On the Definition of Algebraic Integers

R. C. Daileda

1 Introduction

A complex number $\alpha \in \mathbb{C}$ is called *algebraic (over $\mathbb{Q}$)* if it is a root of a nonzero polynomial over $\mathbb{Q}$. Let $E_\alpha : \mathbb{Q}[X] \to \mathbb{C}$ denote the evaluation at α homomorphism. By assumption the kernel is nontrivial, so there is a unique monic $f(X) \in \mathbb{Q}[X]$ so that $\ker E_\alpha = (f)$. We call f the *minimal polynomial* of α and $\deg f$ the *degree* of α. The minimal polynomial f has the property that if $g(X) \in \mathbb{Q}[X]$ and $g(\alpha) = 0$, then f divides g in $\mathbb{Q}[X]$. The image of E_α is a subring of $\mathbb{C}$, so it must be a domain. Therefore f is prime. But $\mathbb{Q}[X]$ is a PID, in which primes and irreducibles coincide, so can we conclude that the minimal polynomial $f(X)$ of α is irreducible in $\mathbb{Q}[X]$. This means (f) is actually maximal. Hence the image of E_α, the ring $\mathbb{Q}[\alpha]$ of all rational polynomials in α, must be a field. The smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and α is denoted $\mathbb{Q}(\alpha)$. We therefore have $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Scaling f by an appropriate integer in order to "clear denominators," we can assume that $f(X) \in \mathbb{Z}[X]$. If we factor out and cancel the GCD of the coefficients, we can also assume that f is *primitive*, i.e. the GCD of its coefficients is 1. This form of the minimal polynomial of α is also (essentially) unique. For if $g(X) \in \mathbb{Z}[X]$ is primitive, has the same degree as f and vanishes at α, let f and g have leading coefficients $a, b \in Z$, respectively. Then α is a root of $h(X) = \frac{b}{a}f(X) - g(X) \in \mathbb{Q}[X]$. Hence f divides h in $\mathbb{Q}[X]$. But $\deg h < \deg f$, so this can only occur if $h = 0$. This in turn implies that $bf = ag$. Because f and g are primitive, the GCD of the coefficients of bf is $|b|$, while that of ag is $|a|$. From the equality $bf = ag$ we then deduce that $|a| = |b|$, and hence, by cancellation, $f = \pm g$. Scaling by -1 if necessary, we can assume the leading coefficient of f is positive. This additional restriction makes f completely unique. In this form we will call f a *primitive minimal polynomial* for α.

If K is a subfield of $\mathbb{C}$ containing $\mathbb{Q}$, then ordinary multiplication by elements of $\mathbb{Q}$ makes K into a $\mathbb{Q}$-vector space. When $\alpha \in \mathbb{C}$ is algebraic of degree n, we will later prove in class that $\mathbb{Q}(\alpha)$ has dimension n over $\mathbb{Q}$. That is, there are n numbers $\beta_1, \beta_2, \dots, \beta_n \in \mathbb{Q}(\alpha)$ so that for every $\beta \in \mathbb{Q}(\alpha)$ there exist unique $a_i \in \mathbb{Q}$ so that $\beta = \sum_i a_i\beta_i$. In particular, $\mathbb{Q}(\alpha)$ is *finitely generated* over $\mathbb{Q}$. The field of rational numbers is the so-called *quotient field* of $\mathbb{Z}$, the smallest subfield of $\mathbb{C}$ containing $\mathbb{Z}$. Analogously, it isn't hard to argue that $\mathbb{Q}(\alpha)$ is the quotient field of the ring $\mathbb{Z}[\alpha]$ of polynomials in α with integral coefficients. A natural question to ask is whether $\mathbb{Z}[\alpha]$ is finitely generated over $\mathbb{Z}$,[1] in the same way that $\mathbb{Q}(\alpha)$ is finitely generated over $\mathbb{Q}$. That is, are there elements $\beta_1, \dots, \beta_k \in \mathbb{Z}[\alpha]$ so that every element of $\mathbb{Z}[\alpha]$ can be expressed in the form $\sum_i a_i\beta_i$, for some $a_i \in \mathbb{Z}$?

2 Finitely Generated $\mathbb{Z}$-Modules[2]

To answer this question, let's begin by considering what $\mathbb{Z}[\alpha]$ being finitely generated over $\mathbb{Z}$ says about α. Assume $\mathbb{Z}[\alpha]$ can be generated by $\beta_1, \dots, \beta_k$. Since $\alpha\beta_i \in \mathbb{Z}[\alpha]$ for all i, there exist $a_{ij} \in \mathbb{Z}$ so that

$$\alpha\beta_i = \sum_{j=1}^{k} a_{ij}\beta_j \tag{1}$$

[1] This is equivalent to $\mathbb{Z}[\alpha]$ being finitely generated as an additive abelian group.

[2] A $\mathbb{Z}$-*module* is simply an additive abelian group, on which $\mathbb{Z}$ acts in the usual way.

for each i. The linear system (1) is equivalent to the matrix equation

$$\alpha \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kk} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_k \end{pmatrix}, \tag{2}$$

which shows that α is an eigenvalue of the coefficient matrix $A = (a_{ij})$. Recall that the eigenvalues of a matrix are the roots of its characteristic polynomial. The characteristic polynomial is always monic and has coefficients in the same ring as the entries of the matrix. In our case this means that α must be a root of a monic $g(X) \in \mathbb{Z}[X]$. That is, if $\mathbb{Z}[\alpha]$ is finitely generated, then α must be a root of a *monic* polynomial in $\mathbb{Z}[X]$.

The converse holds as well. Suppose $\alpha \in \mathbb{C}$ is a root of the monic polynomial $g(X) \in \mathbb{Z}[X]$. Let $\beta \in \mathbb{Z}[\alpha]$. Then there is a $p(X) \in \mathbb{Z}[X]$ so that $\beta = p(\alpha)$. Since g is monic, we can use the division algorithm to write $p = qg + r$, where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r < \deg g$. Thus $\beta = p(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = r(\alpha)$,[3] since $g(\alpha) = 0$. What does this amount to? Let $m = \deg g$. Then $r(\alpha)$ is a $\mathbb{Z}$-linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$. Because $\beta \in \mathbb{Z}[\alpha]$ was arbitrary, this shows that $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ generate $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$, i.e. $\mathbb{Z}[\alpha]$ is finitely generated. Let's record this important observation.

Theorem 1. *Let $\alpha \in \mathbb{C}$. The ring $\mathbb{Z}[\alpha]$ is (additively) finitely generated if and only if there is a monic $g(X) \in \mathbb{Z}[X]$ so that $g(\alpha) = 0$.*

The complex numbers satisfying either of the equivalent conditions in Theorem 1 are called *algebraic integers*. When α is an algebraic integer, the ring $\mathbb{Z}[\alpha]$ is an example of an *order* in $\mathbb{C}$ (see *Orders in* $\mathbb{C}$). We mention that one can use Gauss' lemma (see [1] or [2]) to prove that if $\alpha \in \mathbb{C}$ is an algebraic integer, then its primitive minimal polynomial in $\mathbb{Z}[X]$ must be monic. This is equivalent to saying that the minimal polynomial of α over $\mathbb{Q}$ has integral coefficients. However, as we have seen, the existence of *any* monic polynomial in $\mathbb{Z}[X]$ having α as a root is sufficient to establish that α is an algebraic integer.

Example. If $\alpha \in \mathbb{C}$ is algebraic but not an algebraic integer, $\mathbb{Z}[\alpha]$ cannot be finitely generated over $\mathbb{Z}$. This sounds somewhat intimidating, and surely such numbers must be extremely exotic. Except that they aren't. If $g(X) \in \mathbb{Z}[X]$ is monic, the rational root test implies that the only rational roots of g (if there are any) must be integers. This means that a rational number as mundane as $\frac{1}{2}$ cannot be an algebraic integer. Thus, $\mathbb{Z}[\frac{1}{2}]$ isn't finitely generated. While this may seem surprising at first glance, it's easy to explain. First note that

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{m}{2^n} \,\middle|\, m \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}.$$

Let $\frac{m_1}{2^{n_1}}, \ldots, \frac{m_k}{2^{n_k}} \in \mathbb{Z}[\frac{1}{2}]$. By scaling both the numerator and denominator of each of these fractions by powers of 2, we can assume that $n_1 = n_2 = \cdots = n_k = N$. Then every $\mathbb{Z}$-linear combination of $\frac{m_1}{2^N}, \ldots, \frac{m_k}{N}$ is again of the form $\frac{m}{2^N}$. However, no such fraction can equal $\frac{1}{2^{N+1}}$. If $\frac{m}{2^N} = \frac{1}{2^{N+1}}$, then $2^{N+1}m = 2^N$ which implies $2m = 1$, an obvious contradiction. This shows that no finite subset of $\mathbb{Z}[\frac{1}{2}]$ can generate the entire ring over $\mathbb{Z}$. So $\mathbb{Z}[\frac{1}{2}]$ is not finitely generated. □

The trouble in the preceding example, and in general, is denominators. Suppose α is algebraic and a root of $g(X) = \sum_i a_i X^i \in \mathbb{Z}[X]$ with degree m. We then have

$$0 = a_m^{m-1} g(\alpha) = \sum_{i=0}^{m} a_m^{m-1} a_i \alpha^i = (a_m \alpha)^m + \sum_{i=0}^{m-1} a_m^{m-1-i} a_i (a_m \alpha)^i,$$

which shows that $\beta = a_m \alpha$ is an algebraic integer. If we write this instead as $\alpha = \frac{\beta}{a_m}$, we find that every algebraic number can be written in the form $\frac{\beta}{a}$, where β is an algebraic integer and a is a (rational) integer. If there is no such expression for a given algebraic α with $a = 1$, then α isn't integral and $\mathbb{Z}[\alpha]$ fails to be

[3] We have just taken advantage of the fact that E_α is a homomorphism!

finitely generated. So it is the potential presence of a denominator a that cannot be "absorbed" into β that prevents every algebraic number from being integral.

The following extension of Theorem 1 is particularly useful in applications.

Theorem 2. *For all $\alpha \in \mathbb{C}$, α is an algebraic integer if and only if there is a finitely generated additive subgroup $A \subset \mathbb{C}$ so that $\alpha A \subset A$.*

Proof. If α is an algebraic integer, $A = \mathbb{Z}[\alpha]$ works, by Theorem 1. Conversely, suppose $A \subset \mathbb{C}$ is (additively) finitely generated and that $\alpha A \subset A$. Let $\beta_1, \beta_2, \ldots, \beta_k$ be a set that $\mathbb{Z}$-spans A. Because $\alpha A \subset A$, $\alpha\beta_i \in A$ for all i. We can now employ the same argument used at the beginning of this section verbatim, to conclude that α is an algebraic integer. □

As an application, we prove the following fundamental property of the set $\mathbb{A}$ of algebraic integers.

Theorem 3. *$\mathbb{A}$ is a subring of $\mathbb{C}$.*

Proof. First, $1 \in \mathbb{A}$ since it is a root of $X - 1$. Let $\alpha, \beta \in \mathbb{A}$. Since $\mathbb{Z}[\beta]$ is finitely generated over $\mathbb{Z}$, $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha][\beta]$ is finitely generated over $\mathbb{Z}[\alpha]$. Since $\mathbb{Z}[\alpha]$ is finitely generated over $\mathbb{Z}$, it follows that $\mathbb{Z}[\alpha, \beta]$ is finitely generated over $\mathbb{Z}$ as well. Since $\mathbb{Z}[\alpha, \beta]$ is a ring containing α and β, it is carried into itself under multiplication by $\alpha - \beta$ and $\alpha\beta$. By Theorem 2, $\alpha - \beta, \alpha\beta \in \mathbb{A}$. This proves $\mathbb{A}$ is a subring of $\mathbb{C}$. □

A similar argument using degrees of field extensions can be used to show that if $\alpha, \beta \in \mathbb{C}$ are just algebraic, then $\mathbb{Q}(\alpha, \beta)$ has finite degree (dimension) over $\mathbb{Q}$, which implies that $\alpha - \beta, \alpha/\beta \in \mathbb{Q}(\alpha, \beta)$ are also algebraic (when $\beta \neq 0$). This proves that the set of algebraic numbers is a sub*field* of $\mathbb{C}$. In both cases, finite generation allows us to conclude that the elements in question are roots of the appropriate types of polynomials, without actually finding those polynomials. This is critical, for it is not at all clear how one might find the minimal polynomial for $\alpha - \beta$, say, from the minimal polynomials of α and β. The field of algebraic numbers is typically denoted $\overline{\mathbb{Q}}$. The notation is meant to indicate that $\overline{\mathbb{Q}}$ is the *algebraic closure* of $\mathbb{Q}$ in $\mathbb{C}$, a fact whose proof requires machinery we won't develop here.

References

[1] Hungerford, T. W., *Algebra*, Grad. Texts Math. 73, Springer, 1974.

[2] Marcus, D. A. *Number FIelds*, Springer, 1977.