RINGS OF INTEGERS ARE DEDEKIND DOMAINS: A SHORT AND SIMPLE PROOF

TIMOTHY ALL, CONNOR LANE, AND PAUL POLLACK

ABSTRACT. Let K be a field containing $\mathbb{Q}$ for which $[K:\mathbb{Q}] < \infty$, and let $\mathcal{O}_K$ denote the set of elements of K that are roots of monic polynomials with integer coefficients. We give a streamlined proof — suitable for presentation to undergraduates — that $\mathcal{O}_K$ is a **Dedekind domain**: Noetherian, integrally closed, and such that all of its nonzero prime ideals are maximal. Our chief innovation is a short and seemingly novel argument demonstrating that $\mathcal{O}_K/I$ is finite for every nonzero ideal $I \subseteq \mathcal{O}_K$.

1. INTRODUCTION

Let K be a **number field**, meaning a field containing $\mathbb{Q}$ for which the degree $[K:\mathbb{Q}]$ is finite. In supplements to Dirichlet's *Vorlesungen über Zahlentheorie*, published in 1871, Dedekind associates to K a so-called "ring of integers" and proves that the nonzero ideals of this ring obey a variant of the unique factorization theorem. These results are now part of the standard mathematical canon; every graduate student interested in number theory is fated to encounter them.

Let us spell matters out more precisely. In what follows, rings are always commutative with multiplicative identity 1, and a subring is understood to share the same 1 as the ambient ring. If R is a subring of S, an element $\alpha \in S$ is said to be **integral over** R if α is the root of a monic polynomial in $R[x]$. For each number field K, we let

$$\mathcal{O}_K := \{\alpha \in K : \alpha \text{ is integral over } \mathbb{Z}\}.$$

Dedekind shows $\mathcal{O}_K$ is a ring: this is what was referred to above as **the ring of integers** of K. If I and J are ideals of $\mathcal{O}_K$, define their product IJ as the smallest ideal of $\mathcal{O}_K$ containing all pairwise products $\alpha\beta$, where $\alpha \in I$ and $\beta \in J$. Dedekind's factorization theorem — sometimes called the **Fundamental Theorem of Ideal Theory** — asserts that every nonzero, proper ideal of $\mathcal{O}_K$ admits a unique representation as $P_1 \cdots P_k$, where the P_i are prime ideals of $\mathcal{O}_K$ and uniqueness is up to the order of the factors P_i. (We remind the reader that an ideal P of a ring R is a **prime** ideal of R if $P \neq R$ and R/P is an integral domain.)

In 1927, Noether investigated abstract conditions on a ring that are equivalent to the conclusion of the Fundamental Theorem [4]. The following definition of a **Dedekind domain** is a modern simplification of the axiom scheme Noether proposed.[1]

2020 *Mathematics Subject Classification.* Primary 11R04; Secondary 13F05.

Key words and phrases. algebraic integer, Dedekind domain, number field, ring of integers.

[1] Noether had five axioms. Her Axiom III asserts that R has a multiplicative identity (*not* part of her definition of a ring) while Axiom IV is the nonexistence of zero divisors in R. Conditions (i) and (ii) appear

Definition 1. An integral domain R is a **Dedekind domain** if

(i) R is **Noetherian**: there is no infinite strictly ascending chain of ideals of R

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots,$$

(ii) R is **integrally closed** meaning that every α belonging to the fraction field of R that is integral over R in fact belongs to R, *and*

(iii) every nonzero prime ideal of R is maximal.

These axioms completely characterize domains that obey the Fundamental Theorem. If R is a Dedekind domain, then every nonzero, proper ideal of R factors uniquely as a product of prime ideals. Conversely, any domain R in which the latter holds is necessarily a Dedekind domain (see, e.g., [2, Theorem 10.6]).

Today, the usual path to Dedekind's Fundamental Theorem is to (a) first prove that $\mathcal{O}_K$ is a Dedekind domain, (b) prove that all Dedekind domains enjoy unique factorization of ideals. (Sometimes (a) and (b) are reversed.) This note provides another exposition of (a).

Theorem 1. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Why bother? One can read perfectly good proofs of Theorem 1 elsewhere, for instance in the superb textbooks of Marcus [3] and Samuel [5]. Our motivation is primarily pedagogical; we would like to make the important Theorem 1 accessible to students (and nonspecialists) who may only have seen (or may only remember!) basics of field theory, group theory, linear algebra, etc. Notably, we require from linear algebra only the most basic properties of dimension, avoiding any use of determinants. We are also able to dispense with any mention of norm, trace, or discriminant. Perhaps the deepest theorem we use is that a submodule of a finitely generated $\mathbb{Z}$-module is finitely generated, whose (standard) proof is included below (Lemma 3) for completeness.

The rest of this note is structured as follows. In §2, we prove that $\mathcal{O}_K$ is a domain and verify that $\mathcal{O}_K$ is integrally closed. Here we eschew the traditional use of determinants following the elegant treatment of Swinnerton-Dyer in [6]. In §3, we prove that $\mathcal{O}_K$ is **residually finite**: For every nonzero ideal I of $\mathcal{O}_K$, the quotient $\mathcal{O}_K/I$ is finite. The usual proofs of this fact require one to first establish that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of finite rank. Our method of avoiding this (via Proposition 6 below) is the chief innovation of the note. That $\mathcal{O}_K$ is Noetherian with every nonzero prime ideal maximal follows immediately from residual finiteness, by (entirely standard) arguments which we recount in §4.

2. Why is $\mathcal{O}_K$ a ring? And why is it integrally closed?

For the remainder of the paper, K denotes a number field. Below, **finitely generated** always means finitely generated as a $\mathbb{Z}$-module (abelian group). That is, M is finitely generated if there are finitely many elements $m_1, \dots, m_r \in M$ with $M = \mathbb{Z}m_1 + \dots + \mathbb{Z}m_r$.

as Axioms I and V. The following Axiom II takes the place of our (iii): For each nonzero ideal I of R, the ring R/I has no infinite descending chain of ideals. See Cohen's paper [1] for a discussion of this last condition. Incidentally, [1] may be the earliest English-language occurrence of the term "Dedekind domain."

Proposition 2. *Let α be an element of K.*

(i) *If $\mathbb{Z}[\alpha]$ is finitely generated, then $\alpha \in \mathcal{O}_K$.*

(ii) *Let R be a subring of K which is finitely generated. If α is integral over R (in particular, if $\alpha \in \mathcal{O}_K$), then $R[\alpha]$ is finitely generated.*

Proof. We start with (i). If $\mathbb{Z}[\alpha]$ is finitely generated, then there are $f_1(x), \dots, f_k(x) \in \mathbb{Z}[x]$ for which $\mathbb{Z}[\alpha] = \mathbb{Z}f_1(\alpha) + \cdots + \mathbb{Z}f_k(\alpha)$. Choose an integer n exceeding the degree of every $f_i(x)$, and write

$$\alpha^n = c_1 f_1(\alpha) + \cdots + c_k f_k(\alpha),$$

with $c_1, \dots, c_k \in \mathbb{Z}$. Then α is a root of the monic polynomial

$$x^n - (c_1 f_1(x) + \cdots + c_k f_k(x)) \in \mathbb{Z}[x],$$

so that $\alpha \in \mathcal{O}_K$.

Turning to (ii), suppose α is a root of $x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 \in R[x]$. Then

$$\alpha^n = -(r_{n-1}\alpha^{n-1} + \cdots + r_1\alpha + r_0) \in \sum_{i=0}^{n-1} R\alpha^i, \quad \text{so that} \quad R\alpha^n \subseteq \sum_{i=0}^{n-1} R\alpha^i. \tag{1}$$

We prove, by induction, that $\alpha^m \in \sum_{i=0}^{n-1} R\alpha^i$ for each nonnegative integer m. Indeed, this containment certainly holds when $m = 0$. Assuming it holds for m, we have that

$$\alpha^{m+1} = \alpha^m \cdot \alpha \in \sum_{i=1}^{n} R\alpha^i = \sum_{i=1}^{n-1} R\alpha^i + R\alpha^n \subseteq \sum_{i=0}^{n-1} R\alpha^i,$$

using (1) in the last step. Since elements of $R[\alpha]$ are finite R-linear combinations of the α^m, we deduce that $R[\alpha] = \sum_{i=0}^{n-1} R\alpha^i$.

To finish off, recall that R itself is finitely generated. Thus, there are $\beta_1, \dots, \beta_\ell \in R$ with $R = \sum_{j=1}^{\ell} \mathbb{Z}\beta_j$. It follows that

$$R[\alpha] = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{\ell} \mathbb{Z}\beta_j \right) \alpha^i = \sum_{\substack{0 \le i \le n-1 \\ 1 \le j \le \ell}} \mathbb{Z}\beta_j\alpha^i,$$

so that $R[\alpha]$ is generated by the $\beta_j\alpha^i$ (for $i = 0, \dots, n-1$ and $j = 1, \dots, \ell$). □

Lemma 3. *If the $\mathbb{Z}$-module M is finitely generated, then every submodule of M is also finitely generated.*

Proof. We show what at first glance seems a very special case:

Every submodule of $\mathbb{Z}^r$ is finitely generated (for each $r \in \mathbb{Z}_{>0}$).

As it turns out, this special case suffices for the whole kit and caboodle. Indeed, suppose M is a finitely generated $\mathbb{Z}$-module, with generators $m_1, \dots, m_r$. Let $\phi \colon \mathbb{Z}^r \to M$ be the homomorphism sending $(n_1, \dots, n_r)$ to $n_1 m_1 + \cdots + n_r m_r$. If $N \subseteq M$ is a submodule of M, then $\phi^{-1}(N)$ is a submodule of $\mathbb{Z}^r$. Furthermore, if the finitely many elements $v_1, \dots, v_k$ generate $\phi^{-1}(N)$, then $\phi(v_1), \dots, \phi(v_k)$ generate N.

We proceed by induction on r. A $\mathbb{Z}$-submodule of $\mathbb{Z}$ is an ideal of $\mathbb{Z}$ and so always admits a single generator ($\mathbb{Z}$ is a Principal Ideal Domain). This handles the case $r = 1$.

Assume all submodules of $\mathbb{Z}^r$ are finitely generated, and let N be a submodule of $\mathbb{Z}^{r+1}$. Let $\pi\colon \mathbb{Z}^{r+1} \to \mathbb{Z}$ be "projection to the first coordinate", so that $\pi(n_1, \dots, n_{r+1}) = n_1$. Let

$$N' = \{n \in N : \pi(n) = 0\}.$$

Identifying $\{v \in \mathbb{Z}^{r+1} : \pi(v) = 0\}$ with $\mathbb{Z}^r$, we may view N' as a submodule of $\mathbb{Z}^r$. By our induction hypothesis, N' admits finitely many generators, say $d_2, \dots, d_s \in N'$. Continuing, let $d \in \mathbb{Z}$ be a generator of the ideal $\{\pi(n) : n \in N\} \subseteq \mathbb{Z}$, and choose $d_1 \in N$ with $\pi(d_1) = d$.

We claim that $d_1, \dots, d_s$ generate N. Indeed, start with any $n \in N$. By the choice of d, we have $\pi(n) = k_1 d$ for some $k_1 \in \mathbb{Z}$. But then $n - k_1 d_1 \in N'$, and so $n - k_1 d_1 = k_2 d_2 + \dots + k_s d_s$ for some integers $k_2, \dots, k_s$. Hence, $n = k_1 d_1 + \dots + k_s d_s \in \mathbb{Z}d_1 + \dots + \mathbb{Z}d_s$. □

Theorem 4. *$\mathcal{O}_K$ is a domain. Moreover, $\mathcal{O}_K$ is integrally closed.*

Proof. Clearly, $\mathbb{Z} \subseteq \mathcal{O}_K$, since $a \in \mathbb{Z}$ is a root of $x - a$. In particular, $1 \in \mathcal{O}_K$. Now suppose $\alpha, \beta \in \mathcal{O}_K$. By Proposition 2(ii) and the fact that $\mathbb{Z}$ itself is finitely generated we have that $\mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha][\beta]$ is finitely generated. Thus, its submodule $\mathbb{Z}[\alpha + \beta]$ is also finitely generated (Lemma 3). That $\alpha + \beta \in \mathcal{O}_K$ now follows from Proposition 2(i). Similarly, $\alpha\beta \in \mathcal{O}_K$. Thus, $\mathcal{O}_K$ is a subring of K. As K is a field, $\mathcal{O}_K$ is an integral domain.

Now we show that $\mathcal{O}_K$ is integrally closed. It suffices to show that if $\alpha \in K$ is integral over $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.[2] Suppose α is a root of $x^n + \beta_{n-1}x^{n-1} + \dots + \beta_1 x + \beta_0$, where each $\beta_i \in \mathcal{O}_K$, and let $R = \mathbb{Z}[\beta_0, \dots, \beta_{n-1}]$. By Proposition 2(ii), we have first that R is finitely generated and then, by a second application of the same Proposition, that $R[\alpha]$ is finitely generated. Hence, $\mathbb{Z}[\alpha] \subseteq R[\alpha]$ is also finitely generated, and $\alpha \in \mathcal{O}_K$. □

3. Interlude: $\mathcal{O}_K$ has finite quotients

Theorem 5. *If I is a nonzero ideal of $\mathcal{O}_K$, then $\#\mathcal{O}_K/I < \infty$.*

We can reduce the proof of Theorem 5 to the case when $I = n\mathcal{O}_K$ for some $n \in \mathbb{Z}_{>0}$. Indeed, let I be any nonzero ideal of $\mathcal{O}_K$, and let α be a nonzero element of I. Since $\alpha \in \mathcal{O}_K$, there is a relation

$$\alpha^m + a_{m-1}\alpha^{m-1} + \dots + a_1\alpha + a_0 = 0,$$

where $a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}$. If we suppose m is chosen as small as possible, then necessarily $a_0 \neq 0$ (otherwise we could divide through by α). Then

$$a_0 = \alpha(-a_1 - a_2\alpha - \dots - a_{m-1}\alpha^{m-2} - \alpha^{m-1}) \in \alpha\mathcal{O}_K \subseteq I.$$

We take $n = \pm a_0$, with the sign chosen so that $n > 0$. Then $n \in \mathbb{Z}_{>0}$, $n\mathcal{O}_K \subseteq I$, and there is a canonical surjection $\mathcal{O}_K/n\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/I$. In particular, if $\mathcal{O}_K/n\mathcal{O}_K$ is finite, so is $\mathcal{O}_K/I$.

[2] It is not so hard to prove that K is the fraction field of $\mathcal{O}_K$, but we do not use this here.

Let d denote the degree of K over $\mathbb{Q}$. Then $K \cong \mathbb{Q}^d$ as $\mathbb{Q}$-vector spaces, and hence also as abelian groups. This allows us to identify $\mathcal{O}_K$ with a subgroup of $\mathbb{Q}^d$. So in view of the previous paragraph, Theorem 5 is an immediate consequence of the following Proposition.

Proposition 6. *Let d be a positive integer, and let H be a subgroup of $\mathbb{Q}^d$. Then H/nH is finite for every positive integer n.*

Proof. Let us first see why $\#H/pH < \infty$ for a prime p. Since H is a $\mathbb{Z}$-module, H/pH is a module over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, i.e., an $\mathbb{F}_p$-vector space. We will prove that $\dim_{\mathbb{F}_p} H/pH \le d$, so that $\#H/pH \le p^d$. If $\dim_{\mathbb{F}_p} H/pH > d$, then there are $d+1$ $\mathbb{F}_p$-linearly independent elements of H/pH. Lift them to $d+1$ elements of H, say $h_1, \dots, h_{d+1}$. Since $H \subseteq \mathbb{Q}^d$ while $\dim_{\mathbb{Q}} \mathbb{Q}^d = d$, there is a $\mathbb{Q}$-dependence among $h_1, \dots, h_{d+1}$. Write

$$c_1 h_1 + \cdots + c_{d+1} h_{d+1} = 0, \tag{2}$$

where each $c_i \in \mathbb{Q}$ and not all $c_i = 0$. Clearing denominators, we may assume each $c_i \in \mathbb{Z}$. Dividing through by $\gcd(c_1, \dots, c_{d+1})$, we may also assume not all of the c_i are multiples of p. But then reducing the relation (2) modulo pH yields an $\mathbb{F}_p$-dependence among our original $d+1$ elements of H/pH.

Now, suppose n is a positive integer for which we know that H/nH is finite, say $\#H/nH = r$. Let $a_1, a_2, \dots, a_r \in H$ such that

$$H = \bigcup_{1 \le i \le r} (a_i + nH).$$

From what we've already proven, nH/pnH is also finite, say $\#nH/pnH = s$. Let $b_1, b_2, \dots, b_s \in nH$ such that

$$nH = \bigcup_{1 \le k \le s} (b_k + pnH).$$

It follows that

$$H = \bigcup_{\substack{1 \le i \le r \\ 1 \le k \le s}} (a_i + b_k + pnH).$$

So H/pnH is also finite.

The proposition now follows by induction on the number of prime divisors of n. □

4. Completion of the Proof of Theorem

Proposition 7. *Let K be a number field. Then $\mathcal{O}_K$ is Noetherian, and each of its nonzero prime ideals is maximal.*

Proof. The ring $\mathcal{O}_K$ is integrally closed by Theorem 4. Suppose for a contradiction that $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ is an infinite, strictly ascending chain of ideals. We can assume $I_1 \ne 0$: Otherwise, delete I_1 and renumber. Then $I_1/I_1 \subsetneq I_2/I_1 \subsetneq I_3/I_1 \subsetneq \dots$ is an infinite, strictly ascending chain of ideals in the ring $\mathcal{O}_K/I_1$. By Theorem 5, $\mathcal{O}_K/I_1$ is finite. But this is absurd: a finite ring has finitely many ideals! Thus, $\mathcal{O}_K$ is Noetherian.

Next, let P be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/P$ is a finite (again, by Theorem 5) integral domain, hence a field. Thus, P is maximal. □

Acknowledgments. The authors of this note were among the instructors of a dorm course on algebraic number theory offered to junior counselors (JCs) at the 2025 Ross Indiana Mathematics Camp. They thank these students for their enthusiastic participation.

References

[1] I. S. Cohen, *Commutative rings with restricted minimum condition*, Duke Math. J. **17** (1950), 27–42.

[2] N. Jacobson, *Basic algebra. II*, second ed., W. H. Freeman and Company, New York, 1989.

[3] D. A. Marcus, *Number fields*, second ed., Universitext, Springer, Cham, 2018.

[4] E. Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. **96** (1927), 26–61.

[5] P. Samuel, *Algebraic theory of numbers*, Houghton Mifflin Co., Boston, MA, 1970.

[6] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001.

Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, IN 47803

Email address: timothy.all@rose-hulman.edu

Department of Mathematics, University of California, Santa Barbara, Isla Vista, CA 93117

Email address: connorlane@ucsb.edu

Department of Mathematics, University of Georgia, Athens, GA 30602

Email address: pollack@uga.edu