DIRICHLET CLASS NUMBER FORMULA FOR IMAGINARY QUADRATIC FIELDS

Süeda Şentürk Avcı

November 18, 2023

Chapter 1

Lattices

Lattices occur many areas of Algebraic Number Theory such as Elliptic Curves, Class Groups, etc.

In this chapter, we will define what a complex lattice is, basis of a complex lattice and its order.

1.1 Complex Lattices

Definition 1.1.1. A complex lattice $\Lambda \subset \mathbf{C}$ is defined for any complex numbers $\omega_1, \omega_2 \in \Lambda$ satisfying following conditions:

1. ω_1, ω_2 are not real multiples of each other,
2. the set of lattice points precisely defined as;

$$\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbf{Z}\}. \tag{1.1}$$

Pairs that satisfying the conditions above are called *basis* of the lattice. To set some kind of ordering for the basis we say a basis is *normalized* if $\Im \frac{\omega_2}{\omega_1} > 0$. Later, we will see that this normalized basis will allow us to observe some good features.

A lattice have more than one normalized basis. Say the following $\langle \omega_1, \omega_2 \rangle$ and $\langle \omega_1', \omega_2' \rangle$ are normalized basis for the lattice Λ. Then, it satisfies

$$\mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2' = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2. \tag{1.2}$$

To prove that, we will first show

$$\mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2' \subset \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2. \tag{1.3}$$

For $a, b, c, d \in \mathbf{Z}$, we have

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

since $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$.

This equation shows that,

$$\mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2' \subset \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2. \tag{1.4}$$

Since two bases span the same lattice, we should be able to show

$$\mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \subset \mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2'. \tag{1.5}$$

Easiest way to show this is to perform the same matrix operation for the basis $\langle \omega_1, \omega_2 \rangle$ with the inverse of the matrix above.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a. \end{bmatrix}$$

Since a, b, c, d are integers, $ad - bc$ can be either 1 or -1. But observe that since $\langle \omega_1, \omega_2 \rangle$ and $\langle \omega_1', \omega_2' \rangle$ are normalized only possibility is $\dfrac{1}{ad - bc} = 1$. Hence, we see that the normalized bases can be transformed into each other with a matrix $\Omega \in \mathrm{SL}_2(\mathbf{Z})$.

1.2 Homothety

Any point in a complex lattice has the form $x + yi$ for $x, y \in \mathbf{R}$. By rotating and extending the shape of one lattice, we can obtain other lattices and they can be converted to each other. To observe this by using one point, take $x + yi$.

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \cos\theta x + \sin\theta y \\ -\sin\theta x + \cos\theta y \end{bmatrix}$$

This equals to

$$(\cos\theta + i\sin\theta) \cdot (x + yi) \tag{1.6}$$
$$= e^{i\theta} \cdot (x + yi). \tag{1.7}$$

And to extend this point, all we need to do is to multiply each point with a real number r. Set $\gamma = re^{i\theta}$. We can repeat this process for in point in the lattice Λ and obtain a new lattice. Observe that since the matrix above is invertible, we can obtain the former point by multiplying the point with the inverse of this matrix.

Definition 1.2.1. Two lattices Λ, Λ' are called *homothetic* if $\Lambda' = \gamma \cdot \Lambda$ for a γ as mentioned above and denoted as $\Lambda \sim \Lambda'$.

For the sake of future computations, let us set $\dfrac{\omega_2}{\omega_1} = \tau$. Obviously $\Im\tau > 0$. Then from the previous change of basis above, we have

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \tau \\ 1. \end{bmatrix}$$

$\omega_1' = a\tau + b$ and $\omega_2' = c\tau + d$.

$$\frac{\omega_2'}{\omega_1'} = \frac{c\tau + d}{a\tau + b} = \frac{(c\tau + d)(a\overline{\tau} + b)}{(a\tau + b)(a\overline{\tau} + b)} \tag{1.8}$$

$$= \frac{ac|\tau|^2 + ad\overline{\tau} + bc\tau + bd}{a^2|\tau|^2 ab(\tau + \overline{\tau}) + b^2} = \frac{ac|\tau|^2 + ad\overline{\tau} + bc\tau + bd}{|a\tau + b|^2} = \tau'. \tag{1.9}$$

Here,

$$\Im\tau' = \frac{\Im\tau \cdot (ad - bc)}{|a\tau + b|^2}. \tag{1.10}$$

So, we can make the exact change of basis for τ as we have done for ω_1 and ω_2.

$$\mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 = \omega_1(\mathbf{Z} \oplus \mathbf{Z}\tau) \tag{1.11}$$

$$= \omega_1'(\mathbf{Z} \oplus \mathbf{Z}\tau') = \mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2'. \tag{1.12}$$

As we defined τ above, it is easy to see that if two lattices are homothetic there will be at least one basis in each lattice such that their ratio will be the same as in a normalized basis.

Definition 1.2.2. Let Λ be a complex lattice. $J - set$ is defined as

$$J(\Lambda) = \{\tau : \Lambda = \omega_1 \Lambda_\tau\}.$$

We know that τ has positive imaginary part, hence it is located in the upper-half plane in the complex plane. We also know that matrices in $SL_2(\mathbf{Z})$ preserve the sign of the imaginary part of τ, so lattice point will remain in the upper-half plane. The question is if it is possible to cover all the upper half plane with some matrices. Turns out it is possible to cover the whole upper plane with two actions from $SL_2(\mathbf{Z})$.

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \cdot \tau = \tau + 1 \quad and \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot \tau = \frac{-1}{\tau}$$

By acting on finitely many on in a restricted region, we can cover the whole upper-half plane. Let's call this region F, and it's defined as

$$F = \{\Im(z) > 0, |z| \geq 1, \frac{-1}{2} < \Re(z) < \frac{1}{2} \quad and \quad \Re(z) > 0 \, if \, |z| = 1\}.$$

Definition 1.2.3. Let Λ be a complex lattice. The intersection $J(\Lambda) \cap F$ consist of exactly one element, which is denoted as $j(\Lambda)$.

This is because of the coverage of the region F. By acting on it with the matrices above, one can cover the upper-plane of lattice, hence there is enough to have only one point for each point in the upper-plane.

1.3 Complex Multiplication

Remember what we mentioned about the homothety of two lattices. There exists a complex number $\gamma \in \mathbf{C}$ such that $\Lambda' = \gamma\Lambda$. One can observe that if γ is an integer, then the points in Λ' are already existing in Λ. Then, $\Lambda' \subset \Lambda$ and it's called the *sublattice* of Λ. But, this is not always correct for a non-integer γ since the multiplication can change the shape of the lattice. If this multiplication results as a sublattice, then we have a special case.

Definition 1.3.1. Let $\gamma \in \mathbf{C}$ be a non-integer. Then the lattice Λ has *complex multiplication* with γ if the result is a sublattice of Λ.

This result can also be denoted as $\mathbf{Z}\omega_1' \oplus \mathbf{Z}\omega_2' \subset \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$ for the bases $< \omega_1', \omega_2' >$ and $< \omega_1, \omega_2 >$ for the lattices Λ', Λ respectively. This is,

$$\begin{bmatrix} \omega_1' \\ \omega_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

In addition to that, since Λ' is a sublattice of Λ we also have,

$$\begin{bmatrix} \gamma & 0 \\ 0 & \gamma \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix}$$

for some $\gamma \in \mathbf{C}$. The last matrix equality gives us

$$\begin{bmatrix} a-\gamma & b \\ c & d-\gamma \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \end{bmatrix} = 0.$$

Finally, since the matrix above has the determinant 0, we have

$$(a-\gamma)(d-\gamma) - bc = 0 \tag{1.13}$$

$$\gamma^2 - (a+d)\gamma + ad - bc = 0. \tag{1.14}$$

And this gives us the form of γ which is needed to a complex multiplication

$$\gamma = \frac{1}{2}(a + d \pm \sqrt{(a+d)^2 - 4(ad-bc)})$$

$$\gamma = \frac{1}{2}(B \pm \sqrt{B^2 - 4C})$$

for $B = a + d$ and $C = ad - bc$. Here, we obtain the following lemma.

Lemma 1.3.1. *Let Λ be a complex lattice with complex multiplication by γ. Then*

$$\gamma = \frac{1}{2}(B \pm \sqrt{B^2 - 4C}) \tag{1.15}$$

for some integers B, C with $B^2 - 4C < 0$.

Proof. Given above. □

Lemma 1.3.2 (Exercise 1.2)**.** *A lattice Λ has complex multiplication by $\gamma \in \mathbf{C} - \mathbf{Z}$ if and only if it has complex multiplication by $\gamma - n$ for all $n \in \mathbf{Z}$.*

Proof. For the first part of the proof, let $\gamma \cdot \Lambda$ be a complex multiplication of Λ for $\gamma \in \mathbf{C} - \mathbf{Z}$. Then we have

$$\gamma \cdot \Lambda \subset \Lambda \Rightarrow (\gamma - n) \cdot \Lambda \subset \Lambda.$$

Since a lattice is closed under addition, we have

$$(\gamma - n) \cdot \Lambda = \underbrace{\gamma \cdot \Lambda}_{\subset \Lambda} - \underbrace{n \cdot \Lambda}_{\subset \Lambda} \subset \Lambda.$$

For the second part of the proof, let the lattice Λ has a complex multiplication by $(\gamma - n)$ as given in the lemma. So, obviously

$$(\gamma - n) \cdot \Lambda \subset \Lambda \Rightarrow \gamma \cdot \Lambda \subset \Lambda.$$

Again, since Λ is closed under addition,

$$(\gamma - n) \cdot \Lambda = \gamma \cdot \Lambda - \underbrace{n \cdot \Lambda}_{\subset \Lambda} \subset \Lambda. \tag{1.16}$$

From (1.16), $\gamma \cdot \Lambda$ must be a subset of Λ to suffice the relation. Hence we get,

$$\gamma \cdot \Lambda \subset \Lambda \iff (\gamma - n) \cdot \Lambda \subset \Lambda.$$

□

Lemma 1.3.2 enables us to eliminate some possibilities for γ to be a CM with Λ. For instance, if B is even, by the Lemma 1.3.2,

$$\gamma = \sqrt{\left(\frac{B}{2}\right)^2 - C}.$$

If B is odd, then since square of an odd integer is 1 (mod 4), we can write,

$$\gamma = \frac{1}{2} + \frac{1}{2}\sqrt{B^2 - 4C}.$$

Therefore, we can set γ which satisfies CM as

$$\sqrt{-n} \quad \text{for } n \equiv 1{,}2 \pmod 4 \text{ and } \quad \frac{1+\sqrt{-n}}{2} \quad \text{for } n \equiv 3 \pmod 4$$

for $n \in \mathbf{Z}^+$.

By replacing γ in the equation (1.14) with $\sqrt{-n}$ we obtain

$$\begin{aligned} -n - (a+d)\sqrt{-n} + ad - bc = 0 \\ ad - bc - n = (a+d)\sqrt{-n}. \end{aligned}$$

Here, we can observe $a = -d$ since there is no other possibility. So, we obtain

$$\begin{aligned} ad - n &= bc \\ a^2 + n &= -bc \end{aligned}$$

and therefore

$$b|(a^2+n). \tag{1.17}$$

By (1.17) and setting some other restrictions we can obtain the following theorem.

Theorem 1.3.1. *Let $n \equiv 1, 2$ (mod 4) be a square-free positive integer. Then every lattice with CM by $\sqrt{-n}$ is homothetic to a unique lattice of the form*

$$\left\langle 1, \frac{a+\sqrt{-n}}{b} \right\rangle$$

with

1. $a, b \in \mathbf{Z}$
2. $0 < b \leq 2\sqrt{\frac{n}{3}}$
3. $-b < 2a \leq b$
4. $a^2 + n \geq b^2$
5. $b|(a^2+n)$.

1.4 Class Number

Definition 1.4.1. Let n be a square-free positive integer which satisfies $n \equiv 1, 2$ (mod 4). *Class group* of $-n$ is defined as the set of complex numbers $\dfrac{a+\sqrt{-n}}{b}$ satisfying the conditions in the Theorem 1.3.3 above and denoted as $Cl(-n)$.

Corollary 1.4.1. *$Cl(-n)$ is finite.*

Proof. Obvious from the conditions in Theorem 1.3.3. □

1.5 L-series

For a square-free positive integer n, let

$$L(-n) = \sum_{m=1}^{\infty} \left(\frac{-n}{m}\right) \cdot \frac{1}{m}.$$

$\left(\frac{\cdot}{p}\right)$ is called the *extended Legendre symbol*, for a prime $p \neq 2$,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ a nonzero square modulo } p \\ -1 & a \text{ not a square modulo } p \\ 0 & p|a \end{cases}$$

while

$$\left(\frac{a}{2}\right) = \begin{cases} 1 & a \equiv 1 \pmod 8 \\ -1 & a \equiv 5 \pmod 8 \\ 0 & \text{otherwise.} \end{cases}$$

Chapter 2

Ideal Factorizations

Theorem 2.0.1 (Fundamental Theorem of Aritmetic)**.** *Every integer a with $|a| > 1$ can be written as a product of prime numbers and this factorization is unique up to re-ordering and multiplication by* ± 1.

As fundamental theorem of arithmetic states, there is only one unique way to factorize an integer in $\mathbf{Z}$. But this not always the case for elements in some number fields. In this chapter, we will dive into the topic to understand what are properties of these fields such that

$$\mathbf{Q}(\sqrt{-n}) = \{a + b\sqrt{-n} \mid a, b \in \mathbf{Q}\}.$$

2.1 Algebraic Integers

Definition 2.1.1. A unit in a ring is an element which has an multiplicative inverse.

As we observe in the Theorem 1.0.1, factorization of an element is unique up to multiplication of this fields unit. Since every element in $\mathbf{Q}(\sqrt{-n})$ is unit, we will examine the number fields which have the structure

$$\mathbf{Z}[\sqrt{-n}] = \{a + b\sqrt{-n} \mid a, b \in \mathbf{Z}\}.$$

Definition 2.1.2. Let's consider $\alpha \in \mathbf{Z}[\sqrt{-n}]$ which is of the form $\alpha = a + b\sqrt{-n}$. The polynomial which α is the root

$$x^2 - 2ax + (a^2 + nb^2)$$

called *the characteristic polynomial* of α where $a, b \in \mathbf{Z}$.

Definition 2.1.3. The *ring of algebraic integers O_{-n}* of $\mathbf{Q}(\sqrt{-n})$ is the set of all $\alpha \in \mathbf{Q}(\sqrt{-n})$ such that the characteristic polynomial of α has integer coefficients.

The elements in O_{-n} can be classified by the modular correspondence of n.

$$O_{-n} = \begin{cases} \{a + b\sqrt{-n} : \ a, b \in \mathbf{Z}\} \quad \text{if } n \equiv 1, 2 \text{ (mod4)} \\ \{a + b\sqrt{-n} : \ 2a, 2b \in \mathbf{Z} \ a \equiv b \text{ (mod 2 if } n \equiv 3 \text{ (mod 4)}\}. \end{cases}$$

One can easily check that O_{-n} is closed under addition and multiplication, hence it is a ring.

If $n \equiv 1, 2$ (mod 4) then the roots of the characteristic polynomial lies in $\mathbf{Z}[\sqrt{-n}]$. However, if $n \equiv 3$ (mod 4), then some roots lie in $\mathbf{Q}(\sqrt{-n})$.

Let

$$\overline{\omega}_{-n} = \begin{cases} \sqrt{-n} & n \equiv 1, 2 \text{ (mod 4)} \\ \frac{1+\sqrt{-n}}{2} & n \equiv 3 \text{ (mod 4)} \end{cases}.$$

The roots that are in these forms are denoted by $\overline{\omega}_{-n}$. In this case, the elements of the ring of algebraic integers are

$$O_{-n} = \{a + b\overline{\omega}_{-n} : \ a, b \in \mathbf{Z}\}.$$

Definition 2.1.4. For any $\alpha \in O_{-n}$, $\overline{\alpha}$ is called the *conjugate* of α.

For $n \equiv 1, 2$ (mod 4), the conjugate of $\alpha = a + b\overline{\omega}_{-n}$ is $a - b\overline{\omega}_{-n}$ since $\overline{\omega}_{-n} = \sqrt{-n}$. But for the case $n \equiv 3$ (mod 4), since $\overline{\omega}_{-n} = \frac{1+\sqrt{-n}}{2}$, we have

$$\alpha = a + b\overline{\omega}_{-n} = a + b\Big(\frac{1 + \sqrt{-n}}{2}\Big) = \frac{2a + b}{2} + \frac{b\sqrt{-n}}{2}.$$

Therefore,

$$\overline{\alpha} = \frac{2a + b}{2} - \frac{b\sqrt{-n}}{2}.$$

Definition 2.1.5. For $\alpha \in O_{-n}$, the *norm* $N(\alpha)$ and *trace* $tr(\alpha)$ of α are the coefficients of the characteristic polynomial

$$x^2 - tr(\alpha)x + N(\alpha)$$

where $tr(\alpha) = \alpha + \overline{\alpha}$ and $N(\alpha) = \alpha\overline{\alpha}$.

Before we examine the forms of $tr(\alpha)$ and $N(\alpha)$, notice that norm is multiplicative and trace is additive, i.e.

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$
$$tr(\alpha + \beta) = tr(\alpha) + tr(\beta)$$

since conjugation is additive and multiplicative.

The forms of trace and norm for $\alpha = a + b\overline{\omega}_{-n}$ with $a, b \in \mathbf{Z}$ are the following;

$$tr(\alpha) = \begin{cases} 2a & n \equiv 1, 2 \text{(mod 4)} \\ 2a + b & n \equiv 3 \text{(mod 4)} \end{cases}$$

$$N(\alpha) = \begin{cases} a^2 + nb^2 & n \equiv 1, 2 \text{(mod 4)} \\ a^2 + ab + \frac{1+n^2}{4} b^2 & n \equiv 3 \text{(mod 4)} \end{cases}.$$

Definition 2.1.6. A non-unit $\alpha \in O_{-n}$ is irreducible if for $\alpha = a \cdot b$ either a or b is a unit.

In the upcoming sections, we will deal with some problems which will require to apply some division algorithm. It is easy for only $\mathbf{Z}$ itself but a relatively challenging for other number rings. To overcome some parts of this problem, we use norm as a handy tool. In the following lemma, there are properties of norm that we will be using in the remaining part of the chapter.

Lemma 2.1.1. *For any $\alpha, \beta \in O_{-n}$ and $N(\alpha), N(\beta) \in \mathbf{Z}$,*

1. *If $\alpha | \beta$, then $N(\alpha) | N(\beta)$.*
2. *α is a unit $\iff |N(\alpha)| = 1$.*
3. *If $N(\alpha)$ is a prime, then α is irreducible.*

Proof.

1. Let $\beta = \alpha \cdot \gamma$ for some $\gamma \in O_{-n}$. Then, $N(\beta) = N(\alpha \cdot \gamma) = N(\alpha) \cdot N(\beta)$. Therefore, $N(\alpha) | N(\beta)$.
2. If α is a unit, then since only units are $\mathbf{Z}$ are ± 1, $N(\alpha) | \pm 1$. Therefore $|N(\alpha)| = 1$ and for $n > 0$, $N(\alpha)$ is always 1.
3. In $\mathbf{Z}$, primes can only be factorized into itself and it's associate. Hence if $N(\alpha)$ is a prime, then by 2.1.6 α is irreducible.

□

Corollary 2.1.1. *For $n = 1$, the units are $\{\pm 1, \pm i\}$ and for $n = 3$, the units are $\{\pm 1, \pm \omega, \pm \omega^2\}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$. For the rest of the n, the units will be ± 1.*

Proof. For O_{-1}, we have $a^2 + b^2 = 1$. Here, only possibilities for $a^2, b^2 \in \mathbf{Z}$ are $\{\pm 1, \pm i\}$. □

2.2 Irreducibles in $\mathbf{Z}[\sqrt{-5}]$

As we stated and proved in 2.1.1(3), if $N(\alpha)$ is prime in $\mathbf{Z}$ then α is irreducible in $\mathbf{Z}[\sqrt{-n}]$. Therefore, it is an important step to find out which norms that are primes in $\mathbf{Z}$ are not possible in $\mathbf{Z}[\sqrt{-5}]$, so that the elements corresponding those norms are irreducible.

Definition 2.2.1. Two elements $\alpha, \beta \in \mathbf{Z}[\sqrt{-n}]$ are called *associates* if $N(\frac{\alpha}{\beta}) = 1$.

In this case, associates in $\mathbf{Z}[\sqrt{-5}]$ will have the ratio ± 1. Let us give some examples to demonstrate the irreducible elements:

Example 2.2.1 (Irreducibles Corresponding to Norms)**.**

$$\begin{aligned} N(\alpha) = 4 &\longrightarrow \alpha = 2 \\ N(\alpha) = 5 &\longrightarrow \alpha = \sqrt{-5} \\ N(\alpha) = 29 &\longrightarrow \alpha = 3 \pm 2\sqrt{-5} \end{aligned}$$

Finding out irreducibles elements in $\mathbf{Z}[\sqrt{-n}]$ for $n > 0$ is not that challenging. For $\mathbf{Z}[\sqrt{-5}]$, take $3 + \sqrt{-5}$. $N(3 + \sqrt{-5}) = 14 = 2 \cdot 7$. Obviously, there is no $a, b \in \mathbf{Z}$ such that $(a + \sqrt{-5}b) \cdot (a - b\sqrt{-5}) = a^2 + 5b^2 \neq 2, 7$. Let us find which other primes does not satisfy $a^2 + 5b^2$.

Let $p|(a^2 + 5b^2)$ where p is prime in $\mathbf{Z}$. Then,

$$\begin{aligned} a^2 + 5b^2 &\equiv 0 \pmod{p} \\ a^2 &\equiv -5b^2 \pmod{p}. \end{aligned}$$

So, we obtain

$$\left(\frac{a}{b}\right)^2 \equiv -5 \pmod{p}.$$

Let us continue our examination by using quadratic reciprocity.

$$\left(\frac{-5}{p}\right) = 1 \Rightarrow \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right) = 1 \Rightarrow \left(\frac{-1}{p}\right) \cdot \left(\frac{p}{5}\right) = 1.$$

If $p \equiv 1 \pmod 4$, then

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = 1.$$

Since only squares in modulo 5 are 1,4 and since 4 is not possible because of $p \equiv 1 \pmod 4$, we have $p \equiv 1, 9 \pmod{20}$.

If $p \equiv 3 \pmod 4$, then

$$\left(\frac{-1}{p}\right) \cdot \left(\frac{p}{5}\right) = -\left(\frac{p}{5}\right) = 1 \Rightarrow \left(\frac{p}{5}\right) = -1.$$

This is possible only if $p \equiv 2, 3 \pmod 5$, but again because of $p \equiv 3 \pmod 4$, we have $p \equiv 3, 7 \pmod{20}$.

This gives us if $p|(a^2 + 5b^2)$, then $p \equiv 1, 3, 7, 9 \pmod{20}$. So, if norm is $p \equiv 11, 13, 17, 19 \pmod{20}$, then the element is irreducible.

2.3 Ideals

We have been discussing what kind of an algebraic number ring $\mathbf{Z}[\sqrt{-5}]$ is. There are some elements in this ring which have prime norms and this disables $\mathbf{Z}[\sqrt{-5}]$ to be a unique factorization domain. For example,

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

So, 6 can be factorized in two different ways since all of the factors are irreducible. What about the divisors of these irreducible elements? Norms of these elements are $4, 9, 6, 6$ respectively. Take 2 and $1 + \sqrt{-5}$. Norms are 4 and 6. Their greatest common divisor is 2. By 2.1.6 we know that if $\alpha | \beta$ then $N(\alpha)|N(\beta)$. So, this doesn't directly apply that there exists an element $N(\alpha) = 2$ such that α divides both of the irreducibles. Also, obviously there exists no $a, b \in \mathbf{Z}$ such that $a^2 + 5b^2 = 2$ is satisfied. Here, we define a new consept which solves the problem.

Definition 2.3.1. An *ideal* I of O_{-n} is a subset of O_{-n} such that:

1. if $\alpha, \beta \in I$, then $\alpha + \beta \in I$;
2. if $\alpha \in O_{-n}$ and $\beta \in I$, then $\alpha \cdot \beta \in I$;
3. there exists $\alpha \neq 0 \in I$.

So an ideal is closed and addition and multiplication, in fact being closed under addition is applied for not only for the elements in the ideal but also for all the elements of the ring of algebraic integers.

Definition 2.3.2. An ideal I is said to be *principal* if there exists a single element $\alpha \in I$ such that $\alpha \cdot R = I$ for the ring R.

In this case, let's take $(2, 1 + \sqrt{5})$. We know that there is no element in $\mathbf{Z}[\sqrt{-5}]$ that divides both of them. Let

$$2(a + b\sqrt{-5}) + (1 + \sqrt{-5})(c + d\sqrt{-5}) = (2a + c - 5d) + (2b + c + d)\sqrt{-5}$$

be the form of elements which are generated by $(2, 1 + \sqrt{5})$. Here we observe that there is a connection between $m = 2a + c - 5d$ and $n = 2b + c + d$. The set of elements can be written as

$$\{m + n\sqrt{-5} \mid m \equiv n \pmod 2\}.$$

It's obvious that the elements are closed under addition and multiplication, also for $m_1 + n_1\sqrt{-5}$,

$$(m + n\sqrt{-5})(m_1 + n_1\sqrt{-5}) = mm_1 - 5nn_1 + (mn_1 + m_1n)\sqrt{-5}$$
$$mm_1 - 5nn_1 \equiv mn_1 + m_1n \pmod 2.$$

Therefore $(2, 1 + \sqrt{5})$ is an ideal of $\mathbf{Z}[\sqrt{-5}]$.

Example 2.3.1. Let's consider the set generated by $(2, \sqrt{-5}) = I$. $N(2) = 4$, $N(\sqrt{-5}) = 5$, so they are coprime. Also,

$$2 \cdot 2 + \sqrt{-5} \cdot \sqrt{-5} = 1 \in I.$$

So $1 \cdot \mathbf{Z}[\sqrt{-5}] = I$. The ideal is principal by 2.3.2.

Let go through a more complex example for principal ideals.

Example 2.3.2. Let $(29, 13 - \sqrt{-5}) = I_1$ be an ideal of $\mathbf{Z}[\sqrt{-5}]$ and $(3 + 2\sqrt{-5}) = I_2$ be a principal ideal where $I_1 = I_2$. First let us show $I_1 \subset I_2$.

$$\begin{aligned} 29 &= (3 + 2\sqrt{-5}) \cdot (3 - 2\sqrt{-5}) \\ 13 - \sqrt{-5} &= (3 + 2\sqrt{-5}) \cdot (1 - \sqrt{-5}). \end{aligned}$$

Next, let's show $I_2 \subset I_1$.

$$3 + 2\sqrt{-5} = 1 \cdot 29 - 2 \cdot (13 - \sqrt{-5}).$$

So $I_1 = I_2$.

Lemma 2.3.1. *Let I, J be ideals of O_{-n}. Then $I \cdot J \subset I, J$.*

This result is obvious if both of the ideals are principal. Assume that $I = (\alpha)$ and $J = (\beta)$. Then $I \cdot J = (\alpha) \cdot (\beta) = (\alpha \cdot \beta)$. If they are not principal, then let us look the next example:

Example 2.3.3. Consider the ideals

$$\begin{aligned} I_2 &= (2, 1 + \sqrt{-5}) \\ I_2' &= (2, 1 - \sqrt{-5}) \\ I_3 &= (3, 1 + \sqrt{-5}) \\ I_3' &= (3, 1 - \sqrt{-5}). \end{aligned}$$

Their multiples can be computed by multiplying their generators with each other.

$$I_2 \cdot I_2' = (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6) = (2)$$

since minimum element can be written by generators is 2 and each of the generators can be divided by 2. (Also, 2 is in the intersection of the generators.) Similarly,

$$\begin{aligned} I_3 \cdot I_3' &= (3) \\ I_2 \cdot I_3 &= (1 + \sqrt{-5}) \\ I_2' \cdot I_3' &= (1 - \sqrt{-5}). \end{aligned}$$

When we look at the generators of the each of multiples, we observe that they are quite similar with the equation

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

which corresponds to

$$(I_2 \cdot I_2') \cdot (I_3 \cdot I_3') = (I_2 \cdot I_3) \cdot (I_2' \cdot I_3').$$

This example shows us factorization of the elements can be reflected to ideals by rearranging their generators.

2.4 Unique Factorization of Ideals

We've seen that in non-UFD number rings, we can overcome the unique factorization problem by working with the ideals. But this is also restricted to some conditions of our number ring we are working with. To be able to use unique factorization of ideals, our number ring must be a Dedekind domain. To be able to introduce what a Dedekind domain is, we must give some definitions beforehand.

Definition 2.4.1. A Dedekind domain is an integral domain R such that

1. Every ideal is finitely generated.
2. Every nonzero prime ideal is a maximal ideal.
3. R is integrally closed in its field of fractions
$$K = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}.$$

2.5 Exercises

1. Verify that $\mathbf{Q}(\sqrt{-n})$ is a field.

Solution:
Let $a + b\sqrt{-n}, c + d\sqrt{-n} \in \mathbf{Q}\sqrt{-n}$ for $a, b, c, d \in \mathbf{Q}$. Obviously $(a + b\sqrt{-n}) + (c+d\sqrt{-n}) = (a+c)+(b+d)\sqrt{-n}$ and $(a+b\sqrt{-n})\cdot(c+d\sqrt{-n}) = (ac-nbd) + (ad + bc)\sqrt{-n}$ are in $\mathbf{Q}(\sqrt{-n})$, it is closed under addition and multiplication.

Let $(a + b\sqrt{-n}) \cdot (c + d\sqrt{-n}) = (a + b\sqrt{-n})$. Then

$$\begin{aligned}(a + b\sqrt{-n}) = (ac - nbd) + (ad + bc)\sqrt{-n} &\iff a = ac - nbd \ \ \& \ \ b = ad + bc \\ &\iff a(1 - c) = -nbd \ \ \& \ \ b(1 - c) = ad.\end{aligned}$$

Here, we find $d = 0$ and $c = 1$. So, $\mathbf{Q}\sqrt{-n}$ has an identity element 1. Finally, if $(a + b\sqrt{-n}) \cdot (c + d\sqrt{-n}) = 1$, then

$$c + d\sqrt{-n} = \frac{1}{a + b\sqrt{-n}} \iff c = \frac{a}{a^2 + nb^2} \ \ \& \ \ d = \frac{-b}{a^2 + nb^2}.$$

Since $\frac{a}{a^2+nb^2}, \frac{-b}{a^2+nb^2} \in \mathbf{Q}(\sqrt{-n})$ each non-zero element have inverses in $\mathbf{Q}(\sqrt{-n})$. Hence it is a field. (Associativity and distributivity are quite obvious.)

2. If $a, b \in \mathbf{Q}$ and $b \neq 0$, verify that the polynomial $x^2 - 2ax + (a^2 + nb^2)$ is the unique monic quadratic polynomial with rational coefficients having $a + b\sqrt{-n}$ as a root.

Solution:
Remember that the characteristic polynomial of an algebraic integer $\alpha = a + b\sqrt{-n}$ is $x^2 - tr(\alpha) + N(\alpha)$ where $tr(\alpha) = 2a$ and $N(\alpha) = a^2 + nb^2$. Therefore

there is no other monic polynomial satisfying these conditions because of $tr(\alpha)$, $N(\alpha)$ is unique for α and characteristic polynomial is minimal, so it is unique.

3. Verify that $a+b\sqrt{-n}$ with $a, b \in \mathbf{Q}$ has characteristic polynomial with integer coefficients if and only if $a, b \in \mathbf{Z}$ or $n \equiv 3 \pmod 4$, $2a, 2b \in \mathbf{Z}$ and $2a \equiv 2b \pmod 2$.

Solution:
($\Leftarrow$): This part is easy since if $a, b \in \mathbf{Z}$, then obviously the characteristic polynomial has the form $x^2 - 2ax + (a^2 + nb^2)$. If $n \equiv 3$, then $tr(\alpha) = 2a \in \mathbf{Z}$ and $N(\alpha) = a^2 + nb^2 \in \mathbf{Z}$ since if $a = e/2$, $b = f/2$ for odd e, f $e^2, f^2 \equiv 1 (\text{mod } 4)$. Hence

$$e^2 + nf^2 \equiv 0 \pmod 4 \Rightarrow a^2 + nb^2 = \frac{e^2 + nf^2}{4} \in \mathbf{Z}.$$

($\Rightarrow$):

Chapter 3

Ideals and Lattices

The name of this chapter is saying quite a lot about what we will do next. When we consider all the things we did in the past two chapters it starts two feel somehow natural to merge the basis of an ideal and basis of lattices up. In fact, when we are talking about about lattices with finite basis which are of the form $(m, a + b\sqrt{-n})$, there can be observed a huge similarity with the basis of lattices. In this chapter, our intention is to prove that and find out what the properties are.

3.1 The Ideal Class Group

Definition 3.1.1. Two ideals I, J are said to be *similar*, written $I \sim J$, if there are $\alpha, \beta \in O_{-n}$ such that $(\alpha) \cdot I = (\beta) \cdot J$. It is obviously an equivalence relation.

Definition 3.1.2. An equivalence class for similarity is called an *ideal class*; we write the ideal class of an ideal I as C_I. The *ideal class group* $Cl(-n)$ of O_{-n} is the set of all ideal classes in O_{-n}.

First of all, observe that if $I = O_{-n}$, then the class group will consist all of the principal ideals since

$$(1) \cdot (\alpha) = (\alpha) \cdot O_{-n},$$

where (α) is the principal ideal in O_{-n}. Also, any ideal similar to O_{-n} is principal since if $(\alpha), (\beta)$ are principal ideals, we have

$$(\alpha) \cdot I = (\beta) \cdot O_{-n} = (\beta) \implies I = (\beta/\alpha)$$

and since I is an ideal in O_{-n} β must divide α, hence it is principal. So, we've shown that all principal ideals lies in the class $C_{O_{-n}}$.

As the meaning comes from the name, there exists a group structure (under multiplication) in the ideal class groups. Let's check that it actually satisfies the group properties.

Lemma 3.1.1. *Let I, I', J, J' be ideals of O_{-n} such that $I \sim J$ and $I' \sim J'$. Then $I \cdot I' \sim J \cdot J'$.*

Proof. Let $\alpha, \alpha', \beta, \beta' \in O_{-n}$ and

$$(\alpha) \cdot I = (\beta) \cdot J$$
$$(\alpha') \cdot I' = (\beta') \cdot J'.$$

Then we can multiply both sides with each other and obtain

$$(\alpha\alpha') \cdot (I \cdot I') = (\beta\beta') \cdot (J \cdot J').$$

Since $(\alpha\alpha'), (\beta\beta')$ are obviously principal, we conclude that $I \cdot I' \sim J \cdot J'$. □

By using the Lemma above, we can observe

$$C_I \cdot C_J = C_{IJ},$$

and since similar ideal will exist in the same ideal class, the choice of ideals does not matter.

Proposition 3.1.1. *$Cl(-n)$ is an abelian group with identity element the class C_1 of principal ideals.*

Proof. Let C, C' be two ideals classes in $Cl(-n)$. Then

$$C \cdot C' = C_I \cdot C_J = C_{IJ} = C_{JI} = C_J \cdot C_I = C' \cdot C$$

proves the commutativity and associativity can be proved in the manner too. Also for any $C \in Cl(-n)$,

$$C \cdot C_1 = C_I \cdot C_{O_{-n}} = C_{I \cdot O_{-n}} = C_I = C$$

proves C_1 is the identity element of $Cl(-n)$. Finally, to show there exists multiplicative inverses for each element let us set

$$C^{-1} = \{\overline{I} : I \in C\}$$

where $\overline{I}$ is the conjugate ideal of I. Then

$$C \cdot C^{-1} = C_I \cdot C_{\overline{I}} = C_{I \cdot \overline{I}} = C_1$$

proves the inverses. □

3.2 Ideals as Complex Lattices

Let

$$\varpi_{-n} = \begin{cases} \sqrt{-n} & n \equiv 1, 2 \pmod 4 \\ \frac{1+\sqrt{-n}}{2} & n \equiv 3 \pmod 4). \end{cases}$$

Lemma 3.2.1. *Let I be an ideal of O_{-n}. Regarding I as a subset of the complex numbers, it is a complex lattice with CM by $\overline{\omega}_{-n}$. If m is the least positive integer in I and $a+b\sqrt{-n}$ is an element of I with minimal positive coefficient of $\sqrt{-n}$, then $m, a+b\sqrt{-n}$ is a lattice basis of I.*

Proof. We will show that

$$I = \{mx + (a+b\sqrt{-n})y : x, y \in \mathbf{Z}\}$$

is a lattice for m and $a+b\sqrt{-n}$ defined as in the Lemma above. Since any linear combination of m and $a+b\sqrt{-n}$ will be in I, if we can show an arbitrary $c+d\sqrt{-n}$ will be in I, we are done.

Choose y such that $0 \leq d - by < b$.

$$(c+d\sqrt{-n}) - y(a+b\sqrt{-n}) = (c-ay) + (d-by)\sqrt{-n},$$

is an element in I with the positive coefficient of $\sqrt{-n}$, therefore by our first setup we get $by = d$. Also,

$$c - ay = (c+d\sqrt{-n}) - y(a+b\sqrt{-n}) \in I$$

is an integer and hence must be divisible by m. So, there exists $x \in \mathbf{Z}$ such that $c - ay = mx$, and hence

$$c + d\sqrt{-n} = mx + (a+b\sqrt{-n})y.$$

Since I is an ideal of O_{-n}, it has a CM by $\overline{\omega}_{-n}$. □

Lemma 3.2.2. *Two ideals I, J of O_{-n} are similar if and only if they are homothetic lattices. In particular, I, J are similar if and only if $j(I) = j(J)$ with $j(\cdot)$ the j-invariant of the ideal regarded as a lattice.*

Proof. ($\Longrightarrow$) : Let I and J be similar lattices. Then there exist nonzero $\alpha, \beta \in O_{-n}$ such that

$$(\alpha) \cdot I = (\beta) \cdot J \iff I = (\beta/\alpha) \cdot J.$$

So, I, J are homothetic.

($\Longleftarrow$) : Let I, J be homothetic as lattices. Then there exists $\gamma \in \mathbf{C}^{\times}$ such that $I = \gamma \cdot J$. Fix $j \in J$, then clearly $\gamma \cdot j \in I$, nad

$$\gamma = \frac{\gamma \cdot j}{j} \in \mathbf{Q}(\sqrt{-n}).$$

Let $m \in \mathbf{Z}$ be a nonzero integer,

$$(m) \cdot I = (m \cdot \gamma) \cdot J$$

so $I \sim J$ lattices. □

Lemma 3.2.3. *Let $\frac{a+\sqrt{-n}}{b}$ be the j-invariant of a lattice with CM by $\overline{\omega}_{-n}$. Then $(b, a+\sqrt{-n})$ is an ideal of O_{-n} which has j-invariant $\frac{a+\sqrt{-n}}{b}$ when regarded as a complex lattice.*

Corollary 3.2.1. *Let n be a squarefree positive integer. The map $Cl(-n) \to Cl'(-n)$ sending an ideal class C to $j(I)$ for any $I \in C$ is a bijection.*

3.3 Example: $n = 14$

From Chapter 1, we know the elements of the class group of -14 will be

$$Cl(-n) = \left\{ \sqrt{-14}, \frac{\sqrt{-14}}{2}, \frac{-1+\sqrt{-14}}{3}, \frac{1+\sqrt{-14}}{3} \right\}.$$

Then, we find j-invariants are

$$\begin{aligned} j(O_{-14}) &= \sqrt{-14} \\ j(2, \sqrt{-14}) &= \frac{\sqrt{-14}}{2} \\ j(3, 1-\sqrt{-14}) &= \frac{1-\sqrt{-14}}{3} \\ j(3, 1+\sqrt{-14}) &= \frac{1+\sqrt{-14}}{3}. \end{aligned}$$

So we have,

$$\begin{aligned} C_1 &= C_{O_{-14}} \\ C_2 &= C_{(2,\sqrt{-14})} \\ C_3 &= C_{(3,1-\sqrt{-14})} \\ C_3' &= C_{(3,1+\sqrt{-14})}. \end{aligned}$$

One can easily check

$$C_2^2 = C_1 \quad C_3^4 = C_1$$
$$(C_3')^4 = C_1,$$

and all the other elements will be mapped to each other uniquely by the Corollary above. Hence, we observe that $Cl(-14) \cong \mathbf{Z}/4\mathbf{Z}$.

Chapter 4

Computing The Class Number

4.1 The Riemann Zeta Function

Definition 4.1.1. Let

$$a_1, a_2, a_3, \ldots$$

be an infinite sequence of real numbers. Then

$$f(x) := \sum_{m=1}^{\infty} a_m x^m$$

called the *generating function.*

Definition 4.1.2. A (real) *Dirichlet series* is a function of the form

$$f(s) := \sum_{m=1}^{\infty} a_m x^{-s}$$

for real numbers $a_1, a_2, \ldots$.

The version we will use to compute class number formula that will be derived from the Dirichlet series is called *Riemann Zeta Function*, which is of the form

$$\zeta(s) := \sum_{m=1}^{\infty} m^{-s}$$

obtained by setting $a_m = 1$ for all m.

4.2 Euler Product

After setting $a_m = 1$ for all m, we can work on the summation formula and turn it into products which is easier to work with.

Let p be any prime and

$$(1-p^{-s})^{-1} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \dots$$

from the formula $(1+x)^{-1} = 1 + x + x^2 + x^3 + \dots$ when $|x| < 1$. Now take the Riemann zeta function. Observe can it can be factorized into its primes by using the Euler product as defined above, since sum of x^{-s} will include product of all of the primes.

Proposition 4.2.1. *For $s > 1$, we have*

$$\zeta(s) = \prod_p (1-p^{-s})^{-1}$$

where the product is over all prime numbers p.

This proposition can be extended for some other series with coefficients other than 1, regarding whether they are multiplicative or totally multiplicative.

Proposition 4.2.2. *Let $a_1, a_2, \dots$ be a multiplicative sequence such that there is a constant $c > 0$ with $\sum_{m=1}^{M} |a_m| \leq cM$ for all M. Then*

$$\sum_{m=1}^{\infty} a_m m^{-s} = \prod_p \Big(\sum_{j=0}^{\infty} a_{p^j} p^{-js} \Big)$$

for $s > 1$. If also $a_1, a_2, \dots$ is completely multiplicative and $|a_p| \leq p$ for all primes p, then in fact

$$\sum_{m=1}^{\infty} a_m m^{-s} = \prod_p (1 - a_p p^{-s})^{-1}$$

for all $s > 1$.

4.3 L-functions

Let $f(x)$ be the characteristic polynomial for $\overline{\omega}_{-n}$, and therefore of the form

$$f(x) = \begin{cases} x^2 + n & n \equiv 1, 2 \pmod 4 \\ x^2 - x + \frac{1+n}{4} & n \equiv 3 \pmod 4. \end{cases}$$

Definition 4.3.1. For a prime p, the *extended Legendre symbol* $\left(\frac{-n}{p}\right)$ is one less then the number of roots of $f(x)$ in $\mathbf{F}_p$. Then, it agrees with the usual

Legendre symbol for odd p

$$\left(\frac{-n}{p}\right) = \begin{cases} 1 \quad n \equiv 7 \pmod 8 \\ -1 \quad n \equiv 3 \pmod 8 \\ 0 \quad n \equiv 1,2 \pmod 4. \end{cases}$$

Also, for $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ it satisfies

$$\left(\frac{-n}{p}\right) = \left(\frac{-n}{p_1}\right)^{e_1} \left(\frac{-n}{p_2}\right)^{e_2} \dots \left(\frac{-n}{p_r}\right)^{e_r}.$$

Now, let's give the L-function.

Definition 4.3.2. The L-function $L_{-n}(s)$ is defined as

$$L_{-n}(s) := \sum_{m=1}^{\infty} \left(\frac{-n}{m}\right) m^{-s}.$$

Proposition 4.3.1. *$L_{-n}(s)$ converges to a continuous function for $s > 0$. For $s > 1$ there is a product expansion*

$$L_{-n}(s) = \prod_p \left(1 - \left(\frac{-n}{p}\right) p^{-s}\right)^{-1}.$$

4.4 The Dedekind Zeta Function and Class Number Formula

Let a_m denote the number of ideals of O_{-n} of norm m for some $m \geq 1$. Then if m is a prime p, we have

$$a_p = \begin{cases} 2 & \left(\frac{-n}{p}\right) = 1 \\ 1 & \left(\frac{-n}{p}\right) = 0 \\ 0 & \left(\frac{-n}{p}\right) = -1. \end{cases}$$

Lemma 4.4.1. *1. The sequence $a_1, a_2, \dots$ is multiplicative.*

2. For a prime p

$$\sum_{j=0}^{\infty} = \begin{cases} (1 - p^{-s})^{-2} & \left(\frac{-n}{p}\right) = 1 \\ (1 - p^{-s})^{-1} & \left(\frac{-n}{p}\right) = 0 \\ (1 - p^{-2s})^{-1} & \left(\frac{-n}{p}\right) = -1 \end{cases}$$

for $s > 1$.

Now, we can define the Dedekind Zeta Function and derive class number formula from it.

Definition 4.4.1. The *Dedekind zeta function* of O_{-n} is defined as the Dirichlet series

$$\zeta_{-n}(s) = \sum_{m=1}^{\infty} a_m m^{-s}.$$

By using the Lemma above, we can give the following proposition for the Dedekind zeta function.

Proposition 4.4.1. *The Dedekind zeta function converges for $s > 1$ and has the Euler product*

$$\zeta_{-n}(s) = \prod_{p,(\frac{-n}{p})=1} (1-p^{-s})^{-2} \cdot \prod_{p,(\frac{-n}{p})=0} (1-p^{-s})^{-1} \cdot \prod_{p,(\frac{-n}{p})=-1} (1-p^{-2s})^{-1}$$

for $s > 1$.

One can observe that the Euler product on the Dedekind zeta function is nothing but factorizing Riemann zeta function by respecting the L-function given in this chapter. Hence, the following proposition is a natural result.

Proposition 4.4.2. *For $s > 1$,*

$$\zeta_{-n}(s) = \zeta(s) \cdot L_{-n}(s).$$

Proof.

$$\begin{aligned}
\zeta_{-n}(s) &= \prod_{p,(\frac{-n}{p})=1} (1-p^{-s})^{-2} \cdot \prod_{p,(\frac{-n}{p})=0} (1-p^{-s})^{-1} \cdot \prod_{p,(\frac{-n}{p})=-1} (1-p^{-2s})^{-1} \\
&= \prod_{p,(\frac{-n}{p})=1} (1-p^{-s})^{-2} \cdot \prod_{p,(\frac{-n}{p})=0} (1-p^{-s})^{-1} \cdot \prod_{p,(\frac{-n}{p})=-1} (1-p^{-s})^{-1}(1+p^{-s})^{-1} \\
&= \prod_{p} (1-p^{-s})^{-1} \cdot \prod_{p} \Big(1 - \Big(\frac{-n}{p}\Big) p^{-s}\Big)^{-1} \\
&= \zeta(s) \cdot L_{-s}(s).
\end{aligned}$$

□

Corollary 4.4.1. *Let n be a sequence positive integer and let*

$$\omega_{-n} = \begin{cases} 2 & n \neq 1,3 \\ 4 & n = 1 \\ 6 & n = 3. \end{cases}$$

Let $h(-n)$ denote the class number pf O_{-n}. If $n \equiv 1, 2 \pmod 4$, then

$$L_{-n}(1) = \frac{h(-n)\pi}{\sqrt{n}\omega_{-n}}.$$

If $n \equiv 3 \pmod 4$, then

$$L_{-n}(1) = \frac{2h(-n)\pi}{\sqrt{n}\omega_{-n}}.$$

So, for the value of L-function at 1, we can compute the class number analitically.

Corollary 4.4.2. *For any squarefree positive integer n we have $L_{-n}(1) > 0$.*