A radical excursion: from irrational roots to Prüfer domains and back

Ben Griffith[*] Greg Oman[†]

August 13, 2016

Abstract

We begin with a review of some standard facts on the irrationality of certain roots of positive integers. We then give a gentle and self-contained introduction to Prüfer domains. Finally, we interpret the notion of irrationality in this more general algebraic environment and show how to translate the standard facts on irrationality to this setting.

1 Introduction

The irrationality of $\sqrt{2}$ is a staple of classical mathematics. Indeed, it was known to the Pythagoreans thousands of years ago. Even today, one would be hard-pressed to find an undergraduate 'Discrete Structures' or 'Transition to Advanced Mathematics' course which does not delight (torture?) students with a demonstration of this fact. Aside from the standard textbook arguments, there are a staggering number of published proofs in the literature, some of which are relatively recent. Indeed, they range from analytic to number-theoretic to order-theoretic to geometric. We refer the reader to Bloom [3], Ferreno [4], Gauntt [7], Kalman [11], and Miller [12] for a sampling of some nifty arguments.

More generally, one learns (possibly in an undergraduate course on elementary number theory) that if k is a positive integer which is not a perfect square, then $\sqrt{k}$ is irrational (see Flanders [5], Ungar [14], and Waterhouse [15] for a variety of proofs of this assertion). Even more generally, if k is positive integer which is not an nth power ($n \geq 1$ an integer), then $\sqrt[n]{k}$ is irrational. The standard proof of this fact uses unique factorization properties of the integers. However, several authors have presented alternative proofs which are not number-theoretic in nature (see Beigel [2] and Schielack [13], for example). All of these facts follow immediately from the so-called Integral Root Theorem which states that if a rational number r is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$,[1] then $r \in \mathbb{Z}$. A quick proof of the irrationality of $\sqrt[n]{k}$, k not

[*] University of Colorado, Colorado Springs (undergraduate)

[†] University of Colorado, Colorado Springs

[1] $\mathbb{Z}[X]$ denote the ring of polynomials with coefficients in $\mathbb{Z}$.

an nth power, proceeds as follows. Note first that $\sqrt[n]{k}$ is a root of the monic polynomial $X^n - k \in \mathbb{Z}[X]$. If $\sqrt[n]{k}$ were rational, then $\sqrt[n]{k} \in \mathbb{Z}$ by the Integral Root Theorem. This contradicts our assumption that k is not an nth power. The standard proof of the Integral Root Theorem again uses unique factorization properties of the integers, and again, there exist slick alternative arguments (see Gilat [8], for instance).

The purpose of this note is to investigate the Integral Root Theorem and irrationality in a more general algebraic environment. In particular, we study these concepts relative to *Prüfer domains* (we relegate the definition to the next section), the class of which properly includes the class of principal ideal domains along with many domains which do not possess nice factorization properties (this will be made more explicit shortly).

2 Main Results

We begin by recalling a definition which will play a fundamental role throughout this note.

Definition 1 *Let D be a commutative integral domain (that is, a commutative ring with identity without zero divisors). Let K be the set of all formal symbols $\frac{x}{y}$ where $x, y \in D$ and $y \neq 0$. Define $\frac{x_1}{y_1} = \frac{x_2}{y_2}$ if and only if $x_1y_2 = x_2y_1$.*[2] *Further, we define the following addition and multiplication on K:*

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} := \frac{x_1y_2 + x_2y_1}{y_1y_2}, \textit{ and} \tag{1}$$

$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} := \frac{x_1x_2}{y_1y_2}. \tag{2}$$

Then K is a field, called the fraction field (or quotient field or field of fractions) of D.

It is routine to verify that the above operations yield a field structure on K. The additive identity of K is $\frac{0}{1}$, the multiplicative identity is $\frac{1}{1}$, and the multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$ for $a \neq 0$ (these assertions are all trivial to check). Moreover,

$$\text{the map } d \mapsto \frac{d}{1} \text{ is a ring isomorphism of } D \text{ into } K. \tag{3}$$

We identify D and its image in K (and hence view D as a subring of K). The impetus for this construction is to obtain a field K which is, in some sense, smallest with respect to containing D. In fact, K is characterized up to isomorphism by the following so-called universal property: if F is any field containing D and $f\colon D \to F$ is an injective ring homomorphism, then f may be

[2] More formally, the relation $\sim$ defined by $\frac{x_1}{y_1} \sim \frac{x_2}{y_2}$ iff $x_1y_2 = x_2y_1$ is an equivalence relation on K.

uniquely extended to a homomorphism of K into F. The reader may not find surprising the fact that the fraction field of $\mathbb{Z}$ is isomorphic to $\mathbb{Q}$; see Hungerford [10], pp. 142–144 for further details.

We now study a method of constructing rings which are "sandwiched" between a domain D and its quotient field K. This is done by means of a *multiplicatively closed set*, defined as follows.

Definition 2 *Let D be a domain and suppose $S \subseteq D$. Then S is multiplicatively closed provided $0 \notin S$, $1 \in S$, and for any $x, y \in S$, also $xy \in S$.*

We are now ready to present the construction. Let D be a domain with quotient field K and suppose $S \subseteq D$ is multiplicatively closed. Then one checks at once that $D_S := \{\frac{d}{s} \colon d \in D, s \in S\}$ is a subring of K which contains D. We call D_S the *quotient ring of D with respect to S*. We pause to illustrate this concept with several examples.

Example 1 *Let D be a domain, and let $S := \{1\}$. Then S is multiplicatively closed, and $D_S \cong D$.*

Example 2 *Suppose D is a domain, and set $S := D \backslash \{0\}$. Then (since D is a domain) S is multiplicatively closed, and $D_S \cong K$.*

Example 3 *$S = \{2^n \colon n \geq 0\}$ is a multiplicatively closed subset of the ring $\mathbb{Z}$ of integers, and $\mathbb{Z}_S$ is the ring of dyadic rational numbers.*

Example 4 *Let D be a domain and let P be a prime ideal of D. Then $S := D \backslash P$ is multiplicatively closed, and the ring D_S (commonly denoted by D_P) is called the localization of D with respect to P.*

We are almost ready to define Prüfer domains. First, we need one more definition.

Definition 3 ([10], p. 409) *Let D be an integral domain with quotient field K. Then D is a valuation domain if and only if for every nonzero $x \in K$, either $x \in D$ or $x^{-1} \in D$ (recall from (3) that we identify D with its canonical image in K).*

It is also possible to define valuation domains internally as follows: a domain D is a valuation domain if and only if for any $a, b \in D$: either $a|b$ or $b|a$ (here, $a|b$ means that there is $x \in D$ such that $ax = b$). To help the reader intuit this definition, we present two more examples.

Example 5 *Every field is a valuation domain.*

To see why this is true, suppose F is a field and let $a, b \in F$ be arbitrary. If $a = b = 0$, clearly $a|b$. Suppose now that $a \neq 0$. Then $a(a^{-1}b) = b$, and again $a|b$.

Example 6 *Let p be a prime number. Then the ring $\mathbb{Z}_{\langle p\rangle}$ is a valuation domain.*[3]

Proof: Consider arbitrary nonzero elements $x, y \in \mathbb{Z}_{\langle p\rangle}$ (in case $x = 0$ or $y = 0$, it is obvious that one divides the other). We may write $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where

$$p \text{ divides neither } b \text{ nor } d. \tag{4}$$

Write $a = p^{m_1}k_1$ and $c = p^{m_2}k_2$, where $m_1, m_2 \geq 0$ and k_1, k_2 are integers such that

$$p \text{ divides neither } k_1 \text{ nor } k_2. \tag{5}$$

We may assume without loss of generality that $m_1 \leq m_2$. Then

$$\frac{y}{x} = \frac{\frac{c}{d}}{\frac{a}{b}} = \frac{cb}{ad} = \frac{p^{m_2}k_2b}{p^{m_1}k_1d} = \frac{p^{m_2-m_1}k_2b}{k_1d} := z. \tag{6}$$

It follows from (4) and (5) that $z \in \mathbb{Z}_{\langle p\rangle}$. Therefore, $x|y$ in $\mathbb{Z}_{\langle p\rangle}$, and we have shown that $\mathbb{Z}_{\langle p\rangle}$ is a valuation domain. QED

Finally, we are ready to introduce Prüfer domains.

Definition 4 ([10], p. 409) *Let D be an integral domain. Then D is a Prüfer domain if and only if D_J is a valuation domain for every maximal ideal J of D.*[4]

The class of Prüfer domains is a vast and important class of domains which properly contains the class of principal ideal domains and, more generally, the class of Dedekind domains (domains for which every proper nonzero ideal is uniquely a finite product of prime ideals). Indeed, some 40 equivalent definitions of Prüfer domains appear in the literature. It is not our purpose to recount them here; we refer the reader instead to Fontana [6] and to Chapter 4 of Gilmer [9] for a sampling.

Now let D be a domain and let $a, b \in D\backslash\{0\}$. Then a *gcd* of a and b is an element $c \in D$ such that $c|a$, $c|b$, and whenever $x \in D$ divides both a and b, then $x|c$. Not every Prüfer domain has the property that any two nonzero elements of D have a GCD (that is, not every Prüfer domain is a *GCD domain*). A simple example is the following:

Example 7 $\mathbb{Z}[\sqrt{10}] := \{a + b\sqrt{10}\colon a, b \in \mathbb{Z}\}$ *is a Prüfer domain for which not every pair of nonzero elements has a gcd.*[5]

[3] Recall from Example 4 that $\mathbb{Z}_{\langle p\rangle} = \{\frac{a}{b}\colon a \in \mathbb{Z}, b \in \mathbb{Z}\backslash\langle p\rangle\}$.

[4] If J is a maximal ideal of a commutative ring R, then R/J is a field, hence also an integral domain. It follows that J is a prime ideal of R; hence D_J is well-defined.

[5] A self-contained verification of this fact would take us too far afield, but we sketch details for the interested reader. This domain $\mathbb{Z}[\sqrt{10}]$ is a classical example of a Dedekind domain which is not a principal ideal domain (p. 407 of [10]). As every Dedekind domain is Prüfer,

We pause to recall the Integral Root Theorem and sketch the standard proof.

Theorem 1 (Integral Root Theorem for $\mathbb{Z}$) *If $r \in \mathbb{Q}$ is a root of a monic polynomial $f(X) \in \mathbb{Z}[X]$, then $r \in \mathbb{Z}$.*

Proof: Let $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$, where each $a_i \in \mathbb{Z}$ and suppose that $f(r) = 0$. Without loss of generality, we may assume that

$$r = \frac{p}{q}, \text{ where } p \text{ and } q \text{ are relatively prime integers.} \tag{7}$$

Multiplying both sides of $f(r) = 0$ by q^n and rearranging algebra shows that

$$q|p^n; \text{ since } p \text{ and } q \text{ are relatively prime, } q|p. \tag{8}$$

But then $q = \pm 1$, and we see that $r \in \mathbb{Z}$. QED

Recall that the usual proofs of (7) and (8) above employ the fact that every pair of nonzero integers has a gcd. Because of Example 7, the above proof of the Integral Root Theorem for $\mathbb{Z}$ cannot be translated *mutatis mutandis* to Prüfer domains. Perhaps surprisingly, it is possible to prove the more general result for Prüfer domains in a way that avoids number theory.

We now work toward establishing the following theorem (cf. [9], Theorem 23.4):

Theorem 2 (Integral Root Theorem for Prüfer Domains) *Let D be a Prüfer domain with quotient field K. If $\alpha \in K$ is a root of a monic polynomial $f(X) \in D[X]$, then $\alpha \in D$.*

Translated to ideal-theoretic terms, Theorem 2 says that a Prüfer domain is *integrally closed.* To prove this theorem, we will need two lemmas. The lemmas are well-known, but we present short, self-contained proofs.

Lemma 1 ([9], Theorem 17.5) *Every valuation domain is integrally closed.*

Proof: Let V be a valuation domain with quotient field K. Suppose further that $x \in K$ and

$$v_0 + v_1x + v_2x^2 + \cdots + v_{n-1}x^{n-1} + x^n = 0 \tag{9}$$

for some $v_0, v_1, \ldots, v_{n-1} \in V$. We will show that $x \in V$. Clearly we may assume that $x \neq 0$ and thus $n > 1$. Since V is a valuation domain, it follows by definition that either $x \in V$ or $\frac{1}{x} \in V$. If $x \in V$, we have what we need. Thus suppose that $\frac{1}{x} \in V$. Multiplying both sides of (9) by $\frac{1}{x^{n-1}}$, we get

$\mathbb{Z}[\sqrt{10}]$ is Prüfer. It is known (see p. 85 of Ali [1], for example) that a Prüfer domain is a GCD domain if and only if it is a *Bezout domain*, that is, every finitely generated ideal is principal. Now, if $\mathbb{Z}[\sqrt{10}]$ were a GCD domain, then $\mathbb{Z}[\sqrt{10}]$ would be a Bezout domain. However, since $\mathbb{Z}[\sqrt{10}]$ is Noetherian, this would imply that $\mathbb{Z}[\sqrt{10}]$ is a principal ideal domain, a contradiction.

$$\frac{v_0}{x^{n-1}} + \frac{v_1}{x^{n-2}} + \cdots + v_{n-1} + x = 0. \tag{10}$$

Recall that $\frac{1}{x} \in V$. As V is a ring and $v_0, \ldots, v_{n-1} \in V$, also $\frac{v_0}{x^{n-1}}, \frac{v_1}{x^{n-2}}, \ldots, v_{n-1}$ belong to V. Solving (10) for x, we see that $x \in V$. QED

The proof of our next lemma requires the following definition.

Definition 5 *Let I and J be ideals of a commutative ring R. Then the ideal quotient of I by J, denoted $[I\colon J]$, is defined by $[I\colon J] := \{r \in R\colon rJ \subseteq I\}$ (that is, $r \in [I\colon J]$ if and only if $rj \in I$ for every $j \in J$).*

One checks easily that for any ideals I and J of a commutative ring R, $[I\colon J]$ is an ideal of R. We now show that the intersection of all localizations of a domain D at its maximal ideals is equal to D.

Lemma 2 ([9], Theorem 4.10) *Let D be a domain, and let $\{J_i\colon i \in I\}$ be the collection of maximal ideals of D. Then $D = \bigcap_{i\in I} D_{J_i}$.*

Proof: For any $d \in D$ and $i \in I$, we have $d = \frac{d}{1} \in D_{J_i}$ (as J_i is by definition a proper ideal of D, $1 \notin J_i$). Therefore, $D \subseteq \bigcap_{i\in I} D_{J_i}$. For the other containment, let

$$\frac{a}{b} \in \bigcap_{i\in I} D_{J_i}. \tag{11}$$

We will show that $\frac{a}{b} \in D$. First we claim that the ideal quotient $[\langle b\rangle\colon \langle a\rangle] = D$ (here $\langle b\rangle$ and $\langle a\rangle$ are the principal ideals generated by b and a, respectively). Suppose by way of contradiction that $[\langle b\rangle\colon \langle a\rangle] \neq D$. Then $[\langle b\rangle\colon \langle a\rangle]$ is a proper ideal of D, whence $[\langle b\rangle\colon \langle a\rangle] \subseteq J_k$ for some $k \in I$. By (11), $\frac{a}{b} \in D_{J_k}$. Thus $\frac{a}{b} = \frac{d}{s}$ for some $d \in D$ and $s \in D\backslash J_k$, and we deduce that $sa = bd$. But then by definition, $s \in [\langle b\rangle\colon \langle a\rangle]$. Recall that $[\langle b\rangle\colon \langle a\rangle] \subseteq J_k$, and therefore $s \in J_k$, a contradiction. We conclude that $[\langle b\rangle\colon \langle a\rangle] = D$ after all, and hence $1 \in [\langle b\rangle\colon \langle a\rangle]$. But this implies that $1 \cdot a = a \in \langle b\rangle$; therefore there exists $c \in D$ such that $a = cb$. We conclude that $\frac{a}{b} = c \in D$, as required. QED

Finally, we are equipped to prove Theorem 2, which asserts that all Prüfer domains are integrally closed.

Proof: Let D be a Prüfer domain with quotient field K, and suppose that $\alpha \in K$ is a root of some monic polynomial $f(X) \in D[X]$. We will show that $\alpha \in D$. Toward this end, let J be an arbitrary maximal ideal of D. Then note that as $D \subseteq D_J \subseteq K$, K is also the quotient field of D_J. Further (since $D \subseteq D_J$), $f(X) \in D_J[X]$. Since D_J is a valuation domain, it follows from Lemma 1 that D_J is integrally closed. Thus $\alpha \in D_J$. As J was an arbitrary maximal ideal of D, we conclude from Lemma 2 that $\alpha \in D$. QED

Now that we have Theorem 2 under our belt, we return to our discussion of irrationality. Recall the following well-known number-theoretic fact mentioned in the Introduction:

Fact 1 *If k and n are positive integers and k is not an nth power, then $\sqrt[n]{k}$ is irrational.*

We conclude the paper by generalizing this result to Prüfer domains. This generalization is of interest because its proof (via the proof of the Integral Root Theorem for Prüfer domains) does not invoke the gcd, nor any order-theoretic, analytic, combinatorial, or geometric methods. Informally, the following theorem says that if d is an element of a Prüfer domain D which is not an nth power in D, then any nth root of d is "irrational." [6]

Theorem 3 *Let D be a Prüfer domain with quotient field K. Further, let $d \in D$ and let n be a positive integer. If d is not an nth power in D, then there does not exist $\alpha \in K$ such that $\alpha^n = d$.*

Proof: We assume that D is a Prüfer domain with quotient field K, $d \in D$, and that d is not an nth power in D. Suppose by way of contradiction that there exists $\alpha \in K$ such that $\alpha^n = d$. Then α is a root of the monic polynomial $f(X) := X^n - d \in D[X]$. Since D is integrally closed, $\alpha \in D$. But then d is an nth power in D, a contradiction. QED

References

[1] Ali M. and Smith D., *Generalized GCD rings II,* Beitrage Algebra Geom., Vol. 44, No. 1, pp 75-98, 2003.

[2] Beigel R., *Irrationality without number theory,* Amer. Math. Monthly, Vol. 98, No. 4, pp 332-335, 1991.

[3] Bloom D., *A one-sentence proof that $\sqrt{2}$ is irrational,* Math. Mag., Vol. 68, No. 4, p 286, 1995.

[4] Ferreno N., *Yet another proof of the irrationality of $\sqrt{2}$,* Amer. Math. Monthly, Vol. 116, No. 1, pp 68-69, 2009.

[5] Flanders H., *Irrationality of $\sqrt{m}$,* Math. Mag., Vol. 72, No. 3, p 235, 1999.

[6] Fontana M., Huckaba J., and Papick I., "Prüfer Domains", Marcel Dekker, Inc., 1997.

[7] Gauntt R., *The irrationality of $\sqrt{2}$,* Amer. Math. Monthly, Vol. 63, No. 4, p 247, 1956.

[8] Gilat D., *Gauss's Lemma and the irrationality of roots, revisited,* Math. Mag., Vol. 85, No. 2, pp 114-116, 2012.

[9] Gilmer R., "Multiplicative Ideal Theory", Queen's Papers in Pure and Applied Mathematics, 1992.

[6] Note that an nth root of d exists in an algebraic closure of the quotient field K of D.

[10] Hungerford T., “Algebra”, Springer-Verlag, 1980.

[11] Kalman D., Mena R., and Shahriari S., *Variations on an irrational theme – geometry, dynamics, algebra,* Math. Mag., Vol. 70, No. 2, pp 93-104, 1997.

[12] Miller S., and Montague D., *Picturing irrationality,* Math. Mag., Vol. 85, No. 2, pp 100-114, 2012.

[13] Schielack V., *A quick counting proof of the irrationality of* $\sqrt[n]{k}$*,* Math. Mag., Vol. 68, No. 5, p 386, 1995.

[14] Ungar P., *Irrationality of square roots,* Math. Mag., Vol. 79, No. 2, pp 147-148, 2006.

[15] Waterhouse W., *The teaching of mathematics: Why square roots are irrational,* Amer. Math. Monthly, Vol. 93, No. 3, pp 213-214, 1986.

About the authors:

Ben Griffith is a junior at UCCS majoring in mathematics. His senior year will be spent at Stony Brook, where he will take some courses not offered at UCCS in preparation for graduate school. Ultimately, he plans to pursue a Ph.D. in an area of pure mathematics.

Greg Oman is an assistant professor at UCCS. He works in a number of areas including group theory, ring theory, semigroup theory, topology, and logic. One of the most fulfilling aspects of his job is engaging bright students in research projects. It truly was a pleasure working with Ben on this paper.

Ben Griffith

University of Colorado, Colorado Springs
1420 Austin Bluffs Parkway
Colorado Springs, CO 80918
bpgriffith@icloud.com

Greg Oman

University of Colorado, Colorado Springs
1420 Austin Bluffs Parkway
Colorado Springs, CO 80918
goman@uccs.edu