Algebraic Number Theory – Lecture 13

Lee Butler

"I have yet to see any problem, however complicated, which, when you looked at it in the right way, did not become still more complicated."

– Poul Anderson

1. The unit group

We've learnt quite a bit about the class group $\mathcal{H} = \mathcal{F}/\mathcal{P}$ of a number field K, and quite right too. This group and the group of units $\mathcal{O}_K^\times$ of $\mathcal{O}_K$ are two of the most studied objects in algebraic number theory. But why? The answer lies in the exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow \mathcal{F} \longrightarrow \mathcal{H} \longrightarrow 1.$$

Recall an exact sequence means the image of each map is the kernel of the next one. The middle map $K^\times \to \mathcal{F}$ is given by $a \mapsto (a)$.

So $\mathcal{H}$ measures the expansion that takes place passing from elements a to ideals (a). The bigger the image of this map, the smaller $\mathcal{H}$ will be, and vice versa. The unit group $\mathcal{O}_K^\times$, meanwhile, measures the contraction in this process. If $K^\times \to \mathcal{F}$ has a big kernel then $\mathcal{O}_K^\times$ is big, and vice versa. So both these groups are worth studying.

Definition. The group of units of a number field K is

$$\mathcal{O}_K^\times = \{u \in \mathcal{O}_K \,:\, \exists v \in \mathcal{O}_K \; uv = 1\}.$$

A finite subgroup of this group is the group of roots of unity

$$\mu(K) = \{\alpha \in K \,:\, \exists m \in \mathbb{N} \; \alpha^m = 1\}.$$

Usually $\mathcal{O}_K^\times$ itself isn't finite. But how big is it? The answer is contained in Dirichlet's unit theorem and says that the size of $\mathcal{O}_K^\times$ depends on the number of real and complex embeddings of K. To prove it we need some set up.

2. Lattices and vector spaces

Recall from Mike's talk on the finiteness of the class number that a number field K of degree n can be embedded into a real vector space of dimension n. If K has r real embeddings ρ_i and s pairs of complex embeddings $\sigma_j, \overline{\sigma_j}$, then he defined $L^{rs} = \mathbb{R}^r \times \mathbb{C}^s$ and a map $j : K \to L^{rs}$ by

$$j(a) = (\rho_1(a), \dots, \rho_r(a), \sigma_1(a), \dots, \sigma_s(a)).$$

The image of this map is the $\mathbb{R}$-vector space $K_\mathbb{R} \cong \mathbb{R}^{r+2s}$. If one writes vectors explicitly as $(r + 2s)$-tuples then one has vectors looking like

$$(\rho_1(a), \dots, \rho_r(a), \operatorname{Re}\sigma_1(a), \operatorname{Im}\sigma_1(a), \dots, \operatorname{Re}\sigma_s(a) \operatorname{Im}\sigma_s(a)).$$

A second $\mathbb{R}$-vector space can be gleaned from this, the space $[\prod_\tau \mathbb{R}]^+$ of points like the above where $\overline{\operatorname{Re}\sigma_1(a)} = \operatorname{Im}\sigma_1(a)$. So the s pairs of points are all of the form (x, x), hence we may map them to, say, $2x$ and identify $[\prod_\tau \mathbb{R}]^+$ with $\mathbb{R}^{r+s}$. If this looks like a funky definition it's because it's a restriction to complex-conjugation invariant points of a complex vector space.

Anyway, there is a commutative diagram

$$\begin{tikzcd}
K^\times \arrow[r, "j"] \arrow[d, "N_{K/\mathbb{Q}}"'] & K_\mathbb{R}^\times \arrow[r, "\ell"] \arrow[d, "N"'] & \left[\prod_\tau \mathbb{R}\right]^+ \arrow[d, "Tr"'] \\
\mathbb{Q}^\times \arrow[r] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R}
\end{tikzcd}$$

where ℓ is the homomorphism induced by $\log|\cdot|$, N is the product of the coordinates, and Tr is the sum of the coordinates. We take subgroups of the top row:

$$\mathcal{O}_K^\times = \{\varepsilon \in \mathcal{O}_K \,:\, N_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}, \quad \text{the group of units,}$$
$$S = \{y \in K_\mathbb{R}^\times \,:\, N(y) = \pm 1\}, \quad \text{the "norm-one surface",}$$
$$H = \{x \in [\textstyle\prod_\tau \mathbb{R}]^+ \,:\, Tr(x) = 0\}, \quad \text{the "trace-zero" hyperplane.}$$

So we have homomorphisms

$$\mathcal{O}_K^\times \xrightarrow{j} S \xrightarrow{\ell} H,$$

and we let $\lambda = \ell \circ j : \mathcal{O}_K^\times \to H$. We let $\Gamma = \lambda(\mathcal{O}_K^\times) \subseteq H$, and then get the short exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \longrightarrow 0.$$

Our new task, then, is to understand Γ.

We know that there are only finitely many ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ of a given norm, and the same holds true for elements.

Proposition 1. *Up to multiplication by units, there are only finitely many elements in $\mathcal{O}_K$ of a given norm.*

H is a subspace of $[\prod_\tau \mathbb{R}]^+$ given by one equation (hence a hyperplane), so it has dimension $r + s - 1 = t$. Using proposition 1, one can show the following.

Proposition 2. *The group Γ is a complete lattice in H, so is isomorphic to $\mathbb{Z}^t$.*

Sketch proof. To be a lattice it suffices to show any bounded domain in H contains only finitely many elements of Γ. To do this one takes the preimage of a bounded domain under ℓ and uses the fact that $j(\mathcal{O}_K)$ is a lattice in $[\prod_\tau \mathbb{C}]^+$.

For completeness it suffices to show the existence of a bounded subset $M \subseteq H$ such that $M + \gamma$, $\gamma \in \Gamma$, covers H. To do this one finds such a subset in S and transfers it to H with ℓ. $\square$

3. Dirichlet's unit theorem

We can now prove the following.

Theorem (Dirichlet's unit theorem)**.** *The group $\mathcal{O}_K^\times$ is isomorphic to the direct product $\mu(K) \otimes \mathbb{Z}^{r+s-1}$.*

This means there are $t = r + s - 1$ units $\varepsilon_1, \ldots, \varepsilon_t$, called the fundamental units, such that any unit ε can be written uniquely as

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t}$$

for a root of unity ζ and integers ν_i.

Proof. Consider the exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{\lambda} \Gamma \longrightarrow 0.$$

By proposition 2, Γ is a free abelian group of rank t. Let $v_1, \ldots, v_t$ be a $\mathbb{Z}$-basis for Γ, let $\varepsilon_1, \ldots, \varepsilon_t$ be the preimage of each v_i under λ, and let $A \subset \mathcal{O}_K^\times$ be the subgroup of $\mathcal{O}_K^\times$ generated by these ε_i. Then λ gives the isomorphism $A \cong \Gamma$, so in particular $\mu(K) \cap A = \{1\}$. So $\mathcal{O}_K^\times \cong \mu(K) \otimes A$. $\square$

Since Γ is a lattice it has a fundamental parallelepiped. The volume of this is equal to $R\sqrt{r+s}$, where R is called the regulator of K. It is equal to the absolute value of any minor of rank t of the matrix

$$\begin{pmatrix} \log|\rho_1(\varepsilon_1)| & \cdots & \log|\rho_1(\varepsilon_t)| \\ \vdots & & \vdots \\ \log|\rho_r(\varepsilon_1)| & \cdots & \log|\rho_r(\varepsilon_t)| \\ \log|\sigma_1(\varepsilon_1)| & \cdots & \log|\sigma_1(\varepsilon_t)| \\ \vdots & & \vdots \\ \log|\sigma_s(\varepsilon_1)| & \cdots & \log|\sigma_s(\varepsilon_t)| \end{pmatrix}.$$