Math 129: Algebraic Number Theory
Lecture 9

William Stein

Thursday, March 4, 2004

Today we prove that the class group of the ring of integers of a number field is finite, discuss how to compute it in some examples, then introduce the group of units. We will prove the main structure theorem for the group of units on Tuesday. The notes about proof of finiteness of the class group are not given below, since they are in the handout for Lecture 8.

1 Remarks on Computing the Class Group

If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, then the intersection $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ is a prime ideal of $\mathbf{Z}$. We say that $\mathfrak{p}$ *lies over* $p \in \mathbf{Z}$. Note $\mathfrak{p}$ lies over $p \in \mathbf{Z}$ if and only if $\mathfrak{p}$ is one of the prime factors in the factorization of the ideal $p\mathcal{O}_K$. Geometrically, $\mathfrak{p}$ is a point of $\mathrm{Spec}(\mathcal{O}_K)$ that lies over the point $p\mathbf{Z}$ of $\mathrm{Spec}(\mathbf{Z})$ under the map induced by the inclusion $\mathbf{Z} \hookrightarrow \mathcal{O}_K$.

Lemma 1.1. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then the class group $\mathrm{Cl}(K)$ is generated by the prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ lying over primes $p \in \mathbf{Z}$ with $p \le B_K = \sqrt{|d_K|} \cdot \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n}$, where s is the number of complex conjugate pairs of embeddings $K \hookrightarrow \mathbf{C}$.*

Proof. We proved before that every ideal class in $\mathrm{Cl}(K)$ is represented by an ideal I with $\mathrm{Norm}(I) \le B_K$. Write $I = \prod_{i=1}^m \mathfrak{p}_i^{e_i}$, with each $e_i \ge 1$. Then by multiplicativity of the norm, each $\mathfrak{p}_i$ also satisfies $\mathrm{Norm}(\mathfrak{p}_i) \le B_K$. If $\mathfrak{p}_i \cap \mathbf{Z} = p\mathbf{Z}$, then $p \mid \mathrm{Norm}(\mathfrak{p}_i)$, since p is the residue characteristic of $\mathcal{O}_K/\mathfrak{p}$, so $p \le B_K$. Thus I is a product of primes $\mathfrak{p}$ that satisfies the norm bound of the lemma, whcih proves the lemma. $\square$

This is a sketch of how to compute $\mathrm{Cl}(K)$:

1. Use the "factoring primes" algorithm to list all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that appear in the factorization of a prime $p \in \mathbf{Z}$ with $p \le B_K$.

2. Find the group generated by the ideal classes $[\mathfrak{p}]$, where the $\mathfrak{p}$ are the prime ideals found in step 1. (In general, one must think more carefully about how to do this step.)

The following three examples illustrate computation of $\mathrm{Cl}(K)$ for $K = \mathbf{Q}(i), \mathbf{Q}(\sqrt{5})$ and $\mathbf{Q}(\sqrt{-6})$.

Example 1.2. We compute the class group of $K = \mathbf{Q}(i)$. We have

$$n = 2, \quad r = 0, \quad s = 1, \quad d_K = -4,$$

so

$$B_K = \sqrt{4} \cdot \left(\frac{4}{\pi}\right)^1 \cdot \left(\frac{2!}{2^2}\right) = \frac{8}{\pi} < 3.$$

Thus $\mathrm{Cl}(K)$ is generated by the prime divisors of 2. We have

$$2\mathcal{O}_K = (1+i)^2,$$

so $\mathrm{Cl}(K)$ is generated by the principal prime ideal $\mathfrak{p} = (1+i)$. Thus $\mathrm{Cl}(K) = 0$ is trivial.

Example 1.3. We compute the class group of $K = \mathbf{Q}(\sqrt{5})$. We have

$$n = 2, \quad r = 2, \quad s = 0, \quad d_K = 5,$$

so

$$B = \sqrt{5} \cdot \left(\frac{4}{\pi}\right)^0 \cdot \left(\frac{2!}{2^2}\right) < 3.$$

Thus $\mathrm{Cl}(K)$ is generated by the primes that divide 2. We have $\mathcal{O}_K = \mathbf{Z}[\gamma]$, where $\gamma = \frac{1+\sqrt{5}}{2}$ satisfies $x^2 - x - 1$. The polynomial $x^2 - x - 1$ is irreducible mod 2, so $2\mathcal{O}_K$ is prime. Since it is principal, we see that $\mathrm{Cl}(K) = 1$ is trivial.

Example 1.4. In this example, we compute the class group of $K = \mathbf{Q}(\sqrt{-6})$. We have

$$n = 2, \quad r = 0, \quad s = 1, \quad d_K = -6,$$

so

$$B = \sqrt{6} \cdot \frac{4}{\pi} \sim 3.1.$$

Thus $\mathrm{Cl}(K)$ is generated by the prime ideals lying over 2 and 3. We have $\mathcal{O}_K = \mathbf{Z}[\sqrt{-6}]$, and $\sqrt{-6}$ satisfies $x^2 + 6 = 0$. Factoring $x^2 + 6$ modulo 2 and 3 we see that the class group is generated by the prime ideals

$$\mathfrak{p}_2 = (2, \sqrt{-6}) \qquad \text{and} \qquad \mathfrak{p}_3 = (3, \sqrt{-6}).$$

Also, $\mathfrak{p}_2^2 = 2\mathcal{O}_K$ and $\mathfrak{p}_3^2 = 3\mathcal{O}_K$, so $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define elements of order dividing 2 in $\mathrm{Cl}(K)$.

Is either $\mathfrak{p}_2$ or $\mathfrak{p}_3$ principal? Fortunately, there is an easier norm trick that allows us to decide. Suppose $\mathfrak{p}_2 = (\alpha)$, where $\alpha = a + b\sqrt{-6}$. Then

$$2 = \mathrm{Norm}(\mathfrak{p}_2) = |\,\mathrm{Norm}(\alpha)| = (a + b\sqrt{-6})(a - b\sqrt{-6}) = a^2 + 6b^2.$$

Trying the first few values of $a, b \in \mathbf{Z}$, we see that this equation has no solutions, so $\mathfrak{p}_2$ can not be principal. By a similar argument, we see that $\mathfrak{p}_3$ is not principal either. Thus $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define elements of order 2 in $\mathrm{Cl}(K)$.

Does the class of $\mathfrak{p}_2$ equal the class of $\mathfrak{p}_3$? Since $\mathfrak{p}_2$ and $\mathfrak{p}_3$ define classes of order 2, we can decide this by finding the class of $\mathfrak{p}_2 \cdot \mathfrak{p}_3$. We have

$$\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (2, \sqrt{-6}) \cdot (3, \sqrt{-6}) = (6, 2\sqrt{-6}, 3\sqrt{-6}) \subset (\sqrt{-6}).$$

The ideals on both sides of the inclusion have norm 6, so by multiplicativity of the norm, they must be the same ideal. Thus $\mathfrak{p}_2 \cdot \mathfrak{p}_3 = (\sqrt{-6})$ is principal, so $\mathfrak{p}_2$ and $\mathfrak{p}_3$ represent the same element of $\mathrm{Cl}(K)$. We conclude that

$$\mathrm{Cl}(K) = \langle \mathfrak{p}_2 \rangle = \mathbf{Z}/2\mathbf{Z}.$$

2 The Group of Units

Definition 2.1 (Unit Group). The *group of units* U_K associated to a number field K is the group of elements of $\mathcal{O}_K$ that have an inverse in $\mathcal{O}_K$.

Proposition 2.2. *An element $a \in K$ is a unit if and only if* $\mathrm{Norm}(a) = \pm 1$.

Theorem 2.3. *The group U_K of units of $\mathcal{O}_K$ is the product of a finite cyclic group of roots of unity with a free abelian group of rank $r + s - 1$, where r is the number of real embeddings of K and s is the number of complex conjugate pairs of embeddings.*

Example 2.4 *(Pell's Equation).* The classical Pell's equation is, given square-free $d > 0$, to find all positive integer solutions (x, y) to the equation $x^2 - dy^2 = 1$. Note that if $x + y\sqrt{d} \in \mathbf{Q}(\sqrt{d})$, then

$$\mathrm{Norm}(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

The solutions to Pell's equation thus form a finite-index subgroup of the group of units in the ring of integers of $\mathbf{Q}(\sqrt{d})$. Theorem 2.3 implies that for any d the solutions to Pell's equation form an infinite cyclic group, a fact that takes substantial work to prove using only elementary number theory (for example, using continued fractions).