Algebraic Number Theory – Lecture 2

Michael Harvey

"He who abandons the field is beaten."

– Victor Hugo

1. Algebraic Numbers

Definition 1. A complex number $\alpha \in \mathbb{C}$ is said to be algebraic if it satisfies some polynomial equation $f(x) = 0$ where $f \in \mathbb{Q}[x]$ is nonzero, i.e. $f(\alpha) = 0$.

Remark. The polynomial f is not unique. But there is a unique irreducible polynomial $m(x) \in \mathbb{Q}[x]$ with leading coefficient 1 satisfying $m(\alpha) = 0$. This polynomial is called the minimum polynomial of α. The degree of α is defined to be the degree of m.

Example 1. $\sqrt{5}, i, \varphi$ are all algebraic numbers, where φ is the golden ratio. They have minimum polynomials $x^2 - 5$, $x^2 + 1$, and $x^2 - x - 1$ respectively.

Definition 2. A number field (or algebraic number field) is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$, where $[K : \mathbb{Q}]$ is the dimension of K when viewed as a vector space over $\mathbb{Q}$. The number $[K : \mathbb{Q}]$ is called the degree of K over $\mathbb{Q}$.

Remark. Suppose K is a number field.

(1) If $\alpha \in K$ then α is algebraic;
(2) K is of the form $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ for finitely many algebraic numbers α_i;
(3) the set of all algebraic numbers is not a number field;
(4) $\mathbb{Q}(\pi), \mathbb{Q}(e)$, and so on, are not number fields.

Theorem 1. *If K is a number field then $K = \mathbb{Q}(\alpha)$ for some algebraic number α.*

Sketch proof. By induction it suffices to show that a number field of the form $\mathbb{Q}(\beta, \gamma)$ is of the form $\mathbb{Q}(\alpha)$ for some algebraic α. For an auspicious choice of $c \in \mathbb{Q}$ if we let $\alpha = \beta + c\gamma$ then it can be shown $\gamma \in \mathbb{Q}(\alpha)$. Hence $\beta = \alpha - c\gamma \in \mathbb{Q}(\alpha)$ and so $\mathbb{Q}(\beta, \gamma) \subseteq \mathbb{Q}(\alpha)$. And clearly $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta, \gamma)$, so the two fields are equal.[1] $\square$

Definition 3. A complex number α is called an algebraic integer if there is a nonzero monic polynomial over $\mathbb{Z}$, say $f(x) \in \mathbb{Z}[x]$, such that $f(\alpha) = 0$.

Example 2. $\sqrt{-2}$ and $\frac{1}{2}(\sqrt{29} - 3)$ are algebraic integers, they satisfy $x^2 + 2 = 0$ and $x^2 + 3x - 5 = 0$ respectively.

Remark. The set of all algebraic integers forms a ring, call this B.

[1]Full proof is in Stewart and Tall, pp.40–41.

Definition 4. If K is a number field, the ring of integers of K, denoted $\mathcal{O}_K$, is given by

$$\mathcal{O}_K = K \cap B.$$

Lemma 1. *If $\alpha \in K$ then there is some nonzero $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_K$.*

Proof. If $\alpha \in \mathcal{O}_K$ then we may take $c = 1$. If not consider the minimal polynomial of α, $m(x)$. Say

$$m(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

where $a_i \in \mathbb{Q}$ ($1 \leqslant i \leqslant n-1$). Let $c \in \mathbb{Z}$, $c \neq 0$ be the lowest common denominator of $a_0, a_1, \ldots, a_{n-1}$, and multiply $m(x)$ by c^n:

$$\begin{aligned} c^n m(x) &= c^n x^n + c a_{n-1} c^{n-1} x^{n-1} + \ldots + c^{n-1} a_1 c x + c^n a_0 \\ &= (cx)^n + c a_{n-1} (cx)^{n-1} + \ldots + c^{n-1} a_1 (cx) + c^n a_0. \end{aligned}$$

So $c\alpha$ satisfies the monic polynomial

$$\widetilde{m}(y) = y^n + c a_{n-1} y^{n-1} + \ldots + c^{n-1} a_1 y + c^n a_0 \in \mathbb{Z}[y],$$

and hence $c\alpha \in \mathcal{O}_K$. □

Corollary. *If K is a number field then $K = \mathbb{Q}(\theta)$ for some algebraic integer θ.*

Proof. If $c \in \mathbb{Q}$ is nonzero then clearly $\mathbb{Q}(c\alpha) = \mathbb{Q}(\alpha)$. We know $K = \mathbb{Q}(\alpha)$ for some algebraic number α, and by the previous lemma there is a nonzero rational integer c such that $c\alpha = \theta$ is an algebraic integer, hence $K = \mathbb{Q}(\alpha) = \mathbb{Q}(c\alpha) = \mathbb{Q}(\theta)$. □

2. Integral Basis

Definition 5. Let $\alpha_1, \ldots, \alpha_s \in \mathcal{O}_K$. The set $\{\alpha_1, \ldots, \alpha_s\}$ is an integral basis of $\mathcal{O}_K$ iff every element of $\mathcal{O}_K$ can be written as a unique linear combination of $\alpha_1, \ldots, \alpha_s$ with coefficients in $\mathbb{Z}$.

We note that an integral basis always exists, see Stewart and Tall page 51 for a proof.

Remark. Any integral basis is a basis for K over $\mathbb{Q}$ by the previous lemma. Indeed, if $\alpha \in K$ then there is a nonzero $c \in \mathbb{Z}$ such that $c\alpha \in \mathcal{O}_K$. So $c\alpha$ can be written as a unique linear combination of our integral basis elements over $\mathbb{Z}$, so, dividing through by c, we have that α is a unique linear combination of the integral basis elements over $\mathbb{Q}$.

If $K = \mathbb{Q}(\theta)$ for an algebraic integer θ, and $[K : \mathbb{Q}] = n$, then $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K. However, this is not necessarily an integral basis. For example, consider $K = \mathbb{Q}(\sqrt{5})$. A basis for K over $\mathbb{Q}$ is given by $\{1, \sqrt{5}\}$, but $\frac{1}{2}(1+\sqrt{5}) \in \mathcal{O}_K$ since it satisfies the polynomial equation $x^2 - x - 1 = 0$, but there are no rational integers a_0, a_1 such that $\frac{1}{2}(1+\sqrt{5}) = a_0 + a_1\sqrt{5}$.