

INTEGRAL ELEMENTS AND EXTENSIONS

PETE L. CLARK

Recall that a complex number α is said to be an **algebraic integer** if α is the root of a nonconstant monic polynomial with \mathbb{Z} coefficients: i.e., if there exists an n and integers a_0, \dots, a_{n-1} such that

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

In order to prove the Quadratic Reciprocity Law, we used the following fact:

Proposition 1. *Let n be a positive integer and ζ_n a primitive n th root of unity. Then every element of the ring $R_n = \mathbb{Z}[\zeta_n]$ is an algebraic integer.*

We give two proofs here. The first is a quick one, which however assumes the following fact that one should learn in undergraduate algebra: a subgroup of a finitely generated abelian group is finitely generated. One can deduce this from the structure theory of modules over a PID, although it is in fact easier (if less “undergrady”) to use a little bit of the theory of Noetherian rings. Then we will give a second proof, longer but self-contained, of a much more general result.

1. PROOF OF PROPOSITION 1

Let α be any element of $R_n = \mathbb{Z}[\zeta_n]$, and consider the subring $\mathbb{Z}[\alpha]$ generated by α . Note that R_n is a finitely generated abelian group: indeed, it is generated by $1, \zeta_n, \dots, \zeta_n^{n-1}$. (With a bit more care, one can verify that $R_n \cong \mathbb{Z}[T]/\Phi_n(T)$, so that $R_n \cong \mathbb{Z}^{\varphi(n)}$ as an abelian group. But we don’t need this.)

Instead, we will use the fact that $\mathbb{Z}[\alpha]$, being a subgroup of the finitely generated abelian group R_n , is itself finitely generated: that is, there exists a finite set of elements a_1, \dots, a_N of $\mathbb{Z}[\alpha]$ such that every element of $\mathbb{Z}[\alpha]$ can be written as a \mathbb{Z} -linear combination of the a_i ’s: $\beta \in \mathbb{Z}[\alpha] \implies$

$$\beta = r_1 a_1 + \dots + r_N a_N, \quad r_i \in \mathbb{Z}.$$

Now each element $a_i \in \mathbb{Z}[\alpha]$ is, by definition, a polynomial in α with integer coefficients, say $a_i = f_i(\alpha)$. Let t be the maximum degree of these polynomials. We may therefore write $\beta = \alpha^{t+1}$ as

$$\alpha^{t+1} = r_1 f_1(\alpha) + \dots + r_N f_N(\alpha),$$

which shows that α satisfies the monic polynomial

$$T^{t+1} - r_1 f_1(T) - \dots - r_N f_N(T)$$

and is therefore an algebraic integer.

2. INTEGRALITY IN RING EXTENSIONS

If S is a ring extension of R – i.e., $R \subset S$ – we will say that an element α of S is **algebraic integral** (or just **integral**) over R if there exist $a_0, \dots, a_{n-1} \in R$ such that

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

Theorem 2. *For $R \subset S$ an inclusion of rings, the set I_R of all elements of S which are integral over R form a subring of S .*

Applying Theorem 2 in the case of $R = \mathbb{Z}$, $S = \mathbb{C}$ we deduce:

Theorem 3. *The algebraic integers form a ring.*

Since the ordinary integers and ζ_n are algebraic integers, this provides another proof of Proposition 1.

Let S be an extension ring of R . A subset A of S is said to be a **spanning set** for S over R if for every element α of S there exist finitely many elements a_1, \dots, a_n of A and r_1, \dots, r_n of R such that

$$\alpha = r_1a_1 + \dots + r_na_n.$$

If R is a field, then S may be viewed as a vector space over R , and we have the same definition of spanning set from linear algebra.¹

Definition: S is **finite** over R if there exists a finite spanning set A . Again, in the case that R is a field, this just expresses the condition that S be finite-dimensional as an R -vector space.

Lemma 4. *If $R \subset S \subset T$ and S is finite over R and T is finite over S then T is finite over R .*

Proof: Let a_1, \dots, a_m be a spanning set for T over S , and b_1, \dots, b_n be a spanning set for S over R . Then for any α in T we can write

$$\alpha = s_1a_1 + \dots + s_ma_m,$$

and also for all $1 \leq i \leq m$, $s_i = \sum_j r_{ij}b_j$ with $r_{ij} \in R$, so

$$\alpha = \sum_{i=1}^m \sum_{j=1}^n r_{ij}a_ib_j,$$

which shows that $(a_ib_j)_{1 \leq i \leq m, 1 \leq j \leq n}$ is a finite spanning set for T over R .

For any α in S , we may consider the subring $R[\alpha]$ of S , which consists of all polynomial expressions in α with coefficients in R .

Proposition 5. *Let S be an extension ring of R and α an element of S . The following are equivalent:*

- a) α is integral over R .
- b) $R[\alpha]$ is finite over R .

¹In the general case one cannot necessarily find a spanning set such that the coefficients r_i are unique – i.e., bases need not exist. But this is not an issue for us here.

Proof: If α is integral over R , then there exists a polynomial equation

$$\alpha^n + r_{n-1}\alpha^{n-1} + \dots + r_1\alpha + r_0 = 0,$$

or equivalently

$$\alpha^n = -r_{n-1}\alpha^{n-1} - \dots - r_1\alpha - r_0.$$

This relation allows us to rewrite any polynomial in α with R -coefficients as a polynomial of degree at most $n-1$, which means that $1, \alpha, \dots, \alpha^{n-1}$ is a spanning set for $R[\alpha]$ over R .

The converse is the same argument we used above: suppose that we have a spanning set for $R[\alpha]$, say $f_1(\alpha), \dots, f_r(\alpha)$, where $f_i \in R[T]$ are polynomials. Let n be the maximum of the degrees of the f_i 's. By hypothesis we can write

$$\alpha^{n+1} = \sum_i r_i f_i(\alpha),$$

meaning that α is a root of the monic polynomial $T^{n+1} - \sum_i r_i f_i(T)$.

Suppose that $\alpha \in S$ is integral over R , so that $R[\alpha]$ is a finite extension ring of R . If integral elements form a subring, then we want every element β of $R[\alpha]$ to be integral over R : equivalently we want $R[\beta]$ to be finite over R . Unfortunately it is not clear that if we have $R \subset S \subset T$ and T is finite over R , then S is finite over R . So in the case at hand the following result is the key one:

Theorem 6. *Suppose $R \subset T$ and α is an element of T . If there exists an intermediate ring $R \subset S \subset T$ such that S is finite over R and $\alpha \in S$, then α is integral over R .*

Proof: Let s_1, \dots, s_n be a finite set of generators for S over R , and express each of the elements $s_i\alpha$ in terms of these generators:

$$s_i\alpha = \sum_{j=1}^n r_{ij}s_j, \quad r_{ij} \in R.$$

Let M be the $n \times n$ matrix $\alpha I_n - (r_{ij})$; then recall from linear algebra that

$$MM^* = \det(M) \cdot I_n,$$

where M^* is the ‘‘adjugate’’ matrix (of cofactors). If $s = (s_1, \dots, s_n)$ (the row vector), then the above equation implies $0 = sM = sMM^* = s \det(M) \cdot I_n$. The latter matrix equation amounts to $s_i \det(M) = 0$ for all i . Since we can express 1 as an R -linear combination of the s_i 's, this gives $\det(M) = 0$, which means that α is a root of the monic polynomial $\det(T \cdot I_n - (a_{ij}))$.

From here on in everything is quite routine:

Lemma 7. *If we have rings $R \subset S \subset T$, and $\alpha \in T$ is integral over R , it is necessarily integral over S .*

Proof: This is immediate: by hypothesis there exists a nonconstant polynomial $P \in R[T]$ such that $P(\alpha) = 0$. But since $R \subset S$, P is also a polynomial in $S[T]$.

Corollary 8. *Suppose S is an extension of R and we have elements α_1, α_2 of S , each integral over R . Then $\alpha_1 + \alpha_2$, and $\alpha_1 \cdot \alpha_2$ are integral over R .*

Proof: Since α_2 is integral over R , by the preceding lemma it is certainly also integral over $R[\alpha_1]$, so by Theorem 5 we have $R[\alpha_1][\alpha_2] = R[\alpha_1, \alpha_2]$ is finite over $R[\alpha_1]$. Also, since α_1 is integral over R , $R[\alpha_1]$ is finite over R , and by Lemma 4 we conclude that $R[\alpha_1, \alpha_2]$ is finite over R . By Theorem 6, this implies that the elements $\alpha_1 + \alpha_2$ and $\alpha_1 \cdot \alpha_2$, lying in a finite extension ring of R , are necessarily integral over R .

Theorem 2 follows immediately.

3. ALGEBRAIC NUMBERS

While we are on the topic we may as well also prove the following result:

Theorem 9. *The algebraic numbers are the quotient field of the ring of algebraic integers.*

Proof: This amounts to three statements:

- (i) The algebraic numbers form a ring.
- (ii) The inverse of every nonzero algebraic number is an algebraic number.
- (iii) Every algebraic number is a quotient of two algebraic integers.

We can prove (i) by observing that a complex number is algebraic iff it is integral over \mathbb{Q} : if there exist $a_0, \dots, a_n \in \mathbb{Z}$, $a_n \neq 0$ such that

$$a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$$

then

$$\alpha^n + \left(\frac{a_{n-1}}{a_n}\right)\alpha^{n-1} + \dots + \left(\frac{a_1}{a_n}\right)\alpha + \left(\frac{a_0}{a_n}\right) = 0$$

is a monic polynomial with \mathbb{Q} -coefficients. Therefore we may apply Theorem 2 with $R = \mathbb{Q}$, $S = \mathbb{C}$.

To prove (ii), observe that if $\alpha \neq 0$ satisfies a polynomial as above, then dividing through by α^n gives

$$a_n + a_{n-1}\alpha^{-1} + \dots + a_1(\alpha^{-1})^{n-1} + a_0(\alpha^{-1})^n = 0,$$

which gives a polynomial equation satisfied by α^{-1} .

Finally, in place of (iii) we will prove the stronger:

Lemma 10. *If α is an algebraic number, there exists a positive integer d such that $d\alpha$ is an algebraic integer.*

Proof: If α is algebraic, then there are integers a_0, \dots, a_n , $a_n \neq 0$, such that

$$a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0.$$

Multiply this equation through by a_n^{n-1} to get

$$(a_n \alpha)^n + a_{n-1}(a_n \alpha)^{n-1} + a_{n-2}a_n(a_n \alpha)^{n-2} + \dots + a_1 a_n^{n-2}(a_n \alpha) + a_n^{n-1} a_0 = 0,$$

which shows that $a_n \alpha$ is an algebraic integer.