

# ON CALCULATION OF CLASS NUMBERS

Jiantong Liu

October 27, 2022

## ABSTRACT

We discuss the relevant concepts and techniques that are frequently used when calculating the class number of a number field. We also use these facts to calculate a few class numbers.

## 1 DEFINITION

Unless specified otherwise, we denote  $A$  to be a Dedekind domain and  $F$  to be a number field.

**Definition 1.1** (Fractional Ideal). A fractional ideal  $\mathfrak{a}$  of a domain  $R$  is a non-zero  $R$ -submodule of the field of fractions of  $R$ , such that there exists  $d \in R \setminus \{0\}$  with  $d\mathfrak{a} \subseteq R$ .

**Remark 1.2.** Although there may not be a unique factorization of ideals on  $A^1$ , we do have unique factorizations of fractional ideals on  $A$ .

**Definition 1.3** (Ideal Group). The ideal group  $I(A)$  of  $A$  is the group of fractional ideals of  $A$  under multiplication.

**Definition 1.4** (Principal Ideal Group). The principal ideal group  $P(A)$  is the subgroup of  $I(A)$  of principal fractional ideals.

**Definition 1.5** ((Ideal) Class Group). The (ideal) class group  $Cl(A)$  of  $A$  is  $I(A)/P(A)$ .

**Proposition 1.6.** The class group is trivial if and only if  $A$  is a PID.

**Proposition 1.7.**  $A$  is a PID if and only if it is a UFD.

**Definition 1.8** ((Ideal) Class Group). The ideal class group  $Cl_F$  of a number field  $F$  is  $Cl(\mathcal{O}_F)$ , where  $\mathcal{O}_F$  is the ring of integers of  $F$ . In particular,  $Cl_F = I_F/P_F$  if we set  $I_F = I(\mathcal{O}_F)$  and  $P_F = P(\mathcal{O}_F)$ . Therefore, every ideal in  $I(A)$  is mapped to an equivalence class of ideals in  $Cl(A)$ .

**Remark 1.9.** Every ideal in  $A$  can be generated by two elements.

**Definition 1.10** (Class Number). The class number  $h_F$  of a number field  $F$  is the order of  $Cl_F$ .

**Theorem 1.11.**  $Cl_F$  is finite.

---

<sup>1</sup>For example, the ideal  $(6)$  in  $\mathbb{Z}[\sqrt{-5}]$  can be decomposed in two ways:  $(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$ .

## 2 PROPERTIES

### 2.1 NORM AND DISCRIMINANT

**Proposition 2.1.** Let  $L/K$  be a finite field extension and consider element  $\alpha \in L$ . Let  $f \in K[x]$  be the minimal polynomial of  $\alpha$  over  $K$ . Suppose  $f$  factors in the algebraic closure as  $f = \prod_{i=1}^n (x - \alpha_i)$  where  $\alpha_i$ 's are roots of the polynomial in the closure, and  $n$  is the degree of extension  $[K(\alpha) : K]$ . Then the characteristic polynomial  $m_\alpha$  is  $f^{[L:K(\alpha)]}$ , and  $N_{L/K}(\alpha) = \prod_{i=1}^n \alpha_i^{[L:K(\alpha)]}$  and  $Tr_{L/K}(\alpha) = [L : K(\alpha)] \sum_{i=1}^n \alpha_i$ .

**Proposition 2.2.** Let  $d \neq 1$  be a square-free integer. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{d}], & d \equiv 2, 3 \pmod{4} \end{cases}.$$

Therefore, a  $\mathbb{Z}$ -basis of the ring of integers of  $\mathbb{Q}(\sqrt{d})$  is  $\{1, \frac{1+\sqrt{d}}{2}\}$  (if  $m \equiv 1 \pmod{4}$ ) or  $\{1, \sqrt{d}\}$  (if  $m \equiv 2, 3 \pmod{4}$ ).

**Remark 2.3.** Given a quadratic extension  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ , the norm of any element  $a + b\sqrt{d}$  is  $a^2 - b^2d$ .

**Proposition 2.4.** Let  $d \neq 1$  be a square-free integer, then the field discriminant (i.e. the discriminant of an integral basis) of the extension  $\mathbb{Q}(\sqrt{d})$  is

$$\text{disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d, & d \equiv 1 \pmod{4} \\ 4d, & d \equiv 2, 3 \pmod{4} \end{cases}.$$

**Proposition 2.5.** Consider  $K = \mathbb{Q}(\alpha)$  and let  $f \in \mathbb{Q}[x]$  be the minimal polynomial of  $\alpha$  of degree  $n$ . Then

- Let  $D$  be the discriminant of the basis  $\{1, \alpha, \dots, \alpha^{n-1}\}$  over  $\mathbb{Q}$ , then the discriminant is identical to the discriminant of  $f$ , and therefore  $D = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))$ .<sup>2</sup>
- The field norm  $N_{K/\mathbb{Q}}$  is multiplicative.
- $N_{K/\mathbb{Q}}(b) = b^n$  for  $b \in \mathbb{Q}$ .
- $N_{K/\mathbb{Q}}(\alpha)$  is  $(-1)^n$  times the constant term of  $f$ .

**Proposition 2.6.** Suppose there is a linear transformation  $T$  from a basis  $\{\alpha_1, \dots, \alpha_n\}$  to another basis  $\{\beta_1, \dots, \beta_n\}$ , then  $D(\beta_1, \dots, \beta_n) = (\det(T))^2 D(\alpha_1, \dots, \alpha_n)$ .

<sup>2</sup>Note that this basis may not be integral.

## 2.2 EMBEDDING

**Definition 2.7** (Embedding). Let  $\sigma : F \hookrightarrow \mathbb{C}$  be a field embedding. We say  $\sigma$  is a real embedding if  $\sigma(F) \subseteq \mathbb{R}$ , otherwise we say it is a complex embedding.

**Proposition 2.8.** For an algebraic field extension  $K/\mathbb{Q}$  of degree  $n$ , there is a total of  $n$  embeddings of  $K$  into  $\mathbb{C}$ .

**Proposition 2.9.**  $F \otimes_{\mathbb{Q}} \mathbb{R}$  is isomorphic to  $\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ , where  $r_1$  is the number of real embeddings, and  $r_2$  is the number of pairs of complex embeddings. Therefore, the extension  $F/\mathbb{Q}$  has degree  $r_1 + 2r_2$ .

## 2.3 MINKOWSKI BOUND

**Proposition 2.10.** For any non-zero ideal  $\mathfrak{a}$  of  $\mathcal{O}_F$ , there exists  $\alpha \in \mathfrak{a} \setminus \{0\}$  such that  $N_{F/\mathbb{Q}}(\alpha) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} N(\mathfrak{a}) |\text{disc}(F)|^{\frac{1}{2}}$ .

**Definition 2.11** (Minkowski Bound). The Minkowski bound  $B_F$  of a number field  $F$  is  $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\text{disc}(F)|^{\frac{1}{2}}$ .

**Theorem 2.12** (Minkowski). There exists a set of representatives of  $\text{Cl}_F$  consisting of ideals  $\mathfrak{a}$  such that  $N(\mathfrak{a}) \leq B_F$ . Therefore, we can find an (integral) ideal representing every class with norm less than or equal to the bound.

## 3 CALCULATIONS

In the following calculations, we denote the field in each subsection as  $K$ .

**Proposition 3.1.** The Minkowski bound for an imaginary quadratic field  $F$  is

$$\frac{2}{\pi} |\text{disc}(F)|^{\frac{1}{2}}.$$

*Proof.* For an imaginary quadratic field  $\mathbb{Q}(\sqrt{-n})$  where  $n > 0$ , we know  $r_1 = 0$  and  $r_2 = 1$ . Therefore, the Minkowski bound is

$$\frac{4}{\pi} \times \frac{2!}{2^2} |\text{disc}(F)|^{\frac{1}{2}} = \frac{2}{\pi} |\text{disc}(F)|^{\frac{1}{2}}.$$

□

**Proposition 3.2.** The Minkowski bound for a real quadratic field  $F$  is

$$\frac{1}{2} |\text{disc}(F)|^{\frac{1}{2}}.$$

*Proof.* Similarly, we have  $r_1 = 2$  and  $r_2 = 0$ . Therefore, the Minkowski bound is

$$\left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2} |\text{disc}(F)|^{\frac{1}{2}} = \frac{1}{2} |\text{disc}(F)|^{\frac{1}{2}}.$$

□

3.1  $\mathbb{Q}(\sqrt{-1})$ 

The discriminant is  $-4$ . Therefore, the Minkowski bound is  $1 < \frac{4}{\pi} < 2$ , then every ideal is principal. Therefore, the  $K$  has class number 1.

3.2  $\mathbb{Q}(\sqrt{-2})$ 

The discriminant is  $-8$ . Therefore, the Minkowski bound is  $1 < \frac{4\sqrt{2}}{\pi} < 2$ , then every ideal is principal. Therefore, the  $K$  has class number 1.

3.3  $\mathbb{Q}(\sqrt{-3})$ 

The discriminant is  $-3$ . Therefore, the Minkowski bound is  $1 < \frac{2\sqrt{3}}{\pi} < 2$ , then every ideal is principal. Therefore, the  $K$  has class number 1.

3.4  $\mathbb{Q}(\sqrt{-5})$ 

The discriminant of  $K$  is  $-20$ , then the Minkowski bound is  $B_K = \frac{2}{\pi}\sqrt{20} < 3$ . Because  $\mathbb{Z}[\sqrt{-5}]$  is not a PID, then  $h_K \geq 2$ , and so  $h_K = 2$ .

3.5  $\mathbb{Q}(\sqrt{-7})$ 

The discriminant is  $-7$ . Therefore, the Minkowski bound is  $1 < \frac{2\sqrt{7}}{\pi} < 2$ , then every ideal is principal. Therefore, the  $K$  has class number 1.

3.6  $\mathbb{Q}(\sqrt{-17})$ 

For  $K = \mathbb{Q}(\sqrt{-17})$ , this is an extension of degree 2 and the discriminant is  $-68$ . Note that there are no real embeddings and only a pair of complex embeddings. Therefore, we calculate the Minkowski bound to be

$$B = \frac{2}{4} \cdot \frac{4}{\pi} \cdot \sqrt{68} \approx 5.249.$$

Therefore, the class number is bounded between 1 and 5, inclusive. It suffices to find the ideals with these norms, and classify them.

The ideal with norm 1 is just the ring of integers,  $\mathbb{Z}[\sqrt{-17}]$ .

Consider an ideal with norm 2, then the prime ideal  $\mathfrak{p}$  lies above some other prime ideal  $(p)$  by  $\mathbb{Z}$ . In particular, the norm of this ideal gives

$$N(\mathfrak{p}) = \left| \frac{\mathcal{O}_K}{\mathfrak{p}} \right|,$$

but as a finite field we have  $N(\mathfrak{p}) = N(p)^{[\mathcal{O}_K/\mathfrak{p}:\mathbb{F}_p]}$ . In particular,  $p = 2$ . Therefore,  $\mathfrak{p}$  is a prime lying over  $(2)$ , with residue degree 1.

For an ideal  $\mathfrak{p}$  of norm 2, we must have  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ , which corresponds to surjective mappings  $\mathcal{O}_K \rightarrow \mathbb{Z}/2\mathbb{Z}$  that maps  $x^2 + 17$  to 0. This corresponds to elements  $x \in \mathbb{Z}/2\mathbb{Z}$

such that  $x^2 + 17 = 0$ , which is  $x = 1$ . Therefore, we now have the map with kernel  $(1 + \sqrt{-17})$ . Therefore, the unique ideal with norm 2 is the one generated by  $1 + \sqrt{-17}$  and 2, i.e.  $(2, 1 + \sqrt{-17})$ .<sup>3</sup>

Using the similar idea, an ideal  $\mathfrak{p}$  with norm 3 lies above the prime  $p = 3$ . Therefore,  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/3\mathbb{Z}$ , then the mapping sends  $x^2 + 17$  to 0, and therefore forces  $x^2 = 1$  within  $\mathbb{Z}/3\mathbb{Z}$ , so  $x = 1$  or 2. We conclude that ideals of norm 3 are either  $(3, 1 + \sqrt{-17})$  or  $(3, 2 + \sqrt{-17})$ .

Similarly, ideal  $\mathfrak{p}$  of norm 5 corresponds to the isomorphism  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/5\mathbb{Z}$ , but there are no  $x$ 's that sends  $x^2 + 17$  to 0. Hence, there is no ideal with norm 5.

An ideal  $\mathfrak{p}$  of norm 4 let the quotient ring corresponds to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  or  $\mathbb{Z}/4\mathbb{Z}$ . Note that there is no such mapping to  $\mathbb{Z}/4\mathbb{Z}$ , and the only mapping to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  that works is the product ideal  $(2, 1 + \sqrt{-17})(2, 1 + \sqrt{-17})$ , which is equivalent to (2).

Now, notice that  $(2, 1 + \sqrt{-17})$  is an element in the class group of order 2 since  $(2, 1 + \sqrt{-17})(2, 1 + \sqrt{-17}) = (2)$  and (2) is principal. Therefore, we know the class number is either 2 or 4. Also note that both  $(3, 1 + \sqrt{-17})$  and  $(3, 2 + \sqrt{-17})$  are not principal, and the square of either one does not equal to (3) by direct computation. In particular, both ideals of norm 3 do not have order 2 in the class group, forcing the class group has order greater than 2. In particular, the class number of  $\mathbb{Q}(\sqrt{-17})$  is 4.

### 3.7 $\mathbb{Q}(\sqrt[3]{2})$

The extension  $K/\mathbb{Q}$  is of degree 3, which means it must have a real embedding and a pair of complex embeddings. The determinant of the extension with respect to the basis  $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$  is  $D = -N_{K/\mathbb{Q}}(3\sqrt[3]{4}) = -N_{K/\mathbb{Q}}(3)N_{K/\mathbb{Q}}(\sqrt[3]{2})^2 = -3^2 \cdot 2^2 = -108$ .

### 3.8 $\mathbb{Q}(\sqrt{2})$

The discriminant is 8. Therefore, the Minkowski bound is  $1 < \sqrt{2} < 2$ , which forces an ideal with norm less than the bound to be the trivial ideal, which is principal. Hence, the class number is 1.

### 3.9 $\mathbb{Q}(\sqrt{3})$

The discriminant is 12. Therefore, the Minkowski bound is  $1 < \sqrt{3} < 2$ , which forces an ideal with norm less than the bound to be the trivial ideal, which is principal. Hence, the class number is 1.

### 3.10 $\mathbb{Q}(\sqrt{5})$

The discriminant is 5, and therefore the Minkowski bound is  $1 < \frac{\sqrt{5}}{2} < 2$ , which forces an ideal with norm less than the bound to be the trivial ideal, which is principal. Hence, the class number is 1.

---

<sup>3</sup>The ideal has to be in the form  $(2, \alpha)$  for some  $\alpha$  since  $\mathfrak{p}$  is prime of norm 2 and divides (2). Similar idea works below.

3.11  $\mathbb{Q}(\sqrt{6})$ 

The discriminant is 24, and therefore the Minkowski bound is

$$\left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2} |24|^{\frac{1}{2}} = \sqrt{6} \approx 2.45.$$

Therefore, it suffices to show that every ideal of norm 2 is principal. Note that an ideal of norm 2 must lie above the prime (2). Moreover, an ideal  $\mathfrak{p}$  of norm 2 corresponds to the isomorphism  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ , then it sends  $x^2 - 6$  to 0, and then by the embedding we have  $x^2 - 6 = 0$  in  $\mathbb{Z}/2\mathbb{Z}$ , so  $x = 0$ . Therefore, the unique ideal with norm 2 that lies above 2 is just  $(2, \sqrt{6})$ . Note that  $(2, \sqrt{6}) \subseteq (2 - \sqrt{6})$  because  $2 = (\sqrt{6} - 2)(\sqrt{6} + 2)$  and  $\sqrt{6} = (2 - \sqrt{6})(-3 - \sqrt{6}) = \sqrt{6}$  and obviously we have  $(2, \sqrt{6}) = (2 - \sqrt{6})$ . Therefore,  $(2 - \sqrt{6})$  is the unique ideal with norm 2, and it is principal. This concludes the proof.

3.12  $\mathbb{Q}(\sqrt{13})$ 

The discriminant is 13. Therefore, the Minkowski bound is  $1 < \frac{\sqrt{13}}{2} < 2$ , which forces an ideal with norm less than the bound to be the trivial ideal, which is principal. Hence, the class number is 1.

3.13  $\mathbb{Q}(\sqrt{17})$ 

The discriminant is 17. Therefore, the Minkowski bound is  $2 < \frac{\sqrt{17}}{2} < 3$ . We consider the ideals  $\mathfrak{p}$  of norm 2. Therefore, we must have  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}[\frac{1+\sqrt{17}}{2}]/\mathfrak{p} \cong \mathbb{Z}/2\mathbb{Z}$ , which corresponds to surjective mappings  $\mathcal{O}_K \rightarrow \mathbb{Z}/2\mathbb{Z}$  that sends  $x^2 - x - 4 \mapsto 0$ . In particular, we have  $x = 1$  or 0 in  $\mathbb{Z}/2\mathbb{Z}$ . Therefore, the corresponding ideals are  $(2, \frac{3+\sqrt{17}}{2})$  and  $(2, \frac{1+\sqrt{17}}{2})$ . These ideals correspond to  $(\frac{3+\sqrt{17}}{2})$  and  $(\frac{3-\sqrt{17}}{2})$ , respectively. Therefore, the only ideals of norm 2 are principal ones, so the ideal class number is 1.