MATH 225A: LECTURE 15
NOVEMEBR 16, 2021
SCRIBE: CHENGZHANG SUN

Last Time

We were in the middle of the proof of Dirichlet's unit theorem (Theorem 5.18). The setup is as follows.

Let $K/\mathbb{Q}$ be a number field of degree n. Let s and $2t$ be the number of real and complex embeddings $K \to \mathbb{C}$ respectively. We defined the logarithmic embedding

$$L : K^\times \to \mathbb{R}^{s+t}.$$

We saw that the image of $\mathcal{O}_K^\times$ is contained in the hyperplane

$$H = \left\{ (\xi_1, \dots, \xi_{s+t}) \in \mathbb{R}^{s+t} : \sum_{i=1}^{s} \xi_i + 2 \sum_{i=s+1}^{s+t} \xi_i = 0 \right\}.$$

We identified H with $\mathbb{R}^r$ by

$$(\xi_1, \dots, \xi_{s+t}) \mapsto (\xi_1, \dots, \xi_r), \quad \text{where } r = s + t - 1.$$

The goal was to show that for any nonzero linear functional

$$f(\underset{\sim}{\xi}) = \sum_{i=1}^{r} c_i \xi_i,$$

there exists some $u \in \mathcal{O}_K^\times$ such that f does not vanish at $L(u)$. To this end, we fixed $\alpha \in \mathbb{R}$ such that

$$\alpha \geq \left(\frac{2}{\pi}\right)^t |\,\mathrm{d}_{K/\mathbb{Q}}\,|^{1/2}.$$

For any $\underset{\sim}{\lambda} = (\lambda_1, \ldots, \lambda_r) \in \mathbb{R}_+^r$, we set $\underset{\sim}{\lambda}' = (\lambda_1, \ldots, \lambda_r, \lambda_{s+t}) \in \mathbb{R}_+^{s+t}$ where λ_{s+t} is chosen such that

$$\prod_{i=1}^{t} \lambda_i \prod_{i=s+1}^{s+t} \lambda_i^2 = \alpha.$$

We defined a box

$$B_{\underset{\sim}{\lambda},\alpha} = \{(y_1, \ldots, y_s, z_1, \ldots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t : \forall i, |y_i| \leq \lambda_i, |z_i| \leq \lambda_{s+i}\}.$$

We showed that, by our choice of α,

$$\operatorname{Vol}(B_{\underset{\sim}{\lambda},\alpha}) = 2^s \pi^t \alpha \geq 2^{s+t} |\operatorname{d}_{K/\mathbb{Q}}|^{1/2} = 2^n \operatorname{Vol}(\underset{\sim}{\sigma}(\mathcal{O}_K)).$$

Hence, by Blichfeldt, there exists $x_{\underset{\sim}{\lambda}} \in \mathcal{O}_K \setminus \{0\}$ such that $\underset{\sim}{\sigma}(x_{\underset{\sim}{\lambda}}) \in B_{\underset{\sim}{\lambda},\alpha}$, and we deduced that $\alpha^{-1}\lambda_i \leq |x_{\underset{\sim}{\lambda}}^{\sigma_i}| \leq \lambda_i$ for $i = 1, \ldots, s+t$.

The Present

Taking logarithm of the last inequality, we get

$$\log \lambda_i - \log \alpha \leq \log |x_{\underset{\sim}{\lambda}}^{\sigma_i}| \leq \log \lambda_i.$$

Hence,

$$0 \leq \log \lambda_i - \log |x_{\underset{\sim}{\lambda}}^{\sigma_i}| \leq \log \alpha. \tag{1}$$

By the definition of f and L, we have

$$f(L(x_{\underset{\sim}{\lambda}})) = \sum_{i=1}^{r} c_i \log |x_{\underset{\sim}{\lambda}}^{\sigma_i}|,$$

and thus

$$\left| f(L(x_{\underset{\sim}{\lambda}})) - \sum_{i=1}^{r} c_i \log \lambda_i \right| \leq \sum_{i=1}^{r} |c_i| (\log \lambda_i - \log |x_{\underset{\sim}{\lambda}}^{\sigma_i}|) \leq \sum_{i=1}^{r} |c_i| \log \alpha, \tag{2}$$

where the last inequality is due to (1). We fix any $\beta > \sum_{i=1}^{r} |c_i| \log \alpha$. Note that the inequalities (1) and (2) hold for any $\underset{\sim}{\lambda} \in \mathbb{R}_+^r$.

Next for each $h \in \mathbb{N}$, we can construct a vector

$$\underset{\sim}{\lambda}(h) = (\lambda_1(h), \ldots, \lambda_r(h)) \in \mathbb{R}_+^r$$

such that

$$\sum_{i=1}^{r} c_i \log \lambda_i(h) = 2\beta h. \tag{3}$$

Then we produce a sequence of nonzero algebraic integers $\{x_{\underset{\sim}{\lambda}(h)}\}_{h=1}^{\infty}$. By (2) and (3) (and the choice of β), we have

$$|f(L(x_{\underset{\sim}{\lambda}(h)})) - 2\beta h| < \beta,$$

and thus

$$(2h-1)\beta < f(L(x_{\underset{\sim}{\lambda}(h)})) < (2h+1)\beta. \tag{4}$$

Hence, $f(L(x_{\underset{\sim}{\lambda}(h)}))$'s are distinct.

On the other hand, we can compute the norm of these integers

$$\mathrm{N}_{K/\mathbb{Q}}(x_{\underset{\sim}{\lambda}(h)}) = \prod_{i=1}^{n} x_{\underset{\sim}{\lambda}(h)}^{\sigma_i} \leq \prod_{i=1}^{t} \lambda_i(h) \prod_{i=s+1}^{s+t} \lambda_i(h)^2 = \alpha.$$

Hence, the sequence of integral ideals $\{x_{\underset{\sim}{\lambda}(h)}\mathcal{O}_K\}_{h=1}^{\infty}$ cannot be distinct since there are only finitely many ideals with norm $\leq \alpha$.

We take $i \neq j$ with $x_{\underset{\sim}{\lambda}(i)}\mathcal{O}_K = x_{\underset{\sim}{\lambda}(j)}\mathcal{O}_K$. Then there exists $u \in \mathcal{O}_K^{\times}$ such that $x_{\underset{\sim}{\lambda}(i)} = u x_{\underset{\sim}{\lambda}(j)}$. By the definition of L, we have

$$L(x_{\underset{\sim}{\lambda}(i)}) = L(u) + L(x_{\underset{\sim}{\lambda}(j)}).$$

Finally apply the linear functional f to both sides. We get

$$f(L(x_{\underset{\sim}{\lambda}(i)})) = f(L(u)) + f(L(x_{\underset{\sim}{\lambda}(j)})),$$

which implies that $f(L(u)) \neq 0$ since $f(L(x_{\underset{\sim}{\lambda}(i)})) \neq f(L(x_{\underset{\sim}{\lambda}(j)}))$ by (4). This finishes the proof of Theorem 5.18 as u is a unit such that f does not vanish at $L(u)$. ■

Remarks and calculations with units.

(1) Terminology: Let $u_1, \dots, u_r$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K^\times/\mu_K$, the latter being a free $\mathbb{Z}$-module of rank $r = s + t - 1$ by Dirichlet's unit theorem. We call this a *system of fundamental units* for K. In general this is hard to determine.

(2) Cyclotomic units: Let p be an odd prime, and $\zeta = e^{2\pi i/p}$. Let $K = \mathbb{Q}(\zeta + \zeta^{-1})$. Then we have a tower of fields.

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \Big| \Big)\, 2 \\ K \\ \Big| \Big)\, \frac{p-1}{2} \\ \mathbb{Q} \end{array}$$

We know that $\mathbb{Q}(\zeta)$ is totally imaginary, and it is also easy to see that K is totally real since all Galois conjugates of $\zeta + \zeta^{-1}$ are

$$\zeta^i + \zeta^{-i}, \quad i = 1, \dots, \frac{p-1}{2}.$$

It follows from Dirichlet's unit theorem that

$$r_K = r_{\mathbb{Q}(\zeta)} = \frac{p-1}{2} - 1.$$

Hence, the index

$$(\mathcal{O}_{\mathbb{Q}(\zeta)}^\times : \mathcal{O}_K^\times) < \infty.$$

Let

$$v_i = \frac{\zeta - \zeta^{-1}}{\zeta^i - \zeta^{-i}}, \quad i = 1, \dots, \frac{p-1}{2}.$$

Then $v_i \in \mathcal{O}_K^\times$. (To see that $v_i \in \mathcal{O}_K$, we pick an integer j such that $ij \equiv 1 \pmod{p}$, and then $v_i = \zeta^{i(j-1)} + \zeta^{i(j-3)} + \cdots + \zeta^{i(1-j)} \in \mathcal{O}_K$.

Similarly we see that $v_i^{-1} \in \mathcal{O}_K$.) Using the theory of L-functions, one obtains that

$$(\mathcal{O}_K^\times : \langle v_1, \ldots, v_{\frac{p-1}{2}} \rangle) < \infty,$$

which is equal to the class number of K. (See Washington, Theorem 8.2.) Finally, by Kummer's theorem one can show that

$$\mathcal{O}_{\mathbb{Q}(\zeta)}^\times = \langle \zeta \rangle \times \mathcal{O}_K^\times.$$

(3) Find units of infinite order in $K = \mathbb{Q}(\sqrt[3]{5})$: In this case, $s = 1$, $2t = 2$, so $r_K = 1$. Set $\theta = \sqrt[3]{5}$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$. (Problem sheet #7.) By Kummer's theorem, we know that 3 ramifies in $K/\mathbb{Q}$:

$$3\mathcal{O}_K = \mathfrak{p}^3,$$

since $x^3 - 5 \equiv (x+1)^3 \pmod 3$. Note that $\mathrm{N}_{K/\mathbb{Q}}(2-\theta) = 3$, so $(2-\theta)$ is a prime lying over 3. Hence, $\mathfrak{p} = (2-\theta)$, and 3 differs by a unit from

$$(2-\theta)^3 = 3(1 - 4\theta + 2\theta^2).$$

This implies that $1 - 4\theta + 2\theta^2$ is a unit. It is not a root of unity, so it is a unit of infinite order.

(4) Imaginary quadratic fields: In this case $s = 0$, $2t = 2$, so $r = 0$. We have

$$\mathcal{O}_K^\times = \mu_K = \begin{cases} \text{6th roots of unity}, & d_K = -3; \\ \text{4th roots of unity}, & d_K = -4; \\ \pm 1, & \text{otherwise}. \end{cases}$$

(5) Real quadratic fields: In this case $s = 2$, $2t = 0$, so $r = 1$. Hence,

$$\mathcal{O}_K^\times = \{\pm 1\} \times \langle u \rangle.$$

If $d \not\equiv 1 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. To find a fundamental unit u, we write

$$u = a + b\sqrt{d},$$

and we can assume that $a, b > 0$ by replacing u by $\pm u^{\pm 1}$ if necessary. Note that $u^n = (a + b\sqrt{d})^n = a_n + b_n\sqrt{d}$ where the sequence $\{b_n\}$ is strictly increasing. Hence, if u is a unit as above such that b is minimal, then u must be a fundamental unit.

Example. For $K = \mathbb{Q}(\sqrt{2})$, we have a unit $1 + \sqrt{2}$. Since $b = 1$ is clearly minimal, this is a fundamental unit.

6. Galois action and prime decomposition

Let L/K be a Galois extension of number fields. We consider a prime $\mathfrak{p}$ of $\mathcal{O}_K$ and a prime $\mathfrak{P}$ lying over $\mathfrak{p}$.

$$\begin{array}{ccc} L & \text{———} & \mathfrak{P} \\ \Gamma\big(\Big| & & \Big| \\ K & \text{———} & \mathfrak{p} \end{array}$$

Suppose that

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^e.$$

Recall that the Galois group Γ acts transitively on $\mathfrak{P}_i$'s. (Theorem 4.3.)

Definition 6.1. (1) The *decomposition group* of $\mathfrak{P}/\mathfrak{p}$ in L/K is

$$\Gamma_{\mathfrak{P}} = \{\gamma \in \Gamma : \mathfrak{P}^\gamma = \mathfrak{P}\},$$

i.e., the stabilizer of $\mathfrak{P}$ in Γ.

(2) The *inertial group* of $\mathfrak{P}/\mathfrak{p}$ in L/K is

$$T_{\mathfrak{P}} = \{\gamma \in \Gamma : \forall x \in \mathcal{O}_L, x^\gamma \equiv x \pmod{\mathfrak{P}}\}.$$

Alternatively, write $\mathcal{O}_L/\mathfrak{P} = l$ and $\mathcal{O}_K/\mathfrak{p} = k$. Then reduction modulo $\mathfrak{P}$ induces a group homomorphism

$$\rho : \Gamma_{\mathfrak{P}} \to \mathrm{Gal}(l/k).$$

More precisely, for $\gamma \in \Gamma_{\mathfrak{P}}$ and $x \in \mathcal{O}_L$, we define

$$\bar{x}^{\rho(\gamma)} = \overline{x^{\gamma}}.$$

This is well-defined since $\gamma \in \Gamma_{\mathfrak{P}}$. Then

$$T_{\mathfrak{P}} = \operatorname{Ker} \rho \trianglelefteq \Gamma_{\mathfrak{P}}.$$

Definition 6.2. The *decomposition field* of $\mathfrak{P}/\mathfrak{p}$ in L/K is

$$D_{\mathfrak{P}} = L^{\Gamma_{\mathfrak{P}}},$$

i.e., the subfield of L field by the decomposition group $\Gamma_{\mathfrak{P}}$.