

THE HALF-FACTORIAL PROPERTY IN INTEGRAL EXTENSIONS

Jim Coykendall

Department of Mathematics

North Dakota State University

Fargo, ND. 58105-5075

ABSTRACT. In this paper, the integral closure of a half-factorial subring of a ring of algebraic integers is studied. The *boundary map*, a natural generalization of the length function of Zaks, is used to show that the integral closure of such an order is again an HFD.

1. INTRODUCTION

We recall that a *half-factorial domain* (HFD) R is an atomic domain such that given any two irreducible factorizations in R :

$$\alpha_1 \dots \alpha_n = \beta_1 \dots \beta_m$$

then $n = m$.

Half-factorial domains (a concept introduced in [10], but first studied in [4]) are generalizations of unique factorization domains (UFD's) that have been studied extensively in [1]-[7], [10], and [11]. In particular, it is shown in [4] that if R is the ring of algebraic integers of an algebraic number field, then R is an HFD if and only if the class number of R does not exceed 2.

As a generalization of UFD's, one wishes to discover which "nice" properties of UFD's hold for HFD's. For example, if R is a UFD, then so is its polynomial ring $R[x]$. This does not hold in general for HFD's. In particular, it was shown in [6] that for $R[x]$ to be an HFD, R must be an integrally closed HFD (in the Noetherian case, $R[x]$ is an HFD if and only if R is a Krull domain with class number less than or equal to 2). For example, $\mathbf{Z}[\sqrt{-3}][x]$ is an example of a non-HFD polynomial ring with an HFD coefficient ring.

Of course, any UFD is integrally closed, and the question as to whether the integral closure of an HFD is an HFD has been posed. In this paper, we study this question for the specific case of an *order* in a ring of algebraic integers. Since there appears to be some conflicting definitions of order in the literature, we say here that an order, R , is a subring of a ring of algebraic integers, \overline{R} , such that the quotient fields of R and

\overline{R} coincide.

For the sake of compactness of language, we will say that all rings in this paper are atomic (even ones that appear as overrings). Additionally, our notational convention will be that if R is a ring, S will denote an (atomic) overring of R and, the symbol \overline{R} will denote the integral closure of R .

2. THE BOUNDARY MAP

In this section we introduce a tool that we call the *boundary map*. The boundary map is a natural generalization of the length function defined in [11]. In [11], Zaks defined the length function from the semigroup of nonzero nonunits of a domain to the nonnegative integers by associating with each nonzero nonunit the number of irreducible factors that appear in a given factorization. Zaks showed that HFD's are precisely the class of rings which admit a well-defined length function. Here we shall refine this tool slightly and produce the boundary map, a function that will prove useful in this paper.

We begin with a preliminary lemma.

LEMMA 2.1 If S is integral over R and $\alpha \in S$ then there exists an $r \in R$ such that $r\alpha^n \in R$ for all $n > 0$.

Proof: It is well-known that an element that is integral is contained in the complete integral closure of R .

◇

DEFINITION 2.2 Let R be an HFD with quotient field K . If $R \neq K$, we define the *boundary map* $\partial_R: K \setminus 0 \rightarrow \mathbf{Z}$ by $\partial_R(\alpha) = t - k$ where $\alpha = \frac{\pi_1 \cdots \pi_t}{\xi_1 \cdots \xi_k}$ where π_i, ξ_i are irreducible elements of R for all i . If $R = K$, then we say $\partial_R(\alpha) = 0$ for all $\alpha \in R$.

We remark here that ∂_R is a well-defined homomorphism into the rational integers (and is surjective if R is not a field). What is more, ∂_R restricted to the nonzero nonunits of R is precisely the length function described by Zaks [11]. In other words this restriction of ∂_R "counts" the number of irreducible factors that appear in a given factorization of an element of R , a well-defined quantity if R is an HFD.

We now record a couple of lemmas that highlight some useful properties of the boundary map.

LEMMA 2.3 Let R be an HFD. If $\alpha \in K$ is almost integral over R , then $\partial_R(\alpha) \geq 0$.

Proof: Since α is almost integral over R , there is an element $x \in R$ such that $x\alpha^n \in R$ for all $n \geq 0$. Therefore, we have that

$$\partial_{\mathbf{R}}(x\alpha^n) = \partial_{\mathbf{R}}(x) + n\partial_{\mathbf{R}}(\alpha) \geq 0.$$

Since the inequality above holds for all nonnegative integers n , we have that $\partial_{\mathbf{R}}(\alpha) \geq 0$. \diamond

LEMMA 2.4 If \mathbf{R} is an HFD such that $\partial_{\mathbf{R}}(\alpha)=1$ for all irreducible $\alpha \in \mathbf{S}$, then \mathbf{S} is atomic implies that \mathbf{S} is an HFD.

Proof: Clearly the result holds if \mathbf{S} is a field, so we will ignore this possibility. Assume that we factor an element in \mathbf{S} into irreducible elements in the following two ways:

$$\alpha_1 \dots \alpha_t = \beta_1 \dots \beta_m.$$

As the boundary map is a well-defined homomorphism, we obtain that

$$\sum_{i=1}^t \partial_{\mathbf{R}}(\alpha_i) = \sum_{i=1}^m \partial_{\mathbf{R}}(\beta_i).$$

But by assumption, the boundary map is identically 1 on all irreducibles. Therefore, $t = m$, and \mathbf{S} is an HFD. \diamond

We remark here that the existence of irreducibles in \mathbf{S} of boundary 0 presents a certain problem which will soon become obvious. Many types of HFD's (e.g., HFD's which are orders in Galois rings of integers fixed by the Galois action) admit no irreducibles of boundary 0 in integral overrings. In general, rings of integers in (possibly Galois) number fields may or may not admit boundary 0 irreducibles, but in the next section we construct a proof that sidesteps this possible problem.

THEOREM 2.5 Let \mathbf{R} be an HFD and let \mathbf{S} be an (atomic) overring such that no nonunit of \mathbf{S} has boundary 0. Then \mathbf{S} is an HFD if and only if $\partial_{\mathbf{R}}(\alpha)=1$ for all irreducible elements $\alpha \in \mathbf{S}$.

Proof: We note first that if \mathbf{R} or \mathbf{S} is a field then the result holds trivially, so we will assume that this is not the case. Observe that for all $\alpha \in \mathbf{S}$, $\partial_{\mathbf{R}}(\alpha) \geq 0$, for if there is an element $\alpha \in \mathbf{S}$ with negative boundary (say n) then αr^{-n} (where $r \in \mathbf{R}$ is irreducible and a nonunit in \mathbf{S}) is a nonunit of \mathbf{S} with boundary 0, contradicting our assumption. Assume that $\partial_{\mathbf{R}}(\alpha) = k > 1$ (with α irreducible in \mathbf{S}). Pick $\beta \in \mathbf{S}$ such that $\alpha\beta \in \mathbf{R}$, and we denote the boundary of β by $m \geq 0$.

As $\alpha\beta \in R$ and $\partial_R(\alpha\beta) = k + m$, we have that any factorization of $\alpha\beta$ has precisely $k + m$ irreducible factors in R :

$$\alpha\beta = x_1 \dots x_k y_1 \dots y_m.$$

We note at this point that none of the x_i 's or y_j 's are units in S . If this were the case (say, without loss of generality, that x_1 is a unit in S), then the element αx_1^{-k} would be a nonunit of S with boundary 0.

As $\partial_R(\beta) = m$ and there is no irreducible element of S of boundary 0, we conclude that any irreducible factorization of β has at most m irreducible factors in S . Therefore since α is irreducible in S , $\alpha\beta$ has an irreducible factorization with at most $1 + m$ irreducible factors in S . But as we can factor $\alpha\beta$ as above, we see that $\alpha\beta$ has an irreducible factorization with at least $k + m > 1 + m$ irreducible factors. Therefore S is not an HFD.

The proof of the other direction is almost identical to the proof of Lemma 2.4. \diamond

COROLLARY 2.6 If R is an HFD, and S is an overring of R containing no nonunit of boundary 0, then every irreducible of R either remains irreducible or becomes a unit in S .

Proof: If r is an irreducible in R that has two nonunit factors $r=st$ in S , then $\partial_R(r)=\partial_R(s)+\partial_R(t)\geq 2$, which is a contradiction. \diamond

3. APPLICATION TO THE NUMBER FIELDS CASE

In this section, we apply the machinery of the previous section to the case of an order (a subring of the ring of integers $R \subseteq \bar{R}$ such that R and \bar{R} share the same quotient field) in an algebraic number field. In this case, the boundary map is well-behaved on almost every element of the quotient field (where “almost every” means all elements that are not contained in a certain finite collection of prime ideals). Consequently, we shall see that for this special case, the integral closure of an HFD is an HFD. In fact, we obtain the somewhat surprising (but known) result that if the field is Galois of odd degree, then the integral closure of an HFD must be a UFD.

We begin this section by stating the main theorem; the rest of this section is devoted to its proof.

THEOREM 3.1 Let F/\mathbf{Q} be an algebraic number field with ring of integers \bar{R} . If $R \subseteq \bar{R}$ is an order with

the HFD property, then \overline{R} is an HFD, and if F is Galois of odd degree, then \overline{R} is a UFD.

Before we can prove this theorem, we must develop a couple of tools to help us. We will denote the conductor ideal of R (and \overline{R}) by I , and we will show that for any element $x \in \overline{R}$ that is not contained in any prime containing I , there is an $n > 0$ such that $x^n \in R$. We begin with a couple of preliminary lemmas.

LEMMA 3.2 Let $x \in \overline{R}$ be such that x is not contained in any prime ideal of \overline{R} that contains the conductor I . Then there is an $n > 0$ such that $x^n \in R$.

Proof: Consider the ring \overline{R}/I . Since x is not in any prime containing the conductor ideal I , the coset $x+I$ is a unit in \overline{R}/I , and as \overline{R}/I is a finite ring, the coset is of finite order. Hence there is an $n > 0$ such that $x^n+I=1+I$, so $x^n \in R$. \diamond

LEMMA 3.3 Let \mathcal{P} be a nonzero prime ideal of \overline{R} of order d that does not contain the conductor ideal I . Then \mathcal{P}^d can be generated by an irreducible element of R .

Proof: As the order of \mathcal{P} in the class group is d , we note that $\mathcal{P}^d = \overline{R}x$, where x is an (irreducible) element of \overline{R} . It is easy to see that x is not in any prime ideal containing the conductor ideal I , so there is a $k > 0$ such that $x^k \in R$ by Lemma 3.2. We now choose $n \geq 1$ minimal so that $\overline{R}x^n$ is generated by an element of R , and we let c be this generator. So we have $\overline{R}x^n = \overline{R}c$. It remains to show that c is an irreducible element of R , and, in fact, generates $\overline{R}x$.

Let b be a nonunit divisor of c . As b divides x^n , we see that \mathcal{P} is the only prime ideal of \overline{R} containing b . Therefore, $\overline{R}b = \mathcal{P}^{dm} = \overline{R}x^m$. So by the minimality of n , $m = n$. This gives that $b = uc$ with u a unit of \overline{R} .

We now observe that as $vc = x^n$ with v a unit in \overline{R} , then

$$\partial_R(vc) = \partial_R(x^n) = n\partial_R(x) = 1$$

which shows that $n = 1$. Therefore $\overline{R}x = \overline{R}c$, which completes the proof. \diamond

With these two lemmas in hand, we can now complete the proof that the integral closure of an HFD is an HFD in this case.

LEMMA 3.4 Let R, \bar{R} be as above. Then R is an HFD implies that \bar{R} is an HFD.

Proof: We assume \bar{R} is not an HFD and derive contradictions utilizing the HFD characterization and technique due to Carlitz ([4]). First we shall assume that there is a prime \mathcal{P} in an ideal class of \bar{R} of order $m > 2$. We also assume that \mathcal{P} is different from all the primes containing the conductor. The fact that this can be accomplished follows from the fact that every ideal class contains an infinite number of primes (it is interesting to note that we need to utilize a slightly stronger distributional characteristic of rings of algebraic integers than the existence of a prime ideal in every class used by Carlitz in [4]). We now choose another prime \mathcal{Q} in the class of \mathcal{P}^{-1} also distinct from the set of primes containing the conductor. By Lemma 3.3 we have that

$$\mathcal{P}^m = \bar{R}a; \mathcal{Q}^m = \bar{R}b; \mathcal{P}\mathcal{Q} = \bar{R}c$$

where a, b are irreducible elements of R and c is (irreducible) in \bar{R} .

The above ideal factorizations give the following elemental factorization:

$$c^m = uab$$

where u is a unit of \bar{R} .

Applying the boundary, we obtain:

$$m\partial_R(c) = \partial_R(a) + \partial_R(b) = 2.$$

Which implies that $m \leq 2$ which is a contradiction.

We have now reduced the problem to the case where the class group of \bar{R} is 2-elementary abelian of order at least 4. In this case $\text{Cl}(\bar{R})$ contains a subgroup isomorphic to the Klein 4-group (and we denote the elements of this subgroup as the ordered pairs $(0,0), (1,0), (0,1), (1,1)$ with each entry from \mathbf{Z}_2).

As before we choose primes $\mathcal{P}, \mathcal{Q}, \mathcal{R}$ that do not contain the conductor and in the classes $(1,0), (0,1)$, and $(1,1)$ respectively. Lemma 3.3 again gives us the following factorizations:

$$\mathcal{P}^2 = \bar{R}a, \mathcal{Q}^2 = \bar{R}b, \mathcal{R}^2 = \bar{R}c, \mathcal{P}\mathcal{Q}\mathcal{R} = \bar{R}\alpha$$

where a, b, c are irreducibles of R , and α is (irreducible) in \bar{R} .

This, in turn, gives the elemental factorization:

$$\alpha^2 = abc$$

where u is a unit of \bar{R} .

Once again we apply the boundary and obtain:

$$2\partial_R(\alpha) = \partial_R(a) + \partial_R(b) + \partial_R(c) = 3$$

and this gives the desired contradiction, since $\partial_R(\alpha)$ must be an integer. This establishes the first statement in Theorem 3.1. \diamond

It remains to show the second statement of Theorem 3.1. Lemma 3.5 (below) will complete this proof. For the sake of completeness, we will prove Lemma 3.5, but the interested reader is referred to [8], where more general results were obtained.

LEMMA 3.5 Let F/\mathbf{Q} be a Galois extension of odd degree with ring of integers \bar{R} . Then \bar{R} is an HFD implies that \bar{R} is a UFD.

Proof: Assume that G , the Galois group of F/\mathbf{Q} has order $2k + 1$ where k is an integer. We also assume that \bar{R} is a nontrivial HFD, that is, the class number of \bar{R} is 2. Let \mathcal{P} be a nontrivial prime ideal of \bar{R} . Note that the norm of \mathcal{P} is $N(\mathcal{P}) = \prod_{\sigma \in G} \sigma(\mathcal{P})$. Since there is only one nontrivial ideal class (of order 2) and $\sigma(\mathcal{P})$ must be nontrivial for each $\sigma \in G$, the class of $N(\mathcal{P})$ is the same as the class of \mathcal{P}^{2k+1} , which is, in turn, the same class as \mathcal{P} . But as $N(\mathcal{P})$ must be principal, we have the desired contradiction. \diamond

As a concluding remark, we state that in the case of fields of even degree it is indeed possible to have the integral closure of an HFD be a (non-UFD) HFD. A concrete example of this is the order of index 7 in the ring of integers $R = \mathbf{Z}[\sqrt{10}]$. It is well-known that the class number of R is 2 (that is, R is a non-UFD HFD) and the fact that the order of index 7 is an HFD is an easy computation that follows from [7].

ACKNOWLEDGEMENT

The author would like to extend his heartiest thanks to the referee of this paper for making some key suggestions that greatly increased the scope of the results.

REFERENCES

1. D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorization in integral domains*, J. Pure Appl. Algebra **69** (1990), 1-19.
2. D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorization in integral doamins II*, J. Algebra **152** (1992), 78-93.
3. D. F. Anderson, S. Chapman, and W. Smith, *Overrings of half-factorial domains*, Canad. Math. Bull. **37** (1994), 437-442.
4. L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391-392.
5. S. Chapman and W. Smith, *On the k -HFD property in Dedekind domains with small class group*, Mathematika **39** (1992), 330-340.
6. J. Coykendall, *A characterization of polynomial rings with the half-factorial property*, *Factorization in Integral Domains*, Lecture Notes in Pure and Appl. Math., **189**, Dekker, New York, 1997.
7. J. Coykendall, *Half-factorial domains in quadratic fields*, preprint.
8. K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J. **27** (1966), 239-247.
9. W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," Springer-Verlag/Polish Scientific Publishers, 1990.
10. A. Zaks, *Half factorial domains*, Bull. Amer. Math. Soc. **82** (1976), 721-723.
11. A. Zaks, *Half factorial domains*, Israel J. Math. **37** (1980), 281-302.