HALF-FACTORIAL DOMAINS IN QUADRATIC FIELDS

Jim Coykendall

Department of Mathematics

North Dakota State University

Fargo, ND 58105-5075

Abstract: In this paper, we give a norm-theoretic proof of the characterization of HFDs that appear as orders in quadratic fields. The original characterization of orders that are HFDs in quadratic fields is due to F. Halter-Koch ([10]). Our approach will pay special attention to the normset of such HFDs, and we will give a characterization that relates to the generalized class number of such an order. Additionally, it will be shown that such HFDs are characterized by the factorization properties of their normsets.

1. INTRODUCTION

The terminology half-factorial domain (HFD) was introduced by Zaks in [11] and [12] as a generalization of unique factorization domain (UFD). Of course, Carlitz [1] noticed the importance of the concept for rings of algebraic integers twenty years earlier. We recall that a half-factorial domain is an atomic integral domain R where given any two factorizations of an element a∈R

$$a=\pi_1\pi_2...\pi_n = \xi_1\xi_2...\xi_m$$

with each π_i and ξ_j irreducible, $n = m$. We do not say that irreducible factors necessarily pair up modulo unit factors and ordering (which is, of course, what is required of a UFD).

For rings of algebraic integers there is an elegant and succinct characterization of HFD. Carlitz showed in [1] that a ring of algebraic integers is an HFD if and only if its class number is less than or equal to two. This partitions rings of integers neatly into two classes; namely, class number one means UFD, and class

number two means non-UFD half-factorial domain.

Since its inception, the concept of half-factorial domain has been explored by many authors in a number of different settings (for example, see [2], [3], and [9]), but, for the most part, the context of the investigations has been in an integrally closed setting. One important exception to this is the characterization of HFDs that appear as orders in quadratic fields given in ([10]) by F. Halter-Koch. This characterization is stated in the following beautiful theorem.

THEOREM 1.1.(Halter-Koch) Let R be an order in a quadratic field with integral closure $\overline{R}$. Additionally, let $U(\overline{R})$ denote the unit group of $\overline{R}$ and $n \neq 1$ be the conductor. Then the following are equivalent:

1. R is an HFD.

2. $\overline{R}$ is an HFD, $\overline{R} = RU(\overline{R})$ and n is either a prime or twice an odd prime.

The purpose of this paper is to investigate HFDs from a norm-theoretic point of view. The rings that we consider are the (not necessarily integrally closed) orders in quadratic number fields. We apply some of the techniques developed in [6], [7] and [8] to shed some light on the problem at hand. It should be noted at this point that some of the material found in sections 2 and 3 may be found directly or indirectly in [10]. Any reproduced theorems are couched in a norm-theoretic standpoint as to cast light on the implications of this theory to the generalized class number and the theory of normsets.

2. THE IMAGINARY QUADRATIC CASE

In this section we show that the example given by Zaks ([11]) is the unique, nontrivial imaginary quadratic order. The techniques that we shall employ here depend upon the fact that the integral bases (and hence the norm polynomials) of these rings are well-known. We will begin with these basic, but necessary,

facts that apply to a general quadratic order.

THEOREM 2.1. Let R be an order in the quadratic field $\mathbf{Q}(\sqrt{d})$ of index n in the ring of integers $\overline{\mathrm{R}}$. Then R is of the form:

1. $\mathbf{Z}+\mathbf{Z}[n\sqrt{d}]$ if $d \equiv 2,3 \bmod (4)$
2. $\mathbf{Z}+\mathbf{Z}[\frac{n(1+\sqrt{d})}{2}]$ if $d \equiv 1 \bmod (4)$.

For a proof of this see [4] or [5], for example. $\diamondsuit$

THEOREM 2.2. Let R be an order in a quadratic field $\mathbf{Q}(\sqrt{d})$ of index n. The set of ideals relatively prime to n has unique factorization, and if we restrict to such ideals we obtain an analog to the class group. What is more, the class number of this order is given by:

$$h_n(d) = \frac{nh(d)}{u} \prod_{p|n} (1 - \frac{(d/p)}{p})$$

where $h(d)$ is the class number of the integral closure of R, (d/p) is Kronecker's generalization of the Legendre symbol, and u is the smallest power of the generator of the unit group that is in R.

For a proof of this see [5]. $\diamondsuit$

We now introduce the main theorem of this section in which we see that the non-integrally closed, quadratic HFD produced by Zaks in [11] is the only imaginary example. The proof completely depends on representations in the normset, but the careful reader will notice that, implicit in the proof, is the unit structure of the orders.

THEOREM 2.3. The ring $\mathbf{Z}[\sqrt{-3}]$ is the unique, non-integrally closed imaginary quadratic HFD.

Proof: We shall defer to [11] the fact that $\mathbf{Z}[\sqrt{-3}]$ is an HFD, but, in fact, we shall produce a result later that easily implies this.

In this proof, we will let d <0 and consider two cases. The first case will be when $d \equiv$2,3 mod (4), and the second case will be when $d \equiv$1 mod (4).

In the first case, we have that an order R has the form $\mathbf{Z}+n\mathbf{Z}[\sqrt{d}]$, where n is the index. The norm form associated with this ring is

$$\mathrm{f(x,y)=x^2\text{-}}dn^2\mathrm{y}^2.$$

Let p be a prime dividing n, say n=kp and consider the element $n\sqrt{d}$. The norm of this element is $\text{-}d\mathrm{k}^2\mathrm{p}^2$. We also claim that this element is irreducible. To see this, note that the norm of any proper divisor of this is less than $\text{-}dn^2$, and so the form of the norm tells us that $n\sqrt{d}$ must be divisible by a rational integer, but clearly it is not. So we have the factorization in R given by:

$$(n\sqrt{d})(-n\sqrt{d})=\mathrm{(p)(p)(k)(k)}(d).$$

In particular, since the left hand side is an irreducible factorization, we have that R is not an HFD unless (maybe) k=1 and d=-1. So in this case, the only possible orders are the ones of prime index in the Gaussian integers. So we will now examine this possibility in depth.

Let R be of index p in $\mathbf{Z}$[i]. So R is of the form $\mathbf{Z}$+pi$\mathbf{Z}$. We note that in R, the element p+pi is irreducible; indeed, any proper divisor must have norm 2, p, 2p, or p^2, and checking all of the possibilities shows that p+pi is irreducible. The norm of p+pi is $2\mathrm{p}^2$, so we have the following factorizations in R:

$$\mathrm{(p+pi)(p\text{-}pi)=(2)(p)(p)}$$

and so again, R is not an HFD.

In the second case, we will assume that $d < 0$ and $d \equiv$1 mod (4). In this case, R takes the form $\mathbf{Z}+n\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ with n being the index. In this case, we shall write the norm form g(x,y) in two equivalent ways:

$$\mathrm{g(x,y)=x^2}+n\mathrm{xy}+n^2\mathrm{y}^2\tfrac{(1-d)}{4}=(\mathrm{x}+\tfrac{n}{2}\mathrm{y})^2\text{-}\tfrac{dn^2}{4}\mathrm{y}^2.$$

Letting x=0 and y=1 in the above equations, we obtain an element of norm $(\frac{1-d}{4})n^2$. This element is irreducible. To see this, we note that any proper divisor of this element has a norm necessarily dividing $(\frac{1-d}{4})n^2$. Therefore, we conclude that |y| cannot be greater than or equal to 2. If y=$\pm$1, then the norm of the element is given by

$$\mathrm{x}^2\pm n\mathrm{x}+\tfrac{1-d}{4}n^2$$

and for this norm to divide $\frac{1-d}{4}n^2$, we necessarily must have

$$x^2 \pm nx \leq \frac{d-1}{8}n^2.$$

Some elementary calculus shows, however, that this implies that $d \geq$-1 which is a contradiction. Therefore, y=0, and the divisor of the element $n(\frac{1+\sqrt{d}}{2})$ must be a rational integer, which is a contradiction.

We now conclude that we have the following factorizations in R:

$$(n(\tfrac{1+\sqrt{d}}{2}))(n(\tfrac{1-\sqrt{d}}{2})) = (\tfrac{1-d}{4})(n)(n).$$

Since the left hand side of the above equation is an irreducible factorization, we have contradicted HFD unless d=-3 and n is prime. Therefore, the only possible non-integrally closed HFDs are the ones of prime index in $\overline{R}=\mathbf{Z}[\omega]$ where $\omega = \frac{1+\sqrt{-3}}{2}$ is the primitive complex sixth root of unity. Assume that the index of R in $\overline{R}$ is a prime p>2. Consider the element $p+p\omega \in R$. The norm of this element is $3p^2$, and the general norm polynomial is $h(x,y)=x^2+pxy+p^2y^2$. So we see that this element is reducible only if there is an element of norm 3 or p, but it is easy to check that none of the six elements of norm 3 in $\overline{R}$ are in R, and the form of the norm implies that there is no element in R of norm p. Therefore, we have the following factorizations in R:

$$(p+p\omega)(p+p\overline{\omega})=(3)(p)(p)$$

where $\overline{\omega}$ is the conjugate of ω.

As before, the left hand side of the above is an irreducible factorization, and so R is not an HFD. The only remaining case is that of index 2, and that case has been shown to be an HFD in [11]. $\diamondsuit$

3. THE GENERAL QUADRATIC CASE

We shall now supply necessary and sufficient conditions for an order in a general quadratic field to be an HFD. Here $\overline{R}$ will be the ring of integers in the field $\mathbf{Q}(\sqrt{d})$, and R an order of index n in $\overline{R}$. We remark here that Theorem 3.1 implies that if R is an HFD in $\overline{R}$, then R and $\overline{R}$ have the same normset (modulo units)(see [6]).

THEOREM 3.1. R is an HFD if and only if $\overline{\mathrm{R}}$ is an HFD and every irreducible of R is also irreducible in $\overline{\mathrm{R}}$.

Proof. ($\Longleftarrow$) Assume that $\overline{\mathrm{R}}$ is an HFD, and that every irreducible of R remains irreducible in $\overline{\mathrm{R}}$. Let a$\in$R and consider the following factorizations in R:

$$\mathrm{a}=\pi_1...\pi_k = \xi_1...\xi_m$$

by assumption, these factorizations are irreducible factorizations in $\overline{\mathrm{R}}$, and since $\overline{\mathrm{R}}$ is an HFD, $k = m$. Therefore, we conclude that R is an HFD.

For the other implication, we will show that $\overline{\mathrm{R}}$ is not an HFD implies that R is not an HFD, then we will show that the existence of an irreducible element of R that is not irreducible in $\overline{\mathrm{R}}$ implies that R is not an HFD. We begin the proof with a couple of general facts pertaining to the normsets of quadratic orders.

THEOREM 3.2. Non-HFD quadratic rings of algebraic integers are characterized by the property that there exist three distinct primes p, q, and r $\in\mathbf{Z}$ such that pqr is irreducible in the normset (in particular, the primes p, q, and r are irreducible in the ring).

Proof. Clearly, in the above situation, the element, α, of norm pqr is irreducible, and we have the following irreducible factorizations in $\overline{\mathrm{R}}$:

$$\alpha\overline{\alpha}=\mathrm{pqr}$$

On the other hand, if $\overline{\mathrm{R}}$ is not an HFD, then there are two cases to consider. First we will assume that there is an ideal class ([I]) in Cl($\overline{\mathrm{R}}$) of order $n > 2$. In this case, we pick three split primes $\mathcal{P}$, $\mathcal{Q}$, and $\mathcal{R}$ with relatively prime norm (say p,q, and r) in the classes [I], [I], and $[\mathrm{I}]^{-2}$ (note that by assumption none of these classes is trivial). By construction, $\mathcal{PQR}$ is a principal ideal of norm pqr and it is easy to see that pqr is an irreducible element of the normset.

The other case to consider is the case when every element of Cl($\overline{\mathrm{R}}$) is an involution. As $\overline{\mathrm{R}}$ is not an HFD, this implies that Cl($\overline{\mathrm{R}}$) contains a subgroup isomorphic to $\mathbf{Z}_2\oplus\mathbf{Z}_2$. In this case, we pick $\mathcal{P}, \mathcal{Q}$, and $\mathcal{R}$

in the ideal classes corresponding to the elements (0,1), (1,0), and (1,1) of $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. By the same argument as above we have pqr is irreducible in the normset. This establishes the theorem. $\diamondsuit$

LEMMA 3.3. Let R be an order of index n in the quadratic ring of integers $\overline{\mathrm{R}}$. Any element of R (in particular, any irreducible) dividing n is of the form uk with k$\in\mathbf{Z}$ and u$\in$U($\overline{\mathrm{R}}$)(the unit group of $\overline{\mathrm{R}}$).

Proof. We first remark that any element, say α, that divides n has a norm which is a square (up to a sign) in $\mathbf{Z}$. To see this, we assume that the norm of α is of the form $\mathrm{p}^{2m+1}\mathrm{b}$ with p a prime and b some number relatively prime to p. If α=x+y$n\sqrt{d}$ then we have the following equation:

$$\mathrm{x}^2\text{-}dn^2\mathrm{y}^2=\mathrm{p}^{2m+1}\mathrm{b}$$

Since α divides n, its norm must divide n^2. So we see that p^{2m+1} must divide n^2, and therefore also x^2. As x^2 and n^2 are squares, they must also be divisible by p^{2m+2}, and we have that b is divisible by p, a contradiction.

The case where $d \equiv 1 \bmod (4)$ is a bit more complicated. Under the same assumptions as above we have that

$$\mathrm{x}^2+n\mathrm{xy}\text{-}n^2\mathrm{y}^2\tfrac{1-d}{4}=\mathrm{p}^{2m+1}\mathrm{b}.$$

As before, p^{2m+2} divides n^2, so we have that p^{m+1} divides n and that p^{2m+1} divides x(x+ny). If $\mathrm{p}^k||$x with $k \leq m$ then we have that $\mathrm{p}^{2k}||$x(x+ny) which is a contradiction. Therefore, x must have at least $m+1$ factors of p, which also leads to a contradiction. This establishes the first remark.

When $d \equiv 2,3 \bmod (4)$, we have that α=x+y$n\sqrt{d}$ divides n. By the above remark, the norm of α is $\pm\mathrm{k}^2$ with k$\in\mathbf{Z}$. Consider the norm equation:

$$\mathrm{x}^2\text{-}dn^2\mathrm{y}^2=\pm\mathrm{k}^2.$$

As k^2 divides n^2, k^2 must divide x^2, and hence k divides x. If we say that ka=x and kb=n, we can rewrite α as k(a+yb$\sqrt{d}$), and it is easy to see that a+yb$\sqrt{d}$ is an element of norm ($\pm$)1.

In the case that $d \equiv 1 \bmod (4)$, we have an element α dividing n, hence its norm k^2 must divide n^2. We assume first that k=p^m is a prime power. We assume that $\mathrm{p}^r||$x with $r < m$. As p^{2m} divides x(x+ny), n must have no more than r factors of p, which is a contradiction. The general case follows by induction. $\diamondsuit$

With the above tools in hand, we return to the proof of the main theorem of this section.

Proof of($\Longrightarrow$). Assume first that $\overline{\mathrm{R}}$ is not an HFD. Theorem 3.2 shows that there must exist an element of norm pqr with p,q, and r primes of $\mathbf{Z}$ that are irreducible in $\overline{\mathrm{R}}$. For the first case, we will assume that $d \equiv$2,3 mod (4), and so this element has the form x+y$\sqrt{d}$, and the equation for its norm is given by:

$$\mathrm{x}^2\text{-}d\mathrm{y}^2=\mathrm{pqr}.$$

Multiplying the above by n^2 we get the following equation in R:

$$(n\mathrm{x})^2\text{-}dn^2\mathrm{y}^2=\mathrm{pqr}n^2.$$

The right-hand side of this equation is an irreducible factorization of length 3 plus twice the number of factors of n. The left-hand side, on the other hand, can be factored into an even number of irreducibles, since it is a norm. This establishes that R is an HFD implies that $\overline{\mathrm{R}}$ is an HFD if $d \equiv$2,3 mod (4) and the case where $d \equiv$1 mod (4) is similar.

Now we wish to show that if there is an irreducible of R that does not remain irreducible in $\overline{\mathrm{R}}$ then R is not an HFD. So we will assume that $\pi \in$R is an irreducible such that $\pi = \alpha\beta$ in $\overline{\mathrm{R}}$. We note that

$$\mathrm{N}(\pi)=\pi\overline{\pi} = (\alpha\overline{\alpha})(\beta\overline{\beta})$$

so, in particular, if N(π) has more than two prime factors, then we are done. So it suffices to assume that N(α)=p and N(β)=q are primes in $\mathbf{Z}$ (or, equivalently, α and β are prime elements of $\overline{\mathrm{R}}$). This also demonstrates (by Lemma 3.3) that p and q are prime to n.

We can also assume that no uα or uβ is in R with u$\in$U($\overline{\mathrm{R}}$), for if this were the case, then the factorization

$$\pm\pi\overline{\pi} = (\mathrm{u}\alpha)(\overline{\mathrm{u}\alpha})(\beta\overline{\beta})$$

shows that R is not an HFD.

With the above assumptions in hand, we choose elements x,y$\in$R such that the norm of x (respectively y) is of the form pk_1^2 with k_1 a minimal positive integer dividing n (respectively, the norm of y is of the form qk_2^2 with k_2 minimal with respect to dividing n). Elements of this form exist (e.g. $n\alpha$), and we claim that our chosen minimal elements are irreducible in R. To see this, note that if x factors nontrivially, then there must be a divisor of x whose norm is of the form pm with m a divisor of k_1^2 (and hence of n^2). An argument

similar to the proof of Lemma 3.3 shows that, in fact, m must be a square which contradicts minimality, hence x and y are irreducible in R.

The fact that α and β are prime in $\overline{\mathrm{R}}$ shows that x is of the form $\alpha_1\gamma_1$ where α_1 is either α or its conjugate. Similarly, we say that y=$\beta_2\gamma_2$. We also note that the norm of γ_1 (respectively γ_2) is k_1^2 (respectively k_2^2) and neither k_1 nor k_2 is equal to ± 1 as then we would have α or β being in R up to a unit.

We consider the factorizations:

$$(\pi)(\overline{\pi})(\gamma_1\overline{\gamma_1})(\gamma_2\overline{\gamma_2}) = (\alpha_1\gamma_1)(\overline{\alpha_1\gamma_1})(\beta_2\gamma_2)(\overline{\beta_2}\overline{\gamma_2}).$$

We notice that the right-hand side is an irreducible factorization in R. Since the products $\gamma_1\overline{\gamma_1}$ and $\gamma_2\overline{\gamma_2}$ are nontrivial squares in $\mathbf{Z}$, the left-hand side must yield more than 4 irreducibles factors. This concludes the proof. $\diamondsuit$

Now we would like to investigate some consequences of the theorems of this section. We now enumerate some necessary conditions for R to be an HFD.

COROLLARY 3.4. Let R be an order of index n in $\overline{\mathrm{R}}$ and let p be a prime dividing n. If (d/p)=1 (that is, if p splits in $\overline{\mathrm{R}}$) then R is not an HFD.

Proof. As p is a split prime, the case where $\overline{\mathrm{R}}$ is a UFD is straightforward. That is, p is reducible in $\overline{\mathrm{R}}$, but the form of the norm shows that p is irreducible in R, hence by Theorem 3.1, R is not an HFD.

For the case where $\overline{\mathrm{R}}$ is a non-UFD half-factorial domain, we note that if a prime lying over p is principal, then the proof proceeds as in the previous paragraph. If not, then as p is split there is an irreducible element, α, of norm pq in $\overline{\mathrm{R}}$, with q a prime that does not divide n. Consider the element $n\alpha \in$R. Since p divides n, it is easy to see that the norm of $n\alpha$ must have an odd number of factors of p, but the form of the norm implies that any norm in R divisible by p must have at least two factors of p. Hence there is an irreducible element $z \in$R such that N(z)=p^{2k+1}b where $k \geq 1$. To see that z is reducible in $\overline{\mathrm{R}}$, note that we have the factorization

$$z\overline{z}=\mathrm{p}^{2k+1}\mathrm{b}.$$

Since $\overline{\mathrm{R}}$ is an HFD and the right-hand side of the above equation has at least 3 factors, z cannot be irreducible in $\overline{\mathrm{R}}$.$\diamondsuit$

We omit the proof of the next corollary as it is quite similar to the proof of Corollary 3.4.

COROLLARY 3.5. Let R be an order of index n. If n is not relatively prime to the discriminant of $\mathbf{Q}[\sqrt{d}]$, then R is not an HFD.

COROLLARY 3.6. Let R be an order of index n in $\overline{\mathrm{R}}$ and let R_1 be of index kn in $\overline{\mathrm{R}}$. Then R_1 is an HFD implies that R is an HFD.

Proof. We first remark that R_1 is of index k in R. We factor k into integral primes $k = p_1p_2...p_t$ and note that each p_i, $1 \leq i \leq t$ is a prime element of $\overline{\mathrm{R}}$ by Corollaries 3.4 and 3.5. Let $x \in \mathrm{R}$ be an arbitrary irreducible element. By Theorem 3.1, it suffices to show that x is an irreducible element of $\overline{\mathrm{R}}$. Consider the element $xk = xp_1p_2...p_t \in \mathrm{R}_1$. We factor xk as follows:

$$xk = xp_1p_2...p_t = \alpha_1\alpha_2...\alpha_s$$

where each α_i, $1 \leq i \leq s$ is an irreducible element of R_1. But since R_1 is an HFD, each α_i is irreducible in $\overline{\mathrm{R}}$ as well. Additionally, since each p_j, $1 \leq j \leq t$ is prime in $\overline{\mathrm{R}}$, each α_i, $1 \leq i \leq t$ is equal to (without loss of generality) u_ip_i with u_i a unit in $\overline{\mathrm{R}}$. Hence $s \geq t$ and we obtain that $uk = \alpha_1\alpha_2...\alpha_t$, with u a unit in $\overline{\mathrm{R}}$. We now claim that in fact, u is a unit in R. To see this we write $u = v_1 + v_2\xi$ where ξ is either $\sqrt{d}$ or $\frac{1+\sqrt{d}}{2}$ depending on the reduction of d mod 4. Since $ku \in \mathrm{R}_1$, we have that kv_2 is a multiple of kn, hence v_2 is a multiple of n, so $u \in \mathrm{R}$.

Combining the above observations, we obtain that $x = u\alpha_{t+1}...\alpha_s$ with u a unit in R. Since x is assumed

irreducible in R, $s = t + 1$ and $x = u\alpha_s$. But α_s is irreducible in R_1, hence in $\overline{R}$, so x is irreducible in $\overline{R}$. This completes the proof. $\diamondsuit$

COROLLARY 3.7. If R is an HFD of index n in $\overline{R}$, then n is square-free.

Proof. By Corollary 3.6, it suffices to show that there are no HFDs of index p^2 where p is a prime. Consider the order R in $\overline{R}$ of index p^2 and consider the element $p^2(a+b\sqrt{d})$ in R with $a+b\sqrt{d}$ a unit in $\overline{R}$ such that (b,p)=1. This element is clearly reducible in $\overline{R}$; it suffices to show that it is irreducible in R. Lemma 3.3 shows that any factorization of $p^2(a+b\sqrt{d})$ must be of the form:

$$p^2(a+b\sqrt{d})=p(u_1+pu_2\sqrt{d})p(u_3+pu_4\sqrt{d}).$$

The p's adjacent to the u_i's are necessary to assure that p times the unit is in R. But we note that this factorization implies that p|b which contradicts our assumption. The case $d \equiv 1 \bmod (4)$ is similar.

To see that we need not worry about the case where p|b, note that for R to be an HFD, it is necessary that the index p order containing R must also be an HFD. If p divides b for all units in $\overline{R}$, however, then the u from Theorem 2.2 is 1, and we have that (unless maybe p=2) $h_p(d)>h(d)$. Therefore, it is easy to see that there must be principal ideals of $\overline{R}$ that are not principal in the index p order, and hence there are irreducibles of the index p order that are not irreducible in $\overline{R}$ (see the proof of Corollary 3.4 and [5, p. 114]). So, in this case, if $p\neq 2$, then the index p order (and hence R) is not an HFD. In the case where p=2, assume $h_2(d) = h(d)$. Applying Theorem 2.2, we see that $(d/2)$ must be 1, implying that d is equivalent to 1 mod 8, but this in turn implies that 2 splits, hence R cannot be an HFD. $\diamondsuit$

THEOREM 3.8. The only possible HFDs are those orders of index p or 2p in $\overline{R}$, an HFD, such that p is an inert prime in $\overline{R}$.

Proof. By the previous corollaries, it suffices to eliminate orders of index pq, where p and q are distinct odd primes. We also note that the proof for the case $d \equiv 1 \bmod (4)$ is almost identical to the case $d \equiv 2,3 \bmod (4)$ so we will only show the latter explicitly.

Consider the element pqξ, with ξ the fundamental unit of $\overline{\mathrm{R}}$. To prove the theorem, it suffices to show that this is irreducible in R. If it is not, then Lemma 3.3 shows that it must factor in the form

$$\mathrm{pq}\xi=(\mathrm{p}u_1)(\mathrm{q}u_2)=(\mathrm{p}(v_1+v_2\sqrt{d}))(\mathrm{q}(v_3+v_4\sqrt{d})).$$

For this to be a factorization in R, q must divide v_2 and p must divide v_4. But as ξ is the fundamental unit, $u_1=\pm\xi^s$ and $u_2=\pm\xi^t$. As the orders of index p and q must also be HFDs, this implies that p and q are inert primes in $\overline{\mathrm{R}}$ and that the generalized class number (from Theorem 2.2) of each order must equal the class number of $\overline{\mathrm{R}}$ (a necessary condition for irreducibles in an order to remain irreducible in $\overline{\mathrm{R}}$, as we have seen). Therefore, inspection of the formula in Theorem 2.2 shows that s must be a multiple of q+1 and t must be a multiple of p+1.

So we have the equation

$$\xi=\pm\xi^{(\mathrm{q}+1)m_1+(\mathrm{p}+1)m_2},$$

but the exponent on the right hand side is necessarily even. This gives a contradiction.$\diamondsuit$

Theorem 3.1 and its corollaries show that, in the real quadratic case, HFDs that are not integrally closed (say of some index $n>1$) must be chosen from a small subset of general quadratic orders. First of all, they must be subrings of rings of integers with the HFD property (namely, class number at most 2). Secondly, the index, n, must be of the form p or 2p with p a prime integer, with the further property that p is inert in $\overline{\mathrm{R}}$. Of course, not every index satisfying these strict conditions will be an HFD (which we shall soon see).

The obvious question that one would like to answer is, "Is there an infinite number of real quadratic HFDs?" If we restrict ourselves to the integrally closed case, then we have a question that is a generalization of Gauss' unproven conjecture of the existence of infinitely many real quadratic UFDs. So the problem of proving the existence of an infinite number of real HFDs (in the integrally closed case) is likely to be nearly as difficult as Gauss' conjecture. In the more general, non-integrally closed case the problem has also not been resolved, but in the next section we will construct examples which will give empirical evidence that there is, indeed, an infinite number of real HFDs.

4. SOME EXAMPLES AND A CONJECTURE

In this section, we will use some of the machinery developed in the previous sections to give concrete examples of real quadratic HFDs. We start out by noting that the comments at the end of Section 3 show that the only place to look for real quadratic HFDs are the orders of index p or 2p in quadratic rings of integers of class number 1 or 2. In fact, since it is not known whether or not there is an infinite number of real quadratic rings of integers of class number 1 or 2, one hope of showing the infinitude of real quadratic HFDs lies in showing that there is a specific ring of integers containing an infinite number of orders that are HFDs. In fact, we can take this one step further and notice that Theorem 3.8 of the previous section demonstrates that any hope lies in finding a specific ring of integers, $\overline{\mathrm{R}}$, that contains an infinite number of HFDs of index p or 2p in $\overline{\mathrm{R}}$.

For the sake of completeness, we start with an example that we will generalize later. This example is the first real, non-integrally closed HFD that we have given.

EXAMPLE 4.1. The ring R=$\mathbf{Z}[3\sqrt{2}]$ is a real, non-integrally closed quadratic HFD. To see that this is true, we appeal to Theorem 3.1 and the generalized class number formula given in Theorem 2.2. We see here that the class number of this ring is 1, so all primes (except 3) remain principal primes in R. We also note that the form of the norm implies that any element with norm equal to a power of 3 must be divisible by 3. This shows that the only irreducibles of R are of the form αu, with u a unit of $\mathbf{Z}[\sqrt{2}]$ and α a prime of $\mathbf{Z}[\sqrt{2}]$. By Theorem 3.1, we are done.

To take fullest advantage of the machinery that we have developed, we introduce the following theorem which ties together some earlier computational assertions.

THEOREM 4.2. Let $\overline{\mathrm{R}}$ be a real quadratic ring of integers of class number 1 or 2, and let R be an order of prime index p (with p inert). Then R is an HFD if and only if the generalized class number of R equals the class number of $\overline{\mathrm{R}}$.

Proof. ($\Longrightarrow$) If R is an HFD, then every irreducible of R must remain irreducible in $\overline{\mathrm{R}}$. As we have noticed, every (regular) principal ideal of $\overline{\mathrm{R}}$ must remain principal in R, and this is exactly the condition stated above (c.f. [5, p.114]).

($\Longleftarrow$) If the generalized class number of R is the same as the class number of $\overline{\mathrm{R}}$, then every principal ideal of $\overline{\mathrm{R}}$ relatively prime to p remains principal in R. Therefore, it suffices to show that the irreducibles of R that are not relatively prime to p remain irreducible in $\overline{\mathrm{R}}$. Note that as in the example above, any irreducible that is not prime to p must be divisible by p. This concludes the proof. $\diamondsuit$

EXAMPLE 4.3. We now revisit Example 4.1 with the previous theorem in mind. We would like to classify all possible prime indices p such that $\mathbf{Z}[\mathrm{p}\sqrt{2}]$ has generalized class number 1. Using the formula from Theorem 2.2, we see that a necessary and sufficient condition for $\mathbf{Z}[\mathrm{p}\sqrt{2}]$ to be an HFD is for p+1 to be the smallest power of the fundamental unit, $1+\sqrt{2}$, to be in $\mathbf{Z}[\mathrm{p}\sqrt{2}]$. Put in other terms, we need there to exist an infinite number of primes, p, such that $\sqrt{2} \notin \mathbf{Z}_{\mathrm{p}}$ and $1+\sqrt{2}$ is the generator of the multiplicative group $\mathbf{Z}_{\mathrm{p}}[\sqrt{2}]^*/\mathbf{Z}_p{}^*$. A simple computer program can be written to determine which small values of p work and which do not.

We found for p$\equiv$3 mod (8) that the first counterexample (index value of p that did not generate an HFD) was 59. For small p (say less than 1200) the majority of p's worked, but there were several counterexamples; namely, 59, 179, 227, 251, 379, 419, 443, 643, 683, 827, 1091, and 1187 are the only prime indices equivalent to 3 modulo 8 and less than 1200 that do not give HFDs.

The generalized class number approach to finding HFD orders in quadratic fields has some computational advantages. For example, the order of index 5 in the ring of integers $\mathbf{Z}[\sqrt{2}]$ has generalized class number equal to 2 (and the class number of $\mathbf{Z}[\sqrt{2}]$ has class number 1) so the index 5 order is not an HFD (this can also be seen via a direct computation by showing that $5\sqrt{2}$ is irreducible in the index 5 order, so the rational integer 50 has irreducible factorizations of different lengths). A similar computation shows that the order of index 4 in $\mathbf{Z}[\frac{1+\sqrt{21}}{2}]$ is not an HFD. This corrects a slight error in the tables from [10].

We conjecture that in the real quadratic case, there is an infinite number of HFDs. More specifically, we conjecture that there is an infinite number of non-integrally closed HFDs of prime index in the ring of integers $\mathbf{Z}[\sqrt{2}]$. This is equivalent to the assertion that there are infinitely many primes, p, such that the order of index p in $\mathbf{Z}[\sqrt{2}]$ has generalized class number 1.

We conclude with a theorem and a conjecture on a related topic, namely the integral closure of an HFD order. In [9] the author has shown that the integral closure of an HFD order is again an HFD. An alternative approach can be (possibly) formulated along the following lines.

THEOREM 4.4. Let R be an order inside the ring of algebraic integers $\overline{R}$ and assume that R has a prime ideal in each ideal class. If R is an HFD then $\overline{R}$ is an HFD.

Proof: We first claim that the order of the Picard group of R is less than or equal to 2. First we assume that there is a prime ideal, $\mathcal{P}$, in a class of Pic(R) of order $n > 2$. Pick a prime ideal $\mathcal{Q}$ in the class $\mathcal{P}^{-1}$. We consider the ideal factorizations:

$$\mathcal{P}^n\mathcal{Q}^n = (\mathcal{P}\mathcal{Q})^n$$

which translates to the elemental factorization:

$$\alpha\beta = \gamma^n$$

where α, β, and γ are (irreducible) elements generating $\mathcal{P}^n, \mathcal{Q}^n$, and $\mathcal{P}\mathcal{Q}$, respectively. The factorization above contradicts HFD.

In the second case we assume that Pic(R) contains a subgroup isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. In this case we choose prime ideals $\mathcal{P}, \mathcal{Q}$, and $\mathcal{R}$ in this classes (0,1), (1,0), and (1,1), respectively. We now consider the

ideal factorization

$$\mathcal{P}^2\mathcal{Q}^2\mathcal{R}^2 = (\mathcal{P}\mathcal{Q}\mathcal{R})^2.$$

In a similar fashion to the above, this gives the elemental factorization

$$\alpha\beta\gamma = \delta^2$$

where α, β, γ, and δ are (irreducible elements generating $\mathcal{P}^2, \mathcal{Q}^2, \mathcal{R}^2$, and $\mathcal{P}\mathcal{Q}\mathcal{R}$, respectively. Once again, we have a contradiction.

To complete the proof, we consider the following Cartesian diagram:

$$\begin{array}{ccc} \mathrm{R} & \xrightarrow{\mathrm{g_1}} & \overline{\mathrm{R}} \\ {\scriptstyle \mathrm{g_0}}\downarrow & & \downarrow{\scriptstyle \mathrm{f_1}} \\ \mathrm{R/I} & \xrightarrow{\mathrm{f_0}} & \overline{\mathrm{R}}\mathrm{/I} \end{array}$$

where I is the conductor ideal.

It is well-known that such a diagram gives rise to the exact sequence:

$$0 \longrightarrow \mathrm{U(R)} \longrightarrow \mathrm{U}(\overline{R}) \oplus \mathrm{U(R/I)} \longrightarrow \mathrm{U}(\overline{R}/\mathrm{I}) \longrightarrow \mathrm{Pic(R)} \longrightarrow \mathrm{Pic}(\overline{R}) \oplus \mathrm{Pic(R/I)} \longrightarrow \mathrm{Pic}(\overline{R}/\mathrm{I}).$$

As both R/I and $\overline{R}/I$ are semilocal, their Picard groups vanish, showing that the map

$$\mathrm{Pic}(R) \longrightarrow \mathrm{Pic}(\overline{R})$$

is surjective. Hence the order of the class group of $\overline{R}$ is less than or equal to 2, and $\overline{R}$ is an HFD.

This proof depends upon the assertion that the order R has a prime in every class, and we believe this to

be true in general. We would like to thank Professor David Anderson for pointing out this elegant approach, and note further that the techniques applies in a more general setting (e.g. subrings of Dedekind domains with "nice" prime distributions).

REFERENCES

1. L. Carlitz, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* **11** (1960), 391-392.
2. S. T. Chapman and W. W. Smith, Factorization in Dedekind domains with finite class group, *Israel J. Math.* **71** (1990), 65-95.
3. S. T. Chapman and W. W. Smith, On a characterization of algebraic number fields with class number less than three, *J. Algebra* **135** (1990), 381-387.
4. H. Cohn, "Advanced Number Theory," Dover Publications, New York, 1980.
5. H. Cohn, "Introduction to the Construction of Class Fields," Cambridge University Press, New York, 1985.
6. J. Coykendall, Normsets and determination of unique factorization in rings of algebraic integers, *Proc. Amer. Math. Soc.***124**(1996), 1727-1732.
7. J. Coykendall, Properties of the normset relating to the class group, *Proc. Amer. Math. Soc.***124**(1996), 3587-3593.
8. J. Coykendall, A remark on arithmetic equivalence and the normset, *Acta Arithmetica***92**(2000), 105-108.
9. J. Coykendall, The half-factorial property in integral extensions, *Comm. Algebra***27**(1999), 3153-3159.
10. F. Halter-Koch, Factorization of Algebraic Integers, *Ber. Math. Stat. Sektion im Forschungszentrum* **191**(1983).
11. A. Zaks, Half factorial domains, *Bull. Amer. Math. Soc.* **82** (1976), 721-723.
12. A. Zaks, Half-factorial-domains, *Israel J. Math.* **37** (1980), 281-302.