A Closer Look at Non-Unique Factorization via Atomic Decay and Strong Atoms

Scott T. Chapman and Ulrich Krause

Abstract. Let D be an integral domain and x an irreducible (or atom) of D. We call x a *strong atom* of D if every irreducible divisor of x^k, for k a positive integer, is an associate of x. If x is not a strong atom, then there is a factorization of x of the form $x^k = x_1 \cdots x_n$ where k is minimal and each x_i is irreducible and not associated to x. In this case we say that x admits *atomic decay* with respect to $x_1, \ldots, x_n$. In this paper, we consider various implications of atomic decay in integral domains. We characterize strong atoms in a general integral domain in terms of a separation property involving prime ideals. We then use two classic examples from algebraic number theory to illustrate how atomic decay effects factorization properties in general. While we show that atomic decay behaves in a relatively mild manner in $\mathbb{Z}[\sqrt{-5}]$, we also show that its effect is much more dramatic in the subring $\mathbb{Z}[5\imath]$ of the Gaussian integers $\mathbb{Z}[\imath]$.

Keywords. Non-unique Factorization, Algebraic Number Ring, Prime Ideals, Half-factoriality.

2010 Mathematics Subject Classification. 13F15, 11R04, 20D60.

1 Introduction

In a first course in Abstract Algebra (such as one taught from [5]), the theory of integral domains culminates with the study of the factorization of elements into products of irreducible elements. Of particular interest in such a discussion are two types of elements. If D is an integral domain and x is a nonzero nonunit of D, then

(i) x is *prime* if whenever x divides yz with y and z in D, then either x divides y or x divides z;

(ii) x is *irreducible* (or an *atom*) if whenever $x = yz$ with y and z in D, then either y or z is *unit* of D (a divisor of 1).

An elementary argument shows that a prime element must be irreducible, but the converse fails (see equation $(*)$ and its accompanying description in Section 4). Moreover, it is easy to verify that a prime element p has the nice property that any atom which divides a power p^k of p must be an associate of p. We call an atom which has this property a *strong atom* (in the literature, these atoms have also been called *absolutely irreducible* [1] or [6, Definition 7.1.3], or *completely irreducible* [12]). An atom which is not strong must have a power which is divisible by a nonassociated atom. That is, powers of atoms can decay into other atoms, a phenomenon we refer to as *atomic decay*. More precisely, we have the following definition.

Definition 1.1. Let D be an integral domain and x an atom of D. We call x a *strong atom* of D if each irreducible divisor of x^k (where k is a natural number) is an associate of x. If x is not a strong atom and $x^k = x_1 \cdots x_n$ where none of the atoms $x_1, \ldots, x_n$ are associates of x and $k, n \geq 2$, then we say that x admits *atomic decay* with respect to $x_1, \ldots, x_n$.

A prime element is, of course, a strong atom, but the converse fails (see Proposition 4.1). Both prime elements and strong atoms play their roles in regard to unique factorization in an integral domain D. Recall that D is a *unique factorization domain* (also called a *UFD* or a *factorial domain*) if each nonzero nonunit of D factors into a (finite) product of atoms which is unique up to order of associated factors. It is easily verified, for an *atomic domain* D (i.e., a domain where each nonzero nonunit is a product of atoms), that D is a UFD if and only if every atom is prime. Moreover, as we shall later see, the ring of integers of an algebraic number field is a UFD if and only if each atom is a strong atom. Therefore, for these rings, we can consider nonunique factorization as being rooted in atomic decay. We will demonstrate in this case that some power of any nonzero nonunit can be factored by atomic decay into strong atoms in a unique way (up to order and associates of factors). This can be viewed as a way of restoring uniqueness without leaving the domain or the level of elements.

We break the remainder of our paper into 5 Sections. In Section 2 we characterize for a general integral domain D strong atoms using a separation property involving prime ideals. This allows us to describe, under certain conditions, strong atoms by powers of prime ideals. Section 3 deals with the ring of integers of an algebraic number field for which the conditions in Section 2 are met. Using atomic decay, we obtain the above mentioned factorization of powers of elements into strong atoms which is essentially unique. From this we draw conclusions which characterize various factorization properties in terms of the decay rate of atoms. In Section 4 we discuss in detail an example within the domain $\mathbb{Z}[\sqrt{-5}]$, well known since the time of R. Dedekind, where unique factorization breaks down. Atomic decay works in a relatively mild manner in that all atoms admit a finite and unique decay. By taking squares, two different factorizations of an element reveal hidden uniqueness. We also relate strong atoms to the ideal numbers of E. E. Kummer as viewed by E. Hecke [7]. In Section 5 we consider the failure of uniqueness in the subring $\mathbb{Z}[5\imath]$ of the Gaussian integers $\mathbb{Z}[\imath]$ which appears at first seemingly simpler than $\mathbb{Z}[\sqrt{-5}]$. Atomic decay in this case, however, is much more dramatic. The decay of some atoms never reaches strong atoms and the powers of a single atom are divisible by infinitely many nonassociated atoms. In Section 6 we conclude with some remarks and questions. We ask, for example, if there is a direct way to check whether a given atom is strong. One goal in our paper is to use tools as elementary as possible. Hence, the examples presented are appropriate for students with a limited background in Abstract Algebra. To better facilitate this, we make use of algebraic number rings, where the reader need only have knowledge of the basic facts of ideal theory, which we explicitly state. Readers who desire a deeper or more technical analysis of the theory of nonunique factorizations, are directed to

the well-known monograph of Geroldinger and Halter-Koch [6]. The authors greatly acknowledge comments on an earlier draft of this paper by Alfred Geroldinger, Nathan Kaplan and William W. Smith.

2 Strong Atoms and Prime Ideals

To later describe atomic decay in algebraic number rings, we first analyze strong atoms within the common theory of ideals. We remind the reader of some basic notions. Let D be an integral domain. A subset I of D is called an *ideal* if I is an additive subgroup of D which is closed under the multiplication by elements from D. For $x \in D$, $(x) = \{rx \mid r \in D\}$ is the *principal ideal* generated by x. If $1 \in (x)$, then x is called a *unit*. If $(x) = (y)$, then the elements x and y are *associates*. An ideal P is called a *prime ideal* if $P \neq D$ and whenever $ab \in P$ for a and b in D, then either $a \in P$ or $b \in P$. An ideal M is called a *maximal ideal* if $M \neq D$ and the only ideals containing M are M and D. It is easy to show that a maximal ideal is a prime ideal, but not conversely [5, Theorems 14.3 and 14.4]. If I and J are two ideals of D, then

$$IJ = \left\{ \sum_i a_i b_i \mid a_i \in I \text{ and } b_i \in J \right\}$$

is another ideal of D called the *product* of I and J. The product I^n of n copies of the ideal I is the *nth power of* I. For an ideal I of D, the set

$$\text{rad}(I) = \{x \in D \mid x^n \in I \text{ for some } n \in \mathbb{N}\}$$

is again an ideal called the *radical* of I.

For any integral domain D, the following lemma establishes relationships between strong atoms and prime ideals.

Lemma 2.1. *Let D be an integral domain and $x \in D$ an atom.*

(i) *The atom x is a strong atom if and only if x can be separated from any non-associated atom y by a prime ideal P in the sense that $x \notin P$ but $y \in P$.*

(ii) *If $(x) = M^k$ for some maximal ideal M and $k \in \mathbb{N}$, then x can be separated by a prime ideal from every non-associated atom y with (y) a product of prime ideals.*

(iii) *Let x be a strong atom and (x) a product of prime ideals such that for at least one prime factor P there exists an atom y such that $(y) = P^m$ for some $m \in \mathbb{N}$. Then $(x) = P^m$.*

Proof. (i) ($\Rightarrow$) Let x be a strong atom, $S = \{x^k \mid k \in \mathbb{N}_0\}$ and suppose $S \cap (y) \neq \emptyset$ for an atom y non-associated to x. Then there exists $r \in D$ and $k \in \mathbb{N}_0$ with $x^k = yr$. Since x is a strong atom it follows that x and y are associates. This is a contradiction

and we must have that $S \cap (y) = \emptyset$. By Zorn's Lemma, there exists an ideal P which is maximal with respect to $(y) \subseteq P$ and $S \cap P = \emptyset$. We show that P is a prime ideal. Suppose $a_1 a_2 \in P$ with $a_i \in D$ and $a_i \notin P$ for $i = 1, 2$. Then for the smallest ideal (P, a_i) containing P and a_i, we have for $i = 1, 2$ that $P \subsetneq (P, a_i)$ and $(P, a_i) \cap S \neq \emptyset$. Thus, there exist $s_i \in S$, $r_i \in D$ and $b_i \in P$ such that $s_i = b_i + r_i a_i$ for $i = 1, 2$. We obtain

$$s_1 s_2 = (b_1 + r_1 a_1)(b_2 + r_2 a_2) = b_1 b_2 + b_1 r_2 a_2 + b_2 r_1 a_1 + r_1 r_2 a_1 a_2.$$

Since $a_1 a_2 \in P$ it follows that $s_1 s_2 \in P$. Therefore $S \cap P \neq \emptyset$ which is a contradiction and hence P is a prime ideal. Obviously $y \in P$ and $x \notin P$ since $S \cap P = \emptyset$.

($\Leftarrow$) Assume x can be separated from every nonassociated atom y. Let $x^n = yz$ for some $n \in \mathbb{N}$ where y is an atom and $z \in D$. If y is not an associate of x, then $y \in P$ and $x \notin P$ for some prime ideal P. This implies $x^n \in P$ but $x \notin P$, a contradiction.

(ii) Suppose, for every prime ideal Q, $y \in Q$ implies $x \in Q$. We show that y must be associated to x. By assumption $(y) = P_1 \cdots P_l$ for prime ideals P_i. Since $y \in P_i$, we have $x \in P_i$ and, hence, $M^k = (x) \subseteq P_i$ for all i. If $p \in M$, then $p^k \in M^k \subseteq P_i$ and, hence, $p \in P_i$. That is, $M \subseteq P_i$ for all i. Since M is maximal we have $M = P_i$ for all i. Thus, $(x) = M^k$ and $(y) = M^l$. If $k \leq l$, then $(y) \subseteq (x)$ and if $k \geq l$, then $(x) \subseteq (y)$. In any case, since x and y are atoms, they must be associated.

(iii) Let x be a strong atom with $(x) = P_1 \cdots P_k$ and $P_i^m = (y)$ for some $i, m \in \mathbb{N}$ and atom y. If $y \in Q$ for some prime ideal Q then $P_i^m \subseteq Q$ and, hence, $P_i \subseteq Q$. Thus, $(x) \subseteq Q$ and $x \in Q$. Since x is a strong atom, y has to be associated to x by property (i). Therefore, $(x) = (y) = P_i^m$. □

As Lemma 2.1 indicates, there is a strong connection between the ideal theory of an integral domain and the factorization properties of its elements. We weigh this more carefully by considering three different ideal theoretic conditions on an integral domain D:

($\mathcal{A}$) For every atom $x \in D$ there exist prime ideals $P_1, \ldots, P_k$ of D such that $(x) = P_1 \cdots P_k$.

($\mathcal{B}$) For every nonzero prime ideal P of D, there exists a positive integer $m(P)$ such that $P^{m(P)} = (y)$ where y is an atom of D.

($\mathcal{C}$) Each nonzero prime ideal P of D is maximal.

Using these conditions, we obtain in Theorem 2.2 relationships between a strong atom x and its resulting principal ideal (x). In domains which satisfy conditions ($\mathcal{A}$), ($\mathcal{B}$), and ($\mathcal{C}$), the relationships will all be equivalent, a key fact for our work in Section 3.

Theorem 2.2. *For an atom x in an integral domain D consider the following properties.*

(a) *The ideal (x) is a power of a maximal ideal.*

(b) *The ideal* $\mathrm{rad}(x)$ *is a maximal ideal.*

(c) *The atom x is a strong atom.*

(d) *The ideal (x) is a power of a prime ideal.*

In an integral domain D the following relationships hold.

(i) $(a) \Rightarrow (b)$.

(ii) *If D satisfies* $(\mathcal{C})$, *then* (d) $\Rightarrow$ (a).

(iii) *If D satisfies* $(\mathcal{A})$, *then* (b) $\Rightarrow$ (a) $\Rightarrow$ (c).

(iv) *If D satisfies* $(\mathcal{A})$ *and* $(\mathcal{B})$, *then* (c) $\Rightarrow$ (d).

Hence, if D satisfies $(\mathcal{A})$, $(\mathcal{B})$ *and* $(\mathcal{C})$, *then conditions* (a)–(d) *are equivalent.*

Proof. (i) If $y \in \text{rad}(x)$, then $y^m \in (x) = M^k \subseteq M$ for some maximal ideal M. Since M must be a prime ideal, we have that $y \in M$. Conversely, $y \in M$ implies $y^k \in M^k = (x)$ and, hence, $y \in \text{rad}(x)$. Thus (a) $\Rightarrow$ (b).

The proof of (ii) is obvious.

(iii) Suppose that for each atom y there are prime ideals $P_1, \ldots, P_k$ such that $(y) = P_1 \cdots P_k$. We show that (b) $\Rightarrow$ (a) $\Rightarrow$ (c). Let $\text{rad}(x) = M$ be a maximal ideal. By assumption, $(x) = P_1 \cdots P_k$ with prime ideals P_i. If $y \in M = \text{rad}(x)$, then $y^n \in (x) \subseteq P_i$ and $y \in P_i$. Therefore $M \subseteq P_i$ for all $1 \leq i \leq k$. M a maximal ideal implies $P_i = M$ for all i and $(x) = M^k$. This proves (b) $\Rightarrow$ (a). Furthermore, let $(x) = M^k$ where M is a maximal ideal. From Lemma 2.1 (ii) and (i), it follows that x is a strong atom.

(iv) We note that (c) $\Rightarrow$ (d) follows from Lemma 2.1 (iii). The final statement now easily follows. □

3 Atomic Decay in the Ring of Integers of an Algebraic Number Field

The relationship between strong atoms and ideals given in Theorem 2.2 for integral domains in general becomes particularly neat for the special class of algebraic number rings. First we review some basic notation. An (algebraic) *number field* is a field $K = \mathbb{Q}(\theta)$ obtained as the smallest field containing the rational numbers $\mathbb{Q}$ and a root θ of a polynomial with coefficients in $\mathbb{Z}$. The *ring of integers* of a number field K is the set of all elements in K which are roots of a monic polynomial with coefficients in $\mathbb{Z}$. To describe atomic decay within the ring of integers D of a number field, we will use the following well-known basic facts about the ideal theory in D. Proofs of these facts can be found in [10] or [11].

- **The Fundamental Theorem of Ideal Theory.** *Let I be an nonzero ideal of D with $I \neq D$. There exists a unique (up to order) sequence of prime ideals $P_1, \ldots, P_k$ of D such that $I = P_1 \cdots P_k$.*
- For each (nonzero) prime ideal P there exists $m(P) \in \mathbb{N}$ such that $P^{m(P)}$ is the principal ideal generated by an atom.
- Every (nonzero) prime ideal is a maximal ideal.

By these facts, the properties (a)–(d) in Theorem 2.2 are equivalent for a ring D of integers and strong atoms can be described in greater detail.

Theorem 3.1. *Let D be the ring of integers of a number field.*

(i) *An element $x \in D$ is a strong atom if and only if x is an atom and* $\mathrm{rad}(x)$ *is a prime ideal, or, equivalently, if (x) is a minimal power of a prime ideal.*

(ii) *For each nonzero nonunit $x \in D$, there exists a sequence $x_1, \ldots, x_k$ of strong atoms and a minimal $m \in \mathbb{N}$ such that*

$$x^m = x_1 \cdots x_k \tag{AD}$$

where this representation by atomic decay is unique up to ordering and associates for the $x_1, \ldots, x_k$.

Proof. (i) Follows from Theorem 2.2 according to the equivalence of (a)–(d). Hence, (x) is a minimal power of P if $(x) = P^{m(P)}$. (ii) By the Fundamental Theorem, $(x) = P_1 \cdots P_k$ for nonzero prime ideals $P_1, \ldots, P_k$ of D. Furthermore, $P_i^{m(P_i)} = (y_{P_i})$ for every prime ideal P_i, with $m(P_i) \in \mathbb{N}$ and, by (i), y_{P_i} a strong atom. Let $m = \mathrm{lcm}\{m(P_i) \mid 1 \le i \le k\}$ and for each i set $m = m(P_i)n(P_i)$. Then it follows that $(x)^m = (x^m) = \prod_{i=1}^k P_i^m = \prod_{i=1}^k (y_{P_i})^{n(P_i)}$. Therefore, there exist associates x_{P_i} of y_{P_i}, strong atoms again, such that $x^m = \prod_{i=1}^k x_{P_i}^{n(P_i)}$.

Concerning the uniqueness of this representation, assume $\prod_{i=1}^k v_i^{k_i} = \prod_{j=1}^l w_j^{l_j}$ for strong atoms v_i, w_j and k_i, $l_j \in \mathbb{N}$; the v_i, as well as the w_j are to be pairwise different. By property (i), we have $(v_i) = P_i^{n_i}$, $(w_j) = Q_j^{m_j}$ for nonzero prime ideals P_i and Q_j. Therefore

$$\prod_{i=1}^{k} P_i^{n_i k_i} = \prod_{j=1}^{l} Q_j^{m_j l_j}.$$

From the uniqueness property of the Fundamental Theorem we have $k = l$ and there is a permutation σ of $\{1, \ldots, k\}$ such that $Q_i = P_{\sigma(i)}$, $m_i = n_{\sigma(i)}$, $l_i = k_{\sigma(i)}$. Therefore, $(w_i) = (v_{\sigma(i)})$ and the representation is unique up to order and associates of factors. □

The condition in Theorem 3.1 (ii) has been studied in general. In [4], the current authors define an integral domain D to be a *Cale domain* with base $B \subseteq D$ if a power of every nonzero nonunit of D can be written uniquely as a product of elements from B. For an algebraic ring of integers, the representation (AD) is known as the *Cale representation* of x. It is an interesting feature of (AD) that the representation as well as the definition of strong atoms is purely multiplicative. This is different for the unique representation according to the Fundamental Theorem of Ideal Theory, which does involve the addition operation of the ring. The reader interested in the general Cale concept may find a more technical discussion in [3] or [4].

As a further consequence, we obtain the following characterization of unique factorization into atoms for rings of algebraic integers.

Corollary 3.2. *The ring of integers D of a number field is a UFD if and only if D does not have atomic decay. That is, every atom is a strong atom.*

Proof. Using the norm function (see Section 4 or [10, 11]), it is easily argued that any element of D is a product of atoms. ($\Leftarrow$) If every atom is strong, then by Theorem 3.1 (ii) D is a UFD. ($\Rightarrow$) Assume D is a UFD. If x is an atom then

$$x^n = \underbrace{x \cdots x}_{n \text{ times}}$$

is the unique representation into atoms and any atom dividing x^n must be an associate of x. Hence, x is a strong atom. □

We note that Corollary 3.2 fails if the hypothesis that D is a ring of integers is dropped. While there are domains D with all atoms strong that are not UFDs, we are unaware of an elementary example. Many examples using the theory of Krull domains can be constructed using the main results of the recent paper [1].

If a ring of algebraic integers D is not a UFD, then D has atomic decay and the question arises how to arithmetically describe the different possible kinds of decay. A natural measure to consider is the *decay rate* of a nonzero nonunit $x \in D$, defined by

$$\vartheta(x) = \frac{k}{m}$$

where $x^m = x_1 \cdots x_k$ is the representation by decay (AD) according to Theorem 3.1 (ii). Notice that for any representation $x^n = y_1 \cdots y_l$ with strong atoms y_i one has that $\vartheta(x) = \frac{l}{n}$. Namely, $x^{mn} = (x_1 \cdots x_k)^n = (y_1 \cdots y_l)^m$ and by uniqueness $nk = ml$. The decay rate can be used to analyze two important invariants in the study of non-unique factorizations. If x is a nonzero nonunit of D, then the *elasticity* of x is defined by

$$\rho(x) = \sup\left\{\frac{k}{l} \;\middle|\; x = a_1 \cdots a_k = b_1 \cdots b_l \text{ for atoms } a_1, \ldots, a_k, b_1, \ldots, b_l \text{ of } D\right\}$$

and the elasticity of D by

$$\rho(D) = \sup\{\rho(x) \mid x \text{ a nonzero nonunit of } D\}.$$

The elasticity of a ring of algebraic integers was first studied by Valenza [13]. Notice that if D is a UFD, then $\rho(x) = 1$ for each nonzero nonunit and hence $\rho(D) = 1$. The converse of this statement is false (see Corollary 4.2). Hence, an integral domain D with $\rho(D) = 1$ is known as a *half-factorial domain* or *HFD*. The following Corollary gives a relationship between the decay rate and elasticity.

Corollary 3.3. *Let D be the ring of integers of a number field.*

(i) $\vartheta(xy) = \vartheta(x) + \vartheta(y)$ *for nonzero nonunits* $x, y \in D$.

(ii) D *is half-factorial if and only if* $\vartheta(x) = 1$ *for all atoms* x *of* D.

(iii) $\rho(D)$ *is finite if and only if*

$$\sup\{\vartheta(x), \vartheta(x)^{-1} \mid x \text{ is an atom of } D\} < \infty.$$

Proof. (i) Let $x^m = x_1 \cdots x_k$, $y^n = y_1 \cdots y_l$ be the representations of x and y by atomic decay. Then

$$(xy)^{mn} = (x^m)^n (y^n)^m = (x_1 \cdots x_k)^n (y_1 \cdots y_l)^m.$$

From the uniqueness for the representations into strong atoms, we obtain

$$\vartheta(xy) = \frac{nk + ml}{mn} = \frac{k}{m} + \frac{l}{n} = \vartheta(x) + \vartheta(y).$$

(ii) ($\Rightarrow$) If D is half-factorial, then the representation $x^m = x_1 \cdots x_k$ implies $m = k$, that is, $\vartheta(x) = 1$. ($\Leftarrow$) If $x_1 \cdots x_k = y_1 \cdots y_l$ for atoms x_i y_j then by (i) it follows that

$$k = \sum_{i=1}^{k} \vartheta(x_i) = \sum_{j=1}^{l} \vartheta(y_j) = l.$$

(iii) ($\Rightarrow$) The representation $x^m = x_1 \cdots x_k$ implies $\frac{k}{m}$, $\frac{m}{k} \le \rho(D)$ and hence if $C = \sup\{\vartheta(x), \vartheta(x)^{-1} \mid x \text{ an atom}\}$ then $C \le \rho(D)$. ($\Leftarrow$) Let $x_1 \cdots x_k = y_1 \cdots y_l$ for atoms x_i, y_i. If $\vartheta(a) = \min \vartheta(x_i)$, $\vartheta(b) = \min \vartheta(y_j)$, then from (i) it follows that

$$k\vartheta(a) \le \sum_{i=1}^{k} \vartheta(x_i) = \sum_{j=1}^{l} \vartheta(y_j) \le l\vartheta(b).$$

Therefore, $\frac{k}{l} \le \vartheta(b)\vartheta(a)^{-1}$ and C finite implies $\rho(D)$ is finite. □

The point of Corollary 3.3 is that half-factoriality or finite elasticity can be checked for rings of algebraic integers by considering only special factorizations $a_1 \cdots a_k = b_1 \cdots b_l$ where on one side all the elements are equal. With the results thus far obtained, we consider more deeply in Section 4 the failure of nonunique factorization using an example which appears frequently in many entry level textbooks. We follow this in Section 5 with an even more striking example of non-uniqueness whose decay of atoms into strong atoms does not terminate.

4 The Fundamental Example of the Failure of Unique Factorization: $\mathbb{Z}[\sqrt{-5}]$

The ring

$$D = \mathbb{Z}[\sqrt{-5}] = \{m + n\sqrt{-5} \mid m, n \in \mathbb{Z}\}$$

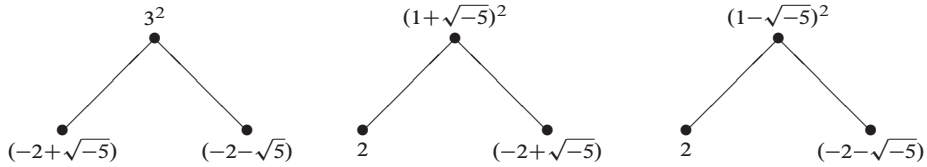
is the ring of integers of the algebraic number field $\mathbb{Q}(\sqrt{-5})$. An example of non-unique factorization into atoms in D, is

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \qquad (*)$$

That the four elements involved are nonassociated atoms of D can be easily verified using the norm function

$$N(m + n\sqrt{-5}) = m^2 + 5n^2$$

which has the property that $N(xy) = N(x)N(y)$ for $x, y \in D$. For example, to see that $1 + \sqrt{-5}$ is an atom notice $N(1 + \sqrt{-5}) = 6$ and that $1 + \sqrt{-5} = xy$ implies $N(x), N(y) \in \{1, 2, 3, 6\}$. That $N(x) = 2$ or 3 is impossible and, hence, $N(x) = 1$ or 6. $N(x) = 1$ for $x \in D$ is an equivalent condition for x to be a unit of D. Therefore, x or y must be a unit which implies that $1 + \sqrt{-5}$ is an atom. Obviously, ± 1 are the units of D and, hence, $1 + \sqrt{-5}$ is not associated to any of the other factors of $(*)$. This non-unique factorization implies also that none of the four factors is a prime element of D. Obviously, for three of the factors, we have the following diagram outlining atomic decay.



The factor 2 does not decay in a nontrivial way as shown by the following proposition.

Proposition 4.1. *The element* 2 *is a strong atom of* D *which is not prime in* D.

Proof. We have verified above that 2 is not prime in D. Suppose in D that an atom $x = m + n\sqrt{-5}$ divides a power 2^k. Then $N(x)$ must divide 2^{2k}, that is $m^2 + 5n^2 = N(x) = 2^l$ with $1 \leq l \leq 2k$. Consider this equation modulo 2. If exactly one of m and n is odd, then 2^l is odd, a contradiction. If m and n are both odd, then $m = 2m_1 + 1$ and $n = 2n_1 + 1$. Thus

$$(2m_1 + 1)^2 + 5(2n_1 + 1)^2 = 4w + 20v + 6 = 2^l$$

for integers w and v. Thus $2w + 10v + 3 = 2^{l-1}$ and $l = 1$. But $m^2 + 5n^2 = 2$ has no solutions in $\mathbb{Z}$. Thus, we must have that m and n are both even and, since x is an atom, it follows that $m = \pm 2$ and $n = 0$. Thus, any atom dividing a power of 2 in D must be equal to ± 2. □

Below we will see that the other factors $-2 \pm \sqrt{-5}$ appearing in the diagram of atomic decay are strong atoms. Thus, by squaring the non-unique factorization $(*)$, we obtain a unique factorization of 6^2 into strong atoms (i.e., the representation of Theorem 3.1 (ii)). The decay diagram also shows that all atoms in $(*)$ have decay rate equal to 1. The common view of restoring uniqueness for equation $(*)$ is to use the Fundamental Theorem of Ideal Theory as follows (see [10, page 60]). The decompositions of the factors of $(*)$ into prime ideals are

$$(2) = P^2, \quad (3) = Q \cdot Q', \quad (1 + \sqrt{-5}) = P \cdot Q \quad \text{and} \quad (1 - \sqrt{-5}) = P \cdot Q'$$

with prime ideals

$$P = (2, 1 + \sqrt{-5}), \quad Q = (3, 1 + \sqrt{-5}) \quad \text{and} \quad Q' = (3, 1 - \sqrt{-5}).$$

Thus, by taking ideals in equation $(*)$, the non-uniqueness results from different groupings of the prime ideals P, Q and Q'. The above decompositions also show that the elements 2, $-2 \pm \sqrt{-5}$ are strong atoms. Namely, $(2) = P^2$ and $(2(-2 + \sqrt{-5})) = (1 + \sqrt{-5})^2 = P^2Q^2$, hence, $(-2 + \sqrt{-5}) = Q^2$. Similarly, $(-2 - \sqrt{-5}) = Q'^2$. Therefore, according to Theorem 3.1 (i), 2 and $-2 \pm \sqrt{-5}$ are strong atoms. Thus, the representation by atomic decay (AD) according to Theorem 3.1 (ii) becomes for the element 6

$$6^2 = 2 \cdot 2 \cdot (-2 + \sqrt{-5})(-2 - \sqrt{-5}). \qquad (**)$$

By using the Fundamental Theorem as above and some further techniques from [10] and [11] involving the *class group* of D, one can argue that the decay rate of all atoms in D is 1. Thus, using Corollary 3.3 and equation $(*)$, we obtain the following.

Corollary 4.2. *D is a half-factorial domain which is not a unique factorization domain.*

Carlitz [2] was the first to recognize that $\mathbb{Z}[\sqrt{-5}]$ is half-factorial. The interested reader can find many examples of half-factorial domains which are not UFD's as well as examples of domains exhibiting various values of elasticity in [6] and [8].

One is tempted to derive from $(**)$ a factorization of 6 itself by taking square roots. Of course, the complex roots obtained will in general not belong to D and are called *ideal numbers* with respect to D. More precisely, call a complex number α an *ideal prime number* for $\mathbb{Z}[\sqrt{-5}]$ if its square is a strong atom. Thus, complex numbers satisfying $\beta^2 = 2$, $\gamma^2 = -2 + \sqrt{-5}$ or $\delta^2 = -2 - \sqrt{-5}$ are ideal primes for $\mathbb{Z}[\sqrt{-5}]$. Taking roots with a positive sign, the square root of the (AD)-representation $(**)$ becomes $6 = \beta\beta\gamma\delta$. Of course, since by Theorem 3.1 (ii) the (AD)-representation is

unique up to units of D, that is ± 1, we obtain uniqueness for factorization into ideal primes only up to factors of fourth roots of 1. The non-unique factorization $(*)$ reads in ideal primes as

$$2 \cdot 3 = \beta\beta\gamma\delta = \beta\gamma \cdot \beta\delta = (1 + \sqrt{-5})(1 - \sqrt{-5}). \qquad (***)$$

Again, non-uniqueness results from different groupings, this time of ideal primes. The ideal primes can be described by ideals in D as follows. Consider for an ideal prime α the set

$$I(\alpha) = \{y \in D \mid y = \alpha\alpha', \alpha'^m \in D \text{ for some } m \in \mathbb{N}\}.$$

One verifies easily for $D = \mathbb{Z}[\sqrt{-5}]$ that $I(\beta) = \text{rad}(2)$, $I(\gamma) = \text{rad}(-2 + \sqrt{-5})$ and $I(\delta) = \text{rad}(-2 - \sqrt{-5})$. Therefore, $I(\beta)$, $I(\gamma)$ and $I(\delta)$ are ideals in D given as radical ideals for strong atoms. By Theorem 3.1 (i), these 3 ideals are prime ideals. Indeed, one easily verifies that $I(\beta) = P$, $I(\gamma) = Q$ and $I(\delta) = Q'$. Ideal numbers were invented by E. E. Kummer (for the so called cyclotomic fields) prior to the invention of prime ideals by R. Dedekind. E. Hecke, who considered Kummer to be the creator of ideal theory ("Schöpfer der Idealtheorie," [7, page 87]) gave a construction of ideal numbers for the ring of integers of any number field. Though our definition of ideal prime numbers differs from Hecke's treatment, his discussion of another example seems quite similar [7, pages 83–86].

5 A More Striking Example

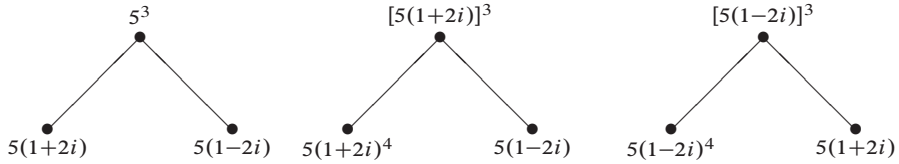
While factorization of elements into products of irreducible elements is not unique in $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[\sqrt{5}\imath]$, we were able to show for the example $(*)$ that atomic decay behaves in a finite manner. Namely, the decay of atoms reaches strong atoms just after one step, the decay rate equals 1 for all atoms and the elasticity of the domain equals 1. In this section, we construct an example of algebraic numbers where atomic decay is not as well mannered. The decay of the atoms involved will never end with strong atoms, infinitely many nonassociated atoms can divide the powers of a single atom and the elasticity $\rho(D)$ is infinite. Consider

$$\mathbb{Z}[5\imath] = \{m + 5n\imath \mid m, n \in \mathbb{Z}\}$$

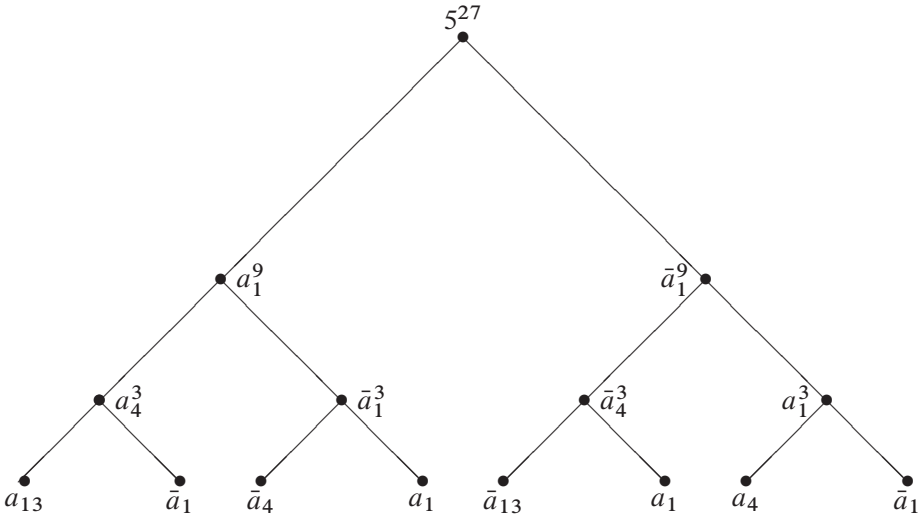
which is a subdomain of $\mathbb{Z}[\imath]$, the domain of Gausssian integers. An example of non-unique factorization in $\mathbb{Z}[5\imath]$ is given by

$$5 \cdot 5 \cdot 5 = (5 + 10\imath)(5 - 10\imath). \qquad (\dagger)$$

All factors are nonassociated atoms in $\mathbb{Z}[5\imath]$ which is easily verified using the norm function $N(m+5n\imath) = m^2+25n^2$ (see also Proposition 5.1 below). It is already clear from equation $(\dagger)$ that $\mathbb{Z}[5\imath]$ is neither factorial nor half-factorial. As for the example $(*)$ in $\mathbb{Z}[\sqrt{-5}]$, the factors in $(\dagger)$ further decay into atoms as can be seen from the following diagram.



The equation (†) is just the decay of 5 in the above diagram. Thus, in a manner simpler than (∗), it is not necessary to square (†) to see that both sides of the equation contain the same atoms. In contrast to (∗), however, all the atoms created above by decay will decay further without reaching strong atoms. This will be demonstrated in Proposition 5.1 and is illustrated by the following diagram where all elements $a_k = 5(1+2\imath)^k$, $k \geq 0$, and their conjugates $\overline{a}_k$ are atoms.



Proposition 5.1. (i) *The elements $a_k = 5(1+2\imath)^k$, $k \geq 0$, are nonassociated atoms in $\mathbb{Z}[5\imath]$.*

(ii) *Any (proper) power of the atom a_k decays into exactly two nonassociated atoms, $a_k^p = a_{p(k+1)-2} \cdot \overline{a}_{p-2}$ for any $p \geq 2$, $k \geq 0$.*

(iii) *For each $k \geq 0$ the set of non-associated atoms dividing a_k^p for some $p \geq 0$ is infinite.*

(iv) *The elasticity of $\mathbb{Z}[5\imath]$ is infinite.*

Proof. (i) Using the Binomial Theorem we obtain

$$a_k = 5(1+2\imath)^k = \sum_{l=0}^{k} \binom{k}{l} 5(2\imath)^l$$

and hence $a_k \in \mathbb{Z}[5\imath]$. Obviously, $N(a_k) < N(a_l)$ for $k < l$ and, hence, the a_k are nonassociated. Suppose $5(1+2\imath)^k = (m+5n\imath)(p+5q\imath)$ is a factorization of a_k in $\mathbb{Z}[5\imath]$. Applying the norm function in $\mathbb{Z}[\imath]$ we obtain

$$N(5(1+2\imath)^k) = N(5)\cdot N(1+2\imath)^k = 5^{k+2} = (m^2+25n^2)(p^2+25q^2).$$

Therefore,

$$m^2+25n^2 = 5^a, \quad p^2+25q^2 = 5^b, \quad \text{and} \quad a+b = k+2 \text{ for } a,b \in \mathbb{N}_0.$$

We shall show that either $a = 0$ or $b = 0$. Then $m+5n\imath = \pm 1$ or $p+5q\imath = \pm 1$ which proves that a_k is an atom. Suppose $a \geq 1$ and $b \geq 1$. Then $m = 5m'$, $p = 5p'$ and $5(1+2\imath)^k = 5(m'+n\imath)5(p'+q\imath)$. It follows that

$$(1+2\imath)^k = (1+2\imath)(1-2\imath)(m'+n\imath)(p'+q\imath).$$

Hence, $k \geq 2$ and

$$(1+2\imath)^{k-1} = (1-2\imath)(m'+n\imath)(p'+q\imath).$$

Now, we can write $1+2\imath = (1-2\imath)(-1+\imath)-\imath$ to obtain by the Binomial Theorem

$$(1+2\imath)^{k-1} = (1-2\imath)\sum_{l=1}^{k-1}\binom{k-1}{l}(1-2\imath)^{l-1}(-1+\imath)^l(-\imath)^{k-1-l} + (-\imath)^{k-1}.$$

Therefore, $(-\imath)^{k-1} = (1+2\imath)^{k-1} - (1-2\imath)\alpha$ with $\alpha \in \mathbb{Z}[\imath]$ and, combining we obtain

$$(-\imath)^{k-1} = (1-2\imath)(m'+n\imath)(p'+q\imath) - (1-2\imath)A = (1-2\imath)\cdot\beta$$

with $\beta \in \mathbb{Z}[\imath]$. Multiplying the two sides of this equation by its conjugate, we obtain $1 = 5\cdot\beta\overline{\beta}$, which is impossible.

(ii) By definition

$$\begin{aligned} a_{p(k+1)-2}\overline{a}_{p-2} &= 5(1+2\imath)^{p(k+1)-2}5(1-2\imath)^{p-2} \\ &= 5^2[(1+2\imath)(1-2\imath)]^{p-2}(1+2\imath)^{pk} \\ &= 5^2 5^{p-2}(1+2\imath)^{pk} \\ &= a_k^p. \end{aligned}$$

(iii) Is immediate from (ii) and (i).

(iv) Is immediate from (ii) and the definition of elasticity. □

Putting $p = 3$ in Proposition 5.1 (ii), one obtains $a_k^3 = a_{3(k+1)-2} \cdot \overline{a}_1$ which is the formula that generates the atomic decay depicted in the diagram Figure 3. Though at first the domain $\mathbb{Z}[5\imath]$ may seem simpler than the domain $\mathbb{Z}[\sqrt{-5}]$, Proposition 5.1 shows that the opposite is the case with respect to atomic decay. In $\mathbb{Z}[5\imath]$, as in $\mathbb{Z}[\sqrt{-5}]$, each nonzero nonunit is a product of atoms, as can again be seen using the norm function. Also, there are strong atoms in $\mathbb{Z}[5\imath]$, for instance 2, as can be seen from the same argument used in Proposition 4.1. But $\mathbb{Z}[5\imath]$ differs from $\mathbb{Z}[\sqrt{-5}]$, as there are not enough strong atoms to represent all elements by atomic decay.

6 Concluding Remarks and Questions

In this paper, we argue that non-unique factorization into atoms descends from atomic decay. Of course, by its very definition an atom cannot be broken up into parts, but after taking powers of an atom, atomic decay can occur, in which case unique factorization fails. For the ring of integers of an algebraic number field, we proved using atomic decay, that for each nonzero nonunit element some power can be factored uniquely (up to order and associates of factors) into strong atoms. In this sense, unique factorization is restored by forcing atoms to decay into strong atoms which can no longer decay. In particular, unique factorization into atoms is possible precisely if each atom is a strong atom. Also, the properties of half-factoriality and finite elasticity descend from atomic decay and can be described by the decay rates of atoms. The decay behavior may differ very much for different rings of algebraic integers. In one example we found decay ending with strong atoms after finitely many steps. In another, the decay turned out to be much more drastic and never ended with strong atoms. As a tool we employed the Fundamental Theorem of Ideal Theory and some well-known related simple properties. Is it possible to obtain unique factorization into strong atoms in a more direct way, without these tools? One might think of "extracting" strong atoms out of atoms in finitely many steps. Can this be done in an elementary way? For an indirect and non-elementary example employing "extraction" see [3]. Also, is it possible to check if a given atom is strong in a direct way? That is, using the norm function but not ideal theory. We did this in the case $\mathbb{Z}[\sqrt{-5}]$ for the element 2, but for other elements we needed ideal theory. In such investigations, the interesting question arises whether for a (rational) prime number p a prime power p^l is of the form $m^2 + kn^2$ for given $k \in \mathbb{N}$. Finally, though we touched upon historical issues in the paper there are further interesting questions here. We mentioned Kummer's ideal numbers, as seen by Hecke, and connected these to strong atoms. It has been argued that Kummer's ideal numbers developed from the work of C. G. J. Jacobi (see the recent paper [9] and the references therein). Do Jacobi's "wahre complexe Primzahlen" (true complex prime numbers) connect in any way to the notion of strong atom?

Acknowledgments. The authors would like to thank the referee for many helpful comments and suggestions.

Bibliography

[1] Baginski, P., Kravitz, R., A new characterization of half-factorial Krull domains. J Algebra Appl. 2010;9:825–837.

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

[3] Chapman, S. T., Halter-Koch, F., Krause, U., Inside factorial monoids and integral domains. J Algebra. 2002;252:350–375.

[4] Chapman, S. T., Krause, U., Cale monoids, Cale domains and Cale varieties. In: Arithmetical properties of commutative rings and monoids. vol. 241 of Lecture notes in pure and applied mathematics. 2005. p. 142–171.

[5] Gallian, J., Contemporary abstract algebra. 7th ed. New York: Brooks Cole Publishing Company; 2009.

[6] Geroldinger, A., Halter-Koch, F., Non-unique factorizations: algebraic, combinatorial and analytic theory. vol. 278 of Pure and applied mathematics. Chapman & Hall/CRC; 2006.

[7] Hecke, E., Vorlesungen über die Theorie der Algebraischen Zahlen. New York: Chelsea Publishing Company; 1970 [1st ed. Leipzig; 1923].

[8] Kim, H., Examples of half-factorial domains. Canad Math Bull. 2000;43:362–367.

[9] Lemmermeyer, F., Jacobi and Kummer's ideal numbers. Abh Math Semin Univ Hamburg. 2009;79:165–187.

[10] Marcus, D. A., Number fields. New York: Springer-Verlag; 1977.

[11] Pollard, H., Diamond, H., The theory of algebraic numbers. vol. 9 of The Carus Mathematical Monographs. Providence, RI: The Mathematical Association of America; 1975.

[12] Rush, D. E., An arithmetic characterization of algebraic number fields with given class group. Math Proc Cambridge Philos Soc. 1983;94:23–28.

[13] Valenza, R., Elasticity of factorization in number fields. J Number Theory. 1990;36(2): 212–218.

Author Information

Scott T. Chapman, Department of Mathematics and Statistics, Sam Houston State University, Huntsville, TX, USA.
E-mail: scott.chapman@shsu.edu

Ulrich Krause, Fachberich Mathematik und Informatik, Universität Bremen, Bremen, Germany.
E-mail: krause@math.uni-bremen.de