Polynomial functions on finite commutative rings

SOPHIE FRISCH Institut für Mathematik, Technische Universität Graz,
A–8010 Graz, Austria e–mail: frisch@blah.math.tu–graz.ac.at

Abstract. Every function on a finite residue class ring D/I of a Dedekind domain D is induced by an integer-valued polynomial on D that preserves congruences mod I if and only if I is a power of a prime ideal. If R is a finite commutative local ring with maximal ideal P of nilpotency N satisfying for all $a, b \in R$, if $ab \in P^n$ then $a \in P^k$, $b \in P^j$ with $k + j \geq \min(n, N)$, we determine the number of functions (as well as the number of permutations) on R arising from polynomials in $R[x]$. For a finite commutative local ring whose maximal ideal is of nilpotency 2, we also determine the structure of the semigroup of functions and of the group of permutations induced on R by polynomials in $R[x]$.

INTRODUCTION

Let R be a finite commutative ring with identity. Every polynomial $f \in R[x]$ defines a function on R by substitution of the variable. Not every function $\varphi: R \to R$ is induced by a polynomial in $R[x]$, however, unless R is a finite field. (Indeed, if the function with $\varphi(0) = 0$ and $\varphi(r) = 1$ for $r \in R \setminus \{0\}$ is represented by $f \in R[x]$, then $f(x) = a_1x + \ldots + a_nx^n$ and for every non-zero $r \in R$ we have $1 = f(r) = (a_1 + \ldots + a_nr^{n-1})r$, which shows r to be invertible.)

This prompts the question how many functions on R are representable by polynomials in $R[x]$; and also, in the case that $R=D/I$ is a residue class ring of a domain D with quotient field K, whether every function on R might be induced by a polynomial in $K[x]$? We will address these questions in sections 2 and 1, respectively.

Other related problems are to characterize the functions on R arising from polynomials in $R[x]$ by intrinsic properties of these functions (such as preservation of certain relations), and to determine the structure of the semigroup of polynomial functions on R and that of the group of polynomial permutations of R.

In section 4, we will answer the second question in the special case that R is a local ring whose maximal ideal is of nilpotency 2. Apart from that, the only result I am aware of is Nöbauer's expression of the group of polynomial permutations on $\mathbb{Z}_{p^n}$ as a wreath product $G \wr S_p$, with G a rather inscrutable subgroup (characterized by conditions on the coefficients of the representing polynomials) of the group of polynomial permutations on $\mathbb{Z}_{p^{n-1}}$ [11]. (There is a wealth of literature on the functions induced by polynomials on finite fields, some of it concerning the structure of the subgroup of S_q generated by special polynomials, see e.g. [8] and its references. Methods from the theory of finite fields do not help much with finite rings, however, except when the rings are algebras over a finite field, see [2].)

A characterization of polynomial functions by preservation of relations has been given for $R=\mathbb{Z}_n$ by Kempner [6]. For finite commutative rings in general there is the criterion of Spira [17] that a function is representable by a polynomial if and only if all the iterated divided differences that can be formed by subsets of the arguments and the respective values are in R.

In what follows, all rings are assumed to be commutative with identity, the natural numbers are written as $\mathbb{N} = \{1, 2, 3, \ldots\}$, and the non-negative integers as $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$.

1 FUNCTIONS INDUCED ON RESIDUE CLASS RINGS BY INTEGER–VALUED POLYNOMIALS

In this section we give the answer, for Dedekind rings, to a question asked by Narkiewicz in his "Polynomial Mappings" book [9]. For

$R=\mathbb{Z}$, the 'if' direction has been shown (for several variables, cf. the corollary) by Skolem [16], the 'only if' direction by Rédei and Szele [12, 13].

If D is a domain with quotient field K, a polynomial $f \in K[x]$ is called *integer-valued on* D if $f(d) \in D$ for all $d \in D$. We write $\mathrm{Int}(D)$ for the set of all integer-valued polynomials on D. If I is an ideal of a domain D, we say that a polynomial $f \in \mathrm{Int}(D)$ induces a function $\varphi\colon {}^{D}/_{I} \to {}^{D}/_{I}$ if $\varphi(d+I) = f(d)+I$ is well defined, i.e., if $c \equiv d$ mod I implies $f(c) \equiv f(d)$ mod I.

THEOREM 1. *Let R be a Dedekind domain and I an ideal of R of finite index. Every function $\varphi\colon {}^{R}/_{I} \to {}^{R}/_{I}$ is induced by a polynomial $f \in \mathrm{Int}(R)$ if and only if I is a power of a prime ideal of R.*

Proof. The case of a finite field or of $I = R = P^0$ is trivial, so we consider R infinite and $I \neq R$. Let P be a prime ideal with $I \subseteq P$. Assume that the characteristic function of $\{0\}$ on R/I is induced by a polynomial $f \in \mathrm{Int}(R)$, then $f(r) \equiv 1$ mod I for $r \in I$ and $f(r) \equiv 0$ mod I for $r \notin I$. We show that I must be a power of P. Suppose otherwise, then $P^n \not\subseteq I$ for all $n \in \mathbb{N}$. Let $c \in R$ and $g \in R[x]$ such that $f(x) = g(x)/c$, and $n = v_P(c)$.

Since g is in $R[x]$, the function $r \mapsto g(r)$ on R preserves congruences mod every ideal of R, in particular mod P^{n+1}. It follows that $r \equiv s$ mod P^{n+1} implies $f(r) \equiv f(s)$ mod P. Now consider an element $r \in P^{n+1} \setminus I$. On one hand, $f(r) \notin P$, since $f(r) \equiv f(0)$ mod P and $f(0) \equiv 1$ mod I; on the other hand, since $r \notin I$, we have $f(r) \in I \subseteq P$, a contradiction.

To show that every function on ${}^{R}/_{P^n}$ (P a prime ideal of finite index) is induced by a polynomial in $\mathrm{Int}(R)$, it suffices to show this for the charcteristic function of $\{0\}$ on the residue class ring. For this, we need only construct a polynomial $f \in \mathrm{Int}(R)$ satisfying $f(r) \in P$ for $r \notin P^n$ and $f(r) \notin P$ for $r \in P^n$; an appropriate power $\tilde{f}(x) = f(x)^m$ will then satisfy $\tilde{f}(r) \in P^n$ for $r \notin P^n$ and $\tilde{f}(r) \equiv 1$ mod P^n for $r \in P^n$.

Let $a_1, \ldots, a_{q^n-1} \in R$ be a system of representatives of the residue classes of P^n other than P^n itself, and let $a_0 \in P^{n-1} \setminus P^n$. Put $h(x) = \prod_{k=0}^{q^n-1}(x-a_k)$ and $\alpha = \sum_{j=1}^{n} \left[\frac{q^n}{q^j}\right] = \frac{q^n-1}{q-1}$, then for all $r \in P^n$

we have $v_P(h(r)) = \alpha - 1$, while $v_P(h(r)) \geq \alpha$ for all $r \in R \setminus P^n$.

Now let $\mathcal{Q} = \{Q \in \operatorname{Spec}(R) \mid Q \neq P;\ \exists k\ a_k \in Q\}$ and for $Q \in \mathcal{Q}$ define $m_Q = \max\{m \in \mathbb{N} \mid \exists k\ a_k \in Q^m\}$. Pick $c \in R$ such that $c \notin P$ and $c \in Q^{m_Q+1}$ for all $Q \in \mathcal{Q}$, and set $b_k = c^{-1}a_k$ and $g(x) = \prod_{k=0}^{q^n-1}(x - b_k)$.

We now set $f(x) = g(x)/g(0)$ and claim that $f \in \operatorname{Int}(R)$ and that for all $r \in R$, $f(r) \in P$ if and only if $r \notin P^n$. To verify this, we check that for all $Q \in \operatorname{Spec}(R)$ and all $r \in R$, $v_Q(g(r)) \geq v_Q(g(0))$ and that $v_P(g(r)) > v_P(g(0))$ for $r \in R \setminus P^n$, while $v_P(g(r)) = v_P(g(0))$ for $r \in P^n$.

First consider those $Q \in \operatorname{Spec}(R)$ with $v_Q(c) > 0$. We have $v_Q(b_k) < 0$ for all k and therefore $v_Q(g(r)) = \sum_{k=0}^{q^n-1} v_Q(b_k) = v_Q(g(0))$ for all $r \in R$.

Now consider a $Q \in \operatorname{Spec}(R)$ with $v_Q(c) = 0$ and $Q \neq P$, then $v_Q(b_k) = 0$ for all k, and for all $r \in R$ we have $v_Q(g(r)) \geq 0 = v_Q(g(0))$.

Concerning P, we observe that $v_P(r - b_k) = v_P(c^{-1}(cr - a_k)) = v_P(cr - a_k)$, such that $v_P(g(r)) = v_P(h(cr))$. Since $v_P(cr) = v_P(r)$, this implies $v_P(g(r)) \geq \alpha$ for $r \in R \setminus P^n$ and $v_P(g(r)) = \alpha - 1$ for $r \in P^n$. $\square$

If K is the quotient field of a domain D and I an ideal of D, we say that $f \in K[x_1, \ldots, x_m]$ induces a function $\varphi\colon (D/I)^m \to D/I$ if $\varphi(d_1 + I, \ldots, d_m + I) = f(d_1, \ldots, d_m) + I$ makes sense, i.e., if $f(d_1, \ldots, d_m) \in D$ for all $(d_1, \ldots, d_m) \in D^m$ and $f(d'_1, \ldots, d'_m) \equiv f(d_1, \ldots, d_m) \bmod I$ whenever $d'_i \equiv d_i \bmod I$ for $1 \leq i \leq m$.

COROLLARY. *If R is a Dedekind domain, P a maximal ideal of finite index and $n \in \mathbb{N}$ then every function $f\colon (R/P^n)^m \to R/P^n$ is induced by a polynomial $f \in K[x_1, \ldots, x_m]$ (K being the quotient field of R).*

Proof. It suffices to have a polynomial $f \in K[x_1, \ldots, x_m]$ that induces the characteristic function of $(0, 0, \ldots, 0) \bmod P^n$. As R/P is a field, there exists a $g \in R[x_1, \ldots, x_m]$ such that $g(r_1, \ldots, r_m) \equiv 1 \bmod P$ if $r_i \in P$ for $1 \leq i \leq m$ and $g(r_1, \ldots, r_m) \equiv 0 \bmod P$ otherwise. By the Theorem, there exists $h \in \operatorname{Int}(R)$ such that $h(r) \in P$ if $r \in P^n$ and $h(r) \notin P$ otherwise. Now $f(x_1, \ldots, x_m) = g(h(x_1), \ldots, h(x_m))$ satisfies $f(r_1, \ldots, r_m) \notin P$ iff $r_i \in P^n$ for $1 \leq i \leq m$, and a suitable power of $g(x) = f(x)^k$ finally satisfies $g(r_1, \ldots, r_m) \equiv 1 \bmod P^n$ if $r_i \in P^n$ for $1 \leq i \leq m$ and $g(r_1, \ldots, r_m) \equiv 0 \bmod P^n$ otherwise, as required. $\square$

Note that the theorem and its proof still hold if we replace Dedekind ring by Krull ring, prime ideal by height 1 prime ideal, and restrict I to ideals with $\mathrm{div}(I) \neq R$.

2 THE NUMBER FORMULAS

For a commutative finite ring R, let us denote by $\mathcal{F}(R)$ the set (or semigroup with respect to composition) of functions on R induced by polynomials in $R[x]$, and by $\mathcal{P}(R)$ the subset (or group) of those polynomial functions on R that are permutations.

When considering the functions induced on a finite commutative ring R by polynomials in $R[x]$, we can restrict ourselves to local rings, since every finite commutative ring is a direct sum of local rings, and addition and multiplication (and therefore evaluation of polynomials in $R[x]$) are performed in each component independently.

For residue class rings of the integers, we know

$$|\mathcal{F}(\mathbb{Z}_{p^n})| = p^{\sum_{k=1}^{n} \beta_p(k)} \quad \text{and} \quad |\mathcal{P}(\mathbb{Z}_{p^n})| = p!p^p(p-1)^p p^{\sum_{k=3}^{n} \beta_p(k)},$$

where p is a prime and $\beta_p(k)$ is the minimal $m \in \mathbb{N}$ such that $p^k \mid m!$ (in other words, the minimal $m \in \mathbb{N}$ such that $\alpha_p(m) \geq k$, with $\alpha_p(m) = \sum_{j \geq 1} \left[\frac{m}{p^j}\right]$).

The most lucid proof, in my opinion, of these two formulas is that by Keller and Olson [5], to whom the second one is due. Kempner's earlier proof [6] of the formula for $|\mathcal{F}(\mathbb{Z}_{p^n})|$ is rather more involved. Singmaster [15] and Wiesenbauer [18] gave proofs for $R=\mathbb{Z}_m$ which do not use reduction to the local ring case. Brawley and Mullen [3] generalized the formulas to Galois rings (rings of the form $\mathbb{Z}[x]/(p^n, f)$, where p is prime and $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}_p$, see [7]) and Nečaev [10] to finite commutative local principal ideal rings.

We will give a proof along the lines of Keller and Olson of a generalization of the formulas to a class of local rings (the suitable rings defined below) that properly contains the rings considered by Brawley, Mullen and Nečaev.

DEFINITION. Let R be a finite commutative local ring R with maximal ideal P and $N \in \mathbb{N}$ minimal with $P^N = (0)$. We call R

"suitable", if for all a, $b \in R$ and all $n \in \mathbb{N}$,

$$ab \in P^n \Longrightarrow a \in P^k \text{ and } b \in P^j \text{ with } k + j \geq \min(N, n).$$

Note that every finite local ring R with maximal ideal P such that $P^2 = (0)$ is suitable, as well as every finite local ring whose maximal ideal is principal.

We may think of this property as inducing a valuation-like mapping $v: R \to H_N$, by $v(r) = k$ if $r \in P^k \setminus P^{k+1}$ and $v(0) = \infty$, where $(H_N, +)$ results from the non-negative integers by identifying all numbers greater or equal N; it is the semigroup with elements $\{0, 1, \ldots, N{-}1, N{=}\infty\}$ and $i{+}j{=}\min(i{+}j, N)$, where the operations on the right are just the usual ones on non-negative integers.

DEFINITION. If R is a finite local ring and P its maximal ideal, for $n \geq 0$, let

$$\alpha(n) = \alpha_{(R,P)}(n) = \sum_{j \geq 1} \left[\frac{n}{[R : P^j]} \right]$$

and let $\beta(n) = \beta_{(R,P)}(n)$ be the minimal $m \in \mathbb{N}$ such that $\alpha_{(R,P)}(m) \geq n$. (If R and P are understood, we suppress the subscript (R, P) of α and β.)

REMARK. Note that $\alpha_{(R,P)}(n)$ is finite if and only if $n < |R|$; we will never use $\alpha_{(R,P)}$ outside that range. Also note that, since $[R/P^k : P^j/P^k] = [R : P^j]$ for $j \leq k$, we have $\alpha_{(R,P)}(n) = \alpha_{(R/P^k, P/P^k)}(n)$ in the range where both values are finite, that is for $n < [R : P^k]$.

THEOREM 2. *Let R be a suitable finite local ring with maximal ideal P, $q = [R : P]$, and $N \in \mathbb{N}$ minimal, such that $P^N = (0)$. Then*

$$|\mathcal{F}(R)| = \prod_{j=0}^{\beta(N)-1} [R : P^{N-\alpha(j)}],$$

where $\alpha(n) = \sum_{j \geq 1} \left[\frac{n}{[R:P^j]} \right]$ and $\beta(n)$ is the minimal $m \in \mathbb{N}$ such that $\alpha(m) \geq n$.

Also, for $N > 1$,

$$|\mathcal{P}(R)| = \frac{q!\,(q-1)^q}{q^{2q}}\,|\mathcal{F}(R)|\,.$$

If $[P^{k-1}:P^k]=q$ *for* $1\le k\le N$, *the formulas simplify to*

$$|\mathcal{F}(R)| = q^{\sum_{k=1}^{N}\beta_q(k)} \quad \text{and} \quad |\mathcal{P}(R)| = q!q^q(q-1)^q\, q^{\sum_{k=3}^{N}\beta_q(k)},$$

where $\alpha_q(m)=\sum_{j\ge 1}\left[\frac{m}{q^j}\right]$ *and* $\beta_q(k)$ *is the minimal* $m\in\mathbb{N}$ *such that* $\alpha_q(m)\ge k$.

We will prove the expression for $|\mathcal{F}(R)|$ at the end of the next section, and that for $|\mathcal{P}(R)|$ at the end of section 4.

3 A CANONICAL FORM FOR THE POLYNOMIAL REPRESENTING A FUNCTION

DEFINITION. Let R be a commutative finite local ring with maximal ideal P of nilpotency N. We call a sequence $(a_k)_{k=0}^{\infty}$ of elements in R a P-sequence, if for $0\le n\le N$

$$a_k-a_j\in P^n \iff [R:P^n]\;\big|\; k-j;$$

and if (a_k) is a P-sequence, we call the polynomials

$$\langle x\rangle_0 = 1 \qquad \text{and} \qquad \langle x\rangle_n=(x-a_0)\dots(x-a_{n-1}) \quad \text{for } n>0$$

the "falling factorials" constructed from the sequence (a_k).

A P-sequence (a_k) for R is easy to construct inductively: Let $a_0,\dots,a_{[R:P]-1}$ be a complete set of residues mod P with $a_0=0$. Once a_k has been defined for $k<[R:P^{n-1}]$ (while $n\le N$), define a_k for $[R:P^{n-1}]\le k<[R:P^n]$ as follows: let $b_0=0$, b_1, ..., $b_{[P^{n-1}:P^n]-1}$ be a complete set of residues of P^{n-1} mod P^n; then, for $k=j[R:P^{n-1}]+r$ with $0\le r<[R:P^{n-1}]$ and $1\le j<[P^{n-1}:P^n]$, let $a_k=b_j+a_r$. After $a_0,\dots,a_{|R|-1}$ have been defined (necessarily a complete enumeration of the elements of R), continue the sequence $|R|$-periodically.

In the following Lemma, we use the convention that $P^\infty=(0)$.

LEMMA. *Let R be a suitable finite local ring with maximal ideal P of nilpotency N, and $\langle x\rangle_n$ the falling factorial of degree n constructed from a P-sequence (a_k). Then for all $n \in \mathbb{N}_0$,*

$$\forall r \in R \quad \langle r\rangle_n \in P^{\alpha(n)} \qquad \textit{and} \qquad \textit{if } \alpha(n) < N \textit{ then } \langle a_n\rangle_n \notin P^{\alpha(n)+1}.$$

Proof. If $n \geq |R|$ (equivalent to $\alpha(n) = \infty$) then, since $a_0, \dots, a_{|R|-1}$ enumerate all elements of R, $\langle r\rangle_n = 0$ for all r.

If $n < |R|$ then $\alpha(n) = \sum_{k=1}^{N} \left[\frac{n}{[R:P^k]}\right]$, while $\langle r\rangle_n \in P^e$, where $e =$

$$\sum_{k=1}^{N-1} k \left|\{j \mid 0 \leq j < n;\ r - a_j \in P^k \setminus P^{k+1}\}\right| +$$

$$+N \left|\{j \mid 0 \leq j < n;\ r - a_j \in P^N\}\right|$$

$$= \sum_{k=1}^{N} \left|\{j \mid 0 \leq j < n;\ r - a_j \in P^k\}\right|$$

and (by definition of suitable) $\langle r\rangle_n$ is in no higher power of P if $e < N$.

From the definition of P-sequence, we see that the cardinality of $\{j \mid 0 \leq j < n;\ r - a_j \in P^k\}$ is either $\left[\frac{n}{[R:P^k]}\right]$ or $\left[\frac{n}{[R:P^k]}\right] + 1$ and the $+1$ doesn't occur for $r = a_n$. □

PROPOSITION 1. *Let R be a suitable finite local ring with maximal ideal P of nilpotency N, (a_k) a P-sequence for R, $\langle x\rangle_k$ the falling factorial of degree k constructed from it and let $0 \leq n \leq N$.*

A polynomial $f \in R[x]$ induces the zero-function on R/P^n if and only if

$$f(x) = \sum_{j \geq 0} c_j \langle x\rangle_j \qquad \textit{with} \qquad c_j \in P^{n-\alpha(j)} \quad \textit{for} \quad 0 \leq j < \beta(n).$$

Proof. As $\langle x\rangle_j$ maps R into $P^{\alpha(j)}$, the "if" direction is evident. To show "only if", assume that $f(x) = \sum_{j\geq 0} c_j \langle x\rangle_j$ maps R into P^n. We show $c_j \in P^{n-\alpha(j)}$ for $0 \leq j < \beta(n)$ by induction on j. (There is no condition on the coefficients for $j \geq \beta(n)$, since $\langle x\rangle_j$ already maps R into P^n for those j.)

For $j=0$, we have $c_0=f(a_0)\in P^n$. Now assume $c_i\in P^{n-\alpha(i)}$ for $i<j$ and consider $f(a_j)$. Since $\langle x\rangle_i$ maps R into $P^{\alpha(i)}$ and $\langle a_j\rangle_k=0$ for $k>j$, we have $f(a_j)\equiv c_j\langle a_j\rangle_j \bmod P^n$. Also, $\langle a_j\rangle_j$ is in no higher power of P than $P^{\alpha(j)}$. Therefore $f(a_j)\in P^n$ implies $c_j\in P^{n-\alpha(j)}$. □

COROLLARY 1. *In the situation of the Proposition, for $0\le j<\beta(n)$, let C_j be a complete set of residues mod $P^{n-\alpha(j)}$. Then every function on R/P^n arising from a polynomial in $R[x]$ arises from a unique polynomial of the form*

$$f(x)=\sum_{j=0}^{\beta(n)-1} c_j\langle x\rangle_j \qquad \textit{with} \qquad c_j\in C_j.$$

For $R=\mathbb{Z}_{p^n}$, other canonical forms for the functions representable by polynomials have been given by Dueball [4], Aizenberg, Semion and Tsitkin [1] and Rosenberg [14] (the latter for polynomials in several variables).

COROLLARY 2. *In the situation of the Proposition, if $n>0$ then for every function induced on the residue classes of P^{n-1} by a polynomial in $R[x]$, there are exactly*

$$\prod_{j=0}^{\beta(n)-1}[P^{n-\alpha(j)-1}:P^{n-\alpha(j)}]$$

different polynomial functions on the residue classes of P^n that reduce to the given function mod P^{n-1}. If $[P^{k-1}:P^k]=q$ for $1\le k\le N$ then the expression simplifies to $q^{\beta_q(n)}$, where $\beta_q(n)$ is the minimal $m\in\mathbb{N}$ such that $\alpha_q(m)=\sum_{j\ge1}\left[\frac{n}{q^j}\right]\ge n$.

Proof of the formula for $|\mathcal{F}(R)|$ in Theorem 2:

$$|\mathcal{F}(R)|=\prod_{j=0}^{\beta(N)-1}[R:P^{N-\alpha(j)}]$$

follows immediately from Corollary 1 with $n=N$. In the special case that $[P^{k-1}:P^k]=q$ for $1\le k\le N$, writing s_k for the number of different functions on R/P^k arising from polynomials in $R[x]$, we see from Corollary 2 that $q^{\beta_q(k)}s_{k-1}=s_k$. Therefore $q^{\sum_{k=1}^{N}\beta(k)}=s_N=|\mathcal{F}(R)|$ in that case. □

4 THE GROUP $\mathcal{P}$(R/P²)

We want to determine the structure of the group $\mathcal{P}(R/P^2)$ with respect to composition of functions, R being a suitable finite local ring as above. To simplify notation, we consider the group $\mathcal{P}(R)$, where R is a finite local ring with maximal ideal P of nilpotency $N=2$.

Some notational conventions: We write the group of *invertible elements* of a monoid M as M^*. If M is a monoid and H a monoid acting on a set S then the *wreath product* $M \wr H$ is the monoid defined on the set $H \times M^S$ by the operation

$$(h,\, (m_s)_{s\in S})(g,\, (l_s)_{s\in S}) = (hg,\, (m_{g(s)} l_s)_{s\in S}).$$

If M acts on a set T then the standard action of $M \wr H$ on $S \times T$ is

$$(h, (m_s)_{s\in S})(x, y) = (h(x), m_x(y)).$$

Note that an element $(h, (m_s)_{s\in S})$ is in $(M \wr H)^*$ if and only if $h \in H^*$ and $m_s \in M^*$ for all $s \in S$, and that therefore $(M \wr H)^* \simeq M^* \wr H^*$.

If D is a commutative ring and M a D-module, we write $\mathbb{A}_D(M)$ for the semigroup with respect to compostion of transformations of M of the form $x \mapsto ax + b$ with $a \in D$ and $b \in M$. We have $|\mathbb{A}_D(M)| = |D/\mathrm{Ann}(M) \times M|$.

PROPOSITION 2. *Let R be a finite local ring with maximal ideal P of nilpotency 2 and $q = [R:P]$. Denote by Q^Q the semigroup of functions from a set of q elements to itself. Then*

$$\mathcal{F}(R) \simeq \mathbb{A}_{R/P}(P) \wr Q^Q \qquad \text{and} \qquad \mathcal{P}(R) \simeq \mathbb{A}^*_{R/P}(P) \wr S_q,$$

and in particular,

$$|\mathcal{F}(R)| = q^q\, |R|^q \qquad \text{and} \qquad |\mathcal{P}(R)| = q!\, (q-1)^q\, |P|^q.$$

Proof. Fix a system of representatives Q of R mod P. We identify R with $Q \times P$ by $r \mapsto (s,t)$ with $s \in Q$, $t \in P$, such that $r = s + t$. Let $f \in R[x]$. We have

$$f(r) = f(s+t) = f(s) + f'(s)t,$$

since this holds mod P^2 by Taylor's Theorem and $P^2 = (0)$ in R. Now let $\varphi(s)$ be the representative in Q of $f(s) + P$, then

$$f(s+t) = \varphi(s) + (f(s) - \varphi(s)) + f'(s)t,$$

with $\varphi(s) \in Q$ and $f(s) - \varphi(s) \in P$. We regard $f'(s)$ as being in R/P. (As it gets multiplied by $t \in P$, only its residue class mod P matters).

If we associate to $f \in R[x]$ the functions $\varphi_f \colon Q \to Q$ and $\psi_f \colon Q \to \mathbb{A}_{R/P}(P)$, where

- $\varphi_f(s)$ is the representative in Q of $f(s) + P$
- $\psi_f(s)$ is the transformation $x \mapsto a_f(s)x + b_f(s)$ on P, where
  - $a_f(s) \in R/P$ is $f'(s)$ mod P,
  - $b_f(s) = f(s) - \varphi(s) \in P$

then φ_f and ψ_f completely determine the function induced by f on R.

Moreover, the function defined on $Q \times P$ by $\varphi \in Q^Q$, $a \in (R/P)^Q$ and $b \in P^Q$ via $(s,t) \mapsto \varphi(s) + a(s)t + b(s)$ determines φ, a and b uniquely, such that for f, $g \in R[x]$ inducing the same function on R we have $\varphi_g = \varphi_f$ and $\psi_g = \psi_f$. Therefore $f \mapsto (\varphi_f, \psi_f)$ depends only on the function induced by $f \in R[x]$ on R and defines a homomorphism from $\mathcal{F}(R)$ to $\mathbb{A}_{R/P}(P) \wr Q^Q$, which takes the action of $\mathcal{F}(R)$ on R (identified with $Q \times P$) to the standard action of $A \wr Q^Q$ arising from the obvious actions of A on P and of Q^Q on Q. We have already seen that this homomorphism is injective.

To check surjectivity, we show that every triple of functions $\varphi \colon Q \to Q$, $b \colon Q \to P$ and $a \colon Q \to R/P$ actually occurs as φ_f, a_f and b_f for some $f \in R[x]$.

Every pair of functions on R/P arises as f mod P and f' mod P for some polynomial $f \in R[x]$, because R/P is a finite field. This takes care of φ_f and a_f. Since the characteristic function of every residue class of P is induced by a polynomial in $R[x]$ (just take a sufficiently high power of a polynomial representing it mod P), we can adjust f to take prescribed values on the $s \in Q$, by adding a P-linear combination of these characteristic functions. This produces a prescribed b_f without disturbing the values of f and f' mod P, since we only add a polynomial in $P[x]$.

If we restrict to polynomials representing permutations or, equivalently, to polynomials for which φ_f is a permutation of Q and $a_f(s) \neq 0 + P$ for all $s \in Q$, we get an isomorphism of $\mathcal{P}(R)$ and $\mathbb{A}^*_{R/P}(P) \wr S_q$, which takes the action of $\mathcal{P}(R)$ on R (identified with $Q \times P$) to the standard action of the wreath product on $Q \times P$ arising from the obvious actions of $\mathbb{A}^*_{R/P}$ on P and of the symmetric group S_q on Q. $\square$

REMARK. We may simplify the expression for $\mathcal{P}(R)$ by noting that $\mathbb{A}_{R/P}(P)$ is isomorphic to the semi-direct product $((R/P)^*, \cdot) \ltimes (P, +)$ with $(R/P)^*$ acting on $(P, +)$ through the scalar mulutiplication of the R/P-vectorspace structure on P.

Proof of the formula for $|\mathcal{P}(R)|$ *in Theorem 2:* For $n \leq N$, let s_n denote the number of functions on the residue classes of P^n induced by polynomials in $R[x]$ and t_n the number of them that are permutations.

If $n \geq 2$, a polynomial induces a permutation mod P^n if and only if it induces a permutation mod P and its derivative is nowhere zero mod P, cf. [7]. In particular, if $n > 2$, a polynomial induces a permutation mod P^n if and only if it induces one mod P^{n-1}. Together with the fact that every class of polynomial functions mod P^n reducing to the same function mod P^{n-1} contains the same number of elements (Corollary 2 of Proposition 1), this implies that $\frac{t_n}{t_{n-1}} = \frac{s_n}{s_{n-1}}$ for all $n > 2$, and therefore $t_n = \frac{t_2}{s_2} s_n$ for all $n \geq 2$.

From Proposition 2 applied to R/P^2 we get $t_2 = q!(q-1)^q [P : P^2]^q$ and $s_2 = q^q [R : P^2]^q$ and the formula for $|\mathcal{P}(R)|$ follows. $\square$

REFERENCES

[1] N. Aizenberg, I. Semion, and A. Tsitkin, Polynomial representations of logical functions, Automatic Control and Computer Sciences (transl. of Automatika i Vychislitel'naya Tekhnika, Acad. Nauk Latv. SSR (Riga)), 5 (1971), pp. 5–11 (orig. 6–13).

[2] D. A. Ashlock, Permutation polynomials of Abelian group rings over finite fields, J. Pure Appl. Algebra, 86 (1993), pp. 1–5.

[3] J. V. Brawley and G. L. Mullen, Functions and polynomials over Galois rings, J. Number Theory, 41 (1992), pp. 156–166.

[4] F. Dueball, Bestimmung von Polynomen aus ihren Werten mod p^n, Math. Nachr., 3 (1949/50), pp. 71–76.

[5] G. Keller and F. Olson, Counting polynomial functions (mod p^n), Duke Math. J., 35 (1968), pp. 835–838.

[6] A. J. Kempner, Polynomials and their residue systems, Trans. Amer. Math. Soc., 22 (1921), pp. 240–266, 267–288.

[7] B. R. McDonald, Finite Rings with Identity, Dekker, 1974.

[8] G. L. Mullen and H. Niederreiter, The structure of a group of permutation polynomials, J. Austral. Math. Soc. Ser. A, 38 (1985), pp. 164–170.

[9] W. Narkiewicz, Polynomial Mappings, vol. 1600 of Lecture Notes in Mathematics, Springer, 1995.

[10] A. Nechaev, Polynomial transformations of finite commutative local rings of principal ideals, Math. Notes, 27 (1980), pp. 425–432. transl. from Mat. Zametki 27 (1980) 885-897, 989.

[11] W. Nöbauer, Gruppen von Restpolynomidealrestklassen nach Primzahlpotenzen, Monatsh. Math., 59 (1955), pp. 194–202.

[12] L. Rédei and T. Szele, Algebraisch-zahlentheoretische Betrachtungen über Ringe I, Acta Math. (Uppsala), 79 (1947), pp. 291–320.

[13] ——, Algebraisch-zahlentheoretische Betrachtungen über Ringe II, Acta Math. (Uppsala), 82 (1950), pp. 209–241.

[14] I. G. Rosenberg, Polynomial functions over finite rings, Glas. Mat., 10 (1975), pp. 25–33.

[15] D. Singmaster, On polynomial functions (mod m), J. Number Theory, 6 (1974), pp. 345–352.

[16] Th. Skolem, Einige Sätze über Polynome, Avh. Norske Vid. Akad. Oslo, I. Mat.-Naturv. Kl., 4 (1940), pp. 1–16.

[17] R. Spira, Polynomial interpolation over commutative rings, Amer. Math. Monthly, 75 (1968), pp. 638–640.

[18] J. Wiesenbauer, On polynomial functions over residue class rings of $\mathbb{Z}$, in Contributions to general algebra 2 (Proc. of Conf. in Klagenfurt 1982), Hölder-Pichler-Tempsky, Teubner, 1983, pp. 395–398.