Introduction to Algebraic Number Theory
Lecture 18

Andrei Jorza

8 Units

(8.1) The purpose of this section is to prove the following theorem of Dirichlet:

Theorem 1 (Dirichlet unit theorem). *Suppose K is a number field with r real and $2s$ complex embeddings. Then $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r+s-1$.*

Remark 1. Note that $\alpha \in \mathcal{O}_K^\times$ iff $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Example 2. $K = \mathbb{Q}(\sqrt{m})$ with $m > 0$. Then $r = 2, s = 0$ and the real quadratic field K has rank 1 unit group. E.g., $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}^\times = \pm(2+\sqrt{3})^{\mathbb{Z}}$.

Example 3. $K = \mathbb{Q}(\sqrt{m})$ with $m < 0$. Then $r = 0, s = 1$ and the imaginary quadratic number field K has finite unit group. E.g., $\mathcal{O}_{\mathbb{Q}(\zeta_3)}^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.

Example 4. $K = \mathbb{Q}(\sqrt[3]{2})$ has $r = 1, s = 1$ and so $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}^\times$ has rank 1. It turns out $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}^\times = \pm(\sqrt[3]{2}-1)^{\mathbb{Z}}$.

Example 5. For a more complicated example, take $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Then $\mathcal{O}_K^\times$ has rank 3 and in fact

$$\mathcal{O}_K^\times = \pm \left(\frac{1+\sqrt{5}}{2}\right)^{\mathbb{Z}} \left(\frac{1+\sqrt{5}}{2} - \sqrt{3}\right)^{\mathbb{Z}} \left(\frac{1+\sqrt{5}}{2} - \sqrt{3} - 1\right)^{\mathbb{Z}}$$

Example 6. $K = \mathbb{Q}(\zeta_{p^n})$ for p a prime. Then K is a quadratic extension of the real subfield $K^+ = \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1}) = \mathbb{Q}(\cos(2\pi/p^n))$. All the embeddings of K^+ are real and $K = K^+(i\sin(2\pi/p^n))$ and so all the $p^{n-1}(p-1)$ embeddings of K are complex. Thus $s = p^{n-1}(p-1)/2$ but we can no longer describe the s generators of $\mathcal{O}_K^\times$ explicitly. However, we can say that $\mathcal{O}_K^\times$ has a finite index subgroup generated (as a group) by ζ_{p^n} and $\zeta_{p^n}^{\frac{1-a}{2}} \dfrac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}} = \pm \dfrac{\sin(\pi a/p^n)}{\sin(\pi/p^n)}$ for $1 < a < p^n/2$ coprime to p.

Remark 2. If $K/\mathbb{Q}$ is Galois then either $r = 0$ or $s = 0$ as the Galois group acts transitively (and in fact can be identified with) the set of embeddings into $\mathbb{C}$.

(8.2) To understand the class group of K we used the embedding $\iota : K \to \mathbb{R}^n$ taking $\mathcal{O}_K$ to the lattice Λ and we implicitly used that this embedding was additive. To study $\mathcal{O}_K^\times$ we would like to transform the unpleasant multiplicative on $\mathcal{O}_K^\times$ to a much more usable additive structure on a vector space.

Consider the map $\log : \mathbb{R}^n \to \mathbb{R}^{r+s}$ given by

$$\log((x_1, \ldots, x_{r+2s})) = (\log|x_1|, \ldots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \ldots)$$

and $\sum : \mathbb{R}^{r+s} \to \mathbb{R}$ given by $\sum(x_1, \ldots, x_{r+s}) = x_1 + \cdots + x_{r+s}$.

Lemma 7.

1. *The composite map $\log \circ \iota : K^\times \to \mathbb{R}^n$ is additive, i.e., $\log(\iota(xy)) = \log(\iota(x)) + \log(\iota(y))$.*
2. *The image of $\mathcal{O}_K^\times$ lies in a hyperplane: $\log(\iota(\mathcal{O}_K^\times)) \subset \Delta$ where $\Delta = \{(x_1, \ldots, x_{r+s}) | x_1 + \cdots + x_{r+s} = 0\}$.*

3. *The additive subgroup* $\log(\iota(\mathcal{O}_K^\times)) \subset \Delta$ *is a discrete abelian subgroup and thus a lattice of rank* $d \le \operatorname{rank}(\Delta) = r + s - 1$.

Lemma 8. *Part one follows from the definition. Part two uses the fact that* $\alpha \in \mathcal{O}_K^\times$ *iff* $|N_{K/\mathbb{Q}}(\alpha)| = 1$ *and* $\sum \log(\iota(\alpha)) = \log |N_{K/\mathbb{Q}}(\alpha)|$. *For part three: the preimage under* $\log$ *of any open subset of* Δ *is an open subset of* $\mathbb{R}^n$ *which contains finitely many* $\iota(\alpha)$ *for* $\alpha \in \mathcal{O}_K^\times$ *as* $\iota(\mathcal{O}_K)$ *is a lattice in* $\mathbb{R}^n$.

(8.3) $\mathcal{O}_K^\times$ vs $\log \iota(\mathcal{O}_K^\times)$.

Proposition 9. *The kernel of* $\log \circ \iota|_{\mathcal{O}_K - 0}$ *consists of the roots of unity in* K *and is finite. Thus* $\mathcal{O}_K^\times$ *is a finitely generated abelian group of the same rank as* $\log \iota(\mathcal{O}_K^\times)$.

Proof. If $\alpha \in \mathcal{O}_K - 0$ has $\log \iota(\alpha) = 0$ then $|\sigma(\alpha)| = 1$ for all embeddings $\sigma : K \hookrightarrow \mathbb{C}$. The minimal polynomial of α is $P_\alpha(X) = \prod(X - \sigma(\alpha)) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ and

$$|a_{n-j}| = |\sum_{i_1 < \ldots < i_j} \sigma_{i_1}(\alpha) \cdots \sigma_{i_j}(\alpha)| \le \sum_{i_1 < \ldots < i_j} 1 = \binom{n}{j}$$

and so $P_\alpha(X)$ is in the finite set $\mathcal{F} = \{X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X] | |a_{n-j} \le \binom{n}{j}\}$. But the same is true of P_{α^k} for all k since the Galois conjugates of α^k are α_i^k. Thus P_{α^k} is in the same set. Since there are infinitely many choices for k it follows that $\alpha^k = \alpha^{k'}$ for at least two $k \ne k'$ and thus α is a root of unity.

If $\zeta_n \in K$ then $\mathbb{Q}(\zeta_n) \subset K$ and so $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \le [K : \mathbb{Q}]$ which puts a bound on n and so K contains finitely many roots of unity.

Therefore $\log \iota(\mathcal{O}_K^\times) \cong \mathcal{O}_K^\times / \mu(K)$ where $\mu(K)$ is the finite group of roots of unity in K and the conclusion follows. □