FINER FACTORIZATION CHARACTERIZATIONS OF CLASS NUMBER 2

SCOTT T. CHAPMAN

ABSTRACT. In **[4]**, class number 2 is characterized among algebraic number rings using basic factorization tools. In this note, we extend these characterizations using finer factorization invariants.

1. Introduction. So what is class number 2? This is a question that can have many answers. In a recent paper, **[4]**, the current author gives an answer using factorization properties of the underlying algebraic number ring R. These characterizations were based on fundamental results from the theory of non-unique factorizations (a good reference for this area is **[14]**) and relied heavily on the structure of the sets of length (denoted $\mathcal{L}(x)$) of nonzero nonunit elements $x \in R$. In this note, we pick up where **[4]** left off and prove a sequence of additional class number 2 characterizations. Our current results will largely be dependent on finer factorization invariants which require more complex tools than those of the previous paper.

In particular, we will use the notion of a *semi-length function* on R. From such a function we construct the *cross number* of an irreducible element of R and show that class number 2 is equivalent to a particular restriction that the values of these cross numbers can attain. We will also introduce the notion of a *chain* of factorizations linking one factorization of an element to another. Using these chains, we will define the notions of the *catenary* and *tame degrees*, and will again show that a restriction of the possible set of these values will define class number 2.

We assume the reader has a working knowledge of abstract algebra (at the level of **[11]**) and algebraic number theory (at the level of **[10]** or **[17]**). We open with a brief review of **[4]**. We start with Carlitz's fundamental factorization result for class number 2.

2020 *Mathematics Subject Classification.* 13F05, 13A05, 11R27.
Keywords and phrases. non-unique factorization, class number, catenary degree, tame degree, cross number.

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

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

then $n = m$.

An atomic integral domain D that satisfies the factorization condition of the Carlitz theorem (i.e., every nonzero nonunit can be factored as a product of irreducible elements and $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$ for each α_i and β_j irreducible implies that $n = m$) is called a *half-factorial domain* (or *HFD*). The survey paper **[5]** is a good general reference on this topic.

1.1. Terminology and Some Results from [4]. For an algebraic number ring R, let $\mathcal{A}(R)$ represent the set of irreducible elements of R, $R^\times$ the set of units of R, $R^\bullet$ the set of nonzero nonunits of R, and $R^* = R - \{0\}$. Recall that x and y in R are *associates*, denoted $x \sim y$, 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 $x \,|\, y$.

Let $x \in R^\bullet$ and

$$(1) \qquad x = \alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$$

where $n \leq m$ and α_i and $\beta_j \in \mathcal{A}(R)$ for each i and j. If $\alpha_i \not\sim \beta_j$ for every $1 \leq i, j \leq m$, then we call the factorization (1) *irredundant*. We note that any irreducible factorization of the form $\alpha_1\alpha_2 = \beta_1 \cdots \beta_m$ with $m > 2$ is necessarily irredundant.

If $x \in R$, then let (x) represent the principal ideal generated by x. If I, J and K are ideals of R with $J = IK$, then we borrow the notation used above for elements and say that $I \,|\, J$. We let $\mathcal{C}(R)$ represent the ideal class group of R, and of course $|\mathcal{C}(R)|$ is the class number of R. For an ideal I of R, we let $[I]$ represent the image of I in $\mathcal{C}(R)$. We will use freely the fact that every ideal class of R contains infinitely many prime ideals **[17,** Theorem 4.6]. Hence, it is always possible to reach into an ideal class $[I]$ and produce prime ideals P_1 and P_2 with $[P_1] = [P_2]$, but $P_1 \neq P_2$.

We briefly review the definitions of the various factorization invariants used in the theory of nonunique factorizations. If x is a nonzero nonunit of R, then set

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

The set $\mathcal{L}(x)$ is known as the *set of lengths* of x and a general survey on this topic can be found at **[12]**. By Carlitz's theorem, if R has class number 2, then $\mathcal{L}(x) = \{k\}$ for some $k \in \mathbb{N}$. Set

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

and

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

In our setting where R is a ring of algebraic integers, $L(x) < \infty$ (in fact, R is a finite factorization domain or FFD; see cf. Corollary 2 (1)). Hence, $\rho(x)$ 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

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

A more precise version of the elasticity has recently become popular in the literature (see **[14,** Chapter 1 Section 4]). For $k \in \mathbb{N}$ we call

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

the *kth elasticity* of R.

Given an algebraic number ring R and x a nonzero nonunit, suppose that

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

where $n_1 < n_2 < \cdots < n_k$ (again note that $n_k < \infty$ as R is an FFD). The delta set of x is defined as

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

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

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

In the interest of limiting the number of necessary definitions, we offer a slightly reduced version of the main result of **[4]**.

Factorization Characterizations for Class Number 2. *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) $\Delta(R) = \emptyset$.

To complete our work in the final 3 sections, we will require two additional lemmas from **[4]**, which we present without proof.

Lemma 1. [**4,** Lemma 1.1] *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* $\sum_{i \in S} [\mathfrak{p}_i] \neq 0$.

A sequence of elements $g_1, \ldots, g_n$ from an abelian group G which 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 *minimial zero-sequence*. It is easy to argue 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 $D(G)$ which 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 (**[3]** is a good source). The next corollary follows directly from Lemma 1.

Corollary 2. [**4,** Lemma 1.2] *Let $x \in R^\bullet$ where R is an algebraic number ring.*

(1) *The element x has finitely many non-asscociated irreducible factorizations.*
(2) *If x is irreducible and $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, then $k \leq D(\mathcal{C}(R))$.*
(3) *If R has class number greater than 2, then there exist not necessarily distinct irreducible elements $\alpha_1, \alpha_2, \beta_1, \beta_2$, and β_3 such that*

$$\alpha_1\alpha_2 = \beta_1\beta_2\beta_3. \tag{‡}$$

We will refer to a factorization of the form (‡) as a *fundamental irredundant factorization in R.*

2. A Characterization Based on the Length Set. Before exploring the characterizations promised involving the cross number and catenary degree, we briefly revisit length sets for a charaterization missed in [**4**] which is related to the notion of the delta set. Let R be an algebraic number ring and $x \in R^\bullet$. R is called a *congruence half-factorial domain* (or *CHFD*) of order r if and only if there is an integer $r > 1$ such that if

$$x = \alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m$$

for $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \mathcal{A}(R)$, then $n \equiv m \pmod r$. Notice that if R is an HFD, then R is CHFD for every $r > 1$. This definition extends in a natural sense to atomic integral domains (i.e., domains in which every nonzero nonunit can be factored as a product of irreducible elements). There are integral domains that are not CHFD for any $r > 1$, and many that are CHFD for some $r > 1$ and not HFD (for specific examples see [**8**]).

Example 3. We offer one such nontrivial example of a CHFD. A Dedekind domain is an integral domain in which every ideal factors uniquely as a product of prime ideals (see [**19**] for a general description). Hence algebraic number rings are types (or examples) of Dedekind domains in which every class of the ideal class group contains a prime ideal. In particular, the results of Lemma 1 are valid in a Dedekind domain. For our construction, we use theorems of Claborn [**9**] and Grams [**16**] which characterizes the distribution of prime ideals in the ideal class group of a Dedekind domain (a version more specific to our purposes can be found in [**15,** Theorem 5]). Let g be a generator of the abelian group $\mathbb{Z}_4$. By the results of **[9]** and **[16]**, there is a Dedekind domain D with ideal class group $\mathbb{Z}_4$ such that the nonprincipal prime ideals of D all lie in the ideal classes $[g]$ and $[g^3]$. Applying Lemma 1, we obtain that a nonprime irreducible x of D is of one of the forms

(1) $(x) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$,
(2) $(x) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$,
(3) $(x) = \mathfrak{p}_1\mathfrak{q}_1$,

where the not necessarily distinct primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ are in ideal class $[g]$ and the not necessarily distinct primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_4$ are in class $[g^3]$. Let x be a nonzero nonunit of D. If $x = x_1 \cdots x_n = y_1 \cdots y_m$ are two irreducible factorizations of x, then the prime associate factors can be canceled (with care justifying the units). Hence, this factorization of x can be reduced to irreducible factors of the types 1, 2, and 3 as illustrated above. Thus we have

$$\alpha_1 \cdots \alpha_a \beta_1 \cdots \beta_b \gamma_1 \cdots \gamma_c = \delta_1 \cdots \delta_d \epsilon_1 \cdots \epsilon_e \theta_1 \cdots \theta_f$$

where the α_i's and δ_i's are of type 1, the β_i's and ϵ_i's are of type 2, and the γ_i's and θ_i's are of type 3. By counting prime ideals from classes $[g]$ and $[g^3]$, we obtain that $4a + c = 4d + f$ and $4b + c = 4e + f$. Thus $a - b = d - e$ and

$$(a - b) + 4b + c = (d - e) + 4e + f \ \Rightarrow a + b + c + 2b = d + e + f + 2e.$$

Thus $a+b+c \equiv d+e+f \pmod 2$ and D is CHFD of order 2. D is not an HFD as the ideal equality $(\mathfrak{p}_1\mathfrak{q}_1)^4 = (\mathfrak{p}_1)^4(\mathfrak{q}_1)^4$ yields a factorization of irreducibles of the form $x^4 = y \cdot z$. The interested reader can find many of constructions such as this one in **[7]** and **[20]**.

We show how the CHFD property fits in with class number 2.

Theorem 4. *Let R be an algebraic number ring. The following statements are equivalent.*

(1) *R has class number less than or equal to 2.*
(2) $\Delta(R) = \emptyset$.
(3) *R is CHFD for all $r \geq 2$.*
(4) *R is CHFD for some $r \geq 2$.*

Proof. (1) and (2) are equivalent due to Carlitz's theorem. Clearly (2) implies (3) and (3) implies (4). So suppose (4) holds and R has class number greater than 2. Any fundamental irredundant factorization in R implies that $2 \equiv 3 \pmod{r}$ for $r > 1$, which is a contradiction. This completes the proof. □

3. A Characterization Based on Additive Number Theory. We again assume that R is an algebraic number ring. A function $R^* \to \mathbb{R}$ is called a *semi-length function* provided that

(1) $\varphi(xy) = \varphi(x) + \varphi(y)$ for all $x, y \in R^*$.
(2) $\varphi(u) = 0$ for all $u \in R^\times$.

Example 5. The Fundamental Theorem of Ideal Theory in an algebraic number ring R suggests a basic semi-length function. Define $\varphi : R \to \mathbb{R}$ by the following.

(1) If $x \in R^\bullet$ with $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ for not necessarily distinct nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, then $\varphi(x) = k$.
(2) If $x \in R^\times$, then $\varphi(x) = 0$.

It is elementary to verify that φ is a semi-length function on R. Notice if R has class number one, then φ merely counts the length of an irreducible factorization of $x \in R^\bullet$ (or is 0 on $R^\times$).

Semi-length functions have been vital in the study of elasticity. For a semi-length function φ on R, set

$$M^* = \sup\{\varphi(x) \mid x \in \mathcal{A}(R)\} \text{ and } m^* = \inf\{\varphi(x) \mid x \in \mathcal{A}(R)\}.$$

If $0 < m^* \leq M^* < \infty$, then φ is called a *bounded semi-length function* on R. If φ is a bounded semi-length function on R, then by [**1,** Theorem 1.2] it follows that

$$\rho(R) \leq \frac{M^*}{m^*}.$$

We now construct a much less straightforward semi-length function on R. For an element $x \in R^*$ with $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ and each $\mathfrak{p}_i$ a nonzero prime ideal of R, set

$$\Bbbk(x) = \sum_{i=1}^{k} \frac{1}{|[\mathfrak{p}_i]|}.$$

The value $\Bbbk(x)$ is known as the *cross number* of x in R. We leave the verification of the following simple observation to the reader.

Lemma 6. *The function* $\Bbbk : R^* \to \mathbb{R}$ *is a bounded semi-length function on* R.

Example 7. The construction of $\Bbbk$ extends naturally again to Dedekind domains with torsion ideal class groups, and we return to Example 3. If x is an irreducible of D of the form $(x) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, then

$$\Bbbk(x) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

Similarly if x is an irreducible of D of the form $(x) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$, then $\Bbbk(x) = 1$. If x is an irreducible of the form $(x) = \mathfrak{p}_1\mathfrak{q}_1$, then

$$\Bbbk(x) = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

For algebraic number rings, the image of $\mathcal{A}(R)$ under $\Bbbk$ completely determines class number 2.

Theorem 8. *If* R *is an algebraic number ring, then the following statements are equivalent:*

(1) R *has class number at most 2;*
(2) R *is a half-factorial domain;*
(3) $\Bbbk(\alpha) = 1$ *for each* $\alpha \in \mathcal{A}(R)$.

Proof. (1) and (2) are equivalent by Carlitz's Theorem. Assume (3) holds and that

$$\alpha_1 \cdots \alpha_s = \beta_1 \cdots \beta_t$$

where each α_i and $\beta_j \in \mathcal{A}(R)$. By the additivity of $\Bbbk$, $\sum_{i=1}^{s} \Bbbk(\alpha_i) = \sum_{j=1}^{t} \Bbbk(\beta_j)$ implies that $s = t$ and thus (2) holds.

So assume (2) holds and there is an irreducible $\alpha \in \mathcal{A}(R)$ with $\Bbbk(\alpha) \neq 1$. In R we have that

$$(\alpha) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

where each $\mathfrak{p}_i$ is a not necessarily distinct nonprincipal prime ideal of R. If n is the exponent of $\mathcal{C}(R)$, then for each i set $n = k_i|[\mathfrak{p}_i]|$. Thus

$$\Bbbk(\alpha) = \sum_{i=1}^{r} \frac{1}{|[\mathfrak{p}_i]|} = \frac{k_1 + \cdots + k_r}{n} \neq 1.$$

Now,

$$(\alpha)^n = \mathfrak{p}_1^n \cdots \mathfrak{p}_r^n = (\mathfrak{p}_1^{|\mathfrak{p}_1|})^{k_1} \cdots (\mathfrak{p}_r^{|\mathfrak{p}_r|})^{k_r}$$

implies that there are irreducibles $\gamma_1, \ldots, \gamma_r$ such that

$$\alpha^n = \gamma_1^{k_1} \cdots \gamma_r^{k_r}.$$

Since R is half-factorial, this implies that $n = k_1 + \cdots + k_r$. This yields that

$$\frac{k_1 + \cdots + k_r}{n} = 1,$$

a contradiction. Hence (2) implies (3) which completes the proof. □

The cross number was first defined by Krause in **[18]**. A global version of the cross number can be defined by considering the largest value of $\Bbbk(x)$ for $x \in \mathcal{A}(R)$. Computations of this global value can be as elusive as the computation of the Davenport constant, and a general discussion of this problem can be found in **[3]**.

4. A Characterization Based on the Factorization Set. We view R as a multiplicative commutative cancellative monoid. The relationship that a and b are associates in R (i.e., $a \sim b$) forms a *congruence* on R in the sense outlined in **[14,** Chapter 1]. The quotient semigroup $R/\sim$ is called the *associated reduced semigroup of* R and denoted R_{red}. Notice that R_{red} maintains the same basic multiplicative structure as R (in the sense of irreducible factorizations of an element), but has a unique unit (${R_{\text{red}}}^{\times} = [1]$).

Define the *factorization monoid of* R by

$$Z(R) = \mathcal{F}(\mathcal{A}(R_{\text{red}}))$$

where $\mathcal{F}(S)$ denotes the free abelian monoid on S. For $z \in Z(R)$ and $x \in \mathcal{A}(R_{\text{red}})$, let $v_x(z)$ denote the coefficient of x in the free basis expansion of z. The monoid homomorphism

$$\pi_R : Z(R) \to R_{\text{red}}$$

defined by

$$\pi_R(z) = \prod_{x \in \mathcal{A}(R_{\text{red}})} x^{v_x(z)}$$

is known as the *factorization homomorphism of* R. Set $|z| = \sum_{x \in \mathcal{A}(R_{\text{red}})} v_x(z)$. The *set of factorizations of* $a \in R$ is defined as

$$Z_R(a) = Z(a) = \pi_R^{-1}(aR^\times) \subset Z(R).$$

Given the above framework, we close with an analysis of the relationships between specific factorizations of a given element. Let R be an algebraic number ring and $x \in R^\bullet$ with irreducible factorizations

$$x = \alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_m.$$

We reorder the factors above so that $\alpha_i \sim \beta_i$ for $1 \leq i \leq s$ and $\alpha_i \not\sim \beta_j$ for i, j with $s+1 \leq i \leq n$ and $s+1 \leq j \leq m$. Note that while this reordering may not be unique, s will remain constant. After cancelling, we obtain

$$\alpha_{s+1} \cdots \alpha_n = u\beta_{s+1} \cdots \beta_m$$

where u is a unit of R. Set

$$\mathbf{d}(\alpha_1 \cdots \alpha_n, \beta_1 \cdots \beta_m) = \max(n-s, m-s).$$

The constant $\mathbf{d}(\alpha_1 \cdots \alpha_n, \beta_1 \cdots \beta_m)$ is known as the *distance* between the factorizations $\alpha_1 \cdots \alpha_n$, $\beta_1 \cdots \beta_m$ of x. The function $\mathbf{d}$ has properties much like a metric, and the interested reader is directed to a list in [**14,** Proposition 1.2.5]. There is one such property that we state without proof.

Lemma 9. *Let R be an algebraic number ring and $x \in R^\bullet$. Suppose that*

$$x = \alpha_1\alpha_2 = \beta_1 \cdots \beta_k \tag{2}$$

with each α_i and $\beta_j \in \mathcal{A}(R)$ where $k \geq 3$. Then

$$\mathbf{d}(\alpha_1\alpha_2, \beta_1 \cdots \beta_k) = k.$$

Let $N \in \mathbb{N}_0$. A sequence

$$z = z_0, z_1, \ldots, z_{n-1}, z_n = z'$$

of factorizations in $Z(s)$ is an N-*chain* if $\mathbf{d}(z_i, z_{i+1}) \leq N$, for each $1 \leq i \leq n-1$. The following are two key invariants studied in factorization theory. The second is in some sense a local version of the first.

Definition 10. Let $x \in R^\bullet$. Define the *catenary degree* of x (denoted $c(x)$) to be the minimal N such that there is an N-chain between any two factorizations of x. Moreover, set

$$c(R) = \sup\{c(x) \mid x \in R^\bullet\}$$

to be the *catenary degree* of R.

We note that for $x \in R^\bullet$, $c(x) = 0$ if and only if $|Z(x)| = 1$.

Definition 11.

(1) For $a \in R$ and $x \in Z(R)$, let $t(a,x) \in \mathbb{N}_0 - \{1\}$ denote the smallest $N \in \mathbb{N}_0 - \{1\}$ with the following property: If $Z(a) \cap xZ(R) \neq \emptyset$ and $z \in Z(a)$, then there exists some factorization $z' \in Z(a) \cap xZ(R)$ such that $\mathbf{d}(z, z') \leq N$. If $Z(a) \cap xZ(R) = \emptyset$, then $t(a,x) = 0$. We call $t(a,x)$ the *tame degree* of a with respect to x.

(2) The *tame degree of* R is defined as

$$t(R) = \sup\{t(a,x) \mid a \in R \text{ and } x \in Z(\mathcal{A}(R_{\text{red}})\}.$$

Example 12. The definitions above extend in a natural manner to any commutative cancellative monoid, and exact calculations of the catenary and tame degrees of various such monoids exist in the literature (for instance, see both **[6]** or **[13]**). More common are attempts to find bounds for these constants; the interested reader can find a basic summary in [**14,** Chapters 1 & 5]. To begin, we cite a very simple example where an exact calculation is possible. Let $1 < a < b$ be relatively prime positive integers and let $\langle a, b\rangle$ represent the additive submonoid of the nonnegative integers which they generate. Since $\underbrace{a + \cdots + a}_{b \text{ times}} = \underbrace{b + \cdots + b}_{a \text{ times}}$ is the minimal relation between these two generators, it is relatively easy to argue that $c(\langle a, b\rangle) = t(\langle a, b\rangle) = b$. By adding more generators, the problem becomes much more complicated. For instance, if we expand the generating set to be an arithmetic sequence of integers of the form $\langle a, a+d, \ldots, a+cd\rangle$ where $c \geq 1$, then **[6,** Theorem 14] yields that $c(\langle a, a+d, \ldots, a+cd\rangle) = \lceil \frac{a}{c} \rceil + d$ and **[6,** Theorem 20] yields that

$$t(\langle a, a+d, \ldots, a+cd\rangle) = \begin{cases} \lceil \frac{a}{c} \rceil + d & \text{if} \quad a \equiv 1 \pmod{c} \\ \lceil \frac{a}{c} \rceil + d + 1 & \text{if} \quad a \not\equiv 1 \pmod{c}. \end{cases}$$

Returning to algebraic number rings, we open with an elementary observation.

Lemma 13. *Suppose R is an algebraic number ring with an element $a \in R^\bullet$ possessing a fundamental irredundant factorization. Then $c(a) \geq 3$ and there is an element $x \in Z(\mathcal{A}(R_{\text{red}}))$ such that $t(a, x) = 3$.*

Proof. Given R, let $a = \alpha_1\alpha_2 = \beta_1\beta_2\beta_3$ be a fundamental irredundant factorization in R. Suppose that

$$z_0, z_1, \ldots, z_k$$

is a chain of factorizations in $Z(a)$ with $z_0 = \alpha_1\alpha_2$ and $z_k = \beta_1\beta_2\beta_3$. By Lemma 9, $\mathbf{d}(z_0, z_k) = 3$. Consider the sequence of integers (all ≥ 2)

$$|z_0|,\ |z_1|, \ldots, |z_k|.$$

Now, there is a first value of i (for $2 \leq i \leq k$) such that $|z_{i-1}| = 2$ and $|z_i| = t \geq 3$. If $z_i = \gamma_1 \cdots \gamma_t$, again by Lemma 9, $\mathbf{d}(z_{i-1}, z_i) = t \geq 3$. Thus $c(a) \geq 3$.

Since $\mathbf{d}(z_0, z_k) = 3$, by definition $t(a, \beta_1) \leq 3$ (viewing $\beta_1 \in Z(R)$). If $t(a, \beta_1) = 2$, then there is an irreducible $\gamma \in \mathcal{A}(R_{\text{red}})$ with $\alpha_1\alpha_2 = \beta_1\gamma$. This yields that $\gamma = \beta_2\beta_3$, contradicting the irreduciblity of γ. Thus $t(a, \beta_1) = 3$ which completes the proof. □

Lemma 13 and Corollary 2 implies the following important result.

Corollary 14. *If R is an algebraic number ring with class number greater than 2, then $c(R) \geq 3$ and $t(R) \geq 3$.*

We now show that class number 2 forces both $c(R)$ and $t(R)$ to be 2. We will require a lemma.

Lemma 15. *Let R be an algebraic number ring with class number 2, $x \in R^{\bullet}$, $z_1, z_2 \in Z(x)$, $k = \mathbf{d}(z_1, z_2) > 2$, and $y \in \mathcal{A}(R_{\text{red}})$ with $v_y(z_2) > 0$ but $v_y(z_1) = 0$. There exists an element $z_3 \in Z(x)$ with $v_y(z_3) > 0$ such that*

$$\mathbf{d}(z_1, z_3) = 2 \text{ and } \mathbf{d}(z_2, z_3) < k.$$

Proof. We note that the hypothesis yields that R is an HFD. Let x, z_1 and z_2 be as above. So suppose after reordering (if necessary), we have that

$$z_1 = \alpha_1 \cdots \alpha_n \gamma_1 \cdots \gamma_k \text{ and } z_2 = \alpha_1 \cdots \alpha_n \delta_1 \cdots \delta_k$$

where each α_i, γ_j, and δ_t is irreducible in R and $\gamma_j \not\sim \delta_t$ for any $1 \leq j \leq k$ and $1 \leq t \leq k$. Thus we obtain that

$$\gamma_1 \cdots \gamma_k = \delta_1 \cdots \delta_k. \tag{3}$$

Since the prime divisors of x have been cancelled, let's consider the remaining irreducibles in (3). If β is one of these irreducibles, then by the Fundamental Theorem of Ideal Theory in R (see [**10,** Chapter VIII]), there exists distinct nonprincipal ideals P and Q of R so that either

(1) $(\beta) = PQ$ or
(2) $(\beta) = P^2$.

In the first case, we will call β *split*, and in the second *ramified*.

Assume first that δ_1 is split. Hence, $(\delta_1) = P_1 P_2$ for distinct nonprincipal prime ideals P_1 and P_2 of R. After reordering (if necessary) the Fundamental Theorem implies that $(\gamma_1) = P_1 P_3$ and $(\gamma_2) = P_2 P_4$ where P_3 and P_4 are not necessarily distinct nonprincipal prime ideals of R. By our assumptions, $P_1 \neq P_4$ and $P_2 \neq P_3$. Thus we can write

$$\gamma_1 \gamma_2 = \delta_1 \epsilon_1$$

where $(\epsilon_1) = P_3 P_4$ and clearly this irreducible factorization is irredundant. Thus

$$\alpha_1 \cdots \alpha_n \gamma_1 \cdots \gamma_k = \alpha_1 \cdots \alpha_n \delta_1 \epsilon_1 \gamma_3 \cdots \gamma_k = \alpha_1 \cdots \alpha_n \delta_1 \cdots \delta_k.$$

Hence, if $z_3 = \alpha_1 \cdots \alpha_n \delta_1 \epsilon_1 \gamma_3 \cdots \gamma_k$, then $\mathbf{d}(z_1, z_3) = 2 < k$ and $\mathbf{d}(z_2, z_3) < k$.

The argument if δ_1 ramifies is similar, but we include it for completeness. If δ_1 ramifies, then $(\delta_1) = P_1^2$ where P_1 is a prime ideal of R. After again reordering (if necessary) we have that $(\gamma_1) = P_1P_2$ and $(\gamma_2) = P_1P_3$ where P_2 and P_3 are not necessarily distinct nonprincipal prime ideals of R with $P_1 \neq P_2$ and $P_1 \neq P_3$. Thus we can write

$$\gamma_1\gamma_2 = \delta_1\epsilon_1$$

where $(\epsilon_1) = P_2P_3$. Again

$$\alpha_1 \cdots \alpha_n\gamma_1 \cdots \gamma_k = \alpha_1 \cdots \alpha_n\delta_1\epsilon_1\gamma_3 \cdots \gamma_k = \alpha_1 \cdots \alpha_n\delta_1 \cdots \delta_k.$$

We again obtain for $z_3 = \alpha_1 \cdots \alpha_n\delta_1\epsilon_1\gamma_3 \cdots \gamma_k$, that $\mathbf{d}(z_1, z_3) = 2$ and $\mathbf{d}(z_2, z_3) < k$. This completes the proof. □

Theorem 16. [**14,** Proposition 1.7.3] *Let R be as in Theorem 1. The following statements are equivalent.*

(1) *R has class number less than or equal to 2.*
(2) *R is a half-factorial domain.*
(3) $c(R) \leq 2$.
(4) $t(R) \leq 2$.

Proof. As before, (1) and (2) are equivalent by Carlitz's Theorem. By contradiction, Corollary 14 yields that both (3) and (4) imply (1).

If we assume (1), and let $a \in R^\bullet$ and $x \in Z(\mathcal{A}(R_{\text{red}})$, then Lemma 13 implies directly that $t(a, x) = 0$ or $t(a, x) = 2$. Since not every $t(a, x) = 0$, we obtain that $t(R) = 2$. Thus (1) implies (4).

Again assuming (1), let $z_0, z_1, \ldots, z_k$ be any chain of factorizations of an element $x \in R^\bullet$. If $\mathbf{d}(z_i, z_{i+1}) > 2$, then applying Lemma 13 (repeatedly if necessary) we can construct a chain $z_i = z_{i_1}, z_{i_2}, \ldots, z_{i_w} = z_{i+1}$ where $\mathbf{d}(z_{i_j}, z_{i_{j+1}}) = 2$ for each j. Thus (1) implies (3). This completes the proof. □

The last proof can be shortened by using the general fact that $c(R) \leq t(R)$ [**14,** Theorem 1.6.6.2]. We prefer the direct approach given, which avoids much of the generalization necessary to state and prove [**14,** Theorem 1.6.6.2]. We also note that [**13,** Corollary 5.6] is much in the spirit of our Theorem 16 as it contains characterizations of Krull monoids where the class groups are at most size 2, size 3, and size 4.

5. Conclusion. We summarize our work by tying together our results from [**4**] with Theorems 4, 8, and 16 for a more indepth characterization of class number 2.

More Factorization Characterizations for Class Number 2. *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) *R is CHFD for all $r \geq 2$.*
(10) *R is CHFD for some $r \geq 2$.*
(11) $\Bbbk(\alpha) = 1$ *for each* $\alpha \in \mathcal{A}(R)$.
(12) $c(R) \leq 2$.
(13) $t(R) \leq 2$.

Acknowledgments. The author thanks the referee for many suggestions that vastly improved the paper. The author also thanks Vadim Ponomarenko, Felix Gotti, and Marly Gotti for comments on an earlier draft of this work.

REFERENCES

1. D.D. Anderson and D. F. Anderson, Elasticity of factorizations in integral domains. *J. Pure Appl. Algebra*, **80**(1992), 217–235.

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

3. S. T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, **189**(1995), 167–190.

4. S. T. Chapman, So what is class number 2?, *Amer. Math. Monthly* **126**(2019), 330–339.

5. S. T. Chapman. and J. Coykendall, Half-Factorial Domains, a Survey, Mathematics and It's Applications-Dordrecht **520**(2000), 97–116.

6. S. T. Chapman, P. García-Sánchez, D. Llena, The catenary and tame degree on numerical semigroups, *Forum Math.* **21**(2009), 117–129.

7. S. T. Chapman and W. W. Smith, On a characterization of algebraic number fields with class number less than three, *J. Algebra* **135** (1990), 381–387.

8. S. T. Chapman and W. W. Smith, On the HFD, CHFD, and k-HFD properties in Dedekind domains, *Comm. Algebra* **20**(1992), 1955–1987.

9. L. Claborn, Every abelian group is a class group, *Pacific. J. Math.* **18** (1966), 219–222.

10. H. Diamond and H. Pollard, *The Theory of Algebraic Numbers*, Washington, DC, Mathematical Association of America, 1950.

11. J. Gallian, Contemporary Abstract Algebra, Cengage Learning, 2016.

12. A. Geroldinger, Sets of lengths, *Amer. Math. Monthly* **123**(2016), 960–988.

13. A. Geroldinger, D. Grynkiewicz, and W. Schmid, Catenary degree of Krull monoids I, *J. Théor. Nombres Bordeaux* **23**(2011), 137–169.

14. A. Geroldinger, F. Halter-Koch, *Nonunique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

15. R. Gilmer, W. Heinzer, and W. W. Smith, On the distribution of prime ideals within the ideal class group, *Houston J. Math.* **22**(1996), 51–59.

16. A. Grams, The distribution of prime ideals of a Dedekind domain, *Bull. Austral. Math. Soc.* **11**(1974), 429–441.

17. G. J. Janusz, Algebraic Number Fields, second edition, Graduate Studies in Mathematics, Volume 7, American Mathematical Society, 1996.

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

19. M. Larsen and P. McCarthy, *Multiplicative Ideal Theory*, Academic Press, New York, NY, 1971.

20. A. Plagne and W. Schmid, On congruence half-factorial Krull monoids with cyclic class group, arXiv preprint arXiv:1709.00859, 2017.

Department of Mathematics and Statistics, Sam Houston State University, Huntsville, TX 77341
Email address: **scott.chapman@shsu.edu**
URL: www.shsu.edu/∼stc008/