International Electronic Journal of Algebra
Volume 24 (2018) 50-61
DOI: 10.24330/ieja.440192

IRREDUCIBILITY OF CERTAIN BINOMIALS IN SEMIGROUP RINGS FOR NONNEGATIVE RATIONAL MONOIDS

Katie Christensen, Ryan Gipson and Hamid Kulosman

Received: 11 October 2017; Revised: 5 March 2018; Accepted: 10 March 2018
Communicated by Burcu Üngör

Dedicated to the memory of Professor John Clark

Abstract. We extend a lemma by Matsuda about the irreducibility of the binomial $X^\pi - 1$ in the semigroup ring $F[X;G]$, where F is a field, G is an abelian torsion-free group and π is an element of G of height $(0,0,0,\dots)$. In our extension, G is replaced by any submonoid of $(\mathbb{Q}_+,+)$. The field F, however, has to be of characteristic 0. We give an application of our main result.

Mathematics Subject Classification (2010): 13F15, 13A05, 12E05
Keywords: Semigroup ring, atomic domain, AP domain, irreducible element, prime element, height $(0,0,0,\dots)$

1. Introduction and preliminaries

The goal of this paper is to extend a lemma by R. Matsuda about the irreducibility of the binomial $X^\pi - 1$ in the semigroup ring $F[X;G]$, where F is a field, G is an abelian torsion-free group and π is an element of G of height $(0,0,0,\dots)$. In our extension we will introduce the notion of height $(0,0,0,\dots)$ for the elements of torsion-free monoids and prove the irreducibility of the binomial $X^\pi - 1$ in the semigroup ring $F[X;M]$, where M is any submonoid of $(\mathbb{Q}_+,+)$ and π is an element of M of height $(0,0,0,\dots)$. The field F has to be of characteristic 0, as there are counterexamples for fields of positive characteristic. We need this extension for our research on semigroup rings $F[X;M]$ for submonoids M of $(\mathbb{Q}_+,+)$ (see [7, Question 5.7]).

We denote by $\mathbb{N}_0$ the set $\{0,1,2,\dots\}$ of nonnegative integers and by $\mathbb{Q}_+, \mathbb{R}_+$ the sets of nonnegative rational and real numbers, respectively.

All monoids and groups in this paper are assumed to be commutative, written additively. All rings are commutative with an identity.

All the notions that we use but not define in this paper can be found in the classical reference books [5] by R. Gilmer and [10] by D. G. Northcott.

Let Γ be a monoid. The elements of the semigroup ring $F[X;\Gamma]$, where F is a field and X is a variable, are the polynomial expressions, also called polynomials,

$$f(X) = a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}, \tag{1}$$

where $a_1, \ldots, a_n \in F,\ \alpha_1, \ldots, \alpha_n \in \Gamma$. The polynomials $f(X) = a$, $a \in F$, are called the *constant polynomials*.

If a monoid M is a submonoid of $(\mathbb{Q}_+, +)$, we assume, if we do not specifically mention otherwise, that in (1) $\alpha_1 > \cdots > \alpha_n$. We say that $a_1X^{\alpha_1}$ is the *leading term* of f, X^{α_1} is the *leading monomial* of f and α_1 is the *degree* of f. The degree of constant polynomials 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 $f \mid h$ for all $g, h \in F[X;M[$. If every nonzero nonunit element of $F[X;M]$ can be written as a finite product of atoms, we say that $F[X;M]$ 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*. 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.

A monoid Γ is called a *cancellative monoid* if it satisfies the following *cancellation property*: for any $\alpha, \beta, \gamma \in \Gamma$, $\alpha + \gamma = \beta + \gamma$ implies $\alpha = \beta$. A monoid Γ is said to be *torsion-free* if for any integer $n \geq 1$ and any $\alpha, \beta \in \Gamma$, $n\alpha = n\beta$ implies $\alpha = \beta$. If Γ is torsion-free, then it satisfies the following weaker property: for any integer $n \geq 1$ and any $\alpha \in \Gamma$, $n\alpha = 0$ implies $\alpha = 0$. If Γ is a group, then Γ is torsion-free if and only if it satisfies this weaker property.

Let Γ, Γ' be two monoids. A map $\mu : \Gamma \to \Gamma'$ is called a *monoid homomorphism* from Γ to Γ' 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 Γ and Γ'. (The inverse bijection $\mu^{-1} : \Gamma' \to \Gamma$ preserves the operation.) To every monoid homomorphism $\mu : \Gamma \to \Gamma'$ we can naturally associate a ring homomorphism $\phi : F[X;\Gamma] \to F[X;\Gamma']$, defined by

$$\phi(a_1X^{\alpha_1} + \cdots + a_nX^{\alpha_n}) = a_1X^{\mu(\alpha_1)} + \ldots a_nX^{\mu(\alpha_n)}.$$

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

Let F be a field and $k \in \mathbb{N}$. Consider the variables $X_1, X_2, \ldots, X_k$ over F. The *elementary symmetric polynomials* in these variables are the elements of the ring $F[X_1, \ldots, X_k]$ defined in the following way:

$$\begin{aligned}
\sigma_1 &= \sum_{1 \leq i \leq k} X_i \\
\sigma_2 &= \sum_{1 \leq i < j \leq n} X_i X_j \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\sigma_k &= X_1 \cdots X_k
\end{aligned}$$

and $\sigma_e = 0$ for $e > k$. The *power sums* in the variables $X_1, X_2, \ldots, X_k$ are the elements of the ring $F[X_1, \ldots, X_k]$ defined in the following way:

$$\pi_e = \sum_{1 \leq i \leq k} X_i^e$$

for $e \geq 1$. The following theorem, given in [1, page A.IV.70], gives the so-called *Newton's relations* between the elementary symmetric polynomials and the power sums in the variables $X_1, X_2, \ldots, X_k$ in the ring $F[X_1, \ldots, X_k]$.

Theorem 1.1 (Newton's relations)**.** *For every integer $e \in \{1, 2, \ldots, k\}$ we have*

$$\pi_e = \sigma_1 \pi_{e-1} - \sigma_2 \pi_{e-2} + \cdots + (-1)^e \sigma_{e-1} \pi_1 + (-1)^{e+1} e \sigma_e.$$

If we replace each variable X_i by an element x_i of the field F, we get Newton's relations between the elementary symmetric polynomials and the power sums of the elements $x_1, x_2, \ldots, x_k$ in the field F.

The following number theory theorem (called *Lucas' Theorem*) is proved by É. Lucas in 1878. A simpler proof is given by N. J. Fine in [3].

Theorem 1.2 (Lucas' Theorem)**.** *Let p be a prime number and let*

$$\begin{aligned}
M &= M_t p^t + M_{t-1} p^{t-1} + \cdots + M_2 p^2 + M_1 p + M_0, \\
N &= N_t p^t + N_{t-1} p^{t-1} + \cdots + N_2 p^2 + N_1 p + N_0
\end{aligned}$$

be the expansions of the nonnegative integers M and N in base p (so that $M_i, N_i \in \{0, 1, \ldots, p-1\}$). Then

$$\binom{M}{N} \equiv \binom{M_t}{N_t} \binom{M_{t-1}}{N_{t-1}} \cdots \binom{M_2}{N_2} \binom{M_1}{N_1} \binom{M_0}{N_0} \pmod{p},$$

where we assume that $\binom{M_i}{N_i} = 0$ if $M_i < N_i$.

For a given natural number n with the prime-power factorization $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ consider the n-th roots of unity in the field of complex numbers $\mathbb{C}$. The next theorem is the main theorem (namely, Theorem 5.2) of the paper [8] by T Y. Lam and K. H. Leung (we call it *Lam-Leung Theorem*). It describes all the numbers t such that there are t n-th roots of unity in $\mathbb{C}$ whose sum is 0.

Theorem 1.3 (Lam-Leung Theorem)**.** *The set of all numbers t such that there are t n-th roots of unity in $\mathbb{C}$ whose sum is 0 is equal to $\mathbb{N}_0\, p_1 + \mathbb{N}_0\, p_2 + \cdots + \mathbb{N}_0\, p_r$.*

2. Elements of height $(0, 0, 0, \dots)$ in torsion-free monoids

For a prime number p the notion of the *p-height* $h_p(a)$ of an element a of a torsion-free group G is defined in [4, page 108] as the nonnegative integer r such that $a \in p^r G \setminus p^{r+1} G$ if such an integer exists and as ∞ otherwise. The sequence $(h_2(a), h_3(a), h_5(a), \dots)$ of p-heights of a as p goes through all prime numbers in the increasing order is called the *height sequence* of a. For the purpose of this paper we will consider the elements of height $(0, 0, 0, \dots)$, but, more generally, in the torsion-free monoids instead of groups.

Definition 2.1. We say that an element a of a torsion-free monoid Γ is of height $(0, 0, 0, \dots)$ if for every prime number p the equation $px = a$ cannot be solved for an $x \in \Gamma$.

Examples 2.2.

(1) *There are no elements of height $(0, 0, 0, \dots)$ in the monoids $\{0\}$, $(\mathbb{Q}_+, +)$, $(\mathbb{R}_+, +)$.*

(2) *In the monoid $(\mathbb{N}_0, +)$ the only element of height $(0, 0, 0, \dots)$ is 1.*

(3) *In the submonoid $\langle 2, 3\rangle$ of $(\mathbb{N}_0, +)$ the elements of height $(0, 0, 0, \dots)$ are precisely the prime numbers $2, 3, 5, \dots$.*

(4) *In the submonoid $\langle 2, 5\rangle$ of $(\mathbb{N}_0, +)$ the elements of height $(0, 0, 0, \dots)$ are the prime numbers $2, 5, 7, 11, \dots$ and the composite number 9.*

(5) *There are infinitely many elements of height $(0, 0, 0, \dots)$ in the monoid $\left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots; \frac{1}{5} \right\rangle$, but there are no elements of height $(0, 0, 0, \dots)$ in the monoid $\left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots \right\rangle$.*

Proposition 2.3. *Let $\mu : \Gamma \to \Gamma'$ be an isomorphism between two torsion-free monoids. For any $a \in \Gamma$, a is of height $(0, 0, 0, \dots)$ in Γ if and only if $\mu(a)$ is of height $(0, 0, 0, \dots)$ in Γ'.*

Proof. Easy. □

3. Matsuda's lemma and Matsuda monoids

Note that an element π of a monoid M is not of height $(0, 0, 0, \dots)$ if and only if $\pi = n\alpha$ for some $\alpha \in M$ and some integer $n \geq 2$. In that case the binomial $X^\pi - 1$ has the following factorization in $F[X; M]$:

$$X^\pi - 1 = (X^\alpha - 1)(X^{(n-1)\alpha} + X^{(n-2)\alpha} + \cdots + X^\alpha + 1).$$

It is natural to ask if these are the only possible factorizations in $F[X; M]$ of the binomials $X^\pi - 1$. In other words, if for every integer $n \geq 2$ the equation $n\alpha = \pi$ has no solutions for α in M, is $X^\pi - 1$ necessarily irreducible in $F[X; M]$? The next theorem, which is Lemma 2.2 in the paper [9] by R. Matsuda, shows that it indeed is if M is a non-zero torsion-free group. (For the sake of completness we include Matsuda's proof. The proof uses another lemma from [9], which in turn uses a statement about pure subgroups from [4].) We will show in the next section (in our main theorem 4.1) that an analogous result holds if M is any submonoid of $(\mathbb{Q}_+, +)$ and F is a field of characteristic 0.

Theorem 3.1 (Matsuda's Lemma)**.** *Let F be a field, $G \neq 0$ a torsion-free group, and π an element of G of height $(0, 0, 0, \dots)$. Then $X^\pi - 1$ is an irreducible element of $F[X; G]$.*

Proof. Suppose $X^\pi - 1 = gh$, where $g, h \in F[X; G]$. Let H be the subgroup generated by π and the power exponents appearing in g and h. By [9, Lemma 2.1], $\mathbb{Z}\pi$ is a direct summand of H. Let $H = \mathbb{Z}\pi \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, $X^\pi = Y$, $X^{e_i} = X_i$. The set $Y, X_1, \dots, X_n$ is algebraically independent over F. Hence $Y - 1$ is irreducible in $F_{\mathbb{Z}}[Y, X_1, \dots, X_n]$. Here $F_{\mathbb{Z}}[Y, X_1, \dots, X_n]$ denotes the quotient ring of $F[Y, X_1, \dots, X_n]$ by the multiplicative system generated by $Y, X_1, \dots, X_n$. □

Inspired by Matsuda's lemma, we introduce the following notion.

Definition 3.2. We call a cancellative torsion-free monoid Γ a *Matsuda monoid* if for every element $\pi \in \Gamma$ of height $(0, 0, 0, \dots)$ the binomial $X^\pi - 1$ is irreducible in $F[X; \Gamma]$ for every field F. We call a cancellative torsion-free monoid Γ a *Matsuda monoid of type* 0 (respectively, *p, where p is a prime number*) if for every element $\pi \in \Gamma$ of height $(0, 0, 0, \dots)$ the binomial $X^\pi - 1$ is irreducible in $F[X; \Gamma]$ for every field F of characteristic 0 (respectively, p).

Every group is a Matsuda monoid by Theorem 3.1.

Examples 3.3. (1) *The monoids $\{0\}$, $(\mathbb{Q}_+, +)$, $(\mathbb{R}_+, +)$ have no elements of height $(0, 0, 0, \dots)$, so they are Matsuda monoids.*

(2) *Let* $M = (\mathbb{N}_0, +)$. *Then* 1 *is the only element of height* $(0, 0, 0, \dots)$ *in* M. *Since* $X^1 - 1$ *is irreducible in* $F[X; M]$ *for every field* F, M *is a Matsuda monoid.*

(3) *In the monoid* $M = \langle 2, 3 \rangle$, *as we have seen earlier, the elements of height* $(0, 0, 0, \dots)$ *are precisely the all prime numbers.* M *is not a Matsuda monoid of type* 2 *since in* $\mathbb{F}_2[X; M]$ *we have*

$$X^7 - 1 = (X^4 + X^3 + X^2 + 1)(X^3 + X^2 + 1).$$

M is not a Matsuda monoid of type 3 *since in* $\mathbb{F}_3[X; M]$ *we have*

$$X^{11} - 1 = (X^6 - X^5 + 2X^4 - X^3 + X^2 - 1)(X^5 + X^4 + 2X^3 + X^2 + 2).$$

One wonders if M is a Matsuda monoid of any finite type. However, it follows from the main theorem of this paper that M is a Matsuda monoid of type 0.

4. Submonoids of $(\mathbb{Q}_+, +)$ are Matsuda monoids of type 0

Here is our main theorem.

Theorem 4.1. *Every submonoid of* $(\mathbb{Q}_+, +)$ *is a Matsuda monoid of type* 0.

Proof. We will first prove the statement for the submonoids of $(\mathbb{N}_0, +)$.

By Example 3.3 (2), $\mathbb{N}_0$ is a Matsuda monoid. Let us assume that M is a submonoid of $(\mathbb{N}_0, +)$ such that $1 \notin M$. Let $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ be a prime-power factorization (in the multiplicative semiring $\mathbb{N}_0$) of an element $n \in M$ of type $(0, 0, 0, \dots)$. It is enough to show that $X^n - 1$ cannot be factored into a product of two polynomials of degree ≥ 1 in $F[X; M]$ for any algebraically closed field F of characteristic 0. So let F be an algebraically closed field of characteristic 0. Then F contains the field $\mathbf{A}$ of algebraic numbers. Suppose to the contrary, i.e., that the binomial $X^n - 1$ can be factored in $F[X; M]$ as $g(X)h(X)$, where g and h are two monic polynomials of degrees $k \geq 1$ and $l \geq 1$, respectively. We will assume that $k \geq l$. Since $X^n - 1$ can be factored in $F[X]$ as a product of n monic linear polynomials $X - \zeta$, where ζ is an n-th root of unity (in $\mathbf{A}$), we have $g(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$, where $\alpha_1, \alpha_2, \dots, \alpha_k$ are n-th roots of unity (in $\mathbf{A}$). Let $\beta_i = \alpha_i^{-1}$ for $i = 1, 2, \dots, k$. Let us also write $g(x)$ as

$$g(X) = X^k + g_{k-1}X^{k-1} + \cdots + g_1 X + g_0,$$

where $g_0, \dots, g_{k-1} \in F$.

Claim 1. *Let e be an element of $\mathbb{N}_0$ such that $e < k$ and $e \notin M$. Then*

$$\sigma_e(\beta_1, \ldots, \beta_k) = 0,$$
$$\pi_e(\beta_1, \ldots, \beta_k) = 0.$$

Proof of Claim 1. Since $e \notin M$, the coefficient g_e by X^e in $g(X)$ is equal to 0, hence

$$\sum \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_{k-e}} = 0,$$

where the sum goes over all $(k-e)$-element subsets $\{i_1, \ldots, i_{k-e}\}$ of $\{1, 2, \ldots, k\}$. Hence

$$\sum \beta_{j_1}\beta_{j_2}\cdots\beta_{j_e} = 0,$$

where the sum goes over all e-element subsets $\{j_1, \ldots, j_e\}$ of $\{1, 2, \ldots, k\}$. Thus

$$\sigma_e(\beta_1, \ldots, \beta_k) = 0.$$

We prove the second relation by induction on e. For $e = 1$ we have

$$\pi_1(\beta_1, \ldots, \beta_k) = \sigma_1(\beta_1, \ldots, \beta_k) = 0.$$

Suppose that

$$\pi_f(\beta_1, \ldots, \beta_k) = 0$$

for all elements $f \in \mathbb{N}_0$ such that $f < e$ and $f \notin M$. We have the Newton relation (see Theorem 1.1)

$$\pi_e = \sigma_1\pi_{e-1} - \sigma_2\pi_{e-2} + \cdots + (-1)^e\sigma_{e-1}\pi_1 + (-1)^{e+1}e\sigma_e, \tag{2}$$

where each of σ_i, π_i is a function of $\beta_1, \ldots, \beta_k$. Since $e \notin M$, $\sigma_e = 0$ by the first relation. Also, in each of the sets $\{1, e-1\}$, $\{2, e-2\}$, $\ldots$, $\{\lfloor\frac{e}{2}\rfloor, \lfloor\frac{e+1}{2}\rfloor\}$ at least one of the elements is not in M, otherwise their sum, which is e, would be in M. If in any of these sets $\{j, e-j\}$ say $j \notin M$, then $\sigma_j = 0$ by the first relation of this claim and $\pi_j = 0$ by the inductive hypothesis. Hence $\sigma_j\pi_{e-j} = 0$ and $\sigma_{e-j}\pi_j = 0$. Hence all the addends on the left hand side of (2) are 0 and so $\pi_e(\beta_1, \ldots, \beta_k) = 0$.

Claim 1 is proved.

Claim 2. *Let $d < n$ be a divisor of n. Let e be an element of $\mathbb{N}_0$ such that $ed \leq k$ and $ed \notin M$. Then*

$$\pi_e(\beta_1^d, \ldots, \beta_k^d) = 0,$$
$$\sigma_e(\beta_1^d, \ldots, \beta_k^d) = 0.$$

Proof of Claim 2. We have

$$\pi_e(\beta_1^d, \ldots, \beta_k^d) = \pi_{de}(\beta_1, \ldots, \beta_k) = 0$$

by Claim 1 as $ed \notin M$. We prove the second relation by induction on e. For $e = 1$ we have

$$\sigma_1(\beta_1^d, \ldots, \beta_k^d) = \pi_d(\beta_1, \ldots, \beta_k) = 0$$

by Claim 1 as $d \notin M$. Let e be an element of $\mathbb{N}_0$ such that $ed \leq k$ and $ed \notin M$. Suppose that

$$\sigma_f(\beta_1^d, \ldots, \beta_k^d) = 0$$

for all elements $f \in \mathbb{N}_0$ such that $f < e$ and $fd \notin M$. We have the Newton relation

$$\sigma_e = \frac{(-1)^{e+1}}{e} \left[\pi_e - \sigma_1\pi_{e-1} + \sigma_2\pi_{e-2} - \cdots + (-1)^{e-1}\sigma_{e-1}\pi_1\right], \tag{3}$$

where each of σ_i, π_i is a function of $\beta_1^d, \ldots, \beta_k^d$. Since $ed \notin M$, $\pi_e = 0$ by the first relation. Consider any of the sets $\{1, e-1\}$, $\{2, e-2\}$, $\ldots$, $\{\lfloor\frac{e}{2}\rfloor, \lfloor\frac{e+1}{2}\rfloor\}$, say $\{j, e-j\}$. At least one of the elements $jd, (e-j)d$ is not in M, otherwise their sum, which is ed, would be in M. If say $jd \notin M$, then $\pi_j = 0$ by the first relation of this claim and $\sigma_j = 0$ by the inductive hypothesis. Hence $\sigma_j\pi_{e-j} = 0$ and $\sigma_{e-j}\pi_j = 0$. Hence all the addends on the right hand side of (3) are 0 and so $\sigma_e(\beta_1^d, \ldots, \beta_k^d) = 0$.

Claim 2 is proved.

Let now $j \in \{1, 2, \ldots, r\}$. For $e = p_1^{\nu_1} \cdots \widehat{p_j^{\nu_j}} \cdots p_r^{\nu_r}$ (where $\widehat{\ }$ means that the factor is omitted), by Claim 1,

$$\pi_e(\beta_1, \ldots, \beta_k) = \beta_1^e + \cdots + \beta_k^e = 0,$$

i.e.,

$$\sigma_1(\beta_1^e, \ldots, \beta_k^e) = 0.$$

Each of the elements $\beta_1^e, \ldots, \beta_k^e$ is a $p_j^{\nu_j}$-th root of unity, hence, by Lam-Leung Theorem,

$$k \in \mathbb{N}_0\, p_j.$$

We will prove by induction on s that $k \in \mathbb{N}_0\, p_j^s$ for every $s = 1, 2, \ldots, \nu_j$. For $s = 1$ we have already done that. Suppose that $k \in \mathbb{N}_0\, p_j^{s-1}$ for some $s \in \{2, \ldots, \nu_j\}$. We want to show that $k \in \mathbb{N}_0\, p_j^s$. Suppose to the contrary, i.e., that $k \notin \mathbb{N}_0\, p_j^s$. Then k can be written as

$$k = k_t p_j^t + k_{t-1} p_j^{t-1} + \cdots + k_s p_j^s + k_{s-1} p_j^{s-1},$$

where t is some number, $k_t, k_{t-1}, \ldots, k_s, k_{s-1}$ are from $\{0, 1, \ldots, p-1\}$ and $k_{s-1} \neq 0$. Let $d = p_1^{\nu_1} \cdots \widehat{p_j^{\nu_j}} \cdots p_r^{\nu_r}$ and $e = p_j^{s-1}$. Then by Claim 2,

$$\sigma_e(\beta_1^d, \ldots, \beta_k^d) = 0.$$

Since each β_j^d is $p_j^{\nu_j}$-th root of unity, the last equation is a vanishing sum of $\binom{k}{e} = \binom{k}{p_j^{s-1}}\, p_j^{\nu_j}$-th roots of unity, hence, by Lam-Leung Theorem,

$$\binom{k}{p_j^{s-1}} \in \mathbb{N}_0\, p_j.$$

However, by Lucas' Theorem,

$$\binom{k}{p_j^{s-1}} \equiv \binom{k_{s-1}}{1} = k_{s-1} \neq 0 \pmod{p_j},$$

a contradiction. Thus $k \in \mathbb{N}_0\, p_j^s$. Since this holds for any $s \leq \nu_j$, we have

$$k \in \mathbb{N}_0\, p_j^{\nu_j}.$$

This holds for all $j = 1, 2, \ldots, r$, hence

$$k \equiv 0 \pmod{n},$$

which is in contradiction with our starting hypothesis that $X^n - 1$ can be factored into two nonconstant polynomials, one of which is of degree k. Hence $X^n - 1$ is an irreducible element of $\overline{F}[X; M]$ and, in particular, of $F[X; M]$. The statement is proved for submonoids of $(\mathbb{N}_0, +)$.

Let now M be a submonoid of $(\mathbb{Q}_+, +)$. Let π be an element of M of height $(0, 0, 0, \ldots)$. Suppose to the contrary, i.e., that $X^\pi - 1 = g(X)h(X)$, where g and h are two elements of $\overline{F}[X; M]$ of degree $\neq 0$. Let N be the submonoid of M generated by π and the exponents of the polynomials g and h. N is then a finitely generated submonoid of M in which π is also of height $(0, 0, 0, \ldots)$ and the factorization $X^\pi - 1 = g(X)h(X)$ is in $\overline{F}[X; N]$. Let d be the least common denominator of all the generators of N. Then $\mu_d : N \to dN$ is a monoid isomorphism between N and the submonoid dN of $(\mathbb{N}_0, +)$. By Proposition 2.3, the element $d\pi$ is of height $(0, 0, 0, \ldots)$ in dN. The associated ring isomorphism $\phi_d : \overline{F}[X; N] \to \overline{F}[X; dN]$ transports the factorization $X^\pi - 1 = g(X)h(X)$ from $\overline{F}[X; N]$ into the factorization $X^{d\pi} - 1 = \phi_d(g)\phi_d(h)$ in $\overline{F}[X; dN]$, with both polynomials $\phi_d(g)$, $\phi_d(h)$ nonconstant. We already proved that this is not possible for submonoids of $(\mathbb{N}_0, +)$, so we got a contradiction.

The theorem is proved. □

5. An application: a submonoid M of $(\mathbb{Q}_+, +)$ without essential generators, such that $F[X; M]$ is not AP

We introduced in [7] the following notion of an essential generator of a monoid.

Definition 5.1. An element a of a monoid Γ is called an *essential generator* of Γ if $\langle \Gamma \setminus \{a\} \rangle \neq \Gamma$.

Note that if an element of Γ is an essential generator, it is of height $(0, 0, 0, \dots)$. The converse, however, does not hold.

If a submonoid $M \neq \{0\}$ of $\mathbb{Q}$ has no essential generators, then it is non-atomic by [7, Proposition 2.10]. An example is $M = \mathbb{Q}_+$. However, it was shown by Daileda in [2] that for this monoid, $F[X; M]$ is AP for any field F. We asked in [7] if there is an example of a submonoid M of $(\mathbb{Q}_+, +)$ which has no essential generators, but $F[X; M]$ is not AP for some field F. Specifically, we asked if $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \dots \right\rangle$ is such a monoid. Using the main theorem of this paper we can show that it indeed is.

Proposition 5.2. *Let* $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \dots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \dots \right\rangle$ *and let* F *be a field of characteristics* 0. *Then the semigroup ring* $F[X; M]$ *is not AP.*

Proof. We have $\frac{1}{2} + \frac{1}{5^2} = \frac{27}{2 \cdot 5^2} = \frac{27}{50} \in M$. Let us show that this element is of height $(0, 0, 0, \dots)$. Indeed, from $\frac{27}{2 \cdot 5^2} = p\,(\frac{a}{2^m} + \frac{b}{5^n})$, where p is a prime number, $a, b \geq 1$, $\frac{a}{2^m}$ and $\frac{b}{5^n}$ are in reduced form, and $m, n \geq 1$, we get $3^3 \cdot 2^m \cdot 5^n = p \cdot 2 \cdot 5^2 \cdot (a5^n + b2^n)$. Since $a5^n + b2^m$ is not divisible by 2 nor by 5, we have three cases:

(a) $p = 3$; then $m = 1$, $n = 2$ and $a5^2 + b2^1 = 3$, which is not possible;

(b) $p = 2$; then $m = n = 2$ and $27 = 25a + 4b$, which is not possible;

(c) $p = 5$; then $m = 1$, $n = 3$ and $27 = a5^3 + b2^1$, which is not possible.

Thus we showed that $\frac{27}{50}$ is of height $(0, 0, 0, \dots)$. By Theorem 4.1, the binomial $X^{27/50} - 1$ is an irreducible element of $F[X; M]$. Let us show that it is not prime. We have

$$(X^{27/50} - 1) \mid (X^{27/25} - 1) = (X^{9/25} - 1)(X^{18/25} + X^{9/25} + 1).$$

However $X^{27/50} - 1$ does not divide $X^{9/25} - 1$ since this polynomial has a smaller degree and it does not divide $X^{18/25} + X^{9/25} + 1$ since the relation $(X^{27/50} - 1) \cdot f(X) = X^{18/25} + X^{9/25} + 1$ would imply $\deg(f) = \frac{9}{50}$, but $\frac{9}{50} \notin M$.

The proof is finished. □

6. Concluding remarks and questions

In connection with the main theorem of this paper, the following two questions are natural to ask:

(a) Is any proper submonoid of $(\mathbb{N}_0, +)$ a Matsuda monoid of any finite type?

(b) Is every cancellative torsion-free monoid a Matsuda monoid of type 0?

Now about Section 5. In view of the facts that for $M = \mathbb{Q}_+$, $F[X; M]$ is AP and for $M = \left\langle \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \ldots; \frac{1}{5}, \frac{1}{5^2}, \frac{1}{5^3}, \ldots \right\rangle$, $F[X; M]$ is non-AP, a natural question is to characterize all submonoids M of $(\mathbb{Q}_+, +)$ such that $F[X; M]$ is AP (at least for some class of fields, for example, the fields of characteristics 0). The only case which remains to be considered is when M has no essential generators (then it has to be infinitely generated), the other cases are resolved in [7].

This question is in the spirit of the following "generic question" (Q_E), raised by R. Gilmer in [6]: *if R is a ring, Γ a monoid and E some ring-theoretic property, under what conditions does the semigroup ring $R[X; \Gamma]$ have the property E*? He mentioned that "in most cases, the answer to (Q_E) isn't known unless some restrictions are placed on R and/or Γ." He also mentioned that "in general, polynomial rings over R serve as fair models of what may be expected in answer to generic questions (Q_E) in the case where Γ is torsion-free and cancellative."

Acknowledgement. The authors are grateful to the referees for a careful reading of this paper. Their comments and suggestions have improved the quality of the paper.

References

[1] N. Bourbaki, Algebra II, Chapters 4-7, Springer-Verlag, Berlin-Heidelberg, 2003.

[2] 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`.

[3] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly, 54 (1947), 589-592.

[4] L. Fuchs, Infinite Abelian Groups, Vol. II, Pure and Applied Mathematics, Vol. 36-II, Academic Press, New York-London, 1973.

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

[6] R. Gilmer, *Property E in commutative monoid rings*, Group and semigroup rings (Johannesburg, 1985), North-Holland Math. Stud., 126, Notas Mat., 111, North-Holland, Amsterdam, (1986), 13-18.

[7] R. Gipson and H. Kulosman, *Atomic and AP semigroup rings $F[X;M]$, where M is a submonoid of the additive monoid of nonnegative rational numbers*, Int. Electron. J. Algebra, 22 (2017), 133-146.

[8] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra, 224(1) (2000), 91-109.

[9] R. Matsuda, *On algebraic properties of infinite group rings*, Bull. Fac. Sci. Ibaraki Univ. Ser. A, 7 (1975), 29-37.

[10] D. G. Northcott, Lessons on Rings, Modules and Multiplicities, Cambridge University Press, London, 1968.

Katie Christensen, **Ryan Gipson** and **Hamid Kulosman** (Corresponding Author)
Department of Mathematics
University of Louisville
South 3rd Street
40292 Louisville, KY, USA
e-mails: katie.christensen@louisville.edu (K. Christensen)
ryan.gipson@louisville.edu (R. Gipson)
hamid.kulosman@louisville.edu (H. Kulosman)