

Lattices and a Volume Computation

We fix a number field K . The degree of K over \mathbb{Q} is denoted by n . There are n embeddings $\sigma: K \rightarrow \mathbb{C}$; there are r embeddings into \mathbb{R} and s pairs of complex conjugate embeddings into \mathbb{C} (not real). Thus $n = r + 2s$. These embeddings are ordered so that $\sigma_i: K \rightarrow \mathbb{R}$ for $i \leq r$ and $\sigma_{i+s} = \overline{\sigma_i}$ for $r + 1 \leq i \leq r + s$, 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

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

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

$$\rho(\alpha) = \left(\sigma_1(\alpha), \dots, \sigma_r(\alpha), \Re(\sigma_{r+1}(\alpha)), \dots, \Re(\sigma_{r+s}(\alpha)), \Im(\sigma_{r+1}(\alpha)), \dots, \Im(\sigma_{r+s}(\alpha)) \right).$$

Note that this is slightly different indexing than what we did in class on March 6.

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

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

(Proof done in class, March 6.)

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

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

where $\mathbf{x} = (x_1, \dots, x_n)$. 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 $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. This shows that 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 $\frac{2^{r-s}\pi^s}{n!}$.

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 $r + 1 \leq i \leq r + s$, with $w_i \geq 0$ and $0 \leq \theta_i \leq 2\pi$. Then the volume of C is equal to

$$2^r (2\pi)^s \int \dots \int_{D_1} \prod_{i=1}^{r+s} w_i^{e_i-1} dw_i,$$

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

$$2^{r-s} \pi^s \int \cdots \int_{D_2} \prod_{i=1}^{r+s} z_i^{e_i-1} dz_i,$$

where D_2 is defined by $z_i \geq 0$ for all $1 \leq i \leq r+s$ and $z_1 + \cdots + z_{r+s} \leq 1$.

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 $y_1, \dots, y_m \in \mathbb{R}$ 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 $|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n} (4/\pi)^s \sqrt{|\Delta_K|} N(\mathfrak{A})$.

Proof: Let λ be the positive real number with $\lambda^n = n!(4/\pi)^s \sqrt{|\Delta_K|} N(\mathfrak{A})$. Since the volume of λC is $\lambda^n \text{Vol}(C)$, Theorem 1, Lemma 1, Lemma 2 and Minkowski's theorem imply that there is a non-zero $\alpha \in \mathfrak{A}$ with $\rho(\alpha)$ contained in λC . By definition of ρ and C , we have

$$\frac{1}{n} \sum_{i=1}^n |\sigma_i(\alpha)| \leq \frac{\lambda}{n}.$$

Applying Lemma 3 gives the result.

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

Proof: Apply Theorem 2 to the case $\mathfrak{A} = \mathfrak{D}_K$. Since $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$ for all non-zero $\alpha \in \mathfrak{D}_K$ and $N(\mathfrak{D}_K) = 1$, we have

$$\sqrt{|\Delta_K|} \geq (\pi/4)^s \frac{n^n}{n!}.$$

One easily sees that $n^n \geq 2^{n-1} n!$ and obviously $4/\pi < 2$. Since $s \leq n/2$ and $n-1 \geq n/2$ for $n \geq 2$, we have $\sqrt{|\Delta_K|} > 1$ whenever $n \geq 2$.

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