An Application of Minkowski’s Theorem  
Math 681, Spring 2018

We need to set some notation. 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 set

$$
e_i = \begin{cases} 1 & \text{if } i \leq r_1, \\ 2 & \text{if } r_1 + 1 \leq i \leq r_1 + r_2. \end{cases}$$

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

$$\rho'(\alpha) = \left( \sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathbb{R}(\sigma_{r+1}(\alpha)), \ldots, \mathbb{R}(\sigma_{r+s}(\alpha)), \mathbb{I}(\sigma_{r+1}(\alpha)), \ldots, \mathbb{I}(\sigma_{r+s}(\alpha)) \right).$$

Note that this is slightly different than the mapping $\rho: K \to \mathbb{C}^n$ we’ve been using.

**Theorem 1:** Let $\mathfrak{A}$ be a non-zero fractional ideal of $K$. Then $\rho'(\mathfrak{A})$ is a lattice in $\mathbb{R}^n$ with

$$\det(\rho'(\mathfrak{A})) = N(\mathfrak{A})2^{-r_2}\sqrt{|\Delta_K|}.$$

**Proof:** This is almost exercise #1 from the fourth homework assignment; the difference is that there you (essentially) prove that

$$\det(\rho(\mathfrak{A})) = N(\mathfrak{A})\sqrt{|\Delta_K|}.$$

Theorem 1 follows via elementary row operations on the resulting bases for the lattices, and is left as an exercise.

Let $f: \mathbb{R}^n \to \mathbb{R}$ be defined by

$$f(\mathbf{x}) = |x_1| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+s+1}^2} + \cdots + 2\sqrt{x_{r+s}^2 + x_{r+2s}^2},$$

where $\mathbf{x} = (x_1, \ldots, x_n)$. Let $C \subset \mathbb{R}^n$ be the set of $\mathbf{x}$ with $f(\mathbf{x}) \leq 1$.

**Lemma 1:** The set $C$ is a convex body.

**Proof:** One can show without much difficulty that $f(\mathbf{x} + \mathbf{y}) \leq f(\mathbf{x}) + f(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Since $f$ is clearly continuous at the origin, we see that it is continuous everywhere and the set $C$ is compact. It is also clear that $f(t\mathbf{x}) = |t|f(\mathbf{x})$ for all $t \in \mathbb{R}$ and $\mathbf{x} \in \mathbb{R}^n$. The case $t = -1$ shows that $C$ is symmetric about the origin. Since

$$f(t\mathbf{x} + (1-t)\mathbf{y}) \leq f(t\mathbf{x}) + f((1-t)\mathbf{y}) = |t|f(\mathbf{x}) + |1-t|f(\mathbf{y})$$

for all $t \in \mathbb{R}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $C$ is convex. Obviously the origin is an interior point of $C$, so $C$ is a convex body.

**Lemma 2:** The volume of $C$ is $\frac{2^{r_1-r_2}\pi^{r_2}}{n!}$. 

Proof: First let \( w_i = |x_i| \) for \( 1 \leq i \leq r \) and convert to polar coordinates for the remaining subscripts: \( x_i = w_i \cos \theta_i \) and \( x_i + s = w_i \sin \theta_i \) for \( r_1 + 1 \leq i \leq r_1 + r_2 \), with \( w_i \geq 0 \) and \( 0 \leq \theta_i \leq 2\pi \). Then the volume of \( C \) is equal to

\[
2^{r_1}(2\pi)^{r_2} \int \cdots \int_{D_1} \prod_{i=1}^{r_1+r_2} w_i^{e_i-1} dw_i,
\]

where \( D_1 \) is the region defined by \( w_i \geq 0 \) and \( \sum_{i=1}^{r_1+r_2} e_i w_i \leq 1 \). Letting \( z_i = e_i w_i \), one sees that the volume of \( C \) is equal to

\[
2^{r_1-r_2} \pi^s \int \cdots \int_{D_2} \prod_{i=1}^{r_1+r_2} z_i^{e_i-1} dz_i,
\]

where \( D_2 \) is defined by \( z_i \geq 0 \) for all \( 1 \leq i \leq r_1 + r_2 \) and \( z_1 + \cdots + z_{r_1+r_2} \leq 1 \).

For non-negative integers \( r, s \) with \( r + s > 0 \) and real \( B \geq 0 \), let

\[
V(r, s, B) = \int \cdots \int_{D_3} \prod_{i=1}^{r+s} y_i^{e_i-1} dy_i,
\]

where the domain of integration \( D_3 \) is given by \( y_i \geq 0 \) for all \( i \) and \( y_1 + \cdots + y_{r+s} \leq B \). A straightforward induction on \( r + s \) shows that \( V(r, s, B) = B^{r+2s}/(r+2s)! \). The case \( B = 1 \) completes the proof of the lemma.

Lemma 3 (The arithmetic/geometric mean inequality): For any non-negative \( y_1, \ldots, y_m \in \mathbb{R} \) we have

\[
\left( \prod_{i=1}^{m} y_i \right)^{1/m} \leq \frac{\sum_{i=1}^{m} y_i}{m},
\]

with equality if and only if \( y_1 = \cdots = y_m \).

Proof: A routine application of Lagrange multipliers shows that the function \( y_1 \cdots y_m \) subject to the constraint \( y_1 + \cdots + y_m = k \) \((k > 0)\) is maximized when all \( y_i \)'s are equal. The lemma follows.

Theorem 2: Let \( \mathfrak{A} \) be a non-zero fractional ideal of \( K \). Then there is a non-zero \( \alpha \in \mathfrak{A} \) with \( |N_{K/Q}(\alpha)| \leq \frac{n!}{m!} (4/\pi)^{r_2} \sqrt{|\Delta_K|} |N(\mathfrak{A})| \).

Proof: By Theorem 1, Lemmas 1 and 2, and Minkowski’s theorem, the first successive minima \( \lambda_1 \) of \( \rho'(\mathfrak{A}) \) with respect to \( C \) satisfies

\[
\lambda_1^n \leq n! (4/\pi)^{r_2} \sqrt{|\Delta_K|} |N(\mathfrak{A})|.
\]

Now there is a non-zero \( \alpha \in \mathfrak{A} \) with \( \rho'(\alpha) \) contained in \( \lambda_1 C \). By definition of \( \rho' \) and \( C \), we have

\[
\frac{1}{n} \sum_{i=1}^{n} |\sigma_i(\alpha)| \leq \frac{\lambda_1}{n}.
\]

Applying Lemma 3 gives the result.

Corollary 1: If \( K \neq \mathbb{Q} \) (i.e., if \( n > 1 \)) then \( \sqrt{|\Delta_K|} > 1 \).

Proof: Exercise.
**Corollary 2:** If $\mathfrak{A}$ is a non-zero fractional ideal, then there is a non-zero $\alpha \in K$ such that $\alpha \mathfrak{A}$ is a non-zero ideal in $\mathcal{O}_K$ with

$$N(\alpha \mathfrak{A}) \leq \frac{n!}{n^n (4/\pi)^r} r^2 \sqrt{|\Delta_K|}.$$ 

**Proof:** Apply Theorem 2 to the fractional ideal $\mathfrak{A}^{-1}$. Since $\alpha \in \mathfrak{A}^{-1}$, we have $\alpha \mathfrak{A} \subseteq \mathcal{O}_K$. Clearly $\alpha \mathfrak{A} = \alpha \mathcal{O}_K \mathfrak{A}$ (a product of fractional ideals), so that by a previous exercise $N(\alpha \mathfrak{A}) = N(\alpha \mathcal{O}_K)N(\mathfrak{A}) = |N_{K/Q}(\alpha)|N(\mathfrak{A})$.

The non-zero principal fractional ideals (those of the form $\alpha \mathcal{O}_K$ for some $\alpha \in K^\times$) clearly form a subgroup of the group of all non-zero fractional ideals. The quotient group (our group is abelian, so no problems here) is called the *ideal class group* of $K$. The upshot of Corollary 2 is that this quotient group is finite. The order of the quotient group is called the *class number* of the field $K$, and typically denoted $h_K$ or just $h$ if the field is understood. Note that $h = 1$ is the same as saying $\mathcal{O}_K$ is a principal ideal domain.

**Corollary 3:** There is a positive integer $h$ (the class number, as defined above) such that $\mathfrak{A}^h$ is a principal ideal for all ideals $\mathfrak{A} \subseteq \mathcal{O}_K$.

**Example:** Suppose $D$ is a positive square-free integer and $K = \mathbb{Q}(\sqrt{D})$. Here $n = 2 = r_1$ and $r_2 = 0$. If $D \equiv 1 \mod 4$, then $\sqrt{|\Delta_K|} = \sqrt{D}$ and Theorem 2 implies that every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with $|N_{K/Q}(\alpha)| \leq \frac{N(\mathfrak{A}) \sqrt{D}}{2}$. If $D \equiv 2, 3 \mod 4$, then $\sqrt{|\Delta_K|} = 2\sqrt{D}$ and every non-zero ideal $\mathfrak{A}$ contains a non-zero element $\alpha$ with $|N_{K/Q}(\alpha)| \leq N(\mathfrak{A}) \sqrt{D}$.

It’s known (you looked this up in the first homework assignment) that $h_K = 1$ for only finitely many imaginary quadratic number fields (those above with $D < 0$). It’s famously conjectured, but still unproven, that $h_K = 1$ for infinitely many real quadratic number fields.