Factorizations of Algebraic Integers, Block Monoids, and Additive Number Theory

Paul Baginski and Scott T. Chapman

Abstract

Let D be the ring of integers in a finite extension of the rationals. The classic examination of the factorization properties of algebraic integers usually begins with the study of norms. In this paper, we show using the ideal class group, $\mathcal{C}(D)$, of D that a deeper examination of such properties is possible. Using the class group, we construct an object known as a block monoid, which allows us to offer proofs of three major results from the theory of nonunique factorizations: Geroldinger's Theorem, Carlitz's Theorem and Valenza's Theorem. The combinatorial properties of block monoids offer a glimpse into two widely studied constants from additive number theory, the Davenport Constant and the cross number. Moreover, block monoids allow us to extend these results to the more general classes of Dedekind domains and Krull domains.

1 Introduction.

In an introductory abstract algebra class, the notion of a unique factorization domain (UFD) is carefully developed and plays an important role. A wide array of UFDs are usually identified in such a course (such as $\mathbb{Z}$, $K[X]$ where K is a field, and $\mathbb{Z}[i]$ the Gaussian integers) before deeper algebraic structures, such as Euclidean domains or principal ideal domains, are introduced. To convince a student of the usefulness of the definition of a UFD (also known as a *factorial domain*), it is necessary to provide an example of an integral domain in which the notion of unique factorization fails. While there is an abundance of such examples, the one most commonly used in many basic level texts is

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

in the algebraic number ring $\mathbb{Z}[\sqrt{-5}]$. Though students (and perhaps teachers) may be content with seeing different numbers and verifying that the two products are equal, there is more to be done. A true verification that equation (1) is a non-unique factorization of 6 into irreducible elements requires two additional arguments:

(i) $2, 3, (1 + \sqrt{-5})$, and $(1 - \sqrt{-5})$ are indeed irreducible elements, and

(ii) neither 2 nor 3 is an associate of either $(1 + \sqrt{-5})$ or $(1 - \sqrt{-5})$.

Any further issues involving factoring elements in $\mathbb{Z}[\sqrt{-5}]$ are normally relegated to exercises at the end of the topic section. This is somewhat unfortunate, as $\mathbb{Z}[\sqrt{-5}]$ has a very nice property concerning factorizations of its elements into products of irreducibles. Specifically, if $\alpha_1, \ldots \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ with

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m, \tag{2}$$

then $n = m$. In factorization theory parlance, we say the two factorizations have the same *length* (number of irreducibles, counting multiplicity). Therefore, even though $\mathbb{Z}[\sqrt{-5}]$ may not be a UFD, all irreducible factorizations of a given nonzero nonunit x in $\mathbb{Z}[\sqrt{-5}]$ have the same length. In general, an integral domain with this property is known as a *half-factorial domain* (HFD).

An arithmetic verification of the property illustrated in equation (2) is likely beyond a beginning level algebra student. However, using the notion of the ideal class group (and, more generally, the class number), one can construct a very simple proof of this fact for $\mathbb{Z}[\sqrt{-5}]$; Carlitz first illustrated this argument in [5]. This line of reasoning leads to a deeper understanding of how elements factor in an algebraic ring of integers. The purpose of our paper is to develop this understanding by using a structure, known as a *block monoid*, that is associated with the class group. In fact, block monoids' utility extends beyond just analyzing factorizations in algebraic number rings. We shall show that block monoids can be used in a similar line of analysis in more general classes of integral domains, such as Dedekind domains and Krull domains. Appealingly, the definition of a block monoid can be understood by any undergraduate who has seen the definition of a group, even if they cannot yet grasp the theory underlying the class group construction. Our investigations will involve a close study of the combinatorial properties of block monoids and lead to an examination of two actively researched concepts from additive number theory known as the *Davenport constant* and the *cross number*.

We divide our work into four sections. In Section 2, we review some basic definitions from algebraic number theory and commutative algebra and use them to perform some motivating calculations with the class group. In Section 3, we define block monoids and develop a factorization theory for them that parallels ideas from factorization in domains. In Section 4, these parallels are made explicit. We construct a monoid homomorphism from an algebraic number ring (or more generally a Dedekind domain) to an appropriately chosen block monoid. We prove a theorem of Alfred Geroldinger which shows that this homomorphism preserves lengths of irreducible factorizations. Hence, to study lengths of irreducible factorizations of elements in a Dedekind domain, one merely needs to understand the factorization properties of the associated block monoid. This allows us to give an elementary proof of a well-known result of Carlitz: the ring of integers of an algebraic number field $\mathcal{O}_K$ is half factorial if and only if the class number of $\mathcal{O}_K$ is less than or equal to two. In Section 5, we demonstrate some additional applications of Geroldinger's theorem in the theory of non-unique factorizations. We introduce two invariants of block

monoids, the Davenport constant and the cross number, which permit a finer analysis of factorization in a Dedekind domain. In particular, we prove a theorem of Valenza which determines, for rings of algebraic integers, the degree to which lengths of irreducible factorizations can vary. We assume that the reader is familiar with a two semester course in abstract algebra. Some knowledge of algebraic number rings is useful, but we will attempt in Section 2 to make our work self-contained. Any undefined terminology can be found in [13].

2 Terminology and Basic Background.

Let $K = \mathbb{Q}(\alpha)$ be a finite extension of the rationals. The ring of integers of K is given as

$$\mathcal{O}_K = \{a \in K \mid f(a) = 0 \text{ for a monic polynomial } f \text{ with integer coefficients } \}.$$

In the usual integers $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$, we are able to factor integers n, with $|n| > 1$, into (unique) products of prime numbers. In general rings of integers $\mathcal{O}_K$, we shall not always be able to factor nonzero nonunits into products of *prime* elements, i.e. nonzero nonunits $x \in \mathcal{O}_K$ such that if $x|ab$ then $x|a$ or $x|b$. Instead, we must be content with factoring elements as products of irreducible elements. A nonzero nonunit $a \in \mathcal{O}_K$ is *irreducible* if whenever $bc = a$ for some $b, c \in \mathcal{O}_K$ then either b or c is a unit. Every prime is irreducible, but not conversely. In fact, $\mathcal{O}_K$ is a UFD if and only if all irreducibles are prime, for if a prime p divides an element a, then p (or an associate) must appear in every factorization of a.

To understand the factorizations in a general $\mathcal{O}_K$, we must investigate the structure of its ideals. If $x_1, \ldots, x_k$ are elements of $\mathcal{O}_K$, then let $(x_1, \ldots, x_k)$ represent the ideal generated by $x_1, \ldots, x_k$ in $\mathcal{O}_K$. If I is an ideal of $\mathcal{O}_K$ and there exist elements $x_1, \ldots, x_k$ of $\mathcal{O}_K$ such that $I = (x_1, \ldots, x_k)$, then I is *finitely generated*. If $I = (x)$ for some $x \in \mathcal{O}_K$, then I is a *principal ideal* of $\mathcal{O}_K$. An ideal I of $\mathcal{O}_K$ is *prime* if whenever $x, y \in \mathcal{O}_K$ and $xy \in I$ then either $x \in I$ or $y \in I$. A principal ideal (x) is prime ideal if and only if x is a prime element.

If (x) and (y) are two principal ideals, then clearly the set $\{ab \,|\, a \in (x),\, b \in (y)\}$ is an ideal, namely (xy). We write $(x)(y) = (xy)$ as the product of principal ideals. Note that $(x)(y) = (z)$ if and only if $xy = uz$ for some unit $u \in D$. For general ideals I and J, we must be more careful in defining their product, since the set $\{ab \,|\, a \in I, b \in J\}$ may not be closed under addition. Therefore, the product of two ideals I and J of $\mathcal{O}_K$ is defined to be all finite sums of products from I and J, which is easily argued to be another ideal:

$$IJ = \left\{ \sum_{i=1}^{k} a_i b_i \;\middle|\; k \in \mathbb{N},\ a_i \in I \text{ and } b_i \in J \right\}.$$

If we are now given two factorizations $x_1 \cdots x_m = y_1 \cdots y_n$ of the same element, then we obtain an equation in terms of principal ideals as well: $(x_1) \cdots (x_m) = (y_1) \cdots (y_n)$. These principal ideals, however, may split into products of other

non-principal ideals, revealing additional levels of interaction within the product. Understanding factorizations of elements will thus require uncovering how general ideals can combine and recombine into principal ideals, particularly principal ideals generated by an irreducible element.

Let $\mathcal{I}(\mathcal{O}_K)$ represent the set of nonzero ideals of $\mathcal{O}_K$ and $\mathcal{P}(\mathcal{O}_K)$ its associated subset of nonzero principal ideals. Notice that both $\mathcal{I}(\mathcal{O}_K)$ and $\mathcal{P}(\mathcal{O}_K)$ form multiplicative monoids under ideal multiplication, with the principal ideal (1) as the identity element. The ideal structure of $\mathcal{O}_K$ has several celebrated properties. Proofs of assertions (1) and (2) below can be found in [17] or [19] and a proof of (3) can be found in [13, Theorem 2.10.14].

Proposition 2.1. *Let I be an ideal of $\mathcal{O}_K$ and $\mathcal{I}(\mathcal{O}_K)$ and $\mathcal{P}(\mathcal{O}_K)$ be as above.*

1. *I is finitely generated. Moreover, there exist elements α and β in $\mathcal{O}_K$ such that $I = (\alpha, \beta)$.*
2. *The factor monoid $\mathcal{C}(\mathcal{O}_K) = \mathcal{I}(\mathcal{O}_K)/\mathcal{P}(\mathcal{O}_K)$ forms a finite abelian group.*
3. *Let $[I]$ represent the image of the ideal I in $\mathcal{C}(\mathcal{O}_K)$. Then, for each $g \in \mathcal{C}(\mathcal{O}_K)$ there exists a prime ideal P of $\mathcal{O}_K$ such that $[P] = g$.*

The group $\mathcal{C}(\mathcal{O}_K)$ is known as the *class group* of $\mathcal{O}_K$. Its order $|\mathcal{C}(\mathcal{O}_K)|$ is the *class number* of $\mathcal{O}_K$. The class number gives a classic answer to the question of when a ring of algebraic integers admits unique factorization (see [13, Theorem 1.7.3] for a proof, or see Theorem 2.4 below).

Theorem 2.2. *The ring of integers $\mathcal{O}_K$ in an algebraic number field K is a unique factorization domain if and only if the class number of $\mathcal{O}_K$ is 1.*

In fact, the size of the class group of $\mathcal{O}_K$ was generally assumed to be a measure of how far a ring of integers was from being a UFD. The key to our analysis of the factorization properties of $\mathcal{O}_K$ lies in Dedekind's celebrated Fundamental Theorem of Ideal Theory for rings of algebraic integers.

The Fundamental Theorem of Ideal Theory. *[19, Theorem 8.20] Let I be an ideal of $\mathcal{O}_K$. There exists a unique (up to order) list of prime ideals $P_1, \ldots, P_k$ in $\mathcal{O}_K$ so that $I = P_1 \cdots P_k$.*

In a more general context, an integral domain D which satisfies the Fundamental Theorem of Ideal Theory is called a *Dedekind domain* (see [15, Chapter VIII.6]). In a general Dedekind domain, the factor monoid $\mathcal{I}(D)/\mathcal{P}(D)$ is still an abelian group, but it may not be finite. Moreover, property (3) of Proposition 2.1 may fail for a general Dedekind domain. In order to use the Fundamental Theorem effectively, we will need to pay particular attention to the distribution of prime ideals in the class group $\mathcal{C}(D)$. We define $S = \{g \in \mathcal{C}(D) \mid \text{ there exists a prime ideal } P \text{ of } D \text{ such that } [P] = g\}$ to be the *set of classes containing prime ideals*. Proposition 2.1 part (3) implies that $S = \mathcal{C}(D)$ when $D = \mathcal{O}_K$, the ring of integers in an algebraic number field, but for general Dedekind domains, S can be a proper subset (see [13, Theorem 3.7.8]). Whenever possible, we will couch our results in the language of

Dedekind domains, demonstrating in the process how factorization problems in general Dedekind domains depend upon the distribution of prime ideals in the class group $\mathcal{C}(D)$.

We now begin revealing the connection between the ideas developed above and problems involving the factorizations of elements in a Dedekind domain D. The following result characterizes the irreducible elements of D in an ideal theoretic sense. We view the class group $\mathcal{C}(D)$ of D additively by writing $[I] + [J] = [IJ]$ for ideals I and J; under this convention, its identity is $0 = [D] = [(1)]$.

Proposition 2.3. *Let D be a Dedekind domain and for $k \geq 1$, let $P_1, \ldots, P_k$ be not necessarily distinct prime ideals of D. Then*

(1) $P_1 \cdots P_k$ is a principal ideal of D if and only if $[P_1] + \cdots + [P_k] = 0$ in $\mathcal{C}(D)$.

Suppose now $(x) = P_1 \cdots P_k$, for $x \in D$ a nonzero nonunit.

(2) The element x is prime in D if and only if $k = 1$.

(3) The element x is irreducible in D if and only if for every nonempty proper subset $T \subset \{1, \ldots, k\}$, $\sum_{i \in T} [P_i] \neq 0$.

Proof. Claim (1) follows from the definition of the class group and (2) holds since in any integral domain x is prime if and only if the ideal (x) is a prime ideal. We prove (3) by contrapositive. ($\Rightarrow$) Suppose for some proper subset T that $\sum_{i \in T} [P_i] = 0$. Then $\prod_{i \in T} P_i = (y)$ for some nonzero nonunit $y \in D$. Let $\overline{T} = \{1, \ldots, k\} \backslash T$. By (1) we have $[P_1] + \cdots + [P_k] = 0$, so $\sum_{i \in \overline{T}} [P_i] = 0$ also. Thus, $\prod_{i \in \overline{T}} P_i = (z)$ for some nonzero nonunit $z \in D$. Hence $(x) = (y)(z)$, which implies that $x = uyz$ where u is a unit of D and so x is reducible. ($\Leftarrow$) Suppose that x is reducible in D, i.e. $x = yz$ for nonunits y and z in D. By the Fundamental Theorem, there is a proper nonempty subset $T \subset \{1, \ldots, k\}$ such that $(y) = \prod_{i \in T} P_i$. By (1), in $\mathcal{C}(D)$, $\sum_{i \in T} [P_i] = 0$. □

This proposition allows us to recast Theorem 2.2 for Dedekind domains, characterizing unique factorization in terms of $\mathcal{C}(D)$ and S.

Theorem 2.4. *Let D be a Dedekind domain, $\mathcal{C}(D)$ its class group, and $S \subseteq \mathcal{C}(D)$ be the set of classes containing prime ideals, as defined above. Then the following are equivalent:*

1. *D is a UFD*
2. *S is trivial, i.e. $S = \{0\}$*
3. *$\mathcal{C}(D)$ is the trivial group*
4. *D is a principal ideal domain.*

Proof. To show (1) $\Rightarrow$ (2), we need the fact that in a Dedekind domain all prime ideals $P \neq (0)$ are maximal ideals (see [15, Chapter VIII.6]). Let P be a prime ideal of D and choose a nonzero, nonunit $a \in P$. We may factor $a = x_1 \cdots x_n$ as a (unique) product of irreducibles and since P is prime, $x_i \in P$ for some i. Since x_i is irreducible and D is a UFD, x_i is prime and thus (x_i) is a prime ideal. But $P \supseteq (x_i)$, so by the maximality of prime ideals, $P = (x_i)$. In terms of the class group, $[P] = 0$ and since P was arbitrary, $S = \{0\}$.

For (2) $\Rightarrow$ (3), note that if $S = \{0\}$, then all prime ideals P are principal, i.e. $P \in \mathcal{P}(D)$. If I is any ideal of D, then by the Fundamental Theorem it equals a product of prime ideals, which lies in the monoid $\mathcal{P}(D)$. Therefore $\mathcal{I}(D) = \mathcal{P}(D)$ and $\mathcal{C}(D)$ is trivial. The implication (3) $\Rightarrow$ (4) is clear, since $\mathcal{C}(D)$ is trivial if and only if $\mathcal{I}(D) = \mathcal{P}(D)$. Finally, (4) implies (1) is well-known (see [15, Theorem 3.7]). $\square$

We illustrate the ideas of this section with a closer look at our previously mentioned example. For $n > 1$ we denote the cyclic group $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}_n$, enumerated as $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$, where $\overline{k}$ denotes the congruence class of k modulo n.

Example 2.5. Let $K = \mathbb{Q}(\sqrt{-5})$. It is well known that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, the only units of $\mathcal{O}_K$ are ± 1, and that the class number of $\mathcal{O}_K$ is 2 (see [17]). Hence $\mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_2$. Consider the non-unique factorization

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{3}$$

in $\mathbb{Z}[\sqrt{-5}]$. Let us consider what is happening here in terms of ideals. Using [17], we see that the prime ideal decompositions of (2) and (3) in $\mathbb{Z}[\sqrt{-5}]$ are

$$(2) = (2, 1 + \sqrt{-5})^2 \text{ and } (3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Hence,

$$(6) = (2)(3) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}). \tag{4}$$

The second factorization in equation (3) is obtained by rearranging the product in equation (4),

$$\begin{aligned}(6) &= (2)(3) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5})(2, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (1 + \sqrt{-5})(1 - \sqrt{-5}).\end{aligned}$$

By Proposition 2.3 (1), for every nonprincipal ideal I of $\mathcal{O}_K$, $[I] \neq 0$. Since the class group of $\mathbb{Z}[\sqrt{-5}]$ has exactly one nontrivial element, all nonprincipal ideals I of $\mathbb{Z}[\sqrt{-5}]$ have the same ideal class $[I] = \overline{1}$. If P_1, P_2 are any two nonprincipal prime ideals, then $[P_1] + [P_2] = 0$, so by Proposition 2.3 part (1), $P_1 P_2$ is principal. Furthermore, by Proposition 2.3 part (3), $P_1 P_2 = (x)$ for some irreducible element x, so we conclude $2, 3, 1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are all irreducible. Since every two nonprincipal prime ideals of $\mathbb{Z}[\sqrt{-5}]$ produce a principal ideal, we have exhausted all possible the factorizations of 6 in $\mathbb{Z}[\sqrt{-5}]$ up to associates.

Proposition 2.3 and Example 2.5 motivate a closer examination of the class group $\mathcal{C}(D)$ and how elements within it combine to form the identity. Indeed, in Example 2.5 such combinations of elements of $\mathcal{C}(D)$ were intimately tied to products of ideals yielding principal ideals generated by irreducibles; these irreducibles in turn divided our original element. These motivations spur the central definition of the next section.

3 Block Monoids and Their Basic Divisibility Properties.

Let G be an abelian group. Let $\mathcal{F}(G)$ represent the free abelian monoid on G, defined in the following sense. We write the elements of $\mathcal{F}(G)$ as $C = \prod_{g \in G} g^{v_g}$ where v_g is a nonnegative integer and all but finitely many of the v_g are nonzero. The exponent v_g is the number of times the element g appears in C. If C and T are elements in $\mathcal{F}(G)$, the monoid operation is given by

$$C \cdot T = \prod_{g \in G} g^{v_g} \cdot \prod_{g \in G} g^{v'_g} = \prod_{g \in G} g^{v_g + v'_g}.$$

Definition 3.1. Let G be an abelian group. The set

$$\mathcal{B}(G) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g} \text{ with } \sum_{g \in G} v_g g = 0 \right\}$$

forms a submonoid of $\mathcal{F}(G)$ known as the *block monoid of* G. If S is a nonempty subset of G, then the set

$$\mathcal{B}(G, S) = \left\{ C \;\middle|\; C = \prod_{g \in G} g^{v_g} \text{ with } \sum_{g \in G} v_g g = 0 \text{ and } v_g = 0 \text{ if } g \notin S \right\}$$

is a submonoid of $\mathcal{B}(G)$ known as the *block monoid of* G *restricted to* S.

We will refer to the elements of $\mathcal{B}(G, S)$ as *blocks*. We call the identity of $\mathcal{B}(G, S)$, $E = \prod_{g \in G} g^0$, the *empty block*. A block B *divides* a block C, denoted $B \mid C$, if there is a block T such that $C = BT$. From the definitions, it is easy to see that a block $B = \prod_{g \in G} g^{v_g}$ divides a block $C = \prod_{g \in G} g^{v'_g}$ if and only if $v_g \leq v'_g$ for all $g \in G$. If $B, C \in \mathcal{F}(G, S)$, then whenever any two of B, C, and BC are in $\mathcal{B}(G, S)$, so is the third. For the block $B = \prod_{g \in G} g^{v_g}$, we set $|B| = \sum_{g \in G} v_g$ to be the *size* of B.

By Proposition 2.3 part (1), if D is a Dedekind domain and $P_1, \ldots, P_k$ are prime ideals of D, then $P_1 \cdots P_k$ is a principal ideal of D if and only if $[P_1] + \ldots + [P_k] = 0$ in $\mathcal{C}(D)$. By definition, this is equivalent to $[P_1] \cdots [P_k]$ being a block in $\mathcal{B}(\mathcal{C}(D))$. This observation provides only the first taste of the relationship between factorization in Dedekind domains and block monoids. To describe it fully, we must develop our knowledge of block monoids further.

A block $B \neq E$ is *irreducible* if $B = CT$ for C, T in $\mathcal{B}(G,S)$ implies that either $C = E$ or $T = E$, i.e. B has no nontrivial blocks dividing it other than itself. A block $B \neq E$ which is not irreducible will be called *reducible*. A block $B \neq E$ is *prime* if whenever $B \mid CT$ then either $B \mid C$ or $B \mid T$. As with integral domains, we can consider factorizations of blocks into irreducible blocks. Many standard assertions easily transfer to this setting; for instance a prime block B is irreducible, but not conversely. We also define natural analogues of factorization properties. A block monoid $\mathcal{B}(G,S)$ is *half factorial* if whenever $B_1, \ldots, B_n, C_1, \ldots, C_m \in \mathcal{B}(G,S)$ are irreducible blocks and $B_1 \cdots B_n = C_1 \cdots C_m$, then $m = n$. The block monoid is *factorial* if under these hypotheses we can additionally conclude that there is a permutation $\sigma \in \mathrm{Sym}(n)$ such that $B_i = C_{\sigma(i)}$ for all $i \leq n$. "Factorial" is simply another name for "unique factorization." As with domains, a block monoid in which all irreducibles are prime must be factorial. We illustrate the factorization properties of block monoids with an elementary example.

Example 3.2. Let $G = \mathbb{Z}_4$. Here

$$\mathcal{B}(\mathbb{Z}_4) = \{\overline{0}^{x_0}\overline{1}^{x_1}\overline{2}^{x_2}\overline{3}^{x_3} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 + 3x_3 \equiv 0 \pmod 4\}.$$

Notice that the following blocks are the irreducible blocks of $\mathcal{B}(\mathbb{Z}_4)$ since they alone have no blocks properly dividing them:

$$\overline{0}^1,\ \overline{1}^4,\ \overline{2}^2,\ \overline{3}^4,\ \overline{1}^2\overline{2}^1,\ \overline{1}^1\overline{3}^1, \text{ and } \overline{2}^1\overline{3}^2.$$

Other than $\overline{0}^1$, none of these irreducibles is prime. Moreover, in this monoid it is easy to produce factorizations of blocks into irreducible blocks which differ in length. For instance,

$$B = (\overline{1}^4)(\overline{3}^4) = (\overline{1}^1\overline{3}^1)^4$$

is a factorization of B into 2 and 4 irreducible blocks respectfully. Now, let $S = \{\overline{1}, \overline{2}\}$. We have

$$\mathcal{B}(\mathbb{Z}_4, S) = \{\overline{1}^{x_1}\overline{2}^{x_2} \mid \text{each } x_i \geq 0 \text{ and } x_1 + 2x_2 \equiv 0 \pmod 4\}$$

and the irreducible blocks decrease to

$$B_1 = \overline{1}^4,\ B_2 = \overline{2}^2,\ B_3 = \overline{1}^2\overline{2}^1.$$

Now suppose B is a block in $\mathcal{B}(\mathbb{Z}_4, S)$ and $B = B_1^{y_1}B_2^{y_2}B_3^{y_3} = B_1^{z_1}B_2^{z_2}B_3^{z_3}$ are two factorizations of B into irreducibles. For each element s of S, we may count the number of times s appears in each factorization. This yields the equations $4y_1+2y_3 = 4z_1+2z_3$ and $2y_2+y_3 = 2z_2+z_3$, hence $y_1-z_1 = (z_3-y_3)/2 = y_2-z_2$ and

$$(y_1 + y_2 + y_3) - (z_1 + z_2 + z_3) = (z_3 - y_3) + (y_3 - z_3) = 0.$$

Thus, while factorizations may not be unique (as $B_1B_2 = B_3^2$), the lengths of these factorizations will always be the same. So in contrast to $\mathcal{B}(\mathbb{Z}_4)$, $\mathcal{B}(\mathbb{Z}_4, S)$ is half factorial (an alternate proof of this will be developed in Section 5 using Lemma 5.10).

Example 3.2 shows that $\mathcal{B}(\mathbb{Z}_4)$ is not half factorial. In fact, only two abelian groups yield a half-factorial block monoid $\mathcal{B}(G)$.

Proposition 3.3. *Let G be an abelian group. The following statements are equivalent.*

1. *$\mathcal{B}(G)$ is factorial.*
2. *$\mathcal{B}(G)$ is half factorial.*
3. *$|G| \leq 2$.*

Proof. (1) $\Rightarrow$ (2) since every factorial monoid is half factorial.

(2) $\Rightarrow$ (3) Suppose $\mathcal{B}(G)$ is half factorial and that $|G| > 3$. Then G has two distinct nonzero elements g_1 and g_2 with $g_3 = g_1 + g_2 \neq 0$ and $g_3 \neq g_1, g_2$. The blocks $A_1 = (-g_3)^1 g_1^1 g_2^1$, $A_2 = g_3^1(-g_1)^1(-g_2)^1$, $B_1 = g_1^1(-g_1)^1$, $B_2 = g_2^1(-g_2)^1$, and $B_3 = g_3^1(-g_3)^1$ are all irreducibles of $\mathcal{B}(G)$. But $A_1A_2 = B_1B_2B_3$, so $B(G)$ is not half factorial, a contradiction. Hence $|G| \leq 3$. If $|G| = 3$, then $G \cong \mathbb{Z}_3$. If $A = \overline{1}^3$, $B = \overline{2}^3$, and $C = \overline{1}^1\overline{2}^1$, then $AB = C^3$ and $\mathcal{B}(\mathbb{Z}_3)$ is not half factorial. Hence, we conclude that $|G| \leq 2$.

(3) $\Rightarrow$ (1) Our condition forces $G \cong \{0\}$ or $\mathbb{Z}_2$. In the first case the only irreducible of $\mathcal{B}(\{0\})$ is 0^1, and in $\mathcal{B}(\mathbb{Z}_2)$ the irreducibles are 0^1 and 1^2. All three irreducibles are prime, so both these block monoids are factorial. □

In contrast, every nontrivial finite abelian group G has a nontrivial subset S such that the restricted block monoid $\mathcal{B}(G, S)$ is half factorial. This can be done with the added condition that the set S generate the group G. To see this, if $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ then let e_i represent the element of G with 1 in the ith coordinate and zero elsewhere. Set $S = \{e_1, \ldots, e_k\}$. Then clearly S generates G and the irreducible blocks of $\mathcal{B}(G, S)$ are $B_i = e_i^{n_i}$ for each i. Elementary arguments show that all these irreducibles are prime, so $\mathcal{B}(G, S)$ is half factorial (in fact, factorial). As Example 3.2 illustrates, half-factorial examples also exist where not all the irreducibles are prime.

We compile a few basic facts about block monoids. The statement about irreducible blocks can be seen as an analogy to part (3) of Proposition 2.3: in both cases we want to exclude the existence of a subset whose terms sum to zero.

Proposition 3.4. *Let G be an abelian group and S a nonempty subset of G.*

1. *The block $B = \prod_{g \in S} g^{v_g} \neq E$ is irreducible in $\mathcal{B}(G, S)$ if and only if for each nonempty subset T of S we have $\sum_{g \in T} v'_g g \neq 0$ for any integers v'_g with $0 \leq v'_g \leq v_g$ where at least one $v'_g \neq 0$ and at least one $v'_g < v_g$.*
2. *If $B \neq E$ in $\mathcal{B}(G, S)$, then B can be written as a product of irreducible blocks in $\mathcal{B}(G, S)$.*
3. *If $0 \in S$, then the block 0^1 is prime in $\mathcal{B}(G, S)$.*
4. *If G is finite, then $\mathcal{B}(G, S)$ contains finitely many irreducible blocks.*

Proof. (1) ($\Rightarrow$) Suppose there exists a nonempty subset T and integers v'_g as above with $\sum_{g\in T} v'_g g = 0$. Then

$$B = \Big(\prod_{g\in T} g^{v'_g}\Big)\Big(\prod_{g\in T} g^{v_g - v'_g} \prod_{g\in S\setminus T} g^{v_g}\Big)$$

is a proper factorization of B in $\mathcal{B}(G,S)$. ($\Leftarrow$) Suppose $B = CD$ is a proper factorization of B in $\mathcal{B}(G,S)$. If $C = \prod_{g\in G} g^{v'_g}$, then setting $T = \{g \mid v'_g \neq 0\}$ we get our desired subset and integers by the definition of C being a block.

(2) If $B = \prod_{g\in S} g^{v_g}$ and $B' \neq E$ with $B'|B$, then $1 \leq |B'| \leq |B|$. So B can be expressed as a product of at most $|B|$ many nontrivial blocks. Let $B = B_1 \dots B_n$ be a product involving a maximal number of blocks; by maximality all the blocks B_i must be irreducible. The proof of (3) is obvious. (4) Since any block $B = \prod_{g\in S} g^{v_g}$ with some $v_g > \mathrm{ord}(g)$ is reducible, our result follows. □

Part (2) of the above proposition assures us that factorization in block monoids is indeed a sensible pursuit. In general domains and monoids, one must exercise caution, since factorizations into irreducibles are not guaranteed to exist (see [9]). Domains and monoids in which every element has a factorization into irreducibles are said to be *atomic*. Demonstrating that $\mathbb{Z}$ is atomic is half the Fundamental Theorem of Arithmetic. More generally, Dedekind domains are atomic; our proof of this fact shall imitate that of part (2) above.

Proposition 3.5. *If D is a Dedekind domain, then D is atomic.*

Proof. Let $G = \mathcal{C}(D)$ be the class group of D. Given a nonzero nonunit $x \in D$, there are unique prime ideals $P_1, \dots, P_k$ such that $(x) = P_1 \cdots P_k$. If a nonzero nonunit y properly divides x, then by uniqueness of the P_i, we know $(y) = \prod_{i\in S} P_i$ for some proper nonempty $S \subseteq \{1, \dots, k\}$. So x can be expressed as a product of at most k nonzero nonunits y. Let $x = y_1 \cdots y_n$ be a product involving a maximal number of nonunits y_i; by maximality the y_i are irreducible. □

4 Factorizations in Dedekind Domains and Their Relationship to Block Monoids.

In this section, we shall justify the analogues of the previous section with an explicit connection between Dedekind domains and block monoids. In order to streamline our discussion of these structures, we shall need a uniform terminology for factorizations and their lengths. Let M be a commutative, cancellative, atomic monoid, such as a block monoid $\mathcal{B}(G,S)$ or the multiplicative monoid of a Dedekind domain. Let $\mathcal{A}(M)$ represent the set of irreducible elements of M and $M^\times$ its set of units. For $x \in M\setminus M^\times$, set

$$\mathcal{L}(x) = \{n \in \mathbb{N} \mid \text{ there exist } x_1, \dots, x_n \in \mathcal{A}(M) \text{ with } x = x_1 \cdots x_n\}.$$

We will refer to $\mathcal{L}(x)$ as the *set of lengths of* x in M. We can extend $\mathcal{L}(x)$ to a global descriptor by setting

$$\mathcal{L}(M) = \{\mathcal{L}(x) \mid x \in M \backslash M^\times\}.$$

We will refer to $\mathcal{L}(M)$ as the *set of lengths of* M.

Example 4.1. To illustrate the above ideas, we compute the sets of length for the block monoid $\mathcal{B}(\mathbb{Z}_3)$. We label the irreducible blocks as

$$A_1 = \overline{0}^1,\ A_2 = \overline{1}^3,\ A_3 = \overline{2}^3,\ A_4 = \overline{1}^1\overline{2}^1.$$

If $B = \overline{0}^{x_1}\overline{1}^{x_2}\overline{2}^{x_3}$ is in $\mathcal{B}(G)$, then $x_2 + 2x_3 \equiv 0 \pmod 3$, so $x_2 \equiv x_3 \pmod 3$. Write $x_2 = 3q_2 + r$ and $x_3 = 3q_3 + r$, where $0 \le r < 3$. If $B = A_1^{y_1}A_2^{y_2}A_3^{y_3}A_4^{y_4}$, then $y_1 = x_1$, $3y_2 + y_4 = x_2$ and $3y_3 + y_4 = x_3$. So

$$y_1+y_2+y_3+y_4 = x_1+(x_2-y_4)/3+(x_3-y_4)/3+y_4 = x_1+q_2+q_3+r+(y_4-r)/3.$$

For $y_1 + y_2 + y_3 + y_4$ to be an integer, we must have $y_4 \equiv r \pmod 3$. Since the y_i are nonnegative and $(y_4 - r)/3 = q_2 - y_2 = q_3 - y_3$, it must be that $0 \le (y_4 - r)/3 \le \min\{q_2, q_3\}$. The extremal values $(y_4 - r)/3 = 0$ and $(y_4 - r)/3 = \min\{q_2, q_3\}$ both yield legitimate factorizations, as $B = A_1^{x_1}A_2^{q_2}A_3^{q_3}A_4^{r}$ and $B = A_1^{x_1}A_2^{q_2-\min\{q_2,q_3\}}A_3^{q_3-\min\{q_2,q_3\}}A_4^{3\min\{q_2,q_3\}+r}$, respectively. Thus, for the length set, we simply let $(y_4-r)/3$ run through all the integers in the interval $[0, \min\{q_2, q_3\}]$. We then obtain

$$\mathcal{L}(B) = \{x_1 + q_2 + q_3 + r + k \,|\, 0 \le k \le \min\{q_2, q_3\}\}.$$

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be factored uniquely into a product of prime numbers. Number theorists celebrate Dedekind's Fundamental Theorem of Ideal Theory for extending this result to algebraic number rings: ideals can be factored uniquely into products of prime ideals. However, as the example of 6 in $\mathbb{Z}[\sqrt{-5}]$ indicates, when one descends to the level of factoring elements, the unique factorization breaks down. To a large extent, this failure results from only being able to factor elements into irreducibles, instead of primes. In order to extend the Fundamental Theorem of Arithmetic to elements—rather than ideals—we need to part with unique factorization and understand how different products of irreducibles can combine to form elements of D. As we saw in Example 2.5, this ties in with the class group $G = \mathcal{C}(D)$ of D. In fact, elements of D correspond to blocks of $\mathcal{B}(G)$; irreducibles of D correspond to irreducible blocks of $\mathcal{B}(G)$; and the factorization of elements of D is transferred to a problem of factoring the corresponding block of $\mathcal{B}(G)$. More accurately, the block monoid we need to consider is $\mathcal{B}(G, S)$, the block monoid on G restricted to the set $S = \{g \in G \,|\, g = [P] \text{ for some prime ideal of } D\}$ of divisor classes of $\mathcal{C}(D)$ containing prime ideals. These principles are precisely formulated in the following theorem of Geroldinger, an analogue of the Fundamental Theorem of Arithmetic for elements of arbitrary Dedekind domains.

Geroldinger's theorem. *[12, Proposition 1] Let D be a Dedekind domain with divisor class group $G = \mathcal{C}(D)$, D^* the multiplicative monoid of D, and S be the set of divisor classes of $\mathcal{C}(D)$ containing prime ideals. Suppose further that for $x \in D^*$, we have $(x) = P_1 \cdots P_k$ for not necessary distinct prime ideals $P_1, \ldots, P_k$ of D. The function*

$$\varphi : D^* \to \mathcal{B}(G, S)$$

defined by

$$\varphi(x) = [P_1] \cdots [P_k]$$

is a well-defined monoid homomorphism that is surjective and preserves lengths of factorizations into irreducibles (i.e., $\mathcal{L}(x) = \mathcal{L}(\varphi(x))$ for each $x \in D^*$). Hence

$$\mathcal{L}(D) = \mathcal{L}(\mathcal{B}(G, S)).$$

Geroldinger's theorem can be extended to include the more general class of integral domains known as *Krull domains*. Details on both Krull domains and the extension can be found in [13, Sections 2.3 & 2.10].

Example 4.2. The ring of algebraic integers of $K = \mathbb{Q}(\sqrt{-23})$ is:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right] = \left\{ \frac{a+b\sqrt{-23}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

This algebraic number ring has class number 3, meaning its class group $G = \mathcal{C}(\mathcal{O}_K) \cong \mathbb{Z}_3$. In $\mathcal{O}_K$,

$$\begin{aligned} 18 &= 2 \cdot 3 \cdot 3 && (5)\\ &= 3 \cdot \frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2} && (6)\\ &= \frac{7+\sqrt{-23}}{2} \cdot \frac{7-\sqrt{-23}}{2}. && (7) \end{aligned}$$

Only the first of the factorizations can be immediately deduced (though it is not immediate that 2 and 3 are irreducible in $\mathcal{O}_K$). Using Geroldinger's theorem, we shall be able to discover the other factorizations and see that these three are the only factorizations of 18 into irreducibles. To apply Geroldinger's theorem, we must determine the factorization of (18) into prime ideals. This can be done quickly by using the classic theory of prime ramification in quadratic number fields (see [17]), but we will work out the details.

Recall that an ideal I of a Dedekind domain D is prime if and only if D/I is a field. Let $\omega = (1+\sqrt{-23})/2$ and $\overline{\omega}$ be its complex conjugate. Observe that every $x \in \mathcal{O}_K$ can be written uniquely as $x = m + n\omega$, for some $m, n \in \mathbb{Z}$, i.e. $\{1, \omega\}$ is a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. The ideal (18) factors as the product of ideals (2)(3)(3), however none of these are prime ideals since $\omega\overline{\omega} = 6$ belongs to each of the ideals, but neither ω nor $\overline{\omega}$ belongs to any of them. If we adjoin ω (or its conjugate) to these ideals, then the representation of elements of $\mathcal{O}_K$ in terms

of the basis yields, for instance, that $\mathcal{O}_K/(3,\omega) \cong \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}_3$, a field. Thus $P_1 = (2,\omega), P_2 = (2,\overline{\omega}), P_3 = (3,\omega)$, and $P_4 = (3,\overline{\omega})$ are all prime ideals. Yet $P_1P_2 = (2)$ and $P_3P_4 = (3)$, so $(18) = P_1P_2P_3^2P_4^2$ is the (unique) factorization of (18) as a product of prime ideals. We conclude $\varphi(18) = [P_1][P_2][P_3]^2[P_4]^2$.

Now we must determine which elements of $\mathbb{Z}_3$ these $[P_i]$ correspond to. Since $[P_1]$ is a nonzero element of $\mathbb{Z}_3$, it generates the group and we may without loss of generality assign it to be $\overline{1}$. Since $(2) = P_1P_2$, we have $0 = [P_1] + [P_2]$ and so $[P_2] = \overline{2}$. Similarly, $(3) = P_3P_4$, so $[P_3] = -[P_4]$. Finally, since the $P_1P_4^2 = (\frac{7-\sqrt{-23}}{2})$, we have $0 = [P_1] + 2[P_4]$, so $[P_4] = [P_1] = \overline{1}$ and thus $[P_3] = \overline{2}$.

So $\varphi(18) = \overline{1}^3\overline{2}^3$, whose only factorizations are $(\overline{1}\,\overline{2})^3$ and $(\overline{1}^3)(\overline{2}^3)$. By Geroldinger's theorem, $\mathcal{L}(18) = \mathcal{L}(\varphi(18)) = \{2,3\}$. Furthermore, the only factorizations of 18 correspond to products of the P_i that map onto one of these two factorizations. The irreducible $\overline{1}^3$ can only be created by taking $[P_1]$ and the two copies of $[P_4]$; complementarily, $\overline{2}^3$ requires $[P_2]$ and the two copies of $[P_3]$. Thus $(\overline{1}^3)(\overline{2}^3)$ corresponds to the third factorization in equation (7). The irreducible $\overline{1}\,\overline{2}$ can be expressed as $[P_1][P_2]$ or $[P_1][P_3]$ or $[P_4][P_2]$ or $[P_4][P_3]$. But we only have one instance of $[P_1]$ and one of $[P_2]$ to choose from, so we get two combinations: $([P_1][P_4])([P_2][P_3])([P_3][P_4])$, which corresponds to the factorization from equation (6), and $([P_1][P_2])([P_3][P_4])^2$, which corresponds to the factorization in equation (5).

Proof of Geroldinger's theorem. We first define our mapping $\varphi : D^* \to \mathcal{B}(G,S)$. If $d \in D$ is a nonzero nonunit, then by the Fundamental Theorem of Ideal Theory we can factor the ideal (d) as a product of prime ideals $P_1 \cdots P_k$. By Proposition 2.3, $[P_1] + \ldots + [P_k] = 0$, and by the definition of S, each $[P_i] \in S$, so the sequence of $[P_1] \cdots [P_k]$ is an element of $\mathcal{B}(G,S)$. Keep in mind here that we use multiplicative notation to write elements in $\mathcal{F}(G,S)$ and $\mathcal{B}(G,S)$, and additive notation for the group operation in G. We set $\varphi(d) = [P_1] \cdots [P_k]$. The uniqueness of the list of prime ideals factoring (d) guarantees that φ is well defined. Since $(dd') = (d)(d')$, the uniqueness of the prime ideal decomposition also gives us that $\varphi(dd') = \varphi(d)\varphi(d')$. Clearly $\varphi(u) = E$ for any unit $u \in D$ and so φ is a well-defined monoid homomorphism.

Given $g_1 \cdots g_k \in \mathcal{B}(G,S)$, then all the g_i are in S by definition of the block monoid. Hence there are prime ideals P_i such that $[P_i] = g_i$ for all $1 \le i \le k$. By Proposotion 2.3 part (1), since $0 = g_1 + \ldots + g_k = [P_1] + \ldots + [P_k]$, we know that $P_1 \ldots P_k$ is a principal ideal (d) for some $d \in D$. Then clearly $\varphi(d) = g_1 \cdots g_k$ and so φ is surjective.

Let $\varphi(d) = B = g_1 \cdots g_k$ and suppose $B = CT$ in $\mathcal{B}(G,S)$. Then $C = \prod_{i \in I} g_i$ for some subset $I \subseteq \{1,\ldots,k\}$. But these g_i are $[P_i]$ for prime ideals P_i that divide (d). Since $C \in \mathcal{B}(G,S)$, we know $\sum_{i \in I}[P_i] = 0$ and so by Proposition 2.3 (1), $\prod_{i \in I} P_i = (a)$ for some $a \in D$. But $(a) \supseteq \prod_{i=1}^{k} P_i = (d)$ and thus $d = ab$ for some $b \in D$. Note that $\varphi(a) = C$. Since $T = \prod_{i \notin I} g_i$, it is clear that $\varphi(b) = T$.

From this, several statements immediately follow. First, $d \in D$ is irreducible

if and only if $\varphi(d)$ is irreducible in $\mathcal{B}(G, S)$. Second, every factorization of d into irreducibles corresponds to a factorization of $\varphi(d)$ into irreducibles and, conversely, every factorization of $\varphi(d)$ into irreducibles can be pulled back by φ to a factorization of d. The equality of length sets is immediate. □

In the course of the above proof, it is important to note that the set S is precisely the subset of the class group we must use: the blocks mapped to by φ can only use elements of the class group that correspond to prime ideals. In general, S will be a proper subset of G (see [13, Theorem 3.7.8]), so we must be careful to distinguish S from G. However, when $D = \mathcal{O}_K$ is the ring of integers of a finite extension K of the rationals, Proposition 2.1 part (3) states that $S = G$, so Geroldinger's theorem establishes a correspondence between $\mathcal{O}_K$ and the full block monoid $\mathcal{B}(G)$ over the class group. The following well-known theorem of Carlitz now follows as a corollary to Geroldinger's theorem with the aid of Proposition 3.3.

Carlitz's theorem. *Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then $\mathcal{O}_K$ is half factorial if and only if the class number of $\mathcal{O}_K$ is less than or equal to 2. Equivalently, $\mathcal{O}_K$ is half factorial if and only if $|\mathcal{C}(\mathcal{O}_K)| \leq 2$.*

5 Further Applications of Geroldinger's Theorem.

Geroldinger's theorem transfers factorization questions from a Dedekind domain D to a specific block monoid $\mathcal{B}(G, S)$, a purely combinatorial structure over an abelian group. We have already seen how the length set of a nonzero nonunit $d \in D$ corresponds to the length set of the block $\varphi(d) \in \mathcal{B}(G, S)$. Calculating a full length set may still be difficult at times, however length sets enjoy a rich structure which we will begin to examine in this section. Using Geroldinger's theorem, we shall develop techniques for obtaining a cursory, yet highly informative, picture of length sets.

As we have already seen in Example 3.2, the structure of the block monoid's irreducible blocks becomes vital to understanding the factorizations of its elements and, more generally, the factorization of elements in general Dedekind domains. Of key importance is the largest size of an atom, which spurs the following definition.

Definition 5.1. Let G be an abelian group. The *Davenport constant* of G is defined as

$$D(G) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G)\}.$$

If S is a nonempty subset of G, then

$$D(G, S) = \sup\{\, |B| \mid B \text{ is an irreducible element of } \mathcal{B}(G, S)\}$$

is known as the *Davenport constant* of G relative to S.

No closed formula is known that computes the Davenport constant. According to the introduction in [14], the study of the Davenport constant emanated from a series of questions posed by Davenport at the Midwestern Conference on Group Theory and Number Theory at Ohio State University in 1966. Moreover, techniques from many different branches of mathematics (including graph theory [10]) have been used to prove results concerning the Davenport constant. The Davenport constant arises in several unexpected areas. Alford, Granville and Pomerance [1] used the bound $D(G) \leq \exp(G)(1 + \log(|G|/\exp(G)))$ to prove there are infinitely many Carmichael numbers. Here $\exp(G)$ denotes the *exponent* of G, which is the least positive integer e such that $eg = 0$ for all elements g of G.

Before proceeding, we offer two elementary observations concerning $D(G)$. Recall that every finite abelian group G can be written uniquely in the form $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$, where $n_i \mid n_{i+1}$ for each $1 \leq i < k$. Clearly in this form $\exp(G) = n_k$, while the integer k is known as the *rank* of G. We write $\{e_1, \ldots, e_k\}$ for the standard basis of G, where e_i is 1 in the ith coordinate and 0 in every other coordinate. If G is a finite abelian group written in this manner, then set

$$M(G) = \Big[\sum_{i+1}^{k}(n_i - 1)\Big] + 1.$$

Proposition 5.2. *Let G be an abelian group.*

1. *If $|G| = \infty$, then $D(G) = \infty$.*
2. *If $|G| < \infty$, then $M(G) \leq D(G) \leq |G|$.*

Proof. (1) If G is infinite, select g_1 to be any nonzero element of G. We proceed recursively. Assume $g_1, \ldots, g_n$ have already been chosen. Let $G_n = \{\sum_{i\in I}(-g_i) \,|\, I \subseteq \{1, \ldots, n\}\}$, which is a finite set. Since G is infinite, we may choose $g_{n+1} \in G \backslash G_n$. Now for each $k \geq 1$, consider the element $h_k = -\sum_{i=1}^{k} g_i$. Then by construction $A_k = g_1^1 g_2^1 \cdots g_k^1 h_k^1$ is an irreducible block, which completes the argument.

(2) Suppose $|G| = n$ and $g_1, \ldots, g_{n+1}$ is a sequence of $n + 1$ elements of G. We shall show that it contains a proper zero-sum subsequence. Set $a_1 = g_1$, $a_2 = g_1 + g_2, \ldots, a_{n+1} = g_1 + \ldots + g_{n+1}$. By the Pigeonhole Principle, $a_j = a_k$ for some $j < k$. But then $0 = a_k - a_j = g_k + \ldots + g_{j+1}$ and so we have found a proper subsequence, $g_k, \ldots, g_{j+1}$, that sums to zero. By Proposition 3.4 part (1), every element of $\mathcal{B}(G)$ of size greater than n has a nontrivial block dividing it and hence is reducible. We conclude $D(G) \leq n = |G|$. For the lower bound, set $g = e_1 + \cdots + e_k$ and $B = e_1^{n_1-1} \cdots e_k^{n_k-1} g^1$. Clearly B is irreducible with size $M(G)$ and hence $M(G) \leq D(G)$. □

Example 5.3. Proposition 5.2 part (2) immediately implies that $D(\mathbb{Z}_n) = n$. However, it is possible for the upper inequality in part (2) to be strict. Indeed, one can readily verify that $D(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 3$. According to [18], Erdős conjectured in the mid-sixties that $D(G) = M(G)$. It was not until the publication of [21]

in 1969 that this conjecture was disproved. In particular, [21] shows that both the groups $G_1 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$ and $G_2 = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6$ are counterexamples. The group G_1 is the smallest counterexample with respect to order and the group G_2 is the smallest known counterexample with respect to rank. Indeed, by [6, Theorem 1.8] if G is of rank less than or equal to 2, then $D(G) = M(G)$. It is unknown whether there is a counterexample of rank 3, and this, in fact, is an active area of research (see [11]).

Suppose D is a Dedekind domain with class group G and let $S \subseteq G$ be the set of divisor classes containing prime ideals. If G is finite, then so is the Davenport constant $D(G, S)$ and there is an irreducible $B \in \mathcal{B}(G)$ with $|B| = D(G, S)$. By the surjectivity of φ in Geroldinger's theorem, there is a $d \in D^*$ with $\varphi(d) = B$. This d must be irreducible and (d) factors as a product of $D(G, S)$ many prime ideals. On the other hand, Geroldinger's theorem tells us that any irreducible d' must correspond to an irreducible $\varphi(d)$ and hence (d') factors as at most $D(G, S)$ many prime ideals. The Davenport constant $D(G, S)$ therefore is the greatest number of prime ideals to appear in a factorization of a principal ideal generated by an irreducible element. In contrast, if G is infinite then $D(G)$ is infinite and there is no bound on the number of prime ideals appearing in a factorization of a principal ideal generated by an irreducible.

When we consider factorizations of arbitrary elements of D^*, the Davenport constant $D(G, S)$ manifests even more prominently as a bound. To describe this restriction, we introduce some additional terminology from the theory of non-unique factorizations (see [13]). For M a commutative, cancellative, atomic monoid and $x \in M \backslash M^\times$ set

$$L(x) = \sup\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}$$

and

$$l(x) = \inf\{n \mid \text{there are } x_1, \ldots, x_n \in \mathcal{A}(M) \text{ such that } x = x_1 \cdots x_n\}.$$

While $1 \leq l(x) < \infty$ it may be that $L(x) = \infty$ (examples of x with $L(x) = \infty$ can be constructed using semigroup rings as in [2, Example 2.1]). The *elasticity of* x is defined as

$$\rho(x) = \frac{L(x)}{l(x)}.$$

We can again extend this definition to all of M by setting

$$\rho(M) = \sup\{\rho(x) \mid x \in M \backslash M^\times\}$$

and call $\rho(M)$ the *elasticity of* M. Intuitively speaking, the elasticity $\rho(M)$ bounds how much a product of irreducibles can be "stretched" into a longer product of irreducibles, or "compressed" into a shorter product of irreducibles. A good general reference on elasticity can be found in [3].

Example 5.4. Reconsider Example 4.1, where we obtained an explicit formula for $\mathcal{L}(B)$ for blocks $B \in \mathcal{B}(\mathbb{Z}_3)$. From this formula, we see $\rho(B) =$

$1 + \min\{q_2, q_3\}/(x_1 + q_2 + q_3 + r)$. This formula is maximized when $q_2 = q_3$ and $x_1 = r = 0$, so that $\rho(\mathcal{B}(\mathbb{Z}_3)) = 3/2$. We will obtain this value much more easily in Proposition 5.5.

We shall now show how the Davenport constant can be used to compute the elasticity of a ring of algebraic integers. Doing this for a general Dedekind domain D is much more difficult, but an algorithm can be found in [7]; we shall only provide bounds. To simplify the statements, we shall assume for part of this proposition that $S = -S$, i.e. that the set of classes containing prime ideals is closed under negation.

Proposition 5.5. *Let D be a Dedekind domain with class group G and S be the set of divisor classes of $\mathcal{C}(D)$ containing prime ideals.*

1. *D is a UFD if and only if $S = \{0\}$, in which case $D(G, S) = \rho(D) = 1$.*
2. *if $D(G, S) < \infty$ and $S \neq \{0\}$, then $\rho(D) \leq \frac{D(G,S)}{2}$.*
3. *if $D(G, S) < \infty$ and $S = -S \neq \{0\}$, then $\rho(D) = \frac{D(G,S)}{2}$. Moreover, in this case there is an $x \in D^*$ with $\rho(x) = \rho(D)$.*
4. *if $D(G, S) = \infty$ and $S = -S \neq \{0\}$, then $\rho(D) = \infty$.*

Proof. (1) is simply Theorem 2.4. Hence, assume $S \neq \{0\}$ (and thus D is not a UFD). As with the bound on longest factorizations of principal ideals generated by irreducibles, the problem becomes transparent when we translate it to the framework of block monoids.

We establish (2). Assume that $D(G, S) < \infty$. By Geroldinger's theorem, for all nonunits $x \in D^*$ $L(x) = L(\varphi(x))$ and $\ell(x) = \ell(\varphi(x))$. We may write $\varphi(x)$ as $0^k A$, where $A \in \mathcal{B}(G, S)$, $k \geq 0$ and 0 does not occur in A. Since 0^1 is prime by Proposition 3.4, it must appear in every factorization of $\varphi(x)$, demonstrating that $L(\varphi(x)) = k + L(A)$ and $\ell(\varphi(x)) = k + \ell(A)$. If $A = E$ is trivial, then $\rho(\varphi(x)) = 1$, so assume A is nontrivial. Each irreducible factor of A has size at most $D(G, S)$ and at least 2 (since 0^1 is the sole block of size 1). Thus $L(A) \leq |A|/2$ and $\ell(A) \leq |A|/D(G, S)$. So

$$\rho(x) = \rho(\varphi(x)) = \frac{k + L(A)}{k + \ell(A)} \leq \frac{L(A)}{\ell(A)} \leq \frac{|A|/2}{|A|/D(G, S)} = \frac{D(G, S)}{2}.$$

To establish (3) and (4), we will find lower bounds on $\rho(D)$ by examining the elasticities of particular elements. Let $B = g_1 \cdots g_k$ be an irreducible of $\mathcal{B}(G, S)$ and, using our added assumption that $S = -S$, let $-B \in \mathcal{B}(G, S)$ be the irreducible block obtained by negating all the terms of B. Then $(B)(-B) = \prod_{i=1}^{k} [g_i(-g_i)]$ gives factorizations of $(B)(-B)$ into 2 irreducibles and k irreducibles, so $\rho(B(-B)) \geq k/2$. If $D(G, S)$ finite, we can find an irreducible B with $k = D(G, S)$, and use the surjectivity of φ (Geroldinger's theorem) to pull it back to an element of $d \in D^*$, giving $\rho(d) \geq D(G, S)/2$ (and hence equal by (2)). If $D(G, S)$ infinite, we can find irreducibles with arbitrarily large k and pull them back to get elements of D of arbitrarily large elasticity $k/2$, so $\rho(D) = \infty$. □

As mentioned before the proposition, we assumed $S = -S$ for parts (3) and (4). This is to assure that $-B \in \mathcal{B}(G,S)$ for the given block $B \in \mathcal{B}(G,S)$ that we used to bound $\rho(D)$ from below. Indeed, unless S has some symmetry under negation, we will generally have $\rho(D) < D(G,S)/2$, as in Example 3.2 where $S = \{\overline{1}, \overline{2}\}$ yielded a half-factorial block monoid but $D(G,S) = 4$. See [4, Proposition 3] for a characterization of the subsets $S \subseteq G$ which yield an equality $\rho(D) = D(G,S)/2$. While the assumption on S may seem strong, by Proposition 2.1 part (3) it is automatically satisfied by the ring of integers in a finite extension of the rationals. Along with Proposition 5.5 part (3), we obtain an easy proof of a well-known extension of Carlitz's theorem by Valenza [20].

Valenza's theorem. *Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Then*

$$\rho(\mathcal{O}_K) = \frac{D(\mathcal{C}(\mathcal{O}_K))}{2}.$$

The Davenport constant determines the elasticities of Dedekind domains (and block monoids) for which $S = -S$, yet it falls short of explaining the difference in Example 3.2 between the factorization properties of $\mathcal{B}(\mathbb{Z}_4)$ and $\mathcal{B}(\mathbb{Z}_4, \{\overline{1}, \overline{2}\})$. The following combinatorial constants are a first step in a complete explanation of this type of behavior and gaining a more fine-grained analysis of factorizations.

Definition 5.6. Let G be a finite abelian group. If $B = \prod_{g \in G} g^{v_g}$ is an element of $\mathcal{B}(G)$, then

$$\Bbbk(B) = \sum_{g \in G} \frac{v_g}{\mathrm{ord}(g)}$$

is known as the *cross number of* B in $\mathcal{B}(G)$. The constant

$$\mathbf{K}(G) = \sup\{\Bbbk(B) \mid B \text{ an irreducible of } \mathcal{B}(G)\}$$

is known as the *cross number of* G. As with the Davenport constant, we extend $\mathbf{K}(G)$ in an obvious manner to $\mathbf{K}(G,S)$.

Example 5.7. We return to Examples 3.2 and 5.3. The cross numbers of the irreducible blocks in $\mathcal{B}(\mathbb{Z}_4)$ are as follows:

$$\Bbbk(\overline{0}^1) = \Bbbk(\overline{1}^4) = \Bbbk(\overline{2}^2) = \Bbbk(\overline{3}^4) = \Bbbk(\overline{1}^2\overline{2}^1) = \Bbbk(\overline{2}^1\overline{3}^2) = 1 \text{ and } \Bbbk(\overline{1}^1\overline{3}^1) = \frac{1}{2}.$$

Hence, $\mathbf{K}(\mathbb{Z}_4) = \mathbf{K}(\mathbb{Z}_4, \{\overline{1}, \overline{2}\}) = 1$. Recall the Davenport constants were both 4 for these block monoids. For $\mathcal{B}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$, we saw earlier that the Davenport constant is 3. To compute the cross number, set $g_1 = (\overline{1}, \overline{0})$, $g_2 = (\overline{0}, \overline{1})$, $g_3 = (\overline{1}, \overline{1})$ and $e = (\overline{0}, \overline{0})$. The irreducible blocks of $\mathcal{B}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$ are

$$e^1,\ g_1^2,\ g_2^2,\ g_3^2,\ g_1^1 g_2^1 g_3^1,$$

with cross numbers

$$\Bbbk(e^1) = \Bbbk(g_1^2) = \Bbbk(g_2^2) = \Bbbk(g_3^2) = 1 \text{ and } \Bbbk(g_1^1 g_2^1 g_3^1) = 3/2.$$

Hence $\mathbf{K}(\mathbb{Z}_2 \oplus \mathbb{Z}_2) = 3/2$. That $K(G) > 1$ here is not surprising. In fact, a well known result of Krause [16] shows that a finite abelian group G has $K(G) = 1$ if and only if $G \cong \mathbb{Z}_{p^k}$ for some prime number p.

As with the Davenport constant, no closed formula for the computation of $\mathbf{K}(G)$ is known. We used an explicit example to define $M(G)$, a lower bound for $D(G)$; similarly we will obtain a lower bound for $\mathbf{K}(G)$. If $B = e_1^{n_1-1} \cdots e_k^{n_k-1} g^1$ is the irreducible block used in the proof of Proposition 5.2 (2), then set

$$K^*(G) = \Bbbk(B) = \sum_{i=1}^{k} \frac{n_i - 1}{n_i} + \frac{1}{n_k}.$$

Proposition 5.8. *Let $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ be a finite abelian group with $n_i \mid n_{i+1}$ for $1 \leq i < k$.*

1. *If B and C are in $\mathcal{B}(G)$, then $\Bbbk(BC) = \Bbbk(B) + \Bbbk(C)$.*
2. *$\mathbf{K}(G) \geq K^*(G) \geq 1$.*

Proof. (1) follows directly from the definition of the function $\Bbbk$. For (2), since B is an irreducible block of $\mathcal{B}(G)$, the first inequality follows. The second inequality is easily verified, since each summand is nonnegative, and $1/n_k$ plus the final summand ($i = k$) equals 1. □

The inequality $M(G) \leq D(G)$ is known to be strict for certain groups G. In contrast, it is unknown whether there exists a finite abelian group G with $\mathbf{K}(G) > K^*(G)$. An extended discussion of this can be found in [6, Section 2].

We close this section with some basic properties concerning the cross number and its use in factorization theory. The cross number can be thought of intuitively as assigning weights to blocks and it assigns these weights additively by the above proposition. This gives us a tactic to estimate the factorization lengths of a block without factoring it. We illustrate with an example:

Example 5.9. We return again to Example 3.2, where $G = \mathbb{Z}_4$. In Example 5.7, we calculated the cross numbers of the irreducibles of $\mathcal{B}(G)$ and saw $\mathbf{K}(G) = 1$. Now, if $B = C_1 \ldots C_m$ is a factorization of a block B over G, then $\Bbbk(B) = \sum_{i=1}^{m} \Bbbk(C_i) \leq m\mathbf{K}(G) = m$, so we quickly have that $\Bbbk(B)$ is a lower bound on $L(B)$.

For a general finite abelian group, the reasoning in the example shows that $\Bbbk(B)/\mathbf{K}(G)$ is always a lower bound on $L(B)$. As we previously saw in Proposition 5.8, $\mathbf{K}(G) \geq 1$, and so $\Bbbk(B) \leq L(B)$ for all $B \in \mathcal{B}(G, S)$. The case where this lower bound achieves equality corresponds to a familiar property.

Lemma 5.10. *Let G be a finite abelian group and $S \subseteq G$. The following are equivalent:*

1. *$\Bbbk(B) = L(B)$ for all $B \in \mathcal{B}(G, S)$,*

2. $\Bbbk(A) = 1$ *for all irreducible* $A \in \mathcal{B}(G, S)$*, and*

3. $\mathcal{B}(G, S)$ *is half factorial.*

Proof. We begin by showing that (1) and (2) are equivalent. (1) $\Rightarrow$ (2) Follows since $L(B) = 1$ for all irreducibles B. (2) $\Rightarrow$ (1) If $B = C_1 \cdots C_r$ is a longest factorization of B, then $\Bbbk(B) = \sum_{i=1}^{r} \Bbbk(C_i) = r = L(B)$.

We complete the proof by showing that (2) and (3) are equivalent. (2) $\Rightarrow$ (3) If $B_1 \cdots B_r = C_1 \cdots C_s$ are two irreducible factorizations of the same element, then $r = \sum_{i=1}^{r} \Bbbk(B_i) = \sum_{i=1}^{s} \Bbbk(C_i) = s$. (3) $\Rightarrow$ (2) Let $C = \prod_{i=1}^{r} g_i^{v_i}$ be an irreducible of $\mathcal{B}(G, S)$. Let $m = \operatorname{lcm}(\operatorname{ord}(g_1), \ldots, \operatorname{ord}(g_r))$. Then $C^m = (g_1^{\operatorname{ord}(g_1)})^{v_1 m/\operatorname{ord}(g_1)} \cdots (g_r^{\operatorname{ord}(g_r)})^{v_r m/\operatorname{ord}(g_r)}$. The factorization on the right has length

$$\sum_{i=1}^{r} \frac{v_i m}{\operatorname{ord}(g_i)} = m\Bbbk(C),$$

while the one on the left has length m. By half-factoriality, $m = m\Bbbk(C)$ and $\Bbbk(C) = 1$. □

Proposition 5.5 part (3) solves the elasticity problem for Dedekind domains where each ideal class of $\mathcal{C}(D)$ contains a prime ideal. If the set of ideal classes S is properly contained in $\mathcal{C}(D)$, then the upper bound for the elasticity offered in Proposition 5.5 part (2) is often not sharp. Expanding upon the ideas in Lemma 5.10, we can use the cross number to obtain a better bound for finite groups (see [8, Examples 1.9 & 1.10] for comparisons of these bounds). Assume that G is a finite group, set

$$\mathfrak{M} = \max\{\Bbbk(B) \mid B \in \mathcal{A}(\mathcal{B}(G, S)) \text{ and } B \text{ is not prime}\}$$

and

$$\mathfrak{m} = \min\{\Bbbk(B) \mid B \in \mathcal{A}(\mathcal{B}(G, S)) \text{ and } B \text{ is not prime}\}.$$

Proposition 5.11. *[8, Corollary 1.7] If* G *is a finite abelian group and* $S \subseteq G$ *which generates* G*, then*

$$\max\{\mathfrak{M}, \mathfrak{m}^{-1}\} \leq \rho(\mathcal{B}(G, S)) \leq \frac{\mathfrak{M}}{\mathfrak{m}}. \tag{8}$$

Hence, if either $\mathfrak{M} = 1$ *or* $\mathfrak{m} = 1$*, then* $\rho(\mathcal{B}(G, S)) = \frac{\mathfrak{M}}{\mathfrak{m}}$.

Proof. If $\frac{n}{m} \geq 1$ then $\frac{n}{m} \geq \frac{n+k}{m+k}$ for k a positive integer. Hence, in computing the elasticity of $\mathcal{B}(G, S)$, we merely need consider blocks B which are not divisible by prime blocks. Thus, let B be such a block and assume that $B = A_1 \cdots A_n = C_1 \cdots C_m$ where each A_i and C_j are non-prime irreducible blocks. Now, $\Bbbk(B) \geq n \cdot \mathfrak{m}$ and $\Bbbk(B) \leq m \cdot \mathfrak{M}$. From $n \cdot \mathfrak{m} \leq m \cdot \mathfrak{M}$ we obtain that $\frac{n}{m} \leq \frac{\mathfrak{M}}{\mathfrak{m}}$ and the upper inequality in equation (8) holds.

For the lower inequality, suppose B is an irreducible block (as above) with $B = g_1^1 \cdots g_s^1$ for not necessarily distinct group elements $g_1, \ldots, g_s$. Let n_i be

the order of g_i in G. Suppose that e is the exponent of G and that $e = n_i t_i$ for each i. Then $\Bbbk(B) = \sum_{i=1}^{s} \frac{1}{n_i} = \sum_{i=1}^{s} \frac{1}{e/t_i} = (\sum_{i=1}^{s} t_i)/e$. We also have the factorization

$$B^e = (g_1^1 \cdots g_s^1)^e = (g_1^{n_1})^{t_1} \cdots (g_s^{n_s})^{t_s}$$

where each $g_i^{n_i}$ is an irreducible block of $\mathcal{B}(G, S)$. Hence, a product of e irreducibles in $\mathcal{B}(G, S)$ factors as a product of $\sum_{i=1}^{s} t_i$ irreducibles and thus $\rho(B^e) \geq \max\{\Bbbk(B), \Bbbk(B)^{-1}\}$. The lower bound now follows.

The final statement holds since clearly $\max\{\mathfrak{M}, \mathfrak{m}^{-1}\} = \frac{\mathfrak{M}}{\mathfrak{m}}$ if and only if either $\mathfrak{M} = 1$ or $\mathfrak{m} = 1$. □

Note, in general $\mathcal{B}(G, S)$, can have other primes besides 0^1. For instance, in $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, if $S = \{(\overline{1}, \overline{0}), (\overline{0}, \overline{1})\}$ then both $(\overline{1}, \overline{0})^2$ and $(\overline{0}, \overline{1})^2$ are prime. We close with an example which illustrates the utility of Proposition 5.11.

Example 5.12. Let $G = \mathbb{Z}_7$ and set $S = \{\overline{1}, \overline{3}\}$. An easy calculation yields that the irreducible blocks of $\mathcal{B}(\mathbb{Z}_7, S)$ are

$$B_1 = \overline{1}^{\,7},\ B_2 = \overline{3}^{\,7},\ B_3 = \overline{1}^{\,1}\overline{3}^{\,2},\ \text{and}\ B_4 = \overline{1}^{\,4}\overline{3}^{\,1}.$$

None of these are prime and $\Bbbk(B_1) = \Bbbk(B_2) = 1$, $\Bbbk(B_3) = \frac{3}{7}$, and $\Bbbk(B_4) = \frac{5}{7}$. It follows from Proposition 5.11 that $\rho(\mathcal{B}(\mathbb{Z}_7, S)) = \frac{7}{3} < \frac{7}{2}$ and hence is strictly less than the upper bound seen in Proposition 5.5 part (2).

Acknowledgments. The first author received support from the National Science Foundation, Grant #IRFP–0853293.

References

[1] W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Annals of Math. (2)* **139** (1994), 703–722.

[2] D.D. Anderson, D.F. Anderson and M. Zafrullah, Factorization in integral domains, *J. Pure Appl. Algebra* **69** (1990), 1-19.

[3] D.F. Anderson, Elasticity of factorizations in integral domains: a survey, *Lecture Notes in Pure and Appl. Math.* **189** (1997), 1–29.

[4] D.F. Anderson and S.T. Chapman, On the elasticities of Krull domains with finite cyclic divisor class group, *Comm. Algebra* **28** (2000), 2543–2553.

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

[6] S.T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, **171** (1995), 167-190.

[7] S.T. Chapman, J.I. García-García, P.A. García-Sánchez and J.C. Rosales, Computing the elasticity of a Krull monoid, *Linear Algebra Appl.* **336** (2001), 201–210.

[8] S.T. Chapman and W.W. Smith, An analysis using the Zaks-Skula constant of element factorizations in Dedekind domains, *J. Algebra* **159** (1993), 176–190.

[9] J. Coykendall, D.E. Dobbs, and B. Mullins, On integral domains with no atoms. *Comm. Algebra* **12** (1999), 5813–5831.

[10] S. Elledge and G. Hurlbert, An application of graph pebbling to zero-sum sequences in abelian groups, *Integers* **5** (2005), #A17.

[11] W.D. Gao, On Davenport's constant of finite abelian groups with rank three, *Discrete Math.* **222** (2000), 111-124.

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

[13] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Chapman & Hall/CRC, Boca Raton, Fl., 2006.

[14] A. Geroldinger and R. Schneider, On Davenport's Constant, *J. Comb. Theory Ser. A* **61** (1992), 147–152.

[15] T. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[16] U. Krause, A characterization of algebraic number fields with cyclic class group of prime power order, *Math. Z.* **186** (1984), 143-148.

[17] D.A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.

[18] H.B. Mann and J. Olson, Sums of sets in the elementary abelian group of type (p, p), *J. Comb. Theory* **2** (1967), 275–284.

[19] H. Pollard and H. Diamond, *The Theory of Algebraic Numbers*, The Carus Mathematical Monographs #9, The Mathematical Association of America, Providence, Rhode Island, 1975.

[20] R.J. Valenza, Elasticity of factorization in number fields, *J. Number Theory* **36** (1990), 212–218.

[21] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite abelian groups, III, Report ZW-1969-008, Math. Centre, Amsterdam (1969).

Paul Baginski received his B.S. and M.S. from Carnegie Mellon University in 2003 and his Ph.D. from the University of California, Berkeley in 2009. He is currently an NSF International Research Fellow, fulfilling his postdoctoral appointment at the Institut Camille Jordan at Université Lyon 1 in France. His non-mathematical hobbies include travel, cooking, and cinema, especially from the silent era.
Institut Camille Jordan, Université Claude Bernard Lyon 1, 21 Avenue Claude Bernard, 69622 Villeurbanne, France
baginski@gmail.com

Scott T. Chapman received his B.A. from Wake Forest University in 1981, his M.S. from the University of North Carolina at Chapel Hill in 1984 and his Ph.D. from the University of North Texas in 1987. He is currently the *Scholar in Residence* at Sam Houston State University in Huntsville, Texas. He is serving as Editor-Elect of the *American Mathematical Monthly* during 2011 and will serve a five year term as Editor starting in 2012.
Department of Mathematics and Statistics, Sam Houston State University, Box 2206, Huntsville, TX 77341-2206
scott.chapman@shsu.edu