So What is Class Number 2?

Scott T. Chapman

Abstract. Using factorization properties, we give several characterizations for a ring of algebraic integers to have class number at most 2.

1. INTRODUCTION. I was recently at an algebra colloquium when some questions involving small class numbers of algebraic number rings arose. Of the 30 or so participants, almost everyone in the room recognized that an algebraic number ring is a unique factorization domain (or UFD) if and only if its class number is one (i.e., the ideal class group of R is trivial). Almost no one in the room was aware of the following theorem of Carlitz, which is well known among mathematicians who work in the theory of nonunique factorizations (see [**12**] for a general reference to this area).

Carlitz's Theorem for Class Number 2. *[3] Let R be an algebraic number ring. R has class number at most 2 if and only if whenever $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ are irreducible elements of R with*

$$\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m \qquad (\dagger)$$

then $n = m$.

An integral domain D in which each nonzero nonunit can be factored as a product of irreducible elements is known as an *atomic domain*. An atomic domain D that satisfies the condition in Carlitz's theorem (i.e., satisfies (†)) is known as a *half-factorial domain* (or *HFD*). Notice that a UFD is an HFD and hence, if R exactly has class number 2, it is an example of an HFD that is not a UFD (the classic such example is $\mathbb{Z}[\sqrt{-5}]$ and the nonunique factorization $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$). Thus, the Carlitz theorem can be restated as follows.

Carlitz's Theorem Redux. *Let R be an algebraic number ring. R has class number at most 2 if and only if R is a half-factorial domain.*

Carlitz's theorem was the beginning of quantitative and qualitative research into nonunique factorizations in integral domains and monoids. This research began with papers concerning HFD's (see [**20**], [**22**], [**23**], and a comprehensive survey article [**6**]) and has expanded into the study of a host of combinatorial constants that measure deviation of factorizations from the UFD condition. The purpose of this article is not to deeply explore the general topic of factorization, but to give a series of factorization-inspired characterizations of class number 2. We do this solely in terms of algebraic number fields and thus avoid the abstraction and generality that more difficult factorization problems entail. Our characterizations will involve constants of increasing complexity, and in light of this, we will offer the various needed definitions directly before each result. We hope that our work gives the reader a better appreciation of Carlitz's theorem and its related substantive factorization problems. For those who want a more in-depth treatment of nonunique factorizations, several recent papers on this topic can be found in this MONTHLY ([**4**], [**11**], [**18**]).

Throughout we assume an understanding of abstract algebra at the level of [**10**] and a basic familiarity with algebraic number theory at the level of [**17**]. (An approach that might be more friendly to a novice can be found in [**9**].) For clarity, we review the basic definitions necessary for the remainder of this work. If $\mathbb{Q}$ represents the field of rational numbers, then an algebraic number field K is any finite extension of $\mathbb{Q}$. An element $\alpha \in K$ is an algebraic integer if it is a root of a monic polynomial in $\mathbb{Z}[X]$. By [**9**, Theorem 6.2], the set R of algebraic integers in K is an integral domain, which we refer to as an algebraic number ring.

When dealing with an algebraic number ring R, we use the usual notions of divisibility from the theory of integral domains. Let $\mathcal{A}(R)$ represent the set of irreducible elements (or atoms) of R, $\mathcal{U}(R)$ the set of units of R, and $R^\bullet$ the set of nonzero nonunits of R. Recall that x and y in R are associates if there is a unit $u \in R$ with $x = uy$. If x, y, and z are in R with $y = xz$, then we say that x divides y and denote this by $x \mid y$.

Let $\mathcal{I}(R)$ denote the set of ideals of R. If $x \in R$, then let (x) represent the principal ideal generated by x and $\mathcal{P}(R)$ the subset of $\mathcal{I}(R)$ consisting of principal ideals of R. For I and J in $\mathcal{I}(R)$, set

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_j \mid a_i \in I \text{ and } b_j \in J \right\}.$$

Using [**9**, Theorem 8.1], it is easy to argue that IJ is another ideal of R which is known as the product of I and J. If I, J, and K are ideals of R with $J = IK$, then we borrow the notation used above for elements and say that $I \mid J$.

Define an equivalence relation on $\mathcal{I}(R)$ by $I \sim J$ if and only if there exist α and β in R with $(\alpha)I = (\beta)J$. If $[I]$ represents the equivalence class of the ideal I under $\sim$, then by [**9**, Lemma 10.1] the operation

$$[I] + [J] = [IJ]$$

is well-defined. By [**9**, Theorem 8.13], the set $\mathcal{C}(R) = \mathcal{I}(R)/\sim$ forms an abelian group under $+$ called the class group of R. By [**9**, Theorem 10.3], $|\mathcal{C}(R)|$ is finite and is known as the class number of R. As previously mentioned, classical algebraic number theory ([**9**, Theorem 9.4]) asserts that R is a unique factorization domain if and only if its class number is one. Throughtout the rest of our work we will use freely the fact asserted in [**3**] that every ideal class of $\mathcal{C}(R)$ contains infinitely many prime ideals.

To completely understand how elements factor in an algebraic number ring R, we will need this fundamental result concerning the factorizations of ideals in R.

The Fundamental Theorem of Ideal Theory. *[**9**, Theorem 8.27] Let R be an algebraic number ring. If I is an ideal of R, then there exists a unique (up to order) list of not necessarily distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ of R such that*

$$I = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_k. \qquad (\star)$$

The key to comprehending factorizations in R lies in understanding products of the form $(\star)$ where $\sum_{i=1}^{k} [\mathfrak{p}_i] = 0$ in $\mathcal{C}(R)$ (see Lemma 1 below).

2. MORE ON THE CARLITZ CHARACTERIZATION.

We open with a few simple lemmas which will prove useful, especially in our later work. The first will characterize the irreducible elements of R in terms of the class group.

Lemma 1. *Let R be an algebraic number ring and x a nonzero nonunit of R with*

$$(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n,$$

where $n \geq 1$ and the $\mathfrak{p}_i$'s are not necessarily distinct prime ideals of R. The element x is irreducible in R if and only if

1. $\sum[\mathfrak{p}_i] = 0$, *and*
2. *if $S \subsetneq \{1, \ldots n\}$ is a nonempty subset then $\sum_{i \in S}[\mathfrak{p}_i] \neq 0$.*

Proof. ($\Rightarrow$) That $\sum[\mathfrak{p}_i] = 0$ follows from the definition of the class group. Suppose there is a proper subset S of $\{1, \ldots n\}$ with $\sum_{i \in S}[\mathfrak{p}_i] = 0$. Let $S' = \{1, \ldots, n\} - S$. Then both

$$\sum_{i \in S}[\mathfrak{p}_i] = 0 \text{ and } \sum_{i \in S'}[\mathfrak{p}_i] = 0$$

and hence there are nonunits y and z in R with

$$(y) = \prod_{i \in S} \mathfrak{p}_i \text{ and } (z) = \prod_{i \in S'} \mathfrak{p}_i.$$

Thus, there is a unit $u \in R$ with $x = uyz$ and x is not irreducible.

($\Leftarrow$) Suppose that $x = yz$ in R. By the fundamental theorem of ideal theory in R, there are nonempty subsets S, S' of $\{1, \ldots, n\}$ so that

$$(y) = \prod_{i \in S} \mathfrak{p}_i \text{ and } (z) = \prod_{i \in S'} \mathfrak{p}_i.$$

Then $\sum_{i \in S}[\mathfrak{p}_i] = 0$ contradicting condition (2). This completes the proof. ∎

Example 2. We illustrate the results of the lemma with some examples. Let $\mathfrak{p}$ be a nonprincipal prime ideal of R with $|[\mathfrak{p}]| = n$ (where $|[\mathfrak{p}]|$ represents of order of $[\mathfrak{p}]$ in $\mathcal{C}(R)$). Then

$$\mathfrak{p}^n = (x),$$

where x is irreducible in R. Moreover, if $\mathfrak{q}$ is any prime ideal taken from class $-[\mathfrak{p}]$, then

$$\mathfrak{pq} = (y),$$

where y is irreducible in R. Hence, in the case where $|\mathcal{C}(R)| = 2$, an irreducible element takes one of three forms:

(i) α where $(\alpha) = \mathfrak{p}$ for a principal prime ideal $\mathfrak{p}$ of R;
(ii) α where $(\alpha) = \mathfrak{p}^2$ for a nonprincipal prime ideal $\mathfrak{p}$ of R;
(iii) α where $(\alpha) = \mathfrak{pq}$ where $\mathfrak{p}$ and $\mathfrak{q}$ are distinct nonprincipal prime ideals of R.

In case (i), the irreducible α is actually a prime element; in case (ii), α is called *ramified*; and in case (iii), α is called *split*.

Lemma 1 implies some important finiteness conditions. A sequence of elements $g_1, \ldots, g_n$ from an abelian group G that satisfies the sum condition in the lemma (i.e., $g_1 + \cdots + g_n = 0$ and no proper subsum of this sum is zero) is known as a *minimal zero-sequence*. A good reference on the interplay between factorizations in an algebraic number ring and minimal zero-sequences is [**13**]. An elementary exercise (see for example [**5**]) shows that the number of minimal zero-sequences in a finite abelian group is finite. Since there are finitely many, there is a finite constant known as $D(G)$ that bounds above the number of elements in this minimal zero-sequence. The computation of $D(G)$, known as the Davenport constant of G, is elusive and better left to our references ([**5**] is a good source). These facts imply the following corollary.

Corollary 3. *Let $x \in R^\bullet$ where R is an algebraic number ring.*

(1) *The element x has finitely many nonasscociated irreducible factorizations.*
(2) *If x is irreducible and $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, then $k \leq D(\mathcal{C}(R))$.*

Having established that irreducible factorizations are essentially finite in number, we produce one below which will be of particular interest.

Lemma 4. *Let R be a ring of algebraic integers of class number greater than 2. Then there are not necessarily distinct irreducible elements $\alpha_1, \alpha_2, \beta_1, \beta_2$, and β_3 such that*

$$\alpha_1\alpha_2 = \beta_1\beta_2\beta_3. \qquad (\ddagger)$$

Proof. Suppose that $\mathcal{C}(R)$ contains an element g with $|g| = n > 2$. Let $\mathfrak{p}_1$ be a prime ideal of R taken from class g, $\mathfrak{p}_2$ a prime ideal taken from class $2g$, $\mathfrak{p}_3$ a prime ideal taken from class $(n-2)g$, and $\mathfrak{p}_4$ a prime ideal taken from class $(n-1)g$. (In the cases $n = 3$ or 4, you can pick these ideals distinctly.) Define the irreducible elements α, β, γ, and δ of R by

1. $(\alpha) = \mathfrak{p}_1\mathfrak{p}_4$,
2. $(\beta) = \mathfrak{p}_1^2\mathfrak{p}_3$,
3. $(\gamma) = \mathfrak{p}_2\mathfrak{p}_3$,
4. $(\delta) = \mathfrak{p}_2\mathfrak{p}_4^2$.

The ideal equation $(\mathfrak{p}_1^2\mathfrak{p}_3)(\mathfrak{p}_4^2\mathfrak{p}_2) = (\mathfrak{p}_1\mathfrak{p}_4)^2(\mathfrak{p}_2\mathfrak{p}_3)$ yields that

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

for some $u \in \mathcal{U}(R)$.

If all the nonidentity elements of $\mathcal{C}(R)$ are of order 2, then let g_1 and g_2 be such elements with $g_1 \neq g_2$. Suppose further that $g_3 = g_1 + g_2$. Thus, g_1, g_2, and g_3 are all distinct elements of $\mathcal{C}(R)$ of order 2. If $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $\mathfrak{p}_3$ are prime ideals of $\mathcal{C}(R)$ taken from the classes g_1, g_2, and g_3 respectively, then

$$\mathfrak{p}_1^2 = (\beta_1),\ \mathfrak{p}_2^2 = (\beta_2),\ \mathfrak{p}_3^2 = (\beta_3),\ \text{ and } \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 = (\alpha)$$

with β_1, β_2, β_3, and α irreducible elements of R. Thus in R we have

$$\alpha^2 = u\beta_1\beta_2\beta_3$$

for some unit u of R. This completes the proof. ∎

We are now in a position to offer a very short proof of Carlitz's theorem.

Proof of Carlitz's Theorem. ($\Leftarrow$) If R is half-factorial, then ($\ddagger$) implies that $|\mathcal{C}(R)| \leq 2$.

($\Rightarrow$) Let $x \in R^\bullet$ with

$$(x) = \mathfrak{q}_1 \cdots \mathfrak{q}_n \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$

where the prime ideals $\mathfrak{q}_i$ are principal and the prime ideals $\mathfrak{p}_j$ are not principal. By our remarks in Example 2, m is even and any factorization of x into irreducibles has length $n + \frac{m}{2}$. Thus (2) holds and the proof is complete. ∎

3. CHARACTERIZATIONS INVOLVING THE LENGTH SET. If R is an algebraic number ring and x a nonzero nonunit of R, then set

$$\mathcal{L}(x) = \{k \mid \exists \text{ irreducibles } \alpha_1, \ldots, \alpha_k \in R \text{ with } x = \alpha_1 \cdots \alpha_k\}.$$

The set $\mathcal{L}(x)$ is known as the set of lengths of x and a general MONTHLY survey on this topic can be found in [**11**]. Corollary 3 implies that $|\mathcal{L}(x)| < \infty$ for any $x \in R^\bullet$. By Carlitz's theorem, if R has class number 2, then $\mathcal{L}(x) = \{k\}$ for some $k \in \mathbb{N}_0$, and if $|\mathcal{C}(R)| > 2$, then Lemma 4 implies that there is an $x \in R$ with $|\mathcal{L}(x)| > 1$. Set

$$L(x) = \max \mathcal{L}(x),\ \ell(x) = \min \mathcal{L}(x),$$

and

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

Since $L(x) < \infty$, $\rho(x)$ is a rational $q \geq 1$ which is known as the *elasticity* of x in R. We can turn this combinatorial constant into a global descriptor by setting

$$\rho(R) = \sup\{\rho(x) \mid x \in R\}.$$

Hence, R is half-factorial if and only if $\rho(R) = 1$ and by Lemma 4, if R has class number greater than 2, then $\rho(R) \geq \frac{3}{2}$. A detailed study of elasticity in number rings can be found in [**21**] and a more general survey on the subject in [**1**]. In [**21**] it is established that

$$\rho(R) = \frac{D(\mathcal{C}(R)}{2},$$

where again $D(\mathcal{C}(R))$ represents Davenport's constant.

A more precise version of the elasticity has recently become popular in the literature. Let $k \in \mathbb{N}$ and set

$$\rho_k(R) = \sup\{\sup \mathcal{L}(x) \mid \min \mathcal{L}(x) \leq k \text{ for } x \in R^\bullet\}.$$

Using Corollary 3 along with [**12**, Proposition 1.4.2], the fact that R is an algebraic number ring yields a slightly simpler version of this definition:

$$\rho_k(R) = \sup\{\max \mathcal{L}(x) \mid k \in \mathcal{L}(x) \text{ for } x \in R^\bullet\}.$$

We prove a few convenient facts concerning the $\rho_k(R)$'s.

Lemma 5. *If R is an algebraic number ring, then the following assertions hold.*

(1) $\rho_1(R) = 1$.
(2) $\rho_k(R) \geq k$ *for all* $k \in \mathbb{N}$.
(3) *For each* $k \in \mathbb{N}$, $\rho_k(R) < \infty$.
(4) *For each* $k \in \mathbb{N}$, $\rho_k(R) < \rho_{k+1}(R)$.

Proof. The proof of (1) follows directly from the definition of an irreducible element. For (2), if x is a prime element of R, then $\mathcal{L}(x^k) = \{k\}$ so $k \in \mathcal{L}(x^k)$ and $k = \max \mathcal{L}(x^k)$. That $\rho_k(R) \geq k$ now follows.

For (3), suppose that $k \in \mathcal{L}(x)$ for some $x \in R^\bullet$. Thus $x = \alpha_1 \cdots \alpha_k$ where each $\alpha_i \in \mathcal{A}(R)$. Write each $(\alpha_i) = \mathfrak{p}_{i,1} \cdots \mathfrak{p}_{i,t_i}$ where each $\mathfrak{p}_{i,j}$ is a prime ideal of R. By our previous comment, each $t_i \leq D(\mathcal{C}(R))$. Thus, (x) factors into at most $k \cdot D(\mathcal{C}(R))$ prime ideals, which also bounds the length of a factorization of x into irreducibles. Hence $\max \mathcal{L}(x) \leq k \cdot D(\mathcal{C}(R))$ for each $x \in R^\bullet$ and thus $\rho_k(R) \leq k \cdot D(\mathcal{C}(R))$.

For (4), suppose $m = \rho_k(R)$. Then there are irreducible elements $\alpha_1, \ldots, \alpha_k$, $\beta_1, \ldots, \beta_m$ of R with $\alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_m$. If x is any irreducible element of R, then $x\alpha_1 \cdots \alpha_k = x\beta_1 \cdots \beta_m$ and hence $\rho_{k+1}(R) \geq m + 1 > \rho_k(R)$. ∎

The true relationship between $\rho(R)$ and the $\rho_k(R)$'s can be found in [**12**, Proposition 6.3.1]:

$$\rho(R) = \sup \left\{ \frac{\rho_k(R)}{k} \mid k \in \mathbb{N} \right\} = \lim_{k \to \infty} \frac{\rho_k(R)}{k}.$$

Lemma 4 again allows us to make an immediate deduction. (Part of this result can be found prior to [**12**, Proposition 1.4.2].)

Theorem 6. *Let R be an algebraic number ring. The following statements are equivalent.*

(1) *R has class number less than or equal to 2.*
(2) $\rho(R) = 1$.
(3) $\rho_2(R) = 2$.
(4) $\rho_k(R) = k$ *for some* $k \geq 2$.
(5) *For all irreducibles x and y in R,* $\mathcal{L}(xy) = \{2\}$.
(6) *For all irreducibles x and y in R,* $|\mathcal{L}(xy)| = 1$.

Proof. Assertions (1) and (2) are equivalent by the Carlitz theorem. If (2) holds, then every $\mathcal{L}(x)$ with $2 \in \mathcal{L}(x)$ is of the form $\{2\}$. Thus $\max \mathcal{L}(x) = 2$ which yields $\rho_2(R) = 2$ and (3) holds. Clearly (3) implies (4). Assume (4) holds. If R has class number greater than 2, then Lemma 4 implies that $\rho_2(R) \geq 3$. It easily follows from Lemma 5 item (4) and induction that $\rho_k(R) > k$ for all $k \geq 2$, a contradiction. Thus R has class number at most 2 and (1) holds. Hence (1), (2), (3), and (4) are equivalent.

If (3) holds, then $2 \in \mathcal{L}(x)$ implies that $2 = \max \mathcal{L}(x)$ and $\mathcal{L}(x) = \{2\}$, which yields (5). Statements (5) and (6) are equivalent by the definition of the length set. If (6) holds, then $|\mathcal{L}(xy)| = 1$ implies that $\max \mathcal{L}(xy) = 2$, which in turn yields (3). This completes the proof. ∎

Let's take a slightly different look at the length set. Given an algebraic number ring R and x a nonzero nonunit, suppose that

$$\mathcal{L}(x) = \{n_1, \ldots, n_k\}$$

where $n_1 < n_2 < \cdots < n_k$. The delta set of x is defined as

$$\Delta(x) = \{n_i - n_{i-1} \,|\, 2 \leq i \leq k\}$$

with $\Delta(x) = \emptyset$ if $k = 1$. We can convert this local descriptor into a global one by setting

$$\Delta(R) = \bigcup_{x \in R^\bullet} \Delta(x).$$

When R is a Krull domain (a more general structure than an algebraic number ring) a great deal is known about the structure of $\Delta(R)$ (see [**12**, Section 6.7] and [**19**]).

We show how the notion of the Δ-set fits in with class number 2.

Theorem 7. *Let R be an algebraic number ring. Then R has class number at most 2 if and only if $\Delta(R) = \emptyset$.*

Proof. The implication ($\Rightarrow$) clearly holds by Carlitz's Theorem. For ($\Leftarrow$), if $\Delta(R) = \emptyset$ and R has class number greater than 2, then Lemma 4 yields a contradiction. This completes the proof. ∎

4. BEYOND THE LENGTH SET. Our characterizations to this point have been solely dependent on the length set. We now consider an invariant that relies on individual factorizations as much as or more than the set $\mathcal{L}(x)$. It offers a numeric measure of how far an element is from being prime.

Definition 8. Let R be an algebraic number ring. For $x \in R^\bullet$, we define $\omega(x) = n$ if n is the smallest positive integer with the property that whenever $x \mid a_1 \cdots a_t$, where each $a_i \in \mathcal{A}(R)$, there is a $T \subseteq \{1, 2, \ldots, t\}$ with $|T| \leq n$ such that $x \mid \prod_{k \in T} a_k$. If no such n exists, then $\omega(x) = \infty$. For $x \in \mathcal{U}(R)$, we define $\omega(x) = 0$. Finally, set

$$\omega(R) = \sup\{\omega(\alpha) \,|\, \alpha \in \mathcal{A}(R)\}.$$

The definition above is taken from [**8**], but there are several other equivalent versions that can be found in the literature (see [**2**]). It follows directly from the definition that an element $x \in R$ is prime if and only if $\omega(x) = 1$. The survey paper [**18**] is a good general reference on the ω-function and we illustrate Definition 8 by appealing directly to the class number 2 case.

Example 9. Suppose that R is an algebraic number ring of class number 2. We use the classification of irreducible elements of R given in Example 2 to determine the ω-values of the irreducibles of R. If α is a prime element, then $\omega(\alpha) = 1$. So, let α be a nonprime element of $\mathcal{A}(R)$ where $(\alpha) = \mathfrak{p}^2$ for a nonprincipal prime ideal $\mathfrak{p}$ of R. Thus $\omega(x) > 1$, so suppose that $\alpha \,|\, \beta_1 \cdots \beta_r$ where each β_i is irreducible in R and $r \geq 2$. Hence, either one of the β_i's is of the form $(\beta_i) = \mathfrak{p}^2$, or there are irreducibles β_i and β_j (with $i \neq j$) so that $(\beta_i) = \mathfrak{p}\mathfrak{q}_1$ and $(\beta_j) = \mathfrak{p}\mathfrak{q}_2$ where $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are nonprincipal prime ideals of R distinct from $\mathfrak{p}$. In the first case, α is an associate of β_i and in the second, $\alpha \,|\, \beta_i\beta_j$ and hence $\omega(\alpha) = 2$. A similar argument shows that $\omega(\alpha) = 2$ if $(\alpha) = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p}$ and $\mathfrak{q}$ are distinct nonprincipal prime ideals of R.

We introduce an aid which will simplify the computation of $\omega(x)$.

Definition 10. Let $x \in R^\bullet$ where R is an algebraic number ring. A *bullet* for x is a product $\beta_1 \cdots \beta_r$ of irreducible elements $\beta_1, \ldots, \beta_r$ of R such that

(i) x divides the product $\beta_1 \cdots \beta_r$, and
(ii) for each $1 \leq i \leq r$, x does not divide $\beta_1 \cdots \beta_r/\beta_i$.

The set of bullets of x is denoted $\mathrm{bul}(x)$.

The notion of bullet gives us a nice tool to compute $\omega(x)$. To see this, if $\beta_1 \cdots \beta_r$ is a bullet for $x \in R^\bullet$, then x divides no product of the form $\beta_1 \cdots \beta_r/\beta_i$ for any i, and by definition $\omega(x) \geq r$. On the other hand, if $\alpha_1 \cdots \alpha_t$ is a product of t irreducibles of R with $x \,|\, \alpha_1 \cdots \alpha_t$ and $\alpha_1 \cdots \alpha_t$ is not a bullet of x, then some subproduct of $\alpha_1 \cdots \alpha_t$ must be a bullet. We have essentially shown the following (a complete proof can be found in [**18**, Proposition 2.10]) .

Proposition 11. *If R is an algebraic number ring and $x \in R^\bullet$, then*

$$\omega(x) = \sup\{r \,|\, \beta_1 \cdots \beta_r \in \mathrm{bul}(x) \text{ where each } \beta_i \in \mathcal{A}(R)\}.$$

Hence, for R with class number 2, Example 9 shows that $\omega(R) = 2$. Proposition 11 implies another nice finiteness condition.

Corollary 12. *Let R be an algebraic number ring and $x \in \mathcal{A}(R)$. Then*

$$\omega(x) \leq D(\mathcal{C}(R)) < \infty$$

and hence $\omega(R) \leq D(\mathcal{C}(R)) < \infty$.

In fact, the interested reader can find a proof that $\omega(R) = D(\mathcal{C}(R))$ in [**2**, Corollary 3.3].

Proof of Corollary 12. We prove only the first assertion, as the second follows directly from it. Let $x \in \mathcal{A}(R)$. Write $(x) = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_k^{t_k}$ for distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ in R. Let $\alpha_1, \ldots, \alpha_n$ be irreducibles of R such that $x \,|\, \alpha_1 \cdots \alpha_n$. For each $\mathfrak{p}_i$ choose a minimal subset $T_i \subseteq \{1, \ldots, n\}$ so that $\mathfrak{p}_i^{t_i} \,|\, (\prod_{j \in T_i} \alpha_j)$. Set $A_i = \{\alpha_j \,|\, j \in T_i\}$. By the minimality of T_i, each (α_j), with α_j in A_i, is divisible by $\mathfrak{p}_i$ and hence $|A_i| \leq t_i$. If $A = \cup_{j=1}^k A_i$, then by Corollary 3, $|A| \leq t_1 + \cdots + t_k \leq D(\mathcal{C}(R))$. By using the multiplicative properties of prime ideals, we obtain that $x \mid \prod_{\alpha_i \in A} \alpha_i$, which completes the proof. ∎

A slight adjustment in the proof of Corollary 12 yields a class number 2 characterization (see [**2**, Theorem 3.4]).

Theorem 13. *Let R be an algebraic number ring. Then R has class number at most 2 if and only if $\omega(R) \leq 2$.*

Proof. While the argument is trivial using the remark directly following Corollary 12, for completeness we offer a proof. Our work in Example 9, along with the fact that class number 1 trivially implies $\omega(R) = 1$, yields ($\Rightarrow$). For ($\Leftarrow$), assume $\omega(R) \leq 2$ and that R has class number greater than 2. We pivot in a manner similar to Lemma 4. Suppose $\mathcal{C}(R)$ has an element g with $|g| = n > 2$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct prime ideals of R with $[\mathfrak{p}_i] = g$. Let $x \in \mathcal{A}(R)$ be such that $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. If for each $1 \leq i \leq n$ the irreducible α_i is such that $(\alpha_i) = \mathfrak{p}_i^n$, then it is clear that $\alpha_1 \cdots \alpha_n$ is a bullet for x and $\omega(x) \geq n > 2$. If $\mathcal{C}(R)$ only has nontrivial elements of order 2, then let α, β_1, β_2, and β_3 be the irreducibles constructed in the second part of the proof of Lemma 4. As in the previous case, $\beta_1\beta_2\beta_3$ is a bullet for α and $\omega(x) \geq 3 > 2$. In either case, $\omega(R) > 2$, which completes the proof. ∎

5. THE GRAND FINALE! In these pages we have accomplished a lot. To demonstrate, we tie it all together in one last tribute to class number 2.

Class Number 2 in a Nutshell. *Let R be an algebraic number ring. The following statements are equivalent.*

(1) *R has class number at most 2.*
(2) *R is a half-factorial domain.*
(3) $\rho(R) = 1$.
(4) $\rho_2(R) = 2$.
(5) $\rho_k(R) = k$ *for some* $k \geq 2$.
(6) *For all irreducibles x and y in R,* $\mathcal{L}(xy) = \{2\}$.
(7) *For all irreducibles x and y in R,* $|\mathcal{L}(xy)| = 1$.
(8) $\Delta(R) = \emptyset$.
(9) $\omega(R) \leq 2$.

We note that our work has not endeavored to determine exactly how many irreducible factorizations there are of an element x in a class number 2 algebraic number ring R. If R has class number 2, then a formula for this computation is contained in [**7**]. A detailed study of the asymptotic behavior of factorizations in rings with class number 2 can be found in [**14**]. A more general approach to counting irreducible factorizations (with no restrictions on the class number) can be found in [**16**].

ACKNOWLEDGMENTS. The author gratefully acknowledges support under an Academic Leave during the fall of 2017 funded by Sam Houston State University. He would also like to thank the referees and editor Susan Colley for comments that greatly improved the exposition of this paper.

REFERENCES

1. Anderson, D. F. (1997). Elasticity of factorizations in integral domains: a survey. In: Anderson, D. D., ed. *Factorization in Integral Domains*. Lecture Notes in Pure and Appl. Math., 189. New York, NY: Marcel Dekker, pp. 1–29.
2. Anderson, D. F., Chapman, S. T. (2010). How far is an element from being prime? *J. Algebra Appl.* 9(5): 779–789.
3. Carlitz, L. (1960). A characterization of algebraic number fields with class number two. *Proc. Amer. Math. Soc.* 11: 391–392.
4. Baginski, P., Chapman, S. T. (2011). Factorizations of algebraic integers, block monoids, and additive number theory. *Amer. Math. Monthly*. 118(10): 901–920.
5. Chapman, S. T. (1995). On the Davenport constant, the cross number and their application in factorization theory. In: Anderson, D. F., Dobbs, D. E., eds. *Factorization in Integral Domains*. Lecture Notes in Pure and Appl. Math., 171. New York, NY: Marcel Dekker, pp. 167–190.
6. Chapman, S.T., Coykendall, J. (2000). Half-factorial domains, a survey. In: Chapman, S. T., Glaz, S., eds. *Non-Noetherian Commutative Ring Theory*. Mathematics and Its Applications, 520. Dordrecht: Kluwer, pp. 97–115.
7. Chapman, S. T., Herr, J., Rooney, N. (1999). A factorization formula for class number two. *J. Number Theory*. 79(1): 58–66.
8. Chapman, S. T., Puckett, W., Shour, K. (2014). On the omega values of generators of embedding dimension three numerical monoids generated by an interval. *Involve*. 7: 657–667.
9. Diamond, H., Pollard, H. (1950). *The Theory of Algebraic Numbers*. Washington, DC: Mathematical Association of America.
10. Gallian, J. (2016). *Contemporary Abstract Algebra.* 9th ed. Boston, MA: Cengage Learning.
11. Geroldinger, A. (2016). Sets of lengths. *Amer. Math. Monthly*. 123(10): 960–988.
12. Geroldinger, A., Halter-Koch, F. (2006). *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory*. New York, NY: Chapman & Hall/CRC.

13. Geroldinger, A., Ruzsa, I. Z. (2009). *Combinatorial Number Theory and Additive Group Theory*. Advanced Courses in Mathematics – CRM Barcelona. Basel, CH: Birkhäuser.
14. Halter-Koch, F. (1993). Factorization problems in class number two. *Colloq. Math.* 65(2): 255–265.
15. Larsen M., McCarthy, P. (1971). *Multiplicative Theory of Ideals*. New York, NY: Academic Press.
16. Martin, K. (2011). Nonunique factorization and principalization in number fields. *Proc. Amer. Math. Soc.* 139(9): 3025–3038.
17. Marcus, D. A. (1977). *Number Fields*, New York, NY: Springer.
18. O'Neill, C., Pelayo, R. (2015). How do you measure primality? *Amer. Math. Monthly*. 122(2): 121–137.
19. Schmid, W. (20016). Some recent results and open problems on sets of lengths of Krull monoids with finite class group. In: Chapman, S. T., Fontana, M., Geroldinger, A., Olberding, B. *Multiplicative Ideal Theory and Factorization Theory*. Cham: Springer, pp. 323–352.
20. Skula, L. (1976). On c-semigroups. *Acta Arith.* 31(3): 247–257.
21. Valenza, R. J. (1990). Elasticity of factorization in number fields. *J. Number Theory*. 36(2): 212–218.
22. Zaks, A. (1976). Half factorial domains. *Bull. Amer. Math. Soc.* 82(5): 721–723.
23. Zaks, A. (1980). Half-factorial-domains. *Israel J. Math.* 37(4): 281–302.

SCOTT CHAPMAN is Scholar in Residence and Distinguished Professor of Mathematics at Sam Houston State University in Huntsville, Texas. In December of 2016 he finished a five year appointment as Editor of the American Mathematical Monthly. His editorial work, numerous publications in the area of non-unique factorizations, and years of directing REU Programs, led to his designation in 2017 as a Fellow of the American Mathematical Society.
Department of Mathematics and Statistics, Sam Houston State University, Box 2206, Huntsville, TX 77341
Scott.chapman@shsu.edu