Another Application of Minkowski’s Theorem

MATH 681, Spring 2018

We fix a number field $K$. The degree of $K$ over $\mathbb{Q}$ is denoted by $n$. There are $n$ embeddings $\sigma: K \to \mathbb{C}$; there are $r_1$ embeddings into $\mathbb{R}$ and $r_2$ pairs of complex conjugate embeddings into $\mathbb{C}$ (not real). Thus $n = r_1 + 2r_2$. These embeddings are ordered so that $\sigma_i: K \to \mathbb{R}$ for $i \leq r_1$ and $\sigma_{i+r_2} = \overline{\sigma_i}$ for $r_1 + 1 \leq i \leq r_1 + r_2$, where the overline denotes complex conjugation. As usual $\sqrt{|\Delta_K|}$ denotes the square root of the absolute value of the discriminant of $K$. We also use

$$
\epsilon_i = \begin{cases} 
1 & \text{if } i \leq r, \\
2 & \text{if } r + 1 \leq i \leq r + s.
\end{cases}
$$

Define $\rho': K \to \mathbb{R}^n$ by

$$
\rho'(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \mathbb{R}(\sigma_{r_1+1}(\alpha)), \ldots, \mathbb{R}(\sigma_{r_1+r_2}(\alpha)), \mathbb{I}(\sigma_{r_1+1}(\alpha)), \ldots, \mathbb{I}(\sigma_{r_1+r_2}(\alpha))).
$$

(This is the same embedding used in the other handout on applications of Minkowski’s Theorem.) For positive real numbers $a_1, \ldots, a_{r_1+r_2}$, define

$$
C(a_1, \ldots, a_{r_1+r_2}) := \\
\{x = (x_1, \ldots, x_n) \in \mathbb{R}^n: |x_i| \leq a_i, 1 \leq i \leq r_1 \text{ and } x_i^2 + x_{i+r_2}^2 \leq a_i^2, r_1 < i \leq r_1 + r_2\}.
$$

One readily verifies that such a set is a convex body in $\mathbb{R}^n$, and an almost trivial application of Fubini’s Theorem gives

$$
\text{Vol}(C(a_1, \ldots, a_{r_1+r_2})) = 2^{r_1+r_2} r_1+r_2 \prod_{i=1}^{r_1+r_2} a_i^{\epsilon_i}.
$$

**Lemma:** Suppose $r_1 + r_2 > 1$ and let $i_0 \in \{1, \ldots, r_1 + r_2\}$. There are infinitely many non-zero $\alpha \in \mathcal{O}_K$ with $|N_{K/Q}(\alpha)| \leq \sqrt{|\Delta_K|}(2/\pi)^{r_2}$ and $|\sigma_i(\alpha)| < 1$ for all $i \neq i_0$. There is a unit $u \in \mathcal{O}_K^\times$ with $|\sigma_i(u)| < 1$ for all $i \neq i_0$.

**Proof:** Let $a_i = 1/2$ for $i \neq i_0$ and let $a_{i_0}$ be the positive real number satisfying $\prod_{i=1}^{r_1+r_2} a_i^{\epsilon_i} = \sqrt{|\Delta_K|}(2/\pi)^{r_2}$. Since $\det(\rho'(\mathcal{O}_K)) = 2^{-r_2} \sqrt{|\Delta_K|}$, by Minkowski’s theorem there is a non-zero $\alpha_1 \in \mathcal{O}_K$ with $\rho'(\alpha_1) \in C(a_1, \ldots, a_{r_1+r_2})$. By the definition of $C(a_1, \ldots, a_{r_1+r_2})$ and $\rho'$ we have $|\sigma_i(\alpha_1)| \leq a_i$ for $i = 1, \ldots, r_1 + r_2$. Thus,

$$
|N_{K/Q}(\alpha_1)| \leq \prod_{i=1}^{r_1+r_2} a_i^{\epsilon_i} = \sqrt{|\Delta_K|}(2/\pi)^{r_2}
$$

and $|\sigma_i(\alpha_1)| \leq 1/2$ for all $i \neq i_0$.

Now let $a_i = \frac{|\sigma_i(\alpha_1)|}{2}$ for $i \neq i_0$. This will yield a non-zero $\alpha_2$ satisfying the statement of the lemma and also $|\sigma_i(\alpha_2)| \leq |\sigma_i(\alpha_1)|/2$ for all $i \neq i_0$. Continue on in this fashion, getting a sequence $\alpha_1, \alpha_2, \ldots$ of non-zero integers which satisfy the statement of the lemma and also

$$
|\sigma_i(\alpha_1)| > |\sigma_i(\alpha_2)| > \cdots
$$

for all $i \neq i_0$.

Obviously these $\alpha_j$’s are distinct. But there are only finitely many integral ideals with norm no greater than $\sqrt{|\Delta_K|}(2/\pi)^{r_2}$. Hence, the principal ideals $(\alpha_j)$ cannot all be distinct; $(\alpha_i) = (\alpha_m)$ for some indices $i < m$. This forces $\alpha_m = u\alpha_i$ for some unit $u \in \mathcal{O}_K^\times$. Further,

$$
|\sigma_i(u)||\sigma_i(\alpha_i)| = |\sigma_i(\alpha_m)| < |\sigma_i(\alpha_i)|
$$

for all $i \neq i_0$. This completes the proof.