Square-free ideals and SR condition

Łukasz Matysiak
Kazimierz Wielki University
Bydgoszcz, Poland
lukasz.matysiak@ukw.edu.pl

May 23, 2023

Abstract

In this article, we introduce the concept of a square-free ideal in any ring. We study equivalent definitions and some algebraic properties. In addition, we reformulate Hilbert's Nullstellensatz for square-free ideals. We also study ideals in Boolean rings that are square-free. In the second part of this article, we discuss an SR condition and examine this condition against other conditions such as atomicity, AP, ACCP, factoriality in a commutative cancellative monoid.

1 Introduction

By a ring we mean a commutative ring with unit. The domain is a ring (commutative with unit) without zero divisors. Whereas by a monoid we mean a commutative cancellative monoid. For a given ring R, by R^* we denote a group of invertible elements of R.

The motivations for this article come from different directions. The first direction is the theory of radical ideals. First of all, it comes from the works of A. Reinhart's [9] and [8], where in 2012 he introduced the concept of the radical element in [9]. An element of a monoid is called radical if the principal ideal generated by this element is a radical ideal. The set of all radical elements in the monoid/ring R we denoted by $\mathrm{Rad}(R)$. Let us recall the definition of the radical ideal:

Keywords: Boolean ring, factorization, ideal, radical, square-free .
2010 Mathematics Subject Classification: Primary 13A15, 13A05, Secondary 06E20.

Definition 1.1. Let R be a ring. The ideal I of R is called a radical ideal if for any $x \in I$, $n \in \mathbb{N}$, if $x^n \in I$, then $x \in I$.

It is well known that any maximal ideal of R is a prime ideal, and every prime ideal is radical, as can easily be proved. On the other hand, it is known that any prime element is an irreducible and that any prime element is a radical element of R. In [3] it was shown that any radical element is square-free. Recall:

Definition 1.2. We call an element $s \in R$ square-free if we cannot represent it as $s = x^2y$, where x, $y \in R$, but $x \notin R^*$. The set of square-free elements of the ring/monoid R is denoted by $\operatorname{Sqf} R$.

It is very obvious that any irreducible element is square-free. Thus, seeing some relations between irreducible, prime, radical, and square-free elements and maximal, prime, radical, and square-free ideals, we can define a square-free ideal of R that would be a radical ideal, but any maximal ideal would be a square-free.

In the section 2 in the Definition 2.1 we present a definition of a square-free ideal, which is analogous to the definition of a square-free number. In Theorem 2.3 we present five more equivalent definitions of the square-free ideal. However, if we consider square-free ideals in a Dedekind ring, we can use an additional equivalent definition (Corollary 2.4). Recall, the ring R is called a Dedekind ring if every non-zero proper ideal can be represented as a product of prime ideals. Just as the prime, maximal and radical ideals have their interpretation on quotient rings, in Theorem 2.5 we present an interpretation for the square-free ideal, i.e. R/I is not a Boolean ring (or is a non-Boolean ring). Recall:

Definition 1.3. A ring R is called a Boolean ring if $x^2 = x$ for each $x \in R$, i.e. eevery x is idempotent.

This means that the ring in which we find a non-idempotent will be called a non-Boolean ring. The statements 2.6, 2.10 show that every maximal ideal is square-free and then is radical.

Guided by the theory of radical ideals, it is not difficult to come across Hilbert's Nullstellensatz, which is very well known in algebraic geometry. This theorem says that there is a mutually unambiguous correspondence between the algebraic sets in K^n and the radical ideals in $K[T]$, where K is an algebraically closed field. Therefore, another question arose. Since every square-free ideal is radical, but not vice versa, there are radical ideals that are square-free and there are radical ideals that are not square-free (see 2.11, 2.12). So, is it possible to reformulate Hilbert's Nullstellensatz for radical ideals that are square-free and which are not? The answer is positive. For radical square-free ideals there is a one-to-one correspondence with smooth manifolds in K^n (Theorem 3.2), and for non-square-free radical ideals there is one-to-one correspondence with unequal manifolds in K^n (Theorem 3.3). In both cases, of course, K is an algebraically closed field.

Section 4 is motivated by Theorem 2.5 which says that the ideal I of the ring R is a square-free ideal if and only if R/I is not a Boolean ring. Equivalent conditions for the square-free ideal (Theorem 2.3) prompted thinking about idempotents, and at first it was superficial to think that square-free ideals had a great deal to do with Boolean rings. Therefore, the section 4 was created by initial misconceptions and deals with considerations of Boolean rings. As it turned out, square-free ideals are related to non-boolean rings, and in the section 4 we present some very interesting results about ideals in Boolean rings. In Theorem 4.1 we show that all ideals in a Boolean ring are square-free. On the other hand, in Theorem 4.2 we show that the concepts of prime, maximal, square-free, radical and primary ideals are equivalent. Recall that the ideal I of the ring R is called a primary ideal if for any x, $y \in R$ the condition $xy \in I$ implies that either $x \in I$ or $y^n \in I$ for some $n \in \mathbb{N}$.

The motivation of the section 5 is to work on square-free and radical factorizations in any monoid (cancellative commutative). Of course, the focus is on monoids, but the results transfer analogously to any commutative rings with unit without zero divisors. Many results can be found in the articles [4], [3], [5], [7]. In [5] Sections 3, 4 and [7] Sections 4, 5 we show different conditions for square-free and radical factorizations in monoids with certain properties: factoriality, ACCP, atomicity, GCD, pre-Schreier, AP, SR. Let us recall the definitions from papers [5], [7]:

Definition 1.4. A monoid H is called

(a) a GCD-monoid if any two elements have their greatest common divisor.

(b) a pre-Schreier monoid if any element $a \in H$ satisfies the condition that for any $b, c \in H$ such that $a \mid bc$ there are $a_1, a_2 \in H$ such that $a = a_1a_2$, $a_1 \mid b$ and $a_2 \mid c$. The name comes from the Austrian mathematician Otto Schreier, who defined Schreier rings (completely closed rings satisfying the above condition). Pre-Schreier rings reject complete closure.

(c) atomic if each element of $a \in H \setminus H^*$ is the product of a finite number of irreducible elements (atoms).

(d) factorial if for any non-invertible element $a \in H$ the element a can be uniquely represented as a product of primes. In rings, the equivalent is an unique factorization domain.

(e) an ACCP-monoid if any ascending chain of principal ideals of H stabilizes, i.e. for any sequence of principal ideals $a_0H \subset a_1H \subset a_2H \subset \ldots$ exists $m \in \mathbb{N}_0$ such that $a_nH = a_mH$ for any $n \geqslant m$.

(f) an AP-monoid if any non-invertible element of H is prime.

(g) an SR-monoid if any square-free element of H is a radical element.

The definition of a pre-Schreier monoid was introduced by Zafrullah in [10]. The definition of an SR-monoid was defined in [5]. Although the SR condition is used in the context of factorization, some basic properties of such a condition have been developed in this article. In addition, in the sections 5 and 6, we complete the dependencies between these conditions. Then, taking into account the new results, we obtain the following relationship:

$$\begin{array}{ccccccccc}
factorial & \Rightarrow & ACCP & \Rightarrow & atm & \Rightarrow & SFD & \Leftarrow & RFD \\
\Downarrow & & \Uparrow & & \Uparrow & \searrow & \Uparrow & & \\
GCD & \Rightarrow & pSch & \Rightarrow & AP & \Rightarrow & SR & &
\end{array}$$

In the diagram we also have RFD and SFD properties that have been included. These are the conditions $0r$ and $0s$ found in papers [5] and [7], i.e.

Definition 1.5. A monoid H is called RFD/SFD-monoid (radical factorization domain/square-free factorization domain), if for every non-invertible element $a \in H$ there exist $r_1, r_2, \ldots, r_n \in \operatorname{Rad} H/\operatorname{Sqf} H$ such that

$$a = r_1 r_2 \ldots r_n.$$

It is worth noting that Reinhart in [9] investigates the properties of radically factorial monoids (RFD property). In addition, it is worth extracting the relationships between the properties of factoriality, atomicity, RFD and SFD. These definitions are almost identical due to the factorization of the elements, but depending on what elements we decompose.

$$\begin{array}{ccc}
factorial & \Rightarrow & atm \\
\Downarrow & & \Downarrow \\
RFD & \Rightarrow & SFD
\end{array}$$

In addition, in the section 6, we complete some properties of the square-free and radical factorial monoids, where we obtain the following relations:

$$atm + AP \Leftrightarrow faktorialny$$
$$SR + SFD \Rightarrow RFD$$
$$SR + atm \Rightarrow RFD$$

2 Square-free ideals

In this section we define the notion of a square-free ideal in any ring. We will show the basic properties that are studied in the case of prime, maximal and radical ideals. We will also show that square-free ideals are related to non-Boolean rings.

Definition 2.1. Let R be a ring. The ideal I of R is called a square-free ideal if we cannot express in the form

$$I = J^2K,$$

where J, K are ideals of R, with J being a proper ideal.

Example 2.2. If $n \in \operatorname{Sqf} \mathbb{Z}$, then $(n) = n\mathbb{Z}$ is a square-free ideal. Moreover, if n is not prime, then the ideal (n) is not a maximal ideal, because is contained in the proper ideal (p) where $p \mid n$.

In the following theorem we will introduce several equivalent conditions for the definition of the square-free ideal, which we will use in later results.

Theorem 2.3. *Let R be any ring. Let I be the ideal of R. Then the following conditions are equivalent:*

(a) *I is a square-free ideal.*

(b) *For each $a \in R$ there are at most one element b, $c \in R$ such that $b^2 \mid a$, c^2 mida imply $b \sim_I c$ (b and c are associated with I).*

(c) *For each $x \in R$, if $x^2 \in I$, then $x \in I$.*

(d) *For each x, $y \in R$, if $x^2y \in I$, then $xy \in I$.*

(e) *I is not contained in any ideal J^2, where J is a proper ideal of the ring R.*

(f) *For any $x \in R$ $x^2 - x \in I$ holds.*

Proof. (*b*) $\Rightarrow$ (*a*) Assume (b). Suppose $I = J^2K$, where J, K are ideals of R, J is proper. Let $a \in J$. Then $a^2 \in J^2 \subseteq J^2K = I$. By assumption, we know that there is at most one element in $b \in R$ such that $b^2 \mid a^2$ in I. But we also know that $a \mid a^2$ in I and $(aK) \mid (aK)^2 \subseteq J^2K = I$. So $a \sim aK$ or $u \in R^*$ such that $uaK = a$ or $ua \in K$ exists. Since J is proper, then $u \neq \pm is1$, so $ua \neq \pm a$. That is, $ua \in K \setminus \{\pm a\}$. But this means that K is not proper because it contains an element outside of $\{\pm a\}$ that divides $\pm a$, i.e. it contains an invertible element. Contradiction.

(*a*) $\Rightarrow$ (*c*) Assume (a). Let $x \in R$ such that $x^2 \in I$. Suppose $x \notin I$. Then consider the ideal $J := xR + I$, which is proper because it does not contain unit (if it did, the condition $1 = ax + b$, a, $b \in R$ implies that $x = (1-b)a^{-1} \in I$, contradiction).

Note that $J^2 \subseteq I$ because if c, $d \in J$, then $c = ax_1 + b_1$, $d = ax_2 + b_2$, where a, b, x_1, $x_2 \in R$ and we have $cd = a^2x_1x_2 + ab_1x_2 + ab_2x_1 + b_1b_2$. Since $x^2 \in I$, then $a^2x_1x_2 \in I$ and $ab_1x_2 \in I$, $ab_2x_1 \in I$. Also $b_1b_2 \in I$, because b_1, $b_2 \in I$. So cd is the sum of the elements of I, so $cd \in I$. Hence $J^2 \subseteq I$. But that means $I = J^2K$. Contradiction with the assumption, because J is a proper ideal.

(*c*) $\Rightarrow$ (*d*) Assume (c). Let x, $y \in R$ such that $x^2y \in I$. Then $x^2y^2 = (xy)^2 \in I$. By assumption we have $xy \in I$.

(*d*) $\Rightarrow$ (*b*) Assume (d). Let $a \in R$ such that $b^2 \mid a$, $c^2 \mid a$ for some b, $c \in R$. That is, there are d, $e \in R$ such that $a = b^2d$, $a = c^2e$. Then $b^2d, c^2e \in aR$. From (d) we have that $bd, ce \in aR$. Then there are f, $g \in R$ such that $bd = af$, $ce = ag$. Since $a = b^2d = c^2e$, then the equations $bd = b^2df$, $ce = c^2eg$ show that b, $c \in R^*$. So $b \sim_I c$.

(*a*) $\Leftrightarrow$ (*e*) Obvious.

(*c*) $\Rightarrow$ (*f*) Of course, if $x \in I$, then $x^2 \in I$. The assumption is that if $x^2 \in I$, then $x \in I$. So $x^2 - x \in I$.

Let's assume (*f*). Let $x, r \in R$ and $x^2 \in I$. Then $rx^2 = (rx)x = x(rx)$ belongs to I. So $rx^2 - rx = rx(x-1)$ belongs to I. But since $rx^2 - rx \in I$, the assumption is that $rx \in I$. And since $rx \in I$ for any $r \in R$, then especially for $r = 1$ we have $x \in I$.

□

Corollary 2.4. *If in the above theorem we assume that* R *is a Dedekind ring, then conditions (a) – (f) are equivalent to the following condition:*

(g) $I = M_1 \dots M_n$, *where* M_i *are pairwise maximal ideals for* $i = 1, 2, \dots n$.

In Theorem 2.5 we present an interpretation of the quotient ring R/I, where I is a square-free ideal in the ring R.

Theorem 2.5. *Let R be an integral domain. Then the following conditions are equivalent:*

(a) *The ideal I of the ring R is a square-free ideal.*

(b) *The quotient ring R/I is not a Boolean ring.*

Proof. $(a) \Rightarrow (b)$ Suppose that R/I has some idempotent different from 0 and 1. That is, there is an element $r \in R$ such that $(r+I)^2 = r+I$, $r+I \neq 0$, $r+I \neq 1$. Then we have $r^2+I = r+I$, which is $r^2 - r \in I$. Note that $r^2 - r = r(r-1)$. Since I is a square-free ideal, we cannot represent it as $I = J^2K$, where J and K are ideals, J proper. So neither J nor K can be trivial ideals. But since $r(r-1) \in I = J^2K$, then either $r \in J$ or $r \in K$ or $r-1 \in J$ or $r-1 \in K$. Contradiction.

$(b) \Rightarrow (a)$ Suppose that I is not a square-free ideal. That is, there are ideals J and K such that $I = J^2K$ and J is proper. Let's take any element $r \in J$ but $r \notin K$. Such an element exists because J is proper. Then $r^2 \in J^2 \subset I$, which is $r^2 + I = 0 + I$ in R/I. So $(r+I)^2 = 0+I$. On the other hand, since $r \notin K$, then r is not in $J^2K = I$, which is $r+I \neq 0+I$ in R/I. So $(r+I)^2 \neq r+I$ in R/I. We have found that $r+I$ is idempotent different from 0 and 1 in R/I. Contradiction with the assumption that R/I is a ring without idempotents. □

Now we will discuss the relationship between square-free ideals and other ideals.

Proposition 2.6. *If I is a maximal ideal of R, then I is a square-free ideal of R.*

Proof. 1st way:
Suppose I is a maximal ideal of R, and suppose I is not a square-free ideal. Let $x \in R$ such that $x^2 \in I$. Then $J := xR + I$. But $I \subset J$ and I is maximal. Contradiction. So $x = 0$ (then $J = I$) or $x \in I$ (then also $J = I + I = I$).

2nd way:
If I is a maximal ideal, then the quotient ring R/I is a field. By the Lemma 2.13 (which we will prove later), R/I is not a Boolean ring. By Theorem 2.5 we have that I is a square-free ideal. □

Corollary 2.7. *Any ideal of R is contained in some square-free ideal.*

Proof. This follows from the statement that any ideal is contained in some maximal ideal, and every maximal ideal is a square-free ideal. □

Example 2.8. An ideal (0) is square-free, but is not maximal.

Example 2.9. An ideal (x^2+1) of $\mathbb{Q}[x]$ is square-free. If it wasn't, then x^2+1 would have to be divisible by the square of the irreducible polynomial. But x^2+1 is irreducible in $\mathbb{Q}[X]$, contradiction. This ideal is not maximal because it is contained in the ideal $(x^2+1, x+1)$.

Proposition 2.10. *If I is a square-free ideal of R, then I is a radical ideal of R.*

Proof. Let $x \in R$ such that $x^n \in I$ for any $n \in \mathbb{N}$. Since I is a square-free ideal, then $n = 1$, and so $x \in I$. Hence I is a radical ideal. □

In the examples below, we show that the converse statement of Proposition 2.10 is not true.

Example 2.11. An ideal (x^2) of $\mathbb{Q}[x]$ is radical, because its radical is (x), which contains in (x^2), and we have $Rad(x^2) \subset (x^2)$. But ideal (x^2) is not square-free, because $(x^2) = (x)^2$

Example 2.12. An ideal (x^3, y^2) is radical of $\mathbb{Q}[x]$, because $Rad(x^3, y^2) = (x, y) \subset (x^3, y^2)$. This ideal is not square-free because $(x^3, y^2) = (x, y)^2(x, y)$.

Lemma 2.13. *Let R be a field. Then R is not Boolean ring.*

Proof. Suppose that R is a Boolean ring. Then every element in R is idempotent, i.e. $x^2 = x$ for every $x \in R$. Let's consider two cases:

Let R be of the characteristics zero. Then for every natural number n we have $n1 \neq 0$. So we can write: $(n1)^2 = (n1)(n1) = n^2 1$ and $(n1)^2 = n1$. Comparing these two equations we get: $n(n-1) = 0$. Since n is a positive integer, then $n \neq 0$ and $n - 1 \neq 0$. So we have a contradiction with the assumption that R has no zero divisors (since R is a field).

Now let R be the characteristics of p, where p is prime. Then for every positive integer n we have $pn1 = 0$. So we can write: $(pn1)^2 = (pn1)(pn1) = p^2n^2 1$ and $(pn1)^2 = pn1$. Comparing these two equations we get: $p(pn-n) = 0$. Since p is prime, then $p \neq 0$ and $pn - n \neq 0$. So we have a contradiction with the assumption that R has no zero divisors. □

3 Hilbert's Nullstellensatz for square-free ideals

From Proposition 2.10 we know that any square-free ideal is radical in the ring R. The examples 2.11 and 2.12 show that Proposition 2.10 cannot hold in the reverse case. So we have two kinds of radical ideals. Those that are square-free and those that are not square-free. A question has arisen that relates to Hilbert's Nullstellensatz.

Theorem 3.1 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field. There is a mutually unambiguous correspondence between the algebraic sets in K^n and the radical ideals in $K[T]$.*

Can the above theorem be transformed into radical ideals that are square-free and into radical ideals that are not square-free? It turned out that we can and we present the results below.

Theorem 3.2. *Let K be an algebraically closed field. There is a mutually unambiguous correspondence between square-free ideals in $K[T]$ and smooth manifolds in K^n.*

Proof. We first show that if I is a square-free ideal in $K[T]$ then $V(I)$ is a smooth manifold. Equivalently, we will show that for every $P \in V(I)$ the Jacobian matrix of the system of equations with I has full rank in P.

Suppose that there is a point $P \in V(I)$ at which the Jacobian matrix of the system of equations with I has a rank less than n. Then there is a non-zero vector v belonging to the Jacobian matrix in P. Let $f_1, \ldots, f_m$ be ideal generators I. Then we have $\dfrac{\partial f_i}{\partial x_j}(P)v_j = 0$ for each $i = 1, \ldots, m$, $j = 1, \ldots, n$. Let $g(x) = f_i(x + tv)$, where t is an additional variable. Then g is a polynomial of one variable and we have $g(P) = 0$ and $g'(P) = 0$ for each i. So g has a double root in P for each i. But that means $(x - P)^2 \mid g(x)$, which is $(x - P)^2 \in I$. Since I is a square-free ideal, then $(x - P) \in I$, which means that $V(I)$ is a one-point set. Contradiction to the assumption that I is irreducible. So $V(I)$ is a smooth manifold.

We now show that if V is a smooth manifold, then $I(V)$ is a square-free ideal in $K[T]$. Suppose that there is a polynomial $f \in K[T]$ such that $f^2 \in I(V)$ but $f \notin I(V)$. Then f does not vanish across V, so there is a point $p \in V$ such that $f(p) \neq 0$. Since V is a smooth manifold, the Jacobian matrix of the system of equations with $I(V)$ has full rank in p. So there is a vector v belonging to the Jacobian kernel in p. Let $g(t) = f(p + tv)$, where

t is an additional variable. Then g is a polynomial of one variable and we have $g(0) = f(p) \neq 0$, $g'(0) = 0$. So g has a single root in 0. But that means $t-0 \mid g(t)$, which is $t-0 \mid f(p+tv)$ for every $t \in K$. Since $p+tv \in V$ (because V is closed), we get a contradiction with the assumption that $f^2 \in I(V)$. So $I(V)$ is a square-free ideal. □

Theorem 3.3. *Let K be an algebraically closed field. There is a mutually unambiguous correspondence between non-radical square-free ideals in $K[T]$ and unequal manifolds in K^n.*

Proof. We will show that if I is a non-radical square-free ideal in $K[T]$ then $V(I)$ is an unequal manifold.

Suppose that there is a point $p \in V(I)$ where the Jacobian matrix of the system of equations with I has full rank. Then there is a local isomorphism between the neighborhood of p and the neighborhood of 0 in K^n. So $V(I)$ is locally equal to p. But this means that I is a square-free ideal in the neighborhood of p, a contradiction.

We will show that if V is an unequal manifold, then $I(V)$ is a square-free, non-radical ideal in $K[T]$.

Since V is an unequal manifold, there exists a point $p \in V$ where the Jacobian matrix of the system of equations with $I(V)$ is of rank less than n. Then there is a non-zero vector v belonging to the Jacobian matrix at p. Let $f(x) = xv$, where $x = (x_1, \ldots, x_n)$. Then f is a linear polynomial and we have $\dfrac{\partial f}{\partial x_j}(p)v_j = v_j^2$ for every $j = 1, \ldots, n$. Let $g(t) = f(p+tv)$, where t is an additional variable. Then g is a quadratic polynomial and we have $g(0) = 0$, $g'(0) = 0$. So g has a double root in 0. But that means $(t-0)^2 \mid g(t) = f(p+tv)^2$ for every $t \in K$. Since $p + tv \in V$ (because V is closed), we get $f^2 \in I(V)$. However, $f \notin I(V)$ because $f(p) \neq 0$.

□

Example 3.4. (1) Let $X = \{1, 2\}$. Then $I(X) = (T-1, T-2)$ is a square-free ideal and $V = \{1, 2\}$. The set V is a smooth manifold.

(2) Let $X = \{0, 1\}$. Then $I(X) = (T, T-1)$ is a radical non-square-free ideal and $V = \{0, 1\}$ is an unequal manifold with singularities at 0.

(3) An ideal $I = (T^2+1)$ is square-free in $K[T]$, whereas $V(I) =$ is smooth.

(4) An ideal $I = (T^3 - T)$ is radical non-square-free in $K[T]$, whereas $V(I) = \{0, 1, -1\}$ is an unequal manifold with singularities at 0.

4 Boolean ring

Initially it was thought in Theorem 2.5 that the ideal I is square free if and only if R/I is a Boolean ring. Of course, the truth is different. But in connection with this, ideals in the Boolean ring began to be considered, where, as it turned out, all ideals are square-free.

Theorem 4.1. *Let R be a Boolean ring. Then all ideals of R are square-free.*

Proof. Let R be a Boolean ring and let I be an ideal in R. Suppose that I is not a square-free ideal, i.e. there are ideals J and K in R such that $I = J^2K$, where J is proper. Let $x \in J$. Then $x^2 \in J^2$, so $x^2 \in I$. Because $x^2 = x$, so $x \in I$. So J is a proper subset. Let $y \in I$. Then $y^2 \in I$ because every element of a Boolean ring is idempotent. So I is a subset of I^2. Since I^2 is a subset of I, then $I = I^2$. Since $I = I^2$, we cannot have $I = J^2K$, where J is a proper subset of I. We got a contradiction with the assumption. So I is a square-free ideal. □

Perhaps the fact that all ideals in a Boolean ring are square-free is surprising, the following Theorem shows us that the concepts of prime, maximal, square-free, radical, and primary ideals are equivalent.

Theorem 4.2. *Let R be a Boolean ring and let I be an proper ideal in R. Then the following conditions are equivalent:*

(a) *An ideal I is prime.*

(b) *An ideal I is maximal.*

(c) *An ideal I is square-free.*

(d) *An ideal I is radical.*

(e) *An ideal I is primary.*

Proof. Of course, there are the following implications:

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

Also, from Proposition 2.6) we get $(b) \Rightarrow (c)$, and from Proposition 2.10 we get $(c) \Rightarrow (d)$. Of course, we also have $(a) \Rightarrow (e)$.

$(a) \Rightarrow (b)$ Let I be a prime ideal, and suppose I is not a maximal ideal. Then there is an ideal J in R and $x \in R$ such that $x \in J \setminus I$. Since R is a Boolean ring, then $x^2 = x$. Then $x(x-1) = 0$. Since I is prime, then $x \in I$

or $x-1 \in I$ (because $0 \in I$). If $x \in I$, then we have a contradiction. If $x-1 \in I$, then $x \in I+(1)=R$, contradiction. So I is a maximal ideal.

$(d) \Rightarrow (a)$ Let I be a radical ideal, and suppose it is not a prime ideal, that is, there are $a, b \in R$ such that $ab \in I$, $a \notin I$, $b \notin I$. Since $ab \in I$, then $(ab)^n \in I$. But R is a Boolean ring, so $(ab)^n = ab$. So $ab \in \mathrm{Rad}(I)$, which is $a \in \mathrm{Rad}(I)$ or $b \in \mathrm{Rad}(I)$. Suppose $a \in \mathrm{Rad}(I)$. This means $a^m \in I$ for some m. But R is a Boolean ring, so $a^m = a$. So $a \in I$, a contradiction. We prove similarly for $b \in \mathrm{Rad}(I)$. So I is a prime ideal.

$(e) \Rightarrow (d)$ Let I be a primary ideal. Let $a \in R$. Then $a^2 = a$ because R is a Boolean ring. So if $a \in \mathrm{Rad}(I)$ then $a^n \in I$ for some n. But then $a = a^n \in I$. So $\mathrm{Rad}(I) \subset I$.

On the other hand, if $a \in I$ and M is a maximal ideal containing I, then $a \in M$. So I is included in $\mathrm{Rad}(I)$ because $\mathrm{Rad}(I)$ is also the Jacobson radical of the ideal I, that is, the intersection of all maximal ideals containing I. So $I = \mathrm{Rad}(I)$ and I is a radical ideal. □

Corollary 4.3. *In a Boolean ring, all ideals are simultaneously maximal, prime, square-free, radical, primary.*

Note the following fact.

Theorem 4.4. *Let R be a field of 2 with more than 2 elements. Then R is not a Boolean ring.*

Proof. Let R be a field of characteristic q. By R^* let us denote the multiplicative group of the field R. This group is cyclical. Then there is an element $a \in R^*$ such that $R^* = \{1, a, a^2, \dots, a^q\}$, where q is the number of elements in the field R. If a is idempotent then $a^2 = a$ and $a = 1$ or $a = 0$. But $a \neq 0$ because $a \in R^*$ and $a \neq 1$ because R^* has more than one element. So a cannot be idempotent. So R cannot be a Boolean ring. □

Corollary 4.5. *The field of the characteristic 2 with 2 elements is a Boolean ring.*

Although a Boolean algebra is not the same as a Boolean ring, there has been interest in Boolean rings which may be isomorphic to certain Boolean algebras.

Example 4.6. The field $\mathbb{Z}_2$ is a Boolean ring. It is isomorphic to a Boolean algebra with two elements 0 and 1.

Example 4.7. The set of all subsets of the fixed set X is a Boolean ring. It is isomorphic to the Boolean algebra B where $|B| = 2^{|X|}$.

Example 4.8. $\mathbb{Z}_2^n$ is a finite dimensional Boolean ring. It is isomorphic to the Boolean algebra of n logical variables or as a set of n-bit binary words with XOR and AND.

Example 4.9. The set of continuous functions $f\colon \mathbb{R} \to \{0,1\}$ with pointwise addition and multiplication modulo 2 is a Boolean ring of uncountable dimension. Such a set of continuous functions is isomorphic to the Boolean algebra of logical functions, a set of continuous digital signals.

Example 4.10. A ring of boolean functions, where the elements are boolean functions on some set X (i.e. functions that take the value 0 or 1), and the operations are a logical union and product. The ring of boolean functions is isomorphic to the ring of residuals modulo 2^n, where n is the number of all boolean functions in X.

Example 4.11. The Boolean ring modulo n is isomorphic to the ring of regular functions on an algebraic manifold given by the equation $x^{2n} - 1 = 0$ over $\mathbb{F}_2$.

Example 4.12. A Boolean ring modulo n is isomorphic to a Boolean algebra on the set of residuals modulo n. It suffices to show that the mapping $f\colon \mathbb{Z}_n \to B_n$ given by $f(x) = x(x-1) \pmod{n}$ is an isomorphism.

5 SR condition

The concept of the SR condition was created in the papers [5] and [7], but in the context of factorial properties. In this section, we will show the relationship between the SR condition and other known conditions. Considering the previous section, it can be concluded that every Boolean ring satisfies the SR condition, since the notion of a radical element coincides with the notion of a square-free element. Recall that in every ring the radical element is square-free, but the reverse is not generally true. Thus, the need arose to be interested in rings and monoids in which the square-free element will be radical.

Example 5.1. Let V be the valuation domain with its maximum ideal M. Let K be its fraction field other than V such that $M^{-1} = V$, and let L be a non-trivial extension of K. Then $D = V + XL[[X]]$ satisfies the SR condition, but is not pre-Schreier.

Proposition 5.2. *If H is atomic then H is SR.*

Proof. Suppose $a \in \operatorname{Sqf} H$ and let $a \mid x^n$ for any $x \in H$. Then there is $y \in H$ such that $ay = x^n$.

Since H is atomic, a and x^n can be represented as products of a finite number of irreducible elements. Let $a = p_1p_2 \dots p_k$ and $x^n = q_1q_2 \dots q_m$ be such products. Then

$$ay = p_1p_2 \dots p_ky = q_1q_2 \dots q_m.$$

Since a is a square-free element, none of the factors of p_i is a square of some non-invertible element. Therefore, each of the factors p_i must be a prime element, otherwise it could be decomposed into two non-zero elements different from each other and from one. Since each of the factors p_i is a prime element, it divides the product $q_1q_2 \dots q_m$ if and only if it divides one of the factors q_j. So each of the factors in p_i must also divide x, because x is $q_1q_2 \dots q_m$ raised to the power of $1/n$.

Since each p_i divides x, then $p_1p_2 \dots p_k$ also divides x. But the product of $p_1p_2 \dots p_k$ equals a, so $a \mid x$. □

Proposition 5.3. *If H is an AP-monoid, then H is an SR-monoid.*

Proof. Let H be a monoid satisfying the condition AP, i.e. every irreducible element is a prime element. Let $x \in H$ be a square-free element. We want to show that x is a radical element.

If x is invertible or zero, then the proof is trivial. So let's assume that x is non-invertible and non-zero. Then we can represent x as the product of a finite number of irreducible elements (because H is an atomic monoid):

$$x = p_1p_2 \dots p_k,$$

where p_i are irreducibles and primes. Now suppose $x \mid r^n$ for some $r \in H$ and $n \in \mathbb{N}$. Then there is $q \in H$ such that $r^n = xq$. From the properties of prime elements, it follows that every factor on the left side must be in the right side, and vice versa. So we have:

$$r^n = p_1^{a_1}p_2^{a_2} \dots p_k^{a_k}q,$$

where $a_i \in \mathbb{N}$. Because r^n is a power of r, then it must be that:

$$r = p_1^{b_1}p_2^{b_2} \dots p_k^{b_k}s,$$

where b_i are positive integers and s is invertible or null. Raising both sides to the n power, we get:

$$r^n = p_1^{nb_1}p_2^{nb_2} \dots p_k^{nb_k}s^n.$$

Comparing both sides of the equality, we get:

$$nb_i = a_i$$

for any $i \in \{1, 2, \ldots, k\}$. Since $n > 0$ i $a_i \geqslant 0$, it must be that $b_i > 0$ for any $i \in \{1, 2, \ldots, k\}$. So we have:

$$x = p_1 p_2 \ldots p_k \mid p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k} s = r$$

which ends the proof. □

Recall that the R monoid/ring satisfies the SFD condition when for any non-zero element $a \in R$ there are $s_1,\ s_2,\ \ldots,\ s_n \in \operatorname{Sqf} R$ such that $a = s_1 s_2 \ldots s_n$.

Proposition 5.4. *If H is SR-monoid, then H satisfies SFD.*

Proof. Let $x \in H \setminus \{0\}$. We want to show that x is a finite product of square-free elements.

If x is a square-free element, then there is nothing to prove. So let's assume that x is not a square-free element.

Since x is not a square-free element, there is a $y \in H$ such that $x = y^2$, where $y \in H$ and $y \notin H^*$. Since $y \notin H^*$, then $y \in \operatorname{Rad} H$. By definition of a radical element, there is $z \in H$ such that $y = z^2$ and z is a square-free element. Then $x = y^2 = z^4$.

We can repeat this process for z until we get a square-free or unit. This process must end after a finite number of steps. This means that x can be expressed as a finite product of square-free elements. □

Example 5.5. For any $k \in \mathbb{N}_0$ let

$$H_k = \{(x, y) \in \mathbb{N}_0^2 \colon x + y = k\}.$$

For any $r \in \mathbb{N}$ consider the following submonoid of $\mathbb{N}_{\geqslant k} \cup \{0\}$:

$$H^{(r)} = \bigcup_{k \in \mathbb{N}_0} H_{kr}.$$

If $r = 1$, then elements $(0, 0), (0, 1), (1, 0)$ are radical and square-free.

If $r = 2$, then elements $(0, 0), (1, 1)$ are radical and elements $(0, 0)$, $(0, 2)$, $(1, 1)$, $(2, 0)$ are square-free.

If $r \geqslant 3$, then element $(0, 0)$ is radical and elements $(0, 0), (0, r), (1, r - 1), \ldots, (r - 1, 1), (r, 0)$ are square-free.

Thus, for $r = 1$, the monoid $H^{(r)}$ satisfies the SR condition.

Also, for $r \geqslant 2$, the monoid $H^{(r)}$ is SFD but not RFD.

Example 5.6. Let H be a non-group monoid in which all elements are squares, e.g. $\mathbb{Q}_{\geqslant 0}$, $\left\langle \frac{1}{2^n} \mid n \in \mathbb{N} \right\rangle$. A monoid H satisfies the SR condition, because $\operatorname{Sqf} H = \operatorname{Rad} H = H^*$.

Example 5.7. Consider the following monoid:

$$H = \langle x_1, x_2, \dots, y_1, y_2, \dots \mid y_i = x_{i+1} y_{i+1}, i = 1, 2, \dots \rangle .$$

H is non-factorial GCD-monoid.

$\operatorname{Irr} H = \operatorname{Prime} H = \{x_1, x_2, \dots\}$, so H is AP-monoid.

$\operatorname{Sqf} H = \operatorname{Rad} H = \{x_1, x_2, \dots, y_1, y_2, \dots\}$, so H is SR-monoid.

There are many examples where AP-rings are SR-rings. But the question arose as to when the implication would be the other way around. The answer is in the statement below.

Proposition 5.8. *Let R be a principal ideal domain. If R is SR-ring, then R is AP-ring.*

Proof. Let $a \in R$ be an irreducible element of R. Then it is a square-free element of R. From the SR assumption, a is a radical element in R. We will show that every irreducible element that is radical is a prime element.

Suppose a is not prime, that is, there are b, $c \in R$ such that $a \mid bc$, $a \nmid b$, $a \nmid c$. Then aR is not a maximal ideal because it is contained in bR or cR which are greater than aR. But since R is a principal ideal ring, the ideal aR is maximal. Contradiction. $\square$

Corollary 5.9. *The above theorem holds obviously in the unique factorization domain.*

Example 5.10. Consider $H = \mathbb{Z}[x]_n$. Then H satisfies the SR condition. Indeed, suppose $a = a_0 + a_1 x + \dots + a_n x^n$ is a square-free element, and suppose there are $b \in \mathbb{Z}$ and $k > 1$ such that $a_i = b^k$ for some i. Then $b^2 \mid a_i$, which means that a has a square divisor. A contradiction, therefore b and k do not exist, i.e. a is a radical element.

H does not satisfy AP because $2x$ is irreducible element, but $2x \mid (2 + x)(2 - x) = 4 - x^2$ does not imply that $2x$ divides $2 + x$ or $2 - x$.

Let's note about polynomial composites. Wiele własności można również znaleźć w pracy [6].

Corollary 5.11. *If $T = K + XL[X]$ is atomic and $\operatorname{Irr} T \subset \operatorname{Gpr} T$, then T is radical factorial.*

Note next Proposition.

Proposition 5.12. *Let K and L be fields such that $K \subset L$ and let $T = K + XL[X]$. Then* $\mathrm{Gpr}(T) = (\mathrm{Gpr}(L[X]) \cap T) \cup \{X^2 h; h \in \mathrm{Gpr}(L[X]), h(0) \notin \{a^2 b; a \in L, b \in K\}\}$.

Example 5.13. Let L be a field with char $(L) = 2$ such that L is not perfect, let K be the prime subfield of L and $T = K + XL[X]$. Then $\mathrm{Sqf}\, T \neq \mathrm{Sqf}(L[X]) \cap T$.

Proof. Since char $(L) = 2$ and L is not perfect, we have $L \neq \{a^2; a \in L\}$. Since $K = \{0, 1\}$, this implies that $L \neq \{a^2 b; a \in L, b \in K\}$. It is an immediate consequence of Corollary 2.4 that $\mathrm{Sqf}\, T \neq \mathrm{Sqf}(L[X]) \cap T$. □

In particular, if $T = \mathbb{R} + X\mathbb{C}[X]$, then $\mathrm{Irr}\, T = \{a + bX; a \in \mathbb{R}, b \in \mathbb{C} \setminus \{0\}\}$ and $\mathrm{Sqf}\, T = \{a \prod_{b \in B}(1 + bX); a \in \mathbb{R} \setminus \{0\}, B \subset \mathbb{C}, B$ is finite$\} \cup \{aX \prod_{b \in B}(1 + bX); a \in \mathbb{C} \setminus \{0\}, B \subset \mathbb{C}, B$ is finite$\}$.

Using Corollary 2.4 we easily verify that if L is algebraically closed, then $K + XL[X]$ fulfills 1s/1r - 6s/6r (see [7]).

If L and K are finite fields and it is a proper extension, then $K + XL[X]$ is a non-factorial ACCP domain (see [1], [2]).

6 Square-free factorial monoids

This section is a supplement to the previous section, with more focus on the SFD condition.

Proposition 6.1. *Let H be a monoid that satisfies the condition AP. Then H is atomic.*

Proof. Suppose H is not atomic. Then there exists $a \in H$ such that a is not the product of a finite number of irreducible elements. Let $a = q_1 q_2 \dots q_n$ be the longest possible product of nonzero elements of H. Then none of the factors q_i can be irreducible, otherwise a would be the product of a finite number of irreducible elements. So each of the factors q_i must be the product of two nonzero different from each other and from unit. Let $q_1 = r_1 s_1$ be such a decomposition. Then $a = r_1 s_1 q_2 \dots q_n$ is a longer product of non-zero elements of H than $a = q_1 q_2 \dots q_n$, which contradicts the maximal product length assumption. So H must be atomic. □

Proposition 6.2. *Let H be a pre-Schreier monoid. Then H is ACCP-monoid.*

Proof. Assume H is a pre-Schreier monoid. Suppose H is not a monoid that satisfies ACCP, i.e. there is an infinite increasing sequence of ideals

$$(a_1) \subset (a_2) \subset \dots$$

Let $x \in H \setminus \{0\}$. Then $x \mid a_n$ for each $n \in \mathbb{N}$ because $(a_n) \subset (x)$. So there are $b_n \in H$ such that $a_n = xb_n$. Since x satisfies a pre-Schreier condition, so is b_n. Note that $b_1 \mid b_2 \mid \dots$, which means that there is $c_n \in H$ such that $b_n = c_n b_{n+1}$. So $a_n = xc_n b_{n+1}$. Since H is pre-Schreier, let $x = x_1 x_2$, $c_n = c_{n1} c_{n2}$, $b_{n+1} = b_{n+1,1} b_{n+1,2}$ such that $x_1 \mid c_{n1}$, $x_2 \mid b_{n+1.1}$, $c_{n2} \mid b_{n+1.2}$ and $b_n = c_{n1} b_{n+1.2}$ for each $n \in \mathbb{N}$. In particular, we have $x_2 \mid b_2 \mid b_4 \mid \dots$ which means that there is $d \in H$ such that $x_2 = db_2$. Inserting into $a_2 = xb_2$ we get $a_2 = db_2 x_1 x_2 = db_2^2 x_1$. Because $a_2 \neq 0$, $a_2 \notin H^*$, is $d \in H^*$. Thus, x_2 is the product of two invertible elements, which contradicts that x satisfies the pre-Schreier condition. $\square$

Proposition 6.3. *If H is an atomic monoid, then H is SFD.*

Proof. Since any non-invertible non-zero element of H is a finite product of irreducible elements, it is a finite product of square-free elements. $\square$

Example 6.4. Consider the monoid $\mathbb{Z}_4$. It is the monoid SFD, but 2 cannot be written as a product of two numbers other than zero and unit, so it is not atomic.

Recall that the monoid/ring R satisfies the RFD condition if for any nonzero element $a \in R$ there are $r_1, r_2, \dots, r_n \in \operatorname{Rad} R$ such that $a = r_1 r_2 \dots r_n$.

Proposition 6.5. *If H is a monoid that satisfies the RFD, then it satisfies the SFD.*

Proof. Since any non-invertible non-zero element of H is a finite product of radical elements, it is a finite product of square-free elements. $\square$

Proposition 6.6. *If H is an SR monoid and is an SFD monoid, then H is an RFD monoid.*

Proof. In H, every non-zero non-invertible element is a finite product of square-free elements. By the SR condition, square-free elements are radical. So H satisfies the RFD condition. $\square$

Proposition 6.7. *If H is a monoid that satisfies the SR condition and is an atomic monoid, then H satisfies the RFD condition.*

Proof. In H, every non-zero non-invertible element is a finite product of irreducible elements that are square-free. By the SR condition, square-free elements are radical. So H satisfies the RFD condition. $\square$

References

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

[2] Eftekhari, S., Khorsandi, M.R., *MCD-finite domains and ascent of IDF property in polynomial extensions*, Commun. Algebra 46, 3865–3872 (2018)

[3] P. Jędrzejewicz, M., Marciniak, Ł. Matysiak, J. Zieliński, *On properties of square-free elements in commutative cancellative monoids*, Semigroup Forum, 100, 850-870 (2020)

[4] P. Jędrzejewicz, Ł. Matysiak, J. Zieliński, *A note on square-free factorizations*, Analytic and Algebraic Geometry 2, Łódź Univ. Press, Łódź, 79-84, (2017)

[5] Matysiak, Ł., *On square-free and radical factorizations and existence of some divisors*, (2021)

[6] Matysiak, Ł., *On properties of composites and monoid domains*, Italian Journal of Pure and Applied Mathematics, 47 (2022), 796-811 3

[7] Matysiak, Ł., *On square-free and radical factorizations and relationships with the Jacobian conjecture*, accepted in The Asian Journal of Mathematics (2022).

[8] Olberding, B., Reinhart, A., *Radical factorization in finitary ideal systems*, arXiv:1903.09237

[9] A. Reinhart, *Radical factorial monoids and domains*, Ann. Sci. Math. Québec, v. 36 (2012), 193–229.

[10] M. Zafrullah, *On a property of pre-Schreier domains*, Communications in Algebra, v. 15, 9 (1987), 1895–1920.