

# Chapter 5

## The Ideal Class Group

We will use Minkowski theory, which belongs to the general area of geometry of numbers, to gain insight into the ideal class group of a number field. We have already mentioned the ideal class group briefly in (3.4.5); it measures how close a Dedekind domain is to a principal ideal domain.

### 5.1 Lattices

#### 5.1.1 Definitions and Comments

Let  $e_1, \dots, e_n \in \mathbb{R}^n$ , with the  $e_i$  linearly independent over  $\mathbb{R}$ . Thus the  $e_i$  form a basis for  $\mathbb{R}^n$  as a vector space over  $\mathbb{R}$ . The  $e_i$  also form a basis for a free  $\mathbb{Z}$ -module of rank  $n$ , namely

$$H = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n.$$

A set  $H$  constructed in this way is said to be a *lattice* in  $\mathbb{R}^n$ . The *fundamental domain* of  $H$  is given by

$$T = \{x \in \mathbb{R}^n : x = \sum_{i=1}^n a_i e_i, 0 \leq a_i < 1\}.$$

In the most familiar case,  $e_1$  and  $e_2$  are linearly independent vectors in the plane, and  $T$  is the parallelogram generated by the  $e_i$ . In general, every point of  $\mathbb{R}^n$  is congruent modulo  $H$  to a unique point of  $T$ , so  $\mathbb{R}^n$  is the disjoint union of the sets  $h + T$ ,  $h \in H$ . If  $\mu$  is Lebesgue measure, then the volume  $\mu(T)$  of the fundamental domain  $T$  will be denoted by  $v(H)$ . If we generate  $H$  using a different  $\mathbb{Z}$ -basis, the volume of the fundamental domain is unchanged. (The change of variables matrix between  $\mathbb{Z}$ -bases is unimodular, hence has determinant  $\pm 1$ . The result follows from the change of variables formula for multiple integrals.)

### 5.1.2 Lemma

Let  $S$  be a Lebesgue measurable subset of  $\mathbb{R}^n$  with  $\mu(S) > v(H)$ . Then there exist distinct points  $x, y \in S$  such that  $x - y \in H$ .

*Proof.* As we observed in (5.1.1), the sets  $h + T, h \in H$ , are (pairwise) disjoint and cover  $\mathbb{R}^n$ . Thus the sets  $S \cap (h + T), h \in H$ , are disjoint and cover  $S$ . Consequently,

$$\mu(S) = \sum_{h \in H} \mu(S \cap (h + T)).$$

By translation-invariance of Lebesgue measure,  $\mu(S \cap (h + T)) = \mu((-h + S) \cap T)$ . Now if  $S \cap (h_1 + T)$  and  $S \cap (h_2 + T)$  are disjoint, it does not follow that  $(-h_1 + S) \cap T$  and  $(-h_2 + S) \cap T$  are disjoint, as we are not subtracting the same vector from each set. In fact, if the sets  $(-h + S) \cap T, h \in H$ , were disjoint, we would reach a contradiction via

$$v(H) = \mu(T) \geq \sum_{h \in H} \mu((-h + S) \cap T) = \mu(S).$$

Thus there are distinct elements  $h_1, h_2 \in H$  such that  $(-h_1 + S) \cap (-h_2 + S) \cap T \neq \emptyset$ . Choose (necessarily distinct)  $x, y \in S$  such that  $-h_1 + x = -h_2 + y$ . Then  $x - y = h_1 - h_2 \in H$ , as desired. ♣

### 5.1.3 Minkowski's Convex Body Theorem

Let  $H$  be a lattice in  $\mathbb{R}^n$ , and assume that  $S$  is a Lebesgue measurable subset of  $\mathbb{R}^n$  that is symmetric about the origin and convex. If

- (a)  $\mu(S) > 2^n v(H)$ , or
  - (b)  $\mu(S) \geq 2^n v(H)$  and  $S$  is compact,
- then  $S \cap (H \setminus \{0\}) \neq \emptyset$ .

*Proof.*

(a) Let  $S' = \frac{1}{2}S$ . Then  $\mu(S') = 2^{-n} \mu(S) > v(H)$  by hypothesis, so by (5.1.2), there exist distinct elements  $y, z \in S'$  such that  $y - z \in H$ . But  $y - z = \frac{1}{2}(2y + (-2z))$ , a convex combination of  $2y$  and  $-2z$ . But  $y \in S' \Rightarrow 2y \in S$ , and  $z \in S' \Rightarrow 2z \in S \Rightarrow -2z \in S$  by symmetry about the origin. Thus  $y - z \in S$  and since  $y$  and  $z$  are distinct,  $y - z \in H \setminus \{0\}$ .

(b) We apply (a) to  $(1 + 1/m)S, m = 1, 2, \dots$ . Since  $S$ , hence  $(1 + 1/m)S$ , is a bounded set, it contains only finitely many points of the lattice  $H$ . Consequently, for every positive integer  $m$ ,  $S_m = (1 + 1/m)S \cap (H \setminus \{0\})$  is a nonempty finite, hence compact, subset of  $\mathbb{R}^n$ . Since  $S_{m+1} \subseteq S_m$  for all  $m$ , the sets  $S_m$  form a nested sequence, and therefore  $\bigcap_{m=1}^{\infty} S_m \neq \emptyset$ . If  $x \in \bigcap_{m=1}^{\infty} S_m$ , then  $x \in H \setminus \{0\}$  and  $x/(1 + 1/m) \in S$  for every  $m$ . Since  $S$  is closed, we may let  $m \rightarrow \infty$  to conclude that  $x \in S$ . ♣

### 5.1.4 Example

With  $n = 2$ , take  $e_1 = (1, 0)$  and  $e_2 = (0, 1)$ . The fundamental domain is the unit square, closed at the bottom and on the left, and open at the top and on the right. Let  $S$  be the set of all  $a_1 e_1 + a_2 e_2$  with  $-1 < a_i < 1, i = 1, 2$ . Then  $\mu(S) = 4v(H)$ , but  $S$  contains no nonzero lattice points. Thus compactness is a necessary hypothesis in part (b).

## 5.2 A Volume Calculation

We will use  $n$ -dimensional integration technique to derive a result that will be needed in the proof that the ideal class group is finite. We will work in  $\mathbb{R}^n$ , realized as the product of  $r_1$  copies of  $\mathbb{R}$  and  $r_2$  copies of  $\mathbb{C}$ , where  $r_1 + 2r_2 = n$ . Our interest is in the set

$$B_t = \{(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t\}, t \geq 0.$$

We will show that the volume of  $B_t$  is given by

$$V(r_1, r_2, t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}.$$

The proof is by double induction on  $r_1$  and  $r_2$ . If  $r_1 = 1$  and  $r_2 = 0$ , hence  $n = 1$ , we are calculating the length of the interval  $[-t, t]$ , which is  $2t$ , as predicted. If  $r_1 = 0$  and  $r_2 = 1$ , hence  $n = 2$ , we are calculating the area of  $\{z_1 : 2|z_1| \leq t\}$ , a disk of radius  $t/2$ . The result is  $\pi t^2/4$ , again as predicted. Now assume that the formula holds for  $r_1, r_2$ , and all  $t$ . Then  $V(r_1 + 1, r_2, t)$  is the volume of the set described by

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t$$

or equivalently by

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t - |y|.$$

Now if  $|y| > t$ , then  $B_t$  is empty. For smaller values of  $|y|$ , suppose we change  $|y|$  to  $|y| + dy$ . This creates a box in  $(n + 1)$ -space with  $dy$  as one of the dimensions. The volume of the box is  $V(r_1, r_2, t - |y|)dy$ . Thus

$$V(r_1 + 1, r_2, t) = \int_{-t}^t V(r_1, r_2, t - |y|) dy$$

which by the induction hypothesis is  $2 \int_0^t 2^{r_1} (\pi/2)^{r_2} [(t - y)^n / n!] dy$ . Evaluating the integral, we obtain  $2^{r_1+1} (\pi/2)^{r_2} t^{n+1} / (n + 1)!$ , as desired.

Finally,  $V(r_1, r_2 + 1, t)$  is the volume of the set described by

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| + 2|z| \leq t.$$

As above,

$$V(r_1, r_2 + 1, t) = \int_{|z| \leq t/2} V(r_1, r_2, t - 2|z|) d\mu(z)$$

where  $\mu$  is Lebesgue measure on  $\mathbb{C}$ . In polar coordinates, the integral becomes

$$\int_{\theta=0}^{2\pi} \int_{r=0}^{t/2} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t-2r)^n}{n!} r \, dr \, d\theta$$

which reduces to  $2^{r_1}(\pi/2)^{r_2}(2\pi/n!) \int_{r=0}^{t/2} (t-2r)^n r \, dr$ . We may write the integrand as  $(t-2r)^n r \, dr = -rd(t-2r)^{n+1}/2(n+1)$ . Integration by parts yields (for the moment ignoring the constant factors preceding the integral)

$$\int_0^{t/2} (t-2r)^{n+1} dr/2(n+1) = \frac{-(t-2r)^{n+2}}{2(n+1)2(n+2)} \Big|_0^{t/2} = \frac{t^{n+2}}{4(n+1)(n+2)}.$$

Therefore  $V(r_1, r_2 + 1, t) = 2^{r_1}(\pi/2)^{r_2}(2\pi/n!)t^{n+2}/4(n+1)(n+2)$ , which simplifies to  $2^{r_1}(\pi/2)^{r_2+1}t^{n+2}/(n+2)!$ , completing the induction. Note that  $n+2$  (rather than  $n+1$ ) is correct, because  $r_1 + 2(r_2 + 1) = r_1 + 2r_2 + 2 = n + 2$ .

## 5.3 The Canonical Embedding

### 5.3.1 Definitions and Comments

Let  $L$  be a number field of degree  $n$  over  $\mathbb{Q}$ , and let  $\sigma_1, \dots, \sigma_n$  be the  $\mathbb{Q}$ -monomorphisms of  $L$  into  $\mathbb{C}$ . If  $\sigma_i$  maps entirely into  $\mathbb{R}$ , we say that  $\sigma_i$  is a *real embedding*; otherwise it is a *complex embedding*. Since the complex conjugate of a  $\mathbb{Q}$ -monomorphism is also a  $\mathbb{Q}$ -monomorphism, we can renumber the  $\sigma_i$  so that the real embeddings are  $\sigma_1, \dots, \sigma_{r_1}$  and the complex embeddings are  $\sigma_{r_1+1}, \dots, \sigma_n$ , with  $\sigma_{r_1+j}$  paired with its complex conjugate  $\sigma_{r_1+r_2+j}$ ,  $j = 1, \dots, r_2$ . Thus there are  $2r_2$  complex embeddings, and  $r_1 + 2r_2 = n$ .

The *canonical embedding*  $\sigma : L \rightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$  is the injective ring homomorphism given by

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)).$$

### 5.3.2 Some Matrix Manipulations

Let  $x_1, \dots, x_n \in L$  be linearly independent over  $\mathbb{Z}$  (hence the  $x_i$  form a basis for  $L$  over  $\mathbb{Q}$ ). Let  $C$  be the matrix whose  $k^{\text{th}}$  column ( $k = 1, \dots, n$ ) is

$$\sigma_1(x_k), \dots, \sigma_{r_1}(x_k), \operatorname{Re} \sigma_{r_1+1}(x_k), \operatorname{Im} \sigma_{r_1+1}(x_k), \dots, \operatorname{Re} \sigma_{r_1+r_2}(x_k), \operatorname{Im} \sigma_{r_1+r_2}(x_k).$$

The determinant of  $C$  looks something like a discriminant, and we can be more precise with the aid of elementary row operations. Suppose that

$$\begin{pmatrix} \sigma_j(x_k) \\ \bar{\sigma}_j(x_k) \end{pmatrix} = \begin{pmatrix} x + iy \\ x - iy \end{pmatrix}.$$

We are fixing  $j$  and allowing  $k$  to range from 1 to  $n$ , so we have two rows of an  $n$  by  $n$  matrix. Add the second row to the first, so that the entries on the right become  $2x$

and  $x - iy$ . Then add  $-1/2$  times row 1 to row 2, and the entries become  $2x$  and  $-iy$ . Factoring out 2 and  $-i$ , we get

$$-2i \begin{pmatrix} x \\ y \end{pmatrix} = -2i \begin{pmatrix} \operatorname{Re} \sigma_j(x_k) \\ \operatorname{Im} \sigma_j(x_k) \end{pmatrix}.$$

Do this for each  $j = 1, \dots, r_2$ . In the above calculation,  $\bar{\sigma}_j$  appears immediately under  $\sigma_j$ , but in the original ordering they are separated by  $r_2$ , which introduces a factor of  $(-1)^{r_2}$  when we calculate a determinant. To summarize, we have

$$\det C = (2i)^{-r_2} \det(\sigma_j(x_k))$$

Note that  $j$  and  $k$  range from 1 to  $n$ ; no operations are needed for the first  $r_1$  rows.

Now let  $M$  be the free  $\mathbb{Z}$ -module generated by the  $x_i$ , so that  $\sigma(M)$  is a free  $\mathbb{Z}$ -module with basis  $\sigma(x_i), i = 1, \dots, n$ , hence a lattice in  $\mathbb{R}^n$ . The fundamental domain is a parallelotope whose sides are the  $\sigma(x_i)$ , and the volume of the fundamental domain is the absolute value of the determinant whose rows (or columns) are the  $\sigma(x_i)$ . Consequently [see (5.1.1) for notation],

$$v(\sigma(M)) = |\det C| = 2^{-r_2} |\det \sigma_j(x_k)|.$$

We apply this result in an algebraic number theory setting.

### 5.3.3 Proposition

Let  $B$  be the ring of algebraic integers of a number field  $L$ , and let  $I$  be a nonzero integral ideal of  $B$ , so that by (4.2.4) and (5.3.2),  $\sigma(I)$  is a lattice in  $\mathbb{R}^n$ . Then the volume of the fundamental domain of this lattice is

$$v(\sigma(I)) = 2^{-r_2} |d|^{1/2} N(I);$$

in particular,  $v(\sigma(B)) = 2^{-r_2} |d|^{1/2}$ , where  $d$  is the field discriminant.

*Proof.* The result for  $I = B$  follows from (5.3.2) and (2.3.3), taking the  $x_k$  as an integral basis for  $B$ . To establish the general result, observe that the fundamental domain for  $\sigma(I)$  can be assembled by taking the disjoint union of  $N(I)$  copies of the fundamental domain of  $\sigma(B)$ . To convince yourself of this, let  $e_1$  and  $e_2$  be basis vectors in the plane. The lattice  $H'$  generated by  $2e_1$  and  $3e_2$  is a subgroup of the lattice  $H$  generated by  $e_1$  and  $e_2$ , but the fundamental domain  $T'$  of  $H'$  is larger than the fundamental domain  $T$  of  $H$ . In fact, exactly 6 copies of  $T$  will fit inside  $T'$ . ♣

### 5.3.4 Minkowski Bound on Element Norms

If  $I$  is a nonzero integral ideal of  $B$ , then  $I$  contains a nonzero element  $x$  such that

$$|N_{L/\mathbb{Q}}(x)| \leq (4/\pi)^{r_2} (n!/n^n) |d|^{1/2} N(I).$$

*Proof.* The set  $B_t$  of Section 5.2 is compact, convex and symmetric about the origin. The volume of  $B_t$  is  $\mu(B_t) = 2^{r_1} (\pi/2)^{r_2} t^n / n!$ , with  $\mu$  indicating Lebesgue measure. We

choose  $t$  so that  $\mu(B_t) = 2^n v(\sigma(I))$ , which by (5.3.3) is  $2^{n-r_2} |d|^{1/2} N(I)$ . Equating the two expressions for  $\mu(B_t)$ , we get

$$t^n = 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} N(I).$$

Apply (5.1.3b) with  $H = \sigma(I)$  and  $S = B_t$ . By our choice of  $t$ , the hypothesis of (5.1.3b) is satisfied, and we have  $S \cap (H \setminus \{0\}) \neq \emptyset$ . Thus there is a nonzero element  $x \in I$  such that  $\sigma(x) \in B_t$ . Now by (2.1.6), the absolute value of the norm of  $x$  is the product of the positive numbers  $a_i = |\sigma_i(x)|$ ,  $i = 1, \dots, n$ . To estimate  $N(x)$ , we invoke the inequality of the arithmetic and geometric means, which states that  $(a_1 \cdots a_n)^{1/n} \leq (a_1 + \cdots + a_n)/n$ . It follows that  $a_1 \cdots a_n \leq (\sum_{i=1}^n a_i/n)^n$ . With our  $a_i$ 's, we have

$$|N(x)| \leq \left[ \frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{i=r_1+1}^{r_1+r_2} |\sigma_i(x)| \right]^n.$$

Since  $\sigma(x) \in B_t$ , we have  $|N(x)| \leq t^n/n^n$ . By choice of  $t$ ,

$$|N(x)| \leq (1/n^n) 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} N(I).$$

But  $n - r_1 = 2r_2$ , so  $2^{n-r_1} \pi^{-r_2} = 2^{2r_2} \pi^{-r_2} = (4/\pi)^{r_2}$ , and the result follows. ♣

### 5.3.5 Minkowski Bound on Ideal Norms

Every ideal class [see (3.4.5)] of  $L$  contains an integral ideal  $I$  such that

$$N(I) \leq (4/\pi)^{r_2} (n!/n^n) |d|^{1/2}.$$

*Proof.* Let  $J'$  be a fractional ideal in the given class. We can multiply by a principal ideal of  $B$  without changing the ideal class, so we can assume with loss of generality that  $J = (J')^{-1}$  is an integral ideal. Choose a nonzero element  $x \in J$  such that  $x$  satisfies the norm inequality of (5.3.4). Our candidate is  $I = xJ'$ .

First note that  $I$  is an integral ideal because  $x \in J$  and  $JJ' = B$ . Now  $(x) = IJ$ , so by (4.2.6) and (5.3.4),

$$N(I)N(J) = N(x) \leq (4/\pi)^{r_2} (n!/n^n) |d|^{1/2} N(J).$$

Cancel  $N(J)$  to get the desired result. ♣

### 5.3.6 Corollary

The ideal class group of a number field is finite.

*Proof.* By (4.2.13), there are only finitely many integral ideals with a given norm. By (5.3.5), we can associate with each ideal class an integral ideal whose norm is bounded above by a fixed constant. If the ideal class group were infinite, we would eventually use the same integral ideal in two different ideal classes, which is impossible. ♣

### 5.3.7 Applications

Suppose that a number field  $L$  has a Minkowski bound on ideal norms that is less than 2. Since the only ideal of norm 1 is the trivial ideal  $(1) = B$ , every ideal class must contain  $(1)$ . Thus there can be only one ideal class, and the *class number* of  $L$ , that is, the order of the ideal class group, is  $h_L = 1$ . By (3.4.5),  $B$  is a PID, equivalently, by (3.2.8), a UFD.

If the Minkowski bound is greater than 2 but less than 3, we must examine ideals whose norm is 2. If  $I$  is such an ideal, then by (4.2.9),  $I$  divides  $(2)$ . Thus the prime factorization of  $(2)$  will give useful information about the class number.

In the exercises, we will look at several explicit examples.

### Problems For Section 5.3

1. Calculate the Minkowski bound on ideal norms for an imaginary quadratic field, in terms of the field discriminant  $d$ . Use the result to show that  $\mathbb{Q}(\sqrt{m})$  has class number 1 for  $m = -1, -2, -3, -7$ .
2. Calculate the Minkowski bound on ideal norms for a real quadratic field, in terms of the field discriminant  $d$ . Use the result to show that  $\mathbb{Q}(\sqrt{m})$  has class number 1 for  $m = 2, 3, 5, 13$ .
3. Show that in the ring of algebraic integers of  $\mathbb{Q}(\sqrt{-5})$ , there is only one ideal whose norm is 2. Then use the Minkowski bound to prove that the class number is 2.
4. Repeat Problem 3 for  $\mathbb{Q}(\sqrt{6})$ .
5. Show that the only prime ideals of norm 2 in the ring of algebraic integers of  $\mathbb{Q}(\sqrt{17})$  are principal. Conclude that the class number is 1.
6. Find the class number of  $\mathbb{Q}(\sqrt{14})$ . (It will be necessary to determine the number of ideals of norm 3 as well as norm 2.)

Problems 7-10 consider bounds on the field discriminant.

7. Let  $L$  be a number field of degree  $n$  over  $\mathbb{Q}$ , with field discriminant  $d$ . Show that  $|d| \geq a_n = (\pi/4)^n n^{2n}/(n!)^2$ .
8. Show that  $a_2 = \pi^2/4$  and  $a_{n+1}/a_n \geq 3\pi/4$ . From this, derive the lower bound  $|d| \geq (\pi/3)(3\pi/4)^{n-1}$  for  $n \geq 2$ .
9. Show that  $n/\log |d|$  is bounded above by a constant that is independent of the particular number field.
10. Show that if  $L \neq \mathbb{Q}$ , then  $|d| > 1$ , hence in any nontrivial extension of  $\mathbb{Q}$ , at least one prime must ramify.