A BASIC INTRODUCTION TO CLASS GROUPS

KEVIN XU

Abstract. In this paper we introduce the class group, an important structure that measures to what extent the ring of integers in an algebraic field has unique factorization. The paper assumes moderate knowledge of abstract algebra, and a good understanding of algebraic number theory would be beneficial. There are two sections in this paper: the first introduces the class group, while the latter provides several examples of computing the class group using the Minkowski bound. This paper is dedicated to Simon Rubinstein-Salzedo and members of the Euler Circle; without them this paper would not have been possible.

1. The Class Group

Before jumping into class group theory, we must first define several important structures. Recall that a *group* is a set closed by an associative operation which has an identity and inverses. We introduce the idea of a *semigroup* as follows:

Definition 1.1. A *semigroup* is a set that is closed under an associative operation.

Semigroups allow for the inclusion of sets such as the empty set or the integers under multiplication; however, the latter is better referred to as a *monoid*, a semigroup with an identity.

Now recall that a *field* F is a set closed by two operations addition and multiplication such that F is an abelian group under addition and $F\backslash\{0_F\}$ is an abelian group under multiplication, along with distributivity of multiplication over addition. We now introduce the *ring*, a generalized version of a field.

Definition 1.2. A *ring* R is a set closed under addition and multiplication such that R is an abelian group under addition and a semigroup under multiplication, with the added caveat that multiplication distributes over addition.

Examples of rings include the integers, the integers modulo n, and the set of all n by n matrices. The first two are examples of *commutative rings*, or rings that commute over multiplication. In fact, the integers forms an *integral domain*, a ring that stipulates that the product of nonzero elements must be nonzero. Because rings form groups under addition, we can consider their subgroups. One special kind of subgroup is known as an *ideal*.

Definition 1.3. For some commutative ring R, an *ideal* I is an additive subgroup of R such that $rI \subseteq I \quad \forall r \in R$. The *norm* of I is defined as $[R : I]$.

Ideals appear for rings that do not commute under multiplication as well, but are categorized as left or right ideals depending on whether rI or Ir is a subset of I, respectively.

Ideals are commonly expressed using their *generators*. Specifically, the ideal generated by $g_1, \ldots, g_n$ is

$$(g_1, \ldots, g_n) = \{a_1 g_1 + \cdots + a_n g_n \mid a_1, \ldots, a_n \in R\}.$$

We call $(1_R) = R$ the *unit ideal*, and $(0_R) = \{0_R\}$ the *zero ideal*. Lastly, a *principal ideal* is an ideal generated by one element.

Since ideals are groups under addition, it makes sense to figure out how to multiply two ideals $\mathfrak{a}$ and $\mathfrak{b}$ together. An immediate thought is to use $\mathfrak{ab} = \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$, but it turns out that this product is not necessarily closed under addition. Thus, we must include all finite sums of these products as well.

Once we have the product of ideals, we can consider which ideals are divisible by another. Suppose $\mathfrak{a}, \mathfrak{b}$ are ideals where $\mathfrak{a}|\mathfrak{b}$; that is, there exists $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac}$. But since $c\mathfrak{a} \in \mathfrak{a} \quad \forall c \in \mathfrak{c}$ we have $\mathfrak{ac} \subseteq \mathfrak{a}$. Thus if $\mathfrak{a}|\mathfrak{b}$ then $\mathfrak{a}$ contains $\mathfrak{b}$. In fact, we have the following:

Proposition 1.4. *Let R be a commutative ring and $a, b \in R$. Then $a|b$ iff $(a) \mid (b)$.*

Proof. Suppose $a|b$, so $b = ac$ for $c \in R$. Then $(b) = (ac) = (a)(c)$ implies one direction. If $(a) \mid (b)$, then there exists an ideal $\mathfrak{c}$ such that $(b) = (a)\mathfrak{c}$. But we have

$$(b) = (a)\mathfrak{c} = a\mathfrak{c} = \{ac \mid c \in \mathfrak{c}\},$$

so there must be some c such that $b = ac$. □

These notions of containment give rise to the idea of a *prime ideal*.

Definition 1.5. An ideal I is *prime* iff for ideals $\mathfrak{a}, \mathfrak{b}$, whenever $\mathfrak{ab} \subseteq I$, we have $\mathfrak{a} \subseteq I$ or $\mathfrak{b} \subseteq I$.

We can see that the notion of prime numbers follows from this definition. If (n) is prime for some integer n, then there exists no nontrivial ideal (a) that divides it, implying $a \nmid d$.

Definition 1.6. An *algebraic field* is a finite-dimensional field extension of $\mathbb{Q}$.

This means that the extension has finite dimension when considered as a vector space over $\mathbb{Q}$, or that the degree is finite. In other words, all algebraic fields can be represented as $\mathbb{Q}(\alpha)$ for some *primitive element* α. Examples of algebraic fields include $\mathbb{Q}(\sqrt{d})$ for square-free d and $\mathbb{Q}(\zeta_n)$. Next, we show how to obtain an algebraic field from an integral domain through its *field of fractions*.

Definition 1.7. The *field of fractions* of an integral domain K is the field obtained by adding all elements of the form $\frac{a}{b}$, where a, b are nonzero elements of K.

In other words, the field of fractions of K adds the ability to divide by nonzero elements, and thus is the smallest field containing K. We can also "convert" an algebraic field into an integral domain through the *ring of integers*.

Definition 1.8. The *ring of integers* of an algebraic field K is a subset of K containing all elements are roots of some monic polynomial with integral coefficients. It is an example of a *Dedekind domain* and is denoted as $\mathcal{O}_K$.

One can check readily that the ring of integers is an integral domain and also a superset of $\mathbb{Z}$, the ring of integers of $\mathbb{Q}$. For other algebraic fields, however, "integers" include other numbers as well.

Proposition 1.9. *The ring of integers of $\mathbb{Q}(\sqrt{d})$ for a square-free integer d is $\mathbb{Z}(\frac{1+\sqrt{d}}{2})$ if $d \equiv 1 \pmod 4$ and $\mathbb{Z}(\sqrt{d})$ if $d \equiv 2, 3 \pmod 4$.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ and $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_K$ for $a, b \in \mathbb{Q}$. We proceed to take the minimum polynomial, which turns out to be

$$x^2 - ax + \frac{a^2 - b^2 d}{4}.$$

This implies that $a \in \mathbb{Z}$ and $a^2 - b^2 d \equiv 0 \pmod 4$. We can now go through each individual case: $d \equiv 1 \pmod 4$ implies a, b have the same parity, while $d \equiv 2, 3 \pmod 4$ forces a, b to be even (the latter following from squares being $0, 1$ modulo 4). □

We have defined multiplication (and hence closure) for ideals, so forming a group of ideals is the logical next step. This is certainly possible, though we must first define another mathematical object called a *module*.

Definition 1.10. For a ring R, a *$R-$module* M is an additive abelian group composed with an operation $\cdot$ that sends $R \times M \to M$ such that for all $r, s \in R$ and $m, n \in M$, we have

(1) $r \cdot (m + n) = r \cdot m + r \cdot n$
(2) $m \cdot (r + s) = m \cdot r + m \cdot s$
(3) $(rs) \cdot m = r \cdot (s \cdot m)$
(4) $1_R \cdot m = m$.

Definition 1.11. A *$R-$submodule* N of M is a subgroup of M such that $\forall n \in N, r \in R$, we have $n \cdot r \in N$.

A module is essentially a generalization of a vector space, but coefficients come from rings instead of fields. If a module has a basis (generating set), then it is called a *free module*. The size of the basis is called the *rank* of the module. One example of a module is $\mathbb{Z}$ (over itself), with its ideals as its submodules: $n\mathbb{Z}$. With this, we can define the *fractional ideal* in relation to the ring of integers:

Definition 1.12. Let K be an algebraic field. A *fractional ideal* $J \subset K$ is a $\mathcal{O}_K$-submodule such that there exists nonzero $r \in \mathcal{O}_K$ with $rJ \subset \mathcal{O}_K$.

For example, fractional ideals in $\mathbb{Q}$ are $\mathbb{Z}$-submodules of the form $q\mathbb{Z}$ for some $q \in \mathbb{Q}$. Note that if we have $rJ \subset \mathcal{O}_K$, we have $arJ \subset \mathcal{O}_K$ for any $a \in \mathcal{O}_K$. Since all multiples of r work, we can use $\mathrm{N}_{K/\mathbb{Q}}(r)$. Thus J is a fractional ideal if there exists nonzero $r \in \mathbb{Z}$ such that $rJ \subset \mathcal{O}_K$.

Furthermore, a fractional ideal can be expressed in the form $k\mathfrak{a}$, where $k \in K^\times$ and $\mathfrak{a}$ an ideal of $\mathcal{O}_K$. To see this, note that rJ is an $\mathcal{O}_K$ module in $\mathcal{O}_K$, so rJ is an ideal and $\frac{1}{r}(rJ) = J$. If $\mathfrak{a} = \mathcal{O}_K$, then we call J *principal*. When all fractional ideals are principal, we call the integral domain a *principal ideal domain*, or PID for short.

Proposition 1.13. *Every fractional ideal in K is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

See [Conb] for a proof.

Definition 1.14. Two fractional ideals $I, J \subset K$ are said to be *equivalent* if there exists nonzero $a \in K$ such that $I = aJ$.

Equivalence classes of fractional ideals are called *ideal classes*, and they form a group under multiplication here (thought not always for other integral domains). This group is called the *class group*.

Definition 1.15. The *class group* of an algebraic field K, denoted as $\mathrm{Cl}(K)$, is the abelian group formed by the set of all equivalence classes of the fractional ideals of $\mathcal{O}_K$.

The identity of the class group is the class of all principal ideals, and I^{-1} is defined as the fractional ideal such that II^{-1} is principal. The order of the group is called the *class number* of a field.

The class group measures to what extent *unique factorization* fails in the ring of integers of a field. If the class group is trivial, then all fractional ideals are principal, and thus K is a PID.

2. Minkowski Bound

While we have defined the class group for a field, it remains difficult to compute this group and its order. In this section we will discuss one popular way to do this using the *Minkowski bound*.

Definition 2.1. An *embedding* of an algebraic field K is an injective ring homomorphism $\sigma\colon K \to \mathbb{C}$. Such a map is *real* if its image lies in $\mathbb{R}$, and *complex* otherwise.

Let x be a primitive element of K, and f be the minimum polynomial of x over $\mathbb{Q}$. Whether an embedding is real of complex is whether the root of f that x is mapped to lies in $\mathbb{R}$ or not. Furthermore, if we consider f over $\mathbb{R}$, then f splits into factors of degree 1 or 2. Since there are no repeated factors, any factor of degree 1 will give a real root, and any factor of degree 2 will give two complex conjugate roots. Thus, if K has r_1 real and r_2 complex embeddings, then we have $r_1 + 2r_2 = [K : \mathbb{Q}]$. Now we introduce a few key terms in linear algebra:

Definition 2.2. Let K be an algebraic field and $x \in K$. Viewing K as a finite-dimensional vector space in $\mathbb{Q}$, we construct an endomorphism $\phi_x\colon K \to K$ defined on multiplication by x. We define the *trace* and *norm* of x as $\mathrm{Tr}_K(x) = \mathrm{Tr}(\phi_x)$ and $\mathrm{N}_K(x) = \det(\phi_x)$ respectively.

Definition 2.3. For an algebraic field K, let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the basis of $\mathcal{O}_K$, and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the K-embeddings. The *discriminant* of K is given by $\mathrm{Disc}(K) = \det(M)^2$, where M is the matrix given by $M = \{m_{ij} \mid m_{ij} = \sigma_i(\alpha_j)\}$.

This definition can also be extended to the *discriminant* of an ideal, using its basis and embeddings. We state Minkowki's Theorem, which bounds the norm of prime ideals in $\mathrm{Cl}(K)$.

Theorem 2.4 (Minkowski)**.** *Let r_1, r_2 be the number of real and complex embeddings, respectively, in the algebraic field K of degree n. In any ideal class $C \in \mathrm{Cl}(K)$, there exists ideal $I \in C$ such that*

$$\mathrm{N}(I) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\,\mathrm{Disc}(K)|}.$$

This is derived from Minkowski's result that every convex set in $\mathbb{R}^n$ symmetric with respect to the origin with volume greater than 2^n contains a nonzero lattice point. For further explanation, see [Ull08]. Minkowski's Theorem is very useful in determining whether the ring of integers of an algebraic field is a PID. However, it is quite tricky to compute the discriminant of a general algebraic field, so in this paper we will focus on the fields $\mathbb{Q}(\sqrt{d})$ for square-free d.

Proposition 2.5. *In the algebraic field $\mathbb{Q}(\sqrt{d})$, we have*

$$\mathrm{Disc}(K) = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4. \end{cases}$$

Proof. First suppose that $d \equiv 1 \pmod 4$, so $\mathcal{O}_K$ has basis $[1, \frac{1+\sqrt{d}}{2}]$. Then the discriminant is

$$\mathrm{Disc}(K) = \left[\det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right]^2 = d.$$

If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K$ has basis $[1, \sqrt{d}]$, and the discriminant is

$$\mathrm{Disc}(K) = \left[\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}\right]^2 = 4d.$$

□

Note that if $d > 0$ then K has two real and zero complex embeddings, so upon using Minkowski's Theorem, any algebraic field with $|\mathrm{Disc}(K)| < 16$ contains an ideal of norm one in every ideal class, so K has trivial class group. If $d < 0$, then K has zero real and two complex embeddings, so any algebraic field with $|\mathrm{Disc}(K)| < \pi^2$ has trivial class group. These include the algebraic fields

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{13}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}).$$

Now we tackle a slightly harder problem:

Theorem 2.6. *$\mathbb{Q}(\sqrt{17})$ has trivial class group.*

Proof. From Minkowski's Theorem, we know there must exist an ideal in every ideal class with norm 1 or 2. Suppose we have an ideal class with an ideal of norm 2. Though we quickly see that (2) has norm two, it is not a prime ideal: we have

$$(2) = \left(\frac{3+\sqrt{17}}{2}\right)\left(\frac{3-\sqrt{17}}{2}\right).$$

These two factors are the only prime ideals of norm 2, and since they are principal, the ideal class must contain only principal ideals. This implies that $\mathcal{O}_K$ is a PID, and so the class group is trivial. □

And lastly, we investigate a case where the class group is nontrivial.

Theorem 2.7. *The class group of $\mathbb{Q}(\sqrt{-14})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-14})$, so we still have $[K : \mathbb{Q}] = 2$ and 2 complex embeddings. Note that $\mathrm{Disc}(K) = -56$, so applying Minkowki's Theorem we get a bound of $\mathrm{N}(I) \leq 4$. Now we look at how the minimum polynomial $X^2 + 14$ factors in the primes 2 and 3.

Solving the modular equations, we have

$$X^2 + 14 \equiv X^2 \pmod 2$$

$$X^2 + 14 \equiv (X+1)(X-1) \pmod 3,$$

so there must exist prime ideals $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$ with norms $2, 3, 3$ respectively such that $\mathfrak{p}_2^2 = \mathfrak{p}_3\mathfrak{p}_3' = (1)$. Since $\mathfrak{p}_3' = \mathfrak{p}_3^{-1}$, $\mathrm{Cl}(K)$ is generated by $\mathfrak{p}_2, \mathfrak{p}_3$. Now consider the integer $2 + \sqrt{-14}$, which

has norm $18 = 2 \cdot 3^2$. Because $3 \nmid 2 + \sqrt{-14}$, only one of $\mathfrak{p}_3, \mathfrak{p}_3'$ divides $(2 + \sqrt{-14})$; WLOG let it be $\mathfrak{p}_3$. We have

$$(2 + \sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^2 \Longrightarrow \mathfrak{p}_2 = \mathfrak{p}_3^{-2}.$$

Thus $\mathrm{Cl}(K)$ is generated by $\mathfrak{p}_3$. Now we show that $\mathfrak{p}_3$ is nonprincipal. If $\mathfrak{p}_3$ is principal, there exists $a, b \in \mathbb{Z}$ such that

$$\mathrm{N}(\mathfrak{p}_3) = \mathrm{N}(a + b\sqrt{-14}) \Longrightarrow a^2 + 14b^2 = 3.$$

But this is clearly impossible, so $\mathfrak{p}_3$ is nonprincipal and thus has order 4. Because $\mathfrak{p}_3$ generates the class group, we have $\mathrm{Cl}(K) \cong \mathbb{Z}/4\mathbb{Z}$ as desired. □

Finding the class group of an arbitrary quadratic extension is extremely difficult. The *class number problem*, posed by Gauss in 1801, asks for a given n a list of all imaginary quadratic fields of class number n. Though this has been partially resolved, with Watkins finding specifications for quadratic fields of class number up to 100 (see [Wat04]), there is still much to explore about this interesting group.

References

[Cona] Keith Conrad. *Class group calculations*. University of Connecticut, Storrs, CT.

[Conb] Keith Conrad. *Ideal factorization*. University of Connecticut, Storrs, CT.

[Gan18] Tom Gannon. *Introduction to ideal class groups*. American Mathematical Society, 2018.

[Hoq20] Azizul Hoque. *On the exponents of class groups of some families of imaginary quadratic fields*. arXiv.org, 2020.

[Tia14] Yichao Tian. *Lectures on algebraic number theory*. Morningside Center of Mathematics, Beijing, China, 2014.

[Ull08] Brooke Ullery. *Minkowski theory and the class number*. University of Chicago, 2008.

[Wat04] Mark Watkins. *Class numbers of imaginary quadratic fields*. Mathematics of Computation, 2004.