'} > 0$ which implies $\det[1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'} = 1$. Furthermore, we have

$$\begin{aligned}[1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'}[\mathrm{m}_\alpha]^{\mathbf{a}'}_{\mathbf{a}'}\left([1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'}\right)^{-1} &= [1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}'}[\mathrm{m}_\alpha]^{\mathbf{a}'}_{\mathbf{a}'}[1_{\mathfrak{a}}]^{\mathbf{a}'}_{\mathbf{a}}\\ &= [1_{\mathfrak{a}} \circ \mathrm{m}_\alpha \circ 1_{\mathfrak{a}}]^{\mathbf{a}}_{\mathbf{a}}.\\ &= [\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}.\end{aligned}$$

Thus changing the positive basis from $\mathbf{a}$ to $\mathbf{a}'$ corresponds to a $\mathrm{SL}_n(\mathbb{Z})$-conjugate matrix of $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}$.

We are now ready to define Ψ. We set

$$\Psi([\mathfrak{a}]) = [[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}]_{\mathrm{c}}. \tag{11}$$

We must check that (8) is in fact well-defined. Our construction of Ψ involved two choices. One choice that we made was in the choice of a positive orderd basis for $\mathfrak{a}$ as free $\mathbb{Z}$-module (where we chose $\mathbf{a}$). By what was mentioned above, changing this basis to another basis would result in a matrix which is $\mathrm{SL}_n(\mathbb{Z})$-conjugate to $[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}$ and hence would result in the same conjugacy class $[[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}}]_{\mathrm{c}}$. The other choice that we made was in the choice of a representative of the $\mathbb{Z}[\alpha]$-ideal class $[\mathfrak{a}]$ (where we chose $\mathfrak{a}$) So let $\mathfrak{b}$ be another another coset representative of the coset $[\mathfrak{a}]$, so $\mathfrak{b} \sim \mathfrak{a}$. Choose $x \in \mathbb{Q}(\alpha)^\times$ such $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x) > 0$ and $\mathfrak{b} = x\mathfrak{a}$. Then observe that $x\mathbf{a}$ is a positively oriented ordered basis for $\mathfrak{b}$ as a free $\mathbb{Z}$-module! Indeed, it clearly spans $\mathfrak{b}$ as a $\mathbb{Z}$-module since $\mathfrak{b} = x\mathfrak{a}$. Also, it is $\mathbb{Z}$-linearly independent since it is $\mathbb{Q}$-linearly independent (since multiplication by x is a $\mathbb{Q}$-isomorphism). It is also positively oriented precisely because $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x) > 0$. Furthermore, it is easy to check that since $\mathrm{m}_x\mathrm{m}_\alpha = \mathrm{m}_\alpha\mathrm{m}_x$, we have

$$\begin{aligned}[\mathrm{m}_\alpha]^{\mathbf{a}}_{\mathbf{a}} &= [\mathrm{m}_\alpha]^{x\mathbf{a}}_{x\mathbf{a}}\\ &= [\mathrm{m}_\alpha]^{\mathbf{b}}_{\mathbf{b}}.\end{aligned}$$

Thus (8) is well-defined.

Now we show that Ψ is injective. Let $[\mathfrak{a}]$ and $[\mathfrak{a}']$ be two fractional $\mathcal{O}$-ideals and let $\mathbf{a}$ and $\mathbf{a}'$ be ordered bases for $\mathfrak{a}$ and $\mathfrak{a}'$ as free $\mathbb{Z}$-modules respectively. Suppose $\Psi([\mathfrak{a}]) = \Psi([\mathfrak{a}'])$, that is suppose

$$U[\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} U^{-1} = [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'}$$

for some $U \in \mathrm{SL}_n(\mathbb{Z})$. Let $[\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. That is $[\cdot]_{\mathbf{a}}$ is the unique $\mathbb{Z}$-linear map which sends α_i to e_i for all $1 \le i \le n$, where $\mathbf{e} = (e_1, \dots, e_n)$ is the standard ordered column basis for $\mathbb{Z}^n$ as a free $\mathbb{Z}$-module. Similarly, let $[\cdot]_{\mathbf{a}'} \colon \mathfrak{a}' \to \mathbb{Z}^n$ be the standard column representation map for $\mathfrak{a}$. Then observe that $[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \colon \mathfrak{a} \to \mathfrak{a}'$ gives us an isomorphism of $\mathfrak{a}$ and $\mathfrak{a}'$ as $\mathbb{Z}$-modules. In fact, this is a $\mathbb{Z}[\alpha]$-isomorphism since it commutes with m_α. Indeed, we have

$$\sigma[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \sigma^{-1} = [\cdot]_{\sigma\mathbf{a}'}^{-1} [\sigma]_{\mathbf{a}'}^{\sigma\mathbf{a}'} U [\sigma^{-1}]_{\sigma\mathbf{a}}^{\mathbf{a}} [\cdot]_{\sigma\mathbf{a}}$$

$$\begin{aligned}
[\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}} \mathrm{m}_\alpha &= [\cdot]_{\mathbf{a}'}^{-1} U [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}} [\cdot]_{\mathbf{a}} \\
&= [\cdot]_{\mathbf{a}'}^{-1} [\mathrm{m}_\alpha]_{\mathbf{a}'}^{\mathbf{a}'} U [\cdot]_{\mathbf{a}} \\
&= \mathrm{m}_\alpha [\cdot]_{\mathbf{a}'}^{-1} U [\cdot]_{\mathbf{a}}.
\end{aligned}$$

Isomorphic fractional $\mathbb{Z}[\alpha]$-ideals are scalar multiples of each other, so $\mathfrak{a}' = x\mathfrak{a}$ for some $x \in \mathbb{Q}(\alpha)^\times$. In particular, $[\mathfrak{a}] = [\mathfrak{a}']$. Thus Ψ is injective.

Now let us show that Ψ is surjective. Let $A = (a_{ij})$ be in $\mathrm{M}_n(\mathbb{Z})$ such that $\chi_A(T) = f(T)$. We will find a $\mathbb{Z}[\alpha]$-fractional ideal $\mathfrak{a}$ and a ordered basis $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ of $\mathfrak{a}$ as a free $\mathbb{Z}$-module such that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. First, we make $\mathbb{Q}^n$ into a $\mathbb{Q}(\alpha)$-vector space as follows: Let $x \in \mathbb{Q}(\alpha)$ and let $v \in \mathbb{Q}^n$. Choose $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$ (such a choice is possible since $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$). We define scalar multiplication of $\mathbb{Q}(\alpha)$ on $\mathbb{Q}^n$ by

$$x \cdot v = g(A)v. \tag{12}$$

We need to check that (9) is well-defined. In our construction of (9), we made a choice, namely $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$, so suppose $h(T) \in \mathbb{Q}[T]$ such that $h(\alpha) = x$. Then $(g-h)(\alpha) = 0$ and this implies $f \mid (g-h)$ (since f is the minimal polynomial of α over $\mathbb{Q}$ since it is monic and irreducible with root α) and therefore $g(A) = h(A)$ as matrices, so $g(A)v = h(A)v$ for all $v \in \mathbb{Q}^n$. Thus (9) is well-defined. It is straightforward to check that (9) gives $\mathbb{Q}^n$ a $\mathbb{Q}(\alpha)$-vector space structure. By restricting scalars, (9) also gives $\mathbb{Q}^n$ a $\mathbb{Z}[\alpha]$-module structure. In fact, if $v \in \mathbb{Z}^n$, then $\alpha \cdot v = Av$ is in $\mathbb{Z}^n$ since A has integral entries, so $\mathbb{Z}^n$ is a $\mathbb{Z}[\alpha]$-submodule of $\mathbb{Q}^n$. Treating $\mathbb{Q}^n$ as both a $\mathbb{Q}$-vector space and as a $\mathbb{Q}(\alpha)$-vector space, we have

$$\begin{aligned}
n &= \dim_{\mathbb{Q}}(\mathbb{Q}^n) \\
&= [\mathbb{Q}(\alpha) : \mathbb{Q}] \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n) \\
&= n \dim_{\mathbb{Q}(\alpha)}(\mathbb{Q}^n),
\end{aligned}$$

so $\mathbb{Q}^n$ is 1-dimensional as a $\mathbb{Q}(\alpha)$-vector space. In particular, this means that for any nonzero $v_0 \in \mathbb{Q}^n$, the $\mathbb{Q}(\alpha)$-linear map $\varphi_{v_0} \colon \mathbb{Q}(\alpha) \to \mathbb{Q}^n$ given by

$$\varphi_{v_0}(x) = x \cdot v_0$$

for all $x \in \mathbb{Q}(\alpha)$ is an isomorphism of 1-dimensional $\mathbb{Q}(\alpha)$-vector spaces. Thus, letting $\mathbf{e} = (e_1, \dots, e_n)$ denote the standard ordered column basis for $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space, there exists unique $\alpha_i \in \mathbb{Q}(\alpha)$ such that $\varphi_{v_0}(\alpha_i) = e_i$ for all $1 \le i \le n$. In particular, $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$ is an ordered basis for $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space. Let

$$\mathfrak{a} = \bigoplus_{i=1}^n \mathbb{Z}\alpha_i.$$

Observe that $\mathfrak{a}$ is a $\mathbb{Z}[\alpha]$-fractional ideal. Indeed, it suffices to show that $\alpha\alpha_i \in \mathfrak{a}$ for all $1 \le i \le n$, and this follows from the fact that

$$\begin{aligned}
\varphi_{v_0}\left(\alpha\alpha_i - \sum_{j=1}^n a_{ji}\alpha_i\right) &= \alpha \cdot \varphi_{v_0}(\alpha_i) - \sum_{j=1}^n a_{ji}\varphi_{v_0}(\alpha_i) \\
&= \alpha \cdot e_i - \sum_{j=1}^n a_{ji} e_i \\
&= Ae_i - Ae_i \\
&= 0,
\end{aligned}$$

which implies

$$\alpha\alpha_i = \sum_{j=1}^n a_{ji}\alpha_i \tag{13}$$

since φ_{v_0} is injective. In fact, (10) also shows that $A = [\mathrm{m}_\alpha]_{\mathbf{a}}^{\mathbf{a}}$. So we have realized A as a matrix representation for m_α on a fractional $\mathbb{Z}[\alpha]$-ideal $\mathfrak{a}$. Thus Ψ is onto. $\square$

5 Galois extensions, Frobenius elements, and the Artin map

Let A be a Dedekind domain with fraction field K, let L/K a finite separable extension, let B be the integral closure of A in L. We use $AKLB$ to denote this setup. Furthermore, suppose L/K is also normal, hence Galois, and let $G := \mathrm{Gal}(L/K)$ to denote the Galois group; we will use $AKLBG$ to denote this setup.

5.1 Splitting primes in Galois extensions

Unless otherwise specified, we assume the *AKLBG* setup.

Theorem 5.1. *For each fractional ideal $\mathfrak{b}$ of B and $\sigma \in G$ define*

$$\sigma\mathfrak{b} = \{\sigma(y) \mid y \in \mathfrak{b}\}.$$

The set $\sigma\mathfrak{b}$ is a fractional ideal of B, and this defines a group action on $\mathcal{I}_B$ that makes it into a left G-module. Moreover, the restriction of this action to Spec B *makes it a G-set.*

Proof. First let's recall why $\sigma B = B$ for all $\sigma \in G$. If $b \in B$, then it is a root of a monic polyomial $f \in A[x]$, that is, $f(b) = 0$. Then $f(\sigma b) = \sigma f(b) = 0$ implies σb is also a root of the monic polynomial f. Thus σb is integral over A, hence an element of B. This proves $\sigma B \subseteq B$, and the same argument shows $\sigma^{-1}B \subseteq B$, hence $B \subseteq \sigma B$. It follows that $\sigma B = B$.

Now let $\mathfrak{b} \in \mathcal{I}_B$. Then $\mathfrak{b}$ is a finitely generated B-module contained L, say $\mathfrak{b} = \langle y_1, \ldots, y_n\rangle$. But then $\sigma\mathfrak{b} = \langle \sigma y_1, \ldots, \sigma y_n\rangle$ is a finitely generated σB-module contained in L. Since $\sigma B = B$, it follows that $\sigma\mathfrak{b}$ is a finitely generated B-module contained in L, hence a fractional ideal of B. Note that if $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathcal{I}_B$, then

$$\sigma(\mathfrak{b}_1\mathfrak{b}_2) = (\sigma\mathfrak{b}_1)(\sigma\mathfrak{b}_2),$$

since σ preserves addition and multiplication. Since we already obviously have $(\sigma\tau)\mathfrak{b} = \sigma(\tau\mathfrak{b})$ where $\tau \in G$, it follows that $\mathcal{I}_B$ is a left G-module.

Finally, let $\mathfrak{q}$ be a prime of B and let $\sigma\mathfrak{q} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$ be the unique factorization of $\sigma\mathfrak{q}$ in B. Applying σ^{-1} to both sides yields $\mathfrak{q} = (\sigma^{-1}\mathfrak{q}_1)^{e_1} \cdots (\sigma^{-1}\mathfrak{q}_n)^{e_n}$, and therefore $n = 1$ and $e_1 = 1$, since $\mathfrak{q}$ is prime, thus $\sigma\mathfrak{q} = \mathfrak{q}_1$ is prime and the G-action on $\mathcal{I}_B$ restricts to a G-action on MaxSpec B, and on Spec B, since G fixes the zero ideal. □

Corollary 3. *For each pime $\mathfrak{p}$ of A the group G acts transitively on the set $\{\mathfrak{q}|\mathfrak{p}\}$. In other words, the orbits of the G-action on* Spec B *are the fibers of the contraction map* Spec $B \to$ Spec A.

Proof. Let $\sigma \in G$. For $\mathfrak{q}|\mathfrak{p}$ we have $\mathfrak{p}B \subseteq \mathfrak{q}$ and $\sigma(\mathfrak{p}B) \subseteq \sigma\mathfrak{q}$. Thus $\{\mathfrak{q}|\mathfrak{p}\}$ is closed under the action of G, so we just need to show that it consists of a single orbit. Let $\{\mathfrak{q}|\mathfrak{p}\} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ and suppose that $\mathfrak{q}_1$ and $\mathfrak{q}_2$ lie in distinct G-orbits. The primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are maximal ideals, hence pairwise coprime, so by the CRT we have a ring isomorphism

$$B/\mathfrak{q}_1 \cdots \mathfrak{q}_n \simeq B/\mathfrak{q}_1 \times \cdots \times B/\mathfrak{q}_n,$$

and we may choose $b \in B$ such that $b \equiv 0 \bmod \mathfrak{q}_2$ and $b \equiv 1 \bmod \sigma^{-1}\mathfrak{q}_1$ for all $\sigma \in G$. Then $b \in \mathfrak{q}_2$ and

$$\mathrm{N}_{L/K}(b) = \prod_{\sigma \in G} \sigma(b) \equiv 1 \bmod \mathfrak{q}_1,$$

hence $\mathrm{N}_{L/K}(b) \notin A \cap \mathfrak{q}_1 = \mathfrak{p}$. However $\mathrm{N}_{L/K}(b) \in \mathrm{N}_{L/K}(\mathfrak{q}_2) = \mathfrak{p}^{f_{\mathfrak{q}_2}} \subseteq \mathfrak{p}$, a contradiction. □

As shown in the proof of Theorem (5.1), we have $\sigma B = B$ for all $\sigma \in G$, thus each $\sigma \in G$ restricts to a ring automorphism of B that fixes every element of the subring $A = B \cap K$, and thus every element of any prime $\mathfrak{p}$ of A. It follows that σ induces an isomorphism of residue field extensions $\overline{\sigma} \in \mathrm{Hom}_{A/\mathfrak{p}}(B/\mathfrak{q}, B/\sigma\mathfrak{q})$ defined by $\overline{\sigma}(b + \mathfrak{q}) = \sigma b + \sigma\mathfrak{q}$ for all $b \in B$, which we may write more compactly as $\overline{\sigma}(\overline{b}) = \overline{\sigma(b)}$.

Corollary 4. *Let $\mathfrak{p}$ be a prime of A. The residue field degrees $f_{\mathfrak{q}} := [B/\mathfrak{q} : A/\mathfrak{p}]$ are the same for every $\mathfrak{q}|\mathfrak{p}$, as are the ramification indices $e_{\mathfrak{q}} := v_{\mathfrak{q}}(\mathfrak{p}B)$.*

Proof. For each $\sigma \in G$ we have an isomorphism of the residue fields $B/\mathfrak{q}$ and $B/\sigma\mathfrak{q}$ that fixes $A/\mathfrak{p}$, so they clearly have the same degree $f_{\mathfrak{q}} = f_{\sigma\mathfrak{q}}$, and G acts transitively on $\{\mathfrak{q}|\mathfrak{p}\}$, thus by the previous corollary, the function $\mathfrak{q} \mapsto f_{\mathfrak{q}}$ must be constant on $\{\mathfrak{q}|\mathfrak{p}\}$. Furthermore, we have

$$\begin{aligned} e_{\mathfrak{q}} &= v_{\mathfrak{q}}(\mathfrak{p}B) \\ &= v_{\mathfrak{q}}(\sigma(\mathfrak{p}B)) \\ &= v_{\mathfrak{q}}\left(\sigma \prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_{\mathfrak{r}}}\right) \\ &= v_{\mathfrak{q}}\left(\prod_{\mathfrak{r}|\mathfrak{p}} (\sigma\mathfrak{r})^{e_{\mathfrak{r}}}\right) \\ &= v_{\mathfrak{q}}\left(\prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_{\sigma^{-1}\mathfrak{r}}}\right) \\ &= e_{\sigma^{-1}\mathfrak{r}}. \end{aligned}$$

The transitivity of the G-action on $\{\mathfrak{q}|\mathfrak{p}\}$ again implies that $\mathfrak{q} \mapsto e_{\mathfrak{q}}$ is constant on $\{\mathfrak{q}|\mathfrak{p}\}$. □

Corollary 5. *For each prime $\mathfrak{p}$ of A we have $e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = [L : K]$.*

Proposition 5.1. *Let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. The group homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ defined by $\sigma \mapsto \overline{\sigma}$ is surjective and $B/\mathfrak{q}$ is normal over $A/\mathfrak{p}$.*

Proof. Let F be the separable closure of $A/\mathfrak{p}$ in $B/\mathfrak{q}$ and for $\overline{b} \in F$, pick $b \in B$ such that $b \equiv \overline{b} \bmod \mathfrak{q}$ and $b \equiv 0 \bmod \sigma^{-1}\mathfrak{q}$ (so $\sigma(b) \equiv 0 \bmod \mathfrak{q}$) for all $\sigma \in G \backslash D_{\mathfrak{q}}$; the CRT implies that such a b exists, since for $\sigma \in G \backslash D_{\mathfrak{q}}$ the ideals $\mathfrak{q}$ and $\sigma\mathfrak{q}$ are distinct and therefore coprime (since they are maximal ideals). Now define

$$g(x) := \prod_{\sigma \in G} (x - \sigma(b)) \in A[x],$$

and let $\overline{g}$ denote the image of g in $(A/\mathfrak{p})[x]$. Observe that $\overline{b}$ is the root of a polynomial $\overline{g} \in (A/\mathfrak{p})[x]$ that splits completely in $(B/\mathfrak{q})[x]$, and our choice of $\overline{b}$ was arbitrary, so this applies to every $\overline{b} \in F^\times$. It follows that F is a normal (hence Galois) extension of $A/\mathfrak{p}$, and we have

$$\mathrm{Gal}(F/(A/\mathfrak{p})) \simeq \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}),$$

since F is the separable closure of $A/\mathfrak{p}$ in $B/\mathfrak{q}$.

Now observe that in in $(B/\mathfrak{q})[x]$, we have

$$\overline{g}(x) = \prod_{\sigma \in G}(x - \overline{\sigma b}) = x^m \prod_{\sigma \in D_\mathfrak{q}}(x - \overline{\sigma b})$$

where we set $m = \#(G \backslash D_\mathfrak{q})$. So 0 is a root of $\overline{g}(x)$ with multiplicity at least m and the remaining roots are $\overline{\sigma b}$ for $\sigma \in D_\mathfrak{q}$, all of which are $\mathrm{Gal}(F/(A/\mathfrak{p}))$-conjugates of $\overline{b}$. It follows that $\overline{g}(x)/x^m$ divides a power of the minimal polynomial $f(x)$ of $\overline{b}$, but $f(x)$ is irreducible in $(A/\mathfrak{p})[x]$, so $\overline{g}(x)/x^m$ is a power of $f(x)$ and every $\mathrm{Gal}(F/(A/\mathfrak{p}))$-conjugate of $\overline{b}$ has the form $\overline{\sigma b}$ for some $\sigma \in D_\mathfrak{q}$. Applying this to $\overline{b}$ chosen such that $F = (A/\mathfrak{p})(\overline{b})$ (by the primitive element theorem) shows that the map

$$\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \simeq \mathrm{Gal}(F/(A/\mathfrak{p}))$$

is surjective.

To show that $B/\mathfrak{q}$ is a normal extension of $A/\mathfrak{p}$ we proceed as we did for F: for each $b \in B$ define $g \in A[x]$ and $\overline{g} \in (A/\mathfrak{p})[x]$ as above to show that every $b \in B/\mathfrak{q}$ is the root of a polynomial in $(A/\mathfrak{p})[x]$ that splits completely in $(B/\mathfrak{q})[x]$. ☐

Definition 5.1. Let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. The kernel of the surjective homomorphism $\pi_\mathfrak{q} \colon D_\mathfrak{q} \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q})$ is the **inertia group** $I_\mathfrak{q}$ of $\mathfrak{q}$.

Corollary 6. *We have an exact sequence*

$$1 \to I_\mathfrak{q} \to D_\mathfrak{q} \to \mathrm{Aut}_{A/\mathfrak{p}}(B/\mathfrak{q}) \to 1$$

and $\#I_\mathfrak{q} = e_\mathfrak{p}[B/\mathfrak{q} : A/\mathfrak{p}]_i$.

5.2 Frobenius elements

We now add the further assumption that the residue fields $A/\mathfrak{p}$ (and therefore $B/\mathfrak{q}$) are finite for all primes $\mathfrak{p}$ of A. This holds, for example, whenever K is a global field (a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$). In this situation $B/\mathfrak{q}$ is necessarily a Galois extension of $A/\mathfrak{p}$. Indeed, recall that every finite extension of a finite field $\mathbb{F}$ has a cyclic Galois group generated by the $\#\mathbb{F}$-power Frobenius automorphism $x \mapsto x^{\#\mathbb{F}}$.

In order to simplify notation, when working with finite residue fields we may write $\mathbb{F}_\mathfrak{q} := B/\mathfrak{q}$ and $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$; these are finite fields of p-power order, where p is the characteristic of $\mathbb{F}_p$ (and of $\mathbb{F}_\mathfrak{q}$). Note that the field K (and L) need not have characteristic p (consider the case of number fields), but if the characteristic of K is positive then it must be p (consider the homomorphism $A \to A/\mathfrak{p}$ from the integral domain A to the field $A/\mathfrak{p}$) .

Let $\mathfrak{q}|\mathfrak{p}$ be a prime of B. We have a short exact sequence

$$1 \to I_\mathfrak{q} \to D_\mathfrak{q} \xrightarrow{\pi_\mathfrak{q}} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}) \to 1.$$

If $\mathfrak{p}$ (equivalently, $\mathfrak{q}$) is unramified, then $e_\mathfrak{p} = e_\mathfrak{q} = 1$ and $I_\mathfrak{q}$ is trivial. In this case we have an isomorphism

$$\pi_\mathfrak{q} \colon D_\mathfrak{q} \xrightarrow{\simeq} \mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p}).$$

The Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ is the cyclic group of order $f_\mathfrak{p} = [\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}]$ generated by the Frobenius automorphism

$$x \mapsto x^{\#\mathbb{F}_\mathfrak{p}}.$$

Note that the cardinality of the finite field $\mathbb{F}_\mathfrak{p}$ is necessarily a power of its characteristic p.

Definition 5.2. Assume *AKLBG* with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. The inverse image of the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_\mathfrak{q}/\mathbb{F}_\mathfrak{p})$ under $\pi_\mathfrak{q}$ is the **Frobenius element** $\sigma_\mathfrak{q} \in D_\mathfrak{q} \subseteq G$.

Proposition 5.2. *Assume AKLBG with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified. The Frobenius element $\sigma_\mathfrak{q}$ is the unique $\sigma \in G$ such that for all $b \in B$ we have*

$$\sigma b \equiv b^{\#\mathbb{F}_\mathfrak{p}} \bmod \mathfrak{q}.$$

Proposition 5.3. *Assume AKLBG with finite residue fields and $\mathfrak{q}|\mathfrak{p}$ unramified For all $\mathfrak{q}'|\mathfrak{p}$ the Frobenius elements $\sigma_\mathfrak{q}$ and $\sigma_{\mathfrak{q}'}$ are conjugate in G.*

Definition 5.3. The conjugacy class of the Frobenius element $\sigma_\mathfrak{q} \in G$ is the **Frobenius class** of $\mathfrak{p}$, denoted $\mathrm{Frob}_\mathfrak{p}$.

5.3 Artin symbols

There is another notation commonly used to denote Frobenius elements that includes the field extension in the notation.

Definition 5.4. Assume *AKLBG* with finite residue fields. For each unramified prime $\mathfrak{q}$ of B we define the **Artin symbol**

$$\left(\frac{L/K}{\mathfrak{q}}\right) := \sigma_\mathfrak{q}.$$

When L/K is abelian, the Artin symbol takes the same value for all $\mathfrak{q}|\mathfrak{p}$ and we may write

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma_\mathfrak{p}.$$

instead. In this setting we now view the Artin symbol as a function mapping unramified primes $\mathfrak{p}$ to Frobenius elements $\sigma_{\mathfrak{p}} \in G$. We wish to extend this map to a multiplicative homomorphism from the ideal group $\mathcal{I}_A$ to the Galois group $G = \mathrm{Gal}(L/K)$, but ramified primes $\mathfrak{q}|\mathfrak{p}$ cause problems: the homomorphism $\pi_{\mathfrak{q}} \colon D_{\mathfrak{q}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is not a bijection when $\mathfrak{p}$ is ramified (it has nontrivial kernel $I_{\mathfrak{q}}$ of order $e_{\mathfrak{q}} = e_{\mathfrak{p}} > 1$). For any set S of primes of A, let $\mathcal{I}_A^S$ denote the subgroup of $\mathcal{I}_A$ generated by the primes of A that do not lie in S.

Definition 5.5. Let A be a Dedekind domain with finite residue fields. Let L be a finite abelian extension of $K = \mathrm{Frac}\, A$, and let S be the set of primes of A that ramify in L. The **Artin map** is the homomorphism

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_A^S \to \mathrm{Gal}(L/K)$$

defined by

$$\prod_{i=1}^{m} \mathfrak{p}_i^{e_i} \mapsto \prod_{i=1}^{m} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}.$$

One of the main results of class field theory is that the Artin map is surjective (this is part of what is known as Artin reciprocity). This is a deep theorem that we are not yet ready to prove, but we can verify that it holds in some simple examples.

Example 5.1. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d \neq 1$. Then $\mathrm{Gal}(L/K)$ has order 2 and is certainly abelian. Furthermore, the only ramified primes $\mathfrak{p} = (p)$ of $A = \mathbb{Z}$ are those that divide the discriminant

$$D := \mathrm{disc}(L/K) = \begin{cases} d & \text{if } d \equiv 1 \bmod 4, \\ 4d & \text{if } d \not\equiv 1 \bmod 4. \end{cases}$$

If we identify $\mathrm{Gal}(L/K)$ with the multiplicative group $\{\pm 1\}$, then

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\frac{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}{(p)}\right) = \left(\frac{D}{p}\right) = \pm 1,$$

where $\left(\frac{D}{p}\right)$ is the **Kronecker symbol**. For odd primes $p \nmid D$ we have

$$\left(\frac{D}{p}\right) = \begin{cases} 1 & \text{if } D \text{ is a nonzero square modulo } p, \\ -1 & \text{if } D \text{ is not a square modulo } p, \end{cases}$$

and for $p = 2$ not dividing D (in which case $D = d \equiv 1 \bmod 4$) we have

$$\left(\frac{D}{2}\right) = \begin{cases} 1 & \text{if } D \equiv 1 \bmod 8, \\ -1 & \text{if } D \equiv 5 \bmod 8. \end{cases}$$

6 Weil Cohomology

Let K be a number field. The **Dedekind zeta function** of K is defined to be the formal expression

$$\zeta_K(s) := \prod_{\mathfrak{p}} \frac{1}{1 - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

where $s \in \mathbb{C}$ and where the product runs over of all primes $\mathfrak{p}$ of $\mathcal{O}_K$. The product converges absolutely for $\mathrm{Re}(s) > 1$ and hence defines a holomorphic function without zeroes in that region. By unique factorization, we can rewrite the product as a sum

$$\zeta_K(s) = \sum_I \mathrm{N}_{K/\mathbb{Q}}(I)^{-s}$$

where the sum runs over all nonzero ideals I of $\mathcal{O}_K$.

Theorem 6.1. *The function $\zeta_K(s)$ extends meromorphically to $\mathbb{C}$, with a simple pole at $s = 1$ and with no other poles.*

Part II
Elliptic Curves

Definition 6.1. Let $\Bbbk$ be a field. An **elliptic curve** $E/\Bbbk$ is a smooth projective curve of genus 1 defined over $\Bbbk$ with a distinguished $\Bbbk$-rational point O.

Let $C = \mathrm{V}(f) \subseteq \mathbb{P}^2$ where

$$f = c_1x^3 + c_2x^2y + c_3x^2z + c_4xy^2 + c_5xyz + c_6xz^2 + c_7y^3 + c_8y^2z + c_9yz^2 + c_{10}z^3 \tag{14}$$

where $c_1, \dots, c_{10} \in \overline{\Bbbk}$ (if $c_1 \dots, c_{10} \in \Bbbk$, then we say C is **defined** over $\Bbbk$). Let $C_\infty = C \cap \mathrm{V}(z)$ be the points of C which lie on the line at infinity $\mathrm{V}(z)$. Thus the points of C_∞ are given by $\{(x : y : 0) \mid f_{z=0}(x, y) = 0\}$ where

$$f_{z=0} = c_1x^3 + c_2x^2y + c_4xy^2 + c_7y^3.$$

The the points of C_∞ are in bijection with $\mathrm{V}(f_{z=0}) \subseteq \mathbb{P}^1$. Since $f_{z=0}$ is a cubic, there are exactly three points of $\mathrm{V}(f_{z=0})$, counting multiplicity. We want $O = [0 : 1 : 0]$ to be the *only* point in C_∞ (which would also mean that O has multiplicity three). In order for this to happen, we must have $c_2 = c_4 = c_7 = 0$ and $c_1 \neq 0$. With this in mind, we can rewrite (14) as

$$f = c_1x^3 + c_3x^2z + c_5xyz + c_6xz^2 + c_8y^2z + c_9yz^2 + c_{10}z^3.$$

By re-scaling if necessary, we may assume that $c_1 = 1$. Next, we want C to be a smooth curve, so in particular we want it to be smooth at O. A calculation gives us

$$\begin{aligned}(\partial_x f)(O) &= 0\\ (\partial_y f)(O) &= 0\\ (\partial_z f)(O) &= c_8.\end{aligned}$$

Thus in order for C to be smooth at O, it is necessary that $c_8 \neq 0$. Then by replacing z with $-z/c_8$, we obtain a curve which is projectively equivalent C whose equation has the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{15}$$

where $a_1, \dots, a_6 \in \Bbbk$ (it will be become clear why the coefficients are labeled this way). We generally work in the affine open $\mathrm{D}(z)$ which corresponds to setting $z = 1$ in (15):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If $\mathrm{char}(\Bbbk) \neq 2$, then we can simplify the equation by completing the square. Thus the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ yields the equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in \Bbbk$.

6.1 Weierstrass Equations

Recall that elliptic curves are curves of genus one having a specified base point. We shall see that every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at ∞. Then, after X and Y are scaled appropriately, an elliptic curve has an equation of te form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Here $O = [0 : 1 : 0]$ is the base point and $a_1, \dots, a_6 \in \overline{\Bbbk}$.

6.2 Group Law in Algebraic Terms

Let $E/\Bbbk$ be an elliptic curve defined by the Weirestrass equation

$$y^2 = x^3 + ax + b,$$

and let P and Q be two points on E. We want to compute the point $R = P + Q$ by expressing the coordinates of R as rational functions of the coordinates of P and Q. If either P or Q is the point O at infinity, then R is the other point, so we may assume that P and Q are affine points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. There are two cases to consider:

Case 1: Suppose $x_1 \neq x_2$. The line $\overline{PQ}$ has slope $m = (y_2 - y_1)/(x_2 - x_1)$, which yields the linear equation $y - y_1 = m(x - x_1)$ for $\overline{PQ}$. This line is not vertical, so it intersects the curve E in a third affine point $-R = (x_3, -y_3)$. Plugging the equation for the line $\overline{PQ}$ into the equation for the curve E yields

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b.$$

Expanding the LHS and moving every term to the RHS yields a cubic equation

$$g(x) := x^3 - m^2x^2 + \cdots = 0,$$

where the ellipsis hides lower order terms in x. The monic cubic polynomial $g(x)$ has two roots $x_1, x_2 \in \Bbbk$ and therefore factors in $\Bbbk[x]$ as

$$g(x) = (x - x_1)(x - x_2)(x - x_3),$$

where $x_3 \in \Bbbk$ is the x-coordinate of the third point $-R$ on the intersection $\overline{PQ}$ and E. Comparing the coefficient of x^2 in the two expressions for $g(x)$ shows that $x_1 + x_2 + x_3 = m^2$, and therefore $x_3 = m^2 - x_1 - x_2$. We can then compute the y-coordinate $-y_3$ of $-R$ by plugging this expression for x_3 into the equation for $\overline{PQ}$, and we have

$$\begin{aligned}m &= (y_2 - y_1)/(x_2 - x_1)\\ x_3 &= m^2 - x_1 - x_2\\ y_3 &= m(x_1 - x_3) - y_1,\end{aligned}$$

which expresses the coordinates of $R = P + Q$ as rational functions of the coordinates of P and Q as desired.

Case 2: Suppose $x_1 = x_2$. We must have $y_1 = \pm y_2$. If $y_1 = -y_2$, then $Q = -P$ and $P + Q = R = O$. Otherwise $P = Q$ and $R = 2P$, and the line $\overline{PQ}$ is the tangent to P on the equation for E, whose slope we can compute by implicit differentiation. This yields

$$2y\mathrm{d}y = 3x^2\mathrm{d}x + a\mathrm{d}x,$$

so at the point $P = (x_1, y_1)$ the slope of the tangent line is

$$m = \frac{\mathrm{d}y}{\mathrm{d}x} = \frac{3x_1^2 + a}{2y_1},$$

and once we know m we can compute x_3 and y_3 as above.

Remark 2. These equations can be converted to projective coordinates by replacing x_1, y_1, x_2, and y_2 with x_1/z_1, y_1/z_1, x_2/z_2, and y_2/z_2 respectively, and then writing the resulting expressions for x_3/z_3 and y_3/z_3 with a common denominator. When $P \neq Q$ we obtain

$$\begin{aligned} x_3 &= (x_2z_1 - x_1z_2)\Big((y_2z_1 - y_1z_2)^2z_1z_2 - (x_2z_1 - x_1z_2)^2(x_2z_1 + x_1z_2)\Big) \\ y_3 &= (y_2z_1 - y_1z_2)\Big((x_2z_1 - x_1z_2)^2(x_2z_1 + 2x_1z_2) - (y_2z_1 - y_1z_2)^2z_1z_2\Big) - (x_2z_1 - x_1z_2)^3y_1z_2 \\ z_3 &= (x_2z_1 - x_1z_2)^3z_1z_2 \end{aligned}$$

and for $P = Q$ we obtain

$$\begin{aligned} x_3 &= 2y_1z_1(a^2(z_1^2 + 3x_1^2)^2 - 8x_1y_1^2z_1) \\ y_3 &= a(z_1^2 + 3x_1^2)(12x_1y_1^2z_1 - a^2(z_1^2 + 3x_1^2)^2) - 8y_1^4z_1^2 \\ z_3 &= (2y_1z_1)^3. \end{aligned}$$

These formulas are more complicated, but they have the advantage of avoiding inversions which are more costly than multiplications.

6.3 Elliptic Curves as Abelian Groups

6.4 Isogenies

As abelian varieties, elliptic curves have both an algebraic structure (as an abelian group) and a geometric structure (as a smooth projective curve).

Definition 6.2. Let $C/\mathbb{k}$ be a plane projective curve $f(x,y,z) = 0$ with f a nonconstant homogeneous polynomial in $\mathbb{k}[x,y,z]$ that is irreducible in $\overline{\mathbb{k}}[x,y,z]$. The **function field** $k(C)$ is the set of equivalence classes of rational functions g/h such that

1. g and h are homogeneous polynomials in $k[x,y,z]$ of the same degree;
2. h is not divisible by f, equivalently, h is not an element of the ideal $\langle f\rangle$;
3. g_1/h_1 and g_2/h_2 are considered equivalent whenever $g_1h_2 - g_2h_1 \in \langle f\rangle$.

If L is any algebraic extension of k, the function field $L(C)$ is similarly defined with $g,h \in L[x,y,z]$.

Remark 3. The function field $k(X)$ of an irreducible projective variety X/k given by homogeneous polynomials $f_1,\ldots,f_m \in k[x_0,\ldots,x_n]$ is defined similarly: just replace the homogeneous ideal $\langle f\rangle$ with the homogeneous ideal $\langle f_1,\ldots,f_m\rangle$.

Remark 4. The field $k(C)$ contains k as a subfield (take g and h with degree 0), but it is not an algebraic extension of k, it is transcendental. Indeed, it has transcendence degree 1, consistent with the fact that C is a projective variety of dimension 1.

The fact that g and h have the same degree allows us to meaningfully assign a value to the function g/h at a projective point $P = (x_0 : y_0 : z_0)$ on C, so long as $h(P) \neq 0$. Thus assuming the denominators involved are all nonzero, for $\alpha \in k(C)$ the value of $\alpha(P)$ does not depend on how we choose to represent either α or P. If $\alpha = g_1/h_1$ with $h_1(P) = 0$, it may happen that g_1/h_1 is equivalent to g_2/h_2 with $h_2(P) \neq 0$. This is a slightly subtle point. It may not be immediately obvious whether or not such a g_2/h_2 exists, since it depends on equivalence modulo f; in general there may be no canonical way to write g/h in "lowest terms", because the ring $k[x,y,z]/\langle f\rangle$ is typically not a UFD.

Example 6.1. Suppose C/k is defined by $f(x,y,z) = zy^2 - x^3 - z^2x = 0$, and consider the point $P = (0:0:1) \in C(k)$. We can't evaluate $\alpha = 3xz/y^2 \in k(C)$ at P as written since its denominator vanishes at P, but we can use the equivalence relation in $k(C)$ to write

$$\alpha = \frac{3xz}{y^2} = \frac{3xz^2}{x^3 + z^2x} = \frac{3z^2}{x^2 + z^2},$$

and we then see that $\alpha(P) = 3$.

Definition 6.3. Let C/k be a projective curve with $\alpha \in k(C)$. We say that α is **defined** (or **regular**) at a point $P \in C(\bar{k})$ if α can be represented as g/h for some $g,h \in k[x,y,z]$ with $h(P) \neq 0$.

Remark 5. If C is the projective closure of an affine curve $f(x,y) = 0$, one can equivalently define $k(C)$ as the fraction field of $k[x,y]/\langle f\rangle$; this ring is known as the **coordinate ring** of C, denoted $k[C]$, and it is an integral domain provided that $\langle f\rangle$ is a prime ideal (which holds in our case since we assume f is irreducible). In this case one needs to homogenize the rational functions $r(x,y) = g(x,y)/h(x,y)$ in order to view them as functions defined on projective space.

Definition 6.4. Let C_1 and C_2 be plane projective curves defined over k. A **rational map** $\phi\colon C_1 \to C_2$ is a projective triple $(\phi_x : \phi_y : \phi_z) \in \mathbb{P}^2(k(C_1))$, such that for every $P \in C_1(\bar{k})$ where ϕ_x, ϕ_y, and ϕ_z are defined and not all zero, the projective point $(\phi_x(P) : \phi_y(P) : \phi_z(P))$ lies in $C_2(\bar{k})$. The map ϕ is **defined** (or **regular**) at P if there exists $\lambda \in k(C_1)^\times$ such that $\lambda\phi_x$, $\lambda\phi_y$, and $\lambda\phi_z$ are all defined at P and not all zero at P.

We should note that a rational map is not simply a function from $C_1(k)$ to $C_2(k)$ defined by rational functions, for two reasons. First, it might not be defined everywhere (although for smooth projective curves this does not happen). Second, it is required to map $C_1(\bar{k})$ to $C_2(\bar{k})$, which does not automatically hold for every rational map that carries $C_1(k)$ to $C_2(k)$; indeed, in general $C_1(k)$ could be the empty set (if C_1 is an elliptic curve then $C_1(k)$ is nonempty, but it could contain just a single point).

It is important to remember that a rational map $\phi = (\phi_x : \phi_y : \phi_z)$ is defined only up to scalar equivalence by functions in $k(C)^\times$. There may be points $P \in C_1(\bar{k})$ where one of $\phi_x(P)$, $\phi_y(P)$, $\phi_z(P)$ is not defined or all three are zero, but it may still be possible to evaluate $\phi(P)$ after rescaling $\lambda \in k(C)^\times$; we will see an example of this shortly. The value of $\phi(P)$ is unchanged if we clear denominators in $(\phi_x\colon \phi_y\colon \phi_z)$ by multiplying through by an appropriate homogeneous polynomial (note: this is not the same as rescaling by an element of $\lambda \in k(C)^\times$). This yields a triple $(\psi_x : \psi_y\colon \psi_z)$ of homogeneous polynomials of equal degree that we view as a representing any of the three equivalent rational maps

$$(\psi_x/\psi_z : \psi_y/\psi_z : 1), \qquad (\psi_x/\psi_y : 1 : \psi_z/\psi_y), \qquad (1 : \psi_y/\psi_x : \psi_z/\psi_x)$$

all of which are equivalent to ϕ. We then have $\phi(P) = (\psi_x(P) : \psi_y(P) : \psi_z(P))$ whenever any of ψ_x, ψ_y, ψ_z is nonzero at P. Of course it can still happen that ψ_x, ψ_y, ψ_z all vanish at P, in which case we might need to look for an equivalent tuple of homogeneous polynomials that represents ϕ. The tuples $(\psi_x : \psi_y : \psi_z)$ and $(\psi'_x : \psi'_y : \psi'_z)$ represent the same rational map whenever the polynomials $\psi_x\psi'_y - \psi'_x\psi_y$ and $\psi_x\psi'_z - \psi'_x\psi_z$ and $\psi_y\psi'_z - \psi'_y\psi_z$ all lie in the ideal $\langle f\rangle$ defining C_1.

6.5 Isogenies of Elliptic Curves

Definition 6.5. An **isogeny** $\phi\colon E_1 \to E_2$ of elliptic curves defined over k is a surjective morphism of curves that induces a group homomorphism $E_1(\bar{k}) \to E_2(\bar{k})$. The elliptic curves E_1 and E_2 are then said to be **isogeneous**.

6.5.1 Standard Form for Isogenies

To facilitate our work with isogenies, it will be convenient to put them in a standard form. In order to do so we will assume throughout that we are working with elliptic curves of the form $y^2 = f(x)$, and when it is convenient we will further assume $f(x) = x^3 + Ax + B$ so that our curves are in short Weierstrass form. Implicit in this assumption is that our elliptic curves are defined over a field k whose characteristic is not 2, and when we assume $f(x) = x^3 + Ax + B$ we eliminate some elliptic curves in characteristic 3.

Lemma 6.2. *Let $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ be elliptic curves over k, and let $\alpha\colon E_1 \to E_2$ be an isogeny. Then α can be defined by an affine rational map of the form*

$$\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

where $u, v, s, t \in k[x]$ are polynomials in x with $u \perp v$ and $s \perp t$.

Proof. Suppose α is defined by the rational map $(\alpha_x : \alpha_y : \alpha_z)$. Then for any affine point $(x : y : 1) \in E_1(\bar{k})$ we can write

$$\alpha(x,y) = (r_1(x,y), r_2(x,y)),$$

with $r_1(x,y) = \alpha_x(x,y,1)/\alpha_z(x,y,1)$ and $r_2(x,y) = \alpha_y(x,y,1)/\alpha_z(x,y,1)$. By repeatedly using the curve equation $y^2 = f_1(x)$ for E_1 to replace y^2 with $f_1(x)$, we can assume that both r_1 and r_2 have degree at most 1 in y. We then have

$$r_1(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}$$

for some $p_1, p_2, p_3, p_4 \in k[x]$. We now multiply the numerator and denominator of $r_1(x,y)$ by $p_3(x) - p_4(x)y$, and use the curve equation for E_1 to replace the y^2 in the denominator with $f_2(x)$, putting r_1 in the form

$$r_1(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}$$

for some $q_1, q_2, q_3 \in k[x]$.

We now use the fact that α is a group homomorphism and must therefore satisfy $\alpha(-P) = -\alpha(P)$ for any $P \in E_1(\bar{k})$. Recall that the inverse of an affine point (x,y) on a curve in short Weierstrass form is $(x,-y)$. Thus $\alpha(x,-y) = -\alpha(x,y)$, and we have

$$(r_1(x,-y), r_2(x,-y)) = (r_1(x,y), -r_2(x,y)).$$

Thus $r_1(x,y) = r_1(x,-y)$, and this implies that q_2 is the zero polynomial. After eliminating any common factors from q_1 and q_3, we obtain $r_1(x,y) = u(x)/v(x)$ for some $u, v \in k[x]$ with $u \perp v$, as desired. The argument for $r_2(x,y)$ is similar, except now we use $r_2(x,-y) = -r_2(x,y)$ to show that q_1 must be zero, yielding $r_2(x,y) = s(x)y/t(x)$ for some $s, t \in k[x]$ with $s \perp t$. □

We shall refer to the expression $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ given by Lemma (6.2) as the **standard form** of an isogeny $\alpha\colon E_1 \to E_2$. The fact that the rational functions u/v and s/t are in lowest terms implies that the polynomials $u, v, s,$ and t are uniquely determined up to a scalar in $k^\times$.

Lemma 6.3. *Let $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ be elliptic curves over k and let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ be an isogeny from E_1 to E_2 in standard form. Then v^3 divides t^2 and t^2 divides $v^3 f_1$. Moreover, $v(x)$ and $t(x)$ have the same set of roots in $\bar{k}$.*

Proof. Substituting $\left(\frac{u}{v}, \frac{s}{t}y\right)$ for (x,y) in the equation for E_2 gives $((s/t)y)^2 = f_2(u/v)$, and using the equation for E_1 to replace y^2 with $f_2(x)$ yields

$$(s/t)^2 f_1 = f_2(u/v)$$

as an identity involving polynomials $f_1, f_2, s, t, u, v \in k[x]$. If we put $w = v^3 f_2(u/v)$ and clear denominators we obtain

$$v^3 s^2 f_1 = t^2 w.$$

Note that $u \perp v$ implies $v \perp w$, since any common factor of v and w must divide u. It follows that $v^3 \mid t^2$ and $t^2 \mid v^3 f_1$. This implies that v and t have the same roots in $\bar{k}$: every root of v is clearly a root of t (since $v^3 \mid t^2$), and every root x_0 of t is a double root of $v^3 f_1$ since $t^2 \mid v^3 f_1$, and since f_1 has no double roots (because E_1 is not singular), x_0 must be a root of v (and possibly also a root of f_1). □

Corollary 7. *Let $\alpha(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ be an isogeny $E_1 \to E_2$ in standard form. The affine points $(x_0 : y_0 : 1) \in E_1(\bar{k})$ in the kernel of α are precisely those for which $v(x_0) = 0$.*

Proof. If $v(x_0) \neq 0$, then $t(x_0) \neq 0$, and $\alpha(x_0, y_0) = \left(\frac{u(x_0)}{v(x_0)}, \frac{s(x_0)}{t(x_0)^2} y\right)$ is an affine point and therefore not 0 (the point at infinity), hence not in the kernel of α.

By homogenizing and putting α into projective form, we can write α as

$$\alpha = (ut : vsy : vt),$$

where ut, vsy, and vt are now homogeneous polynomials of equal degree ($s, t, u, v \in k[x, z]$).

Suppose $y_0 \neq 0$. By the previous lemma, if $v(x_0, 1) = 0$, then $t(x_0, 1) = 0$, and since $v^3 \mid t^2$, the multiplicity of $(x_0, 1)$ as a root of t is strictly greater than its multiplicity as a root of v. This implies that, working over $\bar{k}$, we can renormalize α by dividing by a suitable power of $x - x_0 z$ so that α_y does not vanish at $(x_0 : y_0 : 1)$ but α_x and α_z both do. Then $\alpha(x_0 : y_0 : 1) = (0 : 1 : 0) = 0$, and $(x_0 : y_0 : 1)$ lies in the kernel of α as claimed.

If $y_0 = 0$, then x_0 is a root of the cubic $f(x)$ in the equation $y^2 = f_1(x)$ for E_1, and it is not a double root, since E_1 is not singular. In this case we can renormalize α by multiplying by yz and then replacing $y^2 z$ with $f_1(x, z)$. Because $(x_0, 1)$ only has multiplicity 1 as a root of $f_1(x, z)$, its multiplicity as a root of vf_1 is no greater than its multiplicity as a root of t (here again we use $v^3 \mid t^2$), and we can again renormalize α by dividing by a suitable power of $x - x_0 z$ so that α_y does not vanish at $(x_0 : y_0 : 1)$, but α_x and α_z both do (since they are now both divisible by $y_0 = 0$). Thus $(x_0 : y_0 : 1)$ is again in the kernel of α. □

7 Integral Points of Elliptic Curves

Definition 7.1. Let $x \in \mathbb{Q}$ and write $x = p/q$ as a fraction in lowest terms. We set $\mathrm{H}(x) = \max\{|p|, |q|\}$ and call this the **height** of x.

Definition 7.2. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Fix a Weierstrass equation of $E/\mathbb{Q}$ of the form

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in \mathbb{Z}$. The **(logarithmic) height** on $E(\mathbb{Q})$ relative to the Weierstrass equation is the function $\mathrm{h}_x \colon E(\mathbb{Q}) \to \mathbb{R}$ defined by

$$\mathrm{h}_x(P) = \begin{cases} \log \mathrm{H}(x(P)) & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases}$$

Proposition 7.1. *Let $\alpha \in \mathbb{R} \backslash \mathbb{Q}$. There are infinitely many rational numbers $p/q \in \mathbb{Q}$ such that*

$$\left| \frac{p}{q} - \alpha \right| \leq \frac{1}{q^2}.$$

Proof. Let N be a (large) integer and consider the set of real numbers

$$\{n\alpha - \lceil n\alpha \rceil \mid 0 \leq n \leq N\}.$$

Since α is irrational, this set contains $N + 1$ distinct numbers between 0 and 1. Dividing the interval $[0, 1]$ into N equal-sized pieces and applying the pigeonhole principle, we find that there are integers $0 \leq n_1 < n_2 \leq N$ satisfying

$$|(n_1\alpha - \lceil n_1\alpha \rceil) - (n_2\alpha - \lceil n_2\alpha \rceil)| \leq \frac{1}{N}.$$

Therefore setting $p/q = (\lceil n_2\alpha \rceil - \lceil n_1\alpha \rceil) \,/\, (n_2 - n_1)$ gives us

$$\left| \frac{\lceil n_2\alpha \rceil - \lceil n_1\alpha \rceil}{n_2 - n_1} - \alpha \right| \leq \frac{1}{(n_2 - n_1)N} \leq \frac{1}{(n_2 - n_1)^2}.$$

This provides one rational approximation having the desired property.

Finally, having obtained a list of such approximations, let p/q be the one for which $|p/q - \alpha|$ is smallest. Then taking $N > |p/q - \alpha|^{-1}$ ensures that we get a new approximation that is not already in our list. Hence there exist infinitely many rational numbers satisfying the conditions of the proposition. □

Remark 6. A result of Hurwitz says taht the $1/q^2$ on the right-hand side may be replaced by $1/(\sqrt{5}q^2)$, and that this is the best result possible. In particular, for any $\varepsilon > 0$, there exist only finitely many $x \in \mathbb{Q}$ such that

$$|x - \alpha| < \frac{1}{\mathrm{H}(x)^{2+\varepsilon}}.$$

Proposition 7.2. *Let $\alpha \in \overline{\mathbb{Q}}$ have degree $d \geq 2$ over $\mathbb{Q}$. There is a constant $C > 0$ (depending on α) such that for all rational numbers p/q we have*

$$\left| \frac{p}{q} - \alpha \right| \geq \frac{C}{q^d}.$$

Proof. By replacing α with $\mathrm{Im}(\alpha)$ if necessary, we may assume that $\alpha \in \mathbb{R}$. Let π be the minimal polynomial of α over $\mathbb{Q}$ and let

$$C_1 = \sup\{\pi'(t) \mid t \in [\alpha - 1, \alpha + 1]\}.$$

Then the mean value theorem tells us that

$$\left| \pi\left(\frac{p}{q}\right) \right| = \left| \pi\left(\frac{p}{q}\right) - \pi(\alpha) \right| \leq C_1 \left| \frac{p}{q} - \alpha \right|.$$

On the other hand, we know that $q^d\pi(p/q) \in \mathbb{Z}$ and further that $\pi(p/q) \neq 0$. Hence $|q^d\pi(p/q)| \geq 1$. Therefore setting $C = \min\{C_1^{-1}, 1\}$ and combining the last two inequalities yields

$$\begin{aligned}\left|\frac{p}{q} - \alpha\right| &\geq \frac{1}{C_1}\left|\pi\left(\frac{p}{q}\right)\right| \\ &\geq C\left|\pi\left(\frac{p}{q}\right)\right| \\ &\geq \frac{C}{q^d}.\end{aligned}$$

for all $p/q \in \mathbb{Q}$. □

Definition 7.3. Let K be a number field. Let $\tau(d)$ be a positive real-valued function on the natural numbers. A number field K is said to have **approximation exponent** τ if it has the following property:

> Let $\alpha \in \overline{K}$, let $d = [K(\alpha) : K]$, and let $v \in M_K$ be an absolute value on K that has been extended to $K(\alpha)$ in some fashion. Then for any constant C there exist only finitely many $x \in K$ satisfying the inequality
>
> $$|x - \alpha|_v < \frac{C}{\mathrm{H}_K(x)^{\tau(d)}}.$$

Remark 7. Liouville's elementary estimate says that $\mathbb{Q}$ has approximation exponenent $\tau(d) = d + \varepsilon$ for any $\varepsilon > 0$.

Theorem 7.1. *For every $\varepsilon > 0$, every number field K of degree d has approximation exponent $\tau(d) = 2 + \varepsilon$. In particular, for every $\varepsilon > 0$ and for every constant $C > 0$, there are only finitely many $x \in K$ which satisfy the inequality*

$$|x - \alpha| < \frac{C}{\mathrm{H}_K(x)^{2+\varepsilon}}.$$

Example 7.1. Suppose we are trying to solve the equation

$$x^3 - 2y^3 = a$$

where $x, y \in \mathbb{Z}$ and where $a \in \mathbb{Z}$ is fixed. Suppose that (x, y) is a solution with $y \neq 0$. Let ζ be a primitive cube root of unity and factor the equation as

$$\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta\sqrt[3]{2}\right)\left(\frac{x}{y} - \zeta^2\sqrt[3]{2}\right) = \frac{a}{y^3}.$$

The second and third factors in the product are bounded away from 0, so we obtain an estimate of the form

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \leq \frac{C}{y^3},$$

where C is a constant which is independent of x and y. Now Theorem (**??**) tells us that there are only finitely many possibilities for x and y. Hence the equation

$$x^3 - 2y^3 = a$$

has only finitely many solutions in integers.

8 Elliptic Curves over $\mathbb{C}$

We now consider elliptic curves over the complex numbers

8.1 Elliptic Functions

Let $\Lambda \subseteq \mathbb{C}$ be a lattice, that is, Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis for $\mathbb{C}$. In this section, we study meromorphic funcitons on the quotient space $\mathbb{C}/\Lambda$, or equivalently, meromorphic functions on $\mathbb{C}$ that are periodic with respect to the lattice Λ.

Definition 8.1. We make the following definitions

1. A **fundamental parallelogram** for Λ is a set of the form

   $$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\},$$

   where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for Λ. Note that the definition of D implies that the natural map $D \to \mathbb{C}/\Lambda$ is bijective. We denote the closure of D in $\mathbb{C}$ by $\overline{D}$.

2. An **elliptic function** (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies

   $$f(z + \omega) = f(z)$$

   for all $\omega \in \Lambda$.

Proposition 8.1. *Let $f(z)$ be an elliptic function. If f has no poles (i.e. if f is holomorphic), then f is constant. Similarly, if f has no zeros, then f is constant.*

Proof. Let D be a fundamental parallelogram for Λ. The periodicity of f implies $\|f\|_{\mathbb{C}} = \|f\|_{\overline{D}}$. The function f is continuous and the set $\overline{D}$ is compact, so $|f|$ is bounded on $\overline{D}$. Therefor $|f|$ is bounded on all of $\mathbb{C}$. It follows by Liouville's theorem that f is constant. Similarly, if f has no zeros, then $1/f$ has no poles, hence constant. □

Let f be an elliptic function and let $w \in \mathbb{C}$. Then just as for any meromorphic function, we can look at its order of vanishing at w, denoted $\mathrm{ord}_w(f)$, and its residue at w, denoted $\mathrm{res}_w(f)$. Let's briefly

Definition 8.2. Let C be a curve and $P \in C$ a smooth point. The **normalized valuation** on $\overline{K}[C]_P$ is given by

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} \mid f \in \mathfrak{m}_P^d\}.$$

Using $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, we extend ord_P to $\overline{K}(C)$.

Definition 8.3. A **lattice** $L = [\omega_1, \omega_2]$ is an additive subgroup $\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ of $\mathbb{C}$ generated by complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$. If we take the quotient of the complex plane $\mathbb{C}$ modulo a lattice L, we get a torus $\mathbb{C}/L$. Note that this quotient makes sense not just as a quotient of abelian groups, but also as a quotient of topological spaces (where $\mathbb{C}$ has its usual Euclidean topology and L has the discrete topology); the torus $\mathbb{C}/L$ is a compact topological group. A **fundamental parallelogram** for L is any set of the form

$$\mathcal{F}_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 \mid \alpha \in \mathbb{C} \text{ and } 0 \leq t_1, t_2 \leq 1\}.$$

We can identify the points in a fundamental parallelogram with the points of $\mathbb{C}/L$.
A **lattice** is an additive subgroup L of $\mathbb{C}$ which is generated by two complex numbers ω_1 and ω_2 that are linearly independent over $\mathbb{R}$. We express this by writing $L = [\omega_1, \omega_2]$. An **elliptic function** for L is a function $f(z)$ defined on $\mathbb{C}$, except for isolated singularities, which satisfies the following two conditions:

1. $f(z)$ is meromorphic on $\mathbb{C}$.
2. $f(z + \omega) = f(z)$ for all $\omega \in L$.

If $L = [\omega_1, \omega_2]$, then note that the second condition is equivalent to

$$f(z + \omega_1) = f(z + \omega_2) = f(z).$$

Elements in L are often referred to as **periods**.

8.2 Weierstrass $\wp$-function

Definition 8.4. Let L be a lattice. The **Weierstrass $\wp$-function** is defined as follows: given a complex number z not in the lattice L, we set

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

When working with a fixed lattice L, we will usually write $\wp(z)$ instead of $\wp(z; L)$.

8.2.1 Eisenstein Series

Definition 8.5. Let Λ be a lattice in $\mathbb{C}$ and let $k > 2$ be an integer. The **weight-k Eisenstein series** for Λ is the sum

$$G_k(L) = \sum_{\omega \in L^*} \frac{1}{\omega^k} = \sum_{\substack{m_1, m_2 \in \mathbb{Z} \\ (m_1, m_2) \neq (0,0)}} \frac{1}{(m_1\omega_1 + m_2\omega_2)^k}$$

where $L^* = L - \{0\}$.

Remark 8. $G_k(L)$ is a function of the lattice L. In particular, if the lattice L is fixed, then $G_k = G_k(L)$ is a constant. For lattices of the form $L = [1, \tau]$ where $\mathrm{Im}(\tau) > 0$, we often think of G_k as a function of τ via the formula:

$$G_k(\tau) := G_k([1, \tau]) = \sum_{\substack{m, n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + n\tau)^k}.$$

Because it comes from a function defined over a lattice, the function $G_k(\tau)$ has some very nice properties. In particular we have

$$G_k(\tau + 1) = G_k(\tau) \quad \text{and} \quad G_k(-1/\tau) = \tau^k G_k(\tau)$$

for all $\tau \in \mathcal{H}$. Eisenstein series are the simplest example of **modular forms**, which we will learn about later on.

Remark 9. If k is odd, then $G_k(L) = 0$ for any lattice L, since the terms $1/\omega^k$ and $1/(-\omega)^k$ in the sum cancel. Thus the only interesting Eisenstein series are those of even weight.

Lemma 8.1. *For any lattice Λ, the series $G_k(\Lambda)$ converges absolutely for all $k > 2$.*

Proof. Suppose $\Lambda = [\omega_1, \omega_2] = [\boldsymbol{\omega}]$ where we write $\boldsymbol{\omega} = (\omega_1, \omega_2) \in \mathbb{C}^2$. We let $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$ denote the usual inner-product and norm on $\mathbb{C}^2$. In what follows, we think of $\boldsymbol{\omega} = (\omega_1, \omega_2)$ as being fixed, we write $\boldsymbol{x} = (x_1, x_2)$ for an arbitrary element in $\mathbb{R}^2$, and we write $\boldsymbol{m} = (m_1, m_2)$ for an arbitrary element in $\mathbb{Z}^2$. Using this notation, we can re-express the series $G_k(\Lambda)$ as

$$G_k(\Lambda) = \sum_{\boldsymbol{m}} \frac{1}{|\langle \boldsymbol{m}, \boldsymbol{\omega} \rangle|^k},$$

where it is understood that we are summing over $\boldsymbol{m} \in \mathbb{Z}^2 \backslash \{0\}$. The map $\langle \cdot, \boldsymbol{\omega} \rangle \colon \mathbb{R}^2 \to \mathbb{C}$, given by $\boldsymbol{x} \mapsto \langle \boldsymbol{x}, \boldsymbol{\omega} \rangle$, is a bounded linear map. Furthermore, $\langle \cdot, \boldsymbol{\omega} \rangle$ is injective since $\langle \boldsymbol{x}, \boldsymbol{\omega} \rangle = 0$ if and only if $x_1\omega_1 + x_2\omega_2 = 0$ if and only if $x_1 = 0 = x_2$ since $\{\omega_1, \omega_2\}$ is linearly independent over $\mathbb{R}$. Therefore if we set $C = \inf\{|\langle \boldsymbol{x}, \boldsymbol{\omega}\rangle| \mid \|\boldsymbol{x}\| = 1\}$, then $C > 0$ and $|\langle \boldsymbol{x}, \boldsymbol{\omega}\rangle|^k \geq C^k \|\boldsymbol{x}\|^k$. It follows that

$$
\begin{aligned}
G_k(\Lambda) &= \sum_{\boldsymbol{m}} \frac{1}{|\langle \boldsymbol{m}, \boldsymbol{\omega}\rangle|^k} \\
&\leq \frac{1}{C^k} \sum_{\boldsymbol{m}} \frac{1}{\|\boldsymbol{m}\|^k} \\
&= \frac{1}{C^k} \sum_{\boldsymbol{m}} \frac{1}{(\|\boldsymbol{m}\|^2)^{k/2}}.
\end{aligned}
$$

Thus in order to show the sum $G_k(\Lambda)$ converges absolutely, it suffices to show that the series $\sum_{\boldsymbol{m}} \frac{1}{(\|\boldsymbol{m}\|^2)^{k/2}}$ converges. Indeed, this follows from the integral comparison test. We have

$$
\begin{aligned}
\int\limits_{\|\boldsymbol{x}\|^2 \geq 1} \frac{1}{(\|\boldsymbol{x}\|^2)^{k/2}} \mathrm{d}\boldsymbol{x} &= \int_0^{2\pi} \int_0^{\infty} \frac{1}{r^k} r \mathrm{d}r \mathrm{d}\theta \\
&= \int_0^{2\pi} \int_0^{\infty} r^{1-k} \mathrm{d}r \mathrm{d}\theta \\
&= \int_0^{2\pi} \left(\frac{1}{2-k} r^{2-k} \right) \Big|_0^{\infty} \mathrm{d}\theta \\
&= \int_0^{2\pi} \frac{1}{k-2} \mathrm{d}\theta \\
&= \frac{2\pi}{k-2} \\
&< \infty.
\end{aligned}
$$

where we used the fact that $k > 2$ to get from the third line to the fourth line as well as from the sixth line to the seventh line. $\square$

Lemma 8.2. *If $z, w \notin L$, then $\wp(z) = \wp(w)$ if and only if $z \equiv \pm w \bmod L$.*

Proof. One direction is trivial since $\wp(z)$ is an even function. To argue the other way, suppose $L = [\omega_1, \omega_2]$, and fix a number $-1 < \delta < 0$. Let P denote the parallelogram $\{s\omega_1 + t\omega_2 \mid \delta \leq s, t \leq \delta + 1\}$, and let Γ be its boundary oriented counterclockwise. Note that every complex number is congruent modulo L to a number in P.

Fix w and consider the function $f(z) = \wp(z) - \wp(w)$. By adjusting δ, we can arrange that $f(z)$ has no zeros or poles on Γ. Then it is well known that

$$
\frac{1}{2\pi i} \int_\Gamma \frac{f'(z)}{f(z)} \mathrm{d}z = Z - P
$$

where Z is the number of zeros of $f(z)$ in P and P is the number of poles of $f(z)$ in P, each counting multiplicity. Since $f'(z)/f(z)$ is periodic, the integrals on opposite sides of Γ cancel, and thus $\int_\Gamma (f'(z)/f(z))\mathrm{d}z = 0$. This shows that $Z = P$. However, P is easy to compute: from the definition of P, it's obvious that 0 is the only pole of $f(z) = \wp(z) - \wp(w)$ in P. It's a double pole, and thus $Z = P = 2$, so that $f(z)$ has two zeros (counting multiplicity) in P.

There are now two cases to consider. If $w \not\equiv -w \bmod L$, then modulo L, w and $-w$ give rise to two distinct points of P, both of which are zeros of $f(z) = \wp(z) - \wp(w)$. Since $Z = 2$, these are all of the zeros, and their multiplicity is one, that is $\wp'(w) \neq 0$. If $w \equiv -w \bmod L$, then $2w \in L$. Since $\wp'(z)$ is an odd function, we obtain

$$
\wp'(w) = \wp'(w - 2w) = \wp'(-w) = -\wp'(w),
$$

which forces $\wp'(w) = 0$. Thus modulo L, w gives rise to a zero of $f(z)$ of multiplicity ≥ 2 in P, and again $Z = 2$ implies that these are all. This proves the lemma. $\square$

Proposition 8.2. *Let $\wp(z)$ be the Weierstrass $\wp$-function for the lattice L.*

1. *$\wp(z)$ is an elliptic function for L whose singularities consist of double poles at the points of L.*
2. *$\wp(z)$ satisfies the differential equation*
$$
\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),
$$
where the constants $g_2(L)$ and $g_3(L)$ are defined by
$$
\begin{aligned}
g_2(L) &= 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4} \\
g_3(L) &= 140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6}
\end{aligned}
$$
3. *$\wp(z)$ satisfies the addition law*
$$
\wp(z + w) = -\wp(z) - \wp(w) + \frac{1}{4} \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)} \right)^2
$$
whenever $z, w \notin L$ and $z + w \notin L$.

Proof. 1. We first show $\wp(z)$ is holomorphic outside L. Let Ω be a compact subset of $\mathbb{C}$ missing L. It suffices to show that the sum

$$
\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)
$$

converges absolutely and uniformly on Ω. Choose $R > 0$ such that $|z| \leq R$ for all $z \in \Omega$. Now suppose that $z \in \Omega$ and that $\omega \in L$ satisfies $|\omega| \geq 2R$. Then $|z - \omega| \geq |\omega|/2$, and one see that

$$\begin{aligned}\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| &= \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \\ &\leq \frac{R(2|\omega| + |\omega|/2)}{|\omega|^2(|\omega|^2/2)} \\ &= \frac{10R}{|\omega|^3}.\end{aligned}$$

Since the inequality $|\omega| \geq 2R$ holds for all but finitely many elements of L, it follows from Lemma (8.1) that the sum in the $\wp$-function converges absolutely and uniformly on Ω. Thus $\wp(z)$ is holomorphic on $\mathbb{C}\backslash L$ and has a double pole at the origin.

To show that $\wp(z)$ is periodic, first note that differentiating the series for $\wp(z)$ gives us

$$\wp'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

Arguing as above, the series converges absolutely, and it follows easily that $\wp'(z)$ is an elliptic function for L. Now suppose that $L = [\omega_1, \omega_2]$. The functions $\wp(z)$ and $\wp(z + \omega_i)$ have the same derivative since $\wp'(z)$ is periodic, and hence they differ by a constant, say $\wp(z) = \wp(z + \omega_i) + C$. Evaluating this at $-\omega_i/2$, we obtain

$$\begin{aligned}\wp(-\omega_i/2) &= \wp(-\omega_i/2 + \omega_i) + C \\ &= \wp(\omega_i/2) + C.\end{aligned}$$

Since $\wp(z)$ is an even function (check!), it follows that $C = 0$, and hence periodicity is proved. It follows that the poles of $\wp(z)$ are all doubles poles and lie exactly on the points of L.

2. To prove this, we first calculate the Laurent expansion of $\wp(z)$ about the origin: we claim that

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}.$$

Indeed, for $|x| < 1$, we have the series expansion

$$\frac{1}{(1-x)^2} = 1 + \sum_{n=1}^{\infty}(n+1)x^n.$$

Thus if $|z| < |\omega|$, then we can put $x = z/\omega$ in the above series, and it follows easily that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}\frac{n+1}{\omega^{n+2}}z^n.$$

Summing over all $\omega \in L\backslash\{0\}$ and using absolute convergence gives us

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(L)z^{2n}.$$

Since $\wp(z)$ is an even function, all of the odd coefficients must vanish, giving us the desired Laurent expansion.

From this, we see that

$$\wp'(z) = \frac{-2}{z^3} + \sum_{n=1}^{\infty}2n(2n+1)G_{2n+2}(L)z^{2n-1},$$

and then one computes the first few terms of $\wp(z)^3$ and $\wp'(z)^2$ as follows:

$$\begin{aligned}\wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4(L)}{z^2} + 15G_6(L) + \cdots \\ \wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4(L)}{z^2} - 80G_6(L) + \cdots .\end{aligned}$$

Now consider the elliptic function

$$F(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4(L)\wp(z) + 140G_6(L).$$

Using the above expansions, it's easy to see that $F(z)$ vanishes at the origin, and then by periodicity, $F(z)$ vanishes at all points of L. But it is also holomorphic on $\mathbb{C}\backslash L$, so that $F(z)$ is holomorphic on all of $\mathbb{C}$. An easy argument using Liouville's Theorem shows that $F(z)$ is constant, so that $F(z)$ is identically zero. Since $g_2(L)$ and $g_3(L)$ were defined to be $60G_4(L)$ and $140G_6(L)$ respectively, we are done.

3.

□

$$\begin{aligned}\wp(z+\omega_1; L) &= \frac{1}{(z+\omega_1)^2} + \sum_{\omega \in L\backslash\{0\}}\left(\frac{1}{(z+\omega_1-\omega)^2} - \frac{1}{\omega^2}\right) \\ &= \frac{1}{(z+\omega_1)^2} + \sum_{\omega' \in L\backslash\{0\}}\left(\frac{1}{(z-\omega')^2} - \frac{1}{(\omega'+\omega_1)^2}\right) \qquad \omega' = \omega - \omega_1\end{aligned}$$

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

8.3 Differentials

Definition 8.6. Let C be a curve. The **space** of **(meromorphic) differential forms** on C, denoted Ω_C, is the $\overline{K}(C)$-vector space generated by symbols of the form $\mathrm{d}x$ for $x \in \overline{K}(C)$, subject to the relations

1. $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$ for all $x, y \in \overline{K}(C)$;
2. $\mathrm{d}(xy) = x\mathrm{d}y + y\mathrm{d}x$ for all $x, y \in \overline{K}(C)$;
3. $\mathrm{d}c = 0$ for all $c \in \overline{K}$.

Let $\phi\colon C_1 \to C_2$ be a nonconstant map of curves. The associated function field map $\phi^*\colon \overline{K}(C_2) \to \overline{K}(C_1)$ induces a map of differentials $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ defined by

$$\phi^*\left(\sum f_i \mathrm{d}x_i\right) = \sum (\phi^* f_i)\mathrm{d}(\phi^* x_i).$$

This map provides a useful criterion for determining when ϕ is separable.

Part III
Analytic Number Theory

Let $r > 0$ and let $z \in \mathbb{C}$. We use the following notation throughout these notes:

$$\begin{aligned}
\mathrm{B}_r(z) &= \{s \in \mathbb{C} \mid |s-z| < r\} \\
\mathrm{B}_r[z] &= \{s \in \mathbb{C} \mid |s-z| \leq r\} \\
\mathrm{B}_r(\infty) &= \{s \in \mathbb{C} \mid \mathrm{Re}(s) > r\} \\
\mathrm{B}_r[\infty] &= \{s \in \mathbb{C} \mid \mathrm{Re}(s) \geq r\}
\end{aligned}$$

9 Riemann Zeta Function

The **Riemann zeta function** is the complex function defined by the series

$$\zeta(s) := \sum_{n \geq 1} n^{-s} \tag{16}$$

for $\mathrm{Re}(s) > 1$, where n varies over positive integers. More generally, for any $S \subseteq \mathbb{N}$ we define the **partial Riemann zeta function** with respect to S to be the complex function defined by the series

$$\zeta_S(s) := \sum_{n \in S} n^{-s} \tag{17}$$

for $\mathrm{Re}(s) > 1$. In particular, $\zeta_{\mathbb{N}}(s) = \zeta(s)$.

Proposition 9.1. *The series (17) converges absolutely and locally uniformly on* $\mathrm{Re}(s) > 1$.

Proof. Let $\delta > 0$. Then for any $s \in \mathrm{B}_{1+\delta}(\infty)$, we have

$$\begin{aligned}
\sum_{n \in S} |n^{-s}| &= \sum_{n \in S} n^{-\mathrm{Re}(s)} \\
&\leq \sum_{n \in S} n^{-1-\delta} \\
&\leq \sum_{n \geq 1} n^{-1-\delta} \\
&\leq \int_1^\infty x^{-1-\delta} \mathrm{d}x \\
&= \left(\frac{x^{-\delta}}{-\delta} \right) |_1^\infty \\
&= \frac{1}{\delta}.
\end{aligned}$$

It follows that the series (17) converges absolutely on $\mathrm{Re}(s) > 1 + \delta$ (and hence on $\mathrm{Re}(s) > 1$ since $\delta > 0$ was arbitrary). Furthermore, it converges uniformly on $\mathrm{Re}(s) > 1 + \delta$ (and even on $\mathrm{Re}(s) \geq 1 + \delta$). Indeed, this follows from an easy application of the Weirestrass M-test with $M_n = n^{-1-\delta}$. □

It now follows from a basic theorem in complex analysis (which we will state below) that $\zeta_S(s)$ is holomorphic on $\mathrm{Re}(s) > 1$. Furthermore, we can express its derivative in terms of the series

$$\zeta_S'(s) = -\sum_{n \in S} (\log n) n^{-s}$$

which again converges absolutely and uniformly on $\mathrm{B}_{1+\delta}(\infty)$ for all $\delta > 0$. Here's the theorem:

Theorem 9.1. *A sequence or series of holomorphic functions f_n that converges locally uniformly on an open set U converges to a holomorphic function f on U, and the sequence or series of derivative f_n' then converges locally uniformly to f' (and if none of the f_n has a zero in U and $f \neq 0$, then f has no zeros in U).*

9.0.1 Euler Product

Theorem 9.2. *For Re$(s) > 1$, we have*

$$\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_p (1-p^{-s})^{-1},$$

where the product converges absolutely. In particular, $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$.

The product in the theorem above ranges over primes p. This is a standard practice in analytic number theory that we will follow: the symbol p always denotes a prime, and any sum or product over p is understood to be over primes, even if this is not explicitly stated.

Proof. We have

$$\begin{aligned}
\sum_{n\geq 1} n^{-s} &= \sum_{n\geq 1} \prod_p p^{-v_p(n)s} \\
&= \prod_p \sum_{e\geq 0} p^{-es} \\
&= \prod_p (1-p^{-s})^{-1}.
\end{aligned}$$

To justify the second equality, consider the **partial zeta function** $\zeta_m(s)$, which restricts the summation in $\zeta(s)$ to the set S_m of m-smooth integers (those with no prime factors $p > m$). If $p_1, \ldots, p_k$ are the primes up to m, then absolute convergence implies

$$\begin{aligned}
\zeta_m(s) &:= \sum_{n\in S_m} n^{-s} \\
&= \sum_{e_1,\ldots,e_k\geq 0} (p_1^{e_1}\cdots p_k^{e_k})^{-s} \\
&= \prod_{1\leq i\leq k} \sum_{e_i\geq 0} (p_i^{-s})^{e_i} \\
&= \prod_{p\leq m} (1-p^{-s})^{-1} \\
&:= P_m(s),
\end{aligned}$$

where we denoted $P_m(s) := \prod_{p\leq m}(1-p^{-s})^{-1}$. For any $\delta > 0$, the sequence of functions $\zeta_m(s)$ converges uniformly on $\mathrm{Re}(s) > 1+\delta$ to $\zeta(s)$. The sequence of functions clearly converges locally uniformly to $\prod_p (1-p^{-s})^{-1}$ on any region in which the latter function is absolutely convergent (or even just convergent). On $\mathrm{Re}(s) > 1$, we have

$$\begin{aligned}
\sum_p \left|\log(1-p^{-s})^{-1}\right| &= \sum_p \left|\sum_{e\geq 1} \frac{1}{e} p^{-es}\right| \\
&\leq \sum_p \sum_{e\geq 1} \left|p^{-s}\right|^e \\
&= \sum_p (|p^s|-1)^{-1} \\
&\leq \sum_n (n^{\mathrm{Re}(s)}-1)^{-1} \\
&< \infty,
\end{aligned}$$

where we have used the identity $\log(1-z) = -\sum_{n\geq 1}\frac{1}{n}z^n$, valid for $|z| < 1$. It follows that $\prod_p (1-p^{-s})^{-1}$ is absolutely convergent (and in particular, nonzero) on $\mathrm{Re}(s) > 1$. If D is a disk contained in $\mathrm{Re}(s) > 1$, then there exists $M \geq 0$ such that $\left|\prod_p (1-p^{-s})^{-1}\right| \leq M$ for all $s \in D$. Thus, given $\varepsilon > 0$ we have

$$\begin{aligned}
\left|\prod_{p\leq m}(1-p^{-s})^{-1} - \prod_p (1-p^{-s})^{-1}\right| &= \left|\prod_{p\leq m}(1-p^{-s})^{-1}\left(1-\prod_{p>m}(1-p^{-s})^{-1}\right)\right| \\
&\leq M\left(1-\prod_{p>m}(1-p^{-s})^{-1}\right) \\
&< \varepsilon
\end{aligned}$$

for all sufficiently large m. □

9.0.2 Analytic Continuation

Theorem 9.3. *(Analytic Continuation I) For $\mathrm{Re}(s) > 1$ we have*

$$\zeta(s) = \frac{1}{1-s} + \phi(s),$$

where $\phi(s)$ is a holomorphic function on $\mathrm{Re}(s) > 0$. Thus $\zeta(s)$ extends to a meromorphic function on $\mathrm{Re}(s) > 0$ that has a simple pole at $s = 1$ with residue 1 and no other poles.

Proof. For $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}\zeta(s) - \frac{1}{1-s} &= \sum_{n\geq 1} n^{-s} - \int_1^\infty x^{-s}\mathrm{d}x \\ &= \sum_{n\geq 1}\int_n^{n+1}(n^{-s} - x^{-s})\mathrm{d}x \\ &= \sum_{n\geq 1}\phi_n(s),\end{aligned}$$

where we set $\phi_n(s) := \int_n^{n+1}(n^{-s} - x^{-s})\mathrm{d}x$. Note that ϕ_n is holomorphic on $\mathrm{Re}(s) > 0$. We will show series $\sum_n \phi_n$ converges locally normally on $\mathrm{Re}(s) > 0$, and this in turn will imply $\zeta(s) - (1-s)^{-1}$ is holomorphic on $\mathrm{Re}(s) > 0$. For each fixed s in $\mathrm{Re}(s) > 0$ and $x \in [n, n+1]$ we have

$$\begin{aligned}|n^{-s} - x^{-s}| &= \left|\int_n^x st^{-s-1}\mathrm{d}t\right| \\ &\leq \int_n^x \frac{|s|}{|t^{s+1}|}\mathrm{d}t \\ &= \int_n^x \frac{|s|}{t^{1+\mathrm{Re}(s)}}\mathrm{d}t \\ &\leq \frac{|s|}{n^{1+\mathrm{Re}(s)}},\end{aligned}$$

In particular, this implies $|\phi_n(s)| \leq |s|/n^{1+\mathrm{Re}(s)}$. For any s_0 with $\mathrm{Re}(s_0) > 0$, if we put $\varepsilon := \mathrm{Re}(s_0)/2$ and $U := \mathrm{B}_\varepsilon(s_0)$, then for each $n \geq 1$,

$$\sup_{s\in U}|\phi_n(s)| \leq \frac{|s_0| + \varepsilon}{n^{1+\varepsilon}} := M_n,$$

and $\sum_n M_n = (|s_0| + \varepsilon)\zeta(1+\varepsilon)$ converges. By the Weierstarss M-test, $\sum_n \phi_n$ converges locally uniformly to a function $\phi(s) = \zeta(s) - \frac{1}{s-1}$ that is holomorphic on $\mathrm{Re}(s) > 0$. □

9.0.3 Location of Zeros

We now show that $\zeta(s)$ has no zeros on $\mathrm{Re}(s) = 1$; this fact is crucial to the prime number theorem. For this we use the following ingenious lemma, attributed to Mertens.

Lemma 9.4. *(Mertens) For $x, y \in \mathbb{R}$ with $x > 1$ we have $|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)| \geq 1$.*

Proof. From the Euler product $\zeta(s) = \prod_p (1-p^{-s})^{-1}$, we see that $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}\log|\zeta(s)| &= -\sum_p \log|1-p^{-s}| \\ &= -\sum_p \mathrm{Re}\log(1-p^{-s}) \\ &= \sum_p\sum_{n\geq 1}\frac{\mathrm{Re}(p^{-ns})}{n},\end{aligned}$$

since $\log|z| = \mathrm{Re}\log z$ and $\log(1-z) = -\sum_{n\geq 1}\frac{z^n}{n}$ for $|z| < 1$. Plugging in $s = x+iy$ yields

$$\log|\zeta(x+iy)| = \sum_p\sum_{n\geq 1}\frac{\cos(ny\log p)}{np^{nx}},$$

since

$$\begin{aligned}\mathrm{Re}(p^{-ns}) &= p^{-ns}\mathrm{Re}(e^{-iny\log p}) \\ &= p^{-nx}\cos(-ny\log p) \\ &= p^{-nx}\cos(ny\log p).\end{aligned}$$

Thus

$$\log|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)| = \sum_p\sum_{n\geq 1}\frac{3+4\cos(ny\log p)+\cos(2ny\log p)}{np^{nx}}.$$

We now note that the trigonometric identity $\cos(2\theta) = 2\cos^2\theta - 1$ implies

$$3 + 4\cos\theta + \cos(2\theta) = 2(1+\cos\theta)^2 \geq 0.$$

Taking $\theta = ny\log p$ yields $\log|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)| \geq$, which proves the lemma. □

Corollary 8. *$\zeta(s)$ has no zeros on $Re(s) \geq 1$.*

Proof. We know from Theorem (9.2) that $\zeta(s)$ has no zeros on $\mathrm{Re}(s) > 1$, so suppose $\zeta(1+iy) = 0$ for some $y \in \mathbb{R}$. Then $y \neq 0$, since $\zeta(s)$ has a pole at $s = 1$, and we know that $\zeta(s)$ does not have a pole at $1 + 2iy \neq 1$ by Theorem (9.3). We therefore must have

$$\lim_{x\to 1}|\zeta(x)^3\zeta(x+iy)^4\zeta(x+2iy)| = 0,$$

since $\zeta(s)$ has a simple pole at $s = 1$, a zero at $1+iy$, and no pole at $1+2iy$. But this contradicts Lemma (9.4) □

9.0.4 Meaure Theory Interpretation of the Riemann Zeta Function

Let $(X, \mathcal{M}, \mu)$ be a σ-finite measure space and let $f\colon X \to \mathbb{C}$ be an integrable function. We can construct a finite complex measure on $\mathcal{M}$, denoted μ_f, by defining $\mu_f(A) = \int_A f \mathrm{d}\mu$ for all $A \in \mathcal{M}$. Furthermore, we can also construct a pseudometric d_f on $\mathcal{M}$ giving it the structure of a pseudometric space, where d_f is defined by $\mathrm{d}_f(A, B) = |\mu_f|(A \Delta B)$ for all $A, B \in \mathcal{M}$ where $|\mu_f|$ is the total variation of μ_f (so $|\mu_f|(A) = \int_A |f| \mathrm{d}\mu$). This pseudometric space induces a metric space (which we denote by $\mathcal{M}$ again) with the understanding that two sets $A, B \in \mathcal{M}$ are identified if $\mu(A \Delta B) = 0$. With this in mind, let us focus on the case where $X = \mathbb{R}_{>0}$, $\mathcal{M} = \mathbb{B}(\mathbb{R}_{>0})$, and μ is the usual Borel measure on $\mathcal{M}$.

Proposition 9.2. *Let $f\colon X \to \mathbb{C}$ be an integrable function such that $|f|$ is decreasing and let (A_m) be a sequence of measurable sets. Then we have $A_m \xrightarrow{\mathrm{d}_f} \mathbb{R}_{>0}$ if and only if $A_m \supseteq (0, k]$ eventually in m for all $k \in \mathbb{N}$.*

Proof. Observe that $A_m \xrightarrow{\mathrm{d}_f} X$ if and only if $|\mu_f|(A_m^c) \to 0$ if and only if $\int_{A_m^c} |f| \mathrm{d}\mu \to 0$. If $A_m \supseteq (0, k]$ eventually in m, then $A_m^c \subseteq (k, \infty)$ eventually in m, and thus for all m sufficiently large we have

$$\int_{A_m^c} |f| \mathrm{d}\mu \leq \int_k^\infty |f| \mathrm{d}\mu.$$

The integral on the right goes to 0 as $k \to \infty$ since f is integrable. It follows that $\int_{A_m^c} |f| \mathrm{d}\mu \to 0$ as $m \to \infty$, and hence $A_m \xrightarrow{\mathrm{d}_f} X$.

Conversely, suppose $A_m \xrightarrow{\mathrm{d}_f} X$. Then $\int_{A_m^c} |f| \mathrm{d}\mu \to 0$ as $m \to \infty$. Assume for a contradiction that there exists a k such that $A_m \not\supseteq (0, k]$ frequently in m. Then there exists a subsequence $(A_{\pi(m)})$ of (A_m) such that $B_m = A_{\pi(m)} \cap (0, k]$ has μ_f measure nonzero:

$$\mu_f(B_m) = \int$$

(B_m) of measurable sets such that

$$\int_{A_m^c} |f| \mathrm{d}\mu \leq \int_k^\infty$$

$$\begin{aligned} \infty &> \int_0^\infty |f| \mathrm{d}\mu \\ &= \int_0^m |f| \mathrm{d}\mu + \int_m^\infty |f| \mathrm{d}\mu \end{aligned}$$

if and only if for all $\varepsilon > 0$ there exists $M_\varepsilon \in \mathbb{N}$ such that $m \geq M_\varepsilon$ implies $\int_{A_m^c} |f| \mathrm{d}\mu < \varepsilon$. If $A_m \not\supseteq (0, k]$ eventually in m, then $A_m^c \supseteq (0, k]$ frequently in m, which means $\int_{A_m^c} |f| \mathrm{d}\mu \geq \int_{(0,k]} |f| \mathrm{d}\mu$ frequently in m. Thus if $A_m \xrightarrow{\mathrm{d}_f} \mathbb{N}$, then it must be the case that $A_m \supseteq (0, k]$ eventually in m.

Conversely, suppose $A_m \supseteq (0, k]$ eventually in m. By passing to a subsequence if necessary, we may assume that $A_m \supseteq (0, m]$ for all m. Then observe that

$$\begin{aligned} \int_{A_m^c} |f| \mathrm{d}\mu &\leq \int_m^\infty |f| \mathrm{d}\mu \\ &\to 0 \end{aligned}$$

as $m \to \infty$.

$$\begin{aligned} \infty &> \int_0^\infty |f| \mathrm{d}\mu \\ &= \int_0^m |f| \mathrm{d}\mu + \int_m^\infty |f| \mathrm{d}\mu \end{aligned}$$

$$\begin{aligned} \infty &> \int_0^\infty |f| \mathrm{d}\mu \\ &= \int_{A_m} |f| \mathrm{d}\mu + \int_{A_m^c} |f| \mathrm{d}\mu \\ &\geq \int_0^m |f| \mathrm{d}\mu + \int_{A_m^c} |f| \mathrm{d}\mu \\ &\geq m|f(m)| + \int_{A_m^c} |f| \mathrm{d}\mu. \end{aligned}$$

$$\int_{A_m^c} |f| \mathrm{d}\mu$$

: there exists $\pi(k) \in \mathbb{N}$ such that $m \geq \pi(k)$ implies $A_m \supseteq \mathbb{N}_{\leq k}$. Conversely, if $k \in A_m$ eventually in m for all $k \in \mathbb{N}$, then $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ since $\limsup A_m = \mathbb{N} = \liminf A_n$. $\square$

For each $s \in \mathrm{B}_1(\infty)$, define $f_s \colon \mathbb{R}_{>0} \to \mathbb{R}$ by

$$f_s(x) = \sum_{n=1}^{\infty} n^{-s} 1_{[n,n+1]}(x).$$

Since $\mathrm{Re}(s) > 1$ this function is integrable, so as noted above, we obtain a complex measure $\mu_s = \mu_{f_s}$ defined by

$$\mu_s(A) = \sum_{n=1}^{\infty} \mu(A_{[n]}) n^{-s} = \zeta_A(s).$$

for all $A \in \mathcal{M}$ where $A_{[n]} = A \cap [n, n+1]$. We also obtain a pseudometric d_s on $\mathcal{M}$ defined by

$$\begin{aligned}
\mathrm{d}_s(A,B) &= |\mu_s|(A \Delta B) \\
&= \int_{A\Delta B} |f_s| \mathrm{d}\mu \\
&= \int_{A\Delta B} \left| \sum_{n=1}^{\infty} n^{-s} 1_{[n,n+1]} \right| \mathrm{d}\mu \\
&= \int_{A\Delta B} \left(\sum_{n=1}^{\infty} n^{-\mathrm{Re}(s)} 1_{[n,n+1]} \right) \mathrm{d}\mu \\
&= \sum_{n=1}^{\infty} \mu((A\Delta B)_{[n]}) n^{-\mathrm{Re}(s)}.
\end{aligned}$$

In particular, observe that $A_m \to A$ if and only if $\mu((A_m \Delta A)_{[n]}) \to 0$ as $m \to \infty$ for each $n \in \mathbb{N}$. For each $s \in \mathrm{B}_1(\infty)$, define $g_s \colon \mathbb{R}_{>0} \to \mathbb{R}$ by

$$g_s(x) = x^{s-1} e^{-x}.$$

We obtain a complex measure ν_s defined by

$$\nu_s(A) = \int_A x^{s-1} e^{-x} \mathrm{d}\mu = \Gamma_A(s).$$

We also obtain a pseudometric d_s on $\mathcal{M}$ defined by

$$\begin{aligned}
\mathrm{d}_s(A,B) &= |\nu_s|(A \Delta B) \\
&= \int_{A\Delta B} |f_s| \mathrm{d}\mu \\
&= \int_{A\Delta B} |x^{s-1} e^{-x}| \mathrm{d}x \\
&= \int_{A\Delta B} x^{\mathrm{Re}(s)-1} |e^{-x}| \mathrm{d}x
\end{aligned}$$

In particular, observe that $A_m \to A$ if and only if $\int_{A_m \Delta A} x^{\mathrm{Re}(s)-1} |e^{-x}| \mathrm{d}x \to 0$ if and only if $\mu((A_m \Delta A)_{[n]}) \to 0$ as $m \to \infty$ for each $n \in \mathbb{N}$.

Proposition 9.3. *We have $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ if and only if $k \in A_m$ eventually in m for all $k \in \mathbb{N}$.*

Proof. Observe that $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ if and only if for all $\varepsilon > 0$ there exists $M_\varepsilon \in \mathbb{N}$ such that $m \geq M_\varepsilon$ implies $\sum_{n \notin A_m} n^{-s} < \varepsilon$. If $k \notin A_m$ frequently in m, then $\sum_{n \notin A_m} n^{-s} \geq k^{-s}$ frequently in m. Thus if $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$, then it must be the case that $k \in A_m$ eventually: there exists $\pi(k) \in \mathbb{N}$ such that $m \geq \pi(k)$ implies $A_m \supseteq \mathbb{N}_{\leq k}$. Conversely, if $k \in A_m$ eventually in m for all $k \in \mathbb{N}$, then $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ since $\limsup A_m = \mathbb{N} = \liminf A_n$. □

Proposition 9.4. *We have $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ if and only if $k \in A_m$ eventually in m for all $k \in \mathbb{N}$.*

Proof. Observe that $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ if and only if for all $\varepsilon > 0$ there exists $M_\varepsilon \in \mathbb{N}$ such that $m \geq M_\varepsilon$ implies $\sum_{n \notin A_m} n^{-s} < \varepsilon$. If $k \notin A_m$ frequently in m, then $\sum_{n \notin A_m} n^{-s} \geq k^{-s}$ frequently in m. Thus if $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$, then it must be the case that $k \in A_m$ eventually: there exists $\pi(k) \in \mathbb{N}$ such that $m \geq \pi(k)$ implies $A_m \supseteq \mathbb{N}_{\leq k}$. Conversely, if $k \in A_m$ eventually in m for all $k \in \mathbb{N}$, then $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$ since $\limsup A_m = \mathbb{N} = \liminf A_n$. □

Proposition 9.5. *If $A_m \xrightarrow{\mathrm{d}_s} \mathbb{N}$, then $\zeta_{A_m}(s)$ converges to $\zeta(s)$ uniformly on $\mathrm{B}_{1+\delta}(\infty)$ for all $\delta > 0$.*

Proof. By Proposition (9.4), we know that $k \in A_m$ eventually in m for all $k \in \mathbb{N}$. By passing to a subsequence if necessary, we may assume that $A_m \supseteq \mathbb{N}_{\leq m}$. Let $\varepsilon, \delta > 0$ and choose M such that $M^{-\delta}/\delta < \varepsilon$. Then observe that $m \geq M$ implies

$$\begin{aligned}
|\zeta(s) - \zeta_A(s)| &= \left|\mu_{f_s}(\mathbb{R}_{>0}) - \mu_{f_s}(A)\right| \\
&= |\mu_{f_s}(A^c)| \\
&= \left|\sum_{n=1}^{\infty} \mu(A^c \cap [n, n+1])n^{-s}\right| \\
&\leq \sum_{n=1}^{\infty} \mu(A^c \cap [n, n+1])n^{-1-\delta} \\
&= \\
&\leq \int_m^\infty x^{-1-\delta} \mathrm{d}x \\
&= \frac{1}{\delta} m^{-\delta} \\
&< \varepsilon
\end{aligned}$$

$$\begin{aligned}
|\zeta(s) - \zeta_{A_m}(s)| &= |\mu_s(\mathbb{N}) - \mu_s(A_m)| \\
&= \mu_s(\mathbb{N} \backslash A_m) \\
&\leq \mu_s(\mathbb{N}_{\geq m}) \\
&\leq \mu_{1+\delta}(\mathbb{N}_{\geq m}) \\
&= \sum_{n \geq m} n^{-1-\delta} \\
&\leq \int_m^\infty x^{-1-\delta} \mathrm{d}x \\
&= \frac{1}{\delta} m^{-\delta} \\
&< \varepsilon
\end{aligned}$$

for all $s \in \mathrm{B}_{1+\delta}(\infty)$. □

9.1 The Prime Number Theorem

The prime counting function $\pi \colon \mathbb{R} \to \mathbb{Z}_{\geq 0}$ is defined by

$$\pi(x) := \sum_{p \leq x} 1;$$

it counts the number of primes up to x. The prime number theorem (PNT) states that

$$\pi(x) \sim \frac{x}{\log x}.$$

The notation $f(x) \sim g(x)$ means $\lim_{x \to \infty} f(x)/g(x) = 1$; one says that f is **asymptotic** to g. This conjectured growth rate for $\pi(x)$ dates back to Gauss and Legendre in the 18th century. In fact Gauss believed the asymptotically equivalent but more accurate statement

$$\pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t}.$$

Rather than work directly with $\pi(x)$, it is more convenient to work with the log-weighted prime-counting function by Chebyshev:

$$\vartheta(x) := \sum_{p \leq x} \log p,$$

whose growth rate differs from that of $\pi(x)$ by a logarithmic factor.

Theorem 9.5. *(Chebyshev) $\pi(x) \sim x/\log x$ if and only if $\vartheta(x) \sim x$.*

Proof. We clearly have $0 \leq \vartheta(x) \leq \pi(x) \log x$, thus

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x) \log x}{x}.$$

For every $\varepsilon \in (0, 1)$, we have

$$\begin{aligned}
\vartheta(x) &\geq \sum_{x^{1-\varepsilon} < p \leq x} \log p \\
&\geq \log\left(x^{1-\varepsilon}\right)(\pi(x) - \pi(x^{1-\varepsilon})) \\
&= (1-\varepsilon)(\log x)(\pi(x) - \pi(x^{1-\varepsilon})) \\
&\geq (1-\varepsilon)(\log x)(\pi(x) - x^{1-\varepsilon}),
\end{aligned}$$

and therefore

$$\pi(x) \leq \left(\frac{1}{1-\varepsilon}\right)\frac{\vartheta(x)}{\log x} + x^{1-\varepsilon}.$$

Thus for all $\varepsilon \in (0,1)$ we have

$$\frac{\vartheta(x)}{x} \leq \frac{\pi(x)\log x}{x} \leq \left(\frac{1}{1-\varepsilon}\right)\frac{\vartheta(x)}{x} + \frac{\log x}{x^{\varepsilon}}.$$

The second term on the RHS tends to 0 as $x \to \infty$, and the lemma follows: by choosing ε sufficiently small we can make the ratios $\vartheta(x)$ to x and $\pi(x)$ to $x/\log x$ arbitrarily close together as $x \to \infty$, so if one of them tends to 1, so must the other. □

In view of Chebyshev's result, the prime number theorem is equivalent to $\vartheta(x) \sim x$. We thus want to prove $\lim_{x\to\infty} \vartheta(x)/x = 1$. Let us first show that $\lim_{x\to\infty} \vartheta(x)/x$ is bounded, which is indicated by the asymptotic notation $\vartheta(x) = O(x)$.

Lemma 9.6. *(Chebyshev). For $x \geq 1$ we have $\vartheta(x) \leq (4\log 2)x$, thus $\vartheta(x) = O(x)$.*

Proof. For any integer $n \geq 1$, the binomial theorem implies

$$\begin{aligned}
2^{2n} &= (1+1)^{2n} \\
&= \sum_{m=0}^{2n} \binom{2n}{m} \\
&\geq \binom{2n}{n} \\
&= \frac{(2n)!}{n!n!} \\
&\geq \prod_{n<p\leq 2n} p \\
&= \exp(\vartheta(2n) - \vartheta(n)),
\end{aligned}$$

since $(2n)!$ is divisible by every prime $p \in (n, 2n]$ but $n!$ is not divisible by any such p. Taking logarithms on both sides yields

$$\vartheta(2n) - \vartheta(n) \leq 2n\log 2,$$

valid for all integers $n \geq 1$. For any integer $m \geq 1$ we have

$$\begin{aligned}
\vartheta(2^m) &= \sum_{n=1}^{m} (\vartheta(2^n) - \vartheta(2^{n-1})) \\
&\leq \sum_{n=1}^{m} 2^n \log 2 \\
&\leq 2^{m+1}\log 2.
\end{aligned}$$

For any real $x \geq 1$ we can choose an integer $m \geq 1$ so that $2^{m-1} \leq x < 2^m$, and then

$$\begin{aligned}
\vartheta(x) &\leq \vartheta(2^m) \\
&\leq 2^{m+1}\log 2 \\
&= (4\log 2)2^{m-1} \\
&\leq (4\log 2)x,
\end{aligned}$$

as claimed. □

In order to prove $\vartheta(x) \sim x$, we will use a general analytic criterion applicable to any non-decreasing real function $f(x)$.

Lemma 9.7. *Let $f\colon \mathbb{R}_{\geq 1} \to \mathbb{R}$ be a nondecreasing function. If the integral $\int_1^\infty \frac{f(t)-t}{t^2}\mathrm{d}t$ converges, then $f(x) \sim x$.*

Proof. Let $F(x) := \int_1^x \frac{f(t)-t}{t^2}\mathrm{d}t$. The hypothesis is that $\lim_{x\to\infty} F(x)$ exists. This implies that for all $\lambda > 1$ and all $\varepsilon > 0$ we have $|F(\lambda x) - F(x)| < \varepsilon$ for all sufficiently large x. Fix $\lambda > 1$ and suppose there is an unbounded sequence (x_n) such that $f(x_n) \geq \lambda x_n$ for all $n \geq 1$. For each x_n we have

$$\begin{aligned}
F(\lambda x_n) - F(x_n) &= \int_{x_n}^{\lambda x_n} \frac{f(t)-t}{t^2}\mathrm{d}t \\
&\geq \int_{x_n}^{\lambda x_n} \frac{\lambda x_n - t}{t^2}\mathrm{d}t \\
&= \int_1^{\lambda} \frac{\lambda - u}{u^2}\mathrm{d}u \qquad\qquad u = tx_n \\
&= c,
\end{aligned}$$

for some $c > 0$, where we used the fact that f is nondecreasing to get the middle inequality. Taking $\varepsilon < c$, we have $|F(\lambda x_n) - F(x_n)| = c > \varepsilon$ for arbitrarily large x_n, a contradiction. Thus $f(x) < \lambda x$ for all sufficiently large x. A similar argument shows $f(x) > x/\lambda$ for all sufficiently large x. These inequalities hold for all $\lambda > 1$, so $\lim_{x\to\infty} f(x)/x = 1$, or equivalently, $f(x) \sim x$. □

In order to show that the hypothesis of Lemma (9.7) is satisfied for $f = \vartheta$, we will work with the function $H(t) = \vartheta(e^t)e^{-t} - 1$; the change of variables $t = e^u$ shows that

$$\int_1^\infty \frac{\vartheta(t)-t}{t^2}\mathrm{d}t \text{ converges} \quad\iff\quad \int_0^\infty H(u)\mathrm{d}u \text{ converges}.$$

We now recall the Laplace transform:

Definition 9.1. Let $h\colon \mathbb{R}_{>0} \to \mathbb{R}$ be a piecewise continuous function. The **Laplace transform** $\mathcal{L}h$ of h is the complex function defined by

$$\mathcal{L}h(x) := \int_0^\infty e^{-st}h(t)\mathrm{d}t,$$

which is holomorphic on $\mathrm{Re}(s) > c$ for any $c \in \mathbb{R}$ for which $h(t) = O(e^{ct})$.

The following properties of the Laplace transform are easily verified:

- $\mathcal{L}(g+h) = \mathcal{L}g + \mathcal{L}h$ and for any $a \in \mathbb{R}$ we have $\mathcal{L}(ah) = a\mathcal{L}h$.
- If $h(t) = a \in \mathbb{R}$ is constant then $\mathcal{L}h(s) = a/s$.
- $\mathcal{L}(e^{at}h(t))(s) = \mathcal{L}(h)(s-a)$ for all $a \in \mathbb{R}$.

We now define the auxiliary function

$$\Phi(s) := \sum_p p^{-s}\log p,$$

which is related to $\vartheta(x)$ by the following lemma.

Lemma 9.8. *$\mathcal{L}(\vartheta(e^t))(s) = \Phi(s)/s$ is holomorphic on $\mathrm{Re}(s) > 1$.*

9.2 Functional Equation

Definition 9.2. The **Fourier transform** of a Schwartz function $f \in \mathcal{S}(\mathbb{R})$ is the function

$$\widehat{f}(y) := \int_{\mathbb{R}} f(x)e^{-2\pi ixy}\mathrm{d}x,$$

which is also a Schwartz function. We can recover $f(x)$ from $\widehat{f}(y)$ via the inverse transform

$$f(x) = \int_{\mathbb{R}} \widehat{f}(y)e^{2\pi ixy}\mathrm{d}y.$$

The maps $f \mapsto \widehat{f}$ and $\widehat{f} \mapsto f$ are thus linear operators on $\mathcal{S}(\mathbb{R})$.

Lemma 9.9. *For all $t \in \mathbb{R}_{>0}$ and $f \in \mathcal{S}(\mathbb{R})$ we have*

$$\widehat{f(tx)}(y) = \frac{1}{t}\widehat{f}(y/t).$$

Proof. Indeed, we have

$$\begin{aligned}\widehat{f(tx)}(y) &= \int_{\mathbb{R}} f(tx)e^{-2\pi ixy}\mathrm{d}x \\ &= \int_{\mathbb{R}} f(u)e^{-2\pi iuy/t}\frac{\mathrm{d}u}{t} && u = tx \\ &= \frac{1}{t}\widehat{f}(y/t).\end{aligned}$$

□

9.2.1 Jacobi's theta function

We now define the **theta function**

$$\Theta(\tau) := \sum_{n\in\mathbb{Z}} e^{\pi in^2\tau} = 1 + 2\sum_{n\geq 1} e^{\pi in^2\tau}. \tag{18}$$

The series converges absolutely and locally uniformly on $\mathrm{im}\,\tau > 0$. Indeed, let $\delta > 0$ and $\tau = r + it$. Then for $\mathrm{im}\,\tau > \delta$, we have

$$\begin{aligned}\sum_{n\in\mathbb{Z}} |e^{\pi in^2\tau}| &= \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} \\ &= 1 + 2\sum_{n\geq 1}(e^{-\pi t})^{n^2} \\ &\leq 1 + 2\sum_{n\geq 0}(e^{-\pi t})^{n} \\ &\leq 1 + 2\sum_{n\geq 0}(e^{-\pi \delta})^{n} \\ &\leq 1 + \frac{2}{1-e^{-\pi\delta}}.\end{aligned}$$

It follows that the series (18) converges absolutely on $\mathrm{im}\,\tau > \delta$. Furthermore, it converges uniformly on $\mathrm{im}\,\tau > \delta$ by an easy application of the Weirestrass M-test with $M_n = 2e^{-\pi nt}$.

It is easy to check that $\Theta(\tau)$ is periodic modulo 2, that is,

$$\Theta(\tau+2) = \Theta(\tau),$$

but it also satisfies another functional equation.

Lemma 9.10. *For all $t \in \mathbb{R}_{>0}$ we have $\Theta(it) = t^{-1/2}\Theta(i/t)$.*

Proof. Put $g(x) := e^{-\pi x^2}$ and $h(x) := g(t^{1/2}x) = e^{-\pi x^2 t}$. Then observe that

$$\begin{aligned}\widehat{h}(y) &= \widehat{g(t^{1/2}x)}(y)\\ &= t^{-1/2}\widehat{g}(t^{-1/2}y)\\ &= t^{-1/2}g(t^{-1/2}y).\end{aligned}$$

Plugging in $\tau = it$ into $\Theta(\tau)$ and applying Poisson summation yields

$$\begin{aligned}\Theta(it) &= \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}\\ &= \sum_{n\in\mathbb{Z}} h(n)\\ &= \sum_{n\in\mathbb{Z}} \widehat{h}(n)\\ &= \sum_{n\in\mathbb{Z}} t^{-1/2}g(t^{-1/2}n)\\ &= t^{-1/2}\Theta(i/t).\end{aligned}$$

□

10 Modular Forms

The notion of modularity can be set in quite a general context, but for now we consider functions defined on the upper half plane

$$\mathfrak{h} = \{\tau \in \mathbb{C} \mid \operatorname{Im}(\tau) > 0\}.$$

Observe that γ and $-\gamma$ gives the same action, thus it is more natural to consider the group $\mathrm{PSL}_2(\mathbb{R})$.

The functional equations defining modularity are of they type $f(\gamma(\tau)) = f(\tau)$. We will see below that it is essential to consider more general functional equations $f(\gamma(\tau)) = \nu(\gamma,\tau)f(\tau)$ for some **simple** and fixed function ν of γ and τ.

Modularity means the existence of a functional equation of the type $f(\gamma(\tau)) = \nu(\gamma,\tau)f(\tau)$. From the law $\gamma_1(\gamma_2(\tau)) = (\gamma_1\gamma_2)(\tau)$, we see that

$$\nu(\gamma_1\gamma_2,\tau)f(\tau) = f((\gamma_1\gamma_2)(\tau)) = f(\gamma_1(\gamma_2(\tau)) = \nu(\gamma_1,\gamma_2(\tau))\nu(\gamma_2,\tau)f(\tau)$$

implies the *cocycle condition* $\nu(\gamma_1\gamma_2,\tau) = \nu(\gamma_1,\gamma_2(\tau))\nu(\gamma_2,\tau)$. If we want ν to be independent of τ, then this reduces to $\nu(\gamma_1\gamma_2) = \nu(\gamma_1)\nu(\gamma_2)$; in other words, ν must be a character of G.

We note that by the differentiation rule for compositition of functions we have

$$(d/d\tau)(\gamma_1(\gamma_2(\tau))) = ((d/d\tau)\gamma_1)(\gamma_2(\tau))(d/d\tau)\gamma_2(\tau),$$

so the function $\nu(\gamma,\tau) = (d/d\tau)\gamma(\tau)$ satisfies the cocycle condition. If $\gamma = \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)$, we have $(d/d\tau)\gamma(\tau) = \det(\gamma)/(c\tau+d)^2$, which is therefore our basic building block for **automorphy factors**, as functions ν satisfying the cocycled condition are called.

Observe that the cocycle condition is presereved under products or powers of functions. For instance, if ν_1 and ν_2 are two functions which satisfy the cocyle condition, then

$$\begin{aligned}(\nu_1\nu_2)(\gamma_1\gamma_2,\tau) &= \nu_1(\gamma_1\gamma_2,\tau)\nu_2(\gamma_1\gamma_2,\tau)\\ &= \nu_1(\gamma_1,\gamma_2(\tau))\nu_1(\gamma_2,\tau)\nu_2(\gamma_1,\gamma_2(\tau))\nu_2(\gamma_2,\tau)\\ &= \nu_1(\gamma_1,\gamma_2(\tau))\nu_2(\gamma_1,\gamma_2(\tau))\nu_1(\gamma_2,\tau)\nu_2(\gamma_2,\tau)\\ &= (\nu_1\nu_2)(\gamma_1,\gamma_2(\tau))(\nu_1\nu_2)(\gamma_2,\tau).\end{aligned}$$

Notice that we needed to use the fact that $\nu(\gamma,\tau)$ is just a complex number so it belongs to an abelian group. Similarly for $n \in \mathbb{Z}$,

$$\begin{aligned}(\nu^n)(\gamma_1\gamma_2,\tau) &= (\nu(\gamma_1\gamma_2,\tau))^n\\ &= \nu(\gamma_1,\gamma_2(\tau))^n\nu(\gamma_2,\tau)^n\\ &= (\nu^n)(\gamma_1,\gamma_2(\tau))(\nu^n)(\gamma_2,\tau).\end{aligned}$$

Again, this calculation depended on the fact that $\mathbb{C}^\times$ is abelian. So the set of all functions ν which satisfy the cocycle condition form an abelian group.

We have shown that $\nu(\gamma,\tau) = (c\tau+d)^2$ satisfies the cocycle condition.

$$e^{i\tau} = e^{i(r+it)} = e^{-t}e^{ir}$$

10.1 Upper Half Plane

Let $\mathfrak{h} = \{\tau \in \mathbb{C} \mid \operatorname{Im}(\tau) > 0\}$ be the upper half-plane. Then $\mathfrak{h}$ is a model of the hyperbolic plane when endowed with the metric

$$\mathrm{d}s = \frac{1}{y}\sqrt{\mathrm{d}x^2 + \mathrm{d}y^2}.$$

Let P and Q bet two points in the upper half-plane. The **hyperbolic distance** between P and Q in $\mathfrak{h}$ is defined using integration along the line $\overline{PQ}$:

$$\mathrm{d}(P,Q) = \int_P^Q \frac{\sqrt{(\mathrm{d}x/\mathrm{d}t)^2 + (\mathrm{d}y/\mathrm{d}t)^2}}{y(t)}\mathrm{d}t$$

where the integral is taken along the hyperbolic line in $\mathfrak{h}$ from P to Q using a smooth parametrization $\gamma(t) = (x(t),y(t))$ of the segment in $\overline{PQ}$ from P to Q.

Example 10.1. To compute the distance between $y_0 i$ and $y_1 i$, we parametrize the vertical line between them as $\gamma(t) = (0, (1-t)y_0 + ty_1)$ for $0 \le t \le 1$. Then

$$\begin{aligned} d(y_0 i, y_1 i) &= \int_0^1 \frac{\sqrt{0^2 + (y_1 - y_0)^2}}{(1-t)y_0 + ty_1} dt \\ &= |\log y_1 - \log y_0| \\ &= |\log(y_1/y_0)|. \end{aligned}$$

In particular we have $d(yi, i) = |\log y|$ and the midpoint between $y_0 i$ and $y_1 i$ when $y_0 \neq y_1$ is $\sqrt{y_0 y_1} i$ which is always different form the Euclidean midpoint.

Proposition 10.1. *We have* $d_{\mathfrak{h}}(\gamma\tau, \gamma\tau') = d_{\mathfrak{h}}(\tau, \tau')$.

Proof. We have

$$d_{\mathfrak{h}}(\gamma\tau, \gamma\tau') = \int_{\tau}^{\tau'} \frac{\sqrt{(dx/dt)^2 + (dy/dt)^2}}{y(t)} dt$$

□

We denote by $\mathrm{SL}_2(\mathbb{R})$ the group of 2×2 real matrices $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant 1. This group acts on $\mathfrak{h}$ via **Möbius transformations**: if $\tau \in \mathfrak{h}$, then we set

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}.$$

Indeed, that $\gamma\tau \in \mathfrak{h}$ follows from the following proposition:

Proposition 10.2. *We have* $\mathrm{Im}(\gamma\tau) = \mathrm{Im}(\tau)/|c\tau + d|^2$.

Proof. Write $\tau = r + it$. Then

$$\begin{aligned} \gamma\tau &= \frac{a\tau + b}{c\tau + d} \\ &= \frac{a(r+it) + b}{c(r+it) + d} \\ &= \frac{(ar+b) + iat}{(cr+d) + ict} \\ &= \frac{(ar+b)(cr+d) + act^2}{(cr+d)^2 + (ct)^2} + i\frac{at(cr+d) - ct(ar+b)}{(cr+d)^2 + (ct)^2}. \end{aligned}$$

Therefore

$$\begin{aligned} \mathrm{Im}(\gamma\tau) &= \frac{at(cr+d) - ct(ar+b)}{(cr+d)^2 + (ct)^2} \\ &= \frac{t}{|c\tau + d|^2}(a(cr+d) - c(ar+b)) \\ &= \frac{t}{|c\tau + d|^2} \\ &= \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}. \end{aligned}$$

where we used the fact that $\det \gamma = ad - bc = 1$ in order to get the third line from the second line. □

The group $\mathrm{PSL}_2(\mathbb{R})$ acts on $\mathfrak{h}$ by linear fractional transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

In fact $\mathrm{PSL}_2(\mathbb{R})$ is isomorphic to the group of all orientation-preserving isometries of $\mathfrak{h}$.

Let P and Q be two points

Definition 10.1. Throughout these notes, we will denote $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ the subgroup of $\mathrm{SL}_2(\mathbb{R})$ consisting of matrices with integer coefficients and write $\overline{\Gamma}$ for the full modular group, $\mathrm{PSL}_2(\mathbb{Z})$. The groups that we will consider will always be finite index subgroups of Γ, which are evidently Fuchsian groups of the first kind.

Definition 10.2. Let f be a function from $\mathfrak{h}$ to $\mathbb{C}$, let $G \subset \mathrm{SL}_2(\mathbb{R})$ be a cofinite Fuchsian group of the first kind, and let χ be a homomorphism from G to the group of complex numbers of modulus 1. We say that f is **weakly modular** of **weight** k with **multiplier system** χ if for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ we have

$$(f|_k\gamma)\tau := j(\gamma,\tau)^{-k} f(\gamma\tau) = \chi(\gamma) f(\tau),$$

where $j(\gamma,\tau) = c\tau + d$, and we use $\mathrm{M}_k^w(G,\chi)$ to denote the space of all such functions. When k is not an integer it is understood that $j(\gamma,\tau)^k$ is evaluated using the principal branch of the argument. The action of $\gamma \in \mathrm{SL}_2(\mathbb{R})$ given by $f|_k\gamma$ (called the **weight** k **slash-action**) will also be used for $\gamma \in \mathrm{GL}_2(\mathbb{R})$ by the more general formula

$$(f|_k\gamma)\tau := \det(\gamma)^{k/2} j(\gamma,\tau)^{-k} f(\gamma\tau).$$

The reason for using the term "weakly" above is that we have not yet specified any holomorphy or meromorphy condition. We will say that a weakly modular function f of nonzero weight k is

1. a **weakly holomorphic modular form** if f in addition is holomorphic in $\mathfrak{h}$,
2. a **holomorphic modular form** if f extends holomorphically to the so-called **cusps** of G in $\partial\mathfrak{h}$,
3. a **cusp form** if f also vanishes at the cusps of G.

The spaces of functions defined above are denoted by $\mathrm{M}_k^!(G,\chi)$, $\mathrm{M}_k(G,\chi)$, and $\mathrm{S}_k(G,\chi)$ respectively. We will reserve the term modular **function** for weight 0. The reason for this convention is that the weight 0 functions correspond to functions on the quotient $G\backslash\mathfrak{h}$ while nonzero weight functions correspond to **differential forms**. To be precise, if f is a holomorphic modular form of weight $2k$ and trivial multiplier, then $f(z)(\mathrm{d}z)^k$ is invariant under G; that is, it defines a holomorphic differential on $G\backslash\mathfrak{h}$. For instance, f being a modular form of weight $2k$ means $f(\gamma\tau) = j(\gamma,\tau)^{2k} f(\tau)$ for all $\gamma \in G$ and $\tau \in \mathfrak{h}$. Also,

$$\mathrm{d}(\gamma\tau)^k = \det(\gamma)^k j(\gamma,\tau)^{-2k} \mathrm{d}\tau^k$$

So $f(\gamma\tau)\mathrm{d}(\gamma\tau)^k = f(\tau)\mathrm{d}\tau$.

Example 10.2. Here is an example of a homomorphism $\chi : \mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}^\times$ whose image is all the 12th roots of unity:

$$\chi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = e^{\frac{2\pi i}{12}((1-c^2)(bd+3(c-1)d+c+3)+c(a+d-3))}.$$

The function $\Delta(\tau) = e^{2\pi i\tau}\prod_{n\geq 1}(1-e^{2\pi i n\tau})^{24}$ satisfies $\Delta(\gamma\tau) = j(\gamma,\tau)^{12}\Delta(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and its 12th root $f(\tau) = e^{2\pi i\tau/12}\prod_{n\geq 1}(1-e^{2\pi i n\tau})^2$ satisfies $f(\gamma\tau) = \chi(\gamma) j(\gamma,\tau) f(\tau)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$: χ is a multiplying factor here.

There are two group actions we are considering.

$$(\gamma,\tau) \mapsto \gamma\tau \qquad \text{and} \qquad (\gamma,\tau) \mapsto j(\gamma,\tau)^k$$

The first one is obviously a group action. The second one is a group action because $j(\gamma,\tau)$ satisfies the cocycle relation:

$$(\gamma_1\gamma_2,\tau) \mapsto j(\gamma_1\gamma_2,\tau)^k$$

$$(\gamma_2,\tau$$

Note that

$$\gamma\tau + 1 = (e_{12}\gamma)\tau$$

10.2 Bernoulli Numbers and the Gamma and Zeta Functions

Definition 10.3. The **Bernoulli number** B_n are defined by the formal power series (which in fact has radius of convergence 2π):

$$\frac{T}{e^T - 1} = \sum_{n\geq 0} B_n \frac{T^n}{n!}.$$

Proposition 10.3. *The B_n are rational numbers. We have $B_0 = 1$, $B_1 = -1/2$, $B_{2n+1} = 0$ for $n \geq 1$, and $(-1)^{n-1}B_{2n} > 0$ for $n \geq 1$.*

Proof. The rationality follows from that of the power series coefficients of e^T. For the remaining properties note that the hyperbolic cotangent function cotanh is odd and that

$$\frac{T}{e^T-1} + \frac{T}{2} = \frac{T}{2}\mathrm{cotanh}\left(\frac{T}{2}\right).$$

□

Remark 10. In working with modular forms, one should know the values of B_{2n} at least up to B_{16} by heart.

11 Ring of Adeles

Recall that we have a canonical injection

$$\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z} \simeq \prod_p \mathbb{Z}_p,$$

that embed $\mathbb{Z}$ into the product of its nonarchimedean completions.