12. Dirichlet's unit theorem

K = number field, $\mathcal{O}_K$ = ring of integers

$\mathcal{O}_K^\times$ = group of units in $\mathcal{O}_K$, i.e. $x \in \mathcal{O}_K$, s.t. $\exists y \in \mathcal{O}_K : xy = 1$.

Recall: $\forall x \in K \quad N_{K/\mathbb{Q}}(x) = \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(x) \in \mathbb{Q}$

$\forall x \in \mathcal{O}_K \quad N_{K/\mathbb{Q}}(x) \in \mathbb{Z}$

<u>Lemma 12.1</u> $x \in \mathcal{O}_K^\times \iff N_{K/\mathbb{Q}}(x) = \pm 1$

<u>Proof</u> ($\Rightarrow$) If $x \in \mathcal{O}_K^\times$ $\exists y$: $xy = 1$

$\underbrace{N(x)}_{\in \mathbb{Z}} \cdot \underbrace{N(y)}_{\in \mathbb{Z}} = 1 \Rightarrow N(x) = \pm 1$

($\Leftarrow$) Assume $N_{K/\mathbb{Q}}(x) = \pm 1$

Let $K \subset L$ with L Galois ext. of $\mathbb{Q}$

then $N_{L/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(x)^{[L:K]} = \pm 1$

Prop. 4.4, prop. 4.1 (Lecture 3)

and $N_{L/\mathbb{Q}}(x) = \prod_{g \in Gal(L/\mathbb{Q})} g(x)$

Let $y = \underbrace{N_{L/\mathbb{Q}}(x)/x}_{\in K} = \prod_{\substack{g \in Gal(L/\mathbb{Q}) \\ g \neq id}} g(x) \in \underbrace{\mathcal{O}_L \cap K}_{= \mathcal{O}_K}$

and $xy = 1$

$\square$

Recall: $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$,

as $\mathbb{R}$-algebras

there are r_1 real embeddings

$$\sigma_i : K \hookrightarrow \mathbb{R} \qquad i = 1, \dots, r_1$$

and r_2 pairs of conjugate complex emb.

$$\sigma_j, \overline{\sigma_j} : K \hookrightarrow \mathbb{C}, \quad j = r_1+1, \dots, r_1+r_2$$

Under the natural embedding

$$K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R}$$

$$x \longmapsto x \otimes 1$$

$x \in K$ has coordinates

$$\left(\sigma_1(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)\right) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

Consider the map $\rho : \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$

$$\rho(x) = \left(\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1+r_2}(x)|\right)$$

from $\log|ab| = \log|a| + \log|b|$

$\Longrightarrow \rho$ is group homomorphism

Let us introduce a scalar product on $\mathbb{R}^{r_1+r_2}$:

<u>Def</u> for $\lambda = (\lambda_1 \dots \lambda_{r_1+r_2})$, $\mu = (\mu_1, \dots, \mu_{r_1+r_2})$ in $\mathbb{R}^{r_1+r_2}$ let $\langle \lambda, \mu \rangle = \sum_{i=1}^{r_1} \lambda_i \mu_i + 2 \sum_{j=r_1+1}^{r_1+r_2} \lambda_j \mu_j$

This scalar prod. is given by a diag. matrix

$$\begin{array}{c} r_1\{ \\ r_2\{ \end{array}\begin{pmatrix} 1\ldots1 & 0 \\ 0 & 2\ldots2 \end{pmatrix}$$

<u>Denote:</u> $v_0 = (1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$

$$H = v_0^{\perp} \subset \mathbb{R}^{r_1+r_2}$$

orthog. comp. w.r.t. $\langle -,- \rangle$

<u>Lemma 12.2</u> 1) $\forall x \in \mathcal{O}_K^{\times}$

$$\langle v_0, \rho(x) \rangle = \log |N_{K/\mathbb{Q}}(x)|$$

2) $\mathrm{Ker}(\rho) = \{\text{root of unity in } K\}$

3) $\mathrm{Im}(\rho) \subset H$

<u>Proof</u> 1) $\langle v_0, \rho(x) \rangle = \sum_{i=1}^{r_1} \log|\sigma_i(x)| +$

$$+ 2 \sum_{j=r_1+1}^{r_1+r_2} \log|\sigma_j(x)| = \log\left(\prod_{i=1}^{r_1} |\sigma_i(x)| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2\right)$$

$$= \log\left|\prod \sigma_i(x) \cdot \prod \sigma_j(x) \cdot \overline{\sigma_j(x)}\right| = \log|N_{K/\mathbb{Q}}(x)|$$

2) $x \in \mathrm{Ker}(\rho) \Rightarrow |\sigma_i(x)| = 1 \quad \forall i = 1, \ldots r_1+r_2$

Consider the set $M = \{(y_1, \ldots, y_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} :$

$|y_i| \leq 1 \quad \forall i\}$

M is bounded, $\mathcal{O}_K$ is a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$\Rightarrow M \cap \mathcal{O}_K$ is finite

Since $Ker(\rho) \subset M \cap \mathcal{O}_K$,

$Ker(\rho)$ is a fin group; let m = order of this group.

then $\forall x \in Ker(\rho)$ $x^m = 1$

If $y \in \mathcal{O}_K^\times$ is a root of unity

then y is a torsion element of $\mathcal{O}_K^\times$,

so $y \in Ker(\rho)$, because $Im(\rho) \subset \mathbb{R}^{r_1+r_2}$

is torsion-free

3) From Lemma 12.1: $\forall x \in \mathcal{O}_K^\times$

$|N_{K/\mathbb{Q}}(x)| = 1 \Rightarrow$ by part 1

$\langle v_0, \rho(x) \rangle = 0 \Rightarrow \rho(x) \in v_0^\perp = H$ $\square$

What is the image of ρ?

We first show that $Im(\rho)$ spans H

If $Im(\rho) \subset H' \subsetneq H \Leftrightarrow \dim(Im(\rho)^\perp) \geq 2$

$\Leftrightarrow \exists \lambda \in \mathbb{R}^{r_1+r_2}$, s.t. λ and v_0

are linearly indep, and $\langle \lambda, \rho(x) \rangle = 0$

<u>Prop. 12.3</u> Let $\lambda \in \mathbb{R}^{r_1+r_2}$ be s.t. λ and

v_0 are lin. independ. Then $\exists y \in \mathcal{O}_K^\times$, s.t.

$\langle \lambda, \rho(y) \rangle \neq 0$. In particular, $Im(\rho)$ spans H.

Proof Write $\lambda = (\lambda_1, \dots, \lambda_{r_1+r_2})$.

Let $A = \left(\frac{2}{\pi}\right)^{r_2} |d_K|^{1/2}$

Prop 10.2 $\Rightarrow$ $\exists$ only fin. many ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\operatorname{Norm}(\mathfrak{a}) \leq A$; in particular $\exists$ only fin. many principal ideals of Norm $\leq A$

Let $(b_1), \dots, (b_m)$ be all such ideals, $b_i \in \mathcal{O}_K$.

Define $B = \max_{i=1\dots m} |\langle \lambda, \rho(b_i) \rangle| + \log A \cdot \sum_{i=1}^{r_1+r_2} |\lambda_i|$

Claim $\exists\ \mu = (\mu_1 \dots \mu_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}$ s.t.

1) $\langle v_0, \mu \rangle = \log A$

2) $|\langle \lambda, \mu \rangle| > B$

Proof of claim: choose any μ': $\langle v_0, \mu' \rangle = \log A$

$\mu'' \in v_0^{\perp}$ s.t. $\langle \lambda, \mu'' \rangle \neq 0$ - this is possible because λ and v_0 are lin. indep.

Then take $\mu = \mu' + t\mu''$ for $t \gg 0$

We fix μ as in the claim.

Define a subset $S \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$S = \{ (x_1 \dots x_{r_1+r_2}) \mid |x_i| < e^{\mu_i} \ \forall i = 1, \dots r_1+r_2 \}$

$$S = \prod_{i=1}^{r_1} (-e^{\mu_i}, e^{\mu_i}) \times \prod_{j=r_1+1}^{r_2} \Delta_{e^{\mu_j}}$$

where $\Delta_r = \{ z \in \mathbb{C} \mid |z| < r \}$

S is bounded, convex, open, symmetric and $Vol(S) = \prod 2e^{\mu_i} \cdot \prod \pi e^{2\mu_j}$

$$= 2^{r_1} \cdot \pi^{r_2} \cdot e^{\langle v_0, \mu \rangle} = 2^{r_1} \cdot \pi^{r_2} \cdot A$$

Recall: $\mathcal{O}_K$ is a lattice of volume

$$2^{-r_2} |d_K|^{1/2}$$

$$Vol(S) = \underbrace{2^{r_1+2r_2}}_{2^n} \underbrace{2^{-r_2} |d_K|^{1/2}}_{Vol(\mathcal{O}_K)}$$

Prop 11.1 $\Rightarrow \exists\, 0 \neq a \in \mathcal{O}_K \cap \overline{S}$

then $|\sigma_i(a)| \leq e^{\mu_i}$ $\quad i = 1 \dots r_1 + r_2$

hence $Norm((a)) = |N_{K/\mathbb{Q}}(a)| \leq \prod_{i=1}^{r_1} e^{\mu_i} \cdot \prod_{j=r_1+1}^{r_1+r_2} e^{2\mu_j}$

$$\leq e^{\langle v_0, \mu \rangle} = A$$

Also, $1 \leq |N_{K/\mathbb{Q}}(a)| = \prod_{i=1}^{r_1} |\sigma_i(a)| \cdot \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(a)|^2 \leq$

$$\leq |\sigma_{i_0}(a)| \cdot \prod_{i \neq i_0} e^{\mu_i} \cdot \prod_j e^{2\mu_j} = \frac{|\sigma_{i_0}(a)|}{e^{\mu_{i_0}}} \cdot A$$

for any $i_0 = 1 \dots r_1$

$$\Rightarrow \quad |\sigma_i(a)| \geq \frac{e^{\mu_i}}{A} \qquad i = 1 \dots r_1$$

analogously $\quad |\sigma_j(a)|^2 \geq \dfrac{e^{2\mu_j}}{A}, \quad j = r_1+1 \dots r_1+r_2$

We get inequalities:

$$(*) \begin{cases} \dfrac{1}{A} \leq \dfrac{|\sigma_i(a)|}{e^{\mu_i}} \leq 1, & i = 1 \dots r_1 \\[2ex] \dfrac{1}{A} \leq \dfrac{|\sigma_j(a)|^2}{e^{2\mu_j}} \leq 1, & j = r_1+1, \dots, r_1+r_2 \end{cases}$$

We know that $(a) = (b_k)$ for some k, by definition of b_i. This means

$a = y \cdot b_k$ and $b_k = z \cdot a$ for some $y, z \in \mathcal{O}_K$

$\Downarrow$

$a = y \cdot z \cdot a \Rightarrow y \cdot z = 1 \Rightarrow y, z \in \mathcal{O}_K^\times$

We want to prove $\langle \lambda, \rho(y) \rangle \neq 0$

We first estimate

$$|\langle \lambda, \rho(a) \rangle - \langle \lambda, \mu \rangle| = |\langle \lambda, \rho(a) - \mu \rangle|$$

$$\leq \sum_{i=1}^{r_1} |\lambda_i| \cdot \left| \log \frac{|\sigma_i(a)|}{e^{\mu_i}} \right| + \sum_{j=r_1+1}^{r_2} |\lambda_j| \left| \log \frac{|\sigma_j(a)|^2}{e^{2\mu_j}} \right|$$

$$\overset{\text{use } (*)}{\leq} \log A \cdot \sum_{i=1}^{r_1+r_2} |\lambda_i|$$

Then $|\langle \lambda, \rho(y)\rangle - \langle \lambda, \mu\rangle| \leq$

$$\leq |\langle \lambda, \rho(y)\rangle - \langle \lambda, \rho(a)\rangle| + |\langle \lambda, \rho(a)\rangle - \langle \lambda, \mu\rangle|$$

$$\leq \underbrace{|\langle \lambda, \rho(a) - \rho(y)\rangle|}_{|\langle \lambda, \rho(b_k)\rangle|} + \log A \cdot \sum_{i=1}^{r_1+r_2} |\lambda_i| \leq B$$

Now use $|\alpha - \beta| \leq \gamma$ for some $\alpha, \beta, \gamma \in \mathbb{R}$

then $|\beta| \leq |\beta - \alpha| + |\alpha| \leq \gamma + |\alpha|$

$\Rightarrow |\alpha| \geq |\beta| - \gamma$

$\Downarrow$

$$|\langle \lambda, \rho(y)\rangle| \geq |\langle \lambda, \mu\rangle| - B > 0. \quad \square$$

<u>Thm 12.4</u> (Dirichlet's unit theorem)

Let K be a number field, $\mathcal{O}_K$ the ring of integers, $\mu_K \subset \mathcal{O}_K^\times$ the subgroup of roots of unity. Assume that K has r_1 real and r_2 conjugate pairs of complex embedding into $\mathbb{C}$. Then

$$\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r_1+r_2-1}$$

<u>Proof</u> We use $\rho: \mathcal{O}_K^\times \longrightarrow \mathbb{R}^{r_1+r_2}$ as before; $\mathrm{Ker}(\rho) = \mu_K$.

$\mathrm{Im}(\rho)$ spans $H \subset \mathbb{R}^{r_1+r_2-1}$

We need to prove that $\mathrm{Im}(\rho)$ is a lattice in H, because then

$\mathrm{Im}(\rho) \cong \mathbb{Z}^{r_1+r_2-1}$

Consider a bounded neighborhood of zero

$M \subset \mathbb{R}^{r_1+r_2}$: $M = \{(x_1 \ldots x_{r_1+r_2}) \,/\, |x_i| < C\}$

for some const. $C > 0$

$\rho^{-1}(M) = \{x \in \mathcal{O}_K^\times \,/\, |\sigma_i(x)| < e^C\}$

$\Downarrow$

$\rho^{-1}(M)$ is contained in a bounded set.

but $\mathcal{O}_K$ is a lattice $\Rightarrow$

$\rho^{-1}(M)$ is finite

$\mathrm{Im}(\rho) \cap M$ is also finite

$\Rightarrow \mathrm{Im}(\rho)$ is a lattice. $\square$