ALGEBRAIC NUMBER THEORY

MUHAMMAD ATIF ZAHEER

Contents

1. Number Fields and Ring of Integers

1.1. **Basic Definitions and Examples.** 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 $a_0, \dots, a_{n-1} \in \mathbb{Z}$ 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. $\square$

[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 $g, h \in \mathbb{Z}[x]$.

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

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 $q \in \mathbb{Z}$. $\square$

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 $1, \alpha, \ldots, \alpha^{n-1}$ since every power of α can be expressed as a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.

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

(d) $\Rightarrow$ (a): Let A be generated by $\alpha_1, \ldots, \alpha_n$. 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 $\alpha_1, \ldots, \alpha_n$ 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. $\square$

COROLLARY 1.4. *If α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$.*

PROOF. Suppose α and β are algebraic integers. If α and β are roots of monic polynomials over $\mathbb{Z}$ of degree n and m respectively, then note that $\mathbb{Z}[\alpha, \beta]$ is a subring of $\mathbb{C}$ with additive group generated by monomials of the form $\alpha^i\beta^j$, where $i = 0, 1, \ldots, n$ and $j = 0, 1, \ldots, m$. Since $\alpha + \beta$ and $\alpha\beta$ both lie in $\mathbb{Z}[\alpha, \beta]$, it follows by part (c) of Theorem 1.3 that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers as well. $\square$

REMARK 1.5. The above result shows that the set of all algebraic integers form a subring of $\mathbb{C}$ and it is denoted by $\mathbb{Z}$. This implies in particular that the set $\mathbb{Z}_K = \mathbb{Z} \cap K$ of all algebraic integers in K is a subring of K for any number field K. Note that if $L \supset K$ are number fields, then $\mathbb{Z}_L \cap K = \mathbb{Z}_K$. In particular, $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$ as $\mathbb{Z}_\mathbb{Q} = \mathbb{Z}$.

PROPOSITION 1.6. *Let K be a number field. If α is an algebraic integer, then all the conjugates of α over K are also algebraic integers. Moreover, the irreducible polynomial of α over K lies in $\mathbb{Z}_K[x]$.*

PROOF. Since α is an algebraic integer let $g \in \mathbb{Z}[x]$ be a monic polynomial having α as a root. Let f be the irreducible polynomial of α over K. Then clearly $g \in K[x]$ and so f divides g due to being irreducible. Thus every root of f is also a root of g and so every conjugate of α over K is an algebraic integer. Since the coefficients of f are algebraic combinations of the roots all of which are algebraic integers, it follows that the coefficients are also algebraic integers, i.e., $f \in \mathbb{Z}_K[x]$. □

Note that the above proposition is a generalization of Proposition 1.1.

CLAIM 1.7 ($\mathbb{Z}_K$ is integrally closed). *Let K be a number field and let $\mathbb{Z}_K$ be its ring of integers. If $\alpha \in \mathbb{C}$ is a root of a monic polynomial over $\mathbb{Z}_K$, then α is an algebraic integer.*

PROOF. Let $\alpha \in \mathbb{C}$ and let $f(x) \in \mathbb{Z}_K[x]$ be a monic polynomial such that $f(\alpha) = 0$. Let

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0.$$

It is easily observed that $A = \mathbb{Z}[\alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \alpha]$ is a ring with a finitely generated additive group, i.e., A is a finitely generated $\mathbb{Z}$-module. It now immediately follows from Theorem 1.3(c) that α is an algebraic integer. □

1.2. **Cyclotomic Fields.** In this section we will find the irreducible polynomial of ζ_n over $\mathbb{Q}$. This will allows us to determine the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. As an application we will also show that the $\mathbb{Q}(\zeta_n)$ are all distinct for n even.

Note that if θ is a conjugate of ζ_n over $\mathbb{Q}$, then θ must be a primitive nth root of unity for if $\theta^m = 1$ for some $m < n$, then θ is a root of $x^m - 1$. It then follows that the irreducible polynomial of θ which is the same as the irreducible polynomial of ζ_n divides $x^m - 1$. As a result we have $\zeta_n^m = 1$, a contradiction. Hence, the conjugates of ζ_n over $\mathbb{Q}$ are all primitive nth roots of unity.

The irreducible polynomial of ζ_n over $\mathbb{Q}$ is denoted by Φ_n.

We will now show in the next result that every primitive nth root of unity is a conjugate of ζ_n.

THEOREM 1.8. *Every primitive nth root of unity is a conjugate of ζ_n. In particular, the irreducible polynomial of ζ_n over $\mathbb{Q}$ is*

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - \zeta_n^k).$$

PROOF. Note that it suffices to show that if θ is a conjugate of ζ_n, then so is θ^p for every prime p not dividing n.

Let θ be a conjugate of ζ_n, i.e., $\Phi_n(\theta) = 0$ and let p be a prime not dividing n. Let $f \in \mathbb{Q}[x]$ be such that $\Phi_n(x)f(x) = x^n - 1$. Note that $f \in \mathbb{Z}[x]$ by Gauss's lemma. Because θ^p is a root of $x^n - 1$, it follows that θ^p is a root of either Φ_n or f. If $\Phi_n(\theta^p) = 0$, then we are done so suppose that $f(\theta^p) = 0$. Thus θ is a root of $f(x^p)$. This implies that $\Phi_n(x)$ divides $f(x^p)$. Let $g \in \mathbb{Q}[x]$ be such that $\Phi_n(x)g(x) = f(x^p)$. Again by Gauss's lemma we have $g \in \mathbb{Z}[x]$. Reducing the coefficients modulo p we get $\overline{\Phi}_n(x)\overline{g}(x) = \overline{f}(x^p)$. Note that we have $\overline{f}(x^p) = (\overline{f}(x))^p$. Let $h \in \mathbb{Z}_p[x]$ be an irreducible factor of $\overline{\Phi}_n$. Then h divides $\overline{f}(x)$ as well since $\mathbb{Z}_p[x]$ is a unique factorization domain. Due to $\overline{\Phi}_n(x)\overline{f}(x) = x^n - 1$ it follows that h^2 divides $x^n - 1$ in $\mathbb{Z}_p[x]$. Taking the derivative we obtain that h divides $\overline{n}x^{n-1}$ and so h must be a monomial, i.e., of the form $\overline{a}x^k$. But this is a contradiction as x does not divide $x^n - 1$ in $\mathbb{Z}_p[x]$ (or that 0 is a root of h but not of $x^n - 1$). □

COROLLARY 1.9. $[\mathbb{Q}(\zeta_n)/\mathbb{Q}] = \varphi(n)$.

COROLLARY 1.10. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$.

Due to the fundamental theorem of Galois theory we know that the subfields of $\mathbb{Q}(\zeta_n)$ correspond precisely to the subgroups of $\mathbb{Z}_n^\times$. If p is prime, then we know that $\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$. Because $\mathbb{Z}_p^\times$ has a unique subgroups for each divisor d of $p-1$, it follows that $\mathbb{Q}(\zeta_p)$ has a unique subfield K with $[\mathbb{Q}(\zeta_p) : K] = d$ ($[K : \mathbb{Q}] = (p-1)/d$) for each divisor d of $p-1$. In particular, if p is odd, then $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field.

Corollary 1.11. *If n is even, then the only roots of unity in $\mathbb{Q}(\zeta_n)$ are the nth root of unity. If n is odd, then the only roots of unity in $\mathbb{Q}(\zeta_n)$ are the $2n$th roots of unity.*

Proof. It suffices to prove the case when n is even as $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ if n is odd. Now let θ be a primitive mth root of unity in $\mathbb{Q}(\zeta_n)$. Without loss of generality we can take $\theta = \zeta_m$ as ζ_m is some power of θ. Suppose for the sake of contradiction that m does not divide m. Let k be the least common multiple of n and m. Then note that $\mathbb{Q}(\zeta_n)$ contains a primitive kth root of unity for if $a, b \in \mathbb{Z}$ are such that $am + bn = (n, m)$, then $\zeta_n^a \zeta_m^b = e^{2\pi i(am+bn)/nm} = e^{2\pi i(n,m)/nm} = e^{2\pi i/k} = \zeta_k$. Note that because $n \,|\, k$ and $n < k$ (as m does not divide n) we have $\varphi(k) > \varphi(n)$ (here we use the fact that n is even) which is a contradiction as $\mathbb{Q}(\zeta_k) \subset \mathbb{Q}(\zeta_n)$ which in turn leads to $\varphi(k) \,|\, \varphi(n)$. □

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 $s^2 \,|\, 4r^2d$ 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

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