THE POLYPERMUTATION GROUP OF AN ASSOCIATIVE RING

JASON K.C. POLAK

Abstract. We study permutation polynomials through the device of the *polypermutation group* of an associative ring R, denoted by $\mathrm{Pgr}(R)$. We derive some basic properties and compute the cardinality of $\mathrm{Pgr}(\mathbb{Z}/p^k)$ when $p \geq k$. We use this computation to determine the structure of $\mathrm{Pgr}(\mathbb{Z}/p^2)$.

Contents

1. Introduction

Let p be a prime. Why are $\mathbb{Z}/p \times \mathbb{Z}/p$ and $\mathbb{Z}/p^2$ not isomorphic as rings? It's because the latter has more permutations induced by polynomials! That's what this paper is about—permutations of rings like $\mathbb{Z}/p^k$ induced by polynomials. We start with R, an associative ring with identity. We say that a polynomial $f \in R[x]$ is a **permutation polynomial** if the induced evaluation function $R \to R$ is bijective. For example, $x^3 + 6x^2 + x \in \mathbb{Z}/9[x]$ permutes $\mathbb{Z}/9$. For finite fields permutation polynomials have been studied extensively (cf. [LN00, Chapter 7]), and some other finite rings have also been considered. Often, research has focused on finding specific classes of permutation polynomials. In this work, we study this subject from the lesser used perspective of group theory.

1.1. **Definition.** For a ring R, the subset of permutations of R that can be represented by polynomial functions is a monoid, and we define the **polypermutation group** $\mathrm{Pgr}(R)$ of R to be the subgroup generated by this monoid in the symmetric group of R.

If R is a finite field, any function $R \to R$ can be represented by a polynomial and so $\mathrm{Pgr}(R)$ is the symmetric group Δ_R on R. In [Ash93] and [CH72], the polypermutation group was calculated for the group ring $R[G]$ where R is a finite field and G is a finite abelian group.

So what's in this paper? Although the polypermutation group has been considered before a few times, it does not seem to have been studied systematically, so we will start with some

Date: July 2, 2017.
2010 *Mathematics Subject Classification.* Primary: 11T06. Secondary: 16P10, 05A05.
Key words and phrases. Permutation group, polynomial, associative ring.
This research was supported by ARC Grant DP150103525.

basic properties of the polypermutation group in §2, such as the behaviour of $\mathrm{Pgr}(-)$ with respect to products, inverse limits, and ring homomorphisms. For example, it turns out that $\mathrm{Pgr}(-)$ is a functor from the category of finite rings and surjective homomorphisms to the category of groups. The main section is §3, where we compute the size of $\mathrm{Pgr}(\mathbb{Z}/p^k)$ for a prime p and an integer k such that $p \geq k$:

1.2. **Theorem.** *Let p be a prime and $k \geq 2$ be an integer such that $p \geq k$. Then*

$$|\mathrm{Pgr}(\mathbb{Z}/p^k)| = p![(p-1)p^{(k^2+k-4)/2}]^p.$$

As an application of this theorem, we compute the structure of $\mathrm{Pgr}(\mathbb{Z}/p^2)$:

1.3. **Theorem.** *Let p be a prime and let the group $(\mathbb{Z}/p)^\times$ act on the group $\mathbb{Z}/p$ by multiplication. Let Δ_p act on the p-fold products $(\mathbb{Z}/p^\times)^p$ and $(\mathbb{Z}/p)^p$ via permuting the coordinates. Then there exists an isomorphism*

$$\mathrm{Pgr}(\mathbb{Z}/p^2) \cong ((\mathbb{Z}/p)^p \rtimes [(\mathbb{Z}/p)^\times]^p) \rtimes \Delta_p$$

Here, the notation $A \rtimes G$ means the semidirect product with G acting on A.

2. Basic Properties

For any set X, we write Δ_X for the permutation group of X and Δ_n for the permutation group on n letters. We also write D_n for the dihedral group of the regular n-gon if $n \geq 3$, so that $|D_n| = 2n$. By convention we set $D_2 = \Delta_2 \cong \mathbb{Z}/2$ and $D_1 = \{e\}$.

2.1. **Proposition.** *If R_1 and R_2 are associative rings then*

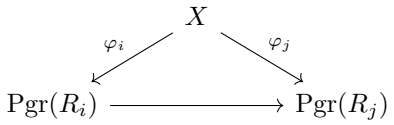
$$\mathrm{Pgr}(R_1 \times R_2) \cong \mathrm{Pgr}(R_1) \times \mathrm{Pgr}(R_2).$$

Proof. Any polynomial permutation of $R_1 \times R_2$ comes from a polynomial with coefficients in $R_1 \times R_2$ and so is given by a pair of polynomials (f_1, f_2) with $f_1 \in R_1[x]$ and $f_2 \in R_2[x]$. □

2.2. **Proposition.** *Let I be a directed poset and consider a functor F from I to the category of rings. Write $R_i = F(i)$ for all $i \in I$. Suppose that for each morphism $i \to j$ in I, the morphism $R_i \to R_j$ with the corresponding morphism $R_i[x] \to R_j[x]$ sends permutation polynomials to permutation polynomials. Then*

$$\mathrm{Pgr}(\varprojlim_F R_i) \cong \varprojlim_F \mathrm{Pgr}(R_i).$$

Proof. We will show that $\mathrm{Pgr}(\varprojlim_F R_i)$ satisfies the universal property of $\varprojlim_F \mathrm{Pgr}(R_i)$. To this end, let X be a group and suppose we have homomorphisms $\varphi_i : X \to \mathrm{Pgr}(R_i)$ for each $i \in I$ such that the diagram



commutes whenever there is a map $\mathrm{Pgr}(R_i) \to \mathrm{Pgr}(R_j)$. Thus $f_i = \varphi_i(x)$ is a permutation polynomial in $R_i[x]$ for all i such that $\varphi_j(x)$ is obtained from $\varphi_i(x)$ by applying $R_i \to R_j$ if such a map exists. So, such a system of polynomials defines a polynomial $f = (f_i)$ with

coefficients in $\varprojlim R_i$; we need to verify that it defines a bijection $\varprojlim R_i \to \varprojlim R_i$. Since each f_i is an injection, the map $\varprojlim R_i \to \varprojlim R_i$ must certainly be an injection.

Now suppose that $(a_i) \in \varprojlim R_i$. Since each f_i is surjective, there exists an element $(b_i) \in \prod R_i$ such that $f_i(b_i) = a_i$ for each i. Let $\alpha : R_i \to R_j$ be the ring homomorphism in the inverse system, so that $\alpha(f_i) = f_j$ and $\alpha(a_i) = a_j$. Applying α to the equation $f_i(b_i) = a_i$ gives

$$f_j(\alpha(b_i)) = a_j,$$

and we already have $f_j(b_j) = a_j$. Since $f_j : R_j \to R_j$ is bijective, $\alpha(b_i) = b_j$ and so $(b_i) \in \varprojlim R_i$, showing that f is also surjective and hence bijective. Thus we get a map $X \to \mathrm{Pgr}(\varprojlim R_i)$, which is a group homomorphism because each φ_i is a group homomorphism, and by construction is the unique homomorphism that makes the appropriate diagram commute. □

2.3. *Remark.* Let R be a commutative ring and suppose that R_1 and R_2 are any two commutative R-algebras. Then there does not seem to be an easy way to determine $\mathrm{Pgr}(R_1 \otimes_R R_2)$ from $\mathrm{Pgr}(R_1)$ and $\mathrm{Pgr}(R_2)$ as can be seen in the case of $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m \cong \mathbb{Z}/\gcd(m,n)$.

The next proposition can be helpful when computing some polypermutation groups by hand.

2.4. **Proposition.** *Let R be a ring such that every translation polynomial $x+r$ is in $\mathrm{Pgr}(R)$ and let $\{f_i : i \in I\}$ be a set of generators for $\mathrm{Pgr}(R)$ containing all translation polynomials. Then each f_i that is not a translation can be replaced by a polynomial with no constant term.*

Proof. Let f be in the generating set for $\mathrm{Pgr}(R)$. Since f is a permutation, $f(r) = 0$ for some $r \in R$. Then $f(x + r)$ is also in $\mathrm{Pgr}(R)$, has no constant term, and may replace f in the generating set. □

Let $R \to S$ be a ring homomorphism. When does the induced map $R[x] \to S[x]$ send permutation polynomials to permutation polynomials? This does not always happen: for example, the homomorphism $\mathbb{Z}/2 \to \mathbb{Z}/2[t]$ sends $f(x) = x^2$ to a polynomial that does not induce a permutation, because $t \in \mathbb{Z}/2[t]$ has no square root! The first hint is a result of Rivest.

2.5. **Theorem** ([Riv01])**.** *Let $w \geq 2$. A polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with integer coefficients reduces to a permutation polynomial in $\mathbb{Z}/2^w[x]$ if and only if a_1 is odd, $(a_2 + a_4 + \cdots)$ is even, and $(a_3 + a_5 + \cdots)$ is even.*

Since Rivest's condition on f is independent of w, and given that such a polynomial would also reduce to a permutation polynomial in $\mathbb{Z}/2[x]$, we see that the reduction homomorphisms $\mathbb{Z}/2^k \to \mathbb{Z}/2^\ell$ for $\ell \leq k$ induce group homomorphisms

$$\mathrm{Pgr}(\mathbb{Z}/2^k) \to \mathrm{Pgr}(\mathbb{Z}/2^\ell)$$

which are surjective, again by Rivest's condition. It is easy to verify that when $m \mid n$, the reduction map $\mathbb{Z}/n \to \mathbb{Z}/m$ induces a map $\mathrm{Pgr}(\mathbb{Z}/n) \to \mathrm{Pgr}(\mathbb{Z}/m)$. Both of these facts are part of a more general result, which is easy to see but nevertheless useful.

2.6. **Proposition.** *Let R be a ring and I an ideal of R. If R/I is finite then the reduction modulo I of any permutation polynomial $f \in R[x]$ is a permutation polynomial in $R/I[x]$.*

Hence, there is an induced map

$$\mathrm{Pgr}(R) \longrightarrow \mathrm{Pgr}(R/I).$$

Proof. Let $f \in R[x]$ be a permutation polynomial. Then its reduction modulo I defines a function on R/I which is surjective and hence injective because R/I is a finite set. □

In particular, $\mathrm{Pgr}(-)$ is a functor from the category of finite rings and surjective morphisms to the category of finite groups. As an example use of this theorem, write

$$\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k$$

for the p-adic integers. Applying Proposition 2.6 and Proposition 2.2, we see that we have an isomorphism

$$\mathrm{Pgr}(\mathbb{Z}_p) \cong \varprojlim_k \mathrm{Pgr}(\mathbb{Z}/p^k)$$

showing that the monoid of polynomial permutations of $\mathbb{Z}_p$ is actually a group. Moreover, we can endow $\mathrm{Pgr}(\mathbb{Z}_p)$ with the topology coming from this inverse limit of finite groups, making $\mathrm{Pgr}(\mathbb{Z}_p)$ into a profinite group, though we will leave an analysis of this p-adic situation for a future paper.

2.7. *Remark.* Here is a question inspired by Proposition 2.6 for which we do not yet have a good answer. Let I be an ideal of a ring R such that R/I is finite. When is

$$\mathrm{Pgr}(R) \longrightarrow \mathrm{Pgr}(R/I)$$

surjective? This is a natural question, because when it is surjective, then $\mathrm{Pgr}(R/I)$ would be a quotient of $\mathrm{Pgr}(R)$. It is certainly not always surjective, such as for $\mathbb{Z} \to \mathbb{Z}/p$ when p is a prime. Even when it is surjective, lifts of permutation polynomials in $R/I[x]$ may not necessarily be permutation polynomials in $R[x]$, as in the case of $\mathbb{Z}/2[u]/u^2 \to \mathbb{Z}/2$ where the polynomial $x^2 \in \mathbb{Z}/2[u]/u^2[x]$ reduces to a permutation polynomial in $\mathbb{Z}/2[x]$ but does not induce a permutation of $\mathbb{Z}/2[u]/u^2$.

3. Quotient Rings of the Integers

In this section we take a look at $\mathrm{Pgr}(\mathbb{Z}/n)$. When writing permutations of $\mathbb{Z}/n$, we will use cycle notation with the elements labeled as $0, 1, \ldots, n-1$. We have already remarked that $\mathrm{Pgr}(R) = \Delta_R$ when R is a finite field.

3.1. **Proposition.** *Let n be squarefree with $n = p_1 p_2 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$. Then*

$$\mathrm{Pgr}(\mathbb{Z}/n) \cong \Delta_{p_1} \times \cdots \times \Delta_{p_k}$$

Furthermore, if $n > 6$ then $\mathrm{Pgr}(\mathbb{Z}/n)$ is a proper subgroup of Δ_n.

Proof. This follows immediately from Proposition 2.1. □

We now consider $\mathbb{Z}/p^k$ where $k > 1$ and p is a prime number. We start with some examples that will elucidate a method that works in principle to compute $\mathrm{Pgr}(R)$ for any finite ring R.

3.2. **Proposition.** *The polypermutation group of* $\mathbb{Z}/4$ *is*

$$\mathrm{Pgr}(\mathbb{Z}/4) \cong D_4,$$

and is generated by $(0,1,2,3)$ *and* $(1,3)$.

Proof. The permutation $(0,1,2,3)$ can be given by the polynomial function $f(x) = x+1$, and the permutation $(1,3)$ can be given by $f(x) = x^4 + x^2 + x$. Since $(0,1,2,3)^2 = (0,2)(1,3)$, we see that $\mathrm{Pgr}(\mathbb{Z}/4)$ contains $(0,2)$ and $(1,3)$. Now suppose $\mathrm{Pgr}(\mathbb{Z}/4)$ is not generated by $(0,1,2,3)$ and $(1,3)$. Then we need at least one more generator for $\mathrm{Pgr}(\mathbb{Z}/4)$, which we can choose by Proposition 2.4 to have no constant term. But then this generator would leave the set $\{0,2\}$ invariant, and so it would be in the subgroup $\{e, (0,2), (1,3), (0,2)(1,3)\}$, and hence we do not need a new generator after all. □

Over the finite field $\mathbb{F}_q$, every function $\mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial of degree strictly less than q. For other finite rings, as shown by the computation of Proposition 3.2, there are some set endomorphisms that cannot be represented by a polynomial of any degree. Nonetheless, there are only finitely many set endomorphisms of a finite ring.

3.3. **Definition.** For a finite ring R, we define the polynomial function bound on R to be the least upper bound of the set of all d such that every polynomial function $R \to R$ can be represented by a polynomial of degree at most d, and we write $\mathrm{pb}(R)$ for this number.

We can always get an upper bound for $\mathrm{pb}(R)$ by computing the largest integer d such that the polynomial functions $x, x^2, \ldots, x^d$ are all distinct; then $\mathrm{pb}(R) \leq d$. For example, by this method we see that $\mathrm{pb}(\mathbb{Z}/9) \leq 7$ and $\mathrm{pb}(\mathbb{Z}/27) \leq 20$. Since there are only finitely many ring structures on a finite set of a given cardinality, one should be able to express this bound in terms of this cardinality. Using this number, we can compute $\mathrm{Pgr}(R)$ for any finite ring. Since this may be the only method for some finite rings, we illustrate it with an example, using Sage to avoid lengthy hand-computations.

3.4. *Example.* We have

$$\mathrm{Pgr}(\mathbb{Z}/8) \cong (\mathbb{Z}/2)^4 \rtimes D_4.$$

Indeed, we first compute powers of elements in $\mathbb{Z}/8$, which gives us $\mathrm{pb}(\mathbb{Z}/8) \leq 4$. We need three permutations to generate $\mathrm{Pgr}(\mathbb{Z}/8)$: the permutation $(0,1,2,3,4,5,6,7)$ given by $f(x) = x+1$, the permutaiton $(1,3,5,7)(2,6)$ given by $f(x) = x^4 + x^2 + x$, and the permutation $(1,5)$ given by $f(x) = x^4 + x^2 + 3x$.

These permutations generate the group $\mathrm{Pgr}(\mathbb{Z}/8)$ which has order 128. It has a normal subgroup isomorphic to $(\mathbb{Z}/2)^4$ fitting into an exact sequence

$$1 \to (\mathbb{Z}/2)^4 \to \mathrm{Pgr}(\mathbb{Z}/8) \to D_4 \to 1.$$

The subgroup isomorphic to $(\mathbb{Z}/2)^4$ can be generated by the set $\{(3,7), (2,6), (1,5), (0,4)\}$, and the quotient D_4 has coset representatives

$$\{e, (1,3)(5,7), (0,1)(2,3)(4,5)(6,7), (0,1,2,3)(4,5,6,7), (0,2)(4,6),$$
$$(0,2)(1,3)(4,6)(5,7), (0,3,2,1)(4,7,6,5), (0,3)(1,2)(4,7)(5,6)\} \subseteq H.$$

The dihedral group D_4 also has the presentation

$$D_4 = \langle\, r, s \mid r^4, s^2, r^k s = s r^{-k} \,\rangle$$

and an isomorphism to the quotient of $\mathrm{Pgr}(\mathbb{Z}/8)$ is given by

$$r \longmapsto (0,1,2,3)(4,5,6,7)$$
$$s \longmapsto (1,3)(5,7)$$

Similarly, an embedding of $(\mathbb{Z}/2)^4$ into $\mathrm{Pgr}(\mathbb{Z}/8)$ is given by

$$(1,0,0,0) \longmapsto (2,6)$$
$$(0,1,0,0) \longmapsto (3,7)$$
$$(0,0,1,0) \longmapsto (0,4)$$
$$(0,0,0,1) \longmapsto (1,5).$$

The intuition is to think of a square whose vertices are labeled by $(2,6), (3,7), (0,4)$ and $(1,5)$ around going either clockwise or counterclockwise. Using these isomorphisms, the action of D_4 on $(\mathbb{Z}/2)^4$ is given on generators by

$$r * (a,b,c,d) = (d,a,b,c)$$
$$s * (a,b,c,d) = (a,c,b,d)$$

and it gives an explicit isomorphism

$$\mathrm{Pgr}(\mathbb{Z}/8) \cong (\mathbb{Z}/2)^4 \rtimes D_4.$$

These techniques can be used for any finite ring but for larger cardinalities, the computations quickly become prohibitive. Next, we will derive a few results necessary to compute the cardinality of $\mathrm{Pgr}(\mathbb{Z}/p^k)$. We first note that if $f \in \mathbb{Z}/p^k[x]$, not necessarily a permutation polynomial, then

$$f(x+mp) = f(x) + mpf'(x) + (mp)^2 f''(x) + \cdots + (mp)^{k-1} f^{(k-1)}(x) \tag{1}$$

for all $x \in \mathbb{Z}/p^k$ and where f' denotes the formal derivative of f. Therefore, f is actually determined by a choice of $0, 1, \ldots, p-1$ and a choice of derivatives $f^{(i)}(0), \ldots, f^{(i)}(p-1)$ for $i = 0, \ldots, k-1$. Can any such choice be represented by a polynomial? This is the content of a theorem of Carlitz.

3.5. **Theorem** ([Car64, Theorem 3]). *A function $f : \mathbb{Z}/p^k \to \mathbb{Z}/p^k$ can be represented by a polynomial in $\mathbb{Z}/p^k[x]$ if and only if*

$$f(x+mp) = f_0(x) + mpf_1(x) + \cdots + (mp)^{k-1} f_{k-1}(x)$$

for all m and $x = 0, \ldots, p-1$ where each $f_i : \mathbb{Z}/p \to \mathbb{Z}/p^k$ is an arbitrary function.

So any function $f : \mathbb{Z}/p^k \to \mathbb{Z}/p^k$ obtained by choosing $f^{(i)}(0), \ldots, f^{(i)}(p-1)$ for $i = 0, \ldots, k-1$ and extending by Equation (1) can also be defined by a polynomial in $\mathbb{Z}/p^k[x]$.

3.6. **Proposition.** *A function $f : \mathbb{Z}/p^k \to \mathbb{Z}/p^k$ obtained by the method just described is a permutation of $\mathbb{Z}/p^k$ if and only if $f(0), \ldots, f(p-1)$ are all distinct modulo p and $f'(0), \ldots, f'(p-1) \in (\mathbb{Z}/p^k)^\times$.*

Proof. Suppose there exists an $x \in \{0, \ldots, p-1\}$ such that $f'(x) \in (p)$. Choosing $m = p^{k-2}$, we see that

$$f(x+mp) = f(x) + p^{k-1} f'(x) = f(x) \in \mathbb{Z}/p^k.$$

Therefore, the conditions: $f(0), \ldots, f(p-1)$ are all distinct modulo p and $f'(0), \ldots, f'(p-1) \in (\mathbb{Z}/p^k)^\times$ is certainly necessary for the corresponding function to be a permutation.

Now we prove sufficiency. Since $f(x+mp)$ and $f(x)$ are the same modulo p, it suffices to fix an x and show that $f(x), f(x+p), \ldots, f(x+(p^{k-1}-1)p)$ are all distinct. Suppose not. Then there exists distinct $m_1, m_2 \in 0, 1, \ldots, p^{k-1}-1$ such that

$$f(x+m_1p) = f(x+m_2p).$$

Then by Equation (1), we must have

$$0 = p(m_1-m_2)f'(x) + p^2(m_1^2-m_2^2)f''(x) + \cdots + p^{k-1}(m_1^{k-1}-m_2^{k-1})f^{(k-1)}(x).$$

Reducing modulo p^2 we see that $m_1 - m_2 \in (p)$. But then $m_1^2 - m_2^2 \in (p)$ and so reducing modulo p^3 we see that $m_1 - m_2 \in (p^2)$. Continuing along this fashion, using that $m_1^\ell - m_2^\ell$ has $m_1 - m_2$ as a factor, we can conclude that $m_1 - m_2 \in (p^{k-1})$. But we have chosen $m_1, m_2 \in \{0, \ldots, p^{k-1}-1\}$, and so $m_1 = m_2$. Thus f is indeed a permutation. □

Looking at Equation (1) again, we see that to obtain any permutation it suffice to choose $f(0), \ldots, f(p-1)$, exactly one from each coset of the ideal (p) in $\mathbb{Z}/p^k$, an ordering of these cosets, and for $x = 0, 1, \ldots, p$ the elements $f'(x) \in (\mathbb{Z}/p^{k-1})^\times$, and $f^{(\ell)}(x) \in \mathbb{Z}/p^{k-\ell}$ for $\ell > 1$. It is easy to see that this gives

$$p!(p^{k-1})^p[p^{k-2}(p-1)]^p[p^{k-2}p^{k-3}\cdots p]^p = p![(p-1)p^{(k^2+k-4)/2}]^p.$$

many choices. Moreover, we consider all of these choices to be elements of $\mathbb{Z}/p^k$ through the set inclusion (not ring homomorphism!) $\mathbb{Z}/p^\ell \to \mathbb{Z}/p^k$ defined by $n \mapsto n$ for $\ell \leq k$; this is to avoid writing the more cumbersome $0, 1, \ldots, p^\ell \in \mathbb{Z}/p^k$. Do different choices necessarily lead to different permutations? Not necessarily. We have to impose one additional condition for this to be so and this is the content of the next result.

3.7. **Theorem.** *Let p be a prime and $k \geq 2$ be an integer such that $p \geq k$. Then*

$$|\operatorname{Pgr}(\mathbb{Z}/p^k)| = p![(p-1)p^{(k^2+k-4)/2}]^p.$$

Proof. Consider two permutations f and g defined by the aforementioned choices of $f^{(i)}(x)$ for $i = 0, 1, \ldots, k-1$ and $x = 0, 1, \ldots, p-1$. Let us suppose that f and g induce the same permutation on $\mathbb{Z}/p^k$. To prove the theorem we must show that $f^{(i)}(x) = g^{(i)}(x)$ for all $i = 0, \ldots, k-1$ and all $x = 0, 1, \ldots, p-1$ or equivalently, that $d_i = f^{(i)}(x) - g^{(i)}(x) \in \mathbb{Z}/p^k$ is zero for all i.

Since f and g are supposed to be the same, the difference of Equation (1) for f and the analogue for g gives the identity in $\mathbb{Z}/p^k$:

$$0 = mpd_1 + (mp)^2d_2 + \cdots + (mp)^{k-1}d_{k-1}$$

that holds for all m. Let $m_1, \ldots, m_{k-1}$ be arbitrary. For each m_i, we obtain an identity, all of which collectively can be expressed in matrix notation:

$$0 = \begin{bmatrix} m_1 & m_1^2 & \cdots & m_1^{k-1} \\ m_2 & m_2^2 & \cdots & m_2^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{k-1} & m_{k-1}^2 & \cdots & m_{k-1}^{k-1} \end{bmatrix} \begin{bmatrix} pd_1 \\ p^2d_2 \\ \vdots \\ p^{k-1}d_{k-1}. \end{bmatrix} \tag{2}$$

The determinant of the matrix with i,j-entry m_i^j is just a variant of the Vandermonde matrix; its determinant is

$$\prod_i m_i \prod_{i>j}(m_i - m_j).$$

The identity in (2) shows that this determinant annihilates $p^\ell d_\ell$ in the ring $\mathbb{Z}/p^k$. Because we have assumed that $p \geq k$, we can choose $m_1, \ldots, m_{k-1}$ in the set $\{1, 2, \ldots, p-1\}$ all *distinct*, and so consequently $p^\ell d_\ell = 0$. But $d_\ell \in \{0, 1, 2, \ldots, p^{k-\ell} - 1\}$ and hence $d_\ell = 0$. □

3.8. *Remark.* The same proof idea does not seem to work for $p < k$ because the determinant annihilating $p^\ell d_\ell$ will only give a lower bound in this case. In fact, we recall Example 3.4 that $|\operatorname{Pgr}(\mathbb{Z}/2^3)| = 2^7$, whereas putting $p = 2$ and $k = 3$ in Theorem 3.7 gives the number 2^9.

3.9. **Theorem.** *Let p be a prime and let the group $(\mathbb{Z}/p)^\times$ act on the group $\mathbb{Z}/p$ by multiplication. Let Δ_p act on the p-fold products $(\mathbb{Z}/p^\times)^p$ and $(\mathbb{Z}/p)^p$ via permuting the coordinates. Then there exists an isomorphism*

$$\operatorname{Pgr}(\mathbb{Z}/p^2) \cong ((\mathbb{Z}/p)^p \rtimes [(\mathbb{Z}/p)^\times]^p) \rtimes \Delta_p$$

Proof. For a polynomial permutation f on $\mathbb{Z}/p^k$, let σ_f be the permutation that f induces on $\mathbb{Z}/p$. By our previous discussion, to give f is the same thing as to give σ_f, elements $a_0, \ldots, a_{p-1} \in \mathbb{Z}/p$, and elements $f_0, \ldots, f_{p-1} \in (\mathbb{Z}/p)^\times$, which defines f by the conditions that

$$\begin{aligned} f(x) &= \sigma_f(x) + a_x p \\ f(x + mp) &= f(x) + mpf_x \end{aligned} \tag{3}$$

for $x = 0, \ldots, p-1$ and m arbitrary. Then it follows that $f(x + mp) = f(x) + mpf_y$ where $y \in \{0, \ldots, p-1\}$ and $y \equiv x \pmod p$. Consider the map:

$$\begin{aligned} \operatorname{Pgr}(\mathbb{Z}/p^2) &\longrightarrow ((\mathbb{Z}/p)^p \rtimes [(\mathbb{Z}/p)^\times]^p) \rtimes \Delta_p \\ f &\longmapsto \big((a_0, \ldots, a_{p-1}), (f_0, \ldots, f_{p-1}), \sigma_f\big) \end{aligned}$$

Theorem 3.7 shows that this map is a bijection. To show that it is a homomorphism we compute the product of two elements in the iterated semidirect product: Suppose g is another polynomial permutation defined by constants $b_i \in \mathbb{Z}/p, g_i \in (\mathbb{Z}/p)^\times$, and σ_g. Then

$$\begin{aligned} [(a_i), (f_i), \sigma_f][(b_i), (g_i), \sigma_g] &= (\sigma_f * ((b_i), (g_i)) + (a_i, f_i), \sigma_g \circ \sigma_f) \\ &= [((b_{\sigma_f(i)}), (g_{\sigma_f(i)}))((a_i), (f_i)), \sigma_g \circ \sigma_f] \\ &= [(b_{\sigma_f(i)} + g_{\sigma_f(i)} a_i), (g_{\sigma_f(i)} f_i), \sigma_g \circ \sigma_f]. \end{aligned}$$

On the other hand, by directly using the formulas in (3), we see that:

$$\begin{aligned} (g \circ f)(i) &= g(\sigma_f(i) + a_i p) \\ &= (\sigma_g \circ \sigma_f)(i) + p(b_{\sigma_f(i)} + a_i g_{\sigma_f(i)}). \end{aligned}$$

and $(g \circ f)(i + mp) = (g \circ f)(i) + mpf_i g_{\sigma_f(i)}$. □

The same proof will not work for $k > 2$; the problem is that the structure of the group $\mathrm{Pgr}(\mathbb{Z}/p^k)$ is more complicated and it is not clear to the author if there is any nice presentation of it. Nonetheless, we emphasize that with Theorem 3.7, it is possible to write a fairly fast algorithm that will determine all the generators of $\mathrm{Pgr}(\mathbb{Z}/p^k)$ for any k as a subgroup of Δ_{p^k}.

3.10. *Remark.* A polynomial permutation of $\mathbb{Z}/p^k$ also induces a permutation of $\mathbb{Z}/p^\ell$ for $\ell = 1, \ldots, k$ by Proposition 2.6. Inspired by this fact, is is tempting to introduce the following definition: Let R be a commutative ring and I an ideal of R. We say that a permutation of R/I^k is an **I-fractal permutation** of R/I^k if it induces permutations of R/I^ℓ for $\ell = 1, \ldots, k$. If the ideal is understood, we simply say **fractal permutation**. Let us write $\mathrm{Fpg}_I(R/I^k)$ for the group of I-fractal permutations of R/I^k.

As we have said, permutation polynomials in $\mathbb{Z}/p^k[x]$ induce fractal permutations of $\mathbb{Z}/p^k$. However, the converse is false in general! Indeed, the following fractal permutation of $\mathbb{Z}/27$ is not given by any polynomial:

$$(0,5)(1,13,7,10,4,25)(2,15,8,3,11,24,17,21,20,6,26,12)(9,14,18,23)(16,19,22)$$

In fact $\mathrm{Pgr}(\mathbb{Z}/p^k)$ is usually a proper subgroup of $\mathrm{Fpg}_p(\mathbb{Z}/p^k)$. Now, using the notion of fractal permutation, we can define the I-fractal permutation group of R, or the fractal permutation group of the pair (R, I) as the limit

$$\mathrm{Fpg}_I(R) := \varprojlim_k \mathrm{Fpg}_I(R/I^k).$$

The structure and meaning of this group are still mysterious, but we leave this for future research.

References

[Ash93] Daniel A. Ashlock. Permutation polynomials of abelian group rings over finite fields. *Journal of Pure and Applied Algebra*, 86:1–5, 1993.

[Car64] Leonard Carlitz. Functions and polynomials (mod p^n). *Acta Arithmetica*, IX:67–78, 1964.

[CH72] Leonard Carlitz and D.R. Hayes. Permutations with coefficients in a subfield. *Acta Arithmetica*, XXI:131–135, 1972.

[LN00] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 2000.

[Riv01] Ronald L. Rivest. Permutation polynomials modulo 2^w. *Finite Fields and Their Applications*, 7:287–292, 2001.

School of Mathematics and Statistics, The University of Melbourne, Parkville, Victoria 3010, Australia

E-mail address: jpolak@jpolak.org