Algebraic Number Theory – Lecture 3

Jobin Lavasani

"Verbum sapienti satis est."

1. Conjugates

If $K = \mathbb{Q}(\theta)$ is a number field there will be, in general, several distinct monomorphisms $\sigma : K \to \mathbb{C}$.

Example. Take $K = \mathbb{Q}(i)$ where $i = \sqrt{-1}$. Then we have

$$\sigma_1(x+iy) = x+iy$$
$$\sigma_2(x+iy) = x-iy$$

where $x, y \in \mathbb{Q}$.

Theorem 1. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then:*

- *there are exactly n distinct monomorphisms $\sigma_i : K \to \mathbb{C}$ $(1 \leqslant i \leqslant n)$, called the embeddings of K into $\mathbb{C}$;*
- *the elements $\theta_i := \sigma_i(\theta)$ are the distinct zeros in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$.*

Proof. See Stewart & Tall page 42. □

Example. For $K = \mathbb{Q}(i)$, the minimal polynomial of i is x^2+1, and K has a basis $\{1, i\}$ over $\mathbb{Q}$. So

$$\sigma_1(i) = i$$
$$\sigma_2(i) = -i.$$

2. The Field Polynomial

Definition. For each $\alpha \in K = \mathbb{Q}(\theta)$ we define the field polynomial of α to be

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha))$$

where the elements $\sigma_i(\alpha)$ are called the K-conjugates of α. Note that f_α depends on the field K.

Theorem 2. • *The field polynomial f_α is a power of the minimal polynomial p_α of α.*

- *The K-conjugates of α are the zeros of p_α in $\mathbb{C}$, each repeated n/m times where m is the degree of p_α.*
- *The element α is in $\mathbb{Q}$ if and only if all of its K-conjugates are equal.*
- *$\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ if and only if all K-conjugates of α are distinct.*

Proof. See Stewart & Tall page 43. □

Definition. Let $K = \mathbb{Q}(\theta)$ be of degree n and let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis. We define the discriminant of this basis to be

$$\Delta[\alpha_1, \ldots, \alpha_n] = \left(\det(\sigma_i(\alpha_j))_{1 \leqslant i,j \leqslant n}\right)^2.$$

Example. Let $K = \mathbb{Q}(i)$. Then,

$$\sigma_1(1) = 1 \qquad \sigma_1(i) = i$$
$$\sigma_2(1) = 1 \qquad \sigma_2(i) = -i.$$

So

$$\Delta[1, i] = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4.$$

Gauss' lemma. *Let $p \in \mathbb{Z}[t]$ and suppose $p = gh$ where $g, h \in \mathbb{Q}[t]$. Then there exists $\lambda \in \mathbb{Q}^\times$ such that $\lambda g, \lambda^{-1} h \in \mathbb{Z}[t]$.*

Lemma 1. *An algebraic number α is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Proof. Let p be the minimal polynomial of α over $\mathbb{Q}$, so p is monic and irreducible in $\mathbb{Q}[t]$.

($\Leftarrow$)**:** If $p \in \mathbb{Z}[t]$ then α is an algebraic integer by definition.
($\Rightarrow$)**:** If α is an algebraic integer then $q(\alpha) = 0$ for some monic polynomial $q \in \mathbb{Z}[t]$, and $p \mid q$, so $q = ph$ for some $h \in \mathbb{Q}[t]$. By Gauss' lemma there is some $\lambda \in \mathbb{Q}^\times$ such that $\lambda p \in \mathbb{Z}[t]$ and $\lambda p \mid q$. But p and q are monic so necessarily $\lambda = 1$.

□

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n and let $\sigma_1, \ldots, \sigma_n$ be the monomorphisms $K \to \mathbb{C}$. By theorem 1, the field polynomial of $\alpha \in \mathbb{Q}(\theta)$ is a power of the minimal polynomial of α. So by lemma 1 and Gauss' lemma it follows that $\alpha \in K$ is an algebraic integer if and only if the field polynomial is in $\mathbb{Z}[t]$.

3. Norm and Trace

Definition. For $\alpha \in K$ we define the norm of α as

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and the trace as

$$T(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Note that they both depend on the field K.

Since the σ_i are monomorphisms it's clear that $N(\alpha\beta) = N(\alpha)N(\beta)$ and if $\alpha \neq 0$ then $N(\alpha) \neq 0$. If $p, q \in \mathbb{Q}$ then we have $T(p\alpha + q\beta) = pT(\alpha) + qT(\beta)$.

Example. If $K = \mathbb{Q}(\sqrt{7})$ then the integers of K are given by $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$. The monomorphisms are

$$\sigma_1(p + q\sqrt{7}) = p + q\sqrt{7}$$
$$\sigma_2(p + q\sqrt{7}) = p - q\sqrt{7}.$$

So

$$N(p + q\sqrt{7}) = p^2 - 7q^2$$
$$T(p + q\sqrt{7}) = 2p,$$

and

$$\Delta[1, \sqrt{7}] = \begin{vmatrix} 1 & \sqrt{7} \\ 1 & -\sqrt{7} \end{vmatrix}^2 = 28.$$

Note that $N(\alpha)$ and $T(\alpha)$ are coefficients of f_α, and so are rational numbers in general, and rational integers if α is an algebraic integer.