ELSEVIER Journal of Pure and Applied Algebra 127 (1998) 205–218

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Criteria for unique factorization in integral domains

D.D. Anderson[a], Scott T. Chapman[b,*,1], Franz Halter-Koch[c], Muhammad Zafrullah[d]

[a] *Department of Mathematics, University of Iowa, Iowa City, IA 52242, USA*
[b] *Department of Mathematics, Trinity University, 715 Stadium Drive, San Antonio, TX 78212-7200, USA*
[c] *Institut für Mathematik, Karl-Franzens-Universität, Heinrichstrasse 36, 8010 Graz, Austria*
[d] *MTA Teleport, 1440 Briggs Chaney Road, Silver Spring, MD 20905, USA*

Communicated by C.A. Weibel; received 28 June 1996; revised 14 October 1996

Abstract

Let R be an integral domain. In this paper, we introduce a sequence of factorization properties which are weaker than the classical UFD criteria. We give several examples of atomic nonfactorial monoids which satisfy these conditions, but show for several classes of integral domains of arithmetical interest that these factorization properties force unique factorization. In particular, we show that if R satisfies any of our properties and is a Krull domain with finite divisor class group, a nonmaximal order in an algebraic number field, or a generalized Cohen–Kaplansky domain, then R in fact must be factorial. © 1998 Elsevier Science B.V. All rights reserved.

AMS Classification: 13F15, 13G05, 20M14

1. Introduction

Throughout this paper, a monoid H is assumed to be commutative and cancellative. We write H multiplicatively and denote by $1 \in H$ its identity element and by $H^\times$ its group of invertible elements. H is called *reduced* if $H^\times = \{1\}$. We use the basic notions of divisibility theory as in [12, Section 6]. By passing from H to $H/H^\times$, we may assume that H is reduced whenever this is convenient. The irreducible elements of H are called *atoms* and H is called *atomic* if every $a \in H \backslash H^\times$ is a product of

[*] Corresponding author. E-mail: schapman@trinity.edu.

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

PII S0022-4049(96)00183-1

atoms. Much recent literature has been devoted to the study of factorization properties of monoids (see, e.g., [10, 13, 15]). Such studies take on added significance since they have immediate applications to ring theory. For an integral domain R, we denote by $R^\bullet = R \setminus \{0\}$ its multiplicative monoid of nonzero elements, and describe the factorization properties of R by means of the monoid $R^\bullet$. In particular, we say that R has some factorization property **P** (e.g., being atomic or factorial) if $R^\bullet$ has property **P**.

If a monoid H is atomic but not factorial, then the factorization of a nonunit of H into atoms is usually not unique. Several notions and arithmetical measures describing the degree of nonuniqueness of factorizations have been introduced in the literature, mainly for Dedekind domains (see [5] for a summary).

In this paper, we introduce a sequence of factorization properties which are weaker than unique factorization. We give simple examples of atomic nonfactorial monoids having these factorization properties, but are unaware of similar examples for integral domains. On the contrary, for large classes of domains of arithmetical interest, we show that our factorization properties already force unique factorization.

2. Definitions and examples

We motivate our work with a proposition.

Proposition 2.1. *For a natural number n and atomic monoid H, the following statements are equivalent:*

(1) If $a_1, \ldots, a_n, b_1, \ldots, b_l$ are not necessarily distinct atoms with $a_1 \cdots a_n = b_1 \cdots b_l$, then $n = l$ and after reordering, a_i and b_i are associates.

(2) If $a_1, \ldots, a_m, b_1, \ldots, b_l$ are not necessarily distinct atoms where $1 \leq m \leq n$ with $a_1 \cdots a_m = b_1 \cdots b_l$, then $m = l$ and after reordering, a_i and b_i are associates.

(3) If $b, a_1, \ldots, a_n$ are not necessarily distinct atoms of H and $b | a_1 \cdots a_n$, then b is associated to a_i for some i.

(4) If $1 \leq m \leq n$ and $b, a_1, \ldots, a_m$ are not necessarily distinct atoms of H with $b | a_1 \cdots a_m$, then b is associated to a_i for some i.

(5) If $1 \leq i \leq m \leq n$ and $b_1, \ldots, b_i, a_1, \ldots, a_m$ are not necessarily distinct atoms of H with $b_1 \cdots b_i | a_1 \cdots a_m$, then, after reordering, b_j and a_j are associates for $j = 1, \ldots, i$.

Proof. Clearly we have $(5) \Rightarrow (4) \Rightarrow (3)$ and $(2) \Rightarrow (1)$.

$(3) \Rightarrow (2)$: Suppose that $a_1 \cdots a_m = b_1 \cdots b_l$. Now $b_1 | a_1 \cdots a_m a_m^{n-m}$, so $b_1 | a_i$ for some i. After reordering, we can take $i = 1$ and since a_1 and b_1 are atoms, they are associates. Cancelling a_1 from both sides, we get $a_2 \cdots a_m = \lambda b_2 \cdots b_l$ for some unit λ. Continuing in this manner, we obtain $m = l$ and after reordering a_i and b_i are associates.

$(1) \Rightarrow (5)$: Suppose $b_1 \cdots b_i | a_1 \cdots a_m$; so $b_1 \cdots b_i c_1 \cdots c_s = a_1 \cdots a_m$ for some atoms $c_1, \ldots, c_s$. Then $b_1 \cdots b_i c_1 \cdots c_s a_m^{n-m} = a_1 \cdots a_m a_m^{n-m}$. Thus, $i+s+n-m = n$ so $i+s = m$. After reordering we get b_j and a_j are associates for $j = 1, \ldots, i$ (and also c_j and a_j for $j = i+1, \ldots, s$). □

Definition. An atomic monoid satisfying any of the five equivalent conditions of Proposition 2.1 is said to be *n-factorial.*

By slighty weakening condition (1), we obtain a condition of some further interest.

(1^*) If $a_1,\dots,a_n,b_1,\dots,b_n$ are not necessarily distinct atoms with $a_1\cdots a_n=b_1\cdots b_n$, then, after reordering, a_i and b_i are associates.

Definition. An atomic monoid H satisfying (1^*) is called *quasi-n-factorial.*

We also consider a third condition.

Definition. An atomic monoid H is called *square-factorial* if whenever u,v and w are irreducible elements of H with $u^2=vw$ then u and v are associates.

An atomic integral domain R is called n-factorial, quasi-n-factorial or square-factorial if its corresponding monoid $R^\bullet$ has these properties.

It was proved in [13] that if the ring of integers of an algebraic number field is square-factorial, then it is already factorial. In this paper we shall extend this property to a large class of domains. We open with some simple consequences of our definitions.

Remark 2.2. Let H be an atomic monoid.

(1) H is 1-factorial.

(2) If H is n-factorial, then H is quasi-n-factorial.

(3) H is factorial if and only if H is n-factorial for all $n\geq 1$.

(4) If H is (quasi-)$(n+1)$-factorial then H is (quasi-)n-factorial. This follows immediately from Proposition 2.1.

(5) If H is quasi-2-factorial, then H is square-factorial.

Example 2.3. For $n\in\mathbb{N}$, $n\geq 2$, the additive monoid $H=\langle n,n+1\rangle\subset\mathbb{N}_0$ is $(n-1)$-factorial, but not n-factorial, and is quasi-k-factorial for all $k\in\mathbb{N}$.

Proof. In order to prove that H is $(n-1)$-factorial, suppose that there is an equation of the form

$$an+b(n+1)=a'n+b'(n+1),$$

where $a,b,a',b'\in\mathbb{N}_0$ and $a+b=n-1$. We must prove that $a=a'$ and $b=b'$. Since $b\equiv b' \pmod n$ and $b<n$, we have $b'=b+b''n$ for some $b''\in\mathbb{N}_0$, and

$$a=a'+b''+b''n$$

follows. From $a<n$ we conclude that $b''=0$, and $a=a'$ follows.

The equation $n(n+1)=(n+1)n$ shows that H is not n-factorial.

In order to prove that H is quasi-k-factorial for $k\in\mathbb{N}$, observe that, for all $a,a'\in\{0,1,\dots k\}$, $an+(k-a)(n+1)=a'n+(k-a')(n+1)$ implies $a=a'$. □

Example 2.4. Let $m > k \geq 1$ be natural numbers and $n = (k+1)m$. Then the additive monoid $H = \langle n, n+1, n+k+1 \rangle \subset \mathbb{N}_0$ is k-factorial but not quasi-$(k+1)$-factorial.

Proof. In order to prove that H is k-factorial, assume that there is an equation of the form

$$an + b(n+1) + c(n+k+1) = a'n + b'(n+1) + c'(n+k+1),$$

where $a, b, c, a', b', c' \in \mathbb{N}_0$ and $a+b+c = k$. This implies $b \equiv b' \pmod{(k+1)}$ and hence $b' = b + (k+1)b''$ with $b'' \in \mathbb{N}_0$, since $b \leq k$. Inserting this, dividing by $(k+1)$ and putting $a = k - b - c$, yields

$$km + c = a'm + bm + (k+1)mb'' + b'' + c'(m+1).$$

Since $km + c < km + m = (k+1)m$, it follows that $b'' = 0$, $c' \leq k$ and $c \equiv c' \pmod{m}$, which implies $c = c'$. Finally $k = a' + b + c'$ implies $a = a'$.

The equation $(k+1)(n+1) = kn + (n+k+1)$ shows that H is not quasi-$(k+1)$-factorial. □

Our next two examples involve block monoids, which will also be of importance later in the study of Krull monoids. Let us recall the definition. For any set P, we denote by $\mathscr{F}(P)$ the free abelian monoid with basis P. Its elements are of the form

$$S = \prod_{p \in P} p^{v_p(S)},$$

where $v_p(S)$ are nonnegative integers, almost all equal to zero. If G is an additive abelian group and G_0 is a subset of G, then we call

$$\mathscr{B}(G_0) = \left\{ B \in \mathscr{F}(G_0) \;\middle|\; \sum_{g \in G_0} v_g(B)g = 0 \in G \right\}$$

the *block semigroup over* G_0. The elements of $\mathscr{B}(G_0)$ are called *blocks*.

Example 2.5. Denote by C_n the cyclic group of order n (written additively), and write $C_n = \{0, 1, \ldots, n-1\}$. It is easily verified that the block semigroups $\mathscr{B}(C_2 \oplus C_2)$ and $\mathscr{B}(C_3)$ are quasi-2-factorial, but not 2-factorial.

Let $n \geq 2$ be a positive integer. We construct a n-factorial monoid which is not factorial. Let $G = \sum_{i=1}^{n} C_{n+3}$ and

$$G_0 = \{(1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1), (n+2, n+2, \ldots, n+2)\}.$$

By an argument similar to that used in [6, Example 7], $\mathscr{B}(G_0)$ is n-factorial but not $(n+1)$-factorial.

Now, let k and j be positive integers with $k > 1$ and $j > 2$. By the argument presented in [7, Example 4.14], $G = \mathbb{Z}^k$ with

$$G_0 = \{(1,1,\dots,1),(-1,0,\dots,0),\dots,(0,\dots,0,-1)$$

$$(j,0,\dots,0),\dots,(0,\dots,0,j),(-j,-j,\dots,-j)\}$$

yields a block semigroup $\mathscr{B}(G_0)$ which is $\min\{k,j\}$-factorial.

3. Krull monoids and Krull domains

We start with a simple but useful lemma whose proof is obvious.

Lemma 3.1. *Let $f : H \to D$ be a homomorphism of reduced atomic monoids.*

(i) *Suppose that f is injective and, for every atom u of H, $f(u)$ is an atom of D. If D is n-factorial (resp. quasi-n-factorial or square-factorial), then so is H.*

(ii) *Suppose that f is surjective and has the following property: If $x \in H$ and $a, b \in D$ are such that $f(x) = ab$, then there exist $u, v \in H$ satisfying $x = uv$, $f(u) = a$ and $f(v) = b$. If H is n-factorial (resp. quasi-n-factorial or square-factorial), then so is D.*

For Krull monoids, we refer the reader to [8, 12] or [16]. By [8], every Krull monoid H splits in the form $H = H_0 \times H^\times$ where H_0 is a submonoid of a free abelian monoid with basis $P, H_0 \subset \mathscr{F}(P)$, such that the following two conditions hold:

1. If $a, b \in H_0$ and $a|b$ in $\mathscr{F}(P)$, then $a|b \in H_0$.
2. Every $a \in \mathscr{F}(P)$ is a greatest common divisor of finitely many elements of H.

Up to isomorphism, $\mathscr{F}(P)$ is uniquely determined by H. The elements of P are called *primes* of H. The factor group $G = \mathscr{F}(P)/H_0$ is called the *divisor class group* of H. It is written additively, and for $a \in \mathscr{F}(P)$, $[a] \in G$ denotes the class containing a. The submonoid $H_0 = H/H^\times$ is a reduced Krull monoid, and H is reduced if and only if $H = H_0$.

If G_0 is a subset of any abelian group G, then the block semigroup $\mathscr{B}(G_0)$ introduced in Section 1 is a Krull monoid (see [10] for a discussion of the arithmetic of block semigroups).

If H is a Krull monoid as above with class group G, and $G_0 = \{[p] \mid p \in P\} \subset G$ denotes the set of all classes containing primes, then the block homomorphism $\beta : H_0 \to \mathscr{B}(G_0)$ defined by

$$\beta(p_1 \cdots p_n) = [p_1] \cdots [p_n],$$

where $p_1, \dots, p_n \in P$ satisfies the assumptions of Lemma 3.1(ii). Therefore, we obtain the following Corollary.

Corollary 3.2. *Let H be a Krull monoid with class group G, let G_0 be the set of classes containing primes, and $\mathscr{B}(G_0)$ be the block monoid. If H is n-factorial (resp. quasi-n-factorial or square-factorial), then so is $\mathscr{B}(G_0)$.*

An integral domain R is a Krull domain if and only if $R^\bullet$ is a Krull monoid (see [16]), and in this case the set of primes may be identified with the set of height one prime ideals of R. An arbitrary Krull monoid H need not satisfy the weak approximation theorem (and hence it is not of the form $H = R^\bullet$ for a Krull domain R). Concerning the distribution of primes in the ideal classes of a Krull monoid, we have the following result.

Lemma 3.3. *Let H be a Krull monoid, P its set of primes and G its class group. For a subset $M \subset G$ we denote by*

$$\langle M\rangle = \{g_1 + \cdots + g_s \mid g_j \in M\} \subset G$$

the submonoid of G generated by M.

(i) *For every $p_0 \in P$, we have $G = \langle\{[p] \mid p \in P\backslash\{p_0\}\}\rangle$.*

(ii) *If R is a Krull domain and $H = R^\bullet$, then we have, for every finite subset $E \subset P$,*

$$G = \langle\{[p] \mid p \in P\backslash E\}\rangle.$$

Proof. See [17]. Observe that (in the notation above)

$$\partial : H \to H_0 \hookrightarrow \mathscr{F}(P)$$

is a divisor theory with class group G. □

Theorem 3.4. *Let H be a Krull monoid with class group G.*

(i) *If there exists a nontrivial class of finite order containing at least two primes, then H is not square-factorial.*

(ii) *If every class containing primes contains at least two primes, then H is not quasi-2-factorial.*

(iii) *If $|G| > 3$, $G \neq C_2 \oplus C_2$, and every nontrivial class contains at least one prime, then H is not quasi-2-factorial.*

Proof. (i) and (ii) As above, we may assume that $H = H_0 \times H^\times$ and $H_0 \subset \mathscr{F}(P)$, where P is the set of primes of H. Suppose that $g \in G\backslash\{0\}$ contains two distinct primes, p_1 and p_2.

If g is of finite order $n \geq 2$, then $u = p_1^{n-1}p_2$, $v = p_1^n$ and $w = p_1^{n-2}p_2^2$ are distinct atoms satisfying $u^2 = vw$.

Assume now that g has infinite order. By Lemma 3.3(i), there exist classes $g_1, \ldots, g_s \in G$ containing primes such that $-g = g_1 + \cdots + g_s$. We may assume that $s \in \mathbb{N}$ is minimal with this property and that $g_1 \neq g$. For $1 \leq i \leq s$ select primes $q_i \in g_i \cap P$, and $q_1' \in g_1 \cap P$ such that $q_1' \neq q_i$ (this is possible since each of these classes contain at least two primes). Setting $u=(p_1q_1q_2\cdots q_s)$, $v=(p_2q_1'q_2\cdots q_s)$, $w=(p_1q_1'q_2\cdots q_s)$ and $z=(p_2q_1q_2\cdots q_s)$ yields that $uv=wz$ in H. Now, u is not an associate of w since $q_1'\neq q_1$ and u is not an associate of z since $p_1\neq p_2$. Hence, H is not quasi-2-factorial.

(iii) By Corollary 3.2, it is sufficient to prove that $\mathscr{B}(G)$ is not quasi-2-factorial. We consider three cases.

Case 1: $2G=0$. Since $|G|>3$ and $G\neq C_2\oplus C_2$, there exist three independent elements $g,h,k\in G$ of order 2, and the relation

$$[(g+h)(g+k)(h+k)]\cdot[(g+h+k)ghk]$$

$$=[(g+h)gh]\cdot[(g+k)(h+k)(g+h+k)k]$$

yields the assertion.

Case 2: $3G=0$. Since $|G|>3$, there exist two independent elements $g,h\in G$ of order 3, and the relation

$$[g(g+h)(g+2h)]\cdot[(2g)(g+h)(2h)]=[g(2g)]\cdot[(g+h)^2(g+2h)(2h)]$$

yields the assertion.

Case 3: There exists some $g\in G$ such that $\operatorname{ord}(g)>3$. In this case, the relation

$$[g(2g)(-3g)]\cdot[g^2(-2g)]=[g^3(-3g)]\cdot[(2g)(-2g)]$$

yields the assertion. □

Corollary 3.5. *Let R be a Krull domain with nontrivial class group G.*

(i) *If some nontrivial class of G of finite order contains at least two primes, then R is not square-factorial.*

(ii) *If every nontrivial class of G contains at least one prime, then R is not quasi-2-factorial.*

Proof. The proof of (i) follows directly from Theorem 3.4(i). For (ii), if $|G|>4$ then the result follows directly from Theorem 3.4(iii). If $|G|\leq 4$ then some nontrivial class contains infinitely primes and the result follows from part i). □

For the n-factorial property, we can prove a slightly different version of the last theorem.

Theorem 3.6. *Let H be a Krull monoid with class group G, $n\in\mathbb{N}$ and $nG=0$. If H is n-factorial, then it is already factorial.*

Proof. It is sufficient to prove that every atom of H is primary. For then H is weakly factorial, and the assertion follows from [15, Corollary 2.9]. We may assume that H is reduced and $H\subset\mathscr{F}(P)$. Let $a\in H$ be an atom and let $p\in P$ be a prime dividing a.

If d is the order of $[p]$ in G, then $d \mid n$, p^d is a primary atom in H and $p^d \mid a^n$. Proposition 2.1(3) now implies that $a = p^d$. □

Next we consider Krull domains with infinite cyclic ideal class group.

Theorem 3.7. *Let R be a Krull domain with class group G isomorphic to $\mathbb{Z}$. Let g be a generator of G and G_0 the set of all nonzero classes of G containing primes.*

(i) *If $G_0 = \{g, -g\}$ then R is square-factorial but not quasi-2-factorial.*

(ii) *If $G_0 \neq \{g, -g\}$ then R is not square-factorial.*

Proof. As above, we assume that $R^\bullet = H_0 \times R^\times$ and $H_0 \subset \mathscr{F}(P)$, where P is the set of primes.

(i) By Lemma 3.3, $g \cap P$ and $(-g) \cap P$ are both infinite. The irreducible elements of R which are not prime are precisely the elements pq, where $p \in g \cap P$ and $q \in (-g) \cap P$. If $(pq)^2 = (p_1 q_1)(p_2 q_2)$, where $p, p_1, p_2 \in g \cap P$ and $q, q_1, q_2 \in (-g) \cap P$, then $p = p_1 = p_2$ and $q = q_1 = q_2$. Therefore R is square-factorial. In order to prove that R is not quasi-2-factorial, let $p_1, p_2 \in g \cap P$ and $q_1, q_2 \in (-g) \cap P$ be distinct and consider the relation $(p_1 q_1)(p_2 q_2) = (p_1 q_2)(p_2 q_1)$.

(ii) First we assert that it is sufficient to consider the following two cases:

(A) There exist $m, n \in \mathbb{N}$ such that $n \geq 2$, $ng \in G_0$, and $(-mg) \cap P$ is infinite.

(B) There exists some $n \in \mathbb{N}$ such that $n \geq 2$, $ng \in G_0$, and the set $\{m \in \mathbb{N} \mid (-m)g \in G_0, m \not\equiv 0 \pmod{n}\}$ is infinite.

Indeed, if $G_0 \neq \{g, -g\}$, then by Lemma 3.3 there exists some $n \in \mathbb{N}$, $n \geq 2$, such that either $ng \in G_0$ or $(-n)g \in G_0$. Interchanging g and $-g$ if necessary, we may assume that $ng \in G_0$. If there exists some $m \in \mathbb{N}$ such that $(-m)g \cap P$ is infinite, then we are in case (A). Therefore, we assume that $(-m)g \cap P$ is finite for all $m \in \mathbb{N}$. If the set $M = \{m \in \mathbb{N} \mid (-m)g \in G_0, m \not\equiv 0 \pmod{n}\}$ is infinite, then we are in case (B). If M is finite, then Lemma 3.3 implies that the set $\{m \in \mathbb{N} \mid (-m)g \in G_0, m \equiv 0 \pmod{n}\}$ is infinite, and that there are infinitely many primes in classes mg, where $m \not\equiv 0 \pmod{n}$. Let $k \in \mathbb{N}$ be such that $(-kn)g \in G_0$, and distinguish two cases.

Case 1: $m_1 g \cap P$ is infinite for some $m_1 \in \mathbb{N}$. Interchanging g and $(-g)$, we see that (A) holds with (kn, m_1) instead of (n, m).

Case 2: The set $\{n \in \mathbb{N} \mid mg \in G_0, m \not\equiv 0 \pmod{n}\}$ is infinite. Interchanging g and $-g$, we see that (B) holds with kn instead of n.

Now we prove that R is not square-factorial under either of the assumptions (A) or (B).

(A) Let $p_1, p_2, p_2' \in (-m)g \cap P$ be distinct and $p \in ng$. Then the relation

$$(p_1^{n-2} p_2 p_2' p^m)^2 = (p_1^{n-2} p_2^2 p^m)(p_1^{n-2} p_2'^2 p^m)$$

shows that R is not square-factorial.

(B) Let $m_1, m_2 \in \mathbb{N}$ be distinct such that $(-m_1)g \in G_0, (-m_2)g \in G_0$ and $m_1 \equiv m_2 \not\equiv 0 \pmod{n}$. Let $t \in \mathbb{N}$ be minimal such that $tm_i \equiv 0 \pmod{n}$, and let $k, l \in \mathbb{N}$ be such that $(t-1)m_1 + m_2 = nk$ and $tm_1 = nl$. Then $t \geq 2$, $2k \geq l$, and if $p_1 \in (-m_1)g \cap P$,

$p_2 \in (-m_2)g \cap P$, $q \in ng \cap P$, then the relation

$$(p_1^{t-1} p_2 q^k)^2 = (p_1^t q^l)(p_1^{t-2} p_2^2 q^{2k-l})$$

shows that R is not quasi-2-factorial. □

Theorem 3.8. *Let H be a Krull monoid, G its class group, $g \in G$ and $n \in \mathbb{N}$ such that $2 \le n \le \operatorname{ord}(g) < \infty$. Suppose that each of the classes jg $(1 \le j < \operatorname{ord}(g))$ contains at least $n+1$ distinct primes. Then there exist pairwise nonassociated atoms $u_0, u_1, \ldots, u_n \in H$ such that $u_0^n = u_1 \cdot \ldots \cdot u_n$.*

Proof. Exactly as in the special case which is in [13, Theorem 1]. □

4. Finitely primary monoids and one-dimensional domains

A monoid T is called *finitely primary of rank $s \in \mathbb{N}$ and of exponent $\alpha \in \mathbb{N}$*, if it is a submonoid of a factorial monoid F containing exactly s mutually nonassociated prime elements $p_1, \ldots, p_s$,

$$T \subset F = \langle p_1, \ldots, p_s \rangle \times F^\times,$$

satisfying the following conditions:

1. $T^\times = T \cap F^\times$.

2. For any $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s} u \in F$ (where $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ and $u \in F^\times$) the following two assertions hold true:

(a) If $a \in T \setminus T^\times$, then $\alpha_1 \ge 1, \ldots, \alpha_s \ge 1$.

(b) If $\alpha_1 \ge \alpha, \ldots, \alpha_s \ge \alpha$, then $a \in T$.

In the following, we use the terminology of [15, Section 4]. For another characterization of finitely primary monoids see [9, Theorem 1].

Theorem 4.1. *Let T be a finitely primary monoid of rank s and exponent α, and suppose that T is not factorial.*

(i) *If $s \ge 2$, then T is not s-factorial and not (2α)-factorial.*

(ii) *If $s = \alpha = 1$, then T is not square-factorial.*

(iii) *If $s = 1$ and $\alpha \ge 2$, then T is not α-factorial.*

Proof. (i) For each $1 \le i \le s$ notice that

$$a_i = (p_1 \cdots p_s)^\alpha p_i^\alpha$$

is an atom of T. Hence

$$a_1 \cdots a_s = (p_1^\alpha \cdots p_s^\alpha)^{s+1},$$

showing that T is not s-factorial.

In order to prove that T is not (2α)-factorial, choose any $N \geq 2\alpha$ and consider the element

$$a = (p_1 \cdots p_s)^{(N+1)\alpha} = [p_1^{\alpha}(p_2 \cdots p_s)^{N\alpha}][p_1^{N\alpha}(p_2 \cdots p_s)^{\alpha}].$$

Each factor on the right-hand side has a factorization into at most α factors, so a has a factorization into at most 2α factors. The left-hand side shows that a has a factorization into at least $N+1 > 2\alpha$ factors.

(ii), (iii) Set $p = p_1$, and let $1 \leq c \leq \alpha$ be minimal such that $p^c\varepsilon \in T$ for some $\varepsilon \in F^{\times}$.

Case 1: $c = \alpha = 1$. Since T is not factorial, there exist some $\eta \in F^{\times}\backslash T^{\times}$. The elements $p^{\alpha}, p^{\alpha}\eta$ and $p^{\alpha}\eta^{-1}$ are nonassociated atoms of T, and the relation $(p^{\alpha})^2 = (p^{\alpha}\eta)(p^{\alpha}\eta^{-1})$ shows that T is not square-factorial.

Case 2: $c = \alpha \geq 2$. Here the relation $(p^{\alpha})^{\alpha+1} = (p^{\alpha+1})^{\alpha}$ shows that T is not α-factorial, since p^{α} and $p^{\alpha+1}$ are atoms.

Case 3: $c < \alpha$. Note that this case can only occur for $\alpha > 1$. Since $p^c\varepsilon$ is an atom of T, the relation $(p^c\varepsilon)^{\alpha} = (p^{\alpha})^{c-1}(p^{\alpha}\varepsilon^{\alpha})$ shows that T is not α-factorial. □

Theorem 4.2. *Let R be a one-dimensional quasilocal domain such that the complete integral closure $\hat{R}$ of R is a semilocal principal ideal domain, $\hat{R} \neq R$ and $[R : \hat{R}] \neq 0$. Then R is not square-factorial.*

Proof. By [9, Theorem 2], the multiplicative monoid $R^{\bullet}$ is finitely primary of rank $s = |\max(\hat{R})|$ and

$$\hat{R}^{\bullet} = \langle p_1, \ldots, p_s \rangle \times \hat{R}^{\times},$$

where $p_1, \ldots, p_s$ is a system of nonassociated primes of $\hat{R}$. The conductor $[R : \hat{R}]$ is of the form

$$[R : \hat{R}] = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}\hat{R},$$

where $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$ (then $R\backslash\{0\}$ is of exponent $\max(\alpha_1, \ldots, \alpha_s)$). We set $p = p_1, \alpha = \alpha_1$ and consider several cases.

Case 1: $s = \alpha = 1$. See Theorem 4.1.

Case 2: $s = 1, \alpha \geq 2$. Let $1 \leq c \leq \alpha$ be minimal such that $u = p^c\varepsilon \in R$ for some $\varepsilon \in \hat{R}^{\times}$.

Case 2A: $c = \alpha$. Since $\eta = 1 + p \in \hat{R}^{\times}\backslash R^{\times}$, the elements $p^{\alpha}, p^{\alpha}\eta$ and $p^{\alpha}\eta^{-1}$ are nonassociated atoms of R, and $(p^{\alpha})^2 = (p^{\alpha}\eta)(p^{\alpha}\eta^{-1})$.

Case 2B: $c < \alpha$. Since $p^{\alpha-c}\hat{R} \not\subset R$, there exists some $\theta \in \hat{R}$ such that $\varepsilon^{-1}\theta p^{\alpha-c} \notin R$, and consequently $\eta = 1 + \varepsilon^{-1}\theta p^{\alpha-c} \in \hat{R}^{\times}\backslash R^{\times}$. Therefore,

$$v = u\eta = u + \theta p^{\alpha} \in R$$

and

$$w = u\eta^{-1} = u + (-\theta\eta^{-1})p^{\alpha} \in R$$

are atoms of R, which are not associated to u. Since $u^2 = vw$, the assertion follows.

Case 3: $s \geq 2$. We set $q = p_2^{\alpha_2} \cdots p_s^{\alpha_s}$.

Case 3A: For all $\beta \geq 1$, if $p^\beta q$ lies in R, then it is an atom of R. Then

$$p^\alpha q, p^{\alpha+1} q, p^{\alpha+2} q$$

are nonassociated atoms of R satisfying

$$(p^{\alpha+1} q)^2 = (p^\alpha q)(p^{\alpha+2} q).$$

Case 3B: There exists some $\beta \geq 1$ such that $p^\beta q$ is a reducible element of R. An atom a of R dividing $p^\beta q$ is of the form

$$a = p^\gamma p_2^{\gamma_2} \cdots p_s^{\gamma_s} \varepsilon,$$

where $\gamma \geq 1, 1 \leq \gamma_j < \alpha_j$ for $j = 2, \ldots, s$ and $\varepsilon \in \hat{R}^\times$. Now, let $u \in R$ be an atom of the form

$$u = p^\gamma q_0,$$

where $\gamma \geq 1, q_0 = p_2^{\gamma_2} \cdots p_s^{\gamma_s} \varepsilon \in \hat{R}, 1 \leq \gamma_j < \alpha_j, \varepsilon \in \hat{R}^\times$ and assume that there is no atom $\tilde{u}$ in R properly dividing u in $\hat{R}$. We set $q_1 = p_2^{\alpha_2 - \gamma_2} \cdots p_s^{\alpha_s - \gamma_s} \varepsilon^{-1} \in \hat{R}$ and $q = q_0 q_1$. Since $p^\alpha q_1 \hat{R} \not\subset R$, there exists some $\theta \in \hat{R}$ such that $\theta p^\alpha q_1 \notin R$, and consequently $\eta = 1 + \theta p^\alpha q_1 \in \hat{R}^\times \backslash R^\times$. Therefore

$$v = u\eta^{-1} = u + \theta p^{\alpha+\gamma} \in R$$

and

$$w = u\eta^{-1} = u + (-\theta\eta^{-1}) p^{\alpha+\gamma} q \in R$$

are atoms of R which are not associated to u. Since $u^2 = vw$, the assertion follows. □

In order to globalize Theorem 4.2, we need some additional technical tools which we formulate in the language of monoids.

Lemma 4.3. *Let* $(H_\lambda)_{\lambda \in \Lambda}$ *be a family of monoids and* $H = \coprod_{\lambda \in \Lambda} H_\lambda$. *If* H *is n-factorial* (*resp. quasi-n-factorial or square-factorial*), *then so are all* H_λ.

Proof. We may assume that all H_λ are reduced. Then we apply Lemma 3.1(i) to the natural injections $H_\lambda \to H$. □

Recall that an integral domain R is weakly Krull if and only if every proper principal ideal of R has a (finite) primary decomposition where all the associated primes have height 1. If R is weakly Krull, we denote by $X^1(R)$ the set of prime ideals of height 1 of R and by $Cl_t(R)$ the t-class group of R (see [3, 14]).

Corollary 4.4. *Let R be a weakly Krull domain with $Cl_t(R) = 0$. If R is n-factorial (resp. quasi-n-factorial or square-factorial), then so are all R_p for $p \in X^1(R)$.*

Proof. Since $Cl_t(R) = 0$, we have an isomorphism of monoids

$$R^\# \to \coprod_{p \in X^1(R)} R_p^\#,$$

where $R^\# = (R^\bullet)/R^\times$ is the associated reduced monoid of the multiplicative monoid of R (see the main result of [4]). Now the assertion follows from Corollary 3.1(ii). □

Theorem 4.5. *Let R be a one-dimensional noetherian domain such that* $\mathrm{Pic}(R) = 0$, *the integral closure $\bar{R}$ of R is a finitely generated R-module and $\bar{R} \neq R$. Then R is not square-factorial.*

Proof. Since R is weakly Krull, $Cl_t(R) = \mathrm{Pic}(R) = 0$, and Corollary 4.4 applies. Therefore it is sufficient to prove that R_p is not square-factorial for some $p \in \max(R)$. Since there exists some $p \in \max(R)$ such that $\bar{R}_p \neq R_p$, the assertion follows from Theorem 4.2. □

An atomic integral domain R is called a *Cohen–Kaplansky domain* (*CK-domain*) if it has finitely many nonassociated irreducible elements, and a *generalized Cohen–Kaplansky domain* (*generalized CK-domain*) if it has finitely many nonassociated irreducible elements which are not prime.

Theorem 4.6. *Let R be a generalized CK-domain which is not factorial. Then R is not square-factorial.*

Proof. By [1, Theorem 4] or [14, Lemma 4.11], R is weakly Krull and $Cl_t(R) = 0$. Thus, by Corollary 4.4, it suffices to prove that R_p is not quasi-2-factorial for at least one $p \in X^1(R)$. By [1, Theorem 6], the integral closure $\bar{R}$ of R is factorial. Therefore we have $\bar{R} \neq R$ and hence $\overline{R_p} \neq R_p$ for some $p \in X^1(R)$. Since R_p is a CK-domain, its integral closure $\overline{R_p}$ is a DVR and $[R_p : \overline{R_p}] \neq 0$ by [2, Theorem 2.4]. Therefore $\overline{R_p}$ is the complete integral closure of R_p, and Theorem 4.2 shows that R_p is not square-factorial. □

Theorem 4.7. *Let R be a nonmaximal order in an algebraic number field. Then R is not square-factorial.*

Proof. If $\mathrm{Pic}(R) = 0$, the assertion follows from Theorem 4.5. Thus we suppose that $\mathrm{Pic}(R) \neq 0$. Let f be the conductor of R, and

$$H = \{a \in R \mid aR + f = R\}.$$

It follows from [11, Section 3] that H is a Krull monoid with finite class group Pic(R), and every class of H contains infinitely many primes. Therefore H is not square-factorial by Theorem 3.4(i), and Lemma 3.1(ii), applied to $H \hookrightarrow R\backslash\{0\}$, completes the proof. □

Remark. Theorem 4.7 continues to hold for orders in homomorphy rings of global fields as considered in [11].

We close with three results concerning polynomial and power series rings.

Theorem 4.8. *Let R be an integral domain. Then $R[X]$ is 2-factorial if and only if R (and hence $R[X]$) is factorial.*

Proof. Suppose that $R[X]$ is 2-factorial. Let $a \in R$ be an atom. We show that a is prime. This proves that R (and hence $R[X]$) is factorial. Suppose that $a|bc$ (where $b, c \in R - \{0\}$), but $a \nmid b$ and $a \nmid c$. Then $aX + b$ and $aX + c$ are atoms in $R[X]$. Now $a|bc$ gives that a divides the coefficients of $(aX + b)(aX + c)$, so $(aX + b)(aX + c) = af$ for some $f \in R[X]$. But then factoring f into irreducibles gives a different factorization of $(aX + b)(aX + c)$, contradicting the hypothesis that $R[X]$ is 2-factorial. □

Remark. If we assume in Theorem 4.8 that R is integrally closed, then $R[X]$ 2-factorial can be replaced by $R[X]$ quasi-2-factorial. To see this, we show that in the factorization $(aX + b)(aX + c) = af$, f must be irreducible. First, assume that $a|f$ in $R[X]$. Then $X^2 + [(b + c)/a]X + (bc/a^2) \in R[X]$ gives that $-b/a$ and $-c/a$ are integral over R, a contradiction. Hence, suppose that $f = aX^2 + (b+c)X + bc/a$ has a monic linear factor. Then this factor must be either $X + b/a$ or $X + c/a$, neither of which is in $R[X]$ since $a \nmid b$ and $a \nmid c$.

Theorem 4.9. *Let $K \subset L$ be integral domains such that $K^\times \neq L^\times$. Then $R = K + XL[X]$ is not square-factorial.*

Proof. For the proof, take $\alpha \in L^\times \backslash K^\times$, and consider the equation $X^2 = (\alpha X)(\alpha^{-1} X)$. Since X and αX, as well as X and $\alpha^{-1} X$, are nonassociated atoms of R, the assertion follows. □

Theorem 4.10. *Let R be an atomic integral domain. Then $R[[X]]$ quasi-2-factorial implies that R is factorial.*

Proof. In the proof of Theorem 4.8, replace the terms $aX + b$ and $aX + c$ by $a + bX$ and $a + cX$. Then $a + bX$ and $a + cX$ are atoms in $R[[X]]$ and $(a + bX)(a + cX) = a^2 + a(b + c)X + bcX^2 = a(a + (b + c)X + (bc/a)X^2)$ are two distinct factorizations of $(a + bX)(a + cX)$ into two atoms. □

References

[1] D.D. Anderson, D.F. Anderson and M. Zafrullah, Atomic domains in which almost all atoms are prime, Comm. Algebra 20 (1992) 1447–1462.

[2] D.D. Anderson and J.L. Mott, Cohen–Kaplansky domains: integral domains with a finite number of irreducible elements, J. Algebra 148 (1992) 17–41.

[3] D.D. Anderson, J.L. Mott and M. Zafrullah, Finite character representations for integral domains, Boll. UMI 6-B (1992) 613–630.

[4] D.D. Anderson and M. Zafrullah, Weakly factorial domains and groups of divisibility, Proc. Amer. Math. Soc. 109 (1990) 907–913.

[5] S.T. Chapman, On the Davenport constant, the cross number and their application in factorization theory, in: D.E. Dobbs and D.F. Anderson (Eds.), Zero-Dimensional Commutative Rings (Marcel Dekker, New York, 1995) 167–190.

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

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

[8] L.G. Chouinard II, Krull semigroups and divisor class groups, Canad. J. Math. 33 (1981) 1459–1468.

[9] A. Geroldinger, On the structure and arithmetic of finitely primary monoids, Czech. Math. J., to appear.

[10] A. Geroldinger and F. Halter-Koch, Non-unique factorizations in block semigroups and arithmetical applications, Math. Slovaca 42 (1992) 641–661.

[11] A. Geroldinger, F. Halter-Koch and J. Kaczorowski, Non-unique factorizations in orders of global fields, J. Reine Angew. Math. 459 (1995) 89–118.

[12] R. Gilmer, Commutative Semigroup Rings (The University of Chicago Press, Chicago and London, 1984).

[13] F. Halter-Koch, On the factorization of algebraic integers into irreducibles, Coll. Math. Soc. János Bolyai 34 (1984) 699–707.

[14] F. Halter-Koch, Divisor theories with primary elements and weakly Krull domains, Boll. UMI 9-B (1995) 417–441.

[15] F. Halter-Koch, Elasticity of factorizations in atomic monoids and integral domains, J. Th. Nomb. Bordeaux 7 (1995) 367–385.

[16] U. Krause, On monoids of finite real character, Proc. Amer. Math. Soc. 105 (1989) 546–554.

[17] L. Skula, Divisorentheorie einer Halbgruppe, Math. Z. 114 (1970) 113–120.