ALGEBRAIC NUMBER THEORY

MUHAMMAD ATIF ZAHEER

Contents

1. Number Fields and Ring of Integers

A *number field* K is a finite field extension of $\mathbb{Q}$. Because every algebraic extension of $\mathbb{Q}$ can be realized as a subfield of $\mathbb{C}$ we generally take a number field K to be a subfield of $\mathbb{C}$. Moreover, since every algebraic extension over $\mathbb{Q}$ is separable, it follows by the primitive element theorem that a number field K is a simple extension of $\mathbb{Q}$, i.e., $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$.

The simplest class of number fields are quadratic fields, i.e., fields of the form $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}$ is not a square of a rational number. Without loss of generality we can take d to be a squarefree integer (different from 1). It can be easily shown that if n and m are distinct squarefree integers, then $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{m})$ are distinct as well (see Exercise 1.1) and as a consequence are nonisomorphic.

Another important class of number fields are cyclotomic fields, i.e., fields of the form $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$. It can be easily seen that if n is odd, then $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ as

$$\zeta_{2n} = \zeta_{2n}^{2n+1} = \zeta_{2n}^{n}\zeta_{2n}^{n+1} = -\zeta_n^{(n+1)/2} \in \mathbb{Q}(\zeta_n).$$

We will show later that $\mathbb{Q}(\zeta_n)$ are all distinct for n even.

A complex number α is said to be an *algebraic integer* if α is a root of a monic polynomial over $\mathbb{Z}$, i.e., $\alpha \in \mathbb{C}$ is an algebraic integer if there exist $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Proposition 1.1. *Let α be an algebraic integer and let $f \in \mathbb{Z}[x]$ be a monic polynomial of minimal degree having α as a root. Then $f(x)$ is irreducible over $\mathbb{Q}$. In particular, the irreducible polynomial of α over $\mathbb{Q}$ lies in $\mathbb{Z}[x]$.*

Proof. If f is not irreducible over $\mathbb{Q}$, then we can write $f = gh$, where g and h are nonconstant polynomials in $\mathbb{Q}[x]$. Without loss of generality we can assume that g and h are monic. It then follows by Gauss's lemma[1] that $h, g \in \mathbb{Z}[x]$. Since α is a root of $f(x)$, α must be a root of either g or h both of which have degrees strictly smaller than f but this contradicts the minimality of the degree of f. $\square$

Corollary 1.2. *The only algebraic integers in $\mathbb{Q}$ are integers.*

[1] A corollary to Gauss's lemma says that if $f, g, h \in \mathbb{Q}[x]$ are all monic, then $f \in \mathbb{Z}[x]$ implies that $g, h \in \mathbb{Z}[x]$.

PROOF. Let $q \in \mathbb{Q}$ be an algebraic integer. Then $x - q$ is the irreducible polynomial of q over $\mathbb{Q}$. Since q is an algebraic integer we must have $x - q \in \mathbb{Z}[x]$ and so $q \in \mathbb{Z}$. □

The above proposition serves as a useful criterion to check if an algebraic number is an algebraic integer. For instance, $i/2$ is an algebraic number but not an algebraic since since its irreducible polynomial $x^2 + 1/4$ over $\mathbb{Q}$ does not have integer coefficients.

THEOREM 1.3. *Let $\alpha \in \mathbb{C}$. Then the following are equivalent:*

(a) α is an algebraic integer.
(b) The additive group of the ring $\mathbb{Z}[\alpha]$ is finitely generated.
(c) α belongs to a subring of $\mathbb{C}$ having finitely generated additive group.
(d) $\alpha A \subset A$ for some nontrivial finitely generated subgroup $A \subset \mathbb{C}$.

PROOF. (a) $\Rightarrow$ (b): Note that if α is a root of a monic polynomial with integer coefficients of degree n, then $\mathbb{Z}[\alpha]$ is generated by $1, \alpha, \dots, \alpha^{n-1}$ since every power of α can be expressed as a linear combination of $1, \alpha, \dots, \alpha^{n-1}$.

The implications (b) $\Rightarrow$ (c) $\Rightarrow$ (d) are obvious.

(d) $\Rightarrow$ (a): Let A be generated by $\alpha_1, \dots, \alpha_n$. Then there is an $n \times n$ matrix M with integer entries such that

$$\begin{pmatrix} \alpha\alpha_1 \\ \vdots \\ \alpha\alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

We can write this matrix equation as

$$(\alpha I - M) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0.$$

Since not all of $\alpha_1, \dots, \alpha_n$ are zero, it follows that the matrix $\alpha I - M$ is singular, i.e., $\det(\alpha I - M) = 0$. Hence, α is a root of the characteristic polynomial $p(x) = \det(xI - M)$ of M which is a monic polynomial over $\mathbb{Z}$. Thus α is an algebraic integer. □

Exercises.

EXERCISE 1.1. Show that if n and m are distinct squarefree integers, then $\mathbb{Q}(\sqrt{n})$ and $\mathbb{Q}(\sqrt{m})$ are distinct as well.

EXERCISE 1.2. Let d be a squarefree integer and let

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Show that the set of algebraic integers in $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\omega_d]$.

SOLUTION. It is easy to see that $\mathbb{Z}[\omega_d] = \{a + b\,\omega_d : a, b \in \mathbb{Z}\}$ as $\omega_d^2 = d$ if $d \equiv 2, 3 \pmod 4$ and $\omega_d^2 = (d-1)/4 + \omega_d$ if $d \equiv 1 \pmod 4$. Now let $\alpha = p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Let $q \neq 0$ and let $x^2 + ax + b \in \mathbb{Q}[x]$ be the irreducible polynomial of α over $\mathbb{Q}$. Plugging in α we get

$$0 = \alpha^2 + a\alpha + b = (p + q\sqrt{d})^2 + a(p + q\sqrt{d}) + b = (p^2 + q^2 d + ap + b) + (2pq + aq)\sqrt{d}.$$

Comparing the coefficients we get

$$p^2 + q^2 d + ap + b = 0 \quad \text{and} \quad 2pq + aq = 0.$$

Because $q \neq 0$ we obtain $a = -2p$ and $b = p^2 - q^2 d$. Thus α is an algebraic integer if and only if $2p$ and $p^2 - q^2 d$ are both integers due to Proposition 1.1. We now treat the cases $d \equiv 2, 3 \pmod 4$ and $d \equiv 1 \pmod 4$ separately.

Suppose that $d \equiv 2, 3 \pmod 4$. Note that $\mathbb{Z}[\sqrt{d}]$ consists only of algebraic integers for if $p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ (with $q \neq 0$), then $2p$ and $p^2 - q^2 d$ are clearly integers.

Now let $p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ be an algebraic integer. If $q = 0$, then p must be integer due to Corollary 1.2 and so $p + q\sqrt{d} = p \in \mathbb{Z}[\sqrt{d}]$. If $q \neq 0$, then $a = 2p$ and $b = p^2 - q^2 d$ are both integers. Substituting a into b we get that $a^2/4 - q^2 d = (a^2 - 4q^2 d)/4$ is an integer. In particular, $4q^2 d$ is an integer. This implies that q is a half-integer. To see this take $q = r/s$, where r and s are coprime integers. Then $s^2 \,|\, 4r^2 d$ and so $s^2 \,|\, 4d$. Because d is squarefree it follows that $s^2 \,|\, 4$ and so $s \,|\, 2$. Let $q = c/2$, where c is an integer. Then we have

$$a^2 - c^2 d \equiv 0 \pmod 4.$$

Because $d \equiv 2, 3 \pmod 4$, it follows that $a^2 \equiv c^2 \equiv 0 \pmod 4$ for if $c^2 \equiv 1 \pmod 4$, then $a^2 \equiv 2, 3 \pmod 4$, a contradiction as 0 and 1 are the only quadratic residues mod 4. Hence a and c are both even and as a consequence $p = a/2$ and $q = c/2$ are both integers. Thus $p + q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Now suppose that $d \equiv 1 \pmod 4$. Let $a + b\omega_d \in \mathbb{Z}[\omega_d]$. Then

$$a + b\omega_d = \left(\frac{2a + b}{2}\right) + \frac{b}{2}\sqrt{d}.$$

Let $p + q\sqrt{d} = a + b\omega_d$, where $p, q \in \mathbb{Q}$. If $b = 0$, then $a + b\omega_d = a$ is clearly an algebraic integer. Now if $b \neq 0$, then $q \neq 0$ and

$$2p = 2a + b \quad \text{and} \quad p^2 - q^2 d = \frac{4a^2 + b^2 + 4ab}{4} - \frac{b^2 d}{4} = a^2 + ab + b^2\left(\frac{1 - d}{4}\right)$$

are both integers. Hence, $a + b\omega_d$ is an algebraic integer.

Now suppose that $p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is an algebraic integer. Again if $q = 0$, then p must be an integer and so $p + q\sqrt{d} = p \in \mathbb{Z}[\omega_d]$. If however $q \neq 0$, then $a = 2p$ and $b = p^2 - q^2 d$ must be integers. Just as before q must be half-integer so let $q = c/2$, where c is an integer. Again we have

$$a^2 - c^2 d \equiv 0 \pmod 4.$$

Because $d \equiv 1 \pmod 4$ we get $a^2 = c^2 \pmod 4$. This implies that $a \equiv c \pmod 2$ and so we have

$$p + q\sqrt{d} = \frac{a}{2} + \frac{c}{2}\sqrt{d} = \frac{a - c}{2} + c\left(\frac{1 + \sqrt{d}}{2}\right) \in \mathbb{Z}[\omega_d].$$