Z-POLYNOMIALS AND RING COMMUTATIVITY

S.M. BUCKLEY AND D. MACHALE

Abstract. We characterise polynomials $f$ with integer coefficients such that a ring with unity $R$ is necessarily commutative if $f(x)$ is central for all $x \in R$. We also solve the corresponding problem without the assumption that the ring has a unity.

1. Introduction

In [4] and [1], characterisations were given for the polynomials $f$ with integer coefficients such that a ring $R$ is necessarily commutative whenever $f(x) = 0$ for all $x \in R$. Here we characterise those polynomials $f$ such that a ring $R$ is necessarily commutative whenever $R$ satisfies the weaker condition that $f(x)$ is central for all $x \in R$. The fact that these two classes of polynomials are different follows from the observation that a ring satisfying the identity $x^2 - 2x = 0$ is necessarily commutative, while there are easy examples to show that there are non-commutative rings where $x^2 - 2x$ is central for all $x$.

Throughout this paper, $f(X) = \sum_{i=1}^{n} a_i X^i \in XZ[X]$. Given a ring $R$, we write $f(R) = 0$ if $f(x) = 0$ for all $x \in R$, and we write $f(R) \subset Z(R)$ if $f(x) \in Z(R)$ for all $x \in R$; here $Z(R)$ is the centre of $R$. For us, a ring does not necessarily have a unity, unless this is assumed.

Given a class $\mathcal{F}$ of rings, we denote by $C_0(\mathcal{F})$ and $C_Z(\mathcal{F})$ the sets of polynomials $f \in XZ[X]$ that force a ring $R \in \mathcal{F}$ to be commutative whenever $f(x)$ always lies in $\{0\}$ or $Z(R)$, i.e.,

$$C_0(\mathcal{F}) = \{ f(X) \in XZ[X] : (R \in \mathcal{F} \text{ and } f(R) = 0) \implies R \text{ commutative} \} ,$$

$$C_Z(\mathcal{F}) = \{ f(X) \in XZ[X] : (R \in \mathcal{F} \text{ and } f(R) \subset Z(R)) \implies R \text{ commutative} \} .$$

We are mainly interested in two classes $\mathcal{F}$: the class of all rings $\mathcal{R}$, and the class of all rings with unity $\mathcal{\hat{R}}$. For each prime $p$, we also define the class $\mathcal{R}_p$ of rings such that $p^k R \subset Z(R)$ for some $k \in \mathbb{N}$, and the class $\mathcal{\hat{R}}_p := \mathcal{\hat{R}} \cap \mathcal{R}_p$. We refer to polynomials in $C_Z(\mathcal{R})$ as Z-polynomials, and polynomials in $C_0(\mathcal{R})$ as C-polynomials.

A well-known result of Jacobson [3, Theorem 11] shows that for $n > 1$, $X^n - X$ is a C-polynomial. More generally, Herstein [2] showed that if $a_1 = \pm 1$, then $f$ is not just a C-polynomial, but also a Z-polynomial. In view of that result, we call $f$ a Herstein polynomial if $a_1 = \pm 1$.

2010 Mathematics Subject Classification. 16R50.
Using Herstein’s result, the second author and Laffey [4] showed that \( f \) is a C-polynomial if and only if \( f \) is either a Herstein polynomial, or \( f \) satisfies the following set of three conditions: \( a_1 = \pm 2 \), \( a_2 \) is odd, and \( \sum_{i=2}^{n} a_i \) is odd. We will see that Z-polynomials form a more restrictive class than C-polynomials. In fact Z-polynomials coincide with Herstein polynomials; see Proposition 4.

Our characterisation of \( C_\mathbb{Z}(\mathcal{R}) \) is not as simple to state as that of \( C_\mathbb{C}(\mathcal{R}) \). It involves the following family of conditions indexed by a prime \( p \):

There is at least one non-multiple of \( p \) among the numbers
\[
T_p := \{a_1\} \cup \{b_j \mid 0 \leq j < p - 1\},
\]
where
\[
b_j = \sum_{i \equiv j (\mod p - 1)}^{1 \leq i \leq n} ia_i, \quad 0 \leq j < p - 1.
\]
Whenever the above condition holds, we say that \( f \) satisfies the \( T_p \) condition.

**Theorem 1.** Suppose \( f(X) = \sum_{i=1}^{n} a_i X^i \in \mathbb{Z}[X] \). Then \( f \in C_\mathbb{Z}(\mathcal{R}) \) if and only if the greatest common divisor of the numbers \( \{a_i\}_{i=1}^{n} \) is 1, and \( f \) satisfies the \( T_p \) condition for all primes \( p \leq n \) that divide \( a_1 \).

By comparison, we note that the main result in [1] states that a polynomial \( f(X) \in \mathbb{X}[X] \) lies in \( C_\mathbb{R}(\mathcal{R}) \) if and only if the greatest common divisor of the numbers \( \{a_i\}_{i=1}^{n} \) is 1, and \( f \) satisfies the \( S_p \) condition for all primes \( p \leq n/2 \) that divide \( a_1 \), where the \( S_p \) condition involves a set \( S_p \) is defined by:
\[
S_p := T_p \cup \{c_j \mid 0 \leq j < p - 1\},
\]
where
\[
c_j = \sum_{i \equiv j (\mod p - 1)}^{1 \leq i \leq n} a_i, \quad 0 \leq j < p - 1.
\]

After reducing the problem to understanding \( C_\mathbb{Z}(\mathcal{R}_p) \) for all primes \( p \) in Section 2, we prove the main results in Section 3.

### 2. Reduction to prime powers

There is one rather obvious necessary condition for \( f \in C_\mathbb{Z}(\mathcal{R}_p) \): given any prime \( p \), the ring \( GL_2(\mathbb{F}_p) \) is non-commutative and of characteristic \( p \), so if every coefficient of \( f \) is divisible by \( p \) then \( f \notin C_0(\mathcal{R}_p) \supset C_\mathbb{Z}(\mathcal{R}_p) \). Thus every a polynomial in \( C_\mathbb{Z}(\mathcal{R}_p) \) (or in \( \bigcap_{p \text{ prime}} C_\mathbb{Z}(\mathcal{R}_p) \)) is primitive, i.e. the greatest common divisor of its coefficients is 1.

The rest of this section is dedicated to proving the following lemma which reduces the task of characterizing \( C_\mathbb{Z}(\mathcal{R}) \) to that of characterizing \( C_\mathbb{Z}(\mathcal{R}_p) \) for all primes \( p \).
Lemma 2. $C_Z(\tilde{R}) = \bigcap_{p \text{ prime}} C_Z(\tilde{R}_p)$.

As a first step, the following simple lemma shows that commutativity of a ring $R$ such that $mR \subset Z(R)$ follows from commutativity of its subrings $R_p$ satisfying $p^k R_p \subset Z(R)$ for some $k \in \mathbb{N}$ and prime factor $p$ of $m$.

Lemma 3. Suppose $mR \subset Z(R)$, where $m \in \mathbb{N}$ has prime factorisation $m = \prod p^{k_p}$. For each prime factor $p$ of $m$, let $m_p := m/p^{k_p}$ and $R_p := m_p R$. Then

(a) $R_p$ is an ideal in $R$, and $p^{k_p} R_p \subset Z(R)$.
(b) Every $x \in R$ can be written in the form
$$x = z + \sum_{p \mid m} x_p, \quad z \in Z(R), \ x_p \in R_p.$$  

(c) $xy = yx$ whenever $x \in R_p$, $y \in R_q$, and $p, q$ are distinct prime factors of $m$.
(d) $R$ is commutative if and only if each $R_p$ is commutative.

Proof. Part (a) is immediate. As for (b), since the greatest common divisor of the numbers $\{m_p : p \mid n\}$ is 1, we can choose $n_p \in \mathbb{Z}$ such that $\sum_{p \mid m} n_p m_p$ equals 1 mod $m$, and then $x = \sum_{p \mid m} n_p (m_p x) \in Z(R)$.

We next prove (c). Let $x = m_p x', y = m_q y'$. Since $m$ divides $m_p m_q$, we can use distributivity repeatedly to get
$$xy = ((m_p m_q) x') y' = y'((m_p m_q) x') = yx.$$  

Finally for (d), the “only if” part is trivial. Conversely, suppose that each of the rings $R_p$ is commutative. Given $x, y \in R$, we write
$$x = z + \sum_{p \mid m} x_p, \quad y = w + \sum_{p \mid m} y_p,$$
where $z, w \in Z(R)$, and $x_p, y_p \in R_p$ for $p \mid m$. Using distributivity we expand $xy$ into a sum of products of pairs of elements from the set $\{z, w\} \cup \left(\bigcup_{p \mid m} \{x_p, y_p\}\right)$. Bearing in mind (c), we see that the factors in each of these products commute, and so $xy = yx$. $\square$

The degree $\deg(f)$ and codegree $\cdeg(f)$ of a nonzero polynomial $f(X) = \sum_{i=1}^n a_i X^i$ are the largest and smallest $i \in \mathbb{N}$, respectively, such that $a_i \neq 0$.

Proof of Lemma 2. Clearly $C_Z(\tilde{R}) \subset \bigcap_{p \text{ prime}} C_Z(\tilde{R}_p)$, so we need only prove the reverse implication. Suppose therefore that $f \in \bigcap_{p \text{ prime}} C_Z(\tilde{R}_p)$, so $f$ is necessarily primitive. Suppose also that $f(R) \subset Z(R)$ for some given unital ring $R$. $f$ must be of degree at least 1. We write $f(X) = \sum_{i=1}^n a_i X^i \in \mathbb{Z}[X]$, where $a_n \neq 0$ and $n \in \mathbb{N}$, so $1 \leq \cdeg(f) \leq \deg(f) = n$. 


If \( \text{codeg}(f) < \deg(f) \) then \( g(X) := 2^n f(X) - f(2X) \) defines another nonzero polynomial such that \( \text{codeg}(g) = \text{codeg}(f) \) and \( \deg(g) \leq \deg(f) - 1 \). In fact
\[
g(X) = \sum_{i=1}^{n-1} (2^n - 2^i)a_i X^i.
\]
Also note that \( g(R) \subset Z(R) \). Iterating this reduction procedure we eventually get a nonzero monomial such that \( h(R) \subset Z(R) \). If \( \deg(h) > 1 \), then simply replace \( h \) by \( H(X) := h(X + 1) - h(1) \). Then \( \deg(H) = \deg(h) \) and \( \text{codeg}(H) = 1 \), so if we again repeat the reduction procedure we eventually get a polynomial \( F(X) = mX, m \in \mathbb{N} \), such that \( F(R) \subset Z(R) \). Thus \( mR \subset Z(R) \).

Define \( m_p \) and \( R'_p \) as in Lemma 3, and let
\[
R'_p = \{m_px + b \cdot 1 \mid x \in R, n \in \mathbb{Z}\}.
\]
Then for each prime factor \( p \) of \( m \), \( R'_p \) is a subring of \( R, 1 \in R'_p \), and \( p^kR'_p \subset Z(R) \), so \( R'_p \in \tilde{R}_p \). Since also \( f(R'_p) \subset Z(R) \cap R'_p = Z(R'_p) \) for all \( p \), and \( f \in C_Z(\tilde{R}_p) \), each \( R'_p \) is commutative. Thus also each \( R_p \) is commutative, and so \( R \) is commutative by Lemma 3. But \( R \) is an arbitrary ring satisfying \( f(R) \subset Z(R) \), so we deduce that \( f \in C_Z(\tilde{R}) \), as required. \( \square \)

3. PROOFS OF RESULTS

We first state and prove our characterisation of \( C_Z(\mathcal{R}) \).

**Proposition 4.** The classes of \( Z \)-polynomials and Herstein polynomials coincide.

**Proof.** The fact that Herstein polynomials are \( Z \)-polynomials is Herstein’s main result in [2]. Conversely, as mentioned in the Introduction, it is shown in [4] that if \( f(X) = \sum_{i=1}^{n} a_iX^i \in Z[X] \) is a \( C \)-polynomial, then either it is a Herstein polynomial or \( a_1 = \pm 2 \). Thus to establish our result, it suffices to exhibit a non-commutative ring \( R \) such that \( f(R) \subset Z(R) \) whenever \( a_1 \) is even.

This is rather easy to do: we simply take \((R, +, \cdot)\) to be the ring of \( 3 \times 3 \) matrices over \( \mathbb{Z}_2 \) of the form
\[
\begin{pmatrix}
0 & a & b \\
0 & 0 & c \\
0 & 0 & 0
\end{pmatrix}
\]
This ring is not commutative since, for instance,
\[
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix}
\neq
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{pmatrix}.
\]
However \( 2x = x^3 = 0 \) for all \( x \in R \). Moreover since \( xyz = 0 \) for all \( x, y, z \in R \), it follows that \( x^2 \in Z(R) \) for all \( x \). Thus if \( a_1 \) is even, then \( f(x) = a_2 x^2 \in Z(R) \) for all \( x \in Z(R) \). \( \square \)
We now turn to the proof of Theorem 1. The main step is the following characterisation of $C_Z(\tilde{R}_p)$.

**Theorem 5.** Suppose $f(X) = \sum_{i=1}^n a_i X^i \in \mathbb{Z}[X]$, and let $p$ be a prime. Then $f \in C_Z(\tilde{R}_p)$ if and only if $f$ satisfies the $T_p$ condition.

**Proof.** We prove sufficiency of the $T_p$ condition. We may assume that $R \in \tilde{R}$ is such that $p^k R \subset \mathbb{Z}(R)$ for some $k \in \mathbb{N}$. When considering $f(R) \subset \mathbb{Z}(R)$ for such rings, we may treat the coefficients of $f$ as either elements of $\mathbb{Z}_{p^k}$, or elements of $\mathbb{Z}$, as suits us.

If $p \nmid a_1$, then $a_1$ is a unit mod $p^k$, so $g(X) := a_1^{-1} f(X) \in \mathbb{Z}_{p^k}[X]$ has the form $X + \sum_{i=2}^n d_i X^i$, and so it is a Herstein polynomial when we view its coefficients as being integers. In particular the condition $g(R) \subset \mathbb{Z}(R)$ forces characteristic $p^k$ rings $R \in \tilde{R}$ to be commutative. We may therefore assume that $p \nmid a_1$.

Suppose that there exists $i$, $0 \leq i < p - 1$, such that $p \nmid b_i$. We treat $f(X)$ as a polynomial in $\mathbb{Z}_{p^k}[X]$, but let us also write $f_p(X)$ for $f(X)$ when instead viewed as an element of $\mathbb{Z}_p[X]$. Expanding $f_p(X + t)$ for $t \in \mathbb{Z}_p$, we see that the coefficient of $X$ is $s_p(t) := \sum_{i=1}^n i a_i t^{i-1}$. Let $S_p(X) := \sum_{i=0}^{p-1} b_i X^i \in \mathbb{Z}_p[X]$. By Fermat’s Little Theorem, $s_p(t) = S_p(t)$ for all $t \in \mathbb{Z}_p$. The fact that $p \nmid b_i$ for some $i$ means that $S_p$ is not the zero polynomial, and so it has at most $p - 1$ roots. Thus there exists $t \in \mathbb{Z}_p$ such that $s_p(t) \neq 0$. It follows that the coefficient of $X$ in the expansion of $f(X + t \cdot 1)$ is coprime to $p$ for some $t \in \mathbb{Z}_{p^k}$. Fixing this value of $t$ and picking $k \in \mathbb{Z}_{p^k}$ which is equivalent to $t$ mod $p$, we get a polynomial $g(X) := f(X + k) - f(k) \in \mathbb{Z}_{p^k}[X]$ such that $g(R) \subset \mathbb{Z}(R)$ and such that the coefficient of $X$ in $g$ is a unit mod $p^k$. This implies the commutativity of $R$ as before.

We now prove the converse. Suppose therefore that the $T_p$ condition fails for a given function $f$. Let $R$ be the ring of matrices

$$ x = \begin{pmatrix} \alpha & \beta & \gamma \\ 0 & \alpha & \delta \\ 0 & 0 & \alpha \end{pmatrix}, $$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_p$. For brevity, let us call $\alpha, \beta, \gamma, \delta$, the first, second, third, and fourth coordinates of $x$, respectively.

Given such a matrix $x$, it can be verified inductively that for all $i > 1$,

$$ x^i = \begin{pmatrix} \alpha^i & i\alpha^{i-1}\beta & * \\ 0 & \alpha^i & i\alpha^{i-1}\gamma \\ 0 & 0 & \alpha^i \end{pmatrix}, $$

where $*$ equals $i\alpha^{i-1}\delta + (\frac{i}{2})\alpha^{i-2}\beta\gamma$ (and $\alpha^0$ is defined to be 1, even for $\alpha = 0$), but the actual value does not affect subsequent calculations.

Consider now $f(x)$. Because $t^p = t$ for all $t \in \mathbb{Z}_p$, it follows from (1) that the second coordinate of $f(x)$ equals $a_1 \beta + \sum_{i=0}^{p-2} d_i \alpha^{p+i-2}\beta$, where $d_1 = b_1 - a_1$ and
\[ d_i = b_i \] for every other index in this sum, and the numbers \( b_i \) are as in the \( T_p \) condition. Now \( T_p \) fails to hold, so \( a_i \) and all the \( b_i \)'s are divisible by \( p \), and so \( p | d_i \) for \( 0 \leq i < p - 1 \). It follows that the second coordinate of \( f(x) \) equals zero, and similarly we see that the fourth coordinate of \( f(x) \) is 0. Thus \( f(x) \) has the form

\[
\begin{pmatrix}
\varepsilon & 0 & 0 \\
0 & \varepsilon & 0 \\
0 & 0 & \varepsilon
\end{pmatrix},
\]

for some \( \varepsilon, \zeta \in \mathbb{Z}_p \). But it is readily verified that all such matrices lie in the centre of \( R \), so we have shown that \( f(x) \in Z(R) \) for all \( x \in R \) whenever \( T_p \) fails.

Now \( R \in \tilde{R}_p \), and it is non-commutative regardless of \( p \), since for instance

\[
\begin{pmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{pmatrix} \neq
\begin{pmatrix}
0 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{pmatrix}.
\]

Thus \( f \notin C_{Z}(\tilde{R}_p) \) if the \( T_p \) condition fails. \( \square \)

**Proof of Theorem 1.** Since \( C_{Z}(\tilde{R}) = \bigcap_{p \text{ prime}} C_{Z}(\tilde{R}_p) \),

it follows that the polynomials in \( C_{Z}(\tilde{R}) \) are precisely those for which the \( T_p \) condition holds for all primes \( p \). If the gcd of the coefficients is not 1, then all coefficients \( a_i \) are divisible by some prime \( p \), and certainly \( f \) does not satisfy the \( T_p \) condition. Thus by Theorem 5, \( f \notin C_{Z}(\tilde{R}). \)

For the converse direction, since \( T_p \) trivially holds when \( p \) does not divide \( a_1 \), it suffices to show that the \( T_p \) condition holds for all primes \( p > n \) as long as the gcd of the coefficients is 1. Because \( p > n \), all the sums in the \( T_p \) condition involve at most one term. Thus, since the gcd of the coefficients is 1, there exists \( i \leq n < p \) such that \( p \nmid ia_i = b_i \). \( \square \)

The characterisation for quadratic polynomials is particularly simple, and follows immediately from Theorem 1.

**Corollary 6.** Suppose \( f(X) = a_1X + a_2X^2 \in \mathbb{Z}[X] \). Then \( f \in C_{Z}(\tilde{R}) \) if and only if \( a_1 \) is odd.

According to [4], a polynomial \( f \) lies in \( C_{Z}(\tilde{R}) \) if and only if it is a Herstein polynomial. Comparing this with Corollary 6 or Theorem 1, it is easy to give examples of polynomials in \( C_{Z}(\tilde{R}) \setminus C_{Z}(\tilde{R}) \), for instance \( 3X + X^2 \) or \( 5X + 2X^3 \). Comparing Theorem 1 with the characterisation of \( C_{0}(\tilde{R}) \) in [1], it is easy to give examples of polynomials in \( C_{0}(\tilde{R}) \setminus C_{Z}(\tilde{R}) \), for instance \( 3X^2 + 2X^3 \) or \( X^2 \).

Lastly we note that the examples proving necessity in Theorem 5 (and so also in Theorem 1) involve only finite rings of prime characteristic. Thus if \( F \) is the
set of all finite rings with unity, then $C_Z(\mathcal{F}) = C_Z(\tilde{\mathcal{R}})$, while if $\mathcal{F}$ consists of all finite rings with unity and characteristic $p$, then $C_Z(\mathcal{F}) = C_Z(\tilde{\mathcal{R}}_p)$. This is analogous to the fact that if $\mathcal{F}$ is the set of all finite rings (without the assumption of unity), then $C_Z(\mathcal{F}) = C_Z(\mathcal{R})$ because the proof in [4] uses only finite rings to prove necessity.

References

[1] S.M. Buckley and D. MacHale, Polynomials that force a unital ring to be commutative, Results Math., to appear; http://dx.doi.org/10.1007/s00025-012-0296-0.

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

D. MacHale:
School of Mathematical Sciences, University College Cork, Cork, Ireland.
E-mail address: d.machale@ucc.ie