ATOMIC AND AP SEMIGROUP RINGS $F[X;M]$, WHERE M IS A SUBMONOID OF THE ADDITIVE MONOID OF NONNEGATIVE RATIONAL NUMBERS

Ryan Gipson and Hamid Kulosman

ABSTRACT. We investigate the atomicity and the AP property of the semigroup rings $F[X;M]$, where F is a field, X is a variable and M is a submonoid of the additive monoid of nonnegative rational numbers. The main notion that we introduce for the purpose of the investigation is the notion of essential generators of M.

Mathematics Subject Classification (2010): 13F15, 13A05
Keywords: Semigroup ring, atomic domain, AP domain, irreducible element, prime element

1. Introduction and preliminaries

All monoids in this paper are assumed to be submonoids of the additive monoid $\mathbb{Q}_+$ of nonnegative rational numbers.

All the notions that we use but not define in this paper can be found in the standard reference book [4] by R. Gilmer. A very important reference is also the paper [2] by D. D. Anderson, D. F. Anderson and M. Zafrullah.

Let M be a monoid. The elements of the semigroup ring $F[X;M]$, where F is a field and X is a variable, are the polynomial expressions

$$f(X) = a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n},$$

where $a_1, \ldots, a_n \in F$, $\alpha_1, \ldots, \alpha_n \in M$ and, if we do not specifically mention otherwise, $\alpha_1 > \cdots > \alpha_n$. We say that $a_1 X^{\alpha_1}$ is the *leading term* of f, X^{α_1} is the *leading monomial* of f and that α_1 is the *degree* of f. The polynomial expressions $f(X) = a$, $a \in F$, are called the *constant polynomial expressions* (or *constants*), their degree is 0, except for $f(X) = 0$, whose degree is $-\infty$. $F[X;M]$ is an integral domain, the nonzero constants are its only invertible elements. A nonzero nonunit element $f \in F[X;M]$ is called an *irreducible element* or an *atom* if it cannot be written as $f = gh$, where both g, h are nonzero nonunits. A nonzero nonunit element $f \in F[X;M]$ is said to be *prime* if $f \mid gh$ implies $f \mid g$ or $f \mid h$. If every

nonzero nonunit element of $F[X; M]$ can be written as a finite product of atoms, we say that the integral domain $F[X; M]$ is *atomic*.

In general, in integral domains every prime element is irreducible, but not vice-versa. Integral domains in which every irreducible element is prime (i.e., where the notions irreducible and prime coincide) are called *AP domains*.
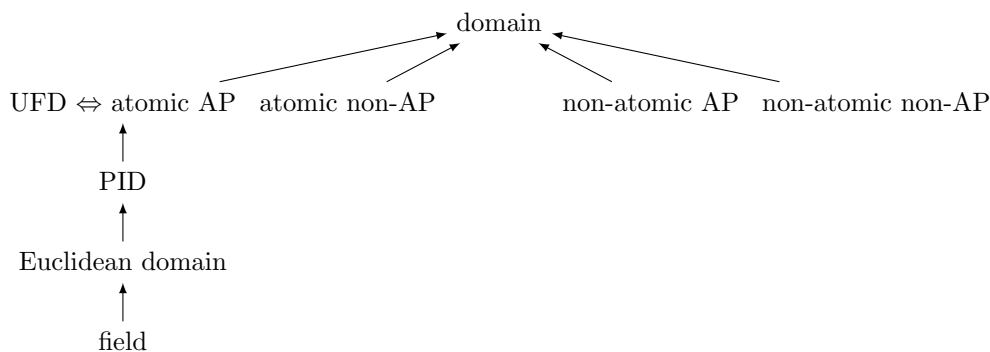
An integral domain R is called a *unique factorization domain (UFD)* if the following two conditions hold:

(i) R is atomic;

(ii) the decomposition of any nonzero nonunit into irreducibles is unique up to associates and the order of the factors.

There is no relation between the notions atomic and AP: an integral domain can be atomic but not AP, and vice-versa, AP but not atomic. It can also be neither atomic, nor AP. Being both atomic and AP is equivalent (as it is easy to show) to being a UFD.

An integral domain R is called a *principal ideal domain (PID)* if every ideal of R is principal.

We have the following implication diagram:

domain

UFD $\Leftrightarrow$ atomic AP   atomic non-AP   non-atomic AP   non-atomic non-AP

PID

Euclidean domain

field

We now describe a factorization process of a nonzero nonunit element of an integral domain. Let R be an integral domain and $x \in R$ a nonzero nonunit. We describe a factorization process of x. If x is irreducible, we stop. If not, we decompose it as $x = x_0 x_1$, where both x_0 and x_1 are nonzero nonunits. If both x_0, x_1 are irreducible, we stop. If not, we take the first from the left of the elements x_0, x_1 which is reducible and decompose it as a product of two nonzero nonunits. Say x_0 is reducible. We decompose it: $x_0 = x_{0,0} x_{0,1}$. Now we have $x = x_{0,0} x_{0,1} x_1$. If all of the $x_{0,0}, x_{0,1}, x_1$ are irreducible, we stop. If not, we take the first from the left of the elements $x_{0,0}, x_{0,1}, x_1$ which is reducible and decompose it as a product

of two nonzero nonunits. Say $x_{0,1}$ is reducible: $x_{0,1} = x_{0,1,0} x_{0,1,1}$. Now we have $x = x_{0,0} x_{0,1,0} x_{0,1,1} x_1$, etc. We call this process a *factorization process* of x. If it stops after finitely many steps, we say that this is a *finite factorization process* of x. If it never stops, we say that this is an *infinite factorization process* of x.

Remark 1.1. *If R is a subring of the domain $F[X]$, F a field, and R contains F, then R is atomic. Indeed, by the degree argument any element $f \in R$ of degree $n \geq 1$ can be decomposed into at most n irreducible factors, so every factorization process of f is finite. (The elements of F are precisely the units of R.)*

Let M, M' be two monoids. A map $\mu : M \to M'$ is called a *monoid homomorphism* from M to M' if $\mu(x + y) = \mu(x) + \mu(y)$ for every $x, y \in M$ and $\mu(0) = 0$. If, in addition, μ is bijective, it is called a *monoid isomorphism* between M and M'. (The inverse bijection $\mu^{-1} : M' \to M$ preserves the operation.) To every monoid homomorphism $\mu : M \to M'$ we can naturally associate a ring homomorphism $\phi : F[X; M] \to F[X; M']$, defined by

$$\phi(a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n}) = a_1 X^{\mu(\alpha_1)} + \ldots a_n X^{\mu(\alpha_n)}.$$

ϕ is an isomorphism if and only if μ is an isomorphism.

Example 1.2. *Let M be a monoid, $\tau \in \mathbb{Q}_+ \setminus \{0\}$. Then $\tau M = \{\tau x \mid x \in M\}$ is a monoid and the map $\mu_\tau : M \to \tau M$, defined by $\mu_\tau(x) = \tau x$, is a monoid isomorphism. Hence the naturally associated map $\phi_\tau : F[X; M] \to F[X; \tau M]$, defined by*

$$\phi_\tau(a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n}) = a_1 X^{\tau \alpha_1} + \ldots a_n X^{\tau \alpha_n},$$

is a ring isomorphism.

The next proposition is easy to prove.

Proposition 1.3. *If $f(X)$ is a divisor in $F[X; M]$ of an element X^α, $\alpha \in M$, then $f(X) = aX^\beta$ with $a \in F$, $\beta \in M$ and $\alpha - \beta \in M$.*

Definition 1.4. We say that a fraction $\dfrac{m}{n}$, $m \in \mathbb{N}_0$, $n \in \mathbb{N}$, is (written) in *reduced form* if $\gcd(m, n) = 1$.

For example, $\dfrac{0}{1}, \dfrac{6}{1}, \dfrac{2}{5}, \dfrac{13}{10}$ are written in reduced form, while $\dfrac{0}{5}, \dfrac{2}{4}$ are not.

Lemma 1.5 (Reduced Form Lemma)**.** *Let $\dfrac{k}{l}, \dfrac{m}{n} \in \mathbb{Q}_+$ be two fractions in reduced form. Then*

$$\frac{k}{l} = \frac{m}{n} \Leftrightarrow k = m \text{ and } l = n.$$

Proof. $\dfrac{k}{l} = \dfrac{m}{n} \Leftrightarrow kn = lm$. Let p^s be a prime power that appears in l but not in n. Let p^t be the power of p that appears in n. Then $0 \leq t < s$. Let $l = p^s \cdot l'$, $n = p^t \cdot n'$. From $kp^t n' = p^s l' m$ we get $p^{s-t} \mid kn'$, a contradiction. Similarly, if we have a prime power that appears in n, but not in l. Hence $l = n$. Then from $kn = lm$, $k = m$. $\qquad\square$

2. Essential generators

Let A be a subset of $\mathbb{Q}_+$. The intersection of all submonoids of $\mathbb{Q}_+$ which contain A is a submonoid of $\mathbb{Q}_+$, in fact, the smallest submonoid of $\mathbb{Q}_+$ containing A. It is called the submonoid *generated* by A and denoted $\langle A \rangle$. We have $\langle \emptyset \rangle = \{0\}$. A nonempty subset A of $\mathbb{Q}_+$ generates a submonoid M of $\mathbb{Q}_+$ if and only if

$$M = \{k_1 a_1 + \cdots + k_n a_n \mid n \in \mathbb{N},\ a_i \in A,\ k_i \in \mathbb{N}_0\ (i = 1, 2, \ldots, n)\}.$$

We call the elements of A *generators* of M. If M can be generated by a finite set A, we say that M is *finitely generated*, otherwise we say that M is *infinitely generated*.

Definition 2.1. An element $a \in M$ is called an *essential generator* of M if $\langle M \setminus \{a\} \rangle \neq M$.

Note that then, in particular, $a \notin \langle M \setminus \{a\} \rangle$.

Examples 2.2.   (i) $M = \mathbb{N}_0 = \langle 1 \rangle$ *is a finitely generated monoid and* 1 *is an essential generator of* M.

   (ii) $M = \langle 2, 5 \rangle$ *is a finitely generated monoid and* $2, 5$ *are essential generators of* M.

   (iii) $M = \mathbb{Q}_+$ *is an infinitely generated monoid with no essential generators.*

   (iv) $M = \langle \dfrac{1}{2}, \dfrac{1}{2^2}, \dfrac{1}{2^3}, \ldots \rangle$ *is an infinitely generated monoid with no essential generators.*

   (v) $M = \langle \dfrac{1}{2}, \dfrac{1}{2^2}, \dfrac{1}{2^3}, \ldots; \dfrac{1}{5} \rangle$ *is an infinitely generated monoid with one essential generator:* $\dfrac{1}{5}$.

   (vi) $M = \langle \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{5}, \ldots \rangle$ *is an infinitely generated monoid and each of the elements* $\dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{5}, \ldots$ *is an essential generator of* M.

   (vii) $M = \{0\}$ *is a finitely generated monoid with no essential generators since* $M = \langle \emptyset \rangle$.

Proposition 2.3. *Let a be an essential generator of M. If $A \subset M$ is a generating set of M, then $a \in A$.*

Proof. Suppose to the contrary, i.e., $a \notin A$. Then $A \subset M \setminus \{a\}$ and $\langle A \rangle = M$, hence $\langle M \setminus \{a\} \rangle = M$, a contradiction. $\square$

Proposition 2.4. *Let A be a generating set of M and let $a \in A$ be such that $\langle A \setminus \{a\} \rangle \neq M$. Then a is an essential generator of M.*

Proof. Suppose to the contrary, i.e.,

$$a = k_1 x_1 + \cdots + k_m x_m, \ x_i \in M \setminus \{a\}, k_i \in \mathbb{N}_0.$$

If each $x_1, \ldots, x_m$ can be generated by the elements of $A \setminus \{a\}$, then a can be generated by the elements of $A \setminus \{a\}$, a contradiction. Hence at least one of the elements $x_1, \ldots, x_m$, when generated by the elements of A, has to use the generator a. Say $x_1 = l_1 a_1 + \cdots + l_n a_n + l_{n+1} a$. Then $a = k_1(l_1 a_1 + \cdots + l_n a_n) + k_1 l_{n+1} a + k_2 x_2 + \cdots + k_m x_m$. Since $x_1 \neq a$, the right hand side (RHS) is bigger than the left hand side (LHS), a contradiction. $\square$

Proposition 2.5. *If $M = \langle A \rangle$, then we can remove from A any finite set consisting of nonessential generators of M and the set A' obtained in that way still generates M.*

Proof. Let $A \setminus A' = \{a_1, a_2, \ldots, a_n\}$. By Proposition 2.4, $\langle A \setminus \{a_1\} \rangle = M$. Assume that $\langle A \setminus \{a_1, \ldots, a_k\} \rangle = M$. Then, again by Proposition 2.4,

$$\langle (A \setminus \{a_1, \ldots, a_k\}) \setminus \{a_{k+1}\} \rangle = \langle A \setminus \{a_1, \ldots, a_k, a_{k+1}\} \rangle = M.$$

It follows that $\langle A \setminus \{a_1, \ldots, a_n\} \rangle = M$, i.e., $\langle A' \rangle = M$. $\square$

Proposition 2.6. *Let M, M' be two monoids, $\mu : M \to M'$ a monoid isomorphism and let $a \in M$. Then a is an essential generator of M if and only if $\mu(a)$ is an essential generator of M'.*

Proof. It is enough to prove that if a is an essential generator of M, $\mu(a)$ is an essential generator of M'. Suppose to the contrary, i.e., $\langle M \setminus \{a\} \rangle \neq M$, however $\langle M' \setminus \mu(a) \rangle = M'$. Let $\mu(a) = b$. We have $b = k_1 y_1 + \cdots + k_n y_n$, where $y_1, \ldots, y_n \in M' \setminus \{b\}$. Let $x_1, \ldots, x_n$ be such that $\mu(x_i) = y_i$. Each of $x_1, \ldots, x_n$ is $\neq a$ (since μ is bijective). Since $\mu(k_1 x_1 + \cdots + k_n x_n) = b$, we have $k_1 x_1 + \cdots + k_n x_n = a$ (since μ is bijective). This contradicts to $\langle M \setminus \{a\} \rangle \neq M$. $\square$

Example 2.7. *A monoid $M = \langle n_1, n_2, \ldots, n_k \rangle$, where $n_1, n_2, \ldots, n_k \in \mathbb{N} = \{1, 2, 3, \ldots\}$ are such that $\gcd(n_1, n_2, \ldots, n_k) = 1$ is called a numerical monoid. For example, $M = \langle 2, 5 \rangle = \{0, 2, 4, 5, 6, 7, \ldots\}$ is a numerical monoid. For this monoid the ring $F[X; M]$ is atomic by Remark 1.1, but is not AP since $X^5 \mid X^{10} =$*

$X^2 \cdot X^2 \cdot X^2 \cdot X^2 \cdot X^2$, however $X^5 \nmid X^2$. The elements $2, 5$ are the essential generators of M. Since $M' = \langle 4, 10 \rangle$ is isomorphic with M (via $\mu_2 : M \to M'$, $\mu_2(x) = 2x$), the ring $F[X; M']$ is isomorphic with $F[X; M]$ (via $\phi_2 : F[X; M] \to F[X; M']$), so $F[X; M']$ is also an atomic non-AP domain. The elements $\mu_2(2) = 4$ and $\mu_2(5) = 10$ are the essential generators of M'. (However M' is not a numerical monoid since $\gcd(4, 10) = 2$.) A similar analysis holds for, for example, $M'' = \left\langle \dfrac{8}{7}, \dfrac{20}{7} \right\rangle$.

Proposition 2.8. *Suppose that a is an essential generator of M and $M \neq \langle a \rangle$. Then X^a is an irreducible non-prime element of $F[X; M]$.*

Proof. Suppose first that there is an element $b \in M$ such that either $0 < b < a$ or b is another essential generator of M. Let $a = \dfrac{p}{q}, b = \dfrac{m}{n}$, both fractions in reduced form. Then $nbp = mp = qam$. Note that $X^a \mid X^{qma}$ since $X^{qma} = X^a \cdot X^{(qm-1)a}$, i.e., $X^a \mid X^{mp} = (X^b)^{np}$, but $X^a \nmid X^b$ (either because $b < a$, or because we would have $b = a + c$ for some $c \in M$, which is not possible since b is an essential generator). Hence X^a ia a non-prime element of $F[X; M]$. On the other side, X^a is irreducible since the relation $X^a = X^{b'} X^{c'}$, $b' \neq 0, c' \neq 0$ (which follows from Proposition 1.3) would imply $a = b' + c'$, which is not possible since a is an essential generator.

Suppose now that a is the smallest non-zero element of M and the only essential generator of M. Consider the intervals $(a, 2a)$, $(2a, 3a)$, $(3a, 4a)$, ... and let $(ma, (m+1)a)$ be the first interval in which we have an element b of $M \setminus \langle a \rangle$. Since b is not an essential generator, then there are non-zero elements $c, d \in M$ such that $c + d = b$. This is not possible since at least one of the elements c, d is $\geq ma$ and the other one is $\geq a$, so that $c + d \geq (m+1)a$, a contradiction. $\square$

Proposition 2.9. *The irreducible elements of $F[X; M]$ of the form X^a, $a \in M$, are precisely the X^a with a an essential generator of M.*

Proof. If a is an essential generator, we cannot have $X^a = X^b X^c$ with $b, c \in M \setminus \{0\}$ since $a = b + c$ implies that a is not essential. Hence, by Proposition 1.3, X^a is irreducible.

Conversely, if X^a is irreducible, we cannot write $a = b + c$ for any $b, c \in M \setminus \{0\}$, hence a cannot be generated by $M \setminus \{a\}$. Hence a is an essential generator of M. $\square$

Proposition 2.10. *If $M \neq \{0\}$ cannot be generated by essential generators, then $F[X; M]$ is not atomic.*

Proof. Suppose to the contrary, i.e., that $F[X; M]$ is atomic. Let A be the set of all essential generators of M. Let $a \in M \setminus \langle A \rangle$ and let $X^a = X^{a_1} X^{a_2} \cdots X^{a_n}$ be an irreducible decomposition of X^a (it has to have this form by Proposition 1.3). Then by Proposition 2.9 each of $a_1, \ldots, a_n$ is an essential generator of M and $a = a_1 + \cdots + a_n$. Hence $a \in \langle A \rangle$, a contradiction. $\qquad\square$

Question 2.11. *Does the opposite direction of Proposition 2.10 hold? In other words, if M can be generated by essential generators, is $F[X; M]$ then necessarily atomic? (The next section provides an example where it is.)*

3. The monoid $M = \left\langle \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{5}, \ldots \right\rangle$

In this section M always denotes the monoid $\left\langle \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{5}, \ldots \right\rangle$.

Lemma 3.1. *Every element $\alpha \in M$ can be uniquely written in the form*

$$\alpha = k + \frac{a_1}{p_1} + \cdots + \frac{a_r}{p_r}, \tag{1}$$

where $k \in \mathbb{N}_0$, $r \geq 0$, $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are integers such that $1 \leq a_i < p_i$ $(i = 1, \ldots, r)$. (We call (1) the unique representation *of α. We call k the* integer part *of α and $\dfrac{a_1}{p_1} + \cdots + \dfrac{a_r}{p_r}$ the* fractional part *of α.)*

Proof. Let $\alpha \in M$. Then

$$\alpha = \frac{b_{i_1}}{p_{i_1}} + \cdots + \frac{b_{i_n}}{p_{i_n}}$$

for some distinct primes $p_{i_1}, \ldots, p_{i_n}$ and integers $b_{i_1}, \ldots, b_{i_n}$ all ≥ 1. Each $\dfrac{b_{i_j}}{p_{i_j}}$ can be written as $k_{i_j} + \dfrac{a_{i_j}}{p_{i_j}}$, where $k_{i_j} \geq 0$ is an integer and $0 \leq a_{i_j} < p_{i_j}$. Writing $k = k_{i_1} + \cdots + k_{i_n}$ and relabeling the denominators of those $\dfrac{a_{i_j}}{p_{i_j}}$ in which $a_{i_j} \geq 1$ as $p_1, \ldots, p_r$, we get the form (1).

Now we show the uniqueness of (1). Suppose

$$\alpha = k + \frac{a_1}{p_1} + \cdots + \frac{a_r}{p_r} = l + \frac{b_1}{q_1} + \cdots + \frac{b_s}{q_s}$$

are two forms (1) of α. Then

$$\frac{kp_1 \ldots p_r + a_1 \widehat{p_1} \ldots p_r + \cdots + a_r p_1 \ldots \widehat{p_r}}{p_1 \ldots p_r} = \frac{lq_1 \ldots q_s + b_1 \widehat{q_1} \ldots q_s + \cdots + b_s q_1 \ldots \widehat{q_s}}{q_1 \ldots q_s}$$

and each fraction is in reduced form. (Here $\widehat{p_i}$ or $\widehat{q_j}$ means that factor is omitted.) Hence by the Reduced Form Lemma we have $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}$. After

relabeling we have

$$k + \frac{a_1}{p_1} + \cdots + \frac{a_r}{p_r} = l + \frac{b_1}{p_1} + \cdots + \frac{b_r}{p_r}.$$

Now if, for example, $a_1 > b_1$, we write

$$k + \frac{a_1 - b_1}{p_1} + \cdots + \frac{a_r}{p_r} = l + \frac{b_2}{p_2} + \cdots + \frac{b_r}{p_r},$$

and so the LHS has p_1 but the RHS does not, a contradiction with what we proved above. Hence $a_i = b_i$ for $i = 1, \ldots, r$. Hence $k = l$. $\qquad\square$

Lemma 3.2. *Let $\alpha, \beta, \gamma \in M$ be such that $\alpha = \beta + \gamma$. Then the sum of the integer parts of β and γ is less than or equal to the integer part of α. In particular, the integer parts of β and γ are less than or equal to the integer part of α.*

Proof. Let

$$\alpha = k_\alpha + \frac{a_1}{p_1} + \cdots + \frac{a_l}{p_l},$$

$$\beta = k_\beta + \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m},$$

$$\gamma = k_\gamma + \frac{c_1}{r_1} + \cdots + \frac{c_n}{r_n}$$

be the unique representations of α, β, γ. Then

$$\beta + \gamma = k_\beta + k_\gamma + \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m} + \frac{c_1}{r_1} + \cdots + \frac{c_n}{r_n}.$$

If $q_i = r_j$, we write $\dfrac{b_i}{q_i} + \dfrac{c_j}{r_j} = \dfrac{b_i + c_j}{q_i} = k_{i,j} + \dfrac{d_{i,j}}{q_i}$, where $0 \leq d_{i,j} < q_i$ and $k_{i,j}$ is 0 or 1. If $d_{i,j} = 0$, we omit $\dfrac{d_{i,j}}{q_i}$. After these additions and omitions, if there are any, and after adding all the $k_{i,j}$ to $k_\beta + k_\gamma$, the RHS is written in the unique representation form. Hence $k_\alpha = k_\beta + k_\gamma + \sum k_{i,j}$. Hence $k_\alpha \geq k_\alpha + k_\beta$. In particular, $k_\alpha \geq k_\beta$ and $k_\alpha \geq k_\gamma$. $\qquad\square$

Lemma 3.3. *The element $\dfrac{1}{p} \in M$, p prime, cannot be written as $\dfrac{1}{p} = \alpha + \beta$ with $\alpha, \beta \in M \setminus \{0\}$.*

Proof. Suppose to the contrary. Then the integer parts of α, β are 0, so the unique representations of α and β are

$$\alpha = \frac{a_1}{p_1} + \cdots + \frac{a_l}{p_l},$$

$$\beta = \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m}.$$

None of $p_1, \ldots, p_r$, $q_1, \ldots, q_s$, can be equal to p, otherwise $\alpha + \beta > \dfrac{1}{p}$. When we write

$$\alpha + \beta = \frac{a_1}{p_1} + \cdots + \frac{a_l}{p_l} + \frac{b_1}{q_1} + \cdots + \frac{b_m}{q_m},$$

then $\alpha + \beta = \dfrac{a}{p_1 \cdots p_l q_1 \cdots q_m}$ for some integer $a \geq 1$, while p does not divide $p_1 \cdots p_l q_1 \cdots q_m$. Thus $\alpha + \beta \neq \dfrac{1}{p}$, a contradiction. $\qquad \square$

Lemma 3.4. *The irreducible elements of $F[X; M]$ of the form X^α, $\alpha \in M$, are precisely the elements $X^{1/p}$, p prime.*

Proof. Follows from Lemma 3.3 and Proposition 2.9. $\qquad \square$

Lemma 3.5. *If the unique representation of $\alpha \in M$ is $\alpha = \dfrac{a_1}{p_1} + \cdots + \dfrac{a_r}{p_r}$, then*

$$X^\alpha = \underbrace{X^{1/p_1} \ldots X^{1/p_1}}_{a_1} \cdots \underbrace{X^{1/p_r} \ldots X^{1/p_r}}_{a_r}$$

is, up to associates, the only decomposition of X^α into irreducibles. In particular, any factorization process of X^α has the (same) finite number of steps.

Proof. Follows from Proposition 1.3 and Lemma 3.4. $\qquad \square$

Lemma 3.6. *For every $\alpha \in M \setminus \{0\}$, X^α has every factorization process finite.*

Proof. The proof is by induction on the integer part of α. If the integer part of α is 0, the statement follows from Lemma 3.5. Suppose that for every $\alpha \in M \setminus \{0\}$ with integer part $< k$ all factorization processes of X^α are finite. Let $\alpha = k + \dfrac{a_1}{p_1} + \cdots + \dfrac{a_r}{p_r}$ be the unique representation of α. Let $X^\alpha = X^\beta \cdot X^\gamma$ be the first step of a fixed factorization process of X^α. If the integer parts of both β, γ are $< k$, then both β, γ have all factorization processes finite by the inductive hypothesis and so the factorization process of α is finite. Suppose that one of β, γ has the integer part equal to k and (by Lemma 3.2) the other one to 0. We will assume that the integer part of β is k (it is not a big difference if we assume that γ has the integer part k). It follows that, after relabeling,

$$\beta = k + \frac{a_1}{p_1} + \cdots + \frac{a_m}{p_m} + \frac{b_{m+1}}{p_{m+1}} + \cdots + \frac{b_n}{p_n},$$
$$\gamma = \frac{c_{m+1}}{p_{m+1}} + \cdots + \frac{c_n}{p_n} + \frac{a_{n+1}}{p_{n+1}} + \cdots + \frac{a_r}{p_r},$$

where $m \geq 0$, $n \geq m + 1$, $b_i + c_i = a_i$ $(i = m + 1, \ldots, n)$. Since γ has at least one addend in its unique representation, the fractional part of the unique representation of β is "smaller" than the fractional part of the unique representation of α. The

next step in the factorization process of X^α would be a factorization of X^β, namely $X^\beta = X^\delta \cdot X^\varepsilon$. If both δ and ε have integer part $< k$, they have finite factorization processes and since X^γ also has a finite factorization process, then the factorization process of $X^\alpha = X^\delta X^\varepsilon X^\gamma$ is finite. If δ has the integer part equal to k (similarly if ε has the integer part equal to k), then the fractional part of δ would be "smaller" than the fractional part of β. There can be only finitely many steps in which the integer part of one of the factors stays k and the fractional part is "smaller" and "smaller", so after finitely many steps the integer parts of both factors become $< k$ and we can apply the inductive hypothesis. $\qquad\square$

Theorem 3.7. *Let* $M = \left\langle \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{5}, \dots \right\rangle$. *Then the domain* $F[X; M]$ *is atomic non-AP. Moreover, no nonzero nonunit element of* $F[X; M]$ *has an infinite factorization process.*

Proof. Let $f \in F[X; M]$ be a nonzero nonunit element. For atomicity of $F[X; M]$ it is enough to show that f has a finite factorization process. We claim that, in fact, every factorization process of f is finite. Suppose to the contrary, i.e., that f has an infinite factorization process. Denote it (after a relabeling at each step)

$$f = f_0 f_1 = f_0 f_{1,0} f_{1,1} = f_0 f_{1,0} f_{1,1,0} f_{1,1,1} = \dots.$$

Denote the leading monomials of $f, f_0, f_1, f_{1,0}, f_{1,1}, \dots$ by X^α, X^{α_0}, X^{α_1}, $X^{\alpha_{1,0}}$, $X^{\alpha_{1,1}}, \dots$ Then

$$X^\alpha = X^{\alpha_0} X^{\alpha_1} = X^{\alpha_0} X^{\alpha_{1,0}} X^{\alpha_{1,1}} = X^{\alpha_0} X^{\alpha_{1,0}} X^{\alpha_{1,1,0}} X^{\alpha_{1,1,1}} = \dots$$

is an infinite factorization process of X^α, which is a contradiction by Lemma 3.6.

$F[X; M]$ is not AP since

$$X^{1/2} \mid X^{1/2} X^{1/2} = X = X^{1/3} X^{1/3} X^{1/3},$$

however $X^{1/2} \nmid X^{1/3}$. ($X^{1/2}$ is irreducible by Lemma 3.4.) $\qquad\square$

4. The case of finitely generated submonoids of $\mathbb{Q}_+$

Proposition 4.1. *If* $M \neq \{0\}$ *is a finitely generated monoid, then* M *has essential generators* $a_1, \dots, a_n$ *such that* $M = \langle a_1, \dots, a_n \rangle$.

Proof. Let $A = \{a_1, \dots, a_n\}$ be a generating set of M such that $|A| \leq |B|$ for all generating sets B of M. Clearly, A exists because M is finitely generated. Thus, by Proposition 2.4, each a_i is an essential generator of M. $\qquad\square$

Theorem 4.2. *Let M be a finitely generated monoid. Then precisely one of the following situations occurs:*

    (i) *$M = \{0\}$; then $F[X; M] = F$, a field.*

    (ii) *$M = \langle a \rangle$, $a \neq 0$; then $F[X; M] \cong F[X]$, an Euclidean domain.*

    (iii) *$M = \langle a_1, \ldots, a_n \rangle$, $n \geq 2$, all a_i essential generators of M; then $F[X; M]$ is an atomic non-AP domain.*

Proof. Taking into account what we have previously said about monoid isomorphisms and associated ring isomorphisms, and taking into account Proposition 2.6 and Proposition 4.1, the only statement of this theorem that remains to be proved is that in the case (iii) $F[X; M]$ is atomic and non-AP. The non-AP part follows from Proposition 2.8. We now show that $F[X; M]$ is atomic. Using the isomorphism μ_τ with τ equal to the least common multiple of the denominators of the elements $a_1, \ldots, a_n$ we may assume that $M \subset \mathbb{N}_0$. Then $F[X; M]$ is a subring of $F[X]$ containing F. Hence $F[X; M]$ is atomic by Remark 1.1. $\qquad\square$

Remark 4.3. *By Theorem 22 of Allen and Dale [1], every submonoid M of $\mathbb{N}_0$ is finitely generated. Hence for $F[X; M]$ precisely one of the three cases from Theorem 4.2 occurs.*

5. The case of infinitely generated submonoids of $\mathbb{Q}_+$

Proposition 5.1. *Suppose M cannot be generated by essential generators. Then every generating set of M contains infinitely many nonessential generators.*

Proof. Suppose to the contrary. Let A be a generating set of M having only finitely many nonessential generators, say $a_1, \ldots, a_n$. We may assume that all of them are $\neq 0$ and that $a_1 < \cdots < a_n$. Then $A \setminus \{a_1\}$ is still a generating set of M by Proposition 2.4. Continuing this process we get that $A \setminus \{a_1, \ldots, a_n\}$ is a generating set of M, a contradiction. $\qquad\square$

Lemma 5.2. *Let $\dfrac{m_1}{n_1}, \ldots, \dfrac{m_t}{n_t} \in M$, in reduced form, at least one of them nonzero. Then $\gcd(m_1, \ldots, m_t)$ and $\operatorname{lcm}(n_1, \ldots, n_t)$ are relatively prime.*

Proof. Suppose to the contrary. Then there is a prime p which divides both $\gcd(m_1, \ldots, m_t)$ and $\operatorname{lcm}(n_1, \ldots, n_t)$. Hence

$$(\forall m_i) \; p \mid m_i,$$

$$(\exists n_j) \; p \mid n_j.$$

Hence $\dfrac{m_j}{n_j}$ is not in reduced form, a contradiction. $\qquad\square$

Lemma 5.3. *Let* $\dfrac{m_1}{n_1}, \ldots, \dfrac{m_t}{n_t} \in M$, *in reduced form, at least one of them nonzero.*
Suppose that

$$\frac{\gcd(m_1, \ldots, m_t)}{\mathrm{lcm}(n_1, \ldots, n_t)} \in M.$$

Then

$$\tau = \frac{\mathrm{lcm}(n_1, \ldots, n_t)}{\gcd(m_1, \ldots, m_t)}$$

is an element of $\mathbb{Q}_+$, *in reduced form, such that:*

$$\tau \frac{m_i}{n_i} \in \mathbb{N}_0 \text{ for all } i;$$

$$\frac{1}{\tau} \in M.$$

Proof. That τ is in reduced form follows from Lemma 5.2. The first claim is clear since τ is in reduced form. The second claim follows from the assumption. $\square$

The next theorem is a slight generalization of a theorem by R. Daileda from [3] (given in Corollary 5.5). The proof follows Daileda's proof.

Theorem 5.4. *Let M be a monoid such that for any elements* $\dfrac{m_1}{n_1}, \ldots, \dfrac{m_t}{n_t}$ *from M, in reduced form, at least one of which is nonzero, we have* $\dfrac{\gcd(m_1, \ldots, m_t)}{\mathrm{lcm}(n_1, \ldots, n_t)} \in M$. *Then $F[X; M]$ is AP.*

Proof. Let $f(X) = a_1 X^{\alpha_1} + \cdots + a_n X^{\alpha_n}$ be an irreducible element of $F[X; M]$. We want to show that f is prime. Suppose that $f(X) \mid a(X)b(X)$, where $a(X), b(X) \in F[X; M]$. We need to show that either $f(X) \mid a(X)$ or $f(X) \mid b(X)$. We have $a(X)b(X) = f(X)h(X)$ for some $h(X) \in F[X; M]$. Let $E(a), E(b), E(f), E(h)$ be the sets of exponents of a, b, f, h, respectively, and let $E = E(a) \cup E(b) \cup E(f) \cup E(h)$. Let $E = \left\{ \dfrac{m_1}{n_1}, \ldots, \dfrac{m_t}{n_t} \right\}$, all elements written in reduced form. At least one of them is nonzero since f is irreducible. Let $\tau = \dfrac{\mathrm{lcm}(n_1, \ldots, n_t)}{\gcd(m_1, \ldots, m_t)}$. In $F[X; \tau M]$ we have the relation

$$\phi_\tau(a)\phi_\tau(b) = \phi_\tau(f)\phi_\tau(h)$$

and all the polynomials in this relation belong to $F[X]$. Hence $\phi_\tau(f)$ divides $\phi_\tau(a)\phi_\tau(b)$ in $F[X]$. Note that $\tau M \supset \mathbb{N}_0$ since $\dfrac{1}{\tau} \in M$, hence $F[X; \tau M] \supset F[X]$. Since f is irreducible in $F[X; M]$, $\phi_\tau(f)$ is irreducible in $F[X; \tau M]$, hence in $F[X]$. Hence $\phi_\tau(f)$ is prime in $F[X]$ and so $\phi_\tau(f) \mid \phi_\tau(a)$ or $\phi_\tau(f) \mid \phi_\tau(b)$, say $\phi_\tau(f) \mid \phi_\tau(a)$. Then $\phi_\tau(a) = \phi_\tau(f) \cdot a'(X)$, where $a'(X) \in F[X] \subset F[X; \tau M]$. If we apply the inverse isomorphism $\phi_{1/\tau} : F[X; \tau M] \to F[X; M]$, we get $a(X) = f(X)\phi_{1/\tau}(a')$, i.e., $f(X) \mid a(X)$. Thus $f(X)$ is prime. Hence $F[X; M]$ is AP. $\square$

Corollary 5.5 (Daileda [3])**.** $F[X; \mathbb{Q}_+]$ *is a nonatomic AP domain.*

Proof. $F[X; \mathbb{Q}_+]$ is an AP domain by the previous theorem. It is nonatomic by Proposition 2.10. $\square$

Corollary 5.6. *Let* $M = \left\langle \dfrac{1}{2}, \dfrac{1}{2^2}, \dfrac{1}{2^3}, \dots \right\rangle$*. Then* $F[X; M]$ *is a nonatomic AP domain.*

Proof. The same arguments as for the previous corollary. $\square$

Question 5.7. *One may now wonder if for any* M *without essential generators* $F[X; M]$ *is AP. Consider, for example, the monoid*

$$M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \dots \right\rangle.$$

For the elements $\dfrac{1}{2}, \dfrac{1}{5}$ *we have* $\dfrac{\gcd(1,1)}{\operatorname{lcm}(2,5)} = \dfrac{1}{10} \notin M$*. So we cannot use Theorem 5.4 to conclude that* $F[X; M]$ *is AP. Is it non-AP? More concretely, is the element* $f(X) = X^{1/2} + X^{1/5}$ *of this domain irreducible? It is not prime since*

$$X^{1/2} + X^{1/5} \mid (X^{1/2} + X^{1/5})^2 = X^{1/5}(X^{4/5} + 2X^{1/2} + X^{2/5}),$$

however $X^{1/2} + X^{1/5}$ *does not divide any of the elements* $X^{1/5}$ *and* $X^{4/5} + 2X^{1/2} + X^{2/5}$*. In general, we would like to characterize all the monoids* M *such that* $F[X; M]$ *is AP.*

Remark 5.8. *If* M *is an infinitely generated monoid, then precisely one of the following situations occurs:*

(i) M *has no essential generators. Then* $F[X; M]$ *is non-atomic (by Proposition 2.10). It can be AP (examples in the corollaries 5.5 and 5.6), the question 5.7 asks if it can be non-AP.*

(ii) M *has at least one essential generator, but cannot be generated by essential generators. Then* $F[X; M]$ *is non-atomic (by Proposition 2.10) and non-AP (by Proposition 2.8). An example of a monoid of this type is*

$$M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots; \frac{1}{5} \right\rangle.$$

(iii) M *can be generated by essential generators. Then* $F[X; M]$ *is non-AP (by Proposition 2.8). It can be atomic (by the example of the section 3), the question 2.11 asks if it can be non-atomic.*

Proposition 5.9. *If* M *is infinitely generated, then* $F[X; M]$ *is not a UFD.*

Proof. Follows from the discussion in Remark 5.8. $\square$

References

[1] P. J. Allen and L. Dale, *Ideal theory in the semiring $\mathbb{Z}^+$*, Publ. Math. Debrecen, 22 (1975), 219-224.

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

[3] R. C. Daileda, *A non-UFD integral domains in which irreducibles are prime*, preprint.
    `http://ramanujan.math.trinity.edu/rdaileda/teach/m4363s07/non_ufd.pdf`.

[4] R. Gilmer, Commutative Semigroup Rings, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1984.

Ryan Gipson and **Hamid Kulosman** (Corresponding Author)

Department of Mathematics

University of Louisville

South 3rd Street

40292 Louisville, KY, USA

e-mails: ryan.gipson@louisville.edu (R. Gipson)

         hamid.kulosman@louisville.edu (H. Kulosman)