Math 361 lecture for Monday, Week 11

Lattices associated with number fields

Let K be a number field of degree n. An embedding $\sigma_i\colon K \to \mathbb{C}$ is *real* if $\sigma_i(K) \subset \mathbb{R}$. Otherwise σ_i is *complex*. Say $\sigma_1, \dots, \sigma_s$ are the real embeddings of K and $\sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ are the complex embeddings. Here, $\overline{\sigma}_{s+j}(\alpha) := \overline{\sigma}_{s+j(\alpha)}$ for $\alpha \in K$. Define

$$\begin{aligned}\mathbb{L}_K^{s,t} = \mathbb{L}^{s,t} &:= \mathbb{R}^s \times \mathbb{C}^t \simeq \mathbb{R}^n \\ (x_1, \dots, x_s, z_1, \dots, z_t) &\mapsto (x_1, \dots, x_s, u_1, v_1, \dots, u_t, v_t)\end{aligned}$$

where $z_j = u_j + v_j i \in \mathbb{C}$ for $j = 1, \dots, t$. Then define

$$\begin{aligned}\sigma_K = \sigma\colon K &\to \mathbb{L}^{s,t} \\ \alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_s(\alpha), \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)).\end{aligned}$$

Exercise 1. Check that σ is an injective ring homomorphism fixing $\mathbb{Q}$.

Define the *norm* of $q = (x_1, \dots, x_s, z_1, \dots, z_t) \in \mathbb{L}^{s,t}$ to be

$$N(q) = x_1 \cdots x_s z_1 \overline{z_1} \cdots z_t \overline{z_t} = x_1 \cdots x_s |z_1|^2 \cdots |z_t|^2.$$

Then $N(q) \in \mathbb{R}$, and $N(qq') = N(q)N(q')$ for all $q, q' \in \mathbb{L}^{s,t}$.
This norm on $\mathbb{L}^{s,t}$ is related to our old norm on K (the product of the conjugates) in an obvious way: for $\alpha \in K$

$$N(\alpha) = \sigma_1(\alpha) \cdots \sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma}_{s+1}(\alpha) \cdots \sigma_{s+1}(\alpha)\overline{\sigma}_{s+t}(\alpha) = N(\sigma(\alpha)).$$

So if we identify $\alpha \in K$ with its image in $\mathbb{L}^{s,t}$, its norm is well-defined.

Example 2.

1. Let $K = \mathbb{Q}(i)$. Then the embeddings of K are $\sigma_1(x+yi) = x+yi$ and $\overline{\sigma}_1(x+yi) = x-yi$ where $x, y \in \mathbb{Q}$. We have

   $$\sigma(x + yi) = x + yi \in \mathbb{L}^{0,1} \simeq \mathbb{R}^2.$$

   and $N(x + yi) = (x + yi)(x - yi) = x^2 + y^2$.
2. Let $K = \mathbb{Q}(\sqrt{2})$. Then the embeddings of K are $\sigma_1(x + y\sqrt{2}) = x + y\sqrt{2}$ and $\sigma_2(x + y\sqrt{2}) = x - y\sqrt{2}$ where $x, y \in \mathbb{Q}$. We have

   $$\sigma(x + y\sqrt{2}) = (x + y\sqrt{2}, x - y\sqrt{2}) \in \mathbb{L}^{2,0} = \mathbb{R}^2.$$

   and $N(x + y\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) = x^2 + 2y^2$.

3. Let $K = \mathbb{Q}(\theta)$ where θ is the real cube root of 2. The minimal polynomial for θ is $x^3 - 2$, which factors as

$$x^3 - 2 = (x - \theta)(x - \omega\theta)(x - \overline{\omega}\theta)$$

where $\omega = e^{2\pi i/3}$. The embeddings are determined by $\sigma_1(\theta) = \theta$, $\sigma_2(\theta) = \omega\theta$, and $\overline{\sigma}_2(\theta) = \overline{\omega}\theta = \omega^2\theta$. For $\alpha = a + b\theta + c\theta^2 \in K$ where $a, b, c \in \mathbb{Q}$, we have

$$\sigma(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha)) = (a + b\theta + c\theta^2, a + b\omega\theta + c\omega^2\theta^2),$$

and

$$\begin{aligned} N(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha)\overline{\sigma}_2(\alpha) \\ &= (a + b\theta + c\theta^2)(a + b\omega\theta + c\omega^2\theta^2)(a + b\omega^2\theta + c\omega\theta^2) \\ &= a^3 + 2b^3 + 4c^3 - 6abc. \end{aligned}$$

Theorem 3. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K, and let

$$\sigma_k(\alpha_\ell) = \begin{cases} x_{k,\ell} & \text{if } 1 \le k \le s \\ u_{k,\ell} + iv_{k,\ell} & \text{if } s+1 \le k \le s+t \end{cases}$$

where the $x_{k,\ell}, u_{k,\ell}$ and $v_{k,\ell}$ are real numbers. So

$$\sigma(\alpha_\ell) = (x_{1,\ell}, \ldots, x_{s,\ell}, u_{s+1,\ell} + iv_{s+1,\ell}, \ldots, u_{s+t,\ell} + iv_{s+t,\ell}) \in \mathbb{L}^{s,t} = \mathbb{R}^s \times \mathbb{C}^t.$$

Identifying $\mathbb{L}^{s,t}$ with $\mathbb{R}^n$, we have corresponding vectors

$$\mathbf{w}_\ell = (x_{1,\ell}, \ldots, x_{s,\ell}, u_{s+1,\ell}, v_{s+1,\ell}, \ldots, u_{s+t,\ell}, v_{s+t,\ell}) \in \mathbb{R}^n.$$

Let

$$F = \{\textstyle\sum_{i=\ell}^n c_i \mathbf{w}_\ell : 0 \le c_\ell < 1\} \in \mathbb{R}^n.$$

Then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ is an $\mathbb{R}$-basis for $\mathbb{L}^{s,t}$ and

$$\text{vol}(F) = 2^{-t}\sqrt{|\Delta[\alpha_1, \ldots, \alpha_n]|}.$$

Proof. Let Think of $\sigma(\alpha_j)$ as an element of $\mathbb{R}^n$ for all j. Then performing row operations,

$$\det \begin{pmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & \ddots & \vdots \\ x_{s,1} & \cdots & x_{s,n} \\ u_{s+1,1} & \cdots & u_{s+1,n} \\ v_{s+1,1} & \cdots & v_{s+1,n} \\ \vdots & \ddots & \vdots \\ u_{s+t,1} & \cdots & u_{s+t,n} \\ v_{s+t,1} & \cdots & v_{s+t,n} \end{pmatrix} = \det \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \cdots & \sigma_s(\alpha_n) \\ \frac{\sigma_{s+1}(\alpha_1)+\overline{\sigma}_{s+1}(\alpha_1)}{2} & \cdots & \frac{\sigma_{s+1}(\alpha_n)+\overline{\sigma}_{s+1}(\alpha_n)}{2} \\ \frac{\sigma_{s+1}(\alpha_1)-\overline{\sigma}_{s+1}(\alpha_1)}{2i} & \cdots & \frac{\sigma_{s+1}(\alpha_n)-\overline{\sigma}_{s+1}(\alpha_n)}{2i} \\ \vdots & \ddots & \vdots \\ \frac{\sigma_{s+t}(\alpha_1)+\overline{\sigma}_{s+t}(\alpha_1)}{2} & \cdots & \frac{\sigma_{s+t}(\alpha_n)+\overline{\sigma}_{s+1}(\alpha_n)}{2} \\ \frac{\sigma_{s+t}(\alpha_1)-\overline{\sigma}_{s+t}(\alpha_1)}{2i} & \cdots & \frac{\sigma_{s+t}(\alpha_n)-\overline{\sigma}_{s+t}(\alpha_n)}{2i} \end{pmatrix}$$

$$= \left(\frac{1}{2}\right)^{2t}\left(\frac{1}{i}\right)^{t}\det\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \dots & \sigma_s(\alpha_n) \\ \sigma_{s+1}(\alpha_1)+\overline{\sigma}_{s+1}(\alpha_1) & \dots & \sigma_{s+1}(\alpha_n)+\overline{\sigma}_{s+1}(\alpha_n) \\ \sigma_{s+1}(\alpha_1)-\overline{\sigma}_{s+1}(\alpha_1) & \dots & \sigma_{s+1}(\alpha_n)-\overline{\sigma}_{s+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{s+t}(\alpha_1)+\overline{\sigma}_{s+t}(\alpha_1) & \dots & \sigma_{s+t}(\alpha_n)+\overline{\sigma}_{s+1}(\alpha_n) \\ \sigma_{s+t}(\alpha_1)-\overline{\sigma}_{s+t}(\alpha_1) & \dots & \sigma_{s+t}(\alpha_n)-\overline{\sigma}_{s+t}(\alpha_n) \end{pmatrix}$$

$$= \left(\frac{1}{2}\right)^{2t}\left(\frac{1}{i}\right)^{t}\det\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \dots & \sigma_s(\alpha_n) \\ 2\sigma_{s+1}(\alpha_1) & \dots & 2\sigma_{s+1}(\alpha_n) \\ \sigma_{s+1}(\alpha_1)-\overline{\sigma}_{s+1}(\alpha_1) & \dots & \sigma_{s+1}(\alpha_n)-\overline{\sigma}_{s+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ 2\sigma_{s+t}(\alpha_1) & \dots & 2\sigma_{s+t}(\alpha_n) \\ \sigma_{s+t}(\alpha_1)-\overline{\sigma}_{s+t}(\alpha_1) & \dots & \sigma_{s+t}(\alpha_n)-\overline{\sigma}_{s+t}(\alpha_n) \end{pmatrix}$$

$$= \left(\frac{1}{2}\right)^{2t}\left(\frac{1}{i}\right)^{t}\det\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \dots & \sigma_s(\alpha_n) \\ 2\sigma_{s+1}(\alpha_1) & \dots & 2\sigma_{s+1}(\alpha_n) \\ -\overline{\sigma}_{s+1}(\alpha_1) & \dots & -\overline{\sigma}_{s+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ 2\sigma_{s+t}(\alpha_1) & \dots & 2\sigma_{s+t}(\alpha_n) \\ -\overline{\sigma}_{s+t}(\alpha_1) & \dots & -\overline{\sigma}_{s+t}(\alpha_n) \end{pmatrix}$$

$$= \left(\frac{1}{2}\right)^{t}\left(-\frac{1}{i}\right)^{t}\det\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_s(\alpha_1) & \dots & \sigma_s(\alpha_n) \\ \sigma_{s+1}(\alpha_1) & \dots & \sigma_{s+1}(\alpha_n) \\ \overline{\sigma}_{s+1}(\alpha_1) & \dots & \overline{\sigma}_{s+1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{s+t}(\alpha_1) & \dots & \sigma_{s+t}(\alpha_n) \\ \overline{\sigma}_{s+t}(\alpha_1) & \dots & \overline{\sigma}_{s+t}(\alpha_n) \end{pmatrix}$$

$$= \pm(-2i)^{-t}\sqrt{|\Delta[\alpha_1,\dots,\alpha_n]|} \neq 0.$$

$\square$

Corollary 4. Let $\mathfrak{a}$ be a nonzero ideal in $\mathfrak{O}_K$. Identifying $\mathbb{L}^{s,t}$ with $\mathbb{R}^n$, regard $\sigma(\mathfrak{a}) \subset \mathbb{R}^n$. Then $\sigma(\mathfrak{a})$ is a lattice with fundamental domain of volume

$$2^{-t} N(\mathfrak{a}) \sqrt{|\Delta|}$$

where Δ is the discriminant of K.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Z}$-basis for $\mathfrak{a}$. Then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K. (To see this, note that we can take a $\mathbb{Q}$-basis for K consisting of integers. Then $\alpha_1, \ldots, \alpha_n$ are related to that basis by a matrix that is invertible over $\mathbb{Q}$.) Therefore, by the theorem we just proved, $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are linearly independent over $\mathbb{R}$. Thus, their $\mathbb{Z}$-span is a lattice in $\mathbb{R}^n$.

By the theorem, we have that a fundamental region for $\sigma(\mathfrak{a}) \subset \mathbb{R}^n$ has volume

$$2^{-t} \sqrt{\Delta[\alpha_1, \ldots, \alpha_n]}.$$

Our result follows from the fact, proved earlier, that

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{\frac{1}{2}}.$$

□

Example 5. Let $K = \mathbb{Q}(\sqrt{7})$, and let $\mathfrak{a} = (3, 1 + \sqrt{7})$ (this is one of the prime factors of $(3) \subset \mathfrak{O}_K$). Let's check the formula for the area of the fundamental domain of the lattice $\sigma(\mathfrak{a})$.

The first task is to find a $\mathbb{Z}$-basis for $\mathfrak{a}$. An arbitrary element of $\mathfrak{a}$ has the form

$$(a + b\sqrt{7}) \cdot 3 + (c + d\sqrt{7})\sqrt{7} = (a + 3c + 7d) + (3b + c + d)\sqrt{7},$$

for some $a, b, c, d \in \mathbb{Z}$. So this set is the $\mathbb{Z}$-image of the matrix

$$\begin{pmatrix} 3 & 0 & 1 & 7 \\ 0 & 3 & 1 & 1 \end{pmatrix}.$$

To find the $\mathbb{Z}$-column span, we may use invertible integer column operations. We find

$$\begin{pmatrix} 3 & 0 & 1 & 7 \\ 0 & 3 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \end{pmatrix}.$$

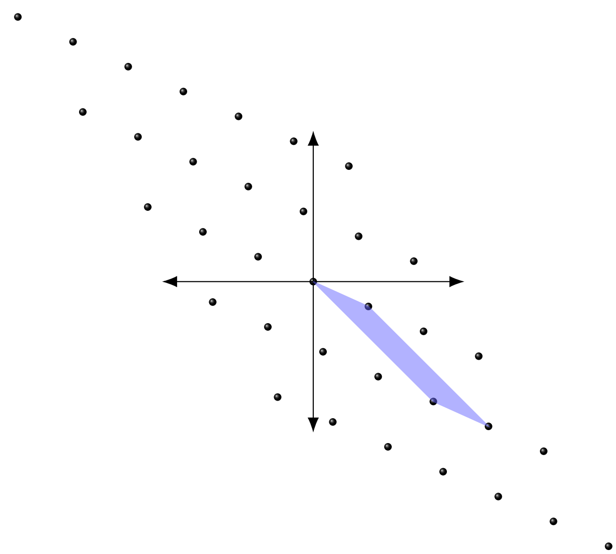
So a $\mathbb{Z}$-basis for $\mathfrak{a}$ is $\{1 + \sqrt{7}, 3\sqrt{7}\}$. The lattice $\sigma(\mathfrak{a})$ is spanned by $\sigma(1+\sqrt{7}) = (1+\sqrt{7}, 1-\sqrt{7})$ and $\sigma(3\sqrt{7}) = (3\sqrt{7}, -3\sqrt{7}) = 3\sqrt{7}(1, -1)$. The area of a fundamental domain is

$$\left| \det \begin{pmatrix} 1+\sqrt{7} & 1-\sqrt{7} \\ 3\sqrt{7} & -3\sqrt{7} \end{pmatrix} \right| = 6\sqrt{7}.$$

We now check that this area equals $2^{-t}N(\mathfrak{a})\sqrt{|\Delta|}$. We have $\mathbb{Z}/3\mathbb{Z} \to \mathfrak{O}_K/\mathfrak{a}$, and $1 \notin \mathfrak{a}$. Hence, $\mathbb{Z}/3\mathbb{Z} \simeq \mathfrak{O}_K/\mathfrak{a}$. So $N(\mathfrak{a}) = 3$. Since $\mathfrak{O}_K = \mathrm{Span}_Z\{1, \sqrt{7}\}$, the discriminant of K is

$$\Delta = \det \begin{pmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{pmatrix}^2 = (-2\sqrt{7})^2.$$

So $2^{-t}N(\mathfrak{a})\sqrt{|\Delta|} = 2^0 \cdot 3 \cdot (2\sqrt{7}) = 6\sqrt{7}$, which agrees with our earlier calculations. Here is a picture of the lattice and the fundamental domain we were considering:



The lattice $\sigma(\mathfrak{a})$ where $\mathfrak{a} = (3, 1+\sqrt{7}) \subset \mathfrak{O}_{\mathbb{Q}(\sqrt{7})}$.