C O L L O Q U I U M   M A T H E M A T I C U M

VOL. LXX | 1996 | FASC. 2

FINITE CYCLIC GROUPS AND THE k-HFD PROPERTY

BY

SCOTT T. CHAPMAN (SAN ANTONIO, TEXAS) AND
WILLIAM W. SMITH (CHAPEL HILL, NORTH CAROLINA)

If D is a Krull domain, then it is well known that D is a unique factorization domain (UFD) if and only if D has trivial divisor class group. The study of several factorization properties weaker than the UFD condition, as well as a general analysis of number theoretic functions related to the factorization of elements into products of irreducible elements in Krull domains and monoids, has been the focus of recent research (see [4]–[10]). In particular, let D be an atomic integral domain and suppose that $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ are irreducible elements of D such that

$$\alpha_1 \ldots \alpha_m = \beta_1 \ldots \beta_n. \tag{1}$$

Then D is a

1. *half-factorial domain* (HFD) if the equation (1) implies that $m = n$;
2. *k-half-factorial domain* (k-HFD), where $k \geq 1$ is some positive integer, if the equation (1) along with the fact that n or m is less than or equal to k, implies that $m = n$.

Every atomic integral domain D is a 1-HFD, and if D is not a t-HFD (for some positive integer t), then D is not a k-HFD for any $k \geq t$. Clearly, if D is a HFD then D is a k-HFD for every $k \geq 1$. If D is the ring of integers in a finite algebraic extension of the rationals, then the converse of this statement is true [4, Theorem 1.3] (this is a generalization of a well-known result of Carlitz [2]). In general, the converse is false; in Example 7 of [4] the present authors construct a Dedekind domain with class group $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ which is not a HFD, but is a 2-HFD. In this note, we will address a conjecture (stated in both [5] and [6]) which asserts that the converse of this relationship holds if D is a Krull domain with finite cyclic class group. While we do not settle the conjecture, we show that it holds for a large class of Krull domains with finite cyclic class group.

1991 *Mathematics Subject Classification*: Primary 13F05.

Part of this work was completed while the first author was on leave at Karl-Franzens-Universität, in Graz, Austria on a Fulbright Fellowship.

Central to our arguments will be a close examination of the set

$$S = \{g \in \mathbb{Z}_n \mid g \neq 0 \text{ and contains a height-one prime ideal of } D\}.$$

For such a set $S = \{s_1, \ldots, s_t\}$, we will always assume that each element $s_i \in S$ is of the form $s_i = r_i + n\mathbb{Z}$, where $0 < r_i \leq n - 1$. We will use the following terminology, consistent with that used in the papers [5] and [6]:

1. S is *unitary* if for some $s_i \in S$ we have $r_i = 1$.
2. S has the *all divisor property* if for every $s_i \in S$, r_i divides n in $\mathbb{Z}$.

For convenience, we shall refer to a set S with the all divisor property as an *$\mathcal{AD}$-set*. We summarize our main results in the following theorem.

THEOREM 1. *Let D be a Krull domain with divisor class group $G = \mathbb{Z}_n$ with set S. Suppose that any of the following conditions hold*:

1. *S contains a generator of $\mathbb{Z}_n$* (see Propositions 2 and 7).
2. *S is an $\mathcal{AD}$-set with $|S| \leq 4$* (see Proposition 6).
3. *S is an $\mathcal{AD}$-set and $G \cong \mathbb{Z}_{p^r q^t}$, where p and q are distinct primes in* $\mathbb{Z}$ (see Proposition 9).

Then D is a HFD if and only if D is a k-HFD for some $k \geq 2$. ■

The papers [5] and [6] contain a detailed study of Dedekind domains D which are k-HFD for some $k \geq 2$. These results easily generalize to the case where D is a Krull domain (see [1] for details). We summarize several of the relevant results of these papers in the following proposition.

PROPOSITION 2. *Let D be a Krull domain with divisor class group G. Suppose that any of the following conditions hold*:

1. *$G \cong \mathbb{Z}_{p^n}$ for some prime integer p and positive integer n.*
2. *$G \cong \mathbb{Z}_{pq}$ for distinct prime integers p and q.*
3. *$|G| \leq 15$.*

Then D is a HFD if and only if D is a k-HFD for some $k \geq 2$. ■

We shall later require the following two results; 1 is Lemma 3.1 in [6], and 2 is Theorem 3.10 in [3].

PROPOSITION 3. *Let D be a Krull domain with divisor class group $\mathbb{Z}_n$.*

1. *If S is unitary and is not an $\mathcal{AD}$-set, then D is not a 2-HFD (and hence not a HFD).*
2. *If $|S| \leq 3$ and S is an $\mathcal{AD}$-set, then D is a HFD.* ■

While our interest in this problem is centered in ring theory, results concerning lengths of factorizations in a Krull domain D are combinatorial results based on the block semigroup associated with the divisor class group of D. Recall the following definitions. Let G be an abelian group, S a subset of the nonzero elements of G, and $\mathcal{F}(G)$ the multiplicative free abelian monoid with basis G. The elements of $\mathcal{F}(G)$ can be viewed as products of the form

$$F = \prod_{g\in G} g^{v_g(F)},$$

where $v_g(F) \in \mathbb{Z}^+$ and $v_g(F) = 0$ for almost all $g \in G$. Set

$$\mathcal{B}(G) = \Big\{ B \in \mathcal{F}(G) \,\Big|\, \sum_{g\in G} v_g(B)g = 0 \Big\}.$$

$\mathcal{B}(G)$ is known as the *block semigroup* over G. More generally, set

$$\mathcal{B}(S) = \{B \in \mathcal{B}(G) \mid v_g(B) = 0 \text{ for } g \in G\backslash S\}.$$

Block semigroups have been studied in great detail in [7], [8], and [10]. An element $B \in \mathcal{B}(S)$ is called *irreducible* if it cannot be written in the form $B = B_1B_2$, where B_1 and B_2 are nonzero blocks of $\mathcal{B}(S)$.

For an atomic monoid M, define M to be a *half-factorial monoid* (HFM), or a *k-half-factorial monoid* (k-HFM) in a manner analogous to the definitions used for atomic integral domains. The paper [1, pp. 99–100] gives a detailed argument that a Krull domain D with divisor class group $G = \mathrm{Cl}(D)$ is a HFD (or k-HFD for some $k \geq 2$) if and only if $\mathcal{B}(S)$ is a HFM (or k-HFM for some $k \geq 2$). Hence, for the remainder of this paper we focus on the block semigroup $\mathcal{B}(S)$ related to the Krull domain D.

If $B = s_1^{n_1} \dots s_t^{n_t}$ is a block in $\mathcal{B}(S)$, then set

$$k(B) = \sum_{i=1}^{t} \frac{n_i}{|s_i|},$$

where $|s_i|$ denotes the order of the element s_i in G. The function k is known as the *weight* of B. If B is the irreducible block associated with an irreducible α in D, then the value $z(\alpha) = k(B)$ is referred to in the literature as the *Zaks–Skula constant* of α (see [5]). A well-known result of Zaks and Skula states that a Dedekind domain D with torsion class group is a HFD if and only if $z(\alpha) = 1$ for every irreducible element $\alpha \in D$ (see [3, Theorem 3.8] for a proof of this fact).

Hence, assume that $G = \mathbb{Z}_n$ and $S = \{s_1, \dots, s_t\} \subset G\backslash\{0\}$ for $1 \leq s_i < n$. Under our assumption that S represents the set of nonzero divisor classes of some Krull domain D which contain height-one prime ideals, it is necessary that S is a generating set of G. If B is an irreducible block of $\mathcal{B}(S)$, then $B = s_1^{x_1} \dots s_t^{x_t}$, where $\sum_{i=1}^{t} s_i x_i = mn$ for some nonnegative integer m. If S is an $\mathcal{AD}$-set, then $k(S) = m$. Set

$$K(\mathcal{B}(S)) = \{k(B) \mid B \text{ is irreducible in } \mathcal{B}(S)\}.$$

LEMMA 4. *Let G and S be as above. Assume that*

1. $A = s_1^{x_1} \dots s_t^{x_t}$ *is an irreducible block in* $\mathcal{B}(S)$ *such that* $k(A) = \mathrm{Max}(K(\mathcal{B}(S)))$.
2. $B = s_1^{y_1} \dots s_t^{y_t}$ *is an irreducible block in* $\mathcal{B}(S)$ *with* $k(A) > k(B)$ *and* $x_i \ge y_i/2$ *for each* i.

Then $\mathcal{B}(S)$ *is not a* 2*-HFM.*

Proof. We write

$$A^2 = s_1^{2x_1} \dots s_t^{2x_t} = B(s_1^{2x_1-y_1} \dots s_t^{2x_t-y_t}).$$

Setting $C = s_1^{2x_1-y_1} \dots s_t^{2x_t-y_t}$, we have $A^2 = BC$, where $C \in \mathcal{B}(S)$. Hence, $2k(A) = k(B) + k(C)$ and $k(C) = 2k(A) - k(B) > k(A)$. Since $k(A) = \mathrm{Max}(\mathcal{B}(S))$, $k(C) > k(A)$ implies that C is not irreducible. Thus $A^2 = BC$ implies that $\mathcal{B}(S)$ is not a 2-HFM. ∎

We derive a corollary to the lemma which will be of later use.

COROLLARY 5. *Let G, S, and A be as in Lemma 4 and suppose that* $\mathcal{B}(S)$ *is a* 2*-HFM. Then*

1. *For any* $B \in \mathcal{B}(S)$ *with* $k(B) < k(A)$ *there is an* i *such that* $x_i < y_i/2$.
2. *If* $k(A) > 1$, *then* $x_i < |s_i|/2$ *for all* i. *In addition, if* S *is an* $\mathcal{AD}$*-set, then* $x_i < n/(2s_i)$ *for all* i.

Proof. Part 1 follows directly from Lemma 4. For part 2, let C_i be the element of $\mathcal{B}(S)$ of the form $C_i = s_i^{|s_i|}$. If $x_i \ge |s_i|/2$, then, since $x_j \ge 0$ for each $i \ne j$, we deduce that $\mathcal{B}(S)$ is not a 2-HFM by part 2 of Lemma 4, a contradiction. Notice that if S is an $\mathcal{AD}$-set, then $|s_i| = n/s_i$. ∎

The corollary allows us to prove part 2 of Theorem 1.

PROPOSITION 6. *Let* $G \cong \mathbb{Z}_n$ *and* $S = \{s_1, \dots, s_t\} \subseteq \mathbb{Z}_n \backslash \{0\}$ *be an* $\mathcal{AD}$*-set with* $|S| \le 4$. $\mathcal{B}(S)$ *is a HFM if and only if* $\mathcal{B}(S)$ *is a* k*-HFM for some* $k \ge 2$.

Proof. Suppose $\mathcal{B}(S)$ is not a HFM and is a 2-HFM. Let $A = s_1^{x_1} \dots s_t^{x_t}$ be an irreducible block in $\mathcal{B}(S)$ such that $k(A) = m = \mathrm{Max}\, K(\mathcal{B}(S)) > 1$ (this is possible since S is an $\mathcal{AD}$-set). By part 2 of Corollary 5, $x_i < n/(2s_i) = |s_i|/2$ for all i. Hence,

$$mn = \sum_{i=1}^{t} s_i x_i < \sum_{i=1}^{t} s_i \frac{n}{2s_i} = \sum_{i=1}^{t} \frac{n}{2} \le 2n$$

since $|S| \le 4$. Thus $m < 2$ implies that $m = 1$, a contradiction. ∎

We proceed to a proposition which will complete the proof of part 1 of Theorem 1.

PROPOSITION 7. *Let $G \cong \mathbb{Z}_n$ and $S = \{s_1, \ldots, s_t\} \subseteq \mathbb{Z}_n \backslash \{0\}$ be a unitary $\mathcal{AD}$-set of G. $\mathcal{B}(S)$ is a HFM if and only if $\mathcal{B}(S)$ is a 2-HFM.*

Proof. Assume there exists a unitary $\mathcal{AD}$-set S for which $\mathcal{B}(S)$ is a 2-HFM but not a HFM. Without loss of generality, assume that $s_1 = 1$. Let such an S be chosen with $|S|$ minimal. Notice that $|S| > 4$ by Proposition 6. We claim that if $B = 1^{y_1} s_2^{y_2} \ldots s_t^{y_t}$ is an irreducible block of $\mathcal{B}(S)$ with $y_1 \neq 0$ and some $y_j = 0$ (for $2 \leq j \leq t$), then $k(B) = 1$. To see this, let $S' = \{s_i \mid y_i \neq 0\}$. Then S' is properly contained in S. Thus, $\mathcal{B}(S')$ is a 2-HFM since $\mathcal{B}(S)$ is a 2-HFM. By the minimality of S, $\mathcal{B}(S')$ is a HFM. Thus $k(B) = 1$.

Now, suppose $A = 1^{x_1} s_2^{x_2} \ldots s_t^{x_t}$ is an irreducible block in $\mathcal{B}(S)$ with $k(A) = \mathrm{Max}(K(\mathcal{B}(S))) > 1$. Since S is an $\mathcal{AD}$-set, $\sum_{i=1}^{t} s_i x_i = mn$, where $k(A) = m$ for some $m > 1$. By part 2 of Corollary 5, $x_i < n/(2s_i)$ for each i. Hence, $0 < n - 2s_i x_i$ for each i. Now, for each $2 \leq j \leq k$, set

$$M_j = s_1^{x_1 + s_j x_j} \prod_{i \neq j} s_i^{x_i}.$$

Notice that since $s_1(x_1 + s_j x_j) + s_2 x_2 + \ldots + s_t x_t = mn$, $k(M_i) = m > 1$. By the observation in the paragraph above, M_i is not irreducible.

For each $2 \leq i \leq t$, set

$$R_i = s_1^{n - s_i x_i} s_i^{x_i}.$$

Since $n - s_i x_i > 0$, each R_i is a block in $\mathcal{B}(S)$ with

$$k(R_i) = ((n - s_i x_i) + s_i x_i)/n = 1.$$

Hence each R_i is irreducible in $\mathcal{B}(S)$. Consider

$$\begin{aligned} AR_i &= (s_1^{x_1} \ldots s_t^{x_t})(s_1^{n - s_i x_i} s_i^{x_i}) = s_i^{2x_i} s_1^{x_1 + n - s_i x_i} \prod_{j \neq i, j > 1} s_j^{x_j} \\ &= (s_i^{2x_i} s_1^{n - 2s_i x_i}) \Big(s_1^{x_1 + s_i x_i} \prod_{j \neq i, j > 1} s_j^{x_j} \Big) = CM_i. \end{aligned}$$

Since A, R_i, and M_i are blocks in $\mathcal{B}(S)$, C is a nontrivial block. By the previous argument each M_i is not irreducible. Thus, the product AR_i can be written as a product of at least three irreducibles. We conclude that $\mathcal{B}(S)$ is not a 2-HFM. ∎

Proof of part 1 of Theorem 1. By previous remark it suffices to consider the block semigroup $\mathcal{B}(S)$. Since S contains a generator, we can use an automorphism argument [5, Lemma 1.9] and assume that S is unitary. By part 1 of Proposition 3, if S is not an $\mathcal{AD}$-set, then $\mathcal{B}(S)$ is neither a 2-HFM nor HFM. Thus S must be an $\mathcal{AD}$-set. Proposition 7 now completes the proof. ∎

The proof of part 3 of Theorem 1 will require a lemma.

LEMMA 8. *Let* $G = \mathbb{Z}_n$ *and* $S = \{s_1, \ldots, s_k\}$ *be an* $\mathcal{AD}$*-set of* G. *Set* $d = \gcd(s_2, \ldots, s_k)$, $m = n/d$, *and* $S' = \{s_1, s_2/d, \ldots, s_k/d\}$. *Then*

1. S' *is an* $\mathcal{AD}$*-set for* $\mathbb{Z}_m$ *and* $\gcd(s_1, s_2/d, \ldots, s_k/d) = 1$.
2. $\mathcal{B}(S)$ *is a HFM* (*or a* k*-HFM for some* $k \geq 2$) *if and only if* $\mathcal{B}(S')$ *is a HFM* (*or a* k*-HFM for some* $k \geq 2$).

Proof. We note that since $\gcd(s_1, \ldots, s_k) = 1$, we have $\gcd(s_1, d) = 1$. Since $s_1 \mid d(n/d)$, $s_1 \mid (n/d)$ and S' is an $\mathcal{AD}$-set for $\mathbb{Z}_m$ with

$$\gcd(s_1, s_2/d, \ldots, s_k/d) \mid \gcd(s_1, s_2, \ldots, s_k) = 1.$$

This completes the proof of 1.

There is a one-to-one correspondence between the irreducible blocks of $\mathcal{B}(S)$ and $\mathcal{B}(S')$, given in the following manner. Let $B = s_1^{x_1} \ldots s_k^{x_k}$ be an irreducible block in $\mathcal{B}(S)$ with $\sum_{i=1}^{k} s_i x_i = nt$. Since $d \mid s_1 x_1$ and $\gcd(d, s_1) = 1$, it follows that $d \mid x_1$ and $B' = s_1^{(x_1/d)} (s_2/d)^{x_2} \ldots (s_k/d)^{x_k}$ is an irreducible block in $\mathcal{B}(S')$ with

$$s_1 \left(\frac{x_1}{d}\right) + \sum_{i=2}^{k} \left(\frac{s_i}{d}\right) x_i = \left(\frac{n}{d}\right) t.$$

A reverse correspondence works in a similar manner (notice for such blocks that $t = k(B) = k(B')$). Hence 2 follows. ■

The next proposition establishes Theorem 1, part 3.

PROPOSITION 9. *Let* $G = \mathbb{Z}_{p^r q^s}$, *where* p *and* q *are distinct primes in* $\mathbb{Z}$, *and let* $S = \{s_1, \ldots, s_t\}$ *be an* $\mathcal{AD}$*-set of* G. *Then* $\mathcal{B}(S)$ *is a HFM if and only if* $\mathcal{B}(S)$ *is a* k*-HFM for some* $k \geq 2$.

Proof. If S contains a generator of G, then the result follows from Proposition 7. So assume that S does not contain a generator of G and that $\mathcal{B}(S)$ is a 2-HFM and not a HFM with $G = \mathbb{Z}_n$, where $n = p^r q^s$. Choose $n = p^r q^s$ minimal for such an example and an $\mathcal{AD}$-set $S = \{s_1, \ldots, s_t\}$ with $|S|$ also minimal. For each $1 \leq i \leq t$ set

$$d_i = \gcd(s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_t).$$

By considering the correspondence set up in Lemma 8, if any of the $d_i > 1$ then we would have a cyclic group $\mathbb{Z}_{n/d_i}$, which is of order strictly less than n, and a corresponding set S' such that $\mathcal{B}(S')$ is a 2-HFM but not HFM, contradicting the minimality of n. Hence, each $d_i = 1$.

We now argue that in S there must be some $1 \leq i < j \leq t$ such that either $s_i \mid s_j$ or $s_j \mid s_i$. Since $\gcd(s_1, \ldots, s_k) = 1$, one of the $s_i = p^v$. Since $d_i = 1$, then one of the $s_j = p^w$ (for $i \neq j$) and hence either $s_i \mid s_j$ or $s_j \mid s_i$.

Without loss of generality, assume that $s_1 \mid s_2$. Suppose $s_1 b = s_2$. Since $\mathcal{B}(S)$ is not a HFM, there is an irreducible block $A = s_1^{x_1} \dots s_t^{x_t}$ with $\sum_{i=1}^{t} s_i x_i = mn$, where $k(A) = m = \mathrm{Max}(K(\mathcal{B}(S))) > 1$. By Corollary 5, $x_i < n/(2s_i)$ for each i. Set

$$M = s_1^{x_1+bx_2} s_3^{x_3} \dots s_t^{x_t}, \qquad B_1 = s_1^{(n/s_1)-bx_2} s_2^{x_2}, \qquad B_2 = s_1^{(n/s_1)-2bx_2} s_2^{2x_2}.$$

Now, $k(M) = m$, $k(B_1) = 1$, and $k(B_2) = 1$. Notice that $x_2 < n/2s_2$ implies that $2bx_2 < 2bn/2s_1 b = n/s_1$. Since $k(B_1) = k(B_2) = 1$, property $\mathcal{AD}$ implies that both B_1 and B_2 are irreducible. Since, for any proper subset S' of S, $\mathcal{B}(S')$ inherits the 2-HFM property, it follows from the minimality of $|S|$ that $\mathcal{B}(S')$ must have the HFM property. Thus M is not irreducible in $\mathcal{B}(S')$ and hence M is not irreducible in $\mathcal{B}(S)$. Thus

$$AB_1 = MB_2$$

implies that the product of 2 irreducibles in $\mathcal{B}(S)$ can be written as the product of more than 2 irreducibles in $\mathcal{B}(S)$, a contradiction. ■

It is of interest to note that the proof of Theorem 1 remains valid if the Krull domain D with divisor class group $\mathbb{Z}_n$ is replaced by a Krull monoid H with identical divisor class group. In this case, the set S would now represent the subset of divisor classes of H which contain at least one prime divisor. The interested reader is referred to [9] for more information on Krull monoids.

Acknowledgements. The authors express their appreciation to Alfred Geroldinger for discussions related to this work.

REFERENCES

[1] D. F. Anderson, S. T. Chapman and W. W. Smith, *Some factorization properties of Krull domains with infinite cyclic divisor class group*, J. Pure Appl. Algebra 96 (1994), 97–112.

[2] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), 391–392.

[3] S. T. Chapman, *The davenport constant, the cross number, and their application in factorization theory*, in: Zero-Dimensional Commutative Rings, Marcel Dekker, New York, 1995, 167–190.

[4] S. T. Chapman and W. W. Smith, *Factorization in Dedekind domains with finite class group*, Israel J. Math. 71 (1990), 65–95.

[5] —, —, *On the HFD, CHFD, and k-HFD properties in Dedekind domains*, Comm. Algebra 20 (1992), 1955–1987.

[6] —, —, *On the k-HFD property in Dedekind domains with small class group*, Mathematika 39 (1992), 330–340.

[7] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, Math. Z. 197 (1988), 505–529.

[8] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations in block semigroups and arithmetical applications*, Math. Slovaca 42 (1992), 641–661.
[9] U. Krause and C. Zahlten, *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitt. Math. Ges. Hamburg 12 (1991), 681–696.
[10] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), 319–330.

Department of Mathematics
Trinity University
715 Stadium Drive
San Antonio, Texas 78212-7200
U.S.A.

Department of Mathematics
The University of North Carolina
at Chapel Hill
Chapel Hill, North Carolina 27599-3250
U.S.A.

Reçu par la Rédaction le 10.7.1995