Math 129: Algebraic Number Theory
Lecture 7

William Stein

Thursday, February 26, 2004

In this lecture we will prove the Chinese Remainder Theorem for rings of integers, deduce several surprising and useful consequences, then learn about discriminants, and finally norms of ideals. We will also define the class group of $\mathcal{O}_K$ and state the main theorem about it. The tools we develop today illustrate the power of what we have already proved about rings of integers, and will be used over and over again to prove other deeper results in algebraic number theory. It is essentially to understand everything we discuss today very well.

1 The Chinese Remainder Theorem

Recall that the Chinese Remainder Theorem from elementary number theory asserts that if $n_1, \ldots, n_r$ are integers that are coprime in pairs, and $a_1, \ldots, a_r$ are integers, then there exists an integer a such that $a \equiv a_i \pmod{n_i}$ for each $i = 1, \ldots, r$. In terms of rings, the Chinese Remainder Theorem asserts that the natural map

$$\mathbf{Z}/(n_1 \cdots n_r)\mathbf{Z} \to (\mathbf{Z}/n_1\mathbf{Z}) \oplus \cdots \oplus (\mathbf{Z}/n_r\mathbf{Z})$$

is an isomorphism. This result generalizes to rings of integers of number fields.

Lemma 1.1. *If I and J are coprime ideals in $\mathcal{O}_K$, then $I \cap J = IJ$.*

Proof. The ideal $I \cap J$ is the largest ideal of $\mathcal{O}_K$ that is divisible by (contained in) both I and J. Since I and J are coprime, $I \cap J$ is divisible by IJ, i.e., $I \cap J \subset IJ$. By definition of ideal $IJ \subset I \cap J$, which completes the proof.

Note: This lemma is true for any ring R and ideals $I, J \subset R$ such that $I + J = R$. For the general proof, choose $x \in I$ and $y \in J$ such that $x + y = 1$. If $c \in I \cap J$ then

$$c = c \cdot 1 = c \cdot (x + y) = cx + cy \in IJ + IJ = IJ,$$

so $I \cap J \subset IJ$, and the other inclusion is obvious by definition. □

Theorem 1.2 (Chinese Remainder Theorem). *Suppose $I_1, \dots, I_r$ are ideals of $\mathcal{O}_K$ such that $I_m + I_n = \mathcal{O}_K$ for any $m \neq n$. Then the natural homomorphism $\mathcal{O}_K \to \bigoplus_{n=1}^r (\mathcal{O}_K/I_n)$ induces an isomorphism*

$$\mathcal{O}_K/\left(\prod_{n=1}^r I_n\right) \to \bigoplus_{n=1}^r (\mathcal{O}_K/I_n).$$

Thus given any $a_n \in I_n$ then there exists $a \in \mathcal{O}_K$ such that $a \equiv a_n \pmod{I_n}$ for $n = 1, \dots, r$.

Proof. First assume that we know the theorem in the case when the I_n are powers of prime ideals. Then we can deduce the general case by noting that each $\mathcal{O}_K/I_n$ is isomorphic to a product $\prod \mathcal{O}_K/\mathfrak{p}_m^{e_m}$, where $I_n = \prod \mathfrak{p}_m^{e_m}$, and $\mathcal{O}_K/(\prod_n I_n)$ is isomorphic to the product of the $\mathcal{O}_K/\mathfrak{p}^e$, where the $\mathfrak{p}$ and e run through the same prime powers as appear on the right hand side.

It thus suffices to prove that if $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals of $\mathcal{O}_K$ and $e_1, \dots, e_r$ are positive integers, then

$$\psi : \mathcal{O}_K/\left(\prod_{n=1}^r \mathfrak{p}_n^{e_n}\right) \to \bigoplus_{n=1}^r (\mathcal{O}_K/\mathfrak{p}_n^{e_n})$$

is an isomorphism. Let $\varphi : \mathcal{O}_K \to \oplus_{n=1}^r (\mathcal{O}_K/\mathfrak{p}_n^{e_n})$ be the natural map induced by reduction mod $\mathfrak{p}_n^{e_n}$. Then kernel of φ is $\cap_{n=1}^r \mathfrak{p}_n^{e_n}$, which by Lemma 1.1 is equal to $\prod_{n=1}^r \mathfrak{p}_n^{e_n}$, so ψ is injective. Note that the projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_n^{e_n}$ of φ onto each factor is obviously surjective, so it suffices to show that the element $(1, 0, \dots, 0)$ is in the image of φ (and the similar elements for the other factors). Since $J = \prod_{n=2}^r \mathfrak{p}_n^{e_n}$ is not divisible by $\mathfrak{p}_1$, hence not contained in $\mathfrak{p}_1$, there is an element $a \in J$ with $a \notin \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is maximal, $\mathcal{O}_K/\mathfrak{p}_1$ is a field, so there exists $b \in \mathcal{O}_K$ such that $ab = 1 - c$, for some $c \in \mathfrak{p}_1$. Then

$$1 - c^{n_1} = (1-c)(1 + c + c^2 + \cdots + c^{n_1 - 1}) = ab(1 + c + c^2 + \cdots + c^{n_1 - 1})$$

is congruent to 0 mod $\mathfrak{p}_n^{e_n}$ for each $n \geq 2$ since it is in $\prod_{n=2}^r \mathfrak{p}_n^{e_n}$, and it is congruent to 1 modulo $\mathfrak{p}_1^{n_1}$.

Note: Surjectivity is easy to prove and holds for any ring. Suppose R is a ring and I, J are ideals in R such that $I + J = R$. Choose $x \in I$ and $y \in J$ such that $x + y = 1$. Then $x = 1 - y$ maps to $(0, 1)$ in $R/I \oplus R/J$ and $y = 1 - x$ maps to $(1, 0)$ in $R/I \oplus R/J$. Thus the map $R/(I \cap J) \to R/I \oplus R/J$ is surjective. Also, as mentioned above, $R/(I \cap J) = R/(IJ)$. □

Example 1.3. The MAGMA command `ChineseRemainderTheorem` implements the algorithm suggested by the above theorem. In the following example, we compute a prime over (3) and a prime over (5) of the ring of integers of $\mathbf{Q}(\sqrt[3]{2})$, and find an element of $\mathcal{O}_K$ that is congruent to $\sqrt[3]{2}$ modulo one prime and 1 modulo the other.

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^3-2);
> OK := MaximalOrder(K);
> I := Factorization(3*OK)[1][1];
> J := Factorization(5*OK)[1][1];
> I;
Prime Ideal of OK
Two element generators:
    [3, 0, 0]
    [4, 1, 0]
> J;
Prime Ideal of OK
Two element generators:
    [5, 0, 0]
    [7, 1, 0]
> b := ChineseRemainderTheorem(I, J, OK!a, OK!1);
> b - a in I;
true
> b - 1 in J;
true
> K!b;
-4
```

The element found by the Chinese Remainder Theorem algorithm in this case is -4.

The following lemma is a nice application of the Chinese Remainder Theorem. We will use it to prove that every ideal of $\mathcal{O}_K$ can be generated by two elements. Suppose I is a nonzero integral ideals of $\mathcal{O}_K$. If $a \in I$, then $(a) \subset I$, so I divides (a) and the quotient $(a)/I$ is an integral ideal. The following lemma asserts that (a) can be chosen so the quotient $(a)/I$ is coprime to any given ideal.

Lemma 1.4. *If I, J are nonzero integral ideals in $\mathcal{O}_K$, then there exists an $a \in I$ such that $(a)/I$ is coprime to J.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime divisors of J. For each n, let v_n be the largest power of $\mathfrak{p}_n$ that divides I. Choose an element $a_n \in \mathfrak{p}_n^{v_n}$ that is not in $\mathfrak{p}_n^{v_n+1}$ (there is such an element since $\mathfrak{p}_n^{v_n} \neq \mathfrak{p}_n^{v_n+1}$, by unique factorization). By Theorem 1.2, there exists $a \in \mathcal{O}_K$ such that

$$a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$$

for all $n = 1, \ldots, r$ and also

$$a \equiv 0 \pmod{I/\prod \mathfrak{p}_n^{v_n}}.$$

(We are applying the theorem with the coprime integral ideals $\mathfrak{p}_n^{v_n+1}$, for $n = 1, \ldots, r$ and the integral ideal $I/\prod \mathfrak{p}_n^{v_n}$.)

To complete the proof we must show that $(a)/I$ is not divisible by any $\mathfrak{p}_n$, or equivalently, that the $\mathfrak{p}_n^{v_n}$ exactly divides (a). Because $a \equiv a_n \pmod{\mathfrak{p}_n^{v_n+1}}$, there is $b \in \mathfrak{p}_n^{v_n+1}$ such that $a = a_n + b$. Since $a_n \in \mathfrak{p}_n^{v_n}$, it follows that $a \in \mathfrak{p}_n^{v_n}$, so $\mathfrak{p}_n^{v_n}$ divides (a). If $a \in \mathfrak{p}_n^{v_n+1}$, then $a_n = a - b \in \mathfrak{p}_n^{v_n+1}$, a contradiction, so $\mathfrak{p}_n^{v_n+1}$ does not divide (a), which completes the proof. □

Suppose I is a nonzero ideal of $\mathcal{O}_K$. As an abelian group $\mathcal{O}_K$ is free of rank equal to the degree $[K : \mathbf{Q}]$ of K, and I is of finite index in $\mathcal{O}_K$, so I can be generated as an abelian group, hence as an ideal, by $[K : \mathbf{Q}]$ generators. The following proposition asserts something much better, namely that I can be generated *as an ideal* in $\mathcal{O}_K$ by at most two elements.

Proposition 1.5. *Suppose I is a fractional ideal in the ring $\mathcal{O}_K$ of integers of a number field. Then there exist $a, b \in K$ such that $I = (a, b)$.*

Proof. If $I = (0)$, then I is generated by 1 element and we are done. If I is not an integral ideal, then there is $x \in K$ such that xI is an integral ideal, and the number of generators of xI is the same as the number of generators of I, so we may assume that I is an integral ideal.

Let a be any nonzero element of the integral ideal I. We will show that there is some $b \in I$ such that $I = (a, b)$. Let $J = (b)$. By Lemma 1.4, there exists $a \in I$ such that $(a)/I$ is coprime to (b). The ideal $(a, b) = (a) + (b)$ is the greatest common divisor of (a) and (b), so I divides (a, b), since I divides both (a) and (b). Suppose $\mathfrak{p}^n$ is a prime power that divides (a, b), so $\mathfrak{p}^n$ divides both (a) and (b). Because $(a)/I$ and (b) are coprime and $\mathfrak{p}^n$ divides (b), we see that $\mathfrak{p}^n$ does not divide $(a)/I$, so $\mathfrak{p}^n$ must divide I. Thus (a, b) divides I, so $(a, b) = I$ as claimed. □

We can also use Theorem 1.2 to determine the $\mathcal{O}_K$-module structure of the successive quotients $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.

Proposition 1.6. *Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let $n \geq 0$ be an integer. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}_K/\mathfrak{p}$ as $\mathcal{O}_K$-modules.*

Proof. (Compare page 13 of Swinnerton-Dyer.) Since $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ (by unique factorization), we can fix an element $b \in \mathfrak{p}^n$ such that $b \notin \mathfrak{p}^{n+1}$. Let $\varphi : \mathcal{O}_K \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ be the $\mathcal{O}_K$-module morphism defined by $\varphi(a) = ab$. The kernel of φ is $\mathfrak{p}$ since clearly $\varphi(\mathfrak{p}) = 0$ and if $\varphi(a) = 0$ then $ab \in \mathfrak{p}^{n+1}$, so $\mathfrak{p}^{n+1} \mid (a)(b)$, so $\mathfrak{p} \mid (a)$, since $\mathfrak{p}^{n+1}$ does not divide (b). Thus φ induces an injective $\mathcal{O}_K$-module homomorphism $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

It remains to show that φ is surjective, and this is where we will use Theorem 1.2. Suppose $c \in \mathfrak{p}^n$. By Theorem 1.2 there exists $d \in \mathcal{O}_K$ such that

$$d \equiv c \pmod{\mathfrak{p}^{n+1}} \qquad \text{and} \qquad d \equiv 0 \pmod{(b)/\mathfrak{p}^n}.$$

We have $\mathfrak{p}^n \mid (c)$ since $c \in \mathfrak{p}^n$ and $(b)/\mathfrak{p}^n \mid (d)$ by the second displayed condition, so $(b) = \mathfrak{p}^n \cdot (b)/\mathfrak{p}^n \mid (d)$, hence $d/b \in \mathcal{O}_K$. Finally

$$\varphi\left(\frac{d}{b}\right) \quad = \quad \frac{d}{b} \cdot b \pmod{\mathfrak{p}^{n+1}} \quad = \quad b \pmod{p^{n+1}} \quad = \quad c \pmod{p^{n+1}},$$

so φ is surjective. $\square$

2 Discriminants

(Compare pages 3–4 of Swinnerton-Dyer.)

Let K be a number field of degree n. Then there are n embeddings

$$\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbf{C}.$$

Let $\sigma : K \to \mathbf{C}^n$ be the product map $a \mapsto (\sigma_1(a), \ldots, \sigma_n(a))$. Let $V = \mathbf{R}\sigma(K)$ be the $\mathbf{R}$-span of $\sigma(K)$ inside $\mathbf{C}^n$.

Proposition 2.1. *The $\mathbf{R}$-vector space $V = \mathbf{R}\sigma(K)$ spanned by the image $\sigma(K)$ has dimension n.*

Proof. We prove this by showing that the image $\sigma(\mathcal{O}_K)$ is discrete. If $\sigma(\mathcal{O}_K)$ were not discrete it would contain elements all of whose coordinates are simultaneously arbitrarily small. The norm of an element $a \in \mathcal{O}_K$ is the product of the entries of $\sigma(a)$, so the norms of nonzero elements of $\mathcal{O}_K$ would go to 0. This is a contradiction, since the norms of elements of $\mathcal{O}_K$ are integers.

The fact that $\sigma(\mathcal{O}_K)$ is discrete in $\mathbf{C}^n$ implies that $\mathbf{R}\sigma(\mathcal{O}_K)$ has dimension equal to the rank n of $\sigma(\mathcal{O}_K)$, as claimed. This last assertion is not obvious, and requires observing that if L if a free abelian group that is discrete in a real vector space W and $\mathbf{R}L = W$, then the rank of L equals the dimension of W. Here's why this is true. If $x_1, \ldots, x_m \in L$ are a basis for $\mathbf{R}L$, then $\mathbf{Z}x_1 + \cdots + \mathbf{Z}x_m$ has finite index in L, since otherwise there would be infinitely many elements of L in a fundamental domain for $\mathbf{Z}x_1 + \cdots + \mathbf{Z}x_m$, which would contradict discreteness of L. Thus the rank of L is $m = \dim(\mathbf{R}L)$, as claimed. $\square$

Since $\sigma(\mathcal{O}_K)$ is a lattice in V, the volume of $V/\sigma(\mathcal{O}_K)$ is finite. Suppose $w_1, \ldots, w_n$ is a basis for $\mathcal{O}_K$. Then if A is the matrix whose ith row is $\sigma(w_i)$, then $|\det(A)|$ is the volume of $V/\sigma(\mathcal{O}_K)$. (Take this determinant as the definition of the volume—we won't be using "volume" here except in a formal motivating way.)

Example 2.2. Let $\mathcal{O}_K = \mathbf{Z}[i]$ be the ring of integers of $K = \mathbf{Q}(i)$. Then $w_1 = 1$, $w_2 = i$ is a basis for $\mathcal{O}_K$. The map $\sigma : K \to \mathbf{C}^2$ is given by

$$\sigma(a + bi) = (a + bi, a - bi) \in \mathbf{C}^2.$$

The image $\sigma(\mathcal{O}_K)$ is spanned by $(1, 1)$ and $(i, -i)$. The volume determinant is

$$\left| \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \right| = |-2i| = 2.$$

Let $\mathcal{O}_K = \mathbf{Z}[\sqrt{2}]$ be the ring of integers of $K = \mathbf{Q}(\sqrt{2})$. The map σ is

$$\sigma(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2}) \in \mathbf{R}^2,$$

and

$$A = \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix},$$

which has determinant $-2\sqrt{2}$, so the volume of the ring of integers is $2\sqrt{2}$.

As the above example illustrates, the volume of the ring of integers is not a great invariant of $\mathcal{O}_K$. For example, it need not be an integer. If we consider $\det(A)^2$ instead, we obtain a number that is a well-defined integer which can be either positive or negative. Note that

$$\det(A)^2 = \det(AA) = \det(AA^t) = \det\left(\sum_{k=1,\ldots,n} \sigma_k(w_i)\sigma_k(w_j)\right) = \det(\mathrm{Tr}(w_i w_j)),$$

so $\det(A)^2$ can be defined purely in terms of the trace without mentioning the embeddings σ_i. Also, changing the basis for $\mathcal{O}_K$ is the same as left multiplying A by an integer matrix U of determinant ± 1, which does not change the squared determinant, since $\det(UA)^2 = \det(U)^2 \det(A)^2 = \det(A)^2$. Thus $\det(A)^2$ is well defined, as does not depend on the choice of basis.

Definition 2.3 (Discriminant). Suppose $a_1, \ldots, a_n$ is any $\mathbf{Q}$-basis of K. The *discriminant* of $a_1, \ldots, a_n$ is

$$\mathrm{Disc}(a_1, \ldots, a_n) = \det(\mathrm{Tr}(a_i a_j)_{i,j=1,n}) \in \mathbf{Q}.$$

The *discriminant* $\mathrm{Disc}(\mathcal{O})$ of an order $\mathcal{O}$ in $\mathcal{O}_K$ is the discriminant of any basis for $\mathcal{O}$. The *discriminant* $\mathrm{Disc}(K)$ of the number field K is the discrimimant of $\mathcal{O}_K$ (Warning: MAGMA does not define $\mathrm{Disc}(K)$ this way!!).

The following proposition asserts that the discriminant of an order $\mathcal{O}$ in $\mathcal{O}_K$ is bigger than $\mathrm{disc}(\mathcal{O}_K)$ by the square of the index.

Proposition 2.4. *Suppose $\mathcal{O}$ is an order in $\mathcal{O}_K$. Then*

$$\mathrm{Disc}(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]^2 \cdot \mathrm{Disc}(\mathcal{O}_K).$$

Proof. Let A be a matrix whose rows are the images via σ of a basis for $\mathcal{O}_K$, and let B be a matrix whose rows are the images via σ of a basis for $\mathcal{O}$. Since $\mathcal{O} \subset \mathcal{O}_K$ has finite index, there is an integer matrix C such that $CA = B$, and $|\det(C)| = [\mathcal{O}_K : \mathcal{O}]$. Then

$$\mathrm{Disc}(\mathcal{O}) = \det(B)^2 = \det(CA)^2 = \det(C)^2 \det(A)^2 = [\mathcal{O}_K : \mathcal{O}]^2 \cdot \mathrm{Disc}(\mathcal{O}_K).$$

□

This result is already enough to give a (horrible) algorithm for computing $\mathcal{O}_K$. Given K, find some order $\mathcal{O} \subset K$, and compute $d = \mathrm{Disc}(\mathcal{O})$. Write $d = s \cdot f^2$, where f^2 is the largest square that divides d. Then the index of $\mathcal{O}$ in $\mathcal{O}_K$ is a divisor of f, and we can tediously enumerate all rings R with $\mathcal{O} \subset R \subset K$ and $[R : \mathcal{O}] \mid f$, until we find the largest one all of whose elements are integral.

Example 2.5. Consider the ring $\mathcal{O}_K = \mathbf{Z}[(1+\sqrt{5})/2]$ of integers of $K = \mathbf{Q}(\sqrt{5})$. The discriminant of the basis $1, a = (1+\sqrt{5})/2$ is

$$\mathrm{Disc}(\mathcal{O}_K) = \left|\begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}\right| = 5.$$

One can show that the discriminant of a quadratic field determines that field.

3 Norms of Ideals

In this section we extend the notion of norm to ideals. This will be helpful in understanding class groups later.

Definition 3.1 (Lattice Index). If L and M are two lattices in vector space V, then the *lattice index* $[L : M]$ is by definition the absolute value of the determinant of any linear automorphism of V (e.g., invertible matrix after choice of basis for V) that sends a basis of L onto a basis for M.

The lattice index has the following properties:

- If $M \subset L$, then $[L : M] = \#(L/M)$.
- If M, L, N are lattices then $[L : N] = [L : M] \cdot [M : N]$.

Definition 3.2 (Norm of Fractional Ideal). Suppose I is a fractional ideal of $\mathcal{O}_K$. The *norm* of I is the lattice index

$$\mathrm{Norm}(I) = [\mathcal{O}_K : I] \in \mathbf{Q}_{\geq 0},$$

or 0 if $I = 0$.

Note that if I is an integral ideal, then $\mathrm{Norm}(I) = \#(\mathcal{O}_K/I)$.

Lemma 3.3. *Suppose $a \in K$ and I is an integral ideal. Then*

$$\mathrm{Norm}(aI) = |\,\mathrm{Norm}(a)|\,\mathrm{Norm}(I).$$

Proof. By properties of the lattice index mentioned above we have

$$[\mathcal{O}_K : aI] = [\mathcal{O}_K : I] \cdot [I : aI] = \mathrm{Norm}(I) \cdot |\,\mathrm{Norm}(a)|.$$

Here we have used that $[I : aI] = |\,\mathrm{Norm}(a)|$, which is because left multiplication ℓ_a is an automorphism of K that sends I onto aI, so $[I : aI] = |\det(\ell_a)| = |\,\mathrm{Norm}(a)|$. □

Proposition 3.4. *If I and J are fractional ideals, then*

$$\mathrm{Norm}(IJ) = \mathrm{Norm}(I) \cdot \mathrm{Norm}(J).$$

Proof. By Lemma 3.3, it suffices to prove this when I and J are integral ideals. If I and J are coprime, then Theorem 1.2 implies that $\mathrm{Norm}(IJ) = \mathrm{Norm}(I)\,\mathrm{Norm}(J)$. Thus we reduce to the case when $I = \mathfrak{p}^m$ and $J = \mathfrak{p}^k$ for some prime ideal $\mathfrak{p}$. By Proposition 1.6, the maximal filtration of $\mathfrak{p}^n$ given by powers of $\mathfrak{p}$ has successive quotients isomorphic to $\mathcal{O}_K/\mathfrak{p}$, so pulling this filtration back to $\mathcal{O}_K/\mathfrak{p}^n$ we see that $\#(\mathcal{O}_K/\mathfrak{p}^n) = \#(\mathcal{O}_K/\mathfrak{p})^n$, which proves that $\mathrm{Norm}(\mathfrak{p}^n) = \mathrm{Norm}(\mathfrak{p})^n$. □

4 The Class Group

We have seen examples in which $\mathcal{O}_K$ is not a unique factorization domain. If $\mathcal{O}_K$ is a principal ideal domain, then it is a unique factorization domain, so it is of interest to understand how badly $\mathcal{O}_K$ fails to be a unique factorization domain. The class group of $\mathcal{O}_K$ measures this failure. As one sees in a course on Class Field Theory, the class group and its generalizations also yield deep incite into the possible abelian Galois extensions of K.

Definition 4.1 (Class Group). Let $\mathcal{O}_K$ be the ring of integers of a number field K. The *class group* C_K of K is the group of nonzero fractional ideals modulo the sugroup of principal fractional ideals (a), for $a \in K$.

Note that if we let $\mathrm{Div}(K)$ denote the group of nonzero fractional ideals, then there is an exact sequence

$$0 \to \mathcal{O}_K^* \to K^* \to \mathrm{Div}(K) \to C_K \to 0.$$

A basic theorem in algebraic number theory is that the class group C_K is finite, which follows from the first part of the following theorem and the fact that there are only finitely many ideals of norm less than a given integer.

Theorem 4.2 (Finiteness of the Class Group). *Every ideal class in C_K contains an integral ideal of norm at most*

$$\sqrt{|\operatorname{Disc}(K)|} \cdot \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n},$$

where s is the number of complex conjugate embeddings of K. Thus the class group C_K of any number field K is finite.

The bound in the theorem is called the Minkowski bound, and I think it is the best known unconditional general bound (though there are better bounds in certain special cases). We will prove this important theorem on Tuesday, March 2.

Conjecture 4.3. *There are infinitely many number fields K such that the class group of K has order* 1.