Introduction to Algebraic Number Theory
Lecture 17

Andrei Jorza

7 The Class Group (continued)

Theorem 1. *If K is a number field with r real and $2s$ complex embeddings then we may choose*

$$\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|}$$

Proof. Let E be the region of $\mathbb{R}^n$ given by

$$|x_1| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + 2\sqrt{x_{r+2s-1}^2 + x_{r+2s}^2} \leq n \sqrt[n]{\lambda ||I||}$$

where λ as in the statement of the theorem. Then E is centrally symmetric and convex (given by inequalities of a function which increases in all directions) and by the lemma we compute

$$\begin{aligned}\operatorname{vol}(E) &= \frac{2^{r-s}\pi^s n^n ||I||}{n!}\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(K)|} \\ &= 2^{r+s}||I||\sqrt{|\operatorname{disc}(K)|}\end{aligned}$$

It suffices to check that $\operatorname{vol}(E) > 2^n \operatorname{vol}(I)$ since then $E \cap I$ would have a nonzero vector α which would then satisfy $|N_{K/\mathbb{Q}}(\alpha)| \leq \lambda ||I||$. But

$$\begin{aligned}\operatorname{vol}(I) &= \operatorname{vol}(\mathbb{R}^n/\iota(I)) \\ &= [\mathcal{O}_K : I] \operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) \\ &= ||I||2^{-s}\sqrt{|\operatorname{disc}(K)|}\end{aligned}$$

from where the inequality $\operatorname{vol}(E) > 2^n \operatorname{vol}(I)$ is immediate.

The only thing to check is that $\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) = 2^{-s}\sqrt{|\operatorname{disc}(K)|}$ and this is left as an exercise. (The idea is that is $e_1, \ldots, e_n$ is an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$ then

$$\begin{aligned}\operatorname{vol}(\mathbb{R}^n/\iota(\mathcal{O}_K)) &= |\det(\sigma_1(e_j), \ldots, \sigma_r(e_j), \operatorname{Re}\sigma_{r+1}(e_i), \operatorname{Im}\sigma_{r+1}(e_i), \ldots)| \\ &= 2^{-s}\det(\sigma_1(e_j), \ldots, \sigma_r(e_j), \sigma_{r+1}(e_i), \overline{\sigma}_{r+1}(e_i), \ldots) \\ &= 2^{-s}\sqrt{|\operatorname{disc}(K)|}\end{aligned}$$

since the discriminant is the square of the matrix of embeddings.

□

Corollary 2. *If K is a number field with $2s$ complex embeddings then*

$$|\operatorname{disc}(K)| \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$$

In particular if $K \neq \mathbb{Q}$ then $K/\mathbb{Q}$ ramifies at some prime.

Proof. The inequality follows from the fact that the Minkowski bound ≥ 1 or else we would get no ideals at all. If $n = [K : \mathbb{Q}] \geq 2$ then the RHS in the inequality is ≥ 2 and we know that $K/\mathbb{Q}$ ramifies at primes dividing the nonunit discriminant. □

(7.3) Computing class groups.

Example 3. The class group of $K = \mathbb{Q}(\sqrt{-21})$ is $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Computing the Minkowski bound for K gives $\lambda = 5.8\ldots$ and so to find the ideals J (representing the classes in $\mathrm{Cl}(K)$) with $||J|| \leq 5$ it suffices to factor $2, 3, 5$ in $\mathcal{O}_K$. Using the problem from the homework 3, we factor $x^2 + 21 \mod 2, 3, 5$ and get (since $\mathrm{disc}(K) = -2^2 \cdot 3 \cdot 7$)

$$(2)\mathcal{O}_K = (2, 1 + \sqrt{-21})^2$$
$$(3)\mathcal{O}_K = (3, \sqrt{-21})^2$$
$$(5)\mathcal{O}_K = (5, 2 + \sqrt{-21})(5, 2 - \sqrt{-21})$$

Let $\mathfrak{q}_2 = (2, 1 + \sqrt{-21})$, $\mathfrak{q}_3 = (3, \sqrt{-21})$ and $\mathfrak{q}_5 = (5, 2 + \sqrt{-21})$. We first check that they are not principal, and only do it for the first ideal. Indeed, if $\mathfrak{q}_2 = (\alpha)$ then $|N_{K/\mathbb{Q}}(\alpha)| = ||\mathfrak{q}_2|| = \sqrt{||(2)\mathcal{O}_K||} = ||(2)\mathbb{Z}|| = 2$ but $\alpha = x + y\sqrt{-21}$ can never have norm 2 (or 3 or 5).

Next, it's quick to see (play around with generators) that $\mathfrak{q}_2\mathfrak{q}_3 = (6, 2\sqrt{-21})$ which again is not principal because it has norm 6 whereas $x^2 + 21y^2$ cannot be 6. Moreover, $\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_5 = (6, 2\sqrt{-21})(5, 2 + \sqrt{-21}) = (30, 3 - \sqrt{-21}) = (3 - \sqrt{-21})$ since $N_{K/\mathbb{Q}}(3 - \sqrt{-21}) = 30$.

Let a, b, c be the images of $\mathfrak{q}_2, \mathfrak{q}_3, \mathfrak{q}_5$ in $\mathrm{Cl}(K)$. Then $a^2 = b^2 = 1$ and $abc = 1$ and $\overline{c}c = 1$. We know that every class in $\mathrm{Cl}(K)$ has an ideal which is a product of prime ideals whose image in $\mathrm{Cl}(K)$ is a product of powers of a, b, c. Since $\overline{c} = c^{-1} = ab$ it follows that the only possibilities are $\{1, a, b, ab\}$ and the result follows.

□

(7.4) A little class field theory.

Theorem 4 (The Hilbert Class Field)**.** *Let K be a number field. There exists a finite Galois extension of number fields H/K (called the Hilbert class field) such that*

1. *$[H : K] = h_K$;*
2. *$\mathrm{Gal}(H/K)$ is an abelian group;*
3. *H/K is unramified at all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$;*
4. *If L/K is any other finite Galois extension with abelian Galois group and which is everywhere unramified then $L \subset H$.*
5. *Every ideal I of $\mathcal{O}_K$ becomes principal in $\mathcal{O}_H$, i.e., $I\mathcal{O}_H$ is principal.*

Example 5. From the homework $K = \mathbb{Q}(\sqrt{15})$ has the extension $H = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ which is quadratic and so abelian Galois over K and is everywhere unramified over K. Since $h_K = 2$ it follows that H is the Hilbert class field of K.

One typical application is the following result about class numbers of cyclotomic fields.

Corollary 6. *If $m \mid n$ then $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$ and $h_{\mathbb{Q}(\zeta_m)} \mid h_{\mathbb{Q}(\zeta_n)}$.*

The study of class numbers of cyclotomic fields is very rich and we mention two results, of which the first one is straightforward while the second one is very deep and difficult.

Theorem 7 (Kummer)**.** *Suppose p is a prime number which does not divide $h_{\mathbb{Q}(\zeta_p)}$. Then $x^p + y^p = z^p$ has no nontrivial integer solutions.*

Theorem 8 (Iwasawa)**.** *Suppose K is a number field. Then there exist integers $\lambda, \mu \geq 0$ and ν such that for n large enough*

$$v_p(h_{K(\zeta_{p^n})}) = \lambda n + \mu p^n + \nu$$

When $K/\mathbb{Q}$ is Galois it is conjectured that $\mu = 0$ and this is known when the Galois group over $\mathbb{Q}$ is an abelian group (by Ferrero-Washington).