

Manuscript Number:

Title: Permutation polynomials over finite rings

Article Type: Regular Article

Keywords: permutation polynomials; local rings; group of permutation polynomials

Corresponding Author: Dr. Gabor Horvath,

Corresponding Author's Institution: University of Debrecen, Institute of Mathematics

First Author: Dalma Görcsös

Order of Authors: Dalma Görcsös; Gabor Horvath; Anett Mészáros

Abstract: Let $\text{PPol}(R)$ denote the group of permutation polynomials over the finite, commutative, unital ring R under composition. We generalize numerous results about permutation polynomials over $\mathbb{Z}_{p^n}$ to local rings by treating them under a unified manner. In particular, we provide a natural wreath product decomposition of permutation polynomials over the maximal ideal $\mathfrak{M}$ and over the finite field $R/\mathfrak{M}$. Further, we give a necessary and sufficient condition for a polynomial $f \in R[x]$ to be a permutation polynomial considering f and f' over the finite field $R/\mathfrak{M}$, thereby generalizing a similar result for $\mathbb{Z}_{p^n}$. We characterize the group of permutation polynomials over $\mathfrak{M}$ whenever the condition $\mathfrak{M}^{\{\text{abs}\{R/\mathfrak{M}\}\}} = \{0\}$ applies by describing a polynomial being identically equal to 0 with the help of the annihilators of the ideals $\mathfrak{M}_k = \left(r^k \mid r \in \mathfrak{M} \right)$. We derive the size of $\text{PPol}(R)$, thereby generalizing the same number formulas for $\mathbb{Z}_{p^n}$. Finally, we completely characterize when the group $\text{PPol}(R)$ is solvable, nilpotent, or abelian.

Dear Professor Mullen,

We would like to submit the attached paper

Permutation polynomials over finite rings
by Dalma Gorcsos, Gabor Horvath and Anett Meszaros to Finite Fields and
Their Applications.

In the paper we consider the group of permutation polynomial over
finite, commutative, unital rings.

Let $\text{PPol}(R)$ denote the group of permutation polynomials over the
finite, commutative, unital ring R under composition.

We generalize numerous results about permutation polynomials over
 $\mathbb{Z}_{p^n}$ to local rings by treating them under a unified manner.

In particular,

we provide a natural wreath product decomposition of permutation
polynomials over the maximal ideal M and over the finite field R/M .
Further,

we give a necessary and sufficient condition for a polynomial $f \in R[x]$
to be a permutation polynomial considering f and f' over the
finite field R/M ,

thereby generalizing a similar result for $\mathbb{Z}_{p^n}$.

We characterize the group of permutation polynomials over M whenever
the condition $M^{\{\text{abs}(R/M)\}} = \text{halmaz}\{0\}$ applies

by describing a polynomial being identically equal to 0 with the help of
the annihilators of the ideals $M_k = \left(r^k \mid r \in M \right)$.

We derive the size of $\text{PPol}(R)$,

thereby generalizing the same number formulas for $\mathbb{Z}_{p^n}$.

Finally,

we completely characterize when the group $\text{PPol}(R)$ is solvable,
nilpotent, or abelian.

We have attached the manuscript in pdf.

Thank you very much for your help.

Best Regards,
Gabor Horvath

PERMUTATION POLYNOMIALS OVER FINITE RINGS

DALMA GÖRCSÖS, GÁBOR HORVÁTH, AND ANETT MÉSZÁROS

ABSTRACT. Let $\text{PPol}(R)$ denote the group of permutation polynomials over the finite, commutative, unital ring R under composition. We generalize numerous results about permutation polynomials over $\mathbb{Z}_{p^n}$ to local rings by treating them under a unified manner. In particular, we provide a natural wreath product decomposition of permutation polynomials over the maximal ideal M and over the finite field R/M . Further, we give a necessary and sufficient condition for a polynomial $f \in R[x]$ to be a permutation polynomial considering f and f' over the finite field R/M , thereby generalizing a similar result for $\mathbb{Z}_{p^n}$. We characterize the group of permutation polynomials over M whenever the condition $M^{|R/M|} = \{0\}$ applies by describing a polynomial being identically equal to 0 with the help of the annihilators of the ideals $M_k = (r^k \mid r \in M)$. We derive the size of $\text{PPol}(R)$, thereby generalizing the same number formulas for $\mathbb{Z}_{p^n}$. Finally, we completely characterize when the group $\text{PPol}(R)$ is solvable, nilpotent, or abelian.

1. INTRODUCTION

Let R be a finite, commutative, unital ring. A polynomial $f \in R[x]$ is called a *permutation polynomial* if the function induced by f permutes the elements of R . The permutation polynomials form a group under composition. We denote this group by $\text{PPol}(R)$.

Permutation polynomials have several applications when R is a finite field, mostly in cryptography and coding theory (see e.g. [5, 7, 8, 10, 15], and for most recent results see e.g. [12, Chapter VIII]). However, the picture is much less clear when it comes to arbitrary commutative rings. There are few existing results, mostly when the ring is a residue class ring of the integers.

Let f be a polynomial with integer coefficients, $f(x) = a_d x^d + \dots + a_1 x + a_0$. Rivest [14] proved that f is a permutation polynomial modulo 2^n if and only if a_1 is odd, and $(a_2 + a_4 + \dots)$ is even and $(a_3 + a_5 + \dots)$ is even, as well. This is a special case of a more general result [6, Theorem 123]: the polynomial f is a permutation polynomial modulo

Date: 23 March, 2017.

2010 Mathematics Subject Classification. 13M10, 11T06.

Key words and phrases. permutation polynomials; local rings; group of permutation polynomials.

Corresponding author: Gábor Horváth, ghorvath@science.unideb.hu

p^n for some prime p if and only if it permutes the elements of the finite field $\mathbb{F}_p$, and if $f'(x) = 0$ has no solutions in $\mathbb{F}_p$. Singh and Maity [16] used this characterization to obtain conditions modulo 3^n and 5^n , similar to those gave by Rivest for modulo 2^n .

Mullen and Stevens [11] applied these characterizations to compute the number of permutation polynomials over the residue class ring $\mathbb{Z}_{p^n}$. Let $\nu(s)$ be the largest positive integer for which $p^{\nu(s)} \mid s!$. That is, $\nu(s) = \sum_{r=1}^{\infty} \lfloor \frac{s}{p^r} \rfloor$. Let N be the biggest positive integer for which $\nu(N) < n$. Then

$$|\text{PPol}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{-2p} \prod_{j=0}^N p^{n-\nu(j)}.$$

Further, for $\delta(N) = \frac{1}{2} \sum_{r=1}^{\infty} p^r \lfloor \frac{N}{p^r} \rfloor (\lfloor \frac{N}{p^r} \rfloor + 1)$ one has

$$|\text{PPol}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{(N+1)(n-\nu(N))+\delta(N)-2p}.$$

Some of these formulas have been generalized. Frisch [3] considered „suitable” finite, commutative, unital, local rings, and computed the number of permutation polynomials for such rings.

Determining the structure of $\text{PPol}(R)$ would be a natural step after computing its size. However, by looking at the number formulas above, one cannot hope to obtain very nice descriptions in the general case. Indeed, even to enumerate and describe the p -Sylow subgroups of $\text{PPol}(\mathbb{Z}_{p^n})$ took considerable effort by Frisch and Krenn [4]. There exist some results on the structure, though. Frisch [3] characterized $\text{PPol}(R)$ as a wreath product when R is a finite, commutative, unital, local ring with maximal ideal of nilpotency class 2. There is another wreath product characterization by Nöbauer [13] for the residue class rings $\mathbb{Z}_{p^n}$.

The aim of this paper is to generalize most of these results by treating them in a unified manner. Every finite, commutative, unital ring is a direct sum of local rings [9, VI.2, p. 95], and the group of permutation polynomials of a direct sum is the direct product of the groups of permutation polynomials of the summands (Lemma 2.2). As a consequence, one only needs to consider local rings to understand how permutation polynomials behave over an arbitrary finite, commutative, unital ring. Surprisingly, however, we have not found a short proof for the latter fact in the literature. Thus we provided a short and elementary proof in Section 2.2.

Let R be a finite, commutative, unital ring, and I be a nontrivial ideal of R . Let $\text{PPol}_R(I)$ denote the restrictions of those polynomials onto I whose restriction permutes the elements of I . We prove in Section 2.3 that $\text{PPol}(R)$ is isomorphic to a subgroup of $\text{PPol}_R(I) \wr \text{PPol}(R/I)$ (see Lemma 2.4). Here $\wr$ denotes the wreath product of two permutation groups. Further, we prove in Theorem 1.1 that if R is local, and I is

its unique maximal ideal, then $\text{PPol}(R)$ is in fact isomorphic to the wreath product:

Theorem 1.1. *Let R be a finite, commutative, unital, local ring with maximal ideal M . Then*

$$\text{PPol}(R) \simeq \text{PPol}_R(M) \wr \text{PPol}(R/M).$$

This generalizes both Frisch's [3] and Nöbauer's [13] characterization by wreath products. Frisch in an email correspondence pointed out that this fact is somewhat folklore, and was probably already known by Nöbauer. Nevertheless, it cannot be found anywhere in the literature in such a general form. Therefore, we decided to include the proof of this characterization in the preliminaries section (see Section 2.3).

From the wreath product decomposition, one needs to understand $\text{PPol}_R(I)$ to have a better grasp on $\text{PPol}(R)$. In Lemma 3.2 we completely characterize when a polynomial of $R[x]$ permutes the elements of the ideal I . Together with Theorem 1.1, one immediately arrives at a complete characterization of a polynomial being a permutation polynomial:

Theorem 1.2. *Let R be a finite, commutative, unital, local ring with maximal ideal M . Assume $M \neq \{0\}$, and $|R/M| = q$. Then a polynomial $f \in R[x]$ is a permutation polynomial over R if and only if f is a permutation polynomial over the field $\mathbb{F}_q$ and f' has no roots in $\mathbb{F}_q$.*

Theorem 1.2 generalizes the similar result for $\mathbb{Z}_{p^n}$, and has several immediate consequences. For one, a polynomial is a permutation polynomial if and only if it is a permutation polynomial modulo M^2 . Further, one can obtain a generalization of Rivest's result [14]:

Corollary 1.3. *Let R be a finite, commutative, unital, local ring with maximal ideal M such that $R/M \simeq \mathbb{F}_2$. Let $f \in R[x]$, $f(x) = a_d x^d + \dots + a_1 x + a_0$. Then f is a permutation polynomial if and only if $a_1 = 1$ in $\mathbb{F}_2$, $(a_2 + a_4 + \dots) = 0$ in $\mathbb{F}_2$ and $(a_3 + a_5 + \dots) = 0$ in $\mathbb{F}_2$.*

The proofs of Theorem 1.2 and Corollary 1.3 are in Section 3. Then we continue Section 3 by characterizing $\text{PPol}_R(M)$ for a local ring R with maximal ideal M by understanding when two polynomials induce the same function over M . Let $M_k = (r^k \mid r \in M)$. Using the annihilators of M_k we are able to characterize when a polynomial is identically 0 on M if $M^{|R/M|} = \{0\}$ holds. Further, we obtain a generalization of the number formulas from [11], and even from [3] whenever our condition applies:

Theorem 1.4. *Let R be a finite, commutative, unital, local ring with maximal ideal M . Let t be the smallest positive integer for which $M^t = \{0\}$, and let us assume $t \geq 2$. Finally, let $q = |R/M|$, and let p denote the characteristic of R/M . Then $\text{PPol}_R(M) = \{a_{t-1}x^{t-1} + \dots + a_1x + a_0 \mid a_0 \in M, a_1 \in R \setminus M\}$, and if $q \geq t$ holds, then*

$f(x) = a_{t-1}x^{t-1} + \cdots + a_1x + a_0$ is identically 0 on M if and only if $a_k \in \text{Ann } M_k$ for every $k = 0, 1, \dots, t-1$. Then

$$|\text{PPol}(R)| = q! \cdot \left(\frac{(q-1) \cdot |R|^{t-1}}{q \cdot \prod_{k=1}^{t-2} |\text{Ann } M_k|} \right)^q.$$

Further, if $p \geq t$ holds, then $M_k = M^k$ for every $k = 0, 1, \dots, t-1$.

Finally, another natural question is what finite groups can be represented as permutation polynomials of finite, commutative, unital rings. In Section 4 we make a step in this direction. With the help of the wreath product decomposition (Lemma 2.4) we completely characterize when $\text{PPol}(R)$ is solvable, nilpotent, or abelian.

Theorem 1.5. *Let R be a finite, commutative, unital, local ring with maximal ideal M . Let $q = |R/M|$. Then the size of $\text{PPol}(R)$ is even, and*

- (1) $\text{PPol}(R)$ is solvable if and only if $q \leq 4$,
- (2) $\text{PPol}(R)$ is nilpotent if and only if $q = 2$
(in which case $\text{PPol}(R)$ is a 2-group),
- (3) $\text{PPol}(R)$ is abelian if and only if $R \simeq \mathbb{F}_2$.

2. PRELIMINARIES

Let R be a finite, commutative, unital ring. A polynomial is a *permutation polynomial* over R if and only if the function it determines is permuting the elements of R , that is if it is bijective over R . Note, that a function over a finite set is bijective if and only if it is surjective if and only if it is injective. Therefore to find out whether or not a polynomial is a permutation polynomial, it is enough to check whether the function is surjective or injective. In the following let $\text{PPol}(R)$ be the group of permutation polynomials over R . Let I be an ideal of R , and let $\text{PPol}_R(I)$ denote the restrictions of $R \rightarrow R$ polynomials onto I whenever this restriction is a permutation over I :

$$(1) \quad \text{PPol}_R(I) = \{ f \upharpoonright_I : f \in R[x], f \upharpoonright_I \text{ is a permutation on } I \}.$$

Further, let $\text{Ann } I$ denote the annihilator of I , that is

$$\text{Ann } I = \{ r \in R : rs = 0 \text{ for all } s \in I \}.$$

2.1. Local rings. We summarise the most important properties of local rings (see e.g. [9, Chapter V]). A ring R is local if and only if it has a unique maximal ideal M . For a commutative, unital, local ring R the factor R/M is field, and $R \setminus M$ is the set of invertible elements of R .

Lemma 2.1. *Let R be a finite, commutative, unital, local ring with maximal ideal M . If $|R/M| = q$, then the size of M is a q -power.*

Proof. Now M^i/M^{i+1} is a vector space over R/M , let its dimension over R/M be n_i . Thus for every i we have $|M^i/M^{i+1}| = q^{n_i}$. Let t be the smallest positive integer for which $M^t = \{0\}$. Then

$$|M| = |M/M^2| \cdot |M^2/M^3| \cdot \dots \cdot |M^{t-1}/M^t| = q^{n_1} \cdot q^{n_2} \cdot \dots \cdot q^{n_{t-1}}.$$

□

2.2. Direct products. Every finite, commutative, unital ring is a direct sum of local rings [9, VI.2, p. 95]. We show that the group of permutation polynomials of a direct sum of two rings is isomorphic to the direct product of the group of permutation polynomials of the two direct summands. Therefore, to understand the group of permutation polynomials for finite, commutative, unital rings it is enough to investigate the group of permutation polynomials over finite, commutative, unital, *local* rings.

Lemma 2.2. *Let A, B be finite, commutative, unital rings. Then*

$$\text{PPol}(A \oplus B) \simeq \text{PPol}(A) \times \text{PPol}(B).$$

Proof. We define homomorphisms

$$\varphi: \text{PPol}(A \oplus B) \rightarrow \text{PPol}(A) \times \text{PPol}(B),$$

$$\psi: \text{PPol}(A) \times \text{PPol}(B) \rightarrow \text{PPol}(A \oplus B),$$

and prove that they are inverses of each other.

Let $f \in \text{PPol}(A \oplus B)$, $f(x) = \sum_{k=0}^m c_k x^k$. Now, every $c_k \in A \oplus B$ can be uniquely written as $c_k = a_k + b_k$, where $a_k \in A, b_k \in B$. Let $f \restriction_A(x) = \sum_{k=0}^m a_k x^k$, and $f \restriction_B(x) = \sum_{k=0}^m b_k x^k$. We show that $f \restriction_A$ is a permutation polynomial over A , $f \restriction_B$ is a permutation polynomial over B . For that we prove $f \restriction_A: A \rightarrow A$ injective. Suppose that for some $a, a' \in A$ we have $f \restriction_A(a) = f \restriction_A(a')$. Further, from $AB \subset A \cap B = \{0\}$ we have $f \restriction_B(a) = b_0$ and $f \restriction_B(a') = b_0$. Then

$$f(a) = f \restriction_A(a) + f \restriction_B(a) = f \restriction_A(a) + b_0,$$

$$f(a') = f \restriction_A(a') + f \restriction_B(a') = f \restriction_A(a') + b_0.$$

Thus $f(a) = f(a')$. Since f is injective, we obtain $a = a'$. One can prove that $f \restriction_B: B \rightarrow B$ is injective in a similar manner. Let

$$(2) \quad \begin{aligned} \varphi: \text{PPol}(A \oplus B) &\rightarrow \text{PPol}(A) \times \text{PPol}(B), \\ f &\mapsto (f \restriction_A, f \restriction_B). \end{aligned}$$

Now we prove that φ is a homomorphism by showing that the action of f on $A \oplus B$ is the same as the action of $(f \restriction_A, f \restriction_B)$ on $A \times B$:

$$\begin{aligned} f(a+b) &= (f \restriction_A + f \restriction_B)(a+b) = f \restriction_A(a+b) + f \restriction_B(a+b) = \\ &= \sum_{k=0}^m a_k(a+b)^k + \sum_{k=0}^m b_k(a+b)^k. \end{aligned}$$

Again, $AB \subset A \cap B = \{0\}$, thus if we multiply an element from A by one from B , then the product is 0. Hence

$$f(a+b) = \sum_{k=0}^m a_k a^k + \sum_{k=0}^m b_k b^k = f \restriction_A (a) + f \restriction_B (b),$$

and φ is a homomorphism.

For the other direction let $g \in \text{PPol}(A), h \in \text{PPol}(B)$. Let m be the maximum of the degrees of $g(x)$ and $h(x)$. Let $g(x) = \sum_{k=0}^m a_k x^k$, and $h(x) = \sum_{k=0}^m b_k x^k$, where $a_k \in A, b_k \in B$. Consider the sum $f = g + h$. We show that f is a permutation polynomial over $A \oplus B$ by proving that it is injective. Assume that for some $r_1, r_2 \in A \oplus B$ we have $f(r_1) = f(r_2)$. Since $r_1, r_2 \in A \oplus B$, they can be written as $r_1 = a_1 + b_1, r_2 = a_2 + b_2$ for some $a_1, a_2 \in A, b_1, b_2 \in B$. Now,

$$\begin{aligned} f(r_1) &= f(a_1 + b_1) = g(a_1 + b_1) + h(a_1 + b_1) \\ &= \sum_{k=0}^m a_k (a_1 + b_1)^k + \sum_{k=0}^m b_k (a_1 + b_1)^k = \sum_{k=0}^m a_k a_1^k + \sum_{k=0}^m b_k b_1^k \\ &= g(a_1) + h(b_1). \end{aligned}$$

Again, we made use of the fact $AB \subset A \cap B = \{0\}$. Similarly,

$$f(r_2) = g(a_2) + h(b_2).$$

From $f(r_1) = f(r_2)$ we obtain

$$g(a_1) - g(a_2) = h(b_2) - h(b_1),$$

where the left-hand side is an element of A , the right-hand side is an element of B , $A \cap B = \{0\}$, thus

$$g(a_1) = g(a_2), \quad h(b_1) = h(b_2).$$

Now, g and h are injective, hence $a_1 = a_2, b_1 = b_2$, and thus $r_1 = r_2$. Therefore $f = g + h \in \text{PPol}(A \oplus B)$. Let

$$(3) \quad \begin{aligned} \psi : \text{PPol}(A) \times \text{PPol}(B) &\rightarrow \text{PPol}(A \oplus B), \\ (g, h) &\mapsto g + h. \end{aligned}$$

Finally, we show that φ and ψ (defined by (2) and (3)) are inverses of each other. For this we show that $\varphi \circ \psi = id_{\text{PPol}(A) \times \text{PPol}(B)}$ and $\psi \circ \varphi = id_{\text{PPol}(A \oplus B)}$. Let $(g, h) \in \text{PPol}(A) \times \text{PPol}(B)$ be arbitrary, then

$$\varphi \circ \psi(g, h) = \varphi(g + h) = ((g + h) \restriction_A, (g + h) \restriction_B) = (g, h),$$

and $\varphi \circ \psi = id_{\text{PPol}(A) \times \text{PPol}(B)}$. Now, let $f \in \text{PPol}(A \oplus B)$ be arbitrary, then

$$\psi \circ \varphi(f) = \psi(f \restriction_A, f \restriction_B) = f \restriction_A + f \restriction_B = f,$$

and $\psi \circ \varphi = id_{\text{PPol}(A \oplus B)}$. Thus φ and ψ are indeed inverses of each other. In particular, $\varphi : \text{PPol}(A \oplus B) \rightarrow \text{PPol}(A) \times \text{PPol}(B)$ is an isomorphism. $\square$

2.3. Wreath product. Based on [2] we recall the definition of wreath products of permutation groups. Let I and T be two sets, where $T = \{0, \dots, |T| - 1\}$. Let G_I be a permutation group acting on I , and G_T be a permutation group acting on T . Let $G_I^{|T|}$ denote the $|T|$ -fold direct product of G_I , where the coordinates are indexed by $0, \dots, |T| - 1$. That is, the elements of $G_I^{|T|}$ are tuples $(g_0, \dots, g_{|T|-1})$, where $g_\delta \in G_I$ ($\delta \in T$). Now, the wreath product of G_I and G_T is

$$G_I \wr G_T = G_I^{|T|} \rtimes G_T,$$

where the conjugation action of G_T permutes the coordinates of $G_I^{|T|}$. Further, $G_I \wr G_T$ acts on $I \times T$ as

$$(g_0, \dots, g_{|T|-1}, h)(\gamma, \delta) = (g_\delta(\gamma), h(\delta))$$

for every $g_0, \dots, g_{|T|-1} \in G_I, h \in G_T, \gamma \in I, \delta \in T$. Note, that the wreath product of two permutation groups is solvable if and only if both permutation groups are solvable.

Notation 2.3. Let R be a finite, commutative, unital ring, let I be an ideal of R , furthermore let T be any representation system of R/I . Let us identify the elements of T and R/I . Then any $r \in R$ can be uniquely written as $r = \gamma + \delta$, where $\gamma \in I, \delta \in T$. Let us identify the elements of R and $I \times T$, such that $(\gamma, \delta) \in I \times T$ corresponds to $\gamma + \delta \in R$.

Let $\text{PPol}_R(I)$ be defined as in (1), and consider the wreath product $\text{PPol}_R(I) \wr \text{PPol}(R/I)$. Its elements are tuples $(g_0, g_1, \dots, g_{|T|-1}, h)$, where $g_\delta \in \text{PPol}_R(I)$ and $h \in \text{PPol}(R/I)$. Now $\text{PPol}_R(I)$ acts on I , and $\text{PPol}(R/I)$ acts on R/I . However, due to the identification of T and R/I , we can consider the action of $\text{PPol}(R/I)$ on T . Thus, the wreath product $\text{PPol}_R(I) \wr \text{PPol}(R/I)$ acts on R (identified by $I \times T$) as

$$(g_0, g_1, \dots, g_{|T|-1}, h)(\gamma, \delta) = (g_\delta(\gamma), h(\delta)).$$

Lemma 2.4. *With R and I being as in Notation 2.3, we have*

$$\text{PPol}(R) \leq \text{PPol}_R(I) \wr \text{PPol}(R/I).$$

Proof. For every $f \in \text{PPol}(R)$ we assign $(g_0, g_1, \dots, g_{|T|-1}, h)$ from $\text{PPol}_R(I) \wr \text{PPol}(R/I)$ such that their actions on R are the same. That is, for every $\gamma \in I, \delta \in T$ we have $f(\gamma + \delta) = (g_0, g_1, \dots, g_{|T|-1}, h)(\gamma, \delta)$.

First, we define h . Since f is a polynomial over R , it can be considered as a polynomial over R/I , as well. Let h be the polynomial f over R/I . By the identification of T and R/I , we can consider h as a function $T \rightarrow T$. We prove that h permutes the elements of T . Indeed, if h were not surjective on T , then for some $t \in T \setminus h(T)$ the permutation f would not map into the coset of t . Thus $h \in \text{PPol}(R/I)$.

Next, we define g_δ ($\delta \in T$). Fix $\delta \in T$, and let $g_\delta: I \rightarrow R$ be defined by $g_\delta(\gamma) = f(\gamma + \delta) - h(\delta)$ for $\gamma \in I$. Then g_δ is a polynomial function over R , and

$$h(\delta) \equiv f(\delta) \equiv f(\gamma + \delta) \pmod{I}.$$

Hence $g_\delta(\gamma) = f(\gamma + \delta) - h(\delta) \equiv 0 \pmod{I}$, thus $g_\delta: I \rightarrow I$.

Now, we show that g_δ is injective. Suppose that $g_\delta(\gamma_1) = g_\delta(\gamma_2)$ for some $\gamma_1, \gamma_2 \in I$. Then from the definition of $g_\delta(\gamma)$ we obtain $f(\gamma_1 + \delta) = f(\gamma_2 + \delta)$, and the injectivity of f yields $\gamma_1 = \gamma_2$. Thus $g_\delta \in \text{PPol}_R(I)$.

Finally, we prove that the action of f is the same as the action of the tuple $(g_0, g_1, \dots, g_{|T|-1}, h)$. Indeed,

$$\begin{aligned} (g_0, g_1, \dots, g_{|T|-1}, h)(\gamma, \delta) &= \\ &= (g_\delta(\gamma), h(\delta)) = g_\delta(\gamma) + h(\delta) = \\ &= f(\gamma + \delta) - h(\delta) + h(\delta) = f(\gamma + \delta). \end{aligned}$$

□

Theorem 1.1 states that Lemma 2.4 holds with equality if R is local and I is its maximal ideal. Now, we prove Theorem 1.1.

Proof of Theorem 1.1. Let us use the identifications of Notation 2.3. By Lemma 2.4 we have $\text{PPol}(R) \leq \text{PPol}_R(M) \wr \text{PPol}(R/M)$. We show that equality holds. For this we need to prove that the action of every tuple $(g_0, g_1, \dots, g_{|T|-1}, h) \in \text{PPol}_R(M) \wr \text{PPol}(R/M)$ is an action of a polynomial function. Let $\exp R^\times$ denote the exponent of the multiplicative group of R . That is, $\exp R^\times$ is the least positive integer k for which $r^k = 1$ holds for every $r \in R^\times$. Recall that $R^\times = R \setminus M$. Further, let

$$u(x) = \left(\prod_{r \in R \setminus M} (x - r) \right)^{\exp R^\times}.$$

Let $s \in R$ be arbitrary. If $s \in R \setminus M$ then one of the factors in the product is 0 yielding $u(s) = 0$. If $s \in M$, then for every $r \in R \setminus M$ we have $(s - r) \in R \setminus M = R^\times$. Therefore, $\prod_{r \in R \setminus M} (s - r) \in R^\times$ yielding

$$\left(\prod_{r \in R \setminus M} (s - r) \right)^{\exp R^\times} = 1. \text{ That is,}$$

$$u(s) = \begin{cases} 1, & \text{if } s \in M, \\ 0, & \text{if } s \notin M. \end{cases}$$

Let

$$f(x) = \sum_{\delta \in T} ((g_\delta(x - \delta)) + h(\delta)) \cdot u(x - \delta).$$

Now, $f(x)$ is a polynomial, since $g_\delta(x)$ and $u(x)$ are polynomials, and $h(\delta)$ is a constant for every δ . Finally, we prove that f acts on R the

same way as $(g_0, g_1, \dots, g_{|T|-1}, h)$ acts on $M \times T$. For $\gamma \in M, \delta \in T$ we have

$$f(\gamma + \delta) = \sum_{\delta' \in T} ((g_{\delta'}((\gamma + \delta) - \delta')) + h(\delta')) \cdot u((\gamma + \delta) - \delta').$$

Now $u((\gamma + \delta) - \delta') = 1$ if $\delta = \delta'$, and $u((\gamma + \delta) - \delta') = 0$ if $\delta \neq \delta'$. Therefore,

$$\begin{aligned} f(\gamma + \delta) &= (g_\delta(\gamma + \delta - \delta) + h(\delta)) \cdot u(\gamma + \delta - \delta) \\ &= (g_\delta(\gamma) + h(\delta)) \cdot u(\gamma) = g_\delta(\gamma) + h(\delta). \end{aligned}$$

By the identification of R and $M \times T$ we have $g_\delta(\gamma) + h(\delta) = (g_\delta(\gamma), h(\delta))$. Thus,

$$f(\gamma + \delta) = (g_\delta(\gamma), h(\delta)) = (g_0, g_1, \dots, g_{|T|-1}, h)(\gamma, \delta).$$

□

3. PERMUTATION POLYNOMIALS WHEN $M^t = \{0\}$

Notation 3.1. Throughout this section R denotes a finite, commutative, unital, local ring with maximal ideal M . Let t be the smallest positive integer for which $M^t = \{0\}$, and let us assume $t \geq 2$. Finally, let $q = |R/M|$, and let p denote the characteristic of R/M .

By Theorem 1.1 one needs to investigate $\text{PPol}(R/M)$ and $\text{PPol}_R(M)$ in order to understand $\text{PPol}(R)$. Since R/M is a finite field, we have $\text{PPol}(R/M) \simeq S_{|R/M|}$. We continue by describing $\text{PPol}_R(I)$ for an arbitrary ideal I .

Lemma 3.2. *Let $I \triangleleft R$, $I \neq \{0\}$. Then*

$$a_n x^n + \dots + a_1 x + a_0 \in \text{PPol}_R(I) \iff a_0 \in I, a_1 \in R \setminus M.$$

(Note, that the condition on a_1 is on the maximal ideal, and not on I .)

Proof. Let $f \in R[x]$ be a polynomial such that $f|_I$ is a permutation over I . Let $f(x) = a_n x^n + \dots + a_1 x + a_0$. Substituting $x = 0$ we obtain $f(0) = a_0 \in I$. Note, that $f(x)$ is a permutation polynomial on I if and only if $f(x) - a_0$ is a permutation polynomial on I . Thus, from now on we assume $a_0 = 0$, and we show $a_1 \in R \setminus M$.

Suppose to the contrary that $a_1 \in M$. Recall, that t is the smallest positive integer for which $M^t = \{0\}$, thus $I \subseteq M$ yields $I^t = \{0\}$, as well. Let g be the t -fold iteration of f with itself, that is $g = f \circ f \circ \dots \circ f$. Now, g is a permutation polynomial over I . Let $g(x) = b_{t-1} x^{t-1} + \dots + b_2 x^2 + b_1 x$ for some $b_0, b_1, \dots, b_{t-1} \in R$. (We can cut g at degree $(t-1)$ due to $I^t = \{0\}$.) Here, $b_1 = a_1^t$, yielding $b_1 = 0$ if $a_1 \in M$. Hence, $g(x) = b_{t-1} x^{t-1} + \dots + b_2 x^2$.

Iterate g with itself t times. Then we obtain a (permutation) polynomial whose lowest degree term corresponds to x^{2^t} . Since $t < 2^t$ and

$x^t = 0$ for $x \in I$, the obtained polynomial is identically zero over I . Consequently, a power of f maps every element of I to 0, while it should permute the elements of I . This contradiction implies that $a_1 \notin M$.

Finally, we show that $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$, where $a_0 \in I$, $a_1 \in R \setminus M$, is a permutation polynomial on I . It suffices to show that f is injective on I . Assume that for some $u, v \in I$ we have $f(u) = f(v)$. Now,

$$\begin{aligned} f(u) &= a_n u^n + \cdots + a_2 u^2 + a_1 u + a_0, \\ f(v) &= a_n v^n + \cdots + a_2 v^2 + a_0 v + a_0, \end{aligned}$$

and

$$f(u) - f(v) = (u - v)(a_1 + a_2(u + v) + \cdots + a_n(u^{n-1} + u^{n-2}v + \cdots + v^{n-1})).$$

Here, the second factor is in the coset $(a_1 + M)$, hence invertible by $a_1 \notin M$. Therefore, $f(u) = f(v)$ yields $u = v$. Thus $f \in \text{PPol}_R(I)$. Therefore, $\text{PPol}_R(I) = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_0 \in I, a_1 \in R \setminus M\}$. $\square$

An immediate corollary is Theorem 1.2 and Corollary 1.3:

Proof of Theorem 1.2. Let $S = \{s_1, \dots, s_q\}$ be an arbitrary representation system for R/M . By the proof of Theorem 1.1 a polynomial $f \in R[x]$ is a permutation polynomial over R if and only if f is a permutation polynomial over $R/M \simeq \mathbb{F}_q$, and for every $s \in S$ we have $f(x + s) - f(s) \in \text{PPol}_R(M)$. By Lemma 3.2 the latter is equivalent to the linear term of $f(x + s)$ being in $R \setminus M$. Let $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$, then the linear term of $f(x + s)$ is

$$(na_n s^{n-1} + \cdots + 2a_2 s + a_1)x = f'(s)x.$$

Since $S = \{s_1, \dots, s_q\}$ is a representation system for $R/M \simeq \mathbb{F}_q$, the linear term of $f(x + s)$ is in $R \setminus M$ for every $s \in S$ if and only if $f'(s) \neq 0$ for every $s \in \mathbb{F}_q$. $\square$

Proof of Corollary 1.3. Let $f \in R[x]$, $f(x) = a_d x^d + \cdots + a_1 x + a_0$. Now, by Theorem 1.2 the polynomial f permutes the elements of R if and only if f is a permutation polynomial over $R/M \simeq \mathbb{F}_2$, and f' has no roots in $\mathbb{F}_2$. The former is equivalent to $(a_1 + a_2 + a_3 + \cdots) = 1$ in $\mathbb{F}_2$. The second is equivalent to $f'(0) = 1$ in $\mathbb{F}_2$ and $f'(1) = 1$ in $\mathbb{F}_2$, that is $a_1 = 1$ in $\mathbb{F}_2$ and $(a_1 + a_3 + \cdots) = 1$ in $\mathbb{F}_2$. Putting these three conditions together finishes the proof of Corollary 1.3. $\square$

We continue investigating the structure of $\text{PPol}_R(I)$.

Lemma 3.3. *Let $I \triangleleft R$, $I \neq \{0\}$. If $I^2 = \{0\}$, then*

$$\text{PPol}_R(I) = \{a_1 x + a_0 \mid a_0 \in I, a_1 \in R \setminus M\} \simeq (I, +) \rtimes (R/\text{Ann } I)^\times.$$

Proof. From Lemma 3.2 we have that $a_n x^n + \cdots + a_1 x + a_0$ is a permutation polynomial over I if and only if $a_0 \in I$, $a_1 \in R \setminus M$. Now,

$I^2 = \{0\}$ implies that we can cut every polynomial at degree 1. Therefore, $\text{PPol}_R(I) = \{a_1x + a_0 \mid a_0 \in I, a_1 \in R \setminus M\}$.

Now, we determine when two linear polynomials define the same function over I . Let $f(x) = a_1x + a_0$, $g(x) = b_1x + b_0$, and assume $f(s) = g(s)$ for all $s \in I$. Substituting $x = 0$ implies $a_0 = b_0$. Therefore, $a_1s = b_1s$ for all $s \in I$, yielding $(a_1 - b_1)s = 0$, which holds for all $s \in I$ if and only if $a_1 - b_1 \in \text{Ann } I$.

Finally, $R/\text{Ann } I$ is a local ring with maximal ideal $M/\text{Ann } I$, thus $(R/\text{Ann } I)^\times = (R/\text{Ann } I) \setminus (M/\text{Ann } I)$. Putting all these together we have $\text{PPol}(R) \simeq (I, +) \rtimes (R/\text{Ann } I)^\times$. $\square$

We obtain one of Frisch's results [3] as an immediate consequence.

Corollary 3.4. *Let R be a finite, commutative, unital, local ring with maximal ideal M , and assume $M^2 = \{0\}$. Then*

$$\text{PPol}(R) \simeq ((M, +) \rtimes (R/M)^\times) \wr S_{|R/M|}.$$

Proof. Theorem 1.1 and Lemma 3.3 proves the corollary provided $M = \text{Ann } M$ holds. Since M is the unique maximal ideal, we have $\text{Ann } M \subseteq M$. Further, $M^2 = \{0\}$ implies $M \subseteq \text{Ann } M$. $\square$

The ideas of Lemma 3.3 can be further generalized under certain conditions.

Notation 3.5. Let R be a unital ring, $I \triangleleft R$. Let $I_k = (r^k \mid r \in I)$ ($k \geq 0$) be the ideal generated by all k -powers. Note $I_0 = R$, $I_1 = I$.

Theorem 3.6. *Let R , M , t , q and M_k be defined as in Notations 3.1 and 3.5. Assume $q \geq t$. Then $f(x) = a_nx^n + \dots + a_1x + a_0$ ($a_k \in R$) is identically zero on M if and only if $a_k \in \text{Ann } M_k$ for all $k = 0, \dots, t-1$.*

Proof. Note first, that we may assume $a_t = \dots = a_n = 0$, since $x^t = 0$ for every $x \in M$. Substituting $x = 0$ yields $f(0) = a_0 = 0$. Thus $a_0 \in \{0\} = \text{Ann } R = \text{Ann } M_0$. Let $r \in R \setminus M$ be arbitrary. If $x \in M$, then $rx \in M$, thus the polynomial $f(rx)$ is identically zero for every $x \in M$. Thus $f(rx) = a_{t-1}r^{t-1}x^{t-1} + \dots + a_2r^2x^2 + a_1rx = 0$ for all $x \in M$. Let us write this in the following way:

$$(4) \quad \begin{pmatrix} r & r^2 & \dots & r^{t-1} \end{pmatrix} \cdot \begin{pmatrix} a_1x \\ a_2x^2 \\ \vdots \\ a_{t-1}x^{t-1} \end{pmatrix} = 0.$$

Since $q \geq t$ there exists invertible elements $r_1, \dots, r_{t-1}$ from different cosets of M . From (4) we have

$$(5) \quad \begin{pmatrix} r_1 & r_1^2 & \dots & r_1^{t-1} \\ r_2 & r_2^2 & \dots & r_2^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{t-1} & r_{t-1}^2 & \dots & r_{t-1}^{t-1} \end{pmatrix} \cdot \begin{pmatrix} a_1x \\ a_2x^2 \\ \vdots \\ a_{t-1}x^{t-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

That is, the vector $(a_1x \ a_2x^2 \ \dots \ a_{t-1}x^{t-1})^T$ is multiplied by a Vandermonde-matrix. Let D be the determinant of this Vandermonde-matrix. Then

$$D = r_1 r_2 \dots r_{t-1} \cdot \prod_{1 \leq i < j \leq t-1} (r_i - r_j).$$

Now, every r_i ($1 \leq i \leq t-1$) is invertible, and every $(r_i - r_j)$ ($1 \leq i < j \leq t-1$) is invertible because r_i and r_j are from different cosets of M . Thus, D is invertible. Therefore, the zero vector is the unique solution of the homogeneous system of linear equations (5), and we have

$$\begin{pmatrix} a_1x \\ a_2x^2 \\ \vdots \\ a_{t-1}x^{t-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Thus $a_k x^k = 0$ for all $x \in M$ ($k = 1, 2, \dots, t-1$). Hence $a_k \in \text{Ann } M_k$ ($k = 0, 1, \dots, t-1$). $\square$

Corollary 3.7. *Let R , M , t , q and M_k be defined as in Notations 3.1 and 3.5. Assume $q \geq t \geq 2$. Then*

$$|\text{PPol}_R(M)| = \frac{(q-1) \cdot |R|^{t-1}}{q \cdot \prod_{k=1}^{t-2} |\text{Ann } M_k|}.$$

Proof. By Lemma 3.2 $f(x) = a_n x^n + \dots + a_1 x + a_0$ is a permutation polynomial over M if and only if $a_0 \in M$, $a_1 \in R \setminus M$. By Theorem 3.6 f is identically zero if and only if $a_k \in \text{Ann } M_k$. Thus, to obtain different polynomials from $\text{PPol}_R(M)$, one can choose a_0 in $|M|$ -many ways, a_1 in $\frac{|R^\times|}{|\text{Ann } M_1|}$ -many ways, and a_k in $\frac{|R|}{|\text{Ann } M_k|}$ -many ways ($2 \leq k \leq t-1$). Finally, note that $\text{Ann } M_{t-1} = M$. Thus, we have

$$\begin{aligned} |\text{PPol}_R(M)| &= |M| \cdot \frac{|R^\times|}{|\text{Ann } M_1|} \cdot \left(\prod_{k=2}^{t-2} \frac{|R|}{|\text{Ann } M_k|} \right) \cdot \frac{|R|}{|\text{Ann } M_{t-1}|} = \\ &= |M| \cdot \frac{|R^\times|}{|\text{Ann } M_1|} \cdot \left(\prod_{k=2}^{t-2} \frac{|R|}{|\text{Ann } M_k|} \right) \cdot \frac{|R|}{|M|} = \\ &= \frac{|R^\times|}{|\text{Ann } M_1|} \cdot |R|^{t-2} \cdot \prod_{k=2}^{t-2} \frac{1}{|\text{Ann } M_k|} = \frac{(q-1) \cdot |R|^{t-1}}{q \cdot \prod_{k=1}^{t-2} |\text{Ann } M_k|}. \end{aligned}$$

$\square$

By a result of Anderson, Knopp, and Lewin [1], if $k!$ is invertible, then the ideal M_k equals to the ideal power M^k :

Lemma 3.8 ([1, Theorem 5]). *Let R be a commutative ring with ideal I . If $k!$ is invertible in R , then $I_k = I^k$.*

Corollary 3.9. *Let R , M , t , q and p be defined as in Notation 3.1. Assume $p \geq t$. Then $f(x) = a_n x^n + \dots + a_1 x + a_0$ ($a_k \in R$) is identically zero on M if and only if $a_k \in \text{Ann } M^k$ for all $k = 0, 1, \dots, t-1$. Further,*

$$|\text{PPol}_R(M)| = \frac{(q-1) \cdot |R|^{t-1}}{q \cdot \prod_{k=1}^{t-2} |\text{Ann } M^k|}.$$

Proof. By Theorem 3.6 $f(x)$ is identically zero on M if and only if $a_k \in \text{Ann } M_k$ for every a_k . If $p \geq t > k$, then $k!$ is invertible in R . By Lemma 3.8 we obtain $M_k = M^k$ for all $k = 0, 1, \dots, t-1$. Corollary 3.7 proves the statement on $|\text{PPol}_R(M)|$. $\square$

Proof of Theorem 1.4. Almost everything is proved in Lemma 3.2, Theorem 3.6, and Corollaries 3.7 and 3.9. The only statement left to prove is about $|\text{PPol}(R)|$. By Theorem 1.1, $\text{PPol}(R) \simeq \text{PPol}_R(M) \wr S_q$, hence

$$|\text{PPol}(R)| = q! \cdot |\text{PPol}_R(M)|^q = q! \cdot \left(\frac{(q-1) \cdot |R|^{t-1}}{q \cdot \prod_{k=1}^{t-2} |\text{Ann } M_k|} \right)^q.$$

$\square$

4. SOLVABILITY, NILPOTENCY AND COMMUTATIVITY OF $\text{PPol}(R)$

We prove Theorem 1.5 in this section.

Proof of Theorem 1.5. Throughout this section R denotes a finite, commutative, unital, local ring with maximal ideal M . Let $q = |R/M|$. By Theorem 1.1 we have $\text{PPol}(R) \simeq \text{PPol}_R(M) \wr S_q$. Since the size of S_q is even, so must be the size of $\text{PPol}(R)$. For characterizing the solvability of $\text{PPol}(R)$, we need the following.

Lemma 4.1. *Let $I \triangleleft R$. If $I^2 = \{0\}$ then $\text{PPol}_R(I)$ is solvable.*

Proof. Now, $\text{PPol}_R(I) \simeq (I, +) \times (R/\text{Ann } I)^\times$ by Lemma 3.3. Since $(I, +)$ and $(R/\text{Ann } I)^\times$ are abelian, $\text{PPol}_R(I)$ is solvable. $\square$

First, we prove the statement about solvability. If $q > 4$, then S_q is not solvable. Thus, by Theorem 1.1 $\text{PPol}(R)$ is not solvable, either. Let t be the smallest positive integer for which $M^{2^t} = \{0\}$. We prove that $\text{PPol}(R)$ is solvable if $q \leq 4$ by induction on t .

If $t = 1$ then $M^2 = \{0\}$. By Theorem 1.1 we have $\text{PPol}(R) \simeq \text{PPol}_R(M) \wr S_q$. Now, $\text{PPol}_R(M)$ solvable by Lemma 4.1, S_q is solvable since $q \leq 4$. Thus $\text{PPol}(R)$ is solvable, as well.

Assume now, that the statement holds for $(t-1)$. That is, $\text{PPol}(R)$ is solvable if $M^{2^{t-1}} = \{0\}$, and let us assume $M^{2^t} = \{0\}$. Let $I = M^{2^{t-1}}$. Then $I^2 = M^{2^t} = \{0\}$. Now, $\text{PPol}(R) \leq \text{PPol}_R(I) \wr \text{PPol}(R/I)$ by Lemma 2.4. By Lemma 4.1 we obtain that $\text{PPol}_R(I)$ is solvable. By the induction hypothesis, $\text{PPol}(R/I)$ is solvable. Therefore, $\text{PPol}_R(I) \wr \text{PPol}(R/I)$ is solvable, yielding that $\text{PPol}(R)$ is solvable, as well.

Now, we prove the statement about nilpotency. By Theorem 1.1 the group S_q is isomorphic to a factor of $\text{PPol}(R)$. Hence if $\text{PPol}(R)$ is nilpotent, then so is S_q , implying $q = 2$. Again, let t be the smallest positive integer for which $M^{2^t} = \{0\}$. As with the case for solvability, we prove that $\text{PPol}(R)$ is a 2-group (and hence nilpotent) if $q = 2$ by induction on t .

If $t = 1$ then $M^2 = 0$. By Corollary 3.4 we have $\text{PPol}(R) \simeq ((M, +) \rtimes (R/M)^\times) \wr S_q$. Since $q = 2$, $|(R/M)^\times| = 1$. By Lemma 2.1 the size of $(M, +)$ is a power of $q = 2$. Thus the size of $\text{PPol}_R(M) \simeq (M, +) \rtimes (R/M)^\times$ is a power of 2. The size of S_q is 2. Hence $|\text{PPol}(R)| = |\text{PPol}_R(M)|^2 \cdot 2$ is a power of 2, as well.

Assume now, that the statement holds for $(t - 1)$. That is, $\text{PPol}(R)$ is a 2-group if $M^{2^{t-1}} = \{0\}$, and let us assume $M^{2^t} = \{0\}$. Let $I = M^{2^{t-1}}$. Now, $\text{PPol}(R) \leq \text{PPol}_R(I) \wr \text{PPol}(R/I)$ by Lemma 2.4. By Lemma 3.3 we have $\text{PPol}_R(I) \simeq (I, +) \rtimes (R/\text{Ann } I)^\times$. Since M is the unique maximal ideal, $(I, +) \leq (M, +)$, hence $|I|$ divides $|M|$, which is a power of $q = 2$ by Lemma 2.1. Further, $M/\text{Ann } I$ is the unique maximal ideal in $R/\text{Ann } I$, hence $|(R/\text{Ann } I)^\times| = (q - 1) \cdot |M/\text{Ann } I| = |M/\text{Ann } I|$ dividing $|M|$, which is a power of 2 by Lemma 2.1. Hence $\text{PPol}_R(I)$ is 2-group. By the induction hypothesis, $\text{PPol}(R/I)$ is a 2-group. Now, $|\text{PPol}_R(I) \wr \text{PPol}(R/I)| = |\text{PPol}_R(I)|^{|\text{PPol}(R/I)|} \cdot |\text{PPol}(R/I)|$ is a power of 2. Hence $\text{PPol}(R)$ can be embedded into a 2-group, thus $\text{PPol}(R)$ is a 2-group, as well.

Finally, we show that $\text{PPol}(R)$ is abelian if and only if $R \simeq \mathbb{F}_2$. We have already proved that $\text{PPol}(R)$ is nilpotent if and only if $q = 2$. By Lemma 2.1 we have that $|M|$ is a power of 2. Assume first that $|M| \geq 2$. By Cauchy's theorem there exists $0 \neq r \in M$ such that $r + r = 0$. Now $\{x \mapsto x, x \mapsto x + r\} \leq \text{PPol}_R(M)$. Thus $\mathbb{Z}_2$ is a subgroup of $\text{PPol}_R(M)$. By Theorem 1.1 we have $\mathbb{Z}_2 \wr S_2 \simeq \{x \mapsto x, x \mapsto x + r\} \wr S_2 \leq \text{PPol}(R)$. However, $\mathbb{Z}_2 \wr S_2 \simeq D_4$ is not commutative. Therefore, if $\text{PPol}(R)$ is abelian, then $q = 2$ and $|M| \leq 1$, that is, $M = \{0\}$. Furthermore, if $q = 2$, $M = \{0\}$, then $R \simeq \mathbb{F}_2$, and $\text{PPol}(\mathbb{F}_2) \simeq S_2$, which is indeed abelian. $\square$

5. ACKNOWLEDGEMENTS

The research was supported by the Hungarian Scientific Research Fund (OTKA) grant no. K109185 and grant no. FK124814.

REFERENCES

- [1] D. D. Anderson, K. R. Knopp, and R. L. Lewin. Ideals generated by powers of elements. *Bull. Austral. Math. Soc.*, 49(3):373–376, 1994.
- [2] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
- [3] S. Frisch. Polynomial functions on finite commutative rings. In D. E. Dobbs, M. Fontana, and S. E. Kabbaj, editors, *Advances in Commutative Ring Theory*,

- volume 205 of *Lecture Notes in Pure and Applied Mathematics*, pages 323–336. Dekker, 1999.
- [4] S. Frisch. Sylow, p -groups of polynomial permutations on the integers. *Journal of Number Theory*, 133:217–222, 2013.
 - [5] I. Gupta, L. Narain, and C. V. Madhavan. Cryptological applications of permutation polynomials. *Electronic Notes in Discrete Mathematics*, 15:91, 2003. Proceedings of the R.C. Bose Centenary Symposium on Discrete Mathematics and Applications.
 - [6] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
 - [7] Y. Laigle-Chapuy. Permutation polynomials and applications to coding theory. *Finite Fields and Their Applications*, 13(1):58–70, 2007.
 - [8] J. Levine and R. Chandler. Some further cryptographic applications of permutation polynomials. *Cryptologia*, 11(4):211–218, 1987.
 - [9] B. R. MacDonald. *Finite rings with identity*. M. Dekker, 1974.
 - [10] R. J. McEliece, D. J. C. MacKay, and J.-F. Cheng. Turbo decoding as an instance of pearl’s. *IEEE Journal on Selected Areas in Communications*, 16(2):140–152, 1998.
 - [11] G. Mullen and H. Stevens. Polynomial functions (mod m). *Acta Mathematica Hungarica*, 44:237–241, 1984.
 - [12] G. L. Mullen and D. Panario, editors. *Handbook of finite fields*. Boca Raton, FL: CRC Press, 2013.
 - [13] W. Nöbauer. Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen. *Monatsh. Math.*, 59:194–202, 1955.
 - [14] R. R. Rivest. Permutation polynomials modulo 2^w . *Finite Fields and Their Applications*, 7:287–292, 2001.
 - [15] R. P. Singh. *Permutation polynomials and their applications in cryptography*. PhD thesis, Indian Institute of Technology, Guwahati, India, Jan. 2010.
 - [16] R. P. Singh and S. Maity. Permutation polynomials modulo p^n . Cryptology ePrint Archive, Report 2009/393, 2009. <http://eprint.iacr.org/2009/393>.
E-mail address: gorcsosdalma@gmail.com
E-mail address: ghorvath@science.unideb.hu
E-mail address: m.anett.ani95@gmail.com

INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN, PF. 400, DEBRECEN, 4002, HUNGARY