Algebraic Number Theory

Lecture 12, 14th January

Recall Lecture 10 :

K: number field
r: # real embeddings
s: # pairs of complex emb.

$$j : K \longrightarrow K_{\mathbb{C}} := \prod_{\tau : K \to \mathbb{C}} \mathbb{C}$$
$$a \longmapsto (\tau(a)) = (a_\tau)$$

$F : z \mapsto \bar{z}$

Action of $G(\mathbb{C}/\mathbb{R}) = \langle F \rangle$ on $\mathrm{Hom}_{\mathbb{Q}}(K; \mathbb{C})$: $F(\tau) = \bar{\tau}$

$K_{\mathbb{C}}$: $(F(z))_\tau = \bar{z}_{\bar{\tau}}$.

$$K_{\mathbb{R}} = \{ z \in K_{\mathbb{C}} \mid z_{\bar{\tau}} = \bar{z}_\tau \}.$$

$\| \quad [K_{\mathbb{C}}]^+$ F-invariant subspace

$(z_\tau) \in K_{\mathbb{C}} \mid z_{\rho} \in \mathbb{R},\ z_{\bar{\sigma}_j} = \bar{z}_{\sigma_j} \}$

$(K_{\mathbb{R}}, \langle , \rangle)$ euclidean vector space

Multiplicative version:

$$j : K^\times \longrightarrow K_{\mathbb{C}}^\times = \prod_\tau \mathbb{C}^\times$$

$$N : K_{\mathbb{C}}^\times \longrightarrow \mathbb{C}^\times, \qquad (z_\tau) \longmapsto \prod_\tau z_\tau.$$

$$\ell : K_{\mathbb{C}}^\times \longrightarrow \prod_\tau \mathbb{R}, \qquad (z_\tau) \longmapsto (\ell(z_\tau)), \quad \ell(z_\tau) = \log(|z_\tau|)$$

Commutative diagram: $\left[\prod_\tau \mathbb{C}^\times\right]^+ = K_{\mathbb{R}}^\times$

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

§ 9 Dirichlet's unit theorem

In this section we want to understand $\mathcal{O}_K^\times$.

Let $\mu(K)$ be the set of roots of unity contained in K. Then we have $\mu(K) \subseteq \mathcal{O}_K^\times$.

We set

$$S = \{ y \in K_{\mathbb{R}}^\times \mid N(y) = \pm 1 \}$$

$$H = \{ x \in [\prod_\tau \mathbb{R}]^+ \mid \mathrm{Tr}(x) = 0 \}$$

and consider the map

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

and define $\Gamma = \lambda(\mathcal{O}_K^\times) \subseteq H$.

Proposition 9.1 The sequence

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

is exact, i.e. $\ker \lambda = \mu(K)$.

Proof: • Let $\varepsilon \in \mathcal{O}_K^\times$ with $\lambda(\varepsilon) = 0$. Then $|\tau(\varepsilon)| = 1$ for all $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.

The points $j(\varepsilon) = (\tau(\varepsilon))_\tau$ therefore lie in a bounded domain of $K_{\mathbb{R}}$. But $j(\varepsilon)$ is also a point of the lattice $j(\mathcal{O}_K)$, i.e. there are just finitely many $\varepsilon \in \mathrm{Ker}(\lambda) \Rightarrow \varepsilon \in \mu(K)$

$$\Rightarrow \mathrm{Ker}(\lambda) \subset \mu(K).$$

- $\mu(K) \subset \mathrm{Ker}(\lambda)$ is clear since for $\varepsilon \in \mu(K)$ we have $|\tau(\varepsilon)| = 1$, i.e $\ell(\tau(\varepsilon)) = 0$. $\square$

Lemma 9.2 For a given $a \in \mathbb{Z}$, there are, up to associates, only finitely many $\alpha \in \mathcal{O}_K$ with $N_{K/\mathbb{Q}}(\alpha) = a$.

Proof: Let $a \in \mathbb{Z}$. We show that every class in $\mathcal{O}_K / a\mathcal{O}_K$ has at most one element of norm a (up to units).

Suppose there are two α, β with $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta) = a$ and

$$\beta = \alpha + a\gamma \qquad \gamma \in \mathcal{O}_K.$$

Then $\quad \dfrac{\alpha}{\beta} = 1 - \underbrace{\dfrac{N(\beta)}{\beta}}_{\in \mathcal{O}_K} \gamma \in \mathcal{O}_K .$

With the same argument we see $\frac{\beta}{\alpha} \in \mathcal{O}$, i.e $\alpha \sim \beta$. Therefore there are at most $[\mathcal{O}_K : a\mathcal{O}_K]$ elements with norm a. $\square$

Proposition 9.3 The group Γ $(= \lambda(\mathcal{O}_K^\times))$ is a complete lattice in the $(r+s-1)$-dimensional vectorspace H, i.e. $\Gamma \cong \mathbb{Z}^{r+s-1}$.

Proof: • First we show that Γ is a lattice (discrete subgroup) of H:

Prop. 5.3

The map $\lambda : \mathcal{O}_K^\times \longrightarrow H$ arises by restricting

$$\begin{array}{ccccc} & & & & H \\ & & & & \cap \\ K^\times & \xrightarrow{j} & \prod_\tau \mathbb{C}^\times & \xrightarrow{\ell} & \prod_\tau \mathbb{R} . \end{array}$$

Want to show: For any $c > 0$, the bounded domain $(*) = \{ (x_\tau) \in \prod_\tau \mathbb{R} \mid |x_\tau| \leq c \}$ just contains fin. many points in Γ.

The preimage of this domain with respect to ℓ ist

$$\{(z_\tau) \in \prod_\tau \mathbb{C}^\times \mid e^{-c} \leq |z_\tau| \leq e^{c}\}$$

$$(\ell(z_\tau) = \log(|z_\tau|))$$

Since $j(\mathcal{O}_K^\times) \subset j(\mathcal{O}_K)$ there are just finitely

lattice in $[\prod_\tau \mathbb{C}^\times]^+$

many points of Γ in $(*)$. Clearly $\dim H = \overset{r+s-1}{\overset{\shortparallel}{\dim [\prod \mathbb{R}]^+ - 1}}$

- <u>Γ is complete:</u> By Lemma 5.4 we need to show that there exists a bounded set $M \subseteq H$ such that

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma).$$

$$\left(\begin{tikzcd}
 & T \arrow[d, phantom, "\cap"] & M \arrow[d, phantom, "\cap"] \\
\mathcal{O}_K^\times \arrow[r] \arrow[d, phantom, "\cap"] & S \arrow[r] \arrow[d, phantom, "\cap"] & H = \ell(S) \arrow[d, phantom, "\cap"] \\
K^\times \arrow[r, "j"] \arrow[d, phantom, "\cup"] & K_{\mathbb{R}}^\times \arrow[r, "\ell"] & {[\prod_\tau \mathbb{R}]^+} \\
\mathcal{O}_K^\times \arrow[rr, "\lambda = \ell \circ j"] & & \Gamma = \lambda(\mathcal{O}_K^\times) \arrow[d, phantom, "\cap"] \\
 & & H
\end{tikzcd}\right)$$

For this we will show that there exists a bounded set $T \subseteq S$ with

$$S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} T\, j(\varepsilon). \qquad (M = \ell(T))$$

If T is bounded then also M will be

bounded, since for x_τ $(x_\tau) \in T$ we have $\prod_\tau |x_\tau| = 1$, i.e. $\exists a, b$: $0 < b \leq |x_\tau| \leq a$ for a, b independent of x.

- <u>Finding T</u>: We choose real $c_\tau > 0$ for $\tau \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ with $c_\tau = c_{\bar\tau}$, s.th

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}.$$

Now set

$$X := \{ (z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < c_\tau \}$$

and for $y = (y_\tau) \in S$ we get

$$Xy = \{ (z_\tau) \in K_{\mathbb{R}} \mid |z_\tau| < \underbrace{c_\tau |y_\tau|}_{=: c'_\tau} \}.$$

We have $c'_{\bar\tau} = c'_\tau$ and

$$\prod_\tau c'_\tau = \prod_\tau c_\tau \underbrace{\prod_\tau |y_\tau|}_{\substack{= |N(y)| = 1 \\ \text{because } y \in S}} = C.$$

By Theorem 6.4 there exist an $a \in \mathcal{O}_K \setminus \{0\}$ with $j(a) \in Xy$. $(\ast)$

By Lemma 9.2. there are (up to units) just fin. many $a \in \mathcal{O}_K$ with $0 < |N_{K/\mathbb{Q}}(a)| \leq C$.

Denote these by $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$ with $\alpha_i \neq 0$.

(Any $a \in \mathcal{O}_K$ with $0 < |N_{K/\mathbb{Q}}(a)| \leq C$ is associated to exactly one of the α_i).

Set
$$T = S \cap \bigcup_{i=1}^{N} X j(\alpha_i)^{-1}.$$

X bounded $\Rightarrow$ $X j(\alpha_i)^{-1}$ bounded $\Rightarrow$ T bounded.

Remains to show: $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} T j(\varepsilon)$

Let $y \in S$, then we can find by $(\ast)$ an $a \in \mathcal{O}_K \setminus \{0\}$ with $j(a) \in X y^{-1}$, i.e $j(a) = x y^{-1}$ for some $x \in X$.

Since $|N_{K/\mathbb{Q}}(a)| = |N(x y^{-1})| = |N(x)| \leq C$

we have $\alpha_i = \varepsilon a$ for some $1 \le i \le N$ and $\varepsilon \in \mathcal{O}_K^\times$.

$$\Rightarrow \quad y = x\, j(a)^{-1} = x\, j(\alpha_i^{-1} \varepsilon).$$

Since $y, j(\varepsilon) \in S$ we get

$$x\, j(\alpha_i^{-1}) \in S \cap X j(\alpha_i^{-1}) \subseteq T$$

$$\Rightarrow \quad y \in T j(\varepsilon) \qquad \square$$

Theorem 9.4 (Dirichlet's unit theorem)

The unit group $\mathcal{O}_K^\times$ is given by a direct product of the cyclic group $\mu(K)$ and a free abelian group of rank $r+s-1$, i.e.

$$\mathcal{O}_K^\times \cong \mu(K) \oplus \mathbb{Z}^{r+s-1}.$$

Proof: In the exact sequence

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

we have that (by Prop. 9.3) that Γ is a free abelian group of rank $t = r+s-1$

Let $v_1, \dots, v_t$ be a $\mathbb{Z}$-basis of Γ and let $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_K^\times$ with $\lambda(\varepsilon_i) = v_i$. Let A be the subgroup of $\mathcal{O}_K^\times$ generated by the ε_i.

Then $\lambda : A \xrightarrow{\sim} \Gamma$ and $\mathcal{O}_K^\times \cong \mu(K) \times A$.
(i.e. $\mu(K) \cap A = \{1\}$)

$\square$

Remark 9.5

By Thm. 9.4 there exist units $\varepsilon_1, \dots, \varepsilon_t$ $(t = r+s-1)$ called the <u>fundamental units</u>, such that any unit $\varepsilon \in \mathcal{O}_K^\times$ can be written as

$$\varepsilon = \zeta\, \varepsilon_1^{v_1} \cdots \varepsilon_t^{v_t}$$

with $\zeta \in \mu(K)$ and $v_1, \dots, v_t \in \mathbb{Z}$.