ANOTHER SHORT PROOF THAT RATIONAL ALGEBRAIC INTEGERS ARE INTEGERS

ALAN ROCHE

Abstract. We give a short proof, prompted by a note by Gary Lawlor, that a rational algebraic integer is an ordinary integer. In contrast to the standard approach, the argument makes no appeal to divisibility.

Gary Lawlor gave a wonderfully short, clever proof that the nth root of a positive integer is an integer or irrational [4]. We show that his method also gives the well-known, more general result that an algebraic integer that is a rational number must be an ordinary integer. In other words, if an algebraic integer is real but not an ordinary integer then it's irrational. The standard proofs use divisibility properties of integers (see, for example, [2, p. 66] or [5, pp. 10-11]). In contrast, the argument below makes no mention of divisibility. See [1] for another proof, an elegant one, that avoids divisibility and [3] for a recasting, also elegant, in the language of linear algebra.

First, a bit about our protagonist in case you haven't met.

Definition. An *algebraic integer* is a complex number that is a root of a monic polynomial with integer coefficients.

Some examples.

1. An ordinary integer k is an algebraic integer; it's a root of $\mathrm{X} - k$. More generally, for n a positive integer and k an integer (nonnegative if n is even), the real number $\sqrt[n]{k}$ is an algebraic integer; it's a root of $\mathrm{X}^n - k$.
2. The golden ratio $\dfrac{1+\sqrt{5}}{2}$ is an algebraic integer; it's a root of $\mathrm{X}^2 - \mathrm{X} - 1$.
3. $\dfrac{1+i}{\sqrt{2}} = e^{\pi i/4}$ is an algebraic integer for $i = \sqrt{-1}$; it's an 8th root of unity, that is, a root of $\mathrm{X}^8 - 1$.

Theorem. *An algebraic integer that is also a rational number must be an ordinary integer.*

We'll give our proof a là Lawlor in a moment. If you apply it to the algebraic integer $\sqrt[n]{k}$ (example 1), you recover Lawlor's original argument [4]. A basic finiteness property of algebraic integers, recorded in the lemma below, underpins the proof. To state the property, we need some notation. Let α be an algebraic integer. Thus there are integers $a_1, \ldots, a_k$ such that $\alpha^k + a_1\alpha^{k-1} + \cdots + a_k = 0$, or equivalently

$$\alpha^k = -a_k - \cdots - a_1\alpha^{k-1}. \tag{1}$$

We write $\mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$ for the set of linear combinations with integer coefficients of $1, \alpha, \ldots, \alpha^{k-1}$. Further, we write $\mathbb{Z}[\alpha]$ for the set of linear combinations with integer coefficients of $1, \alpha, \alpha^2, \ldots$. That is, $\mathbb{Z}[\alpha]$ consists of all complex numbers $c_0 + c_1\alpha + \cdots + c_n\alpha^n$ with $c_0, \ldots, c_n \in \mathbb{Z}$, as n varies through the set of nonnegative integers. The set $\mathbb{Z}[\alpha]$ is the smallest subring of the complex numbers (with identity) that contains α.

Lemma. *We have* $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$.

Proof. It suffices to show that $\alpha^n \in \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$, for $n = 0, 1, 2, \ldots$, which we prove by induction. The base case $n = 0$ is visibly true. For the inductive step, suppose $\alpha^n \in \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$. That is, suppose there are integers $b_1, \ldots, b_k$ such that

$$\alpha^n = b_k + \cdots + b_1\alpha^{k-1}.$$

Multiplying each side by α then gives

$$\alpha^{n+1} = b_k\alpha + \cdots + b_1\alpha^k.$$

Next we substitute the right side of (1) for α^k and multiply through by b_1. Collecting like terms, we conclude that $\alpha^{n+1} \in \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$. We've established the inductive step and so the proof is complete. □

With the lemma in hand, we can apply Lawlor's method to quickly prove the theorem.

Proof. Let α be an algebraic integer that is also a rational number. Write a for the integer with $a \leq \alpha < a + 1$ and set $\theta = \alpha - a$, so that $0 \leq \theta < 1$. For n a positive integer, $\theta^n = (\alpha - a)^n \in \mathbb{Z}[\alpha]$. Invoking the lemma, there is a positive integer k such that $\theta^n \in \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{k-1}$. That is, there are integers $c_0, c_1, \ldots, c_{k-1}$ with

$$\theta^n = c_0 + c_1\alpha + \cdots + c_{k-1}\alpha^{k-1}.$$

By assumption, we can write $\alpha = \dfrac{p}{q}$ for integers p and q with $q > 0$. Thus

$$\begin{aligned}\theta^n &= c_0 + c_1\frac{p}{q} + c_2\frac{p^2}{q^2} + \cdots + c_{k-1}\frac{p^{k-1}}{q^{k-1}} \\ &= \frac{c_0q^{k-1} + c_1pq^{k-2} + \cdots + c_{k-1}p^{k-1}}{q^{k-1}}.\end{aligned}$$

Since $0 \leq \theta^n < 1$, we see that $\theta^n = \dfrac{b}{q^{k-1}}$ for b a nonnegative integer with $b < q^{k-1}$. It follows that the set $\{\theta, \theta^2, \theta^3, \ldots\}$ is finite, and so $\theta = 0$. That is, $\alpha = a$ is an ordinary integer. □

References

[1] Gilat, D. (2012). Gauss's Lemma and the Irrationality of Roots, Revisited, *Math. Mag.* 85(2): 114-116.

[2] Ireland, K., Rosen, M. (1990). *A Classical Introduction to Modern Number Theory.* 2nd ed. Graduate Texts in Math., 84, New York, NY: Springer-Verlag.

[3] Lawlor, G. R. (2021). An Eigenargument for Irrational Roots, *College Math. J.* 52(2): 140-141.

[4] Lawlor, G. R. (2022). A Simple Proof that nth roots are Always Integers or Irrational, *Math. Mag.* 95(4): 332.

[5] Marcus, D. A. (2018). *Number Fields.* 2nd ed. Universitext, New York, NY: Springer.

Alan Roche studied at University College Dublin and the University of Chicago, and has taught at the University of Oklahoma for more years than he is willing to mention. The number of cats in his household, while changing over time, has always been a positive rational algebraic integer—and only briefly a root of unity.

Dept. of Mathematics, University of Oklahoma, Norman, OK 73019.
E-mail address: aroche@ou.edu