THE CLASS NUMBER FORMULA

SHILPA KESAVAN

1. Algebra Background

Because of the extensive background required to prove the class number formula, we will state several theorems without proof or only with a proof outline.

Definition 1.1. An *algebraic integer* is a complex number that is the root of some monic polynomial with integer coefficients. We denote the set of algebraic integers in a field F as $\mathcal{O}_F$, where F is an algebraic extension of $\mathbb{Q}$.

Definition 1.2. The *discriminant* of $\mathbb{Q}(\sqrt{-d})$ is

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

Theorem 1.3. *$\mathcal{O}_F$ is a ring.*

We will show a special case of the class number formula on the ring of algebraic integers in $\mathbb{Q}(\sqrt{-d})$ with d a positive integer, which we will denote $\mathcal{O}$. We can let d be square-free since $\mathbb{Q}(k\sqrt{-d})$ is the same field as $\mathbb{Q}(\sqrt{-d})$ for any integer k. Notice that when $d \equiv 1, 2 \pmod 4$ then

$$\mathcal{O} = \mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} : a, b \in \mathbb{Z}\}$$

and when $d \equiv 3 \pmod 4$,

$$\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right] = \left\{a + b\frac{1+\sqrt{-d}}{2} : a, b \in \mathbb{Z}\right\}.$$

Definition 1.4. Let R be a commutative ring. An *ideal* of R is an additive subgroup I of R with the property that $nm \in I$ whenever $n \in I$ and $m \in R$.

Definition 1.5. An ideal is *principal* and denoted (n) if it is generated by a single element n of R. A principal ideal is *non-zero* if it is not (0).

Definition 1.6. An ideal is *proper* if it is not all of R. A proper ideal is *prime* if whenever $nm \in I$ for $n, m \in R$, we have that at least one of n, m are in I.

Definition 1.7. For ideals I, J, we write $I \cdot J$ to be the ideal generated by the set $\{nm : n \in I, m \in J\}$.

Definition 1.8. For an ideal I of $\mathcal{O}$, we write the norm of I

$$N(I) := [\mathcal{O} : I].$$

Theorem 1.9. *Every nonzero proper ideal in $\mathcal{O}$ can be uniquely factored into a product of nonzero prime ideals in $\mathcal{O}$.*

Corollary 1.10. *For non-zero ideals I, J, we have that $N(I \cdot J) = N(I)N(J)$.*

Proof. As a rough sketch: When I, J are coprime then define the isomorphism from $\mathcal{O}/(I \cdot J) \to \mathcal{O}/I \times \mathcal{O}/J$ taking $n \pmod{I \cdot J}$ to $(n \pmod{I}, n \pmod{J})$ for $n \in \mathcal{O}$. Thus N is multiplicative. To show it is completely multiplicative, define an isomorphism from $\mathcal{O}/p$ to p^j/p^{j+1} for prime p and arbitrary j. □

Theorem 1.11. *Let p be prime in $\mathbb{Q}(\sqrt{-d})$.*

- *If D is a nonzero quadratic residue modulo p, then (p) is the product of two distinct prime ideals P_1, P_2 of norm p.*
- *If p divides D then (p) is $P \cdot P$ for some prime ideal P of norm p.*
- *If D is a quadratic non-residue modulo p then (p) is a prime ideal of norm p.*

2. Kronecker Symbol

Before we move to the statement and proof of the class number formula, we can expand on the algebra above to help us connect our final result to analytic number theory.

Definition 2.1. The Kronecker symbol is a completely multiplicative function such that for each prime p,

$$\chi(p) := \begin{cases} 0 & p \mid D \\ 1 & D \text{ is a nonzero quadratic residue modulo } p \\ -1 & D \text{ is a nonresidue modulo } p \end{cases}.$$

In fact, χ is a Dirichlet character with conductor D.

Theorem 2.2. *For any natural number n, the number of ideals of norm n is equal to $(\mathbb{1} * \chi)(n)$.*

Proof. Since χ is completely multiplicative, $1 * \chi$ is multiplicative. By unique factorization of ideals, the number of ideals of norm n (which we will denote $I(n)$) is also multiplicative. Then, it remains to show that for prime p and positive integer e,

$$\chi(p) + \chi(p)^2 + \ldots + \chi(p)^e = I(p^e).$$

It remains to go case-by-case on whether $D = d, 4d$ and $\chi(p) = 0, 1, -1$, which we will not do. □

Definition 2.3.

$$\zeta_{\mathcal{O}}(s) := \sum_{I} \frac{1}{N(I)^s}$$

Corollary 2.4.

$$\zeta_{\mathcal{O}}(s) = \zeta(s)L(s,\chi).$$

Proof. We know

$$\begin{aligned}\zeta_{\mathcal{O}}(s) &= \sum_{I} \frac{1}{N(I)^s} \\ &= \sum_{n} \frac{(\mathbb{1} * \chi)(n)}{n^s} \\ &= \sum_{n} \frac{\mathbb{1}(n)}{n^s} \sum_{n} \frac{\chi(n)}{n^s} \\ &= \zeta(s)L(s,\chi).\end{aligned}$$

□

3. The Ideal Class Group and Quadratic Forms

The set of ideals of $\mathcal{O}$ form a monoid, not a group. However, we can form a group by defining equivalence classes on them.

Definition 3.1. We say $I \sim J$ if there exists some $n \in \mathbb{Q}(\sqrt{-d})$ such that $I \cdot (n) = J$.

These equivalence classes of ideals in $\mathcal{O}$ form a group, which we call the ideal class group of $\mathcal{O}$. The class number formula essentially computes the size of this group, which we denote $h(D)$. Instead of directly computing the number of equivalence classes of ideals, we will consider equivalence classes on quadratic forms associated with these ideals.

Definition 3.2. For each ideal I of $\mathcal{O}$, we define the quadratic form $Q_I : I \to Z_{\geq 0}$ such that

$$Q_I(n) := n\bar{n}/N(I)$$

where $\bar{n}$ is the complex conjugate of N. We additionally write $Q_I \sim Q_J$ whenever $I \sim J$.

Theorem 3.3. *Suppose n is a natural number, and $Q_1, Q_2, \ldots, Q_{h(D)}$ are representatives of the equivalence classes of positive definite quadratic forms of ideals in $\mathcal{O}$. Then the number of ideals of norm n in $\mathcal{O}$ is equal to the number of representations of n of the form $Q_i(x,y)$ where $i \in \{1,2,\ldots,h\}$ and $x, y \in \mathbb{Z}$ divided by the number ω of units in $Q(\sqrt{-d})$.*

Proof. Suppose $Q_i(x, y) = n$ with i, x, y all chosen as in the theorem. Then Q_i is isomorphic to Q_J for some ideal J, and so $n = Q_J(m)$ for some $m \in J$, implying $N(m) = nN(J)$. Ideals are uniquely factorable and norms are multiplicative, so $(m) = I \cdot J$ for some ideal I of norm n. We will show that this defines an almost-bijection from the representations of n as $Q_i(x, y)$ to the ideals of norm n. In particular, if we change i then we change our ideal J, and if we change x or y, then we change our element m to some m'. We have $(m) = (m')$ precisely when m and m' differ by a unit, so this is an injection if we form equivalence classes on the domain based on whether m and m' differ by a unit. If I is an ideal of norm n, then Lagrange's theorem tells us that $N(I) \in I$, and thus $Q_I(n) = n$. Taking the i that Q_I is represented by in its equivalence class, we have that this is a surjection. □

Corollary 3.4. *The number of ideals I in $\mathcal{O}$ with $N(I) \leq x$ is*

$$\frac{2\pi h(D)}{\omega\sqrt{|D|}}x + O_D(\sqrt{x}).$$

Proof. By Theorem 3.1 we know the number of ideals with norm less than or equal to x is

$$1 + \frac{1}{\omega}\sum_{i=1}^{h(D)} \sum_{Q_i(a,b)\leq x} 1.$$

The inner sum is the number of lattice points in the ellipse $\{(a, b) \in \mathbb{Z}^2 : Q_i(a, b) \leq x\}$, which (as we will not prove, since it is slightly outside our scope) has area $\frac{2\pi x}{\sqrt{|D|}}$. The number of lattice points differs from the area by $O_D(\sqrt{x})$. □

Theorem 3.5 (Dirichlet's Class Number Formula)**.** *As s approaches 1,*

$$(s-1)\zeta_{\mathcal{O}}(s) = \frac{2\pi h(D)}{\omega\sqrt{|D|}} + O_D(1).$$

Proof. This comes from Corollary 3.4, but the rest is mostly beyond our scope and requires complex analysis. We will outline the proof instead. Suppose

$$a_n := (1 * \chi)(n) - \frac{2\pi h(D)}{\omega\sqrt{|D|}}.$$

Then we get that the partial sums of a_n is

$$A_x = \sum_{n\leq x}(1 * \chi)(n) - \frac{2\pi h(D)}{\omega\sqrt{|D|}}x,$$

which as we showed in Corollary 3.4 is bounded by a constant multiple of $\sqrt{x}$. To prove our theorem, we show that the Dirichlet series of the a_n's is equal to $\zeta_{\mathcal{O}}(s) - \frac{2\pi h(D)}{\omega\sqrt{|D|}}\zeta(s)$ and is analytic at $s = 1$. □

Corollary 3.6.

$$h(D) = \frac{\omega\sqrt{|D|}}{2\pi}L(1,\chi)$$

Proof. This follows using Corollary 2.4. □