IRRATIONAL ALGEBRAIC INTEGERS

LEO GOLDMAKHER

Abstract. One of the great achievements of the Greeks was to discover that there exist numbers other than the rationals. In particular, they proved that $\sqrt{2}$ (which arose naturally as the diagonal of a unit square) is irrational. Since then, there have been many other proofs of this. Here I present two particularly striking proofs.

1. Arithmetic Proof

Suppose $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Then $2 = \frac{a^2}{b^2}$, whence $b^2 \mid a^2$. By the fundamental theorem of arithmetic, we deduce that $b \mid a$. But this would imply that $\sqrt{2} = \frac{a}{b} \in \mathbb{Z}$. □

This proof immediately gives the following generalization:

Theorem 1.1. *For any $n \in \mathbb{N}$, either $\sqrt{n} \in \mathbb{N}$ or $\sqrt{n} \notin \mathbb{Q}$.*

2. Algebraic Proof

Let $\mathcal{A} = \{n \in \mathbb{N} : n\sqrt{2} \in \mathbb{N}\}$, and observe that $n \in \mathcal{A} \implies n(\sqrt{2}-1) \in \mathcal{A}$. Since $n(\sqrt{2}-1) < n$, we deduce that $\mathcal{A}$ has no least element, and must therefore be empty. □

This proof also generalizes quite nicely. Recall that $\alpha \in \mathbb{R}$ is called an *algebraic number* if it is the root of some polynomial in $\mathbb{Z}[x]$. If α happens to be the root of some *monic* polynomial in $\mathbb{Z}[x]$, it is called an *algebraic integer*. To emphasize the distinction between algebraic integers and the ordinary integers, the latter are often called the *rational integers*. We prove the following:

Theorem 2.1. *Every non-rational algebraic integer is irrational. In other words, any non-integral root of a monic polynomial over $\mathbb{Z}$ is irrational.*

Proof. Let α be a non-rational algebraic integer. Then it is the root of some monic polynomial $P(x) \in \mathbb{Z}[x]$, of degree d, say. Since $P(x)$ is monic, it follows that any power of α can be written as a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ over $\mathbb{Z}$.

Let $g(x) = (x - \lfloor \alpha \rfloor)^{d-1}$, and consider the set $\mathcal{B} = \{n \in \mathbb{N} : n\alpha, n\alpha^2, \ldots, n\alpha^{d-1} \in \mathbb{Z}\}$. Observe that $n \in \mathcal{B} \implies ng(\alpha) \in \mathcal{B}$. Since $ng(\alpha) < n$, we deduce that $\mathcal{B}$ has no least element, and must therefore be empty. □

I am grateful to Trevor Wooley for introducing me to the algebraic proof.

3. Remarks

It is evident that α is irrational if and only if its minimal polynomial has degree $\geqslant 2$, thus seemingly making the above theorem redundant. This is not the case, since proving the minimality of a polynomial is no easier than proving irrationality! The strength of Theorem 2.1 is precisely that one doesn't need the minimal polynomial of α; *any* monic polynomial which has α as a root will do. Incidentally, the restriction of the polynomial being monic cannot in general be removed. For example, $5x^2 + x - 4$ has $4/5$ as a root.

Most proofs of the irrationality of $\sqrt{2}$ are either arithmetic, in the sense that they rely on unique factorization, or algebraic, in that they use instead some algebraic relation satisfied by $\sqrt{2}$. The proof of Theorem 2.1 given above is algebraic, but one can also give a simple arithmetic proof by deducing it from the Rational Roots theorem.

Neither the arithmetic nor the algebraic approach seems to be useful for numbers such as γ, $\pi + e$, or πe, for which we do not know any algebraic relations.

Department of Mathematics, University of Toronto
40 St. George Street, Room 6290
Toronto, M5S 2E4, Canada
E-mail address: leo.goldmakher@utoronto.ca