Part I
The first part

1 Number Fields

I will assume that every one is familiar with the material in the first year algebra sequence, notably groups, rings, fields, ideals and Galois theory, as well as the material from Number Theory I, though I will review some of the key definitions and results which the undergraduates may not be familiar with, and perhaps the graduate students have forgotten. In this first section, we will go over the basics of number fields, which will largely be a review of the second half of last semester, with some generalizations of notions introduced in the context of quadratic fields. However some fundamental notions will be new to us, such as discriminants. We will for the most part omit proofs of results covered last semester (even if we only sketched the proof) or in a standard Algebra course. For complete proofs, refer to any standard texts on Algebra and Algebraic Number Theory. Since the material in this chapter should be largely familiar to you, and the point is to fill in some things we missed last semester, we will go through this section rather quickly.

The presentation of the material in this chapter is based on [Stewart–Tall].

1.1 Algebraic Numbers

Let $R[x]$ denote the ring of polynomials in x with coefficients in a ring R. We say $p(x) \in R[x]$ is **monic** if the leading coefficient of $p(x)$ is 1. (All rings for us are commutative with 1.) By the Fundamental Theorem of Algebra, any polynomial in $\mathbb{Q}[x]$ factors into linear factors in $\mathbb{C}$. We say $\alpha \in \mathbb{C}$ is an **algebraic number** if it is the root of some $p(x) \in \mathbb{Q}[x]$ (or equivalently a polynomial in $\mathbb{Z}[x]$, but then we can't assume it's monic). Without loss of generality we may assume $p(x)$ is monic. If $p(x)$ is of smallest degree such that this is true, and we say $p(x)$ is the **minimum polynomial** of α (over $\mathbb{Q}$), and the **degree** $\deg(\alpha)$ of α defined to be the $\deg(p(x))$. If in fact $p(x) \in \mathbb{Z}[x]$, we say α is an **algebraic integer**.

Some basic facts from algebra are that

(i) the minimum polynomial $p(x)$ of α is uniquely determined (which is why we make the monic condition),

(ii) $p(x)$ is irreducible over $\mathbb{Q}$ (and therefore $\mathbb{Z}$ if $p(x) \in \mathbb{Z}[x]$), and

(iii) if $q(x) \in \mathbb{Z}[x]$ and $q(\alpha) = 0$, then $p(x)|q(x)$ (in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$ if $p(x) \in \mathbb{Z}[x]$).

Lemma 1.1.1. *Let $\alpha \in \mathbb{C}$. Then $[\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty$ if and only if α is an algebraic integer. In this case $\{1, \alpha, \cdots, \alpha^{m-1}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ where $m = \deg(\alpha)$.*

This was Proposition 10.9 from last semester.

Lemma 1.1.2. *Suppose α is an algebraic number. Then $c\alpha$ is an algebraic integer for some $c \in \mathbb{Z}$.*

Proof. Suppose the minimum polynomial for α is $p(x) = x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \cdots + \frac{a_1}{b_1}x + \frac{a_0}{b_0}$ where each $a_i, b_i \in \mathbb{Z}$. Let $c = b_0 b_1 \cdots b_{n-1}$. Then $p(\frac{y}{c}) = \frac{y^n}{c^n} + \frac{a_{n-1}}{b_{n-1}c^{n-1}}y^{n-1} + \cdots + \frac{a_1}{b_1 c}y + \frac{a_0}{b_0}$. Multiplying by c^n, we see

$$q(y) = c^n p(\frac{y}{c}) = y^n + \frac{a_{n-1}c}{b_{n-1}}y^{n-1} + \cdots \frac{a_1 c^{n-1}}{b_1}y + \frac{a_0 c^n}{b_0} \in \mathbb{Z}[y].$$

But $q(c\alpha) = c^n p(\alpha) = 0$, so y is an algebraic integer. □

Recall from algebra that if R is an integral domain (not the zero ring and has no zero divisors), we can form the smallest field F containing R by considering the set of fractions $F = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}$. This is called the **field of fractions** or **fraction field** of R.

Theorem 1.1.3. *The set $\mathbb{B}$ of all algebraic integers form a subring of $\mathbb{C}$, and the set $\mathbb{A}$ of all algebraic numbers form its field of fractions.*

We omitted the proof last semester, so here it is, in all its glory.

Proof. Note that by the Lemma 1.1.1, $\mathbb{B}$ consists precisely of all elements $\alpha \in \mathbb{C}$ such that $[\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty$. To show it is a subring of $\mathbb{C}$, we want to show if $\alpha, \beta \in \mathbb{B}$, then so are $\alpha + \beta, \alpha - \beta$ and $\alpha\beta$. But these elements are all clearly in $\mathbb{Z}[\alpha, \beta]$, and

$$[\mathbb{Z}[\alpha, \beta] : \mathbb{Z}] = [\mathbb{Z}[\alpha, \beta] : \mathbb{Z}[\alpha]] \cdot [\mathbb{Z}[\alpha] : \mathbb{Z}] \leq [\mathbb{Z}[\beta] : \mathbb{Z}] \cdot [\mathbb{Z}[\alpha] : \mathbb{Z}] < \infty.$$

Since $\mathbb{Z}[\alpha + \beta]$, $\mathbb{Z}[\alpha - \beta]$ and $\mathbb{Z}[\alpha\beta]$ are all contained in $\mathbb{Z}[\alpha, \beta]$, they must all have finite degree.

To see that $\mathbb{A}$ is its field of fractions, one runs through the same argument for fields. Namely, one shows that $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$ if and only if α is algebraic. The above argument shows $\mathbb{A}$ is a field. Lemma 1.1.2 shows that any element of $\mathbb{A}$ is a quotient of two elements in $\mathbb{B}$. □

Exercise 1.1. *Show by example that $[\mathbb{Z}[\alpha, \beta] : \mathbb{Z}[\alpha]]$ need not equal $[\mathbb{Z}[\beta] : \mathbb{Z}]$.*

Definition 1.1.4. *Let K be a subfield of $\mathbb{C}$ We say K is a* **number field** *if $[K : \mathbb{Q}] < \infty$. Its* **ring of integers** *is $\mathcal{O}_K = \mathbb{B} \cap K$.*

From now on we let K denote a number field.

Proposition 1.1.5. *K is the field of fractions of $\mathcal{O}_K$.*

This follows from Lemma 1.1.2 as in the proof of Theorem 1.1.3.

Proposition 1.1.6. *We have $K = \mathbb{Q}(\alpha)$ for some algebraic integer α.*

This is the Primitive Element Theorem from Galois theory. Here α is called a **primitive element** for K (over $\mathbb{Q}$).

Proposition 1.1.7. *We have $[K : \mathbb{Q}] = [\mathcal{O}_K : \mathbb{Z}]$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. By Lemma 1.1.2, any $x \in K$ is a $\mathbb{Q}$-linear combination of $\alpha_1, \ldots, \alpha_n$. Hence to see $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K it suffices to show they are linearly independent of $\mathbb{Q}$. Suppose $\frac{a_1}{b_1}\alpha_1 + \cdots + \frac{a_n}{b_n}\alpha_n = 0$ for some $a_i, b_i \in \mathbb{Z}$. Multiplying through by $b_1 b_2 \cdots b_n$, the fact that the α_i's are linearly independent over $\mathbb{Z}$ (and no $b_i = 0$) implies each $a_i = 0$. □

If $L \subseteq \mathbb{C}$ is a field containing K and $[L : K]$ is finite, we say L is a finite **extension** of K of **degree** $[L : K]$. Clearly this means L is also a number field since $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$.

Corollary 1.1.8. *If L is a finite extension of K, then $[L : K] = [\mathcal{O}_L : \mathcal{O}_K]$.*

Proof. $[L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = [\mathcal{O}_L : \mathbb{Z}]/[\mathcal{O}_K : \mathbb{Z}] = [\mathcal{O}_L : \mathcal{O}_K]$. □

Suppose K is a *quadratic field*, i.e., $[K:\mathbb{Q}]=2$. Recall that we may write $K=\mathbb{Q}(\sqrt{d})$ where $d\in\mathbb{Z}$ is squarefree (and $d\neq 1$). Recall d squarefree means $n^2|d \implies n^2=1$.

Example 1.1.9. *Suppose $d\in\mathbb{Z}$ is squarefree, $d\neq 1$, and let $K=\mathbb{Q}(\sqrt{d})$. Then*

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d\equiv 1 \bmod 4\\ \mathbb{Z}[\sqrt{d}] & d\equiv 2,3 \bmod 4.\end{cases}$$

If $d>0$, we say K is a **real quadratic field** *since $K\subseteq\mathbb{R}$. There are infinitely many units of $\mathcal{O}_K$, and they are generated by a fundamental unit $\epsilon=x+y\sqrt{n}$ (the smallest $\epsilon>1$ such that $N(\epsilon)=x^2-ny^2=\pm1$) and -1.*

If $d<0$, we say K is an **imaginary quadratic field** *since $K\not\subseteq\mathbb{R}$. Here there are only finitely many units of $\mathcal{O}_K$, and precisely they are $\pm1,\pm i$ (the 4-th roots of unity) if $d=-1$; they are $\pm1,\pm\zeta_3,\pm\zeta_3^2$ (the 6-th roots of unity) if $d=-3$; and they are ±1 (the 2-nd roots of unity) otherwise.*

(Recall the units of a ring R are the set of invertible elements and they are a group under multiplication.)

1.2 Some Galois theory

Let L/K be an extension of number fields of degree n, i.e., $[L:K]=n$. An embedding of $L\hookrightarrow\mathbb{C}$ is a field homomorphism from L into $\mathbb{C}$, i.e., a map $\sigma:L\to\mathbb{C}$ such that $\sigma(x+y)=\sigma(x)+\sigma(y)$, $\sigma(xy)=\sigma(x)\sigma(y)$, $\sigma(-x)=-\sigma(x)$ and $\sigma(x^{-1})=\sigma(x)^{-1}$. Necessarily $\sigma(0)=0$, $\sigma(1)=1$, and consequently σ fixes $\mathbb{Q}$, i.e., $\sigma(x)=x$ for each $x\in\mathbb{Q}$.

Example 1.2.1. *Let $L=\mathbb{Q}(i)$. A $\mathbb{Q}$-basis for L is $\{1,i\}$. If $\sigma:L\hookrightarrow\mathbb{C}$ is an embedding, it fixes 1, so it is determined by what it does to i. We must have $\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1$ so i must map to a square root of -1, i.e., either i or $-i$. One may check that both of these give embeddings, $\sigma_j:\mathbb{Q}(i)\to\mathbb{C}$ given by $\sigma_1(a+bi)=a+bi$ (the trivial embedding), and $\sigma_2(a+bi)=a-bi$ (complex conjugation).*

The **Galois group** of L/K, denoted $\mathrm{Gal}(L/K)$ is the group of all embeddings of $L\hookrightarrow\mathbb{C}$ which fix (each element of) K. The **Galois closure** of L/K is the smallest extension L' of L such that each $\sigma\in\mathrm{Gal}(L/K)$ maps into L'. We say the extension L/K is **Galois** if $L'=L$.

Example 1.2.2. *$K=\mathbb{Q}$ and $L=\mathbb{Q}(i)$. Every embedding of L into $\mathbb{C}$ fixes K, so $\mathrm{Gal}(L/K)=\{\sigma_1,\sigma_2\}$ from the example above. Every embedding lies in L, so L/K is Galois.*

By the Primitive Element Theorem, we may write $L=K(\alpha)$ where α is an algebraic integer. Let $f(x)\in K[x]$ be the minimum polynomial for α over K. This means $f(x)$ is the irreducible monic polynomial of smallest possible degree with coefficients in K (in fact $\mathcal{O}_K$ since α is an integer) such that $f(\alpha)=0$. It is not difficult to show that $\deg(f(x))=n$ (in fact, we already did in the case $K=\mathbb{Q}$).

Example 1.2.3. *$K=\mathbb{Q}(\sqrt{2})$ and $L=\mathbb{Q}(\sqrt[4]{2})=K(\alpha)$ where $\alpha^2=\sqrt{2}\in K$. The minimum polynomial for α over K is $f(x)=x^2-\sqrt{2}$. (Contrast this with the minimum polynomial for α over $\mathbb{Q}$: $p(x)=x^4-2$, of degree 4).*

Exercise 1.2. *In the above example, show L/K is Galois, but $L/\mathbb{Q}$ is not.*

Theorem 1.2.4. *Suppose $L = K(\alpha)$ and $f(x)$ is the minimum polynomial of α over K. The n roots of $f(x)$ are all distinct, call them $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$. Every embedding of $L \hookrightarrow \mathbb{C}$ permutes the roots $f(x)$, and $\mathrm{Gal}(L/K)$ acts transitively on the roots. Conversely, every embedding $L \hookrightarrow \mathbb{C}$ is uniquely determined by the way it permutes the roots of $f(x)$. Therefore, $\mathrm{Gal}(L/K)$ is isomorphic to a transitive subgroup of S_n. Further the Galois closure of L/K is $L' = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, i.e., L/K is Galois if and only if L contains all the root of $f(x)$.*

See any reference on Galois theory. Here S_n denotes the symmetric group on n-letters, i.e., the permutations of $\{1, 2, \dots, n\}$. Note that $L' = K(\alpha_1, \dots, \alpha_n)$ is often called the **splitting field** of $f(x)$ (over K), since it is the smallest field such that $f(x)$ splits into linear factors.

Corollary 1.2.5. *Any quadratic extension L/K (i.e., $[L : K] = 2$) is Galois.*

Proof. Write $L = K(\alpha)$ and $f(x)$ as the minimum polynomial for α over K. It is immediate from the quadratic formula that once L contains one root of $f(x)$, it contains the other. Hence L/K is Galois by the above theorem. □

Example 1.2.6. *Let $n > 0$. The splitting field for $f(x) = x^2 + n$ over $K = \mathbb{Q}$ is $L = \mathbb{Q}(\sqrt{-n})$. This also splits the quadratic form $x^2 + ny^2$. The extension L/K is Galois by the above corollary, and the Galois group is given by the maps $\sigma_1(a + b\sqrt{-n}) = a + b\sqrt{-n}$ and $\sigma_2(a + b\sqrt{-n}) = a - b\sqrt{-n}$. The map σ_1 corresponds to the trivial permutation of the roots $\pm\sqrt{-n}$ of $f(x)$, and σ_2 interchanges these two roots.*

Exercise 1.3. *Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. Determine the splitting polynomial $f(x)$ for $\alpha = \sqrt[3]{2}$ over K. Using the above theorem, answer the following. (i) Is L/K Galois? If not, find the Galois closure. (ii) Determine $\mathrm{Gal}(L/K)$ explicitly (either as embeddings or permutations of roots of $f(x)$.*

All of the above is covered in any standard lectures on Galois theory (though we haven't stated the main theorems of Galois theory), but now we will be introducing notions that are more properly a part of a course on Algebraic Number Theory.

Definition 1.2.7. *Let $\alpha \in L$. The **conjugates** of α in L/K are the elements $\alpha^\sigma = \sigma(\alpha)$ where $\sigma \in \mathrm{Gal}(L/K)$. The **norm** of α from L to K is $N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \alpha^\sigma$ and the **trace** of α from L to K is $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \alpha^\sigma$.*

In the case $K = \mathbb{Q}$ and L is understood, we simply write $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ for $N_{L/K}(\alpha)$ and $\mathrm{Tr}_{L/K}(\alpha)$. It is a standard fact from Galois theory that $\alpha \in L$ in fact lies in K if and only if $\alpha^\sigma = \alpha$ for each $\sigma \in \mathrm{Gal}(L/K)$.

Warning: If L/K is not Galois, then the conjugates of α in L/K may not lie in L. Precisely, if L/K is not Galois, then there exist $\sigma \in \mathrm{Gal}(L/K)$ such that the image of σ is not contained in L. Hence there is some $\alpha \in L$ such that the conjugate $\sigma(L) \notin L$. What is true is that they always lie in the Galois closure L' of L, by definition of the Galois closure.

Example 1.2.8. *Let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. For $\alpha = a + b\sqrt{d} \in L$, $N_{L/K}(\alpha) = N(\alpha) = a^2 - db^2$ and $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(\alpha) = 2a$.*

Lemma 1.2.9. *The norm map is multiplicative and the trace map is additive. For $\alpha \in L$, $N_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha) \in K$. Further, if $\alpha \in \mathcal{O}_L$, then $N_{L/K}(\alpha) \in \mathcal{O}_K$ and $\mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$.*

Proof. The first statement is immediate from the definitions. The second statement is true since the product and sum of all the conjugates of α are invariant under $\mathrm{Gal}(L/K)$, and therefore lie in K. For the last statement, observe α is an algebraic integer if and only if each of its conjugates are (since they all have the same minimum polynomial). □

Corollary 1.2.10. *Let α be an algebraic number of degree 2 and $L = \mathbb{Q}(\alpha)$. Then α is an algebraic integer if and only if $N_{L/\mathbb{Q}}(\alpha), \mathrm{Tr}_{L/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Proof. The $\Rightarrow$ direction follows from the lemma. The other direction follows from the fact that the minimum polynomial of α is $x^2 - \mathrm{Tr}_{L/\mathbb{Q}}(\alpha)x + N_{L/\mathbb{Q}}(\alpha)$, which was an exercise last semester. □

Note that this is not true for algebraic numbers of higher degree. In general if α is of degree n, one needs to consider the symmetric functions $\tau_j : L \to \mathbb{Q}$ where $L = \mathbb{Q}(\alpha)$ and $\tau_j(x)$ is the sum of all products of j conjugates. For instance if $x_1 = x, x_2, \ldots, x_n$ denote the n conjugates (not necessarily distinct numbers) of x, then

$$\begin{aligned}
\tau_1(x) =& x_1 + x_2 + \ldots + x_n = \mathrm{Tr}_{L/\mathbb{Q}}(x) \\
\tau_2(x) =& x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots x_2x_n + \cdots + x_{n-1}x_n \\
&\vdots \\
\tau_n(x) =& x_1x_2\cdots x_n = N_{L/\mathbb{Q}}(x).
\end{aligned}$$

Then one can show the minimum polynomial for α is

$$x^n + (-1)^{n-1}\tau_1(\alpha)x^{n-1} + \cdots - \tau_{n-1}(\alpha)x + \tau_n(\alpha).$$

Exercise 1.4. *Suppose $\alpha, \beta \in L$ are conjugates in L/K. Show $N_{L/K}(\alpha) = N_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}_{L/K}(\beta)$.*

Exercise 1.5. *Let $\alpha \in \mathcal{O}_K$. Prove α is a unit of $\mathcal{O}_K$ if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Exercise 1.6. *Write down a $\mathbb{Q}$-basis for $K = \mathbb{Q}(\sqrt[3]{2})$. For each α in this basis, compute $N_{K/\mathbb{Q}}(\alpha)$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$.*

Exercise 1.7. *Let $K = \mathbb{Q}(\sqrt{2})$ and $L = K(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Write down a $\mathbb{Q}$-basis for L. Compute $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/\mathbb{Q})$. (Hint for those who haven't seen Galois theory before: it's not so easy to find a primitive element for $L/\mathbb{Q}$ and determine its minimum polynomial, so it's better to just use the definition of the Galois group. Of course, if you know Galois theory, there are other ways to determine $\mathrm{Gal}(L/\mathbb{Q})$ and you may do it any you like.) For each α in this basis compute $N_{L/K}(\alpha)$ and $N_{L/Q}(\alpha)$. Check that $N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(N_{L/K}(\alpha))$.*

One thing you may have noticed in the examples and exercises above is that $\mathrm{Gal}(L/K)$ tends to equal $[L : K]$. In fact this is always true and is one of the standard results in Galois theory, though you may have only proved it for Galois extensions.

Proposition 1.2.11. $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof. Write $L = K(\alpha)$. Then $1, \alpha, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for K. Thus an embedding $\sigma : L \to \mathbb{C}$ which fixes every element of K is determined by what it does to α.

Let $f(x)$ be the minimum polynomial of α, which has degree $n = [L : K]$. Since σ is a field homomorphism, $\sigma(\alpha)$ must also have minimum polynomial $f(x)$. Since $f(x)$ has n distinct roots, $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, there are n possibilities for $\sigma \in \mathrm{Gal}(L/K)$ given by $\sigma(\alpha) = \alpha_i$. One formally checks that each of these give an embedding into $\mathbb{C}$. □

1.3 Discriminants

Let K be a number field, $n = [K : \mathbb{Q}]$. Then $|\mathrm{Gal}(K/\mathbb{Q})| = n$. Write $\mathrm{Gal}(K/\mathbb{Q}) = \{\alpha_1, \ldots, \alpha_n\}$.

Definition 1.3.1. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis for K. The* **discriminant** *of $\{\alpha_1, \ldots, \alpha_n\}$ is*

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det\left(\sigma_i(\alpha_j)\right)^2 .$$

If $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, we define the **discriminant** *of K to be $\Delta_K = \Delta[\alpha_1, \ldots, \alpha_n]$.*

If R is a ring, we define the $M_n(R)$ to be the set of $n \times n$ matrices with coefficients in R. This is also a ring, with the obvious identity element, and the invertible elements of $M_n(R)$ form a group under multiplication, denoted by $\mathrm{GL}_n(R)$, and called the **general linear group** of rank n over R. If R is an integral domain, then $A \in M_n(R)$ lies in $\mathrm{GL}_n(R)$ if and only if $\det(A)$ is a unit in R.

Lemma 1.3.2. *Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ be two $\mathbb{Q}$-bases for K. Then we can write*

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

for some $C \in \mathrm{GL}_n(\mathbb{Q})$. Then $\Delta[\beta_1, \ldots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n]$.

Further, if $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are $\mathbb{Z}$-bases (also called **integral bases***) for $\mathcal{O}_K$, then we may take $C \in \mathrm{GL}_n(\mathbb{Z})$. in the above. Consequently, $\Delta[\beta_1, \ldots, \beta_n] = \Delta[\alpha_1, \ldots, \alpha_n]$, i.e., Δ_K does not depend on the choice of the integral basis for $\mathcal{O}_K$.*

Proof. The fact that there is some such C is elementary linear algebra. The equation about determinants follows from $(\sigma_i(\beta_j)) = C\,(\sigma_i(\alpha_j))$, which holds because each σ_i fixes $\mathbb{Q}$. (If this isn't clear to you, just write out the equations $\beta_k = \sum c_{jk}\alpha_j$ for, say $n = 2$ or 3, and apply each σ_i.)

The second paragraph follows in the same way. Here we note that if $C \in \mathrm{GL}_n(\mathbb{Z})$, then $\det(C) = \pm 1$, so $\det(C)^2 = 1$. This provides at least one explanation for why we look at the *square* of the determinant in the definition of the discriminant—so that we can define Δ_K as an invariant of a number field, independent of choice of basis for $\mathcal{O}_K$. □

Exercise 1.8. *A priori, the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is defined for an* ordered *$\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K. Show that the above lemma implies this discriminant does not depend upon the order, i.e., for any $\tau \in S_n$, show $\Delta[\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}] = \Delta[\alpha_1, \ldots, \alpha_n]$.*

Note: the quantity $\det(\sigma_i(\alpha_j))$, which is one of the square roots of the discriminant, is called the **different** of $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. We will not use the different in this course (I don't think), but you may see come up if it you look at other texts.

A note on terminology: one can form the different and discriminant for an arbitrary collection of n integers $\alpha_1, \ldots, \alpha_n$. Then the discriminant and different are nonzero if and only if $\alpha_1, \ldots, \alpha_n$ are linearly independent, i.e., form a $\mathbb{Q}$-basis for K. Furthermore, if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ have different discriminants then the *submodules* $M = \{\sum n_i\alpha_i : n_i \in \mathbb{Z}\}$ and $N = \{\sum n_i\beta_i : n_i \in \mathbb{Z}\}$ are distinct.

Example 1.3.3. *Let $d \neq 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Suppose $d \equiv 2, 3 \bmod 4$ so $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. We can take $\{\alpha_1, \alpha_2\} = \left\{1, \sqrt{d}\right\}$ as a choice for an integral basis for $\mathcal{O}_K$. We can write* $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2\}$ *where σ_1 is trivial and σ_2 permutes $\sqrt{d}$ and $-\sqrt{d}$. Hence the matrix*

$$(\sigma_i(\alpha_j)) = \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix},$$

which has determinant $-2\sqrt{d}$. Hence the discriminant of K is $\Delta_K = \Delta[1, \sqrt{d}] = 4d$.

Exercise 1.9. *Let $d \neq 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Suppose $d \equiv 1 \bmod 4$. Compute the discriminant Δ_K of K.*

Lemma 1.3.4. *Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q} \setminus \{0\}$. If $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$, then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z} \setminus \{0\}$.*

Proof. By the previous lemma, the discriminants of any two bases for K differ by rational squares. Hence it suffices to check that it is true for a single $\mathbb{Q}$-basis of K. Then the second statement follows from the first, since the discriminant is then a polynomial expression of algebraic integers, and thus an algebraic integer itself.

We can write $K = \mathbb{Q}(\alpha)$ where α is some algebraic number (integer if we like) of degree n. Then $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right\}$ is a $\mathbb{Q}$-basis for K. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ denote the (distinct) conjugates of α. Then the conjugates of α^i are $\alpha_1^i = \alpha^i, \alpha_2^i, \ldots, \alpha_n^i$. Hence the determinant of this basis is the square of the discriminant of

$$A = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

This matrix is a Vandermonde matrix, and it is a standard algebra exercise that this has determinant $\prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$. (The determinant is a polynomial in the α_i's, and clearly it is zero if some $\alpha_i = \alpha_j$, so each polynomial $\alpha_j - \alpha_i$ divides the determinant. Then one counts the degree of the polynomial, to show that this is correct up to a constant. Comparing coefficients of one of the terms gives the Vandermonde determinant formula. You could also prove this by induction, but the above argument seems simpler.)

Hence $\Delta[\alpha_1, \ldots, \alpha_n] = \prod_{i \neq j} (\alpha_j - \alpha_i)$. Note any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ simply permutes the terms in this product, i.e., $\Delta[\alpha_1, \ldots, \alpha_n]$ is $\mathrm{Gal}(K/\mathbb{Q})$-invariant, and thus in $\mathbb{Q}$. It is clear from the product expression that it is nonzero. □

Exercise 1.10. *Verify the Vandermonde determinant formula given above for $n = 2$ and $n = 3$.*

While, the determination of $\mathcal{O}_K$ was simple for quadratic fields K, in general it is not so easy. There are algorithms to determine $\mathcal{O}_K$, but we will not focus on this problem in general, as we will only need explicit determinations of $\mathcal{O}_K$ in special cases. However, we will briefly indicate how one can use discriminants to help find a ring of integers. It suffices to find an integral basis for $\mathcal{O}_K$.

1. Guess a possible integral basis $\{\beta_1, \cdots, \beta_n\}$ for $\mathcal{O}_K$. Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is an actual integral basis for $\mathcal{O}_K$. Then $\Delta[\beta_1, \cdots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta_K$. In other words,

$\Delta[\beta_1, \cdots, \beta_n]$ is a square (in $\mathbb{Z}$) times Δ_K. Hence if $\Delta[\beta_1, \dots, \beta_n]$ is squarefree, then $\{\beta_1, \dots, \beta_n\}$ is an integral basis for $\mathcal{O}_K$.

2. If $\Delta[\beta_1, \cdots, \beta_n]$ is not squarefree, $\{\beta_1, \cdots, \beta_n\}$ may still be a basis (see Example 1.3.3 above), but if it is not, then $\mathcal{O}_K$ contains an integer of the form $\frac{1}{p}(c_1\beta_1 + c_2\beta_2 + \cdots + c_n\beta_n)$ for some $c_n \in \mathbb{Z}$ and p is some prime such that $p^2|\Delta[\beta_1, \cdots, \beta_n]$. Check to see if any numbers of this form give any new algebraic integers not generated by $\beta_1, \dots, \beta_n$. If so, suitably modify the choice of $\beta_1, \dots, \beta_n$ and repeat. If not, then $\beta_1, \dots, \beta_n$ is an integral basis of $\mathcal{O}_K$.

Exercise 1.11. *In the last section, we considered general extensions of number fields L/K. One reason you might want to do this is the following. We want to use $K = \mathbb{Q}(\sqrt{-5})$ to study the form $x^2 + 5y^2$. However $\mathcal{O}_K$ does not have unique factorization. But we can embed K in the field $L = \mathbb{Q}(\sqrt{-5}, i)$ which does have unique factorization. Now one wants do determine $\mathcal{O}_L$. A first guess might be $\{1, \sqrt{-5}, i, \sqrt{5}\}$ is an integral basis for $\mathcal{O}_L$. It is certainly a $\mathbb{Q}$-basis for L. Compute the discriminant of this $\mathbb{Q}$-basis. Can you determine $\mathcal{O}_L$?*

However we will primarily be concerned with other applications of discriminants this semester, most immediately to ideals in the next section.

Discriminants are a fundamental invariant of number fields. Another thing they provide is natural way to at least partially order number fields. (There are only finitely many fields of a fixed discriminant.) The quadratic fields $\mathbb{Q}(\sqrt{d})$ can easily be ordered by d (which actually is a function of the discriminant, but how can one order fields of a more complicated form, such as $\mathbb{Q}(\sqrt{3}, \sqrt{-19})$ and $\mathbb{Q}(\sqrt{-7}, \sqrt{11})$?) Once one has some sort of ordering, it is meaningful to ask questions like what percentage of fields (of a certain type) have class number 1 or 2, or more generally, how many fields up to a certain point satisfy Property X?

We also remark that there is a geometric interpretation of determinants (and differents), which comes from the geometric interpretation of discriminants. For now, we will just mention it in the simplest case $K = \mathbb{Q}(\sqrt{-d})$ where $d > 0$ squarefree. Then if α, β is a $\mathbb{Q}$-basis for K, α and β generate a lattice $\Lambda = \langle \alpha, \beta \rangle = \{m\alpha + n\beta : m, n \in \mathbb{Z}\}$. Then $\mathrm{vol}(\mathbb{C}/\Lambda) = \frac{1}{2}\sqrt{-\Delta[\alpha, \beta]}$. In particular, $\Delta_K = -4\mathrm{vol}(\mathbb{C}/\mathcal{O}_K)^2$. We can state an analogue of this for arbitrary number fields when we study the *geometry of numbers.*

1.4 Ideals

Let K be a number field. Recall $\mathcal{I}$ is an **ideal** of $\mathcal{O}_K$ if $\mathcal{I}$ is a nonempty subset of $\mathcal{O}_K$ which is closed under addition and multiplication by $\mathcal{O}_K$. The **norm** of an ideal $\mathcal{I}$ of $\mathcal{O}_K$ is $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$.

Lemma 1.4.1. *For any nonzero ideal $\mathcal{I}$ of $\mathcal{O}_K$, the norm $N(\mathcal{I}) = |\mathcal{O}_K/\mathcal{I}|$ is always finite. Furthermore, if $\beta_1, \dots, \beta_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, then $N(\mathcal{I}) = \sqrt{\frac{\Delta[\beta_1, \dots, \beta_n]}{\Delta_K}}$.*

Recall a **free abelian group of rank** n is a group isomorphic to $\mathbb{Z}^n$. For the proof, we use the fact that if A is a free abelian group of rank n, and B is a subgroup of A, then B is also free abelian of rank $\leq n$.

Proof. Let $n = [K : \mathbb{Q}]$. Then $\mathcal{O}_K$ is a free abelian group of rank n (w.r.t. addition). We can regard $\mathcal{I}$ as a subgroup of $\mathcal{O}_K$, which must also be free of rank $\leq n$. Let $i \in \mathcal{I}$ be nonzero. Then $(\mathcal{O}_K i, +)$ is a (free abelian) subgroup of $(\mathcal{I}, +)$ of rank n, hence $\mathcal{I}$ has rank n.

Now we let $\beta_1, \cdots, \beta_n$ be a $\mathbb{Z}$-basis for $\mathcal{I}$. Then there is a $\mathbb{Z}$-basis $\alpha_1, \cdots, \alpha_n$ of $\mathcal{O}_K$ such that for each i we can write $\beta_i = c_i\alpha_i$ for some $c_i \in \mathbb{Z}$. Then it is clear $\mathcal{O}_K/\mathcal{I} = \prod C_{c_i}$, where C_r denotes the cyclic group of order r. In particular $N(\mathcal{I})$ is finite.

Moreover, we have

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_n \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

By Lemma 1.3.2, we have $\Delta[\beta_1, \ldots, \beta_n] = N(\mathcal{I})^2\Delta[\alpha_1, \ldots, \alpha_n] = N(\mathcal{I})^2\Delta_K$. This gives the result since $N(\mathcal{I}) \geq 0$. □

Note that the norm of the zero ideal is infinite as we have defined it, though it may make more sense to define it to be 0 in light of the the next result, which relates norms of ideals to norms of elements. In any case, since we have no particular reason to work with the zero ideal, in order to simplify statements we will **from here on, assume all our ideals our nonzero**, unless explicitly stated otherwise.

Proposition 1.4.2. *Suppose $\mathcal{I} = (\alpha)$ is a principal ideal of $\mathcal{O}_K$. Then $N(\mathcal{I}) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Here the norm on the left is the ideal norm, and the norm on the right is the norm of an element.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Then $\beta_1 = \alpha\alpha_1, \ldots, \beta_n = \alpha\alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{I}$. Write $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$. Note

$$\begin{aligned}
\Delta[\beta_1, \ldots, \beta_n] &= \det \begin{pmatrix} \sigma_1(\alpha)\sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha)\sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha)\sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha)\sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= \det \begin{pmatrix} \sigma_1(\alpha) & & & \\ & \sigma_2(\alpha) & & \\ & & \ddots & \\ & & & \sigma_n(\alpha) \end{pmatrix}^2 \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\
&= N_{K/\mathbb{Q}}(\alpha)^2\Delta[\alpha_1, \ldots, \alpha_n] = N_{K/\mathbb{Q}}(\alpha)^2\Delta_K.
\end{aligned}$$

Now apply the previous lemma. □

This implies that the ideal norm is multiplicative, at least for principal ideals. Of course, we want to know it's multiplicative for all ideals, and this basically follows from some simple isomorphism theorems, but at one point, to keep our argument as simple as possible, we will use fractional ideals. This is justified by Theorem 1.4.4 below (which we have already given last semester), whose proof does not rely on this result. Recall that the product of two ideals $\mathcal{I}$ and $\mathcal{J}$, is the ideal generated by all elements of the form ij for $i \in \mathcal{I}$ and $j \in \mathcal{J}$, i.e., $\mathcal{IJ} = \{\sum i_m j_m : i_m \in \mathcal{I}, j_m \in \mathcal{J}\}$.

Proposition 1.4.3. *Let $\mathcal{I}$, $\mathcal{J}$ be ideals of $\mathcal{O}_K$. Then $N(\mathcal{IJ}) = N(\mathcal{I})N(\mathcal{J})$.*

Proof. By the ring isomorphism theorem, $\mathcal{O}_K/\mathcal{I} \simeq (\mathcal{O}_K/\mathcal{I}\mathcal{J})/(\mathcal{I}/\mathcal{I}\mathcal{J})$. (Just think about the case where $\mathcal{O}_K = \mathbb{Z}, \mathcal{I} = (m), \mathcal{J} = (n)$. Then this says $\mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z})$.) The details are in the exercise below. Hence $N(\mathcal{I}\mathcal{J}) = |\mathcal{I}/\mathcal{I}\mathcal{J}| \cdot N(\mathcal{I})$.

Now it suffices to show $\mathcal{O}_K/\mathcal{J} \simeq \mathcal{I}/\mathcal{I}\mathcal{J}$, say as abelian groups. Consider the map $\phi : \mathcal{O}_K \to \mathcal{I}/\mathcal{I}\mathcal{J}$ given by $\phi(\alpha) = \alpha\mathcal{I} + \mathcal{I}\mathcal{J}$ for $\alpha \in \mathcal{O}_K$. It is clear it is a group homomorphism. Note $\phi(\alpha) = \mathcal{I}\mathcal{J} \iff \alpha\mathcal{I} + \mathcal{I}\mathcal{J} = \mathcal{I}\mathcal{J} \iff \alpha\mathcal{I} \subseteq \mathcal{I}\mathcal{J}$, which, multiplying by $\mathcal{I}^{-1}$ is equivalent to $\alpha\mathcal{O}_K \subseteq \mathcal{J}$, which is equivalent to $\alpha \in \mathcal{J}$. Hence $\ker(\phi) = \mathcal{J}$. On the other hand, it is clear ϕ is surjective. Thus it induces the desired isomorphism $\phi : \mathcal{O}_K/\mathcal{J} \to \mathcal{I}/\mathcal{I}\mathcal{J}$. □

Exercise 1.12. *Show the map $\phi : \mathcal{O}_K/\mathcal{I}\mathcal{J} \to \mathcal{O}_K/\mathcal{I}$ given by $\alpha + \mathcal{I}\mathcal{J} \mapsto \alpha + \mathcal{I}$ for $\alpha \in \mathcal{O}_K$ is well-defined (i.e., ϕ does not depend on the choice of coset representative $\alpha \in \alpha + \mathcal{I}\mathcal{J}$), has kernel $\mathcal{I}/\mathcal{I}\mathcal{J}$, and is surjective. This gives the isomorphism $\mathcal{O}_K/\mathcal{I} \simeq (\mathcal{O}_K/\mathcal{I}\mathcal{J})/(\mathcal{I}/\mathcal{I}\mathcal{J})$ claimed above.*

If $\mathcal{I} \subseteq K$ such that $a\mathcal{I}$ is an ideal of $\mathcal{O}_K$ for some $a \in \mathcal{O}_K$, we say $\mathcal{I}$ is a **fractional ideal** of $\mathcal{O}_K$. Moreover a fractional or ordinary ideal $\mathcal{I}$ is called **principal**, if it is generated by a single element, i.e., if it is of the form $a\mathcal{O}_K$ for some $a \in K$. Denote by $\mathrm{Frac}(\mathcal{O}_K)$ the set of (nonzero) fractional ideals of $\mathcal{O}_K$, and $\mathrm{Prin}(\mathcal{O}_K)$ the set of (nonzero) principal fractional ideals of $\mathcal{O}_K$. Multiplication for fractional ideals is defined the same as for ordinary ideals.

Theorem 1.4.4. $\mathrm{Frac}(\mathcal{O}_K)$ *is an abelian group under multiplication, and* $\mathrm{Prin}(\mathcal{O}_K)$ *is a subgroup.*

If $\mathcal{I}$, $\mathcal{J}$ are ideals of $\mathcal{O}_K$, we say $\mathcal{J}$ divides $\mathcal{I}$ ($\mathcal{J}|\mathcal{I}$) if $\mathcal{J} \supseteq \mathcal{I}$, from which one can conclude from the above theorem that $\mathcal{I} = \mathcal{J}\mathcal{J}'$ for some ideal $\mathcal{J}'$. An ideal $\mathcal{I}$ of $\mathcal{O}_K$ is **proper** if $\mathcal{I} \neq \mathcal{O}_K$. We say a proper ideal $\mathfrak{p}$ is **prime** if $\mathfrak{p}|\mathcal{I}\mathcal{J}$ implies $\mathfrak{p}|\mathcal{I}$ or $\mathfrak{p}|\mathcal{J}$ (technically, the zero ideal is prime, but we are ignoring the zero ideal), and it is **maximal** if $\mathcal{I}|\mathfrak{p}$ implies $\mathcal{I} = \mathfrak{p}$ or $\mathcal{I} = \mathcal{O}_K$.

Recall that $\mathfrak{p}$ is prime if and only if $\mathcal{O}_K/\mathfrak{p}$ is an integral domain, and $\mathfrak{p}$ is maximal if and only if $\mathcal{O}_K/\mathfrak{p}$ is a field. (Remark: this kind of result is one reason we don't allow for a field to have just one element.) Since every finite integral domain is a field, one is able to conclude every (nonzero) prime ideal is maximal and vice versa.

Theorem 1.4.5. (Prime ideal factorization) *Let $\mathcal{I}$ be a proper ideal of $\mathcal{O}_K$. Then $\mathcal{I} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ where the $\mathfrak{p}_i$'s are prime ideals of $\mathcal{O}_K$. Moreover the $\mathfrak{p}_i$'s are determined uniquely up to ordering.*

We proved these theorems last semester, modulo a couple of details about the first theorem. If you want to fill in these details for yourself, you can try to work it out yourself from the Chapter 12 notes from last semester, or see any text on Algebraic Number Theory, such as [Stewart–Tall].

Definition 1.4.6. *The quotient group* $\mathrm{Frac}(\mathcal{O}_K)/\mathrm{Prin}(\mathcal{O}_K)$ *is called the* **class group** *of K, and denoted $\mathcal{Cl}(\mathcal{O}_K)$ or $\mathcal{Cl}_K$. The size of the class group is called the* **class number** *of K, and denoted by h_K.*

Corollary 1.4.7. *$\mathcal{O}_K$ has unique factorization if and only if $h_K = 1$.*

Proof. Note $h_K = 1$ means $\mathcal{O}_K$ is a PID. Since every PID is a UFD (from algebra or last semester), the ⇐ direction holds.

To prove the ⇒ direction, suppose $\mathcal{O}_K$ has unique factorization. Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$. Let $n \in \mathfrak{p}$ and $n = \alpha_1 \cdots \alpha_k$ be unique factorization of n into (non-unit) irreducibles. Note each α_i satisfies the prime divisor property by unique factorization, each α_i is a prime element of $\mathcal{O}_K$, and therefore each (α_i) is a prime ideal. Hence $(n) = (\alpha_1)(\alpha_2)\cdots(\alpha_k)$ is the prime ideal factorization of (n).

On the other hand, since $\mathfrak{p}|(n)$, $\mathfrak{p}$ must equal one of the (α_i)'s by uniqueness of prime ideal factorization. Hence every prime ideal of $\mathcal{O}_K$ is principal. Then by prime ideal factorization again, every ideal must be principal. □

We mentioned last semester that there are only finitely many imaginary quadratic fields with unique factorization, and conjecturally infinitely many such real quadratic fields. We will a bit more talk more about this later, but first we need a way to compute the class group or class number of a field. In fact, perhaps even before that, we want to know the class number is finite. The standard proof for this is via Minkowski's theory of the *geometry of numbers*, and it will in fact give us a bound on the class number, which will in turn allow us to compute the class group in explicit examples. In fact, to get an idea of how one can do such a thing, you may want to look at the Chapter 12 notes from last semester, where, following Stillwell, I prove directly that $h_{\mathbb{Q}(\sqrt{-5})} = 2$, though we didn't have a chance to cover it in lecture last semester. The proof via Minkowski's theorem is somewhat less direct, and to keep things as simple as possible, we will only give a complete proof in the case of quadratic fields. A more sophisticated proof of the finiteness of the class group is via the theory of p-adic numbers and adèles which we will develop in Part III. Time permitting, we will give this proof in the 3rd part of the course for general number fields.

Another way to compute the class number is to use a formula of Dirichlet, which we will turn to after Minkowski's bound. An alternative way to compute the class number and group for quadratic fields will be given by Gauss's theory of binary quadratic forms in Part II (which historically came first).

1.5 Lattices

Before explaining Minkowski's geometry of numbers, we need to know some basic facts about lattices.

Definition 1.5.1. *A* **(complete) lattice** Λ *in* $\mathbb{R}^n$ *is a subset of* $\mathbb{R}^n$ *of the form* $\langle v_1, v_2, \ldots, v_n\rangle = \{\sum a_i v_i : a_i \in \mathbb{Z}\}$ *such that* $v_1, \ldots, v_n \in \mathbb{R}^n$ *are linearly independent over* $\mathbb{R}$*. The set* $v_1, \ldots, v_n$ *is called a* **basis** *for* Λ *(it is a* $\mathbb{Z}$*-basis). As both* $\mathbb{R}^n$ *and* Λ *are abelian groups under addition, we let* $\mathbb{R}^n/\Lambda$ *denote the quotient group. A* **fundamental domain** *for* Λ *(or* $\mathbb{R}^n/\Lambda$*) is a connected, locally convex*[1] Ω *of* $\mathbb{R}^n$ *such that* Ω *contains exactly one element from each coset of* $\mathbb{R}^n/\Lambda$*.*

In other words, the (complete) lattices in $\mathbb{R}^n$ are the $\mathbb{Z}$-spans of bases of $\mathbb{R}^n$. The adjective complete refers to the fact that the number of basis elements of the lattice is maximal. An incomplete lattice of $\mathbb{R}^n$ would be the $\mathbb{Z}$-span of a basis of a proper subspace of $\mathbb{R}^n$. However, for us, all lattices will be complete unless stated otherwise.

Note a lattice is a free abelian subgroup of $\mathbb{R}^n$ of rank n, but not all free abelian subgroups of rank n are lattices. For example, $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R}$ is a free abelian subgroup of $\mathbb{R}^2$ of rank 2 (embedding $\mathbb{R}$ in $\mathbb{R}^2$), generated by 1 and $\sqrt{2}$, but not a lattice since 1 and $\sqrt{2}$ are not linearly independent over $\mathbb{R}$.

The main idea with fundamental domain is that it is a subset of $\mathbb{R}^n$ which looks like the quotient group $\mathbb{R}^n/\Lambda$. More precisely, it is a connected subset of $\mathbb{R}^n$ comprising exactly one representative from each coset of $\mathbb{R}^n/\Lambda$. The condition of local convexity is just to avoid pathological examples of

[1] Locally convex means if two "nearby" points are in the set, then the line between them is in the set.

fundamental domains (see examples below). In any case, it won't be important for us to understand the subtleties of what kinds of sets make up fundamental domains, but rather just the basic idea of what one is, and understanding what the "standard" fundamental domain is. Hopefully this should be clear when we look at the cases in $\mathbb{R}^1$ and $\mathbb{R}^2$.

It is a basic fact that any fundamental domain for Λ has the same volume (length in dimension 1, area in dimension 2). This volume is called the **volume** (or **covolume**) of the lattice Λ (or more properly the quotient $\mathbb{R}/\Lambda_n$), denoted $\mathrm{vol}(\Lambda)$ (or more properly $\mathrm{vol}(\mathbb{R}^n/\Lambda)$). (To be formally complete, we can get away without proving this fact about all fundamental domains having the same volume by defining the volume of the lattice to be the volume of the standard fundamental domain, defined below.) If Λ is an incomplete lattice, then $\mathbb{R}^n/\Lambda$ will have will have infinite volume.

Example 1.5.2. *Since any free abelian group of rank n is isomorphic, as an abelian group, to $\mathbb{Z}^n$, the most obvious example of a lattice in $\mathbb{R}^n$ is $\mathbb{Z}^n$. The standard fundamental domain for $\mathbb{Z}^n$ is $\Omega = [0,1)^n \subseteq \mathbb{R}^n$. It should be clear any element of $\mathbb{R}^n$ is a $\mathbb{Z}^n$ translate of exactly one element in Ω. It is obviously connected and convex, therefore locally convex. It is clear* $\mathrm{vol}(\Lambda) = 1$.

While all lattices of $\mathbb{R}^n$ are isomorphic as abelian groups, they also have an inherent geometry coming from $\mathbb{R}^n$, providing more structure. We will not need this, but just to clear up terminology, we will only say two lattices of $\mathbb{R}^n$ are isomorphic *as lattices* if they (or equivalently, their fundamental domains) have the same shape and size—precisely, they will be isomorphic if one is the image of the other by an isometry (distance preserving map) of $\mathbb{R}^n$. In linear algebra, you may have learned that the (linear) isometries of $\mathbb{R}^n$ are precisely the elements of $\mathrm{O}(n) = \left\{A \in \mathrm{GL}_n(\mathbb{R}) : A^t A = I\right\}$, the *real orthogonal group of rank n*. This means that two lattices of $\mathbb{R}^n$ are isomorphic if and only if (a basis of) one can be transformed into (a basis of) the other by an element of $\mathrm{O}(n)$.

Example 1.5.3. *As a special case of the above example with $n = 1$, $\mathbb{Z}$ is a lattice in $\mathbb{R}$, as is $\Lambda_k = k\mathbb{Z}$. Notice that $\Lambda_k = \Lambda_{k'}$ if and only if $k = -k'$. These are all the lattices in $\mathbb{R}$, in $1-1$ correspondence with $\mathbb{R}_{>0}$, parameterized by this number k. A fundamental domain for $\mathbb{R}/\Lambda_k$ (sometimes also referred to as $\mathbb{R} \bmod k$) is $[0,k)$. In fact any half-open interval of length k is a fundamental domain for Λ_k, and there are no other fundamental domains because of the connectedness requirement. We think of $\mathbb{R}/\Lambda_k$ as the interval $[0,k]$ with the endpoints glued, hence topologically it is a circle. Geometrically, its length is* $\mathrm{vol}(\Lambda_k) = k$.

Example 1.5.4. *A lattice in $\mathbb{R}^2$ is determined by two generators, $u = (x_1, y_1)$ and $v = (x_2, y_2)$, provided they are linearly independent. Precisely, the lattice $\Lambda = \langle u, v\rangle$ generated by u and v is $\Lambda = \{mu + nv : m, n \in \mathbb{Z}\} \subseteq \mathbb{R}^2$. The standard fundamental domain for Λ is $\Omega = \{au + bv : a, b \in [0,1)\}$. In other words, the standard fundamental domain for Λ is the interior of the parallelogram determined by 0, u, v and $u+v$, together with half of the boundary (since opposite boundary points are equivalent modulo Λ, we can only include half of them, and one of the corners). Any $\mathbb{R}^2$-translate of Ω is also a fundamental domain for Λ.*

We may think of the quotient group $\mathbb{R}^2/\Lambda$ as the fundamental domain (parallelogram) Ω, with the addition of two vectors being the sum in the fundamental domain, and if the vector lies outside of Ω, we let it wrap it around the edges of the parallelogram Pacman-style so the sum lies again in Ω. In other words, we think of $\mathbb{R}^2/\Lambda$ as the parallelogram Ω, with opposite sides glued. Topologically this is a torus.

Example 1.5.5. *Let $a, b > 0$. The volume of the lattice $\Lambda_{a,b} = \langle (a,0), (0,b)\rangle$ is ab, since a fundamental domain is a rectangle with corners $0, (a,0), (0,b), (a,b)$ (excluding appropriate boundary points). Two of these rectangular lattices $\Lambda_{a,b}$ and $\Lambda_{c,d}$ will be isomorphic if and only if*

$\{a,b\} = \{c,d\}$. *Hence there are infinitely many non-isomorphic rectangular lattices of volume* 1 *given by* $\Lambda_{a,\frac{1}{a}}$.

To generalize the above examples, the **standard fundamental domain** for $\Lambda = \langle v_1, v_2 \dots, v_n\rangle$ (or more properly for the basis $v_1, \dots, v_n$) is $\Omega = \{\sum a_i v_i : a_i \in [0,1)\}$. It is straightforward to show this is in fact a fundamental domain. Then $\mathbb{R}^n/\Lambda$ looks like an n-dimensional parallelogram (parallelopiped?) and topologically is an n-dimensional torus (the product of n circles). (To be complete, if we define volume of a lattice as the volume of a standard fundamental domain, one should show that any two bases of Λ are related by an element of $\mathrm{GL}_n(\mathbb{Z})$. Then, expressing the volumes of standard fundamental domains as determinants, one can conclude that the volume is independent of the choice of basis.)

Exercise 1.13. *Consider the lattice* $\Lambda = \langle u = (1,0), v = (\frac{1}{2}, \frac{\sqrt{3}}{2})\rangle$ *in* $\mathbb{R}^2$. *Sketch the standard fundamental domain for* $\{u,v\}$ *compute its volume. Write down* 2 *other bases* $\{u_1,v_1\}$, $\{u_2,v_2\}$ *for* Λ *that do not just differ by sign (i.e.,* $\{u,v\} \neq \{\pm u_i, \pm v_i\}$ *and* $\{u_1,v_1\} \neq \{u_2,v_2\}$*). Sketch the standard fundamental domains for* $\{u_1,v_1\}$ *and* $\{u_2,v_2\}$ *and check they have the same volume.*

Exercise 1.14. *Let* $\Lambda = \langle u, v\rangle$ *be a lattice in* $\mathbb{R}^2$ *such that* $\Lambda \subseteq \mathbb{Z}^2$. *Let* Ω *be the standard fundamental domain for the basis* $\{u,v\}$ *of* Λ. *Show the volume of* $\mathbb{R}^2/\Lambda$ *is the number of integral points in* Ω, *i.e.,* $\mathrm{vol}(\mathbb{R}^2/\Lambda) = |\Omega \cap \mathbb{Z}^2|$.

Example 1.5.6. *Consider the lattice* $\mathbb{Z}^2$ *in* $\mathbb{R}^2$. *A non-rectangular fundamental domain may be constructed as follows. Start with a standard fundamental domain and remove a semicirclular shape from one of the sides, then glue this shape onto the opposite side. (Draw a picture). This is no longer convex, but it is still locally convex.*

Now here is a non-example of a fundamental domain, which satisfies all properties except local convexity. Let Ω *be the union of line segments* L_y *for* $0 \le y < 1$ *where* L_y *is the line from* $(0,y)$ *(inclusive) to* $(1,y)$ *(exclusive) if* y *is rational and to* $(-1,y)$ *(exclusive) if* y *is irrational. Then it is clear* Ω *contains exactly one representative from each coset of* $\mathbb{R}^2/\mathbb{Z}^2$, *and it is connected since it is a union of horizontal line segments which are joined by the* y *axis, but it is not locally convex. (Think why, draw a picture.)*

Now to apply this to ideal theory, we need to know Minkowski's Theorem. Recall $X \subseteq \mathbb{R}^n$ is called **symmetric** if $X = -X$.

Theorem 1.5.7. (Minkowski) *Let* Λ *be a lattice in* $\mathbb{R}^n$ *and* X *a bounded symmetric convex subset of* $\mathbb{R}^n$. *If* $\mathrm{vol}(X) > 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$, *then* X *contains a nonzero point of* Λ.

Proof. (It may be helpful to draw a picture for $n = 2$.) Let L be the lattice $L = 2\Lambda$. It is clear $\mathrm{vol}(\mathbb{R}^n/L) = 2^n\mathrm{vol}(\mathbb{R}^n/\Lambda)$, so $\mathrm{vol}(X) > \mathrm{vol}(\mathbb{R}^n/L)$. Thus, if Ω is a fundamental domain for $\mathbb{R}^n/L$, the natural map from $\mathbb{R}^n$ to Ω cannot be injective when restricted to X. Thus there must be two points $x_1, x_2 \in X$ such that $x_1 \equiv x_2 \bmod L$ (i.e., they map to the same point in Ω), i.e., $x_1 - x_2 \in L$. Since X is symmetric $-x_2 \in X$. Then convexity implies $0 \neq \frac{1}{2}x_1 - \frac{1}{2}x_2 \in X \cap \Lambda$. □

Two classical applications of Minkowski's theorem is that is can be used to prove Fermat's two square theorem or Lagrange's four square theorem. See [Stewart–Tall] for both proofs, or the Chapter 8 notes from last semester for the proof of the four square theorem. However, we are more interested in the applications to ideals in the following sections.

1.6 The geometry of numbers: the quadratic case

What Minkowski termed the geometry of numbers is most plain to see in the imaginary quadratic case. Let $K = \mathbb{Q}(\sqrt{-d})$ with $d > 0$ squarefree. Then $\mathcal{O}_K$ is a lattice in $\mathbb{C} \simeq \mathbb{R}^2$. Hence, any ideal of $\mathcal{O}_K$ is a lattice in $\mathbb{C} \simeq \mathbb{R}^2$.

In fact, even if $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, we may think of $\mathcal{O}_K$ as a lattice in $\mathbb{R}^2$. (As we remarked earlier with $\mathbb{Z}[\sqrt{2}]$, even though $K \subseteq \mathbb{R}$, $\mathcal{O}_K$ is not a lattice in $\mathbb{R}$, so Minkowski's idea was to embed K into $\mathbb{R}^2$.) The most naive way to do this is to regard an element $a + b\sqrt{d} \in K$ as the element $(a, b\sqrt{d})$ in $\mathbb{R}^2$. In other words, we are separating out the rational and irrational components on the x- and y- axes of $\mathbb{R}^2$, just like we separate the real and imaginary components of $\mathbb{Q}(\sqrt{-d})$ or $\mathbb{C}$ onto the x- and y- axes in the complex plane picture.

We can unify these two cases as follows. Suppose $K = \mathbb{Q}(\sqrt{d})$ is a real or imaginary quadratic field, i.e., $d > 1$ or $d < 0$ and assume d squarefree. Then we can embed K in $\mathbb{R}^2$ by the map $\phi : K \to \mathbb{R}^2$ such that $\phi(a + b\sqrt{d}) = (a, b\sqrt{|d|})$ for $a, b \in \mathbb{Q}$. In this picture $\mathcal{O}_K$, and thus any ideal of $\mathcal{O}_K$, is a lattice of $\mathbb{R}^2$.

We will work out the part of Minkowski's theory relevant for us in the case of quadratic fields. In the interest of time, we will just state the theorems in the general case, though the basic argument is the same.

Proposition 1.6.1. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$ with $\mathbb{Z}$-basis $\{\alpha, \beta\}$, regarded as a lattice in $\mathbb{R}^2$ via the embedding $\phi : K \to \mathbb{R}^2$ above. Then* $\mathrm{vol}(\mathbb{R}^2/\mathcal{I}) = \frac{1}{2}|\Delta[\alpha, \beta]|^{1/2}$.

In the case where K is imaginary quadratic and $\mathcal{I} = \mathcal{O}_K$, we briefly discussed this at the end of the section on discriminants.

Proof. Let $(x_1, y_1) = \phi(\alpha)$ and $(x_2, y_2) = \phi(\beta)$, so we can write $\alpha = x_1 + \frac{y_1}{\sqrt{|d|}}\sqrt{d}$ and $\beta = x_2 + \frac{y_2}{\sqrt{|d|}}\sqrt{d}$. Note $\Delta[\alpha, \beta] = \alpha\overline{\beta} - \overline{\alpha}\beta$. Since $\alpha\overline{\beta} = x_1x_2 + \frac{d}{|d|}y_1y_2 + (x_1y_2 + x_2y_1)\frac{\sqrt{d}}{\sqrt{|d|}}$, we have $|\Delta[\alpha, \beta]|^{1/2} = 2|x_1y_2 - x_2y_1|$. By the exercise below, this is twice the volume of the parallelogram with corners $(0, 0)$, (x_1, y_1), (x_2, y_2) and (x_1+x_2, y_1+y_2), which is the standard fundamental domain of the lattice $\mathcal{I} \subseteq \mathbb{R}^2$ (with respect to the basis $(x_1, y_1), (x_2, y_2)$). □

Exercise 1.15. *Let $u = (x_1, y_1)$ and $v = (x_2, y_2)$ be linearly independent vectors in $\mathbb{R}^2$. Show the parallelogram with corners 0, u, v and $u + v$ has area $|x_1y_2 - x_2y_1|$.*

Corollary 1.6.2. *With the notation of the previous proposition,* $\mathrm{vol}(\mathbb{R}^2/\mathcal{I}) = \frac{1}{2}N(\mathcal{I})\sqrt{|\Delta_K|}$.

This gives a geometric interpretation of the norm of an ideal in terms of the volume of the corresponding lattice.

Proof. This is immediate since $N(\mathcal{I}) = \sqrt{\frac{\Delta[\alpha,\beta]}{\Delta_K}}$ (Lemma 1.4.1.) □

Lemma 1.6.3. *For any ideal $\mathcal{I}$ of $\mathcal{O}_K$, there is a nonzero $\alpha \in \mathcal{I}$ such that*

$$|N(\alpha)| \leq \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|}.$$

Proof. From the previous corollary, Minkowski's theorem implies that if X is the (open) disc of radius r centered at the origin in $\mathbb{R}^2$, it contains a nonzero lattice point, i.e., a nonzero $\alpha \in \mathcal{I}$, whenever $\pi r^2 > 2N(\mathcal{I})\sqrt{|\Delta_K|}$. Suppose $r^2 > \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|} + \epsilon$ for some $\epsilon > 0$ so there is such an α.

Now if we write $\alpha = x + \frac{y}{\sqrt{|d|}}\sqrt{d}$, we see $N(\alpha) = x^2 \pm y^2$ according to whether K is imaginary quadratic or real quadratic. Now $\alpha \in X$ means $x^2 + y^2 < r^2$, which of course implies $|x^2 - y^2| < r^2$, so in either the imaginary or real case we have $|N(\alpha)| < r^2 = \frac{2}{\pi}N(\mathcal{I})\sqrt{|\Delta_K|} + \epsilon$. Taking $\epsilon \to 0$ gives the desired result. □

Recall if $\mathcal{I}, \mathcal{J}$ are fractional or ordinary ideals of a ring R, we say $\mathcal{I}$ and $\mathcal{J}$ are **equivalent** if $a\mathcal{I} = b\mathcal{J}$ for some $a, b \in R$ and write $\mathcal{I} \sim \mathcal{J}$. Via this equivalence, the class group of R (which we technically have only defined when R is the ring of integers of a number field) is just the group of equivalence classes of fractional ideals.

Lemma 1.6.4. *Let $\mathcal{I}$ be an ideal of $\mathcal{O}_K$. Then $\mathcal{I} \sim \mathcal{J}$ for some ideal $\mathcal{J}$ with norm $\leq \frac{2}{\pi}\sqrt{|\Delta_K|}$.*

Proof. For some $a \in \mathcal{O}_K$, $a\mathcal{I}^{-1} \subseteq \mathcal{O}_K$. Then $\mathcal{I}' = a\mathcal{I}^{-1}$ is a ideal of $\mathcal{O}_K$ such that $\mathcal{I}\mathcal{I}' = (a)$. Let $\alpha \in \mathcal{I}'$ such that $|N(\alpha)| \leq \frac{2}{\pi}N(\mathcal{I}')\sqrt{|\Delta_K|}$, whose existence is guaranteed by the previous lemma. Clearly $\mathcal{I}'|(\alpha)$ so we can write $(\alpha) = \mathcal{I}'\mathcal{J}$ where $\mathcal{J}$ is an ideal of $\mathcal{O}_K$. Now we are done, since $\mathcal{J} \sim \mathcal{I}'^{-1} \sim \mathcal{I}$ and $N(\mathcal{J}) = N(\mathcal{I}')/N((\alpha)) \leq \frac{2}{\pi}\sqrt{|\Delta_K|}$. □

The point is that this lemma allows us to bound, and subsequently determine, the class number in any explicit case, as well as use this to show it is finite in general. Let's first start of with our canonical example. Recall from Section , for $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ squarefree, the discriminant $\Delta_K = d$ if $d \equiv 1 \bmod 4$ and $\Delta_K = 4d$ if $d \equiv 2, 3 \bmod 4$.

Example 1.6.5. *The class number of $K = \mathbb{Q}(\sqrt{-5})$ is 2, and a set of representatives for the class group is $\{\mathcal{O}_K, (2, 1 + \sqrt{-5})\}$.*

Proof. By the lemma, every ideal of $\mathcal{O}_K$ is equivalent to one of norm $\leq \frac{2}{\pi}\sqrt{20} \approx 2.85$. There is only one ideal of norm 1 (think back to the definition of the norm of an ideal), $\mathcal{O}_K$. Suppose $\mathfrak{p}$ is an ideal of norm 2. By Lemma 1.6.3 there is an nonzero $\alpha \in \mathfrak{p}$ with norm at most 5. However $\mathfrak{p}|\alpha$ implies $N(\mathfrak{p})|N(\alpha)$ means $N(\alpha)$ is even, i.e., $N(\alpha) = 2$ or 4. But there are no elements of norm 2 (it is not of the form $x^2 + 5y^2 = N(x + y\sqrt{-5})$), so we must have α is of norm 4, i.e., $\alpha = \pm 2$.

This means $\mathfrak{p}|(2)$, but the prime ideal factorization of (2) in $\mathcal{O}_K$ is $(2) = (2, 1 + \sqrt{-5})^2$ either from last semester or the exercise below. Hence $(2, 1 + \sqrt{-5})$ is the only ideal of norm 2, and it is not principal. □

A more elementary proof of the above fact is in the Chapter 12 notes from last semester, based off of what was in Stillwell. It still uses the lattice picture of ideals, but does not require Minkowski's theorem. In fact, a general proof of finiteness of the class group which avoids Minkowski's theorem is in [Lang].

Exercise 1.16. *Consider the ideal $\mathfrak{p} = (2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. We proved several things about this ideal last semester, but using norms we can give more elegant arguments. In any case, this exercise, and the following ones, should be a good review for you.*

(i) Show $\mathfrak{p}|(2)$ but $\mathfrak{p} \neq (2)$. Using norms, conclude $N(\mathfrak{p}) = 2$.

(ii) From (i) conclude $\mathfrak{p}$ is non-principal and prime.

(iii) Show the prime factorization of (2) is $(2) = \mathfrak{p}^2$.

Exercise 1.17. *Consider the ideals* $\mathfrak{q} = (3, 1+\sqrt{-5})$ *and* $\overline{\mathfrak{q}} = (3, 1-\sqrt{-5})$ *in* $\mathbb{Z}[\sqrt{-5}]$.

(i) Show $N(\mathfrak{q}) = N(\overline{\mathfrak{q}}) = 3$.

(ii) Show $\mathfrak{q}$, $\overline{\mathfrak{q}}$ *are non-principal and prime.*

(iii) Show the prime factorization of (3) *is* $(3) = \mathfrak{q}\overline{\mathfrak{q}}$.

Exercise 1.18. *From the previous two exercises, determine the prime ideal factorization of* (6) *in* $\mathbb{Z}[\sqrt{-5}]$. *Explain how the non-unique factorization of elements* $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ *in* $\mathbb{Z}[\sqrt{-5}]$ *is resolved in terms of the prime ideal factorization of the ideal* (6).

Exercise 1.19. *Let* $K = \mathbb{Q}(\sqrt{-5})$. *By the above exercises, together with the fact that* $h_K = 2$, $\mathfrak{p} \sim \mathfrak{q}$ *in the notation above. Show this explicitly by finding nonzero* $\alpha, \beta \in \mathcal{O}_K$ *such that* $\alpha\mathfrak{p} = \beta\mathfrak{q}$.

Exercise 1.20. *Using Lemma 1.6.4, show* $\mathbb{Q}(\sqrt{d})$ *has class number* 1 *for* $d = -1, -2, -3, -7, 2, 3, 5$.

These are all the cases where Lemma 1.6.4 immediately gives class number 1, but there are other cases.

Exercise 1.21. *Show* $\mathbb{Q}(\sqrt{-11})$ *has class number* 1.

The only other imaginary quadratic fields with class number 1, i.e., with unique factorization in their ring of integers, are $\mathbb{Q}(\sqrt{-d})$ with $d = 19, 43, 67, 163$ (making for a total of 9 such fields). It is not difficult to see that these fields all have class number 1—it is much harder to show that they are the only ones. This is Gauss's class number conjecture, and we will say a little more about this later. For now we will just say it was proven in 1934 by Heilbronn and Linfoot that there are only finitely many such imaginary quadratic fields, and eventually proved that there were no others by Heegner and Stark in the 50's and 60's.

Contrast this with the real quadratic case where it is conjectured that there are infinitely many instances of class number 1 (in fact, it is thought that about 75% should be). Tables of class numbers for small real and imaginary quadratic fields are given below.

Exercise 1.22. *Show* $\mathbb{Q}(\sqrt{-6})$ *has class number* 2.

Now we want to show the finiteness of the class number for a general quadratic field. We need to know one more small fact about ideals first.

Lemma 1.6.6. *Let* K *be a quadratic field and* $n \in \mathbb{N}$. *There are only finitely many ideals* $\mathcal{I}$ *of* $\mathcal{O}_K$ *such that* $N(\mathcal{I}) = n$.

Proof. Regarding $\mathcal{O}_K$ as a lattice in $\mathbb{R}^2$ as above, the ideals of norm n correspond to the lattices of $\mathbb{R}^2$ contained in $\mathcal{O}_K$ (i.e., sublattices of $\mathcal{O}_K$) of (co)volume $\frac{n}{2}\sqrt{|\Delta_K|}$ by Corollary 1.6.2. It is geometrically clear that there are only finitely many such (sub)lattices.

We will see another proof later when we study the behavior of primes in extensions. In particular we will show that if $N(\mathcal{I}) = n$, then $\mathcal{I}|(n)$. But there are only finitely many ideals dividing (n) by the uniqueness of prime ideal factorization. □

Theorem 1.6.7. *Let* K *be a quadratic field. Then* $h_K < \infty$, *i.e.,* $\mathcal{C}l_K$ *is a finite abelian group.*

Proof. By Lemma 1.6.4, there is some n such that any equivalence class of ideals has a representative with norm $\leq n$. Now by the previous lemma, there are only finitely many ideals with norm $\leq n$. □

Table 1: Class numbers of small imaginary quadratic fields $K = \mathbb{Q}(\sqrt{d})$

d	h_K
-1	1
-2	1
-3	1
-5	2
-6	2
-7	1
-10	2
-11	1
-13	2
-14	4
-15	2
-17	4
-19	1
-21	4
-22	2
-23	3
-26	6
-29	6
-30	4
-31	3
-33	4
-34	4
-35	2
-37	2
-38	6
-39	4
-41	8
-42	4
-43	1
-46	4
-47	5
-51	2

Table 2: Class numbers of small real quadratic fields $K = \mathbb{Q}(\sqrt{d})$

d	h_K
2	1
3	1
5	1
6	1
7	1
10	2
11	1
13	1
14	1
15	1
17	1
19	1
21	1
22	1
23	1
26	2
29	1
30	2
31	1
33	1
34	2
35	2
37	1
38	1
39	2
41	1
42	2
43	1
46	1
47	1
51	2

1.7 The geometry of numbers: the general case

Now suppose K is a number field of degree n. In order to look at $\mathcal{O}_K$ "geometrically", i.e., as a lattice, we need a way to embed K into $\mathbb{R}^n$. Of course if $\alpha_1, \ldots, \alpha_n$ is a basis for K (as a $\mathbb{Q}$-vector space), we could send $\sum c_i\alpha_i$ to $(c_1, \ldots, c_n) \in \mathbb{R}^n$, but there are two issues: (i) this is not at all canonical since it is highly dependent on the choice of basis, and (ii) there is no way with such an arbitrary embedding to relate $\mathrm{vol}(\mathbb{R}^n/\mathcal{I})$ with the discriminant/norm of an ideal $\mathcal{I}$ of $\mathcal{O}_K$ in order to get an analogue of Proposition 1.6.1 and its corollary.

In fact, if we look over the proof of Lemma 1.6.3, we see the key is that $|N(\alpha)|$ is $\leq$ the square of the distance from α to the origin in $\mathbb{R}^2$, with equality in the imaginary quadratic case. However, in some sense, the embedding we used in the real quadratic case, while perhaps the most obvious choice, was not natural in that it came from the "standard" basis $1, \sqrt{d}$ of $K = \mathbb{Q}(\sqrt{d})$. One might then ask if there is a more "natural" embedding of a real quadratic field $K = \mathbb{Q}(\sqrt{d}) \hookrightarrow \mathbb{R}^2$. There is, and the idea is to use the Galois group. Let σ_1, σ_2 be the embeddings of $K \hookrightarrow \mathbb{R}$ (all embeddings are real) given by $\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}$ and $\sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}$.

Consider the embedding $K \hookrightarrow \mathbb{R}^2$ given by $\alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha))$. This is "natural" since it does not depend upon a choice of basis for K over $\mathbb{Q}$, and the norm satisfies the desired geometric bound: if $\alpha = a+b\sqrt{d} \mapsto (x, y)$, then $x = a+b\sqrt{d}$, $y = a-b\sqrt{d}$, so $x^2+y^2 = 2(a^2+db^2) \geq 2|a^2-db^2| = 2N(\alpha)$. (Our naive embedding of a real quadratic field into $\mathbb{R}^2$ was of course perfectly fine for our goal in the previous section, but the problem was it is not so helpful in suggesting an appropriate generalization to arbitrary number fields. In fact, our naive embedding gives a better bound than the "natural" one given by the Galois group stated below.)

The standard presentation of the geometry of numbers is as follows. Let K be a number field of degree n. Then there are n embeddings of $K \hookrightarrow \mathbb{C}$, say $\sigma_1, \ldots, \sigma_n$. Assume the first s are *real embeddings*, i.e., $\sigma_1, \ldots, \sigma_s$ actually embed K in $\mathbb{R}$, and that the remaining σ_i's are *complex embeddings*, i.e., they do not map into $\mathbb{R}$. If σ_i is a complex embedding, then $\overline{\sigma}_i$ also is, where $\overline{\sigma}_i(\alpha) = \overline{\sigma_i(\alpha)}$ and the bar denotes usual complex conjugation. In particular, there are an even number $2t$ of complex embeddings, which occur in complex conjugate pairs. Let us denote them $\tau_1, \overline{\tau}_1, \ldots, \tau_t, \overline{\tau}_t$.

Now we define the embedding $\phi : K \to \mathbb{R}^s \times \mathbb{C}^t \simeq \mathbb{R}^{s+2t} = \mathbb{R}^n$ by

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \tau_1(\alpha), \ldots, \tau_t(\alpha)).$$

This is natural, in that it does not depend upon a basis for K. It does technically depend on the ordering of the embeddings σ_i and τ_i, as well as a choice among each conjugate pair of complex embeddings τ_i and $\overline{\tau}_i$, but not in any significant way.

Example 1.7.1. *If $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then $s = 2$ and $t = 0$, and $\phi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha))$ is the embedding described above.*

If $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field, then $s = 0$ and $t = 1$, and $\mathrm{Gal}(K/\mathbb{Q}) = \{\tau_1, \overline{\tau}_1\}$ where $\tau_1 : K \hookrightarrow \mathbb{C}$ is the trivial embedding. Then also $\phi(\alpha) = \tau_1(\alpha) = \alpha$ is the standard embedding into $\mathbb{C} \simeq \mathbb{R}^2$. If we had chosen τ_1 to be complex conjugation, then $\overline{\tau}_1$ would be the identity map on K and we would have that $\phi(\alpha) = \overline{\alpha}$ is the conjugate embedding into $\mathbb{C} \simeq \mathbb{R}^2$.

Thus this embedding generalizes both what we did in the imaginary quadratic case (which was basically nothing, just the standard identification of $\mathbb{C}$ with $\mathbb{R}^2$) as well as our second approach to the real quadratic case.

Example 1.7.2. *Let* $K = \mathbb{Q}(\sqrt[3]{2})$. *Then* $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \tau_1, \overline{\tau}_1\}$ *where* σ_1 *is the trivial automorphism of* K, τ_1 *maps* $\sqrt[3]{2}$ *to* $\zeta_3\sqrt[3]{2}$ *and* τ_2 *maps* $\sqrt[3]{2}$ *to* $\zeta_3^2\sqrt[3]{2}$. *Thus* $\phi : K \hookrightarrow \mathbb{R} \times \mathbb{C} \simeq \mathbb{R}^3$ *by*

$$\phi(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (a + b\sqrt[3]{2} + c\sqrt[3]{4}, a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4}).$$

Exercise 1.23. *Let* $K = \mathbb{Q}(\sqrt[4]{2})$. *Write down explicitly the map* ϕ *in this case. Compute* $\phi(3)$, $\phi(3 + \sqrt[4]{2})$ *and* $\phi(1 + 3\sqrt{2} + \sqrt[4]{2})$.

Exercise 1.24. *Let* $K = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$. *Write down explicitly the map* ϕ *in this case. Compute* $\phi(1 + \sqrt{5})$, $\phi(1 + \sqrt{-5})$ *and* $\phi(2i)$.

With the embedding ϕ given above, $\mathcal{O}_K$ is a lattice in $\mathbb{R}^n$, and as in the quadratic case we did earlier, one can prove the following.

Proposition 1.7.3. *Let* $\mathcal{I}$ *be an ideal of* $\mathcal{O}_K$ *with basis* $\alpha_1, \ldots, \alpha_n$, *regarded as a lattice in* $\mathbb{R}^n$ *via the embedding* ϕ. *Then* $\mathrm{vol}(\mathbb{R}^n/\mathcal{I}) = 2^{-t}\Delta[\alpha_1, \ldots, \alpha_n] = 2^{-t}N(\mathcal{I})\sqrt{|\Delta_K|}$.

Here t is the number of complex embeddings of $K \hookrightarrow \mathbb{C}$ as above. This proposition gives a geometric interpretation of discriminants for general number fields.

Lemma 1.7.4. *Let* $\mathcal{I}$ *be an ideal of* $\mathcal{O}_K$. *Then* $\mathcal{I}$ *is equivalent to an ideal of* $\mathcal{O}_K$ *with norm* $\leq \left(\frac{2}{\pi}\right)^t \sqrt{|\Delta_K|}$.

Note that in the case of real quadratic fields, this gives a weaker bound that what we got in the last section because there will be no factor of $\frac{2}{\pi}$ here. It's possible to improve the bound in the lemma by being more careful. Precisely one can show

Lemma 1.7.5. (Minkowski's bound) *Let* $\mathcal{I}$ *be an ideal of* $\mathcal{O}_K$. *Then* $\mathcal{I}$ *is equivalent to an ideal of* $\mathcal{O}_K$ *with norm* $\leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta_K|}$.

This is better than the simple bound we gave in the previous section in real quadratic case, and the same as our previous bound in the imaginary quadratic case. The better bound in the real case is in line with the notion that the class numbers for real quadratic fields tend to be smaller than those for imaginary quadratic fields, though it provides no real explanation. In any case, we will not be concerned overly much with optimal bounds. For us, the main point is

Theorem 1.7.6. *Let* K *be a number field. Then* $h_K < \infty$.

The proof for the general case is the same as the quadratic case, admitting one of the bounds in the previous lemmas. Complete proofs of these results should be available in any Algebraic Number Theory text.

1.8 Interlude: Dirichlet's Units Theorem

There are several applications of Minkowski's geometry of numbers to classical problems. Apart from the applications to class groups and quadratic forms discussed above, other applications are to bounding the number of lattice points enclosed by a polygon and bounding the number of balls that can fit in a given region (i.e., sphere packing bounds—a remarkable result around 15 years ago was the resolution of Kepler's conjecture on the optimal way to pack spheres in space).

In algebraic number theory, there is another major application of the geometry of numbers, and that is to prove Dirichlet's Units Theorem. Since we will not have need of this theorem, we will not prove it in the interest of time, but it is such a fundamental result about number fields we would be remiss not to mention it.

Theorem 1.8.1. (Dirichlet's Units Theorem) *Let s be the number of real embeddings and $2t$ be the number of complex embeddings of a number field K. Then the group of units U of $\mathcal{O}_K$ is isomorphic (as an abelian group) to $\mathbb{Z}^{s+t-1} \times C_{2m}$ for some $m \in \mathbb{N}$.*

The basic idea of the proof is to embed K in $\mathbb{R}^{s+2t}$. Since the units are multiplicative, applying logarithms coordinate-wise makes an additive subgroup of $\mathbb{R}^{s+2t}$, i.e., an incomplete lattice, which one shows is of rank $s + t - 1$.

We note that the determination of the finite cyclic group C_{2m} appearing in the theorem is simple to determine for any given K. It is simply given by the roots of unity which are contained in K, as any unit of finite order must be a root of unity, and all roots of unity are algebraic integers.

1.9 Debriefing

Dedekind introduced ideal theory to resolve the failure of unique factorization in $\mathcal{O}_K$ for arbitrary number fields K. The first suggestion is that this is a good theory to look at, is that it provides a clear characterization of when $\mathcal{O}_K$ does have unique factorization—namely, if and only if $\mathcal{O}_K$ is a PID, which is if and only if $h_K = 1$. (We stated this before the prime ideal factorization theorem last semester, even though we didn't prove the only if direction until this chapter.) The prime ideal factorization theorem tells us it in fact is an excellent theory to look at, and we saw how it resolved the non-unique factorization of $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. Historically, it was the 3rd approach to resolve these non-unique factorizations, coming after Gauss's theory of quadratic forms (for quadratic fields) and Kummer's theory of "ideal numbers." These ideas are still very interesting, and we will discuss them in Part II.

We began this chapter by generalized some ideas such as conjugates and norms from quadratic fields to arbitrary number fields using Galois groups. As you may be aware from algebra, in many cases the Galois group of an extension can be somewhat difficult to compute, but simple non-quadratic examples are still fairly easy to compute, as we have seen with examples.

The point is the Galois group of a degree n extension is a transitive subgroup of S_n acting on the n roots of the minimal polynomial of a primitive element. When $n = 2$, there is only one transitive subgroup of $S_2 \simeq C_2$, and the extension is necessarily Galois. Here it is immediate what the Galois group is. However for $n > 2$, there is more than one transitive subgroup of S_n (e.g., S_n, A_n, C_n), and one need to do some work to determine what is is. Further, sometimes the primitive element is obvious, but sometimes it is not, e.g., what is a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$? (You can show $\sqrt{2} + \sqrt{3}$ works by a degree argument and the characterization of quadratic fields, but you can see how this can get complicated quickly. Even knowing this, how do you determine the minimum polynomial—what is the minimum polynomial of $\sqrt{2} + \sqrt{3}$?) In general, one probably wants to use the main theorem of Galois theory (which I won't review) to use the subfield lattice to help determine the Galois group. However, the examples we will cover will be simple enough that we don't need to use the full force of Galois theory to determine the Galois group.

Knowing the Galois group of K over $\mathbb{Q}$ it is easy to determine the conjugates and norm of an element in K. What is not so simple is determining the ring $\mathcal{O}_K$. There is an algorithm for doing this using discriminants, though it turns out to be fairly computational even for simple examples like $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, our main reason for looking at discriminants is that they provide a fundamental invariant of a number field K and its ideals (i.e., the ideals of $\mathcal{O}_K$). For K an imaginary quadratic field, the discriminant of $\mathcal{O}_K$ or an ideal $\mathcal{I}$ of $\mathcal{O}_K$ is essentially the volume of the corresponding lattice, as well as essentially the norm of the ideal squared. (We only defined the discriminant of a basis of an ideal, but by the formula in terms of the norm, this is clearly independent of the choice of basis.) Then with Minkowski's theorem, we were able to bound the norm of "minimal" representative of the class group in terms of the discriminant, providing a proof of the finiteness of the class group $\mathcal{C}l_K$, as well as allowing us to explicitly determine the class group in particular cases.

On the other hand, for real quadratic fields $K \subseteq \mathbb{R}$, $\mathcal{O}_K$ is not a lattice, but we have seen at least two ways to embed K in $\mathbb{R}^2$ which makes $\mathcal{O}_K$ a lattice—the naive way, and the approach via Galois conjugates. The second approach generalizes for an arbitrary number field K of degree n, allowing us to view $\mathcal{O}_K$ as a lattice in $\mathbb{R}^n$. As before the norm and discriminant of the ideal are essentially the (co)volume of the lattice $\mathcal{O}_K$, and Minkowski's theorem allows us to show the class group is finite, and bound norms of a set of minimal representatives of the class group.

Stillwell talked about the shape of ideals in imaginary quadratic fields. Two lattices (ideals) in $\mathbb{C} \simeq \mathbb{R}^2$ will have the same shape if and only if they differ by a complex scalar (principal ideal). Hence two ideals will have the same shape if and only if they are equivalent. Thus the class number is the number of different possible shapes of ideals. Similarly, via the geometry of numbers developed by Minkowski, if two ideals are equivalent, they will have they same shape, regarded as lattices in $\mathbb{R}^n$.

The goal of this chapter was to show finiteness of the class group (at least a complete proof in the quadratic case, and the general case is similar in spirit), and show in some specific cases how we can determine the class number and class group. There are two reasons for this: (i) to understand factorization in $\mathcal{O}_K$, which is a basic problem in algebraic number theory, and (ii) applications to Diophantine equations.

First off, the class group of K measures the failure of unique factorization in $\mathcal{O}_K$. The larger it is the more different the set of irreducible factorizations of some algebraic integer $\alpha \in \mathcal{O}_K$ can be. For example, K has class number 2 if and only if every element of $\mathcal{O}_K$ does not have unique factorization but any factorization into irreducibles has the same number of factors. We will come back to this idea in Part II.

Now what is the bearing of the class group on solving Diophantine equations? Well, first of all, the simplest case is when $\mathcal{O}_K$ has unique factorization, i..e, class number 1. We have shown the rings of integers of the fields $\mathbb{Q}(\sqrt{d})$ for $d = -1, -2, -3, -7, -11, 2, 3, 5$ all have unique factorization. Following the approach last semester, this makes it easy to determine which primes are of the form $x^2 + dy^2$ for $d = 1, 2, 3, 7$. In particular, we used unique factorization in $\mathbb{Z}[\sqrt{-2}]$ to show $y^3 = x^2 + 2$ has only one solution $(5, 3)$ in $\mathbb{N}$, and unique factorization in $\mathbb{Z}[\zeta_3]$ to show $x^3 + y^3 = z^3$ has no solutions in $\mathbb{N}$. Lamé gave an argument that $x^p + y^p = z^p$ has no solutions in n for p and odd prime whenever $\mathbb{Z}[\zeta_p]$ has unique factorization.

Even when $\mathbb{Z}[\sqrt{-d}]$ does not have unique factorization, we can still use knowledge of the class group to determine the primes of the form $x^2 + dy^2$. Specifically, we used the fact that $\mathbb{Z}[\sqrt{-5}]$ has class number 2 to determine the primes of the form $x^2 + 5y^2$ at the end of last semester. (Refer to last semester's Chapter 12 notes, or wait till we review this next chapter.) In order to approach this problem for general $d > 0$ squarefree, observe $p = x^2 + dy^2 = (x + y\sqrt{-d})(x - y\sqrt{-d})$, which means the prime p splits into prime ideals $(p) = (x + y\sqrt{-d})(x - y\sqrt{-d})$ in the ring $\mathbb{Z}[\sqrt{-d}]$. This is a particular case of the general question, given an extension of number fields L/K and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, how do we determine how it behaves in L, i.e., what is the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$ in $\mathcal{O}_L$? This is another basic question of Algebraic Number Theory, and in particular when $K = \mathbb{Q}$, it will tell us what is the prime ideal factorization of (n) in $\mathcal{O}_L$. Hence, this is important for studying general Diophantine equations also, and this question will be the focus of the next chapter.

In the following chapter, we will briefly talk about cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p-th root of unity and p is an odd prime. This is the next most important and basic type of number field after the quadratic fields. This will (i) give us a better understanding of the concepts discussed in this chapter for non-quadratic fields, and (ii) provide an opportunity for more applications. The most famous application of these fields is to Kummer's approach to Fermat's last theorem. While a complete proof of Kummer's result would take longer than we would like to spend on this, we will at least give a sketch of the argument using Dedekind's ideal theory (as opposed to Kummer's original approach via ideal numbers).

Finally, a look at the class number tables in this chapter shows that even in the simple case of quadratic fields, the class numbers behave with apparently little regularity, just like prime numbers seem to behave with little regularity. Thus it might seem unlikely that one could come up with an exact formula for the class number h_K. Remarkably, Dirichlet did just that, using the theory of L-functions, which itself is closely related to hidden regularities in prime numbers. This is what we will study at the end of Part I.