

# Introduction to Algebraic Number Theory

## Lecture 19

Andrei Jorza

### 8 Units (continued)

(3.1) Proof of the Dirichlet unit theorem.

**Lemma 1.** 1. *There exists a constant  $\lambda$  (in fact  $\lambda = \log\left(2^s \pi^{-s} \sqrt{|\text{disc}(K)|}\right)$ ) such that for any index  $k$  between 1 and  $r + s$  and any  $\alpha = (a_1, \dots, a_{r+s}) \in \log \iota(\mathcal{O}_K - 0)$  there exists  $\beta = (b_1, \dots, b_{r+s}) \in \log \iota(\mathcal{O}_K^\times - 0)$  with  $\sum \beta < \lambda$  and  $b_i < a_i$  for all  $i \neq k$ .*

2. *For any index  $k$  there exists  $\alpha = (u_1, \dots, u_{r+s}) \in \log \iota \mathcal{O}_K^\times$  such that  $u_i < 0$  when  $i \neq k$ .*

*Proof.* Part one follows from a geometry of numbers type argument. Here's a sketch: choose  $c_i$  such that  $c_i < \exp(a_i)$  for  $i \neq k$  and choose  $c_k$  such that  $\prod c_i = \exp(\lambda)$ . Then finding  $\beta$  as desired is equivalent to finding  $x = (x_1, \dots, x_n) \in \iota(\mathcal{O}_K - 0)$  such that  $|x_i| < c_i$  for  $i \leq r$  and  $x_{r+2i-1}^2 + x_{r+2i}^2 < c_{r+i}$  for  $i > 0$ . The geometry of numbers requires only that the volume of this region be  $> 2^n \text{vol}(\iota(\mathcal{O}_K))$  and the volume can be shown to depend only on  $\lambda$ . For example, if  $K = \mathbb{Q}(\sqrt{m})$ ,  $m > 0$  then  $\mathbb{R}^n = \mathbb{R}^{r+s} = \mathbb{R}^2$  and the region  $|x_i| \leq c_i$  with  $c_1 \exp(a_1)$  and  $c_1 c_2 = \exp(\lambda)$  has area  $4c_1 c_2 = 4 \exp(\lambda)$ .

Part two: part one allows us to construct a sequence  $\alpha_m = (a_{m,1}, \dots, a_{m,r+s}) \ni \log \iota(\mathcal{O}_K - 0)$  with  $(a_{m,i})_m$  decreasing for  $i \neq k$  and  $\sum \alpha_m < \lambda$ . Consider the  $\sum$  map  $\sum : \log \iota(\mathcal{O}_K - 0) \rightarrow \mathbb{R}$  taking  $\log \iota(\alpha)$  to  $\log |N_{K/\mathbb{Q}}(\alpha)|$ . If  $B > 0$  then  $\sum \log \iota(\alpha) \leq B$  implies  $|N_{K/\mathbb{Q}}(\alpha)| \leq \exp(B)$  and so  $N_{K/\mathbb{Q}}(\alpha)$  takes finitely many integral values (between  $-\exp(B)$  and  $\exp(B)$ ). Using the observation with  $B = \lambda$  it follows that if  $\alpha_m = \log \iota(u_m)$  for  $u_m \in \mathcal{O}_K - 0$  then  $|N_{K/\mathbb{Q}}(u_m)| \leq \exp(\lambda)$  for all  $m$ . By the pigeonhole principle there must exist different indices  $m \neq m'$  such that  $|N_{K/\mathbb{Q}}(u_m)| = |N_{K/\mathbb{Q}}(u_{m'})|$  which implies that  $u_m = uu_{m'}$  for some  $u \in \mathcal{O}_K^\times$ . In other words  $\alpha_m = \log \iota(u) + \alpha_{m'}$  for  $m \neq m'$  for some unit  $u \in \mathcal{O}_K^\times$  and the condition on  $u$  follows from the fact that the coordinates of  $\alpha_m$  are decreasing for  $i \neq k$ .  $\square$

**Proof of the Dirichlet Unit Theorem.** It suffices to show that  $\mathcal{O}_K^\times$  has rank at least  $r + s - 1$ . The previous lemma guarantees the existence of units  $u_k$  such that  $\log \iota(u_k)$  have negative coordinates except in index  $k$ . Since  $\sum \log \iota(u_k) = 0$  it follows that the  $k$ -th coordinate of  $\log \iota(u_k)$  must be  $> 0$ .

Consider the matrix  $(u_{i,j})$  where  $\log \iota(u_i) = (u_{i,1}, \dots, u_{i,r+s})$ . To show that  $\text{rank } \mathcal{O}_K^\times = r + s - 1$  it suffices to show that  $r + s - 1$  of the  $\log \iota(u_k)$  are linearly independent, i.e., the rank of this matrix is  $\geq r + s - 1$ .

Suppose the rank is  $< r + s - 1$  in which case we may assume that there exist  $t_1, t_2, \dots, t_{r+s-s}$  such that

$\sum_{j=1}^{r+s-1} t_j u_{i,j} = 0$  for all  $i$ . We may assume that the largest coefficient  $t_k > 0$ . Then

$$\begin{aligned}
0 &= \sum_{j=1}^{r+s-1} t_j u_{k,j} \\
&= t_k u_{k,k} + \sum_{j \neq k, 1 \leq j \leq r+s-1} t_j u_{k,j} \\
&\geq t_k u_{k,k} + \sum_{j \neq k, 1 \leq j \leq r+s-1} t_k u_{k,j} \\
&= t_k \sum_{j=1}^{r+s-1} u_{k,j} \\
&= -t_k u_{k,r+s}
\end{aligned}$$

since  $u_{k,j} < 0$  when  $j \neq k$  and  $\sum_{j=1}^{r+s} u_{k,j} = 0$  for all  $k$ . This of course is not possible since  $t_k > 0$  and  $u_{k,r+s} < 0$  as  $k < r + s$ .  $\square$