POLYNOMIAL PRODUCT SEMIGROUPS AND RING COMMUTATIVITY

S.M. BUCKLEY AND YU. ZELENYUK

ABSTRACT. We give new characterizations of the polynomials $f(X) \in \mathbb{Z}[X]$ such that a unital ring R is necessarily commutative if $f(R) = 0$, or if $f(R) \subset Z(R)$. We use these to characterize semigroups of polynomials under multiplication that have similar properties.

1. Introduction

For certain polynomials $f(X)$ with integer coefficients, the condition $f(R) = 0$ forces a ring to be commutative, in the sense that if $f(x) = 0$ for all x in a ring R, then R is commutative. Sometimes even the weaker condition $f(R) \subset Z(R)$—meaning that $f(x)$ lies in the center $Z(R)$ for all $x \in R$—forces R to be commutative. Characterizations of such polynomials for the condition $f(R) = 0$ are given in [5] and [1] (with the problem posed for all rings, and for unital rings, respectively), and for the condition $f(R) \subset Z(R)$ in [2] (both for all rings and for unital rings).

In this paper, we are interested in semigroups $S \subset \mathbb{Z}[X]$ of polynomials where the semigroup operation is multiplication. We call such semigroups *polynomial product semigroups*. One might wonder if it is possible that all elements of a polynomial product semigroup could consist only of such forcing polynomials. This is a rather strong condition and for most variants of the problem we will see that no such semigroups exist. However for one variant there are examples.

Section 2 contains preliminary material, and also handles the easy cases. Section 3 begins with new characterizations of the polynomials $f(X)$ such that a unital ring R is necessarily commutative whenever $f(R) = 0$, or whenever $f(R) \subset Z(R)$. This enables us to characterize the one type of polynomial product semigroup that actually exists. In the final section, we consider some examples.

2. Preliminaries

We begin by introducing some notation that we use throughout this paper. We usually denote a formal polynomial as $f(X) \in D[X]$ where D will always be either $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime $p \in \mathbb{N}$. We write f for any associated function (on D if $D = \mathbb{Z}_p$, or on some general ring R if $D = \mathbb{Z}$). When evaluating f, we write something such as $f(m)$; this symbol "m" may be anything except "X", the latter being reserved for the formal variable. One exception to these conventions is that whenever $f(X) \in D[X]$ and G is a function defined on $D[X]$, we will consistently write $G(f)$ in place of $G(f(X))$ for stylistic reasons.

Date: 18.10.2012.

2010 *Mathematics Subject Classification.* Primary: 16R50. Secondary: 20M99.

Key words and phrases. unital ring, polynomial identity, commutativity, semigroup.

A polynomial $f(X) \in \mathbb{Z}[X]$ is *primitive* if the greatest common divisor of its coefficients is 1.

For non-negative $i \in \mathbb{Z}$, we define the coefficient maps $a_i : D[X] \to D$ by $a_i(f) = \alpha_i$ where $f(X) = \sum_{j=0}^n \alpha_j X^j$ (and $\alpha_j = 0$ for $j > n$); we omit D in this notation as it will always be understood. We also define the coefficient sum[1] $s(f) = \sum_{j=0}^n \alpha_j$. If $f(X) = \sum_{i=0}^n \alpha_i X^i \in D[X]$, we define its formal derivative $f'(X) = \sum_{i=1}^n i\alpha_i X^{i-1}$, i.e. $a_{i-1}(f') = ia_i(f)$ for all $i \in \mathbb{N}$.

Whenever I is an ideal in D and $\phi : D \to R := D/I$ is the natural quotient map, we get an induced quotient map $\Phi : D[X] \to R[X]$ via the equations

$$\Phi\left(\sum_{i=0}^n \alpha_i X^i\right) = \sum_{i=0}^n \phi(\alpha_i) X^i \,,$$

and both ϕ and Φ are ring epimorphisms. We use this fact only for the special case $D = \mathbb{Z}$ and $R = \mathbb{Z}_p$, where p is a prime, and we denote the natural quotient maps by $\phi_p : \mathbb{Z} \to \mathbb{Z}_p$ and $\Phi_p : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$. As usual, we denote by $\mathbb{Z}_p^*$ the set of units in $\mathbb{Z}_p$, i.e. $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. As is well known, $X^p - X \in \mathbb{Z}_p[X]$ equals $\prod_{i\in\mathbb{Z}_p}(X - i)$.

Given a class $\mathcal{F}$ of (not necessarily unital) rings, we denote by $C_0(\mathcal{F})$ and $C_Z(\mathcal{F})$ the sets of forcing polynomials $f(X) \in \mathbb{Z}[X]$ defined as follows:

$$C_0(\mathcal{F}) = \{f(X) \in \mathbb{Z}[X] \;:\; (R \in \mathcal{F} \text{ and } f(R) = 0) \Longrightarrow R \text{ commutative}\}\,,$$
$$C_Z(\mathcal{F}) = \{f(X) \in \mathbb{Z}[X] \;:\; (R \in \mathcal{F} \text{ and } f(R) \subset Z(R)) \Longrightarrow R \text{ commutative}\}\,.$$

For these definitions, we allow the polynomials $f(X) \in \mathbb{Z}[X]$ to have nonzero constant term only if $\mathcal{F}$ is a class of unital rings, since otherwise $f(R)$ makes no sense. In fact, we will consider only two choices of $\mathcal{F}$: $\mathcal{F} = \mathcal{R}$, the class of all (not necessarily unital) rings, and $\mathcal{F} = \widetilde{\mathcal{R}}$, the class of all unital rings. We refer to polynomials in $C_Z(\mathcal{F})$ and $C_0(\mathcal{F})$ as *Z-polynomials* and *C-polynomials*, respectively, if $\mathcal{F} = \mathcal{R}$, and as *Z-unital polynomials* and *C-unital polynomials*, respectively, if $\mathcal{F} = \widetilde{\mathcal{R}}$.

Note that the condition $f(R) = 0$ implies in particular that $f(0) = 0$. It follows that the condition $f(R) = 0$ for $f(X) = \sum_{i=0}^n \alpha_i X^i$ and $R \in \widetilde{\mathcal{R}}$ can be split into two separate conditions: $\alpha_0 1 = 0$ (i.e. R has characteristic divisible by α_0) and $g(R) = 0$ where $g(X) = \sum_{i=1}^n \alpha_i X^i$. In particular if $a_0(f) = \pm 1$, then $f(R) = 0$ only if R is the trivial ring. By contrast, $f(R) = 0$ for $f(X) = 2 + X - X^2$ if and only if R is a Boolean ring, and $f(R) = 0$ for $f(X) = 3 + X - X^3$ if and only if R is a ring of characteristic 3 for which $X^3 = X$ (and non-trivial rings of this type exist, such as $Z_3[X]/(X^2 - 1)$).

Compared with [2], we have slightly changed the definition of $C_Z(\mathcal{F})$: we are allowing functions with nonzero constant term if $\mathcal{F} = \widetilde{\mathcal{R}}$. Such a term was omitted previously because it does not affect whether or not *a single polynomial* $f(X)$ lies

[1]Of course if $f(X) \in \mathbb{Z}[X]$, $s(f)$ could be written as $f(1)$ where $1 \in \mathbb{Z}$ but, since we evaluate such polynomials on general rings R, we prefer to write $s(f)$ to remove the ambiguity. By contrast we never evaluate a polynomial $g(X) \in \mathbb{Z}_p[X]$ on a ring, so we can (and do) unambiguously write $g(m)$ for any $m \in \mathbb{Z}_p$.

in $C_Z(\widetilde{\mathcal{R}})$. However a change in the constant term of a generator changes other terms of products involving that generator, so we allow such constant terms here.

A well-known result of Jacobson [4, Theorem 11] shows that for $n > 1$, $X^n - X$ is a C-polynomial. Herstein [3] showed that if $f(X) \in X\mathbb{Z}[X]$ with $a_1(f) = \pm 1$, then $f(X)$ is not just a C-polynomial, but also a Z-polynomial. We will refer to any polynomial of the form $f(X) = \pm X + \sum_{i=0}^{n} \alpha_i X^i \in \mathbb{Z}[X]$ as a *Herstein polynomial*.

More generally, we have the following theorem. Here, (a) is the main result in Laffey and MacHale's paper [5], while (b) is Proposition 4 of [2].

Theorem A. *Let $f(X) \in \mathbb{Z}[X]$.*

(a) $f(X)$ is a C-polynomial if and only if $f(X)$ is either a Herstein polynomial, or $f(X)$ satisfies the following set of three conditions: $a_1(f) = \pm 2$, $a_2(f)$ is odd, and $\sum_{i=2}^{n} a_i(f)$ is odd.

(b) $f(X)$ is a Z-polynomial if and only if it is a Herstein polynomial.

We next define some families of conditions indexed by a prime $p \in \mathbb{N}$ that we will need. Let

$$\left.\begin{aligned} b_{p,j}(f) &= \sum_{\substack{1\le i\le n \\ i \equiv j \pmod{p-1}}} i a_i(f) \\ c_{p,j}(f) &= \sum_{\substack{0\le i\le n \\ i \equiv j \pmod{p-1}}} a_i(f) \end{aligned}\right\}, \qquad 0 \le j < p-1\,,$$

and then define the sets

$$\begin{aligned} S_p(f) &:= \{a_0(f), a_1(f)\} \,\cup\, \{b_{p,j}(f), c_{p,j}(f) \mid 0 \le j < p-1\}\,, \\ T_p(f) &:= \{a_1(f)\} \,\cup\, \{b_{p,j}(f) \mid 0 \le j < p-1\}\,, \\ U_p(f) &:= \{a_0(f)\} \cup \{c_{p,j}(f) \mid 0 \le j < p-1\} = S_p(f) \setminus T_p(f)\,. \end{aligned}$$

We say that $f(X) \in \mathbb{Z}[X]$ *satisfies the S_p condition* if $S_p(f)$ contains at least one non-multiple of p. The T_p and U_p conditions are defined analogously. The S_p and T_p conditions were used to characterize C-unital and Z-unital polynomials in [1] and [2] (see below), while the U_p condition will be important in Section 3.

Combining Theorems 1 and 2 of [1], we get the following characterization of C-unital polynomials.

Theorem B. *The following conditions are equivalent for $f(X) \in \mathbb{Z}[X]$:*

(a) $f(X) \in C_0(\widetilde{\mathcal{R}})$;
(b) $f(X)$ satisfies the S_p condition for all primes $p \in \mathbb{N}$;
(c) $f(X)$ is primitive and it satisfies the S_p condition for all primes $p \le n/2$ that divide $a_1(f)$.

The following analogous characterization of Z-unital polynomials is a combination of Theorems 1 and 5 of [2].

Theorem C. *The following conditions are equivalent for $f(X) \in \mathbb{Z}[X]$:*

(a) $f(X) \in C_Z(\widetilde{\mathcal{R}})$;

(b) $f(X)$ *satisfies the* T_p *condition for all primes* $p \in \mathbb{N}$*;*

(c) $f(X)$ *is primitive and it satisfies the* T_p *condition for all primes* $p \leq n$ *that divide* $a_1(f)$*.*

For brevity, we call a polynomial product semigroup S a *forcing semigroup* if $S \subset C_0(\mathcal{F})$ or $S \subset C_Z(\mathcal{F})$. There are potentially four types of forcing semigroups of interest to us: $\mathcal{F}$ could be $\mathcal{R}$ or $\widetilde{\mathcal{R}}$, and "forcing" could mean that $S \subset C_0(\mathcal{F})$ or that $S \subset C_Z(\mathcal{F})$. We consider all four situations, and show that there are only examples of one type.

We already have characterizations of $C_0(\mathcal{F})$ and $C_Z(\mathcal{F})$, so we focus on characterizing forcing semigroups in terms of conditions on the generators. Consequently we make the following definitions.

$$C_0(\mathcal{F}, \mathrm{prod}) = \{G \subset \mathbb{Z}[X] \mid G \neq \emptyset \text{ and } \langle G \rangle \subset C_0(\mathcal{F})\},$$
$$C_Z(\mathcal{F}, \mathrm{prod}) = \{G \subset \mathbb{Z}[X] \mid G \neq \emptyset \text{ and } \langle G \rangle \subset C_Z(\mathcal{F})\}.$$

Above $\langle G \rangle$ means the polynomial product semigroup with generator set G.

We finish this section by showing that forcing semigroups fail to exist in three of the four cases that interest us. We start with the rather trivial fact that there are no polynomial product semigroups of C-polynomials (or Z-polynomials).

Proposition 2.1. $C_0(\mathcal{R}, \mathrm{prod}) = C_Z(\mathcal{R}, \mathrm{prod}) = \emptyset$.

Proof. Since trivially $C_Z(\mathcal{R}, \mathrm{prod}) \subset C_0(\mathcal{R}, \mathrm{prod})$, it suffices to prove that $C_0(\mathcal{R}, \mathrm{prod})$ is empty. By Theorem A(a), $\langle G \rangle \subset C_0(\mathcal{R})$ would imply that each $f(X) \in \langle G \rangle$ had the form $f(X) := \sum_{i=1}^n a_i X^i \in \mathbb{Z}[X]$, where $a_1 \in \{\pm 1, \pm 2\}$. If a generator $f(X)$ is of this form, then certainly $(f(X))^2$ is not. □

Polynomial product semigroups of Z-unital polynomials also fail to exist. This will follow immediately from the following simple lemma.

Lemma 2.2. *If* $f(X) = \sum_{i=0}^n \alpha_i X^i \in \mathbb{Z}[X]$*, and* $p \in \mathbb{N}$ *is a prime, then* $(f(X))^p = g(X) + \sum_{i=0}^n \alpha_i^p X^{ip}$*, where the coefficients of* $g(X)$ *are all divisible by* p*.*

Proof. Let $(f(X))^p = \sum_{i=0}^{pn} \beta_i X^i$. Any given coefficient β_i is the sum of *mixed terms* plus possibly an *unmixed term*, where the possible unmixed term is that of the form α_j^p (occurs only if $i = pj$) and all other contributions can be gathered into mixed terms with coefficients of the form

$$\binom{p}{j_1, \ldots, j_m} \prod_{k=1}^m (\alpha'_k)^{j_k},$$

where $\sum_{k=1}^m j_k = p$ and $\alpha'_k = \alpha_{j_k}$ for some set of distinct indices $1 \leq j_k < p$, $1 \leq k \leq m$, $m \geq 2$. Because p is prime, all such multinomial factors are divisible by p, and the result follows. □

Proposition 2.3. $C_Z(\widetilde{\mathcal{R}}, \mathrm{prod}) = \emptyset$.

Proof. Suppose $\emptyset \neq G \subset \mathbb{Z}[X]$. Let $f(X) \in G$, where $f(X) = \sum_{i=0}^n \alpha_i X^i$. By Lemma 2.2, $(f(X))^p = g(X) + h(X)$, where $g(X)$ is a polynomial all of whose coefficients are divisible by p, and $a_i(h)$ is nonzero only when $p \mid i$. The T_p condition fails for any such polynomial $g(X) + h(X)$, so $G \notin C_Z(\widetilde{\mathcal{R}}, \mathrm{prod})$ by Theorem C. □

3. Main results

We begin by showing that the conditions S_p, T_p, and U_p can be characterized in terms of $\mathbb{Z}_p[X]$ divisibility. We then apply this result to characterize the polynomial product semigroups of C-unital polynomials.

Theorem 3.1. *Let $f(X) \in \mathbb{Z}[X]$.*

(a) $f(X)$ satisfies the S_p condition if and only if $(X^p - X)^2$ does not divide $f_p(X)$.
(b) $f(X)$ satisfies the T_p condition if and only if $X^p - X$ does not divide $f'_p(X)$.
(c) $f(X)$ satisfies the U_p condition if and only if $X^p - X$ does not divide $f_p(X)$.

Proof. We first prove (c). Suppose that $f(X)$ does not satisfy the U_p condition. Now $f(0) = a_0(f)$ is divisible by p, so $f_p(0) = \phi_p(a_0(f)) = 0$. Suppose $m \in \mathbb{Z}_p^*$. By Fermat's Little Theorem, $m^{p-1} = 1$, and so $m^j = m^{j'}$ whenever $(p-1) \mid (j - j')$. Using the fact that ϕ_p is an additive homomorphism, it follows that

$$f_p(m) = \sum_{j=0}^{p-2} \phi_p(c_{p,j}(f)) m^j \,.$$

Because $f(X)$ does not satisfy the U_p condition, $\phi_p(c_{p,j}(f)) = 0$ for all $0 \le j < p-1$, and so $f_p(m) = 0$ for all m. Since $X^p - X = \prod_{i \in \mathbb{Z}_p} (X - i)$, it is clear that $X^p - X$ divides $f_p(X)$.

Conversely suppose $(X^p - X) \mid f_p(X)$. Certainly $a_0(f_p) = 0$ and so $p \mid a_0(f)$. Let

$$g(X) := \sum_{j=0}^{p-2} \phi_p(c_{p,j}(f)) X^j \,.$$

If $m \in \mathbb{Z}_p^*$, then again by Fermat's Little Theorem, $f_p(m) = g(m)$. But $f_p(m) = 0$ and so $g(m) = 0$. Thus $g(X)$ is a polynomial of degree at most $p-2$ with at least $p-1$ distinct roots. Consequently we must have $\phi_p(c_{p,j}(f)) = 0$ for all j, and so $f(X)$ fails to satisfy the U_p condition.

Next note that the T_p condition for $f(X)$ is just the U_p condition for $f'(X)$, and that $\Phi_p(f') = f'_p$. Thus by (c), $f(X)$ satisfies the T_p condition if and only if $X^p - X$ does not divide $f'_p(X)$.

Finally $f(X)$ fails to satisfies the S_p condition if and only if $f(X)$ fails to satisfy both the T_p and U_p conditions, and so if and only if $X^p - X$ divides both $f_p(X)$ and $f'_p(X)$. If $(X^p - X)^2$ divides $f_p(X)$, then the product rule for the formal derivative implies that $X^p - X$ divides $f'_p(X)$. Suppose instead that $X^p - X$ divides $f_p(X)$, but that $(X^p - X)^2$ does not divide $f_p(X)$. Then for some $m \in \mathbb{Z}_p$, we have $f_p(X) = (X - m)g(X)$, where $g(X)$ is not divisible by $X - m$. Again by the product rule, we have $f'_p(X) = g(X) + (X - m)g'(X)$, so $f'_p(m) = g(m) \neq 0$, and consequently $f'_p(X)$ is not divisible by $X - m$. We have shown that $(X^p - X)^2$ divides $f_p(X)$ if and only if $f_p(X)$ and $f'_p(X)$ are both divisible by $X^p - X$, and so if and only $f(X)$ fails to satisfy the S_p condition. $\square$

Using Theorem 3.1 and Theorem B, it is now easy to characterize polynomial product semigroups of C-unital polynomials. We record this as a corollary, and leave the easy proof to the reader.

Corollary 3.2. *Let G be a nonempty subset of $\mathbb{Z}[X]$, and let $S := \langle G \rangle$. Then the following are equivalent:*

(a) $G \in C_0(\widetilde{\mathcal{R}}, \text{prod})$.
(b) For all primes $p \in \mathbb{N}$, there exists an integer m with $0 \le m < p$ such that $p \nmid f(m)$ for all $f(X) \in G$.
(c) Finite products of distinct generators satisfies the U_p condition for all primes $p \in \mathbb{N}$.
(d) Products of at most p distinct generators satisfies the U_p condition for all primes $p \in \mathbb{N}$.

If $G = \{f_1(X), \dots, f_k(X)\}$ and $N = \sum_{i=1}^k \deg(f_i)$, then the above are also equivalent to the following condition.

(e) For all primes $p \le N$, there exists $m \in \mathbb{Z}_p$ such that $\prod_{i=0}^k \Phi_p(f_i)(m) \neq 0$.

The main result in Herstein's paper [3] is stronger than we have earlier indicated. In fact it states that a (not necessarily unital) ring R is necessarily commutative if for each $x \in R$ there exists a Herstein polynomial $f_x(X)$ such that $f_x(x) \in Z(R)$. It would be interesting to obtain a similar characterization for polynomial product semigroups although, in view of Proposition 2.3, it should involve the condition $f_x(x) = 0$ rather than $f_x(x) \in Z(R)$. We state a partial result in this direction.

Theorem 3.3. *The following are equivalent for a polynomial product semigroup S.*

(a) If R is a ring, and for each $x \in R$ there exists $f_x(X) \in S$ such that $f_x(x) = 0$ and $f_x(X) = f_{x+1}(X)$, then R is necessarily commutative.
(b) All elements of S are C-polynomials.
(c) For each prime $p \in \mathbb{N}$, every finite product of at most p distinct generators of S satisfies the U_p condition.

Proof sketch. Corollary 3.2 tells us that (b) and (c) are equivalent, and trivially (a) implies (b), so it suffices to prove that (c) implies (a). To prove this, we first review the proof in [1] that (c) implies (b). First, by the discussion in Section 2 (immediately after the definition of C-unital polynomials), it suffices to show this under the assumption that $a_0(f) = 0$. The proof then reduces to showing that R is necessarily commutative under the assumptions that R has characteristic a power p^k of a prime p, and $f(R) = 0$ for some $f(X) \in X\mathbb{Z}[X]$ satisfying the S_p condition.

Since $p^k R = 0$, we may treat polynomials $g(X)$ for which $g(R) = 0$ as elements of $\mathbb{Z}_{p^k}[X]$ rather than $\mathbb{Z}[X]$. A *Herstein polynomial* in this setting is a polynomial $g(X) \in \mathbb{Z}_{p^k}[X]$ such that $a_1(g) = \pm 1$: such a $g(X)$ has the property that if $g(R) = 0$ for a ring R of characteristic p^k, then R is necessarily commutative.

We showed in [1] that the S_p condition implies that for some $i \in \mathbb{Z}_{p^k}$, either $f(X+i)$ or $(X+i)f(X+i)$ is of the form $cg(X)$, where $g(X)$ is a Herstein polynomial and the constant c is a $\mathbb{Z}_{p^k}$ unit. It then followed that $g(R) = 0$, and so R was commutative.

In our setting, the fact that $f_x(X) = f_{x+1}(X)$ for all $x \in R$ means that $f_x(X) = f_{x+i}(X)$ for all $x \in R$ and $i = i \cdot 1 \in R$. The argument then goes through unchanged; note that the reduction to prime power characteristic also requires this assumption since it uses the fact that $f_i(X)$ is independent of $i = i \cdot 1 \in R$. Thus for all $x \in R$ there exists a Herstein polynomial $g_x(X)$ such that $g_x(x) = 0$, which implies that R is commutative. □

4. Examples

Here we consider polynomial product semigroup examples relevant to Corollary 3.2. In all cases, (e) refers to Corollary 3.2(e).

Example 4.1. For $p = 2$, the U_p condition is equivalent to the statement that either $a_0(f)$ is odd for all generators $f(X)$, or the coefficient sum $s(f)$ is odd for all generators $f(X)$. Thus if $|a_0(f)|$ is a power of 2 for all $f(X) \in G$, and we rule out the uninteresting case[2] where $|a_0(f)| = 1$ for all $f(X) \in G$, then $G \in C_0(\widetilde{\mathcal{R}}, \mathrm{prod})$ if and only if $s(f)$ is odd for all $f(X) \in G$.

Our next example makes it clear that unlike the case $p = 2$, it is not sufficient to verify that generators satisfy the U_p condition when $p > 2$.

Example 4.2. Let $G = \{f(X), g(X)\}$, where $f(X) = 4X - X^2$ and $g(X) = 4X + X^2$. Then the case $p = 2$ of (e) holds since both coefficient sums are odd. Also, both $f(X)$ and $g(X)$ satisfy the U_3 condition: $f_3(X) = X - X^2$ and $g_3(X) = X + X^2$, so $f_3(-1) \neq 0$ and $g_3(1) \neq 0$. However $\Phi_3(fg)(X) = (X - X^2)(X + X^2)$ is divisible by $X^3 - X$, so the case $p = 3$ of (e) fails, and $G \notin C_0(\widetilde{\mathcal{R}}, \mathrm{prod})$.

For one-parameter semigroups, the characterization is very simple.

Example 4.3. $G = \{f(X)\} \in C_0(\widetilde{\mathcal{R}}, \mathrm{prod})$ if and only if $f(X)$ is a primitive polynomial and $f(X)$ satisfies the U_p condition for each prime $p \leq \deg(f)$. For instance, if $f(X)$ is a primitive quadratic then $\{f(X)\} \in C_0(\widetilde{\mathcal{R}}, \mathrm{prod})$ if and only if either $a_0(f)$ or $s(f)$ is odd. In the case of a primitive polynomial of degree at most 4, the same condition is necessary but for a condition that is also sufficient we additionally need that not all the numbers in $\{a_0(f), a_1(f)+a_3(f), a_2(f)+a_4(f)\}$ are divisible by 3.

Example 4.4. Consider $G := \{f(X), g(X)\}$, $f(X) = 2X + X^2$ and $g(X) = X + X^2 + X^3$. We need to verify (e) for all primes $p \leq 5$. First (e) holds for $p = 2$ because both coefficient sums are odd. Defining $h(X) := f(X)g(X)$, we see that

$$h(X) = 2X^2 + 3X^3 + 3X^4 + X^5 .$$

Now $U_3 = \{0, 0{+}2{+}3, 0{+}3{+}1\}$ and $U_5 = \{0, 0{+}3, 0{+}1, 2, 3\}$ include non-multiples of 3 and 5, respectively. Thus $G \in C_0(\widetilde{\mathcal{R}}, \mathrm{prod})$.

[2] This is uninteresting because it implies that $|a_0(g)| = 1$ for all $g(X)$ in the semigroup. Thus if $g(R) = 0$, and in particular $g(0) = 0$, then $1 = 0$ in R, and so R is the trivial ring.

References

[1] S.M. Buckley and D. MacHale, *Polynomials that force a unital ring to be commutative*, Results Math., to appear. (Available at `http://www.maths.nuim.ie/staff/sbuckley/Papers/bm_cpoly.pdf`)

[2] S.M. Buckley and D. MacHale, *Z-polynomials and ring commutativity*, preprint. (Available at `http://www.maths.nuim.ie/staff/sbuckley/Papers/bm_zpoly.pdf`)

[3] I.N. Herstein, *The structure of a certain class of rings*, Amer. J. Math. **75** (1953), 864–871.

[4] N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. Math. **46** (1945), 695–707.

[5] T.J. Laffey and D. MacHale, *Polynomials that force a ring to be commutative*, Proc. Roy. Irish Acad. Sect. A **92A** (1992), 277–280.

S.M. Buckley:
Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.

E-mail address: `stephen.buckley@maths.nuim.ie`

Yu. Zelenyuk:
School of Mathematics, University of the Witwatersrand, Wits 2050, Johannesburg, South Africa.

E-mail address: `yuliya.zelenyuk@wits.ac.za`