Math 361 lecture for Friday, Week 3

Bases for algebraic integers

Recall that if M is a module over a ring R, it may or may not be the case that M has a basis, i.e., an R-linearly independent spanning set. If M does have a basis, we say M is a *free R-module*. Its *rank* is then defined to be the cardinality of any basis. (It is a fact that the notion of *rank* is well-defined.)

Theorem 1. Let K be a number field of degree n over $\mathbb{Q}$, i.e., $[K:\mathbb{Q}] = n$. Then its ring of integers $\mathfrak{O}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Recall that we have already shown that K has a $\mathbb{Q}$-basis consisting of algebraic integers. (Use the primitive element theorem to write $K = \mathbb{Q}(\theta) = Q[\theta]$ where θ is an algebraic integer. Then $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis.

We have shown that the discriminant of a $\mathbb{Q}$-basis for K consisting of algebraic integers is a nonzero rational integer. Among all $\mathbb{Q}$-bases consisting of algebraic integers, for K, let $\alpha_1, \ldots, \alpha_n$ be one such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is minimal. For sake of contradiction, suppose that $\alpha_1, \ldots, \alpha_n$ is not a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. Then there exists $\alpha \in \mathfrak{O}_K$ such that

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n$$

with $c_i \in \mathbb{Q}$ but with not all $c_i \in \mathbb{Z}$. Without loss of generality, suppose $c_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Write $c_1 = c + r$ where $c = \lfloor c_1 \rfloor$ and $0 < r < 1$. Then

$$\alpha = (c+r)\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

Next, define

$$\psi_1 := \alpha - c\alpha_1 = r\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n.$$

and for $i = 2, \ldots, n$, let $\psi_i := \alpha_i$. Then $\psi_1, \ldots, \psi_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers (check: explain why ψ_1 an algebraic integer). To get a contradiction, we compare the discriminants of our two bases. Let C denote the change of basis matrix:

$$\begin{pmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \\ \vdots \\ \psi_n \end{pmatrix} = \underbrace{\begin{pmatrix} r & c_2 & c_3 & \ldots & c_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}}_{C} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

We have

$$|\Delta[\psi_1, \ldots, \psi_n]| = |(\det C)^2 \Delta[\alpha_1, \ldots, \alpha_n]| = r^2 |\Delta[\alpha_1, \ldots, \alpha_n]|$$

contradicting the minimality of $|\Delta[\alpha_1, \ldots, \alpha_n]|$. The result follows. □

We now show that all integral bases for $\mathfrak{O}_K$ have the same discriminant. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two $\mathbb{Z}$-bases for $\mathfrak{O}_K$. Let C be the change of basis matrix from the α_i to the β_i, and let D be the change of basis matrix from the β_i to the α_i. Then both C and D have integer entries (since we are talking about $\mathbb{Z}$-bases), and $CD = I_n$. So, in fact, $D = C^{-1}$. We have $1 - \det(I) = \det(C)\det(D)$ with $\det(C), \det(D) \in \mathbb{Z}$. It follows that $\det(C) = \pm 1$. Hence,

$$\Delta[\beta_i, \ldots, \beta_n] = \det(C)^2 \Delta[\alpha_1, \ldots, \alpha_n] = \Delta[\alpha_1, \ldots, \alpha_n].$$

Definition 2. The *discriminant* of a number field K, denoted $\Delta(K)$ is the discriminant of any integral basis for $\mathfrak{O}_K$.

Example 3. Let $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ and $d \neq 0, 1$. We have seen that $1, \sqrt{d}$ is an integral basis for $\mathfrak{O}_K$ if $d \neq 1 \bmod 4$, and $1, \frac{1+\sqrt{5}}{2}$ is an integral basis if $d = 1 \bmod 4$. We have

$$\det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = -2\sqrt{d} \quad \text{and} \quad \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix} = -\sqrt{d}.$$

Therefore,

$$\Delta(K) = \begin{cases} 4d & \text{if } d \neq 1 \bmod 4 \\ d & \text{if } d = 1 \bmod 4. \end{cases}$$

Proposition 4. Suppose that $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Q}$-basis for K consisting of algebraic integers. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathfrak{O}_K$.

Proof. Let $\beta_1, \ldots, \beta_n$ be an integral basis for $\mathfrak{O}_K$. Then since the α_i are algebraic integers, there exists an $n \times n$ matrix C with integer entries such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = C \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

It follows that

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(C)^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since the α_i and β_i are algebraic integers, these discriminants are rational integers, i.e., elements of $\mathbb{Z}$. Since $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, $\det(C) = \pm 1$. Since C is an integer matrix, it follows that C is invertible over the integers, and hence, the β_i are integer linear combinations of that α_i. It follows that the α_i form a $\mathbb{Z}$-basis for $\mathfrak{O}_K$. □

We will see an example later demonstrating that the converse of this proposition is not true.