A Theory of Permutation Polynomials Using Compositional Attractors

Thesis by
Daniel Abram Ashlock
In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1990
(Submitted May 7, 1990)

Acknowledgments

Warm thanks go to my friend and colleague Jack Lutz who accidentally shoved me toward this thesis with his question, "Aren't the first two congruent to the third mod two?" Thanks go to James Cummings who read this work in its early stages and with whom I had many stimulating discussions. I must credit Heeralal Janwa with providing me with many useful references.

My committee deserves thanks for their investment of time, both in sitting on my committee and in training me in mathematics. I want especially to thank Michael Aschbacher, who read the work in progress and corrected my many blunders in group theory, Dinakar Ramakrishnan, who suggested many topics for future application of my work, and Richard Wilson, my advisor, who has supervised my work for the last four years and has taught me much delightful and beautiful combinatorics.

I must also thank my wife, Wendy, who has been substantially inconvenienced by my graduate studies and nonetheless provided love and support, and my father, Peter Dunning Ashlock, who died while I was working on this thesis. More than any other person he trained me in the philosophy and methods of science and gave me my direction through life.

Table of Contents

Copyright ii
Acknowledgments iii
Table of Contents iv
List of Tables vi
List of Examples vii
Introduction and Summary 1
Chapter
I. Definitions and Basic Results. 6
§0. Introduction and Summary. 6
§1. Equivalence Results. 9
§2. Lifting and Decomposition Lemmas. 12
§3. Properties of Compositional Attractors. 14
II. Results for Finite Fields and the Integers. 16
§0. Introduction and Summary. 16
§1. Compositional Attractors of $GF(p^n)[x]$. 17
§2. The Order of Finite Permutation Polynomial Groups with Finite Field Coefficents. 22
§3. Compositional Attractors of $\mathbf{Z}[x]$. 29
III. The Groups $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$ and $PP_{\mathbf{Z}_n}(\mathbf{Z}_n^{m\times m})$. 35
§0. Introduction and Summary. 35
§1. Singmaster's Result. 37
§2. A Basis for the Ideal $I_{\mathbf{Z}}^{\mathbf{Z}_n}$. 40
§3. The Group $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$. 44
§4. Computation of the Ideal $I_{\mathbf{Z}_n}^{\mathbf{Z}_n^{m\times m}}$. 56
§5. Membership and Enumeration of the Group $PP_{\mathbf{Z}_n}(\mathbf{Z}_n^{m\times m})$. 65

IV. Applications and Topics for Future Work. 72

§0. Introduction and Summary. 72

§1. The Permutation Polynomials of the p-adic Integers. 73

§2. Permutation Polynomials of Abelian Group Algebras over Finite Fields. 74

§3. Questions for Further Study. 78

Appendices

A Explicit Examples of Polynomial Groups. 80

The Group Sym(GF(5)) Realized as Polynomials. 80

The Stabilizer of 0 in $PP(\mathbf{Z}_9)$ 83

B Tables of special functions. 86

C Certain Permutation Polynomial Groups. 88

References 89

List of Tables

Table 3.1, Values of $\kappa(n)$ 41

Table 3.2, Order of $PP_m(\mathbf{Z}_n)$ 71

The Symmetric Group on GF(5) as Cycle and Polynomials 80

Values of $\pi(n)$ 83

Values for $\kappa_m(n)$ 84

List of Examples

Example 1.1, Permutation Polynomials of a Finite Field 7

Example 1.2, A Homomorphism of Polynomial Groups 15

Example 2.1, Compositional Attractors of a Subfield 20

Example 2.2, Compositional Attractors for Matrices over GF(q) 20

Lemma 2.1, The Compositional Attractor of a Polynomial Modular Algebra 20

Example 2.3, An Irreducible of $\mathbf{Z}_{p^n}[x]$ that Factors Modulo p 33

Example 2.4, A Family of Compositional Attractors of $\mathbf{Z}[x]$ 34

Example 3.1, Generators for I_{12}, I_{128} 43

Example 3.2, Computation of a Least Degree Common Multiple 58

Example 4.1, The GF(2)-Permutation Polynmials of GF(2)[C_3] 76

Appendix A, Example 4.2, The number of GF(3)-Permutation Polynomials of GF(3)[C_6] 77

The GF(5)-permutation polynomials of GF(5) as cycles and polynomials of least possible degree 80

Introduction and Summary

In this work I will develop a theory of permutation polynomials with coefficents over finite commutative rings. The general situation will be that we have a finite ring R and a ring S, both with 1, with S commutative, and with a scalar multiplication of elements of R by elements of S, so that for each r in R $1_S \cdot r = r$ and with the scalar multiplication being R bilinear. When all these conditions hold, I will call R an S-algebra. A *permutation polynomial* will be a polynomial of S[x] with the property that the function $r \mapsto f(r)$ is a bijection, or permutation, of R.

Presented here, as far as I know for the first time, is the idea that compositional attractors are integral to the study of permutation polynomials. A *compositional attractor* is an ideal I in a polynomial ring S[x] with the added property that

$$\forall f(x) \in I \; \forall g(x) \in S[x] \left(f(g(x)) \in I \right).$$

There are several reasons that compositional attractors are important.

First of all, a compositional attractor of S[x] is exactly an ideal comprised of the polynomials that are zero everywhere on some S-algebra, i.e., it is the kernal of the representation of S[x] as a ring of functions over R. This means that they capture the equivalence relation associating polynomials that give the same permutation. Such a ideal, zero everywhere on an S-algebra, is called the *compositional attractor associated with an S-algebra.*

Second, polynomial composition modulo an ideal forms a monoid if and only if that ideal is a compositional attractor. One consequence of this is that the polynomials with the identity polynomial $f(x) = x$ in their composition sequence modulo a compositional

attractor form a group under composition.

Third, two S-algebras with the same associated compositional attractors in S[x] necessarily have identical permutation polynomials in S[x]. Since it is often easier to compute a compositional attractor associated with an algebra than to compute the permutation polynomials directly, this gives a powerful tool for locating and enumerating the permutation polynomials of certain S-algebras.

Fourth, if $J \trianglelefteq S[x]$ is a compositional attractor, then S[x]/J is an S-algebra with associated compositional attractor J. This fact gives a canonical domain in which to perform computations. This fact, while quite easy to prove, is of great utility in classifying the permutation polynomial groups when S is taken to be a finite field.

In addition, taken together with the third point, this fourth fact has a wonderful consequence. In a rather nice paper, "Polynomials Over a Ring That Permute the Matrices Over That Ring,"[10] Brawley spends not inconsequential effort doing matrix arithmetic to prove a theorem that characterizes scalar permutation polynomials of matrices. It turns out that in specific instances an alternate proof is possible in which one first computes the associated compositional attractor for the matrix ring and then does the computations in the corresponding canonical algebra, which is commutative.

This thesis is presented in four chapters. The first chapter develops, in abstract, the properties of compositional attractors mentioned above, along with a few other straightforward properties. The set of compositional attractors of a polynomial ring is, for example, closed under intersection and multiplication of ideals.

The second chapter focuses on the cases when S is a finite field or the integers. In the first section I classify the compositional attractors of F[x] for any finite field F. In the second section I compute the size of the permutation polynomial groups that arise modulo these compositional attractors. The work in the second section is essentially a generalization, with new terminology, of a paper, "Permutations with Coefficients in a Subfield,"[9] by L. Carlitz and D. R. Hayes, which treats the case where R is a field and S is a subfield R. In the third section I give a few useful lemmas about the compositional attractors of $\mathbf{Z}$[x] and present an example.

The third chapter explores the situation when S is the integers or the integers modulo n and R is taken to be either the integers modulo n or matrices over the integers modulo n. In the first section I present a new proof, based on the difference operator $\Delta f(x) = f(x+1)-f(x)$ of Singmaster's formula[4] for the number of polynomial functions from $\mathbb{Z}_n$ to itself. In the second section I give a new proof, also with the difference operator, of Niven and Warren's[6] basis theorem for the compositional attractor in $\mathbf{Z}_n$[x] associated with $\mathbf{Z}_n$. In the third section I count the $\mathbf{Z}_n$-permutation polynomials of $\mathbf{Z}_n$, give the isomorphism type of the group for cube-free integers n, and give some information about the isomorphism type of the group for all n.

In the fourth section I compute a basis for the compositional attractor of $\mathbb{Z}_n$[x] associated with the matrices over $\mathbf{Z}_n$ and use the basis to count the number of $\mathbb{Z}_n$-polynomial functions from $\mathbf{Z}_n^{m \times m}$ to itself. In the fifth section I reprove Brawley's[10] characterization of $\mathbf{Z}_n$-permutation polynomials of the matrices over $\mathbf{Z}_n$ and go on to enumerate the group of such polynomials for each n.

In the fourth chapter I skip lightly over easy consequences of the material developed in the first three chapters and give topics for future research. In Section one I compute exactly the membership of the p-adic permutation polynomials of the p-adic integers. In Section two I compute the compositional attractors of F[x] associated with F[G] and count the groups of F-permutation polynomials of F[G] where F is a finite field, G is an abelian group, and F[G] is the group algebra of F over G. As one might expect, the case where the characteristic of F divides the order of G is the hard one, but not too hard. In Section three I define multivariate compositional attractors and give a list of topics for future consideration.

I more or less stumbled into this thesis topic accidentally. In the summer of 1986 I was trying to find some algebraic structure in the rules for generating cellular automata. This is a relatively futile pursuit, but in the process I discovered a number of properties of functions from $\mathbf{Z}_n$ to $\mathbf{Z}_n$. I also reproduced Singmaster's results from[4]. At this point Heeralal Janwa arrived at Caltech for a two-year stint. While I was trying to explain to him what I was working on he said, "This sounds very much like permutation polynomials."

This gave me an application for the material I had developed on functions over $\mathbf{Z}_n$. In particular, the difference operator $\Delta_k f(x) = f(x+k)-f(x)$ leads to nice slick proofs of some known results, contained in the first two sections of Chapter three. I spent a great deal of computer time computing the membership and structure of groups of permutation polynomials over $\mathbf{Z}_n$. In the end I had the membership, size, and some structural information about the groups in question, but not enough material for a

thesis. My advisor, Richard Wilson, suggested that I generalize to the matrix case.

Now the matrix case is severely resistant to computer scans. The problem of computing a least degree monic polynomial zero everywhere on two-by-two matrices over $\mathbf{Z}_4$ is about the limit of what you can do on a personal computer unless you prove some theorems. In addition, many of the nice proofs in the non-matrix case depend heavily on the commutativity of $\mathbf{Z}_n$. At this point I uncovered the material by Brawley, Carlitz, Levine, and others [8], [10], [11]. Their theorems were often theorems that would be true if matrices commuted. In other words, they would have two, essentially identical, theorems for commutative and noncommutative rings with substantially different proofs. At this point, inspired by [9], I decided to leave the matrix case alone and to try computing permutation polynomials over finite commutative rings. The first step in this process was computing the ideal of polynomials zero everywhere on the ring.

I used a computer to find this ideal for a large number of examples, particularly for group algebras over finite fields, which are easy to implement on a computer. At this point I noticed that many different algebras can have the same zeroing ideals and, more importantly, that when they do, they also have the same permutation polynomials. I set out to prove this and in the process was forced into considering the notion of compositional attractors.

After a few months in which I roughed out the material presented in Chapter two, I realized that compositional attractors solved my problem with the matrix case. The theory of compositional attractors gave me a way to construct a commutative algebra with the exact same compositional attractor and hence permutation polynomials as any given noncommutative algebra. Developing this idea put the thesis in more or less its current form.

Chapter 1

Definitions and Basic Results

§0 Introduction and Summary.

Throughout this chapter S will be a commutative ring with 1, and R will be a finite S-algebra with 1. By I_S^R I will denote the set

$$\left\{f(x)\varepsilon S[X] : \forall r\varepsilon R,\ f(r) = 0\right\}.$$

That I_S^R is an ideal of S[X] is elementary; I sometimes call it the S-zeroing ideal of R. F(R, R) denotes the set of functions from R to itself, which I will treat as both a monoid under functional composition and an algebra under the usual extension of the addition and multiplication on R and scalar multiplication by S. I denote by $\epsilon_S^R : S[X] \to F(R, R)$ the evaluation map; i.e., $f(x) \mapsto \left(r \mapsto f(r)\right)$. Note that ϵ_S^R is both a monoid and an algebra homomorphism. The kernel of ϵ_S^R as a monoid homomorphism is $\left\{x+f(x) : f(x)\varepsilon I_S^R\right\}$. As an algebra homomorphism ϵ_S^R has kernel I_S^R. I will denote by $F_S(R)$, the *S-polynomial functions on R*, the image of ϵ_S^R, which is both a submonoid and subalgebra of F(R, R). I will denote by $PP_S(R)$, the *S-permutation polynomials on R*, the subset of $F_S(R)$ that are invertible (bijective) members of the monoid $F_S(R)$. Notice that $PP_S(R)$ is a submonoid of $F_S(R)$ but is *not* a subalgebra of $F_S(R)$. Notice also that the choice of invertible elements makes $PP_S(R)$ a group under composition. Finally, if U is a ring of functions call an ideal I of U a *compositional attractor* if for all $f\varepsilon I$ and for all $g\varepsilon U$, we have $f\circ g\ \varepsilon\ I$, where $\circ$ denotes functional composition.

As motivation for these definitions, I would like to give an overview of the use I will put them to and illustrate it with a basic example. Having fixed R and S, the first problem is to compute the membership of I_S^R and produce, if possible, a nice set of generators for it. Once we have I_S^R it is easy to enumerate $F_S(R)$ and to find, as a side effect, its structure as an S-module. Using results from this chapter, I can often go on

to compute the membership of $PP_S(R)$ and subsequently enumerate $PP_S(R)$. Finally, where possible, I will determine the isomorphism type of the group $PP_S(R)$. For example, if we choose $R = GF(q)$, the field with q elements, and choose $S=R$, then we see immediately from the theory of finite fields, that

Example 1.1.

(i) $I_S^R = \langle x^q - x \rangle$,

(ii) $|F_S(R)| = q^q$,

(iii) $F_s(R)$ can be given the structure of a q-dimensional vector space over S,

(iv) $|PP_S(R)| = q!$

(v) $PP_S(R) \cong Sym(R)$, the group of all permutations of R.

These particular results, while both easy and elementary, are central to the theory of permutation polynomials over a finite commutative ring. The theory of Jacobson radicals tells us that a finite commutative ring modulo its radical is a direct product of finite fields. In this section we observe that for any finite S-algebra R, we may find a commutative S-algebra R', so that $PP_S(R) \cong PP_S(R')$ and that a direct product decomposition of S often induces a direct product decomposition of $PP_S(R)$. Taken together these results make the above example broadly applicable.

On the other hand, when R has a nontrivial Jacobson radical, many interesting things happen that prevent the permutation polynomial groups in question from being merely direct products of symmetric groups. In this instance the utility of the above results follow from the observation that the natural homomorphism of R modulo its Jacobson radical onto an S-algebra with semisimple ring structure induces a group homomorphism of the corresponding permutation polynomial groups.

§1 Equivalence Results.

In this section I will prove several lemmas that allow me to export calculation done for one choice of R and S to others.

Lemma 1.1. For a polynomial $f(x) \varepsilon S[x]$, let $f^{(n)}(x)$ denote composition of f(x) with itself n times. Then:

(i) $PP_S(R) = \left\{f(x)\epsilon_S^R : \exists n\ f^{(n)}(x) \equiv x \pmod{I_S^R}\right\}$, or equivalently

(ii) $PP_S(R) \cong \left\{f(x) \varepsilon S[X]/I_S^R : \exists n\ f^{(n)}(x) \equiv x\right\}$, as a group under composition mod I_S^R.

Proof:

Suppose for $f(x)\varepsilon S[x]$ that $\exists n\ f^{(n)}(x) \equiv x \pmod{I_S^R}$. Then since ϵ_S^R is a monoid homomorphism, it follows that the n-fold composition of $f(x)\epsilon_S^R$ with itself is the identity function on R. This requires $f(x)\epsilon_S^R$ itself to be a bijective function; hence $PP_S(R) \supseteq \left\{f(x)\epsilon_S^R : \exists n\ f^{(n)}(x) \equiv x \pmod{I_S^R}\right\}$. Suppose instead that $f(x)\epsilon_S^R \varepsilon PP_S(R)$. Then since $f(x)\epsilon_S^R$ is a bijection of a finite set, we see that for some n the n-fold composition of $f(x)\epsilon_S^R$ with itself is the identity function. The identity function in $F_s(R)$ is clearly $x+I_S^R$; hence x is among the preimages of $f^{(n)}(x)$ under ϵ_S^R and we see $f^{(n)}(x) \equiv x \pmod{I_S^R}$. This shows that $PP_S(R) \subseteq \left\{f(x)\epsilon_S^R : \exists n\ f^{(n)}(x) \equiv x \pmod{I_S^R}\right\}$. Thus we have (i). To see that (ii) is a restatement of (i), notice that ϵ_S^R has kernel I_S^R as a ring homomorphism. □

Lemma 1.2. Suppose for R, R′, both S-algebras, we have that $I_S^R = I_S^{R'}$. Then $PP_S(R) \cong PP_S(R')$.

Proof:

From Lemma 1.1 (ii) we see

$$PP_S(R) \cong \left\{f(x) \in S[X]/I_S^R : \exists n\ f^{(n)}(x) \equiv x\right\}.$$

Since $I_S^R = I_S^{R'}$, we see

$$\left\{f(x) \in S[X]/I_S^R : \exists n\ f^{(n)}(x) \equiv x\right\} = \left\{f(x) \in S[X]/I_S^{R'} : \exists n\ f^{(n)}(x) \equiv x\right\},$$

and applying Lemma 1.1 (ii) again we see

$$\left\{f(x) \in S[X]/I_S^{R'} : \exists n\ f^{(n)}(x) \equiv x\right\} \cong PP_S(R');$$

hence $PP_S(R) \cong PP_S(R')$. □

The next result is somewhat more substantial and completes the tools to make good on my boast in Section 0 to reduce the problem of computing arbitrary finite S-algebras to the commutative case.

Theorem 1.1. Let R be an S-algebra, let J be a compositional attractor of S[x], and let $T = S[x]/I_S^R$. Then

(i) I_S^R is a compositional attractor of S[x].

(ii) $A = S[x]/J$ is an S-algebra with $I_S^A = J$.

(iii) $PP_S(R) \cong PP_S(T)$.

Proof:

Let $f(x) \in I_S^R$ and let $g(x) \in S[x]$. By definition $f\epsilon_S^R$ is the zero function on R. Since ϵ_S^R is a monoid homomorphism, it follows that $(f \circ g)\epsilon_S^R = \left(f\epsilon_S^R\right) \circ \left(g\epsilon_S^R\right) = 0 \circ \left(g\epsilon_S^R\right) = 0$. This means $(f \circ g) \in \ker(\epsilon_S^R)$ viewed as an algebra homomorphism; hence $(f \circ g) \in I_S^R$, and we see that I_S^R is a compositional attractor.

Notice that the scalar multiplication of S on A is induced by the scalar multiplication of S on S[x]. Now suppose $f(x) \in I_S^A$. Then $\forall g(x)+J \in S[x]/J$; we see from the definition of I_S^A that $f(g(x)+J) = 0$. If we expand $f(g(x)+J)$, we see that this implies

that $f(g(x)) \in J$. Specialize $g(x)$ to x and note $f(x) \in J$; hence $I_S^A \subseteq J$. Now, recalling the definition of compositional attractor, we see for $f(x) \in J$ and any $g(x) \in S[x]$, that $f(g(x)) \in J$; hence $f(g(x)+J) = 0$ in A, and thus $J \subseteq I_S^A$. Combining the two previous inclusions, we see $I_S^A = J$.

Finally, set $J = I_S^R$, so $A = T$ Then (ii) tells us that $I_S^R = I_S^T$. Then by Lemma 1.2 we see that $PP_S(R) \cong PP_S(T)$. □

Notice that while my primary reason for proving this theorem is to allow calculations for a noncommutative R to take place in the commutative domain $S[x]/I_S^R$, this theorem potentially allows me to use other special properties of S[x] besides commutativity. Additionally, part (iii) makes it meaningful to speak of the permutation polynomials that arise modulo a compositional attractor, as in Lemma 1.1. I will conclude this section with the following corollary, which ilustrates the breadth of Theorem 1.1.

Corollary 1.1. An ideal J of S[x] is a compositional attractor iff there exists R, an S-algebra, so that $J = I_S^R$.

Proof:

($\Rightarrow$) Set $R = S[x]/J$ and apply Theorem 1 (ii).

($\Leftarrow$) Theorem 1 (i).

§2 Lifting and Decomposition Lemmas.

In this section I will give a lemma that allows the computation of the permutation polynomials of R from the permutation polynomials of R modulo its Jacobson Radical. For R with nontrivial direct product decomposition, I will give a sufficient condition to induce a direct product decomposition of $PP_S(R)$.

Lemma 1.3 (Lifting Lemma). Let J be a nontrivial nilpotent ideal of R and set A = R/J. Then for $f(x) \in S[X]$ we have that $f(x)\epsilon_S^R \in PP_S(R)$ iff $f(x)\epsilon_S^A \in PP_S(A)$ and for each $a \in A$, for each element $j \in J\backslash\{0\}$, $j\cdot f'(a)$ has the same degree of nilpotency as j.

Proof:

First I claim that for any $f(x) \in S[x]$, $f(x)\epsilon_S^R$ is a function that preserves equivalence classes (mod I) for any ideal I of R. To see this, let $r \in R$, $j \in I$ and compute $f(r+j)-f(r) = j\cdot f'(x)+j^2\cdot\frac{1}{2}f''(x)+\cdots \in I$. With this claim we can now prove the lemma.

($\Rightarrow$) Since $f(x)\epsilon_S^R$ is 1:1 on R, the claim forces $f(x)\epsilon_S^A$ to be 1:1 on A; hence $f(x)\epsilon_S^A \in PP_S(A)$. Suppose there exist $j \in J\backslash\{0\}$, $a \in A$ so that $j\cdot f'(a)$ has a higher degee of nilpotency than j. Well, then $a = r+J$. Set $\alpha = f(r+j)-f(r) = j\cdot f'(r)$. Then $f(x) \notin PP_S(R/\langle\alpha\rangle)$. Since $f(x)\epsilon_S^R$ is 1:1 on R, the claim forces $f(x)\epsilon_S^{R/\langle\alpha\rangle}$ to be 1:1, a contradiction, and the right implication is finished.

($\Leftarrow$) Suppose for $r, s \in R$ that $f(r) = f(s)$. Then from the claim we see that $r \equiv s$ (mod J). From this we see there exists some $j \in J$ so that $s = r+j$. So $f(r)-f(r+j) = 0$, which a simple computation shows is equivalent to the statement,

$$j\cdot f'(r)+j^2\cdot\tfrac{1}{2}f''(r)+\cdots = 0.$$

Since, by hypothesis, $j\cdot f'(r)$ has the same degree of nilpotency as j, it follows that

$$j\cdot f'(r) \neq -\left(j^2\cdot\tfrac{1}{2}f''(r)+\cdots\right),$$

unless j=0. From this we see that r = s; hence $f(x)\epsilon I_S^R \varepsilon PP_S(R)$.

Lemma 1.4. (Decomposition Lemma). Suppose that $R = R_1 \otimes R_2$ is a direct product decomposition of R. Then

(i) If $I_S^{R_1}$ and $I_S^{R_2}$ are relatively prime ideals in S[x], then

$$PP_s(R_1) \cong PP_s(R_1) \otimes PP_s(R_2),$$

(ii) $I_S^R = I_S^{R_1} \cap I_S^{R_1}$, and

(iii) both (i) and (ii) may be applied inductively to arbitrary finite direct products.

Proof:

(i) Since $I_S^{R_1}$ and $I_S^{R_2}$ are relatively prime, we see that the Chinese Remainder Theorem gives us an S-algebra isomorphism

$$\lambda: S[x]/I_S^{R_1} \otimes S[x]/I_S^{R_2} \to S[x]/I_S^R.$$

Notice that $(x+I_S^{R_1}, x+I_S^{R_2})\lambda = x+I_S^R$; hence the characterization of permutation polynomials given in Lemma 1.1 (ii) and the fact that the polynomial composition involved is a combination of addition and multiplication of the sort preserved by λ, tell us that λ is a bijection of $PP_s(R_1) \otimes PP_s(R_2) = PP_s(R)$ that preserves the group operation.

(ii) Clearly a polynomial in S[x] is zero everywhere on R when and only when it is zero everywhere on R_1 and R_2.

(iii) Follows by induction.

§3 Properties of Compositional Attractors.

Compositional attractors are central to the study of permutation polynomials over finite rings. As we saw in Section 1 many different S-algebras can have the same permutation polynomials exactly as they share the same S-zeroing ideal. In this section I will develop a few properties of compositional attractors.

Notice that any ideal of S injected in the natural fashion into S[x] is a compositional attractor of S[x], with the corresponding group of permutation polynomials, as in Lemma 1.1, being the trivial group {x}. Such a compositional attractor is called trivial; all others are called nontrivial.

As we saw in the comments subsequent to Theorem 1, each compositional attractor I of S[x] has a permutation polynomial group attached to it, acting on the elements of S[x]/I. I will introduce the shorthand $G_S(I) := PP_S(S[x]/I)$ for this group.

Lemma 1.5. Suppose that I, J are compositional attractors of S[x]. Then $I \cap J$ and $I \cdot J$, their intersection and product, are also compositional attractors.

Proof: Elementary calculation.

Lemma 1.6. Suppose that I is a compositional attractor of S[x] and that $\pi : S \to T$ is a ring homomorphism with $\overline{\pi} : S[x] \to T[x]$ being the natural extension of π to polynomials. Then $I\overline{\pi}$ is a compositional attractor of T.

Proof:

Polynomial composition is a combination of multiplication and addition of ring elements by one another or by powers of the variable, all operations preserved by $\overline{\pi}$,

hence $\overline{\pi}$ preserves composition of polynomials. □

Lemma 1.6 raises the natural question: Is there any connection between the groups of permutation polynomials $G_S(I)$ and $G_T(I\overline{\pi})$? The answer is yes, as demonstrated in the following lemma, which implies the existence of a functor from the category of S-algebras to the catgory of groups.

Lemma 1.7. Let S, T, π, $\overline{\pi}$, be as above and set $R = S[x]/I$ and $A = T[x]/I\overline{\pi}$. Then there is a well-defined map ρ: $F_S(R) \to F_T(A)$ induced by $\overline{\pi}$ that agrees with $\overline{\pi}$ so as to make $f(x)\overline{\pi}\epsilon_T^A = f(x)\epsilon_S^R\rho$ and which has the additional property that $\omega = \rho|_{G_S(I)}$ is a group homomorphism of $G_S(I)$ with $G_T(A)$.

Proof:

Since I is a compositional attractor, Theorom 1 (ii) tells us that $\ker(\epsilon_S^R)\overline{\pi} = \ker(\epsilon_T^A)$. This is sufficient to show that ρ exists. Since ρ agrees with $\overline{\pi}$ and $\overline{\pi}$ preserves polynomial composition, we see that ρ is a monoid homomorphism of $F_S(R)$ into $F_T(A)$. A monoid homomorphism necessarily induces a group homomorphism on the groups of invertible elements; hence ω exists as specified.

Example 1.2.

Let $S = \mathbf{Z}_{p^2}$, $T = \mathbf{Z}_p$, and let π be the natural map with kernel $<p>$. If we take $I = I_{\mathbf{Z}_{p^2}}^{\mathbf{Z}_{p^2}}$, then Lemma 1.7 tells us there is a group homomorphism $\omega : PP_{\mathbf{Z}_{p^2}}(\mathbf{Z}_{p^2}) \to PP_{\mathbf{Z}_p}(\mathbf{Z}_p)$ given by $f(x)+I_{\mathbf{Z}_{p^2}}^{\mathbf{Z}_{p^2}} \mapsto f(x)+I_{\mathbf{Z}_p}^{\mathbf{Z}_p}$. In plainer language, a polynomial over $\mathbf{Z}_{p^2}$ that permutes $\mathbf{Z}_{p^2}$, is (mod p) a polynomial over $\mathbf{Z}_p$ that permutes $\mathbf{Z}_p$.

Chapter 2

Results for Finite Fields and the Integers.

§0 Introduction and Summary.

In this chapter I will discuss results where the coefficient ring is the integers. I refer to such compositional attractors and permutation polynomials as *scalar*. In some cases I will give generalizations of results when such generalization is without cost. For example, the results on prime finite fields, which I require for the integer case, can be done for all finite fields just as easily. Every finite ring with 1 clearly forms a $\mathbb{Z}$-algebra and hence has scalar polynomial functions and scalar permutation polynomials.

In Section 1 I will give a classification of all compositional attractors of $GF(p^n)[x]$, p prime, as well as several examples of attractors tied to specific $GF(p^n)$-algebras. In Section 2 I will use the classification of compositional attractors to give a complete list of orders of permutation polynomial groups with coefficients in $GF(p^n)$. In Section 3 I will address the question of compositional attractors of $\mathbb{Z}[x]$ in terms of compositional attractors of $\mathbb{Z}_{p^n}[x]$.

§1 Compositional Attractors of $GF(p^n)[x]$.

In this section $F = GF(p^n)$, and let $q = p^n$. Since $F[x]$ is a principal ideal domain the search for compositional attractors in $F[x]$ is reduced to the problem of finding polynomials $f(x)$ with the property $f(x) \mid f(g(x))$ for all $g(x) \in F[x]$. This property has modest application to factorization theory. One question of interest, for example, is to determine when a composition of irreducible polynomials is itself irreducible. As we will see this section tells us that there are many instances when the composition of irreducibles is not irreducible.

Theorem 2.1. A polynomial $f(x) \in F[x]$ generates a compositional attractor iff it is a product of least common multiples of polynomials of the form $\left(x^{q^k} - x\right)$.

Proof:

($\Leftarrow$) Notice that if $Q = GF(q^k)$, then $(x^{q^k} - x)$ generates I_F^Q; hence by Lemma 1.5 all polynomials of the given form generate compositional attractors, as intersecting ideals is equivalent to taking the least common multiple of their generators, and multiplying ideals is the same as multiplying their generators.

($\Rightarrow$) Let $I = \langle c(x) \rangle$ be a compositional attractor of $F[x]$, set $A = F[x]/I$, and suppose that $f(x) \in F[x]$ is irreducible so that $f^n(x)$ is the minimal polynomial of some $\alpha \in A$. Recall that $F[x]$ is a unique factorization domain. I claim that for any irreducible $g(x) \in F[x]$ with degree dividing the degree of $f(x)$, there exists some $\beta \in A$ so that $g^n(x)$ is the minimal polynomial of β. To see this, notice that if $J = J(A)$ is the Jacobson radical of A, then A/J is a direct product of finite fields of characteristic p.

Since $f^n(\alpha) = 0$, it follows that $f(\alpha) \in J$. Now, since $f(x)$ is irreducible it must be the minimal polynomial of an element of one component of the direct product; if not, $f(x)$ would be the product of the minimal polynomials of elements in two different

components and hence would not be irreducible. Let $\mathbf{F}$ be the component of the direct product A/J in which an element for which f(x) is the minimal polynomial lies. Then for any irreducible g(x) with degree dividing the degree of f(x), we know from the theory of finite fields that there is some $\gamma+J \in \mathbf{F}$ for which g(x) is the minimal polynomial. A quick calculation shows that the set $g(\gamma+J)$ is all of J. Since $f(\alpha)$ has nilpotency n, it therefore follows that for some choice of $j \in J$, $g(\gamma+j)$ has nilpotency n; hence $\beta = \gamma+j$ has minimal polynomial $g^n(x)$.

Since $I = I_F^A$, it follows that the minimal polynomials of all elements of A divide c(x). Recalling that $x^{q^k} - x$ is the product of all irreducibles of degree dividing k, once each, we see that the claim shows that c(x) must have the specified form, as the irreducibles of smaller degree in the divisor lattice occur, as divisors of c(x), at least as often as those of larger degree, and as irreducibles of the same degree are forced to occur the same number of times. □

Corollary 2.1. Suppose f(x) generates a compositional attractor of F[x]. Then the following hold:

(i) All irreducible divisors of f(x) having the same degree have the same multiplicity.

(ii) If f(x) has an irreducible divisor of degree d and multiplicity m, then all irreducible divisors of f(x) having a degree dividing d have a multiplicity equaling or surpassing m.

Proof:

Elementary computations show this to be simply a restatement of the preceding theorem.

The following corollaries demonstrate a use for Theorem 2.1 outside the domain of permutation polynomials.

Corollary 2.2. Suppose that $f(x) \varepsilon F[x]$ is an irreducible of prime degree r. Then if $g(x) \varepsilon F[x]$ is a polynomial of degree less than r, there must exist another irreducible $h(x) \varepsilon F[x]$ of degree q so that

$$f(x) \mid h(g(x)).$$

Proof:

$(x^{q^r} - x)$ generates a compositional attractor. Its divisors are exactly the irreducibles of degree r and 1. From Theorem 2.1 we see that this means $(x^{q^r} - x) \mid (g(x)^{q^r} - g(x))$. Since g(x) has degree less than r, the composition of g(x) with one of the linear factors of $(x^{q^r} - x)$ cannot produce a multiple of f(x); hence the composition of g(x) with some h(x) of degree r must have done so. □

One conclusion this corollary leads to is that for any irreducible of degree n, for each prime $r>n$, we find that there exists at least one irreducible h(x) of degree r so that h(g(x)) is not irreducible.

Corollary 2.3. Suppose f(x) is an irreducible of F[x] of degree n. Then there exists some $g(x) \neq x$ of degree less than n so that $f(x) \mid f(g(x))$.

Proof:

For any $g(x) \neq x$, Theorem 2.1 implies $x^q - x \mid \left(g(x)\right)^q - g(x)$. If we set $h(x) = \frac{x^q - x}{f(x)}$, then Theorem 2.1 implies that there exists g(x) so that $h(x) \nmid h(g(x))$. Since $h(x) \cdot f(x) \mid h(g(x)) \cdot f(g(x))$, we may conclude that $f(x) \mid f(g(x))$. From this we see that $f(x) \mid f(\alpha \cdot f(x) + g(x))$; hence we may take g(x) to have degree less than that of f(x),

without loss.

Now I will give examples of compositional attractors tied to various F-algebras. The first is taken from [9] and is the basic compositional attractor from which the others are built.

Example 2.1. If $Q = GF(q^k)$ then $\langle x^{q^k} - x \rangle = I_F^Q$.

My second example is taken from [11].

Example 2.2. If $R = F^{mxm}$ then we see $I_F^R = \langle \prod_{\iota=1}^{m} (x^{q^\iota} - x) \rangle$.

For my third example, which is my own and hence is stated as a lemma, I will use a type of F-algebra fundamental to the analysis of those permutation polynomial groups associated with compositional attractors of F[x].

Lemma 2.1. Suppose that $f(x) = f_1(x)^{e_1} \cdot f_2(x)^{e_2} \cdot \cdots \cdot f_k(x)^{e_k}$ is a factorization of $f(x) \in F[x]$ into powers of distinct irreducibles. Then if $A = F[x]/\langle f(x) \rangle$ we see that

$$I_F^A = \langle \text{L.C.M} \left\{ \left(x^{q^{\deg(f_i(x))}} - x \right)^{e_i} \right\} \rangle.$$

Proof:

Notice that since the various $f_i(x)$'s are relatively prime to one another, the Chinese Remainder Theorem tells us that

$$F[x]/\langle f(x) \rangle \cong \prod_{\iota=1}^{k} F[x]/\langle f_i(x)^{e_i} \rangle.$$

From this we can see that the generator of I_F^A must be a common multiple of the generators of the $I_F^{A_i}$ $i = 1...m$, where $A_i = F[x]/<F_i(x)^{e_i}>$. Since the least common multiple of all these generators is in I_F^A, it follows that it must be the generator. It remains to show that $I_F^{A_i}$ is generated by $\left(x^{q^{\deg(f_i)}} - x\right)^{e_i}$.

To see this, apply Theorem 2.1. Certainly there exists an element in A_i; it is in fact the coset of x, that has $f_i(x)^{e_i}$ as its minimal polynomial. This forces the putative generator to divide the actual generator. It is easy to see that the Jacobson radical $J(A_i)$ of A_i has generator $f_i(x)$; hence the maximum degree of nilpotency of an element of $J(A_i)$ is e_i. Since $A_i/J(A_i) \cong GF(q^{\deg(f_i(x))})$ we see that all minimal polynomials of elements of A_i are powers of irreducibles of degree dividing the degree of $f_i(x)$. From the maximal degree of nilpotency argument, we see that the power of an irreducible in a minimal polynomial need not exceed e_i; hence the actual generator divides the putative generator, forcing them to be one and the same. □

§2 The Order of Finite Permutation Polynomial Groups with Finite Field Coefficients.

In this section $F = GF(p^n)$, and let $q = p^n$. At this point I am ready to tackle the problem of enumerating the permutation polynomial group associated with each compositional attractor of F[x]. Lemma 1.2 makes this equivalent to computing the order of every finite group of permutation polynomials with coefficients in F. The first step is to solve the problem for F-algebras that are direct products of finite fields. At this point I would like to recall the Artin-Wedderburn structure theorem for Rings.

Theorem (Artin-Wedderburn).

For a ring R the maximal nilpotent ideal J(R) of the ring is called its Jacobson Radical. The factor ring R/J(R) is a semisimple ring. In the case we are dealing with, R both finite and commutative, R/J(R) is the direct product of finite fields.

The second step is to employ Lemma 1.3 to lift this result to all F-algebras of the form $F[x]/\langle f(x)\rangle$, at which point the title of the section is satisfied.

Unlike other permutation polynomial groups, enumeration of the permutation polynomials of a finite F-algebra comprising a direct product of finite field is best done by computing the isomorphism type of the group. This process is a simple modification of work presented in [9]. Lemma 2.2(i) is entirely as presented in [9] except for a change of terminology, and is included for completeness and consistency.

Lemma 2.2. Let $Q = GF(q^k)$. Then

(i) $PP_F(Q)$ is the centralizer in $PP_Q(Q)$ of the Frobenius automorphism $\sigma: x \mapsto x^q$.

(ii) $PP_F(Q)$ acts on all subfields of Q containing F.

(iii) $PP_F(Q)$ acts on the sets $Q_d = \{q \varepsilon Q : q \text{ has a minimal polynomial of degree } d\}$.

(iv) $PP_F(Q)$ is the internal direct product of its representation on the Q_d's.

Proof:

(i) Suppose that $f(x)+I_F^Q \varepsilon PP_F(Q)$. Then $(f(x))^q = \left(\sum f_i x^i\right)^q = \sum f_i^q x^{q \cdot i} = \sum f_i x^{q \cdot i} = f(x^q)$, so all members of $PP_F(Q)$ centralize σ. On the other hand, suppose that $f(x)+I_F^Q$ centralizes σ. Since $I_Q^Q = \langle x^{q^k} - x \rangle$, there is some unique representative, take it to be $f(x)$, with degree$<q^k$ of $f(x)+I_F^Q$. Then $f(x)^q = f(x^q)$. If we set $y = x^q$, we see that this equality can be reformulated as $g(y) = \sum_{i=1}^{q^k-1} (f_i - f_i^q) y^i = 0$ for all y in Q. Since $g(y)$ has degree less than q^k, it follows that $f_i = f_i^q$ for all i, placing $f(x)$ squarely in $PP_F(Q)$.

(ii) This follows directly from the fact that all subfields of Q contain F.

(iii) This follows directly from the fact that the partition of Q into the Q_d's is induced by the subsets of Q that are subfields containing F.

(iv) Let G_d be the representation of $PP_F(Q)$ on Q_D. This notion is well defined by (iii). Notice that the characteristic function χ_{Q_d}, $d \mid k$, is in $F_F(Q)$. To see this, simply take $f(x)$ to be $x^{q^k} - x$ divided by each irreducible of degree d in $F[x]$. Since $d \mid k$, $f(x)$ ε $F[x]$. The resulting function is zero off Q_d and equal to the product of all elements of $Q - Q_d$ on Q_d; hence χ_{Q_d} is a scalar multiple of $f(x)$. Since $f(x)$ ε $F[x]$, this scalar is in F; hence $f(x) \epsilon_F^Q = \chi_{Q_d}$.

Once we have $\chi_{Q_d} \varepsilon F[x]$ we see that for $f(x)+I_F^Q \varepsilon PP_F(Q)$, $g(x) = x \cdot (1 - \chi_{Q_d}) + f(x) \cdot \chi_{Q_d}$ is exactly the Q_d-component of the permutation associated with

f(x) on Q_d and identity off Q_d. Therefore, each element of $PP_F(Q)$ has unique internal decomposition into a product of elements from each G_d, giving the specified internal direct product. □

The following lemma also appears with different language in [9]. As we will see subsequently, it has application to all F-algebras that are direct products of finite fields, not just extension fields.

Lemma 2.3. Let G_d be the representation of $PP_S(Q)$ on $Q_d = \{q \varepsilon Q : q \text{ has minimal polynomial of degree } d\}$. Then $G_d \cong C_d$ wr $S_{\pi(d)}$, where $\pi(d)$ is the number of irreducibles of degree d in F[x], and wr denotes the wreath product.

Proof:

Since we know that $PP_Q(Q)$ contains all permutations of Q, we see from Lemma 2.2 that G_d is the centralizer in $Sym(Q_d)$ of the Frobenius automorphism σ: $x \mapsto x^q$. From the theory of finite fields, we know that the action of the Frobinius automorphism on Q_d is the cyclic permutation of the $\pi(d)$ sets of d roots of each irreducible of degree d in F[x]. The centalizer then clearly contains each individual cyclic action induced by σ on the roots of some irreducible of degree d. A simple calculation shows that any permutation centralizing σ must normalize the group generated by these cycles; hence G_d has a normal subgroup N comprising the direct product of $\pi(d)$ cyclic groups of order d.

Note that G_d must contain any permutations that swap sets of roots in a fashion consistent with the cyclic actions of σ upon them. A simple calculation shows that these

together with the members of N comprise all permutations that commute with σ. If $(a_1\ a_2 \cdots a_d)$ and $(b_1\ b_2 \cdots b_d)$ are respectively the cyclic actions on two sets of roots, then $(a_1\ b_1)(a_2\ b_2) \cdots (a_d\ b_d)$ is an involution in G_d. Clearly, the set of all such involutions generates a symmetric group on the sets of roots of irreducibles that form an $S_{\pi(d)}$-complement to N in G_d, making G_d the semidirect product of N by $S_{\pi(d)}$. Notice that the stabilizer of a set of roots in this symmetric action centralizes those roots; hence G_d is a wreath product as specified in [3], page 33. □

Theorem 2.2. Let A be an F-algebra that is a direct product of finite fields

$$\prod_{i=1}^{m} GF(q^{k_i}).$$

Then:

(i) $PP_F(A) \cong \prod_{d \mid k_i} C_d$ wr $S_{\pi(d)}$, and

(ii) $|PP_F(A)| = \prod_{d \mid k_i} d^{\pi(d)} \cdot \pi(d)!$,

where $\pi(d)$ denotes the number of irreducibles of degree d over F.

Proof:

(i) Let $A_d = \{a \varepsilon A : a$ has an irreducible minimal polynomial of degree $d\}$. Notice that $PP_F(A)$ must act on sets of the form $A_d \cap GF(q^{k_i})$; hence the action of $PP_F(A)$ is completely determined by its action on the A_d's. By examining the finite field $\mathbf{F} = GF(q^{LCM(k_i)})$, we see that as in 2.2(iv), $\chi_{A_d} \varepsilon\ F_F(A)$ and that $PP_F(A)$ is therefore a direct product of its representations on the A_d's. I claim further that the action of $PP_F(A)$ on A_d is completely determined by its action on any $Q_d = A_d \cap GF(q^{k_i})$ where $d \mid k_i$. To see this, notice that all such intersections are simply the set of all elements in the field extension $GF(q^d)$ of F that had minimal polynomials of degree d over F. Clearly, a polynomial permutes the set product of several such sets iff it permutes some

one of them; hence the claim is true. With the claim we see, however, that the representation of $PP_F(A)$ on A_d is isomorphic to the representation of $PP_F(GF(q^d))$ on Q_d, as in Lemma 2.3; hence the components of the direct product of (i) above have the specified form.

(ii) The enumeration follows directly from the isomorphism type of the group.

Corollary 2.4. Suppose that $f(x) \in F[x]$ is a square free with irreducible divisors $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ of degree d_1, d_2, ..., d_m, and set $A = F[x]/f(x)$. Then

(i) $PP_F(A) \cong \prod_{s \mid \text{some } d_i} C_s \text{ wr } S_{\pi(s)}$, and

(ii) $|PP_F(A)| = \prod_{s \mid \text{some } d_i} s^{\pi(s)} \cdot \pi(s)!$

(iii) $I_F^A = \langle \text{L.C.M}(x^{q^{d_i}} - x) \rangle$.

Proof:

(i) Notice that the Chinese Remainder Theorem tells us that

$$A \cong \prod_{i=1}^{m} F[x]/\langle f_i(x) \rangle \cong \prod_{i=1}^{m} GF(q^{d_i}).$$

Apply Theorem 2.2 and we have (i).

(ii) Follows from (i) by elementary counting.

(iii) Note that the putative generator of I_F^A is the least common multiple of the minimal polynomials of all elements of A. Since all members of I_F^A are common multiples of all minimal polynomials of elements of A, this suffices to make it the generator of I_F^A.

□

With Corollary 2.4 in hand, we are ready to compute the order of $PP_F(A)$, where A is

F[x] modulo any polynomial. To do this we will employ the lifting Lemma 1.3 from Chapter 1.

Theorem 2.3. Suppose that $f(x) = f_1(x)^{e_1} \cdot f_2(x)^{e_2} \cdot \cdots \cdot f_m(x)^{e_m}$ is a factorization of $f(x)$ into powers of distinct irreducibles of degree $d_1, d_2, \ldots, d_m$, respectively, and let $r_d = \max\{e_i : d \mid \deg(f_i(x))\}$. Then if $A = F[x]/\langle f(x)\rangle$, $S = \{s : s \text{ divides some } d_i\}$, $T = \{t \in S : r_t > 1\}$ we have

$$|PP_F(A)| = \left(\prod_{s \in S} s^{\pi(s)} \cdot \pi(s)!\right) \times \left(q^{\sum_{s \in S} \pi(s) \cdot s \cdot (r_s - 1)}\right) \times \left(\prod_{s \in T} \left(1 - \frac{1}{q^s}\right)^{\pi(s)}\right).$$

Proof:

As I will demonstrate, the three factors in the formula above are, respectively, the number of polynomial permutations of A modulo its Jacobson Radical, the number of F-polynomial functions on A that are also permutations of A modulo its Jacobson radical, and the fraction of those functions that are actually permutations of A. To see that the first two factors are correct is easy. If J(A) is the Jacobson Radical of A and $s(x) = f_1(x) \cdot f_2(x) \cdot \cdots \cdot f_m(x)$, we see first that $J(A) = \langle s(x)\rangle$; hence $A/J(A)$ is isomorphic to an algebra of the form described in Corollary 2.4, and we have the first factor.

If we take t(x) to be the product of all irreducibles in F[x] with degrees in S, then we see from Lemma 2.1 that $I_F^{A/J(A)} = \langle t(x)\rangle$. All the F-polynomial functions on A that give permutations of $A/J(A)$ are then of the form

$$f(x) + t(x) \cdot r(x),\ f(x) + I_F^{A/J(A)} \in PP_F(A/J(A)), \qquad (*)$$

for some polynomial r(x) and further all such functions have a unique representative modulo the generator, g(x), of I_F^A (which, recall, is $\ker(\epsilon_F^A)$). A quick calculation shows that the exponent of q in the second term is exactly degree(g)−degree(t) and hence gives that maximum degree of r, so the second term is correct as there are q possible choices for each coefficient of r.

The third term follows from the Chinese Remainder Theorem and the lifting lemma. Indeed, lemma 1.3 tells us that a polynomial permutes A iff it permutes A/J(A), and that the evaluation of its formal derivative at any point cannot, by multiplication, increase the degree of nilpotency of any element of J(A). A moment's thought will convince one that $J(A) = <t(x)>$. From this we see that the second condition of the lifting lemma is equivalent to the formal derivative at each point being divisible by no irreducible whose degree is in T. Apply this to (*) and we see that for each $a(x) \varepsilon A$, we want

$$f'(a)+t(a)\cdot r'(a)+t'(a)r(a)$$

to be divisible by no irreducible of degree d for which $r_d > 1$. Notice that Corollary 1 implies that t(x) is a compositional attractor; hence t(a) is divisible by all such and the condition we wish to satisfy is exactly

$$f'(a)+t'(a)\cdot r(a) \not\equiv h(a)$$

simultaneously for all irreducibles h(x) with degrees in T. However, this is equivalent to insisting that $f'(x)+t'(x)\cdot r(x)$ not be a multiple of h(x). From the factorization of t(x), the product rule for derivatives makes it obvious that $t'(x)$ is relatively prime to h(x) and the condition becomes that r(x) not assume some one value modulo h(x). This means that exactly the fraction $\left(1 - \frac{1}{q^{\deg(h(x))}}\right)$ of all polynomials modulo h(x) are acceptable. Since the various irreducibles with degrees in T are all relatively prime, the Chinese Remainder Theorem tells us that the fraction of polynomials acceptable modulo all possible irreducibles is simply the product of the fraction acceptable modulo each irreducible; hence the third term is correct. □

Corollary 2.5. The formula given in Theorem 2.3 may be simplified to

$$\prod_{s \varepsilon S} s^{\pi(s)} \cdot \pi(s)! \cdot \prod_{s \varepsilon T} \left(\left(q^s - 1\right) \cdot \left(q^{s\cdot(r_s - 2)} \right) \right)^{\pi(s)}.$$

Proof:

Routine computation.

§3 Compositional Attractors of $\mathbf{Z}[x]$.

In this section we will develop some information about compositional attractors of the integers, setting the stage for Chapter three. Throughout the section p will be a prime, n will be a positive integer, and $\mathbf{Z}_{p^n}$ will denote the ring $\mathbf{Z}/\langle p^n \rangle$. Lemma 1.4 implies that the compositional attractors of $\mathbf{Z}[x]$ are built out of the compositional attractors of $\mathbf{Z}_{p^n}[x]$ for various integers n and primes p. Recall that $\mathbf{Z}_{p^m}[x]$ $(m>1)$ is *not* a UFD or PID; hence the computations in this section will be both messy and farther from the main stream. I can't just say "from the theory of finite fields we see..." anymore. I will begin the section with a useful lemma that quantifies in some sense the degree to which $\mathbf{Z}_{p^m}[x]$ fails to be a PID.

Lemma 2.4. Suppose that I is an ideal of $\mathbf{Z}_{p^m}[x]$, p prime so that the factor module $F = \mathbf{Z}_{p^m}[x]/I$ is finite. Then

$$I = \langle f_1(x), p^{e_2} \cdot f_2(x), \ldots, p^{e_k} \cdot f_k(x) \rangle,$$

so that

(i) $0 = e_1 < e_2 < \cdots < e_k = m$,

(ii) $1 = f_k(x) \mid f_{k-1}(x) \mid \cdots \mid f_1(x)$,

(iii) each $f_i(x)$ is monic, and

(iv) the generating set with its kth element deleted is a basis for I.

Proof:

Let $G = \{g_1(x), g_2(x), \ldots\}$ be any generating set of I ordered so that the p-part of the generators is nondecreasing and all possible p-parts of members of I are represented. Let $G_i = \{g \in G : g \text{ has p-part } p^i\}$. Now for two polynomials with the same p-part, a greatest degree common divisor is a linear combination of those two polynomials with the coefficients being monic polynomials; simply compute the gcd of their primitive parts

(mod p) to obtain such coefficients. From this we deduce that there exists some $\overline{g}_i(x)$ with p-part p^i that is a common divisor of all elements of G_i (mod p^{i+1}). Thus $\{\overline{g}_i(x) : i = 1, \ldots, m\}$ is a generating set of G.

For $\overline{g}_i(x)$, $\overline{g}_j(x)$, $i<j$, we compute a replacement for $\overline{g}_j(x)$ so that the primitive part of the replacement for $\overline{g}_j(x)$ is a divisor of the primitive part of $\overline{g}_i(x)$. This is done by computing the quantity $\gcd(p^{j-i}\overline{g}_i(x), \overline{g}_j(x))$ as a linear combination with monic coefficients exactly as in the previous paragraph, and using this gcd as the replacement. From this we see some finite number of operations reduces the generating set to a new set $\{g_i^*(x) : i=1, \ldots, m\}$ which has the divisibility property on primitive parts of generators that we want for (ii). In addition the reduction step did not change the p-part of the ith generator. Since F is finite we see that the generator with the largest p-part is exactly $g_m^*(x) = p^m$. Since F is finite we see that G contains primitive polynomials, hence $g_1^*(x)$ is primitive. Next we must transform the generating set $\{g_i^*\}$ into a generating set $\{\tilde{g}_i(x)\}$ so as to make each $\tilde{g}_i(x)$ a power of p times a monic polynomial, all without destroying the divisibility property.

Certainly $p^m = g_m^*(x)$ is already $\tilde{g}_i(x)$ (the transformation of $g_m^*(x)$ is to leave it alone). Suppose that the leading coefficient of g_i^* does not have p-part p^i. Then it is a multiple of the p-part of $\tilde{g}_{i+1}(x)$, and as $\deg(\tilde{g}_{i+1}) \leq \deg(g_i^*(x))$, we may subtract a multiple of $\tilde{g}_{i+1}(x)$ and obtain a replacement for $g_i^*(x)$ with leading coefficent that has p-part p^i. Having done this we may then multiply by a well chosen unit (mod p^m) and obtain $\tilde{g}_i(x)$ with leading coefficient exactly p^i. Inductively, we obtain the desired $\tilde{g}_i(x)$, $i = 1, \ldots, m$. Since the reduction simply made each $\tilde{g}_i(x)$ some combination of $\{g_j^* : j>i\}$ we see that the divisibility property is preserved.

At this point we must eliminate redundant members of the generating set. If the primitive part of $\tilde{g}_i(x)$ divides the primitive part of $\tilde{g}_{i+1}(x)$, then $\tilde{g}_{i+1}(x)$ is a multiple of

$\tilde{g}_i(x)$; throw it out. Let $f_i(x)$ be the i*th* survivor of this elimination process on the $\tilde{g}_i(x)$. At this point we see that we have satisfied (i)-(iii). It remains to prove (iv).

Let $h_i(x) = p^{e_i} \cdot f_i(x)$ and assume that the generating set is not a basis. Then for some $1 \leq j \leq k$, $h_j(x)$ is a linear combination of the other generators. Let

(high degree) $$r(x) = \sum_{i<j} c_i(x) \cdot h_i(x), \text{ and}$$

(high content) $$s(x) = \sum_{i>j} c_i(x) \cdot h_i(x),$$

such that $h_j(x) = r(x)+s(x)$. Notice that $f_j(x)$ divides $h_j(x)$. By the divisibility property it also divides $r(x)$; hence it must divide $s(x)$. Also by the divisibility property, the p-part of $s(x)$ is a proper multiple of the p-part of $h_j(x)$. This means that $p^c \cdot h_j(x)$ divides $s(x)$ for some integer $c \geq 1$. Let A be the companion matrix of $h_{j-1}(x)$ over p^m. Now, notice that A satisfies $r(x)$. This means that $h_j(A) = s(A)$. On the other hand, A is not a root of $h_j(x)$, so we have that $s(A)$ is a proper multiple of $g_j(k_j)$, a contradiction, so the given generating set is minimal, and we are done. □

One consequence of this lemma is a statement about the form of compositional attractors over $\mathbf{Z}_{p^n}$.

Corollary 2.6. Suppose that J is a compositional attractor of $\mathbf{Z}_{p^n}[x]$. Then J has a basis

$$\{f_1(x), p^{e_2} \cdot f_2(x), \ldots, p^{e_k} \cdot f_k(x)\},$$

so that

(i) $0 = e_1 < e_2 < \cdots < e_k = m$,

(ii) $1 = f_k(x) \mid f_{k-1}(x) \mid \cdots \mid f_1(x)$, all generate compositional attractors (mod p)

(iii) and each $f_i(x)$ is monic.

Proof:

If we apply Lemma 2.4 to J, we obtain all of the above except the claim that each of the $f_i(x)$ is a compositional attractor. Let $g(x) \varepsilon \mathbf{Z}_{p^n}[x]$ have invertible leading coefficient. Since J is a compositional attractor itself, we see for each i that

$$p^{e_i} \cdot f_i(g(x)) = \sum_{j=1}^{k} c_j(x) \cdot p^{e_j} f_j(x).$$

By considering the powers of p and using the basis and divisibility properties, we see that $c_j(x) = 0$ for $j < i$. Thus we see that

$$f_i(g(x)) = \sum_{j=i}^{k} c_j(x) \cdot p^{e_j - e_i} \cdot f_j(x),$$

so $f_i(g(x)) \equiv c_j(x) \cdot f_j(x) \pmod{p}$, and $f_i(x)$ is a compositional attractor (mod p). □

Corollary 2.6 tells us a form that all compositional attractors of $\mathbf{Z}_{p^n}[x]$ must have. The next step is to further tighten our understanding of which parameters of the form actually yield a compositional attractor.

Lemma 2.5. Let J be a compositional attractor of $\mathbf{Z}_{p^n}[x]$, set $A = \mathbf{Z}_{p^n}[x]/J$, let $B = A/\langle p \rangle$, and take $\langle f(x) \rangle = I_{\mathbf{Z}_p}^{B}$. Then if

$$J = \langle f_1(x), p^{e_2} \cdot f_2(x), \ldots, p^{e_k} \cdot f_k(x) \rangle$$

is a basis of the sort described in Lemma 2.4 and $\iota^k(x)$ is an irreducible power divisor of f(x), then $\iota^k(x)$ divides each $f_i(x)$, $i<k$, (mod p).

Proof:

Since B is a $\mathbf{Z}_p$-algebra, it follows that f(x) is the least common multiple of the minimal polynomials of all elements of B. If $\iota^k(x)$ divides f(x), then there is an element $\alpha + \langle p \rangle \varepsilon B$ which has minimal polynomial g(x) divisible by $\iota^k(x)$. If $\iota^k(x)$, and hence

$g(x)$, fails to divide some $f_i(x) \pmod p$, then $p^{e_i} \cdot f_i(\alpha) \not\equiv 0 \pmod{p^n}$. This, however, violates a property bestowed on J by Theorem 1.1 (ii), giving a contradiction. □

At this point I want to highlight an obnoxious feature of arithmetic in $\mathbf{Z}_{p^n}[x]$. If a polynomial in $\mathbf{Z}_{p^n}[x]$ is congruent to a polynomial that can be factored (mod p), it need not be itself reducible when $n>1$.

Example 2.3. An irreducible polynomial of $\mathbf{Z}_{p^n}[x]$ that factors modulo p.

(i) $p=2$, $n=2$, $f(x) = x^2+2$, $f(0) = 2$, $f(1) = 3$, $f(2) = 2$, $f(3) = 3$; hence $f(x)$ is irreducible in $\mathbf{Z}_4[x]$, yet $f(x) \equiv x \cdot x \pmod 2$.

This situation is not irretrievable, however, as shown by the following lemma.

Lemma 2.6. If $f(x) \in \mathbf{Z}_{p^n}[x]$ is irreducible, then it is congruent modulo p to a power of an irreducible element of $\mathbf{Z}_p[x]$.

Proof:

If $f(x)$ is not congruent to a power of an irreducible (modulo p) then is has a factorization, $f(x) = a(x) \cdot b(x) \pmod p$ into relatively prime factors; this follows from the prime factor theorem for UFDs. In order to prove the lemma I will now construct a factorization for any $f(x)$ over $\mathbf{Z}_{p^n}$ not congruent to a power of a prime (mod p).

Suppose that $a(x), b(x) \in \mathbf{Z}_{p^n}[x]$ are relatively prime modulo p so that

$$f(x) = a(x) \cdot b(x) + p \cdot q(x).$$

Examine the product with undetermined coefficients $c_j^i(x)$:

$$\left(a(x)+p\cdot c_1^1(x)+p^2\cdot c_1^2(x)+p^3\cdot c_1^3(c)+ \cdots\right)\cdot\left(b(x)+p\cdot c_2^1(x)+p^2\cdot c_2^2(x)+p^3\cdot c_2^3(x) \cdots\right),$$

which when expanded becomes

$$a(x)\cdot b(x) + p\cdot\left(c_1^1(x)\cdot b(x)+c_2^1(x)\cdot a(x)\right) + p^2\cdot\left(c_1^1(x)\cdot c_2^1(x)+c_2^2(x)\cdot a(x)+c_1^2(x)\cdot b(x)\right)$$
$$+ p^3\cdot(c_1^1(x)\cdot c_2^2(x)+c_2^1(x)\cdot c_1^2(x)+c_2^3(x)\cdot a(x)+c_2^3(x)\cdot b(x))+\cdots.$$

The fact that a(x) and b(x) are relatively prime (mod p) allows us to apply the Euclidean algorithm and obtain values for $c_1^i(x)$ and $c_2^i(x)$, up to congruence (mod p), so, examining the above expression, we see that we may obtain any possible value for the product (mod p^i) without disturbing its value (mod p^{i-1}). We may in particular choose the coefficents so as to obtain f(x) from the product, hence the lemma is true. □

I want to conclude this section with an example of compositional attractors of $\mathbb{Z}[x]$. The entire thrust of Chapter 3 is to develop two examples of compositional attractors of $\mathbb{Z}$, those associated with $\mathbb{Z}_n$ and with the mxm matrices over $\mathbb{Z}_n$.

Example 2.4 . Suppose that $f(x)+\langle p\rangle$ is the generator of a compositional attractor of $\mathbb{Z}_p[x]$. Then

$$\langle f(x)^n,\ p\cdot f(x)^{n-1},\ p^2\cdot f(x)^{n-1},\ \ldots,\ p^{n-1}f(x),\ p^n\rangle$$

is certainly a compositional attractor of $\mathbb{Z}[x]$. To see this simply note that

$$f(g(x)) = r(x)\cdot f(x)+p\cdot a(x)$$

by hypothesis, which yields the identity

$$f(g(x))^k = \left(r(x)\cdot f(x)+p\cdot a(x)\right)^k = \sum_{m=0}^{k} r(x)^m f(x)^m p^{k-m} a(x)^{k-m},$$

and apply the identity to each basis element.

Example 2.4 is in fact simply an application of Lemma 1.5 to the compositional attractor generated by f(x) and p.

Chapter 3

The Groups $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$ and $PP_{\mathbf{Z}_n}(\mathbf{Z}_n^{m\times m})$.

§0 Introduction and Summary.

In Section 1, I will give a new proof of David Singmaster's result[4], that there are exactly

$$\prod_{k=0}^{n-1} \frac{n}{(n,k!)}$$

functions from $\mathbf{Z}_n$ to itself that can be represented as polynomials in $\mathbf{Z}_n[x]$, which is shorter than the original and matches the notation used in the rest of this paper. In Section 2, I will give a new form of the computation of a basis of $I_{\mathbf{Z}}^{\mathbf{Z}_n}$. In Section 3 I will compute exactly which polynomials over $\mathbf{Z}_n$ are permutation polynomials, and I will give the size of $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$. In addition, I will give some information about the isomorphism type of $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$, establishing the isomorphism type exactly for n = 1, 2. In Section 4 I will compute a basis for the compositional attractor $I_{\mathbf{Z}_n^{m\times m}}^{\mathbf{Z}_n}$. In Section 5 I will compute the membership and order of the group $PP_{\mathbf{Z}_n}(\mathbf{Z}_n^{m\times m})$.

A tool I have found that leads to shorter proof about polynomials (mod n) is the difference operator Δ, defined on any ring of polynomials over a commutative ring with 1, to be

$$\Delta f(x) = f(x+1) - f(x).$$

For an original treatment of the difference operator, see [1]. A more modern introduction to Δ is in [2].

I will call a polynomial $f(x) \in \mathbf{Z}[x]$ *n-ish* if it is a member of $I^{\mathbf{Z}_n}_{\mathbf{Z}}$. Such polynomials are the preimages under the natural homomorphism $\pi: \mathbf{Z}[x] \to \mathbf{Z}_n[x]$ of the residue polynomials of $\mathbf{Z}_n$. Residue polynomials of a ring are those polynomials having all elements of the ring as their roots [5].

Throughout this chapter I will use falling factorial notation,

$$x^{(n)} = x \cdot (x-1) \cdot (x-2) \cdots (x-n+1).$$

In order to avoid confusion with the use of parentheses in standard exponents, an exponent will denote a falling factorial only if it is completely enclosed in parentheses. The falling factorials are preferable to the powers of x as a basis for the polynomials in some situations because of identities like the following [2]. First,

$$\Delta x^{(n)} = n \cdot x^{(n-1)}, \tag{3.1}$$

and using (3.1) for a polynomial $f(x) = a_0 + a_1 x^{(1)} + \cdots + a_m x^{(m)}$, it follows that

$$\Delta^k f(0) = a_k \cdot k!. \tag{3.2}$$

§1 Singmasters Result.

In this section I will re-prove D. Singmaster's 1974 result [4] that the number of functions from $\mathbf{Z}_n$ to itself that can be represented as polynomials is

$$\prod_{k=0}^{n-1} \frac{n}{(n,k!)}.$$

I later use this result to compute $|PP(\mathbf{Z}_n)|$.

Proposition 3.1.

If $f(x) \varepsilon \mathbf{Z}[x]$ is n-ish of degree k, then $\frac{n}{(n,k!)}$ divides the content of f(x).

Proof:

The content of a polynomial is defined to be the greatest common divisor of its coefficients when the polynomial is written with respect to the standard basis, the powers of x. Notice that the gcd of the coefficients does not change if the polynomial is rewritten in the descending factorial basis. Assume then that f(x) is n-ish of degree k and that

$$f(x) = a_0 + a_1 x^{(1)} + a_2 x^{(2)} + \cdots + a_k x^{(k)}.$$

It is trivial to see that Δ preserves n-ishness, so n divides $\Delta^m f(0)$, which means by (3.2) that $n \mid a_m m!$. From this, we see that $\frac{n}{(n,m!)} \mid a_m$. Each m is less than or equal to k, so $\frac{n}{(n,k!)} \mid \frac{n}{(n,m!)}$ for each m; hence $\frac{n}{(n,k!)} \mid a_m$ for each m. As a result $\frac{n}{(n,k!)}$ divides the content of f(x).

A polynomial $p(x) \varepsilon \mathbf{Z}[X]$ induces the function f, where

$$f(x \bmod n) = p(x) \bmod n$$

from $\mathbf{Z}_n$ to itself. This notion is well defined because members of $\mathbf{Z}[X]$ preserve congruence (mod n).

Theorem 3.1. (D. Singmaster, 1974).

The number of functions from $\mathbf{Z}_n$ to itself that can be represented as polynomials is

$$\prod_{k=0}^{n-1} \frac{n}{(n,k!)}.$$

Proof:

To prove the formula I will produce a system of representatives for the equivalence classes of polynomials in $\mathbf{Z}[X]$ that induce the same function over $\mathbf{Z}_n$ and then compute its size.

I claim that the polynomials of the form $\frac{n}{(n,k!)}x^{(k)}$ are n-ish. For any integer a, $a^{(k)}$ is a product of k consecutive integers. An elementary result of number theory is that k! divides the product of k consecutive integers so we see that $k! | a^{(k)}$ and hence $n | \frac{n}{(n,k!)}a^{(k)}$ for each integer a. This proves the claim.

From the claim one can see that if a polynomial induces a function on $\mathbf{Z}_n$, then that same function is induced by a polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ with its coefficients in the range $0 \leq a_k < \frac{n}{(n,k!)}$. One simply subtracts proper integral multiples of n-ish polynomials supplied by the claim, starting with those of highest degree and working down. Since we are bringing the coefficients into the correct range in descending degree order, the later corrections will not disrupt the earlier ones. Further, since n-ish polynomials induce the zero function, subtracting multiples of them does not affect the function induced.

Now let f(x) and g(x) be polynomials with their coefficients in the range specified above, and let $p(x) = f(x) - g(x)$. Then if $d = \deg(p)$, one sees that the leading coefficient of p(x) is strictly bounded in absolute value by $\frac{n}{(n,d!)}$. This means that $\frac{n}{(n,d!)} \not| \text{cont}(p)$. Applying Proposition 3.1 we see that p(x) is not n-ish.

This means that the set of all polynomials with coefficients in the specified range form the desired system of representatives. Counting the number of choices for each coefficient yields the desired formula.

§2 A Basis for the Ideal $I_{\mathbf{Z}}^{\mathbf{Z}_n}$.

Throughout this section I will use the notation I_n for $I_{\mathbf{Z}}^{\mathbf{Z}_n}$. I will start with an interesting property of $\kappa(n)$, defined to be the least k for which $n|k!$; i.e.,

$$\kappa(n) = \min\{k : n \mid k!\},$$

after which I will produce a slightly different version of the Niven and Warren [6] basis for the residue polynomials of $\mathbf{Z}_n$, which basis is also a minimal generating set for I_n. Information about the function $\kappa(n)$ is necessary to produce this basis, and it is also useful for the calculations in Section three. Some form of $\kappa(n)$ appears in [4], [5], and [6]. In [5] Kempner refers to κ as μ, and my definition and use are closer to his than to any other. I do not use the symbol μ so as to avoid confusion with the Möbius function, which pops up repeatedly in the generalization of this work to the matrix case. In [6] Niven and Warren refer to a closely related function t(k), which is in some sense an inverse of $\kappa(n)$ for prime powers. In [4] Singmaster uses the notation n(m) in place of $\kappa(n)$ and then drops the argument and merely refers to the function as n.

A quick pencil-and-paper method of computing $\kappa(n)$ for prime powers and a number of valuable special cases of $\kappa(n)$ appears on page 243 of [5]. As I will show below, knowing the value of $\kappa(n)$ at prime powers rapidly gives one the value of $\kappa(n)$ for all n.

Proposition 3.2. (A. J. Kempner 1921)

For $n \geq 2$, $\kappa(n) = \max\{\kappa(q) : q \text{ a prime power divisor of } n\}$.

Proof:

Assume that $n \geq 2$, and let $d = \max\{\kappa(q) : q \text{ a prime power divisor of } n\}$. Then for

each prime power divisor q of n, $q|d!$ and hence $n|d!$. On the other hand since for some divisor q of n, $\kappa(q) = d$, it follows that $\kappa(n) \geq d$, so $\kappa(n) = d$.

Notice that $\kappa(1) = 0$ and that $\kappa(p) = p$ for p prime. Table 3.1 gives some provocative values of $\kappa(n)$.

Table 3.1

Values of $\kappa(n)$

n	$\kappa(n)$	n	$\kappa(n)$	n	$\kappa(n)$	n	$\kappa(n)$
1	0	9	6	32	8	8192	16
2	2	10	5	64	8	16384	16
3	3	11	11	128	8	32768	16
4	4	12	4	256	10	65536	18
5	5	13	13	512	12		
6	3	14	7	1024	12		
7	7	15	5	2048	14		
8	4	16	6	4096	16		

Now, instead of a basis for the Ideal of residue polynomials in $\mathbf{Z}_n[x]$, as in [6], I will produce a basis for the ideal I_n in $\mathbf{Z}[x]$, which is a preimage under the natural map from $\mathbf{Z}[x]$ to $\mathbf{Z}_n[x]$ of Niven and Warren's basis. My proof produces the basis immediately for all n instead of producing it first for prime powers and then constructing a basis for general n from the prime power bases.

Define:

$$\Lambda_n = \{\kappa(d) : d|n\}.$$

Theorem 3.2. Let I_n denote the ideal of n-ish polynomials in $\mathbf{Z}[x]$. Then

$$I_n = \langle \tfrac{n}{(n,k!)} \cdot x^{(k)} : k \in \Lambda_n \rangle,$$

and further, this basis is minimal.

Let $J_n = \langle \tfrac{n}{(n,k!)} \cdot x^{(k)} : k \in \Lambda_n \rangle$. In the proof of Theorem 3.1, we saw that each generator of J_n was n-ish; hence $J_n \subseteq I_n$. Let $f(x)$ be a member of I_n with degree m, say. If k is the largest member of Λ_n less than m, then $\frac{n}{(n,m!)} = \frac{n}{(n,k!)}$. This is because the members of Λ_n are exactly all those integers a for which a! contains a divisor of n that (a-1)! does not. Now, proposition 1 says that $\frac{n}{(n,m!)} \mid \mathrm{cont}(f)$, so $\frac{n}{(n,k!)} \mid \mathrm{cont}(f)$. As a result there is a multiple of $\frac{n}{(n,k!)} \cdot x^{(k)}$ of degree m with the same leading coefficient as $f(x)$. Subtracting this multiple gives us a new member $f'(x)$ of I_n having lower degree than $f(x)$ but congruent to $f(x)$ (mod J_n). By induction on degree, it follows that all members of I_n are congruent (mod J_n) to 0 or zeroth degree members of I_n, which are exactly the multiples of n. Since $n = \frac{n}{(n,0!)} \cdot x^{(0)}$ is a generator of J_n, it follows that $I_n \subseteq J_n$, and all that remains is to show that the basis is minimal.

Notice that the form of the generators given in Theorem 3.2 has a very nice property. The contents of the various generators and their primitive parts are both totally and strictly ordered by divisibility, with the two orderings running in opposite directions.

Start by ordering $\Lambda_n = \{k_1 > k_2 > \cdots > k_n\}$ and let $g_i(x) = \frac{n}{(n,k_i)} \cdot x^{(k_i)}$. Assume the generating set is not a basis. Then for some $j \in \Lambda_n$, g_j is a linear combination of the other generators. Let

$$r(x) = \sum_{i>j} c_i(x) \cdot g_i(x), \text{ and}$$

$$s(x) = \sum_{i<j} c_i(x) \cdot g_i(x),$$

such that $g_j(x) = r(x)+s(x)$. Notice that $x^{(k_j)}$ divides $g_j(x)$. By the divisibility property above, it also divides $r(x)$; hence it must divide $s(x)$. Also by the divisibility property, the content of $s(x)$ is a proper multiple of the content of $g_j(x)$. This means that $c \cdot g_j(x)$ divides $s(x)$ for some integer $c \geq 2$. Now, notice that k_j is a root of $r(x)$. This means that $g_j(k_j) = s(k_j)$. On the other hand, k_j is not a root of $g_j(x)$, so we have that $s(k_j)$ is a proper multiple of $g_j(k_j)$, a contradiction, so the given generating set is minimal, and we are done. □

Example 3.1. Generators for I_{12}, I_{128}.

(I_{12}) The divisors of 12 are 1, 2, 3, 4, 6, 12. Consulting Table 3.1 we find that $\kappa(d)$ for each of these divisors is 0, 2, 3, 4, 3, and 4, respectively, so $\Lambda_n = \{0, 2, 3, 4\}$. Applying Theorem 3.2, we get that

$$I_{12} = \langle 12, 6x^{(2)}, 2x^{(3)}, x^{(4)} \rangle,$$

and hence that $\mathbf{Z}[x]/I_{12} \cong \mathbf{Z}_{12} \times \mathbf{Z}_{12} \times \mathbf{Z}_6 \times \mathbf{Z}_2$, as an abelian group.

(I_{128}) The divisors of 128 are 1, 2, 4, 8, 16, 32, 64, and 128. Consulting Table 3.1 we find that $\kappa(d)$ for each of these divisors is 0, 2, 4, 4, 6, 8, 8, and 8, respectively, so $\Lambda_n = \{0, 2, 4, 6, 8\}$. Applying Theorem 3.2 we get that

$$I_{128} = \langle 128, 64x^{(2)}, 16x^{(4)}, 8x^{(6)}, x^{(8)} \rangle,$$

and hence that $\mathbf{Z}[x]/I_{128} \cong \mathbf{Z}_{128} \times \mathbf{Z}_{128} \times \mathbf{Z}_{64} \times \mathbf{Z}_{64} \times \mathbf{Z}_{16} \times \mathbf{Z}_{16} \times \mathbf{Z}_8 \times \mathbf{Z}_8$, as an abelian group.

§3 The group $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$.

In the name of legibility, I will refer to $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$ as $PP(\mathbf{Z}_n)$ throughout this section, and I will continue to use the notation I_n for $I^{\mathbf{Z}_n}_{\mathbf{Z}}$. The first step in computing $PP(\mathbf{Z}_n)$ is to reduce the problem of finding the isomorphism type and generators for general n to the same problem for prime powers. I will then produce a surjective homomorphism $\pi: PP(\mathbf{Z}_{p^n}) \to PP(\mathbf{Z}_{p^{n-1}})$ and establish a necessary and sufficient condition for a polynomial over $\mathbf{Z}_{p^n}$ to be a permutation polynomial.

Henceforth when I refer to a permutation polynomial I will actually mean the equivalence class of all permutation polynomials that induce the same permutation. Recall that the residue polynomials of $\mathbf{Z}_n[x]$ are those members of $\mathbf{Z}_n[x]$ having each element of $\mathbf{Z}_n$ as roots; they induce the zero function. The equivalence class of a given permutation polynomial f(x) over $\mathbf{Z}_n$ is thus the set of sums of f(x) with any residue polynomial [5]. This convention simplifies matters substantially, as it allows us to treat composition of polynomials as the composition of the permutations they induce.

Lemma 3.1. If $n = q_1 \cdot q_2 \cdot \cdots \cdot q_m$ is a factorization of n into powers of distinct primes, then

$$PP(\mathbf{Z}_n) \cong PP(\mathbf{Z}_{q_1}) \times PP(\mathbf{Z}_{q_2}) \times \cdots \times PP(\mathbf{Z}_{q_m}).$$

Proof:

Let π: $\mathbf{Z}_n[x] \to \prod \mathbf{Z}_{q_i}[x]$ be the ring isomorphism given by the Chinese Remainder Theorem. Suppose that $(g_1, g_2, \ldots, g_m)$ is an m-tuple of permutation polynomials in

$\prod \mathbf{Z}_{q_i}[x]$. Then by applying the Chinese Remainder Theorem pointwise to the functions induced on the $\mathbf{Z}_{q_i}$'s by the g_i's, we get a 1:1 function on $\mathbf{Z}_n$. This function is, however, the function induced on $\mathbf{Z}_n$ by the preimage of $(g_1, g_2, \ldots, g_m)$ under π. Now suppose that $f(x) \varepsilon \mathbf{Z}_n[x]$ induces a 1:1 function on $\mathbf{Z}_n$. Then the natural projection of this function onto the product of functions on the $\mathbf{Z}_{q_i}$'s must yield 1:1 functions, or we have a contradiction of the Chinese Remainder Theorem; hence the polynomial components of $f\pi$ must be permutation polynomials. This shows that $PP(\mathbf{Z}_n)\pi = \prod PP(\mathbf{Z}_{q_i})$. It remains to show that π preserves group structure.

Recall that our group operation is composition of polynomials. A polynomial composition is a string of ring additions and multiplications, nothing more, and both these operations are preserved by π, a ring isomorphism. It follows that π preserves our group operation, and hence that π restricted to $PP(\mathbf{Z}_n)$ is a group homomorphism. Since π is an isomorphism of finite rings, it preserves the size of a set and hence is a group isomorphism when restricted to $PP(\mathbf{Z}_n)$.

The next lemma is trivial but has great utility.

Lemma 3.2.

If $m \leq n$ and $f(x) \varepsilon PP(\mathbf{Z}_{p^n})$, then $f(x)$ acts on the congruence classes of $\mathbf{Z}_{p^n}$ modulo the ideal generated by p^m.

Proof:

Routine.

Lemma 3.3.

Fix n $\geq$ 2. Let π: $\mathbf{Z}[X]/I_{p^n} \rightarrow \mathbf{Z}[X]/I_{p^{n-1}}$ be the natural map. Then the map ρ that π induces on $PP(\mathbf{Z}_{p^n})$ is a group homomorphism onto $PP(\mathbf{Z}_{p^{n-1}})$.

Proof:

Since $I_{p^n} \subseteq I_{p^{n-1}}$, the natural map π exists. Let $f \in PP(\mathbf{Z}_{p^n})$. We know that f induces a 1:1 function on $\mathbf{Z}_{p^n}$. Lemma 3.2 tells us that f induces a well-defined function on $\mathbf{Z}_{p^{n-1}}$ as well, and it is easy to see that this function must also be 1:1. Since $\ker(\pi) = I_{p^n}$, we know that the function induced by f on $\mathbf{Z}_{p^{n-1}}$ is equal to the function induced by $f\pi$ on $\mathbf{Z}_{p^{n-1}}$. This means that $f\pi$ induces a 1:1 function on $\mathbf{Z}_{p^{n-1}}$ and hence that $\text{Image}(\rho) \subseteq PP(\mathbf{Z}_{p^{n-1}})$.

Since π is a ring homomorphism it preserves addition and multiplication. From this we see that it must preserve polynomial composition, which is just a combination of additions and multiplications. This means that ρ preserves polynomial composition, and hence is a group homomorphism, as specified. □

The next lemma is a special case of Lemma 1.3. I give a difference theoretic proof, more in the spirit of this chapter, rather than refer to Lemma 1.3.

Lemma 3.4.

Let n $\geq$ 2. Then $f(x) \in \mathbf{Z}[x]$ induces a permutation on $\mathbf{Z}_{p^n}$ iff $f'(x)$ has no roots (mod p), and f(x) induces a permutation on $\mathbf{Z}_{p^{n-1}}$.

To prove this lemma, I need to define the q-difference operator and make a claim about it. The q-difference operator Δ_q, which has the same domain as Δ, is defined by

$$\Delta_q f(x) = f(x+q)-f(x).$$

I claim that if n is 2 or more, then for f(x) in $\mathbf{Z}_{p^n}[x]$ we have that $\Delta_{p^{n-1}} f(x) = p^{n-1}\cdot f'(x) \pmod{p^n}$. A routine calculation shows this to be so. Now, the proof of Lemma 3.4.

($\Rightarrow$) Suppose that f(x) induces a permutation on $\mathbf{Z}_{p^n}$. Lemma 3.2 tells us that if $a \equiv b+p^{n-1}$ then $f(a) \equiv f(b) \pmod{p^{n-1}}$. Since the function induced by f(x) is injective, it follows that $f(b)-f(a)$ is a nonzero multiple of p^{n-1}. Since $f(b)- f(a) = (\Delta_{p^{n-1}} f)(a)$ we see that $\Delta_{p^{n-1}} f(x)$ is everywhere nonzero. By the claim this is equivalent to $f'(x)$ having no roots (mod p). As in the proof of Lemma 3.3, the fact that f induces a 1:1 function on $\mathbf{Z}_{p^n}$ is sufficient for it to induce a 1:1 function on $\mathbf{Z}_{p^{n-1}}$.

($\Leftarrow$) Suppose that f(x) induces a permutation on $\mathbf{Z}_{p^{n-1}}$ and that $f'(x)$ has no roots (mod p). Since f induces a 1:1 function on $\mathbf{Z}_{p^{n-1}}$, it suffices to show that f induces a 1:1 function on each equivalence class of $\mathbf{Z}_{p^n} \pmod{p^{n-1}}$. Let $A = \{a, a+p^{n-1}, \ldots, a+(p-1)p^{n-1}\}$ be one such equivalence class.

Since $f'(x)$ has no roots (mod p), the claim tells us that $\Delta_{p^{n-1}} f(x)$ has no roots (mod p^n). On the other hand, two applications of the claim show us that $\Delta^2_{p^{n-1}} f(x) = 0 \pmod{p^n}$. From this we can deduce that for b, $b+p^{n-1} \varepsilon A$, $f(b)-f(b+p^{n-1}) = k\cdot p^{n-1}$ for some $k \neq 0 \pmod{p}$ that doesn't depend on the choice of b. This in turn shows that f induces a 1:1 function on A since

$$A \;\mapsto\; \{f(a), f(a)+k\cdot p^{n-1}, \ldots, f(a)+(p-1)\cdot k\cdot p^{n-1}\},$$

which are all distinct values (mod p^n), as k is simply generating the additive group of $\mathbf{Z}_p$. □

Corollary 3.1.

Let $f(x) \in \mathbf{Z}[x]$. If $f(x)+I_{p^{n-1}} \in PP(\mathbf{Z}_{p^{n-1}})$ then $f(x)+I_{p^n} \in PP(\mathbf{Z}_{p^n})$ for all $n > 2$.

Proof:

If $f(x)+I_{p^{n-1}}$ is a permutation polynomial, it follows that it induces a 1:1 function on $\mathbf{Z}_{p^{n-1}}$. A simple computation shows that a p^{n-1}-ish polynomial has a p-ish derivative; hence for $n>2$, $(f(x)+g(x))' = f'(x) \pmod p$ for any p^{n-1}-ish polynomial g. By Lemma 3.4, $f'(x)$ has no roots (mod p) and hence neither does $(f+g)'$. Since g(x) is a residue polynomial over $\mathbf{Z}_{p^{n-1}}$, it follows that $f(x)+g(x)$ still induces a 1:1 function on $\mathbf{Z}_{p^{n-1}}$, so by Lemma 3.4, $f(x)+g(x)$ is a permutation polynomial over $\mathbf{Z}_{p^n}$ for any p^{n-1}-ish polynomial g(x). □

Notice that the corollary says for $f \in \mathbf{Z}[x]$ and $n > 2$ if $f(x)+I_{p^n}$ is in $PP(\mathbf{Z}_{p^n})$, then $f(x)+I_{p^m}$ is in $PP(\mathbf{Z}_{p^m})$ for any $m \geq n$. With the aid of Lemma 3.4 and Corollary 3.1 it is now possible to prove that ρ is a surjective group homomorphism.

Lemma 3.5.

$\rho : PP(\mathbf{Z}_{p^n}) \to PP(\mathbf{Z}_{p^{n-1}})$ is surjective.

Proof:

First deal with the case $n \geq 3$. Let $f(x)+I_{p^{n-1}}$ be a permutation polynomial in $PP(\mathbf{Z}_{p^{n-1}})$, and let $g(x) = f(x)+I_{p^n}$. Then by Corollary 3.1, $g(x) \in PP(\mathbf{Z}_{p^n})$. From the definition of ρ we see that $g(x)\rho = f(x)$; hence ρ is surjective.

Now take the case n=2. If we take some $f(x)+I_p \in PP(\mathbf{Z}_p)$ and let

$$g(x) = x^{(p)} \cdot (1+f'(x)) + f(x) + I_{p^2},$$

I claim that g(x) is a preimage of f(x) under ρ. A routine calculation with the product rule from [2] shows that $g'(x) \equiv p-1 \pmod p$; hence g' has no roots (mod p). From (3.2) and the fact that Δ preserves p-ishness, it follows that $x^{(p)}$ is p-ish. From this it follows that $g(x) = f(x) \pmod p$ and hence that g(x) induces a 1:1 function on $\mathbf{Z}_{p^{n-1}}$, since f does. This means that g(x) satisfies the conditions of Lemma 3.4 and we may deduce that $g(x) \in PP(\mathbf{Z}_{p^2})$. On the other hand, since $x^{(p)}$ is an element of I_p, it follows that $g\rho = f$, from the definition of ρ. □

Now we have the tools to obtain results on the isomorphism type of $PP(\mathbf{Z}_{p^n})$. The main task of this section is producing the isomorphism type and generators of $\ker(\rho)$. For $n \geq 3$ it turns out that $\ker(\rho)$ is an elementary abelian p-group. At the end of the section I will give a formula for $\left|PP(\mathbf{Z}_{p^n})\right|$.

As we saw in Example 1.1 all permutations of $\mathbf{Z}_p$ are induced by polynomials in $\mathbf{Z}_p[x]$. This follows directly from the fact that all functions from $\mathbf{Z}_p$ to $\mathbf{Z}_p$ can be realized as members of $\mathbf{Z}_p[x]$. Another way to see this is the following remark.

Remark 3.1

Let F be the finite field of order q. Then for each nonzero $a \varepsilon F$, the polynomial $f_a(x) = x+\sum_{k=2}^{q} a^k x^{q-k}$ is a permutation polynomial inducing the transposition (0 a) on F. As a varies through all of F, this gives us a set of transpositions that generate Sym(F). In particular, this means

$$PP(\mathbf{Z}_p) \cong S_p,$$

the symmetric group on p letters.

Now I want to produce the kernel of ρ in the case where $\rho : PP(\mathbf{Z}_{p^2}) \to PP(\mathbf{Z}_p)$. It turns out that the kernal of ρ is isomorphic to the direct product, p times, of the group of affine functions over $\mathbf{Z}_p$, $\{ax+b : a, b \varepsilon \mathbf{Z}_p, a \neq 0\}$.

Lemma 3.6.

If ρ: $PP(\mathbf{Z}_{p^2}) \to PP(\mathbf{Z}_p)$ then $|\ker(\rho)| = [p\cdot(p-1)]^p$.

Proof:

The definition of ρ shows that the elements of $\ker(\rho)$ are of the form $x+f(x)$, where $f(x)$ is p-ish. Theorem 3.2 tells us that I_p has a minimal generating set $\{p, x^{(p)}\}$ and that I_{p^2} has a minimal generating set $\{p^2, p\cdot x^{(p)}, x^{(2p)}\}$. From this we can see that a set of representatives for $\ker(\rho)$ is the set of all permutation polynomials over $\mathbf{Z}_{p^2}$ of the form

$$x+s(x)\cdot x^{(p)}+t(x)\cdot p, \qquad (*)$$

with the degrees and coefficients of r and s in the range 0 to p-1.

Now (*) clearly induces a 1:1 function on $\mathbf{Z}_p$, the identity. By Lemma 3.4 we need only compute how many choices of r and s give (*) a rootless derivative (mod p). If we

compute the derivative of (*), we get

$$s'(x)\cdot x^{(p)} + s(x)\cdot[x^{(p)}]' + p\cdot r'(x) + 1.$$

Removing those terms that are p-ish, we see that (*) is a permutation polynomial if

$$s(x)\cdot[x^{(p)}]' + 1 \neq 0.$$

A simple calculation shows that $[x^{(p)}]' \equiv (-1) \pmod{p}$, so we need only have that $s(x) \neq 1 \pmod{p}$ for all x. A trivial counting argument shows that there are $(p-1)^p$ such functions on $\mathbf{Z}_p$. Since all functions from $\mathbf{Z}_p$ to $\mathbf{Z}_p$ are induced by polynomials in $\mathbf{Z}_p[x]$ of degree less than p, we see that there are $(p-1)^p$ choices for s. The choice of r is completely free among the p^p polynomials that can be substituted for r in (*); hence there are $(p-1)^p \cdot p^p$ permutation polynomials in $\ker(\rho)$. □

Lemma 3.7.

The characteristic function $\chi_{(p)}$ of the ideal (p) generated by p in $\mathbf{Z}_{p^n}$ is a polynomial function.

Proof:

Notice that (p) is exactly the set of nonunits of $\mathbf{Z}_{p^n}$. Let U be the units of $\mathbf{Z}_{p^n}$ and set

$$f(x) = \prod_{u \in U} (x - u).$$

Then for each $u \in U$, $f(u) = 0$. If a is a nonunit, then f(a) is the product of all the elements of U. This means that the value of f is a constant unit γ on all of (p). Simply setting $\chi_{(p)}(x) = \gamma^{-1} f(x)$ gives us the characteristic function of (p) as a polynomial. □

Theorem 3.3.

Let H be the group of affine functions from $\mathbf{Z}_p$ to $\mathbf{Z}_p$. Then $PP(\mathbf{Z}_{p^2}) \cong H \text{ wr } S_p$.

Proof:

Claim 1 : Let $(a\cdot x+b) \varepsilon H$. Then

$$\iota: (a\cdot x+b) \mapsto \chi_{(p)}(x)\cdot(a\cdot x+b\cdot p)+(1-\chi_{(p)}(x))\cdot x$$

is an injective group homomorphism of H into $PP(\mathbf{Z}_{p^2})$ that moves (p) and fixes $\mathbf{Z}_p-(p)$.

Proof:

By Lemma 3.7, $(a\cdot x+b)\iota$ is a polynomial. Routine computation then proves the claim. Now, conjugating $H\iota$ by $(x+a)$ gives us a copy of H that moves a+(p) and fixes the rest of $\mathbf{Z}_p$. This yields p copies of H that move mutually disjoint subsets of $\mathbf{Z}_{p^2}$; hence we have a p-fold direct product of H inside $\ker(\rho)$, call it K. By Lemma 3.6, order considerations force K to be all of $\ker(\rho)$.

Now, I will produce a complement to K in $PP(\mathbf{Z}_{p^2})$ that is isomorphic to $PP(\mathbf{Z}_p)$. Let $R = \{0, 1, \ldots, p\text{-}1\}$ be a set of coset representatives for $\mathbf{Z}_{p^2} \pmod p$.

Claim 2 : For $\bar{\sigma} \varepsilon PP(\mathbf{Z}_p)$ there is some $\sigma^* \varepsilon PP(\mathbf{Z}_{p^2})$, so that $\sigma^*\rho = \bar{\sigma}$ and for a, b ε R such that $a\bar{\sigma} = b$, we have $(a+c\cdot p)\sigma^* = b+c\cdot p$.

Proof:

Let σ be any preimage of $\bar{\sigma}$ under ρ and transform σ into σ^* as follows. We know that $\sigma(a+c\cdot p) - \sigma(a) = \sigma'(a)\cdot cp$ where we saw in the proof of Lemma 3.4 that $\sigma'(x)\cdot p$ is constant $(\mathrm{mod}\ p^2)$ on a+(p). This means that $\sigma(a+c\cdot p) = b + k\cdot p + cp\cdot\sigma'(a)$. In claim 1 we showed there was a permutation that fixed all points not in b+(p) and which had the property that $\left(b + k\cdot p + cp\cdot\sigma'(a)\right) \mapsto \left(b+cp\right)$. Apply this permutation to σ and repeat the process for each member of R. The permutation you obtain in the end has the properties specified for σ^*.

Using the claim it is easy to see that the set $\{\sigma^* : \bar{\sigma}\varepsilon PP(\mathbf{Z}_p)\}$ is a copy of $PP(\mathbf{Z}_p)$

inside $PP(\mathbf{Z}_{p^2})$ that has trivial intersection with K; thus $PP(\mathbf{Z}_{p^2})$ is the semidirect product of K by $PP(\mathbf{Z}_p)$. It remains to show that the copy of $PP(\mathbf{Z}_p)$ acts on K in the fashion necessary for a wreath product. To see this, let H_a be a copy of H acting on a+(p) and let $\bar{\sigma} \in PP(\mathbf{Z}_p)$ take a to b. Then $H_a{}^{\sigma^*} = H_b$ by a simple computation, which is exactly what we need [3]. Since $PP(\mathbf{Z}_p) \cong S_p$, we have

$$PP(\mathbf{Z}_{p^2}) \cong H \text{ wr } S_p. \square$$

Lemma 3.8.

For $n \geq 3$, $\ker(\rho) = \{x + f(x) : f(x) \in I_{p^{n-1}}\}$.

Proof:

Certainly $\ker(\rho) \subseteq \{x + f(x) : f(x) \in I_{p^{n-1}}\}$. Let $f(x) \in I_{p^{n-1}}$. A simple computation shows that $f'(x)$ is p-ish; hence $(f(x)+x)' \equiv 1 \pmod{p}$. Since $f(x)+x$ induces identity on $\mathbf{Z}_{p^{n-1}}$, Lemma 3.4 tells us that $f(x)+x$ is a permutation polynomial.

Lemma 3.9.

Let $n \geq 3$. Then $\ker(\rho)$ is an elementary abelian p-group of order $\upsilon(n)$ where υ gives the size of a set of representative of $I_{p^{n-1}} \bmod I_{p^n}$.

Proof:

Let $\pi: \mathbf{Z}[x] \to \mathbf{Z}[x]/I_{p^n}$ be the natural map. Notice that the additive group G of $I_{p^{n-1}}\pi$ is abelian and that for each $f \in G$, $p \cdot f = 0$; hence G is an elementary abelian p-group. Let θ: $G \to \ker(\rho)$ be defined by $f\theta \mapsto f(x)+x$. I claim that θ is an isomorphism. By Lemma 3.8 θ is a bijection of G with $\ker(\rho)$, so I need only check that θ preserves the group operation. Let $f, g \in G$, with $f(x) = \sum f_i \cdot x^i$. Then

$$\begin{aligned}(f\theta)\circ(g\theta) &= \sum f_i \cdot (x+g(x))^i + g(x) + x, \\ &= f'(x) \cdot g(x) + f(x) + g(x) + x,\end{aligned}$$

$$= f(x) + g(x) + x, \quad \text{(recall } f'(x) \text{ is p-ish)}$$

$$= (f+g)\theta.$$

The fact that θ is an isomorphism gives $\ker(\rho)$ the desired size. □

Corollary 3.2.

Let $n \geq 3$ and let $\{q_i(x) : \iota \varepsilon I\}$ be the image under π of of the minimal generating set of $I_{p^{n-1}}$ given in Theorem 2, with the generator of highest degree removed if its image under π is 0. Then

$$\{x^k \cdot q_i(x) + x : i \varepsilon I,\ 0 \leq k < p\}$$

forms a minimal set of generators for $\ker(\rho)$.

Proof:

$\{x^k \cdot q_i(x) : i \varepsilon I,\ 0 \leq k < p\}$ is clearly a minimal generating set for the additive group of $I_{p^{n-1}}\pi$, and θ is an isomorphism. □

Lemma 3.10.

For the function υ, defined in Lemma 3.9, $\upsilon(n) = p^{\kappa(p^n)}$ for each $n \geq 3$.

Proof:

By looking at representatives of $I_{p^{n-1}}$ *mod* I_{p^n}, *we see that the following recursion* holds:

$$\upsilon(n) = \upsilon(n-1) \cdot p^{(\kappa(p^n) - \kappa(p^{n-1}))}.$$

Check that $\kappa(8) = 4$ and $\kappa(p^3) = 3p$ for all odd p. Then the recursion telescopes, giving the desired formula. □

Theorem 3.4. Size of $PP(\mathbf{Z}_{p^n})$.

(i) $\left|PP(\mathbf{Z}_p)\right| = p!$.

(ii) $\left|PP(\mathbf{Z}_{p^2})\right| = p!\cdot[p\cdot(p-1)]^p$.

(iii) for $n \geq 3$ $\left|PP(\mathbf{Z}_{p^n})\right| = p!\cdot[p\cdot(p-1)]^p \cdot p^{\sum_{k=3}^{n-1} \kappa(p^k)}$

Proof:

(i) follows from a remark. (ii) follows from (i) and Lemma 3.6. (iii) follows from (ii) and Lemma 3.10.

§4 Computation of the ideal $I^{\mathbf{Z}_n^{m\times m}}_{\mathbf{Z}_n}$.

In this section I will abbreviate $I^{\mathbf{Z}_n^{m\times m}}_{\mathbf{Z}_n}$ and $I^{\mathbf{Z}_n^{m\times m}}_{\mathbf{Z}}$ by the more wieldy notation I_n^m, with the meaning of the abbreviation being implied by context. A basis for one of these ideals differs from the other only by the addition or subtraction of p^n. I will call a polynomial in $\mathbf{Z}_n[x]$ m-matrix n-ish if it is a member of the ideal I_n^m. My goal in this chapter is to create a basis for $I_{p^n}^m$ and as a consequence, compute the number of scalar polynomial functions from $\mathbf{Z}_n^{m\times m}$ to itself. For the case n prime, see[11], and refer also to Example 2.2.

The first step is to reduce the problem for general n to prime powers, which is done exactly the way you would think.

Lemma 3.11. Suppose that $n = p_1^{e_1}\cdot p_2^{e_2}\cdot \cdots \cdot p_k^{e_k}$ is a factorization of n into powers of distinct primes. Then

$$I^{\mathbf{Z}_n^{m\times m}}_{\mathbf{Z}} = \bigcap_{i=1}^{k} I^m_{p^{e_i}}.$$

Proof:

Follows from the Chinese Remainder Theorem decomposition

$$\mathbf{Z}_n^{m\times m} \cong \bigotimes_{i=1}^{k} \mathbf{Z}_{p^{e_i}}^{m\times m},$$

and Lemma 1.4 (ii).

Recall[11] that for p prime,

$$I_p^m = \langle \prod_{\iota=1}^{m} (x^{p^\iota} - x) \rangle, \text{ or} \tag{3.3}$$

if we let $\Lambda_\iota = \{f(x) \in \mathbf{Z}_p[x] : f(x) \text{ an irreducible of degree } \iota\}$, then

$$I_p^m = (\prod_{\iota=1}^{m} \prod_{f \varepsilon \Lambda_\iota} f(x)^{\left\lceil \frac{m}{\iota} \right\rceil}).$$

These characterizations both come from noting that every polynomial of degree m has a companion matrix in $\mathbf{Z}_p^{m \times m}$, and taking the least common multiple of all such polynomials to obtain a generator for I_p^m. It is possible to extend a weakened version of this technique to $\mathbf{Z}_{p^n}$ and to obtain generators for $I_{p^n}^m$.

Lemma 3.12. $I_{p^n}^m$ is exactly the ideal of polynomials having each polynomial, of degree m or less, congruent modulo p to a power of an irreducible of $\mathbf{Z}_p[x]$, as a divisor.

Proof:

Lemma 2.6 says that being divisible by any polynomial of degree $\leq$ m is equivalent to the putative condition for membership in $I_{p^n}^m$. It is easy to see that being divisible by any polynomial in $\mathbf{Z}_{p^n}[x]$ of degree m or less is equivalent to being divisible by all monic polynomials of degree exactly m. Now let $f(x) \varepsilon \mathbf{Z}_{p^n}$ be a monic polynomial of degree m and let A be the companion matrix of f(x). The ones that appear above the diagonal of A ensure that A satisfies no polynomial relation of degree less than m. By applying the division algorithm we see that this forces each member of $I_{p^n}^m$ to be divisible by f(x). On the other hand, polynomials divisible by all polynomials of degree $\leq$ m are certainly satisfied by each mxm matrix over $\mathbf{Z}_{p^n}$. □

Lemma 3.12 reduces the problem of finding $I_{p^n}^m$ to one of computing least common multiples in $\mathbf{Z}_{p^n}[x]$. Unfortunately the usual definition of the least common multiple with its intimations of uniqueness doesn't apply here. As it turns out we may be satisfied with least degree common multiples. First notice that the problem may (must) be done separately, one irreducible at a time. I will follow the rough outlines of the technique used to compute I_n in the first two sections of this chapter.

Lemma 3.13. If $f(x) \equiv \iota(x)^k \pmod{p}$ for an irreducible $\iota(x) \varepsilon \mathbf{Z}_p[x]$ of degree d, then the degree of a monic common multiple of all members of $\mathbf{Z}_{p^n}$ congruent to f(x) mod p equals or exceeds

$$\kappa(d\ ,\ k;\ p^n) = d \cdot \min\left\{ i : \sum_{j=0}^{\infty} \left[\frac{i}{p^{j \cdot d \cdot k}} \right] \geq n \right\},$$

and the proof constructs a common multiple attaining the bound.

Proof:

This formula should be reminiscent of the one for the power of a prime dividing a factorial. When d=1 it is exactly a comparison based on that formula. Now notice that the degree of f(x) is exactly $d \cdot k$. Each polynomial in $\mathbf{Z}_{p^n}$ congruent to f(x) (mod p) differs from each other such polynomial by a multiple of p (by definition). Generalizing this one sees that exactly the fraction

$$\left(\frac{1}{p^{\deg(f)}} \right)^j$$

of these polynomials differs from f(x) by a multiple of p^j. This is because each of the deg(f) coefficents, those other than the first, must all differ from the corresponding coefficient of f(x) by a multiple of p^j. This is the key to constructing a polynomial that attains the bound. Simply multiply sets of polynomials congruent to f(x) (mod p) that complete equivalence classes (mod p), (mod p^2), ... as often as possible. This ensures that you will arrive at a set of polynomials so that as many as possible differ from each possible divisor by the highest possible power of p. One then sees this process gives the stated bound. □

Example 3.2 . Compute a least degree common multiple g(x) of all monic polynomials in $\mathbf{Z}_{32}[x]$ congruent to $x^2+x+1 \pmod{2}$.

The set of all such polynomials is of the form

$$D = \left\{x^2+(2k+1)x+(2m+1) : 0 \leq k,m \leq 15\right\}.$$

Lemma 3.13 tells us that we should be able to do the job with an 8th degree polynomial. It should be the product of four members of D that sweep out an equivalence class (mod 4). So take

$$g(x) = (x^2+x+1)\cdot(x^2+x+3)\cdot(x^2+3x+1)\cdot(x^2+3x+3), \text{ or}$$

$$g(x) = x^8+7x^7+30x^6+8x^5+23x^4+5x^3+6x^2+16x+9.$$

With Lemma 3.13 in hand we can compute the degree of a least degree of a monic m-matrix p^n-ish polynomial.

Corollary 3.3. Let $\pi(d)$ denote the number of irreducibles of degree d in $\mathbf{Z}_p[x]$. Then

$$\kappa_m(p^n) = \sum_{d=1}^{m} \pi(d)\cdot\kappa(d, [\tfrac{m}{d}]; p^n)$$

is exactly the least degree of a monic m-matrix p^n-ish polynomial.

Proof:

Lemma 3.12 tells us that we want every polynomial of degree $\leq$ m congruent (mod p) to a power of an irreducible of $\mathbf{Z}_p[x]$ as a divisor of our putative m-matrix p^n-ish polynomial. This polynomial would then be the product, over the set of possible irreducibles, of least degree common multiples of all monic polynomials congruent (mod p) to the highest power of the irreducible of degree not exceeding m. The sum and $\pi(d)$ cover the set of possible irreducibles, and by Lemma 3.13, $\kappa(d, [\frac{m}{d}];p^n)$ is the degree of the required least degree common multiple; hence the stated degree is correct. □

In the case of $\mathbf{Z}_n$, the factorial function handily captured the maximal degree of n-ishness one could expect from a polynomial. For the matrix case we need an analogous

function.

Corollary 3.4. Let

$$\mathfrak{D}_m(k) = \prod_{p \text{ prime}} p^{\max\left\{i \,:\, \kappa_m(p^i) \le k\right\}};$$

then if g(x) is monic of degree d, then it is at best, in the sense of division, m-matrix $\mathfrak{D}_m(d)$-ish.

Proof:

The Chinese Remainder Theorem allows us to find polynomials simultaneously congruent to any choice of polynomials modulo the assorted prime divisors of a given integer. The powers of the primes in the above formula are, by Corollary 3.3, exactly the best one could hope for, given the degree of the polynomial, hence the corollary is true. □

At this point I want to extend $\kappa_m(p^n)$ to nonprime powers. Recalling Proposition 3.2, it is no surprise that I will take

$$\kappa_m(n) = \max\left\{\kappa_m(p^k) \,:\, p^k \text{ a prime power divisor of } m\right\}. \tag{3.4}$$

Corollary 3.5 If g(x) is monic and m-matrix n-ish, then its degree equals or exceeds $\kappa_m(n)$; further, a g(x) with degree exactly $\kappa_m(n)$ can always be found.

Proof:

That this degree is necessary follows from the definition of $\kappa_m(n)$ and Corollary 3.3. That it is sufficient follows from the Chinese Remainder Theorem. That the polynomial desired exists is a consequence of the constructive nature of Corollary 3.3. □

Corollary 3.6. $\kappa_1(n) = \kappa(n)$.

Proof:

Routine computation. □

At this point I want to take a detour off the road leading to the computation of generators for $I^m_{p^n}$ and take time out to perform the obvious generalization of Singmaster's result from Section 1.

Lemma 3.14. If q(x) is m-matrix n-ish of degree d, then $\frac{n}{(n, \mathfrak{D}_m(d))}$ divides the content of q(x).

Proof:

Suppose that the lemma fails for some q(x). Then from (3.4) we deduce that for some prime power divisor p^k of n that $d<\kappa_m(p^k)$. Let $e = \max\{i : d\geq\kappa_m(p^i)\}$. Now if for each such prime it was true that p^{k-e} divided the content of q(x), then the lemma would hold, so assume without loss that p^{k-e} fails to divide the content of q(x). Then for some $j < k-e$, we see that $q(x) = p^j \cdot s(x)$, where s(x) has some coefficient that is invertible (mod p^n). Iterating the reduction of s(x) by appropriate members of $I^m_{p^n}$, the generators given in Corollary 2.6, and multiplying by well-chosen powers of x, we may produce a new polynomial $\bar{s}(x)$ so that $p^j \cdot \bar{s}(x)$ is still m-matric p^k-ish of degree less than or equal to d, but the leading coefficient of $\bar{s}(x)$ is invertible modulo p^k. By multiplying by an appropriate unit of $\mathbf{Z}_{p^k}$ and reducing mod p^k, we find that we have a new polynomial $p^j \cdot s^*(x)$ that is monic, m-matrix p^k-ish, and of degree d or less. From this we deduce that q(x) must be m-matrix p^{k-j}-ish, but since $j < k-e$, we have a

contradiction of Corollary 3.3. □

Theorem 3.5 The number of scalar polynomial functions from $\mathbf{Z}_n^{m\times m}$ to itself is

$$\prod_{d=0}^{\kappa_m(n)-1} \frac{n}{(n,\ \mathfrak{D}_m(d))}.$$

Proof:

Corollary 3.5 and Lemma 3.14 imply that we may construct polynomials of degree d of the form

$$s_d(x) = \frac{n}{(n,\ \mathfrak{D}_m(d))}\cdot f_d(x)$$

with f_d monic so that the set $S = \left\{s_d(x) : d=1, 2, 3, \ldots\right\}$ is a generating set of I_n^m. If we suppose that this is not so, then there exists some f(x) that is m-matrix n-ish that has a nontrivial remainder r(x) when reduced modulo $\langle S\rangle$. This remainder must necessarily violate Lemma 3.14; hence no such f(x) exists. The set of nontrivial remainders modulo $\langle S\rangle$ is then a set of representatives of the distinct $\mathbf{Z}_n$-polynomial functions of $\mathbf{Z}_n^{m\times m}$. These nontrivial remainders can be taken to be polynomials with the coefficient of x^d in the range $0 \leq c < \frac{n}{(n,\ \mathfrak{D}_m(d))}$. This together with the fact that $\mathfrak{D}_m(\kappa_m(n))$ is a multiple of n shows the formula to be correct.

We are now ready to produce a basis for I_n^m. This will be done in a manner analogous to Theorem 3.2. First we need to define

$$\Lambda_n^m = \left\{\kappa_m(d) :\ d \mid n\right\},$$

and let $q_m(x;\ k)$ denote some monic m-matrix $\mathfrak{D}_m(k)$−ish polynomial of degree k. We see from Corollaries 3.3 and 3.4 that such polynomials exist.

Theorem 3.6

$$G = \left\{ \frac{n}{(n,\ \mathfrak{D}_m(k))} \cdot q_m(x;\ k) : k \varepsilon \Lambda_n^m \right\}$$

is a basis for I_n^m in $\mathbf{Z}[x]$.

Proof:

Let $J_n^m = \langle \frac{n}{(n,\ \mathfrak{D}_m(k))} \cdot q_m(x;\ k) : k \varepsilon \Lambda_n^m \rangle$. Then the choice of the scalar factor ensures that $J_n^m \subseteq I_n^m$. Let $f(x)$ be an element of I_n^m and assume by way of contradiction that $f(x) \notin J_n^m$. If the degree and content of $f(x)$ simultaneously exceed those of one of the generators of J_n^m, we may take the remainder of $f(x)$ divided by that generator, obtaining a member of I_n^m that fails to exceed the degree and content. Since the contents of the generators are ordered by divisibility in the reverse order of degree of the generators, we may in fact obtain a member of I_n^m from $f(x)$, simulaneously exceeding or equaling the degree and content of no generator of J_n^m. This resulting polynomial would, however, contradict Lemma 3.14, hence $J_n^m = I_n^m$. It remains to show that the generating set is minimal.

From Lemma 3.13 and the Chinese Remainder Theorem we see that we may assume without loss of generality that for $k_1, k_2 \varepsilon \Lambda_n^m$, $k_1 < k_2 \Rightarrow q_m(x;\ k_1) \mid q_m(x;\ k_2)$. Now order $\Lambda_m^n = \{k_1 > k_2 > \cdots > k_\ell\}$ and set $g_i(x) = \frac{n}{(n,\ \mathfrak{D}_m(k_i))} \cdot q_m(x;\ k_i)$, the various generators. If the generating set given is not a basis, then for some i, $g_i(x)$ must be a linear combination with polynomial coefficients of the others. Let

$$r(x) = \sum_{j>i} c_j(x) \cdot g_j(x), \text{ and}$$

$$s(x) = \sum_{j<i} c_j(x) \cdot g_j(x),$$

so that $g_i(x) = r(x)+s(x)$. Since the contents of the generators are ordered by divisibility in the reverse of their degrees, it follows that $\frac{n}{(n, \mathfrak{D}_m(k_i))}$ divides $s(x)$ and hence $r(x)$. Likewise, since the primitive parts of the generators divide one another it follows that $q(x; k_i)$ divides $r(x)$. Since $g_i(x)$ is a scalar multiple of $q(x; k_i)$, we may conclude that $q(x; k_i)$ divides $s(x)$. Finally, since Λ_n^m captures exactly the point when the content of an m-matrix n-ish polynomial must change to compensate for its degree, the divisibility ordering of the contents of the assorted generators is strict. From this we may deduce that the content of $s(x)$ is a proper multiple of the content of $g_i(x)$. Thus for some constant $C>2$, there are $a(x)$ and $b(x)$ so that

$$g_i(x) = \frac{n}{(n, \mathfrak{D}_m(k_i))} \cdot q(x; k_{i+1}) + C \cdot \frac{n}{(n, \mathfrak{D}_m(k_i))} q(x; k_i) \cdot b(x). \qquad (*)$$

Now since the degree of $q(x; k_{i+1})$ is strictly greater than $q(x; k_i)$, it follows that the companion matrix A of $q(x; k_{i+1})$ satisfies $q(x; k_{i+1})$ but not $q(x; k_i)$. Specialize $(*)$ at A, expand $g_i(x)$ and see that we obtain the identity,

$$\frac{n}{(n, \mathfrak{D}_m(k_i))} \cdot q(A; k_i) = C \cdot \frac{n}{(n, \mathfrak{D}_m(k_i))} q(A; k_i) \cdot b(A).$$

Since integral matrices have integral determinants and the left side of the above expression is not zero, this is impossible; hence $gI(x)$ is not a linear combination of the other generators. □

§5. Membership and Enumeration of the Group $PP_{\mathbf{Z}_n}(\mathbf{Z}_n^{m\times m})$.

In this section I will apply the techniques and tools of the first two chapters to delineating and enumerating the $\mathbf{Z}_n$-permutation polynomials of the matrices over $\mathbf{Z}_n$. In [8] J. V. Brawley computes the order of $PP_m(GF(q))$ and hence by specialization, $PP_m(\mathbf{Z}_p)$. The only material on the isomorphism type of $PP_m(\mathbf{Z}_p)$, of which I am aware, appears in [8] and [9], and no attempt is made to compute the structure of the group. As part of the proof of his formula for the order of $PP_m(GF(q))$, Brawley gives an effective but tedious construction for members of the group; i.e., he can produce the polynomial associated with a given permutation of matrices if one exists, and I see no way of improving his technique. No test for membership in $PP_m(\mathbf{Z}_p)$ exists for arbitrary polynomials. In fact, the problem of determining membership other than by direct testing is the subject of ongoing research in the case $m=1$ (see [7], Chapter 7).

I will denote by ρ_n the group homomorphism from $PP_m(\mathbf{Z}_{p^n})$ to $PP_m(\mathbf{Z}_{p^{n-1}})$, induced by the (mod p) homomorphism as described in Lemma 1.7. As always the Chinese Remainder Theorem allows us to restrict our investigation of $PP_m(\mathbf{Z}_n)$ to $\mathbf{Z}_{p^n}$ in the following fashion.

If $n = q_1 \cdot q_2 \cdot \cdots \cdot q_r$ is a factorization of n into powers of distinct primes, then the Chinese Remainder Theorem implies

$$PP_m(\mathbf{Z}_n) \cong PP_m(\mathbf{Z}_{q_1}) \times PP_m(\mathbf{Z}_{q_2}) \times \cdots \times PP_m(\mathbf{Z}_{q_r}). \tag{3.5}$$

I will continue to use the notation I_n^m for the ideal of m-matrix n-ish polynomials in $\mathbf{Z}[x]$ or $\mathbf{Z}_n[x]$. By $\pi(n)$ I will denote the number of irreducible polynomials of degree n in

$\mathbf{Z}_p[x]$.

The computation of $\left|PP_m(\mathbf{Z}_{p^n})\right|$ breaks into three parts: $n=1$, $n=2$, and $n\geq 3$. The case $n=1$ is done by Brawley in [10] but is also a consequence of Example 2.2 and Corollary 2.5. For completeness I will restate Brawley's result here.

$$\left|PP_m(\mathbf{Z}_p)\right| = \prod_{k=1}^{m} k^{\pi(k)}\pi(k)!\cdot\prod_{k=1}^{[m/2]}\left(\left(p^k-1\right)\cdot\left(p^{k\cdot([m/k]-2)}\right)\right)^{\pi(k)} \tag{3.6}$$

Now, for the remaining cases we will need to ascertain what the specialization of the lifting lemma is in the matrix case. This lemma is a consequence of Theorem 3, page 98, of [10]. My proof is much simpler than the one given in [10] as it avoids tensor products and ugly matrix arithmetic. This is a result of applying Theorem 1.1.

Lemma 3.15 A polynomial $f(x)\varepsilon PP_m(\mathbf{Z}_{p^n})$ iff $f(x)\varepsilon PP_m(\mathbf{Z}_{p^{n-1}})$ and $f'(x)$ is root-free (mod p) on $\mathbf{Z}_p^{m\times m}$.

Proof:

Set $A = \mathbf{Z}_{p^n}[x]/I_{p^n}^m$, and $B = \mathbf{Z}_{p^{n-1}}[x]/I_{p^{n-1}}^m$. Then Theorem 1.1 tells us that $f(x)\varepsilon PP_m(\mathbf{Z}_{p^n})$ iff $f(x)\varepsilon PP_{\mathbf{Z}_{p^n}}(A)$ and $f(x)\varepsilon PP_m(\mathbf{Z}_{p^{n-1}})$ iff $f(x)\varepsilon PP_{\mathbf{Z}_{p^{n-1}}}(B)$, so the problem is reduced to finding when a member $PP_{\mathbf{Z}_{p^{n-1}}}(B)$ lifts to a member of $PP_{\mathbf{Z}_{p^n}}(A)$. Now since $I_{p^n}^m \subseteq I_{p^{n-1}}^m$, we see that B is A modulo the nilpotent ideal $J = I_{p^{n-1}}^m$ taken modulo $I_{p^n}^m$. This means that we may apply Lemma 1.3. The question then becomes, when can $f'(x)$, by multiplication, increase the degree of nilpotency of some element of A? I claim that this happens exactly when $f'(x)$ is divisible (mod p) by

any irreducible in $\mathfrak{J}$, the set of all irreducibles of degree 1, 2, ..., m. Notice that nilpotent elements of A are exactly the cosets of polynomials simultaneously divisible (mod p) by all members of $\mathfrak{J}$. By examining the definition of $\kappa_m(p^n)$, it is easy to see that the generators of $I^m_{p^k}$, $k \geq 2$ are in fact divisible (mod p) by the square of each irreducible in $\mathfrak{J}$; hence there exist elements of A whose degree of nilpotency can be increased by multiplication by any polynomial congruent (mod p) to a multiple of a member of $\mathfrak{J}$.

By the same token, multiplication by a polynomial congruent (mod p) to a multiple of a member of $\mathfrak{J}$ is the only multiplication capable of increasing the nilpotency of a member of J; hence $f'(x)$ must simply avoid having divisors (mod p) in $\mathfrak{J}$. The fact that minimal polynomials of matrices in $\mathbb{Z}_p^{m\times m}$ are exactly products of members of $\mathfrak{J}$ means that this condition on $f'(x)$ is exactly equivalent to being root-free on $\mathbb{Z}_p^{m\times m}$. □

With the correct version of the lifting lemma in hand, we have a test for membership in $PP_m(\mathbb{Z}_{p^n})$. We may now proceed to the enumeration for $n\geq 2$.

Theorem 3.7. The homomorphism ρ_n is surjective, and the size of $\ker(\rho_n)$ is given by

(n=2) Set $q = [\frac{m}{2}]+1$, then

$$|\mathrm{Ker}(\rho_2)| = p^{2p\cdot(p^m-1)/(p-1)}\cdot\prod_{d=q}^{m}\left(1-\frac{1}{p^d}\right)^{\pi(d)}, \text{ and} \qquad (3.7)$$

($n\geq 3$)

$$|\mathrm{Ker}(\rho_n)| = p^{\kappa_m(p^n)}. \tag{3.8}$$

Proof:

In the course of this proof I will compute the number of preimages under ρ_n of an arbitrary element $\alpha(x)$ of $PP_m(\mathbf{Z}_{p^{n-1}})$. That the number of preimages is independent of the choice of the element suffices to show that ρ_n is surjective. Let $L(x)$ be the generator of I_p^m given in Example 2.2. Recall that ρ_n is the restriction to permutation polynomials of the natural map $\bar{\pi} : \mathbf{Z}_{p^n}[x]/I_{p^n}^m \to \mathbf{Z}_{p^{n-1}}[x]/I_{p^{n-1}}^m$ given in Lemma 1.7. In the case (n=2) this means that preimages of $\alpha(x)$ are all of the form

$$\alpha_s^r(x) = \alpha(x)+r(x)\cdot L(x)+s(x)\cdot p,$$

with $r(x)$ and $s(x)$ having degree less than the degree of $L(x)$ and coefficients in the range $0 \leq c < p$. This follows from the fact, given by Theorem 3.6 and routine computation, that

$$I_p^m = \langle L(x), p\rangle, \text{ and}$$

$$I_{p^2}^m = \langle L(x)^2, p\cdot L(x), p^2\rangle,$$

as ideals of $\mathbf{Z}[x]$.

What remains then is to compute how many choices of $r(x)$ and $s(x)$ actually yield a permutation polynomial under the auspices of Lemma 3.15. This amounts to checking when $\alpha_s^r(x)'$ is root-free on $\mathbf{Z}_p^{m\times m}$, or equivalently, when $\alpha_s^r(x)'$ has no irreducible divisors of degree 1, 2, ..., m. Computing the derivative, we obtain

$$\alpha_s^{r\prime}(x) = \alpha'(x)+r(x)\cdot L(x)+r(x)\cdot L'(x)+p\cdot s'(x). \tag{$*$}$$

Any multiple of p is m-matrix p-ish as is $L(x)$ by construction; hence the terms

involving p and L(x) are zero everywhere on $\mathbf{Z}_p^{m\times m}$. What we need then is for the remaining terms to be everywhere nonzero. Thus

$$\alpha(x)'+r(x)\cdot L'(x)$$

must have no irreducible divisors of degree $\leq$ m. This, however, is a type of computation we have done before, in the proof of Theorem 2.3. There are $p^{\deg(L(x))}$ candidates for r(x) and, since $L'(x)$ is constructively root-free on $\mathbf{Z}_p^{m\times m}$, r(x) must avoid a single value modulo each irreducible of degree $\leq$ m that can divide $\alpha'(x)$.

Happily, $\alpha'(x)$ cannot have irreducible divisors (mod p) of degree $\leq [\frac{m}{2}]$. Since L(x) is divisible by the square of such irreducibles and since $\alpha(x)$ is forced by Theorem 1.1 and Lemma 1.1 to be a $\mathbf{Z}_p$-permutation polynomial of $A = \mathbf{Z}_p[x]/(L(x))$, we see Lemma 1.3 and the existence of the nilpotent ideal of A generated by the coset of the maximal square-free divisor of L(x) force $\alpha'(x)$ to be root-free modulo such irreducibles. This leaves us with the irreducibles of degree $[\frac{m}{2}]+1$ or more.

The Chinese Remainder Theorem tells us that the constraints satisfied for each irreducible are independent; thus the fraction of viable candidates is the product of viable candidates modulo each irreducible. So of the possible choices for r(x), exactly the fraction

$$\prod_{k=q}^{m}\left(1-\frac{1}{p_k}\right)^{\pi(k)}$$

of the possible choices allow the satisfaction of Lemma 3.15. There are also $p^{\mathrm{Deg}(L(x))}$ choices for s(x) all of which allow the satisfaction of Lemma 3.15; hence the total number of preimages of $\alpha(x)$ under ρ_2 is

$$p^{\mathrm{Deg}(L(x))} \cdot p^{\mathrm{Deg}(L(x))} \cdot \prod_{k=q}^{m} \left(1-\frac{1}{p_k}\right)^{\pi(k)}.$$

Recall that

$$L(x) = \prod_{k=1}^{m} \left(x^{p^k} - x\right),$$

so $\mathrm{Deg}(L(x)) = p \cdot \frac{p^k-1}{p-1}$. Plugging this into $(*)$ gives the stated result for $n=2$.

Now we turn to the case $n \geq 3$. Notice, as in Lemma 3.10 for κ_1, that the formula given in 3.8 for $|\ker(\rho_n)|$ is exactly the size of a set of representatives of $I_{p^n}^m$ modulo $I_{p^{n-1}}^m$ or, in other words, exactly $|\ker(\bar{\pi})|$. This means that every possible preimage of a $\mathbf{Z}_{p^{n-1}}$-permutation polynomial of $\mathbf{Z}_{p^{n-1}}^{m \times m}$ under $\bar{\pi}$ must be a $\mathbf{Z}_{p^n}$-permutation polynomial of $\mathbf{Z}_{p^n}^{m \times m}$, for each $n \geq 3$. By Lemma 3.15 this is equivalent to all possible preimages having a root-free formal derivative on $\mathbf{Z}_p^{m \times m}$, which, by an application of Lemma 3.15 with $n=2$, must be so. Thus all preimages of permutation polynomials under $\bar{\pi}$ are in fact permutation polynomials themselves, and the formula given for $n \geq 3$ is correct. □

Corollary 3.7. Let $f(x) \in \mathbf{Z}[x]$. If $f(x)+I_{p^n}^m \in PP_m(\mathbf{Z}_{p^n})$, $n \geq 2$, then $f(x)+\langle I_{p_k}^m \rangle \in PP_m(\mathbf{Z}_{p^k})$ for all $k = 1, 2, \ldots$.

Proof:

This is simply a restatement of a portion of the final paragraph of the preceding proof.

Now I will wrap up the chapter by bringing together the assorted information on the size of $PP_m(\mathbf{Z}_{p^n})$. Notice that each of the formulas given below simply build on the previous one.

Corollary 3.8 If $q = [\frac{m}{2}]+1$, then the size of $PP_m(\mathbf{Z}_{p^n})$ is

$$\text{(i)} \prod_{k=1}^{m} k^{\pi(k)} \pi(k)! \cdot \prod_{k=1}^{[m/2]} \left(\left(p^k - 1 \right) \cdot \left(p^{k \cdot ([m/k]-2)} \right) \right)^{\pi(k)}, \qquad (n=1)$$

$$\text{(ii)} \prod_{k=1}^{m} k^{\pi(k)} \pi(k)! \cdot \prod_{k=1}^{[m/2]} \left(\left(p^k - 1 \right) \cdot \left(p^{k \cdot ([m/k]-2)} \right) \right)^{\pi(k)} \times \qquad (n=2)$$

$$p^{2p \cdot (p^m - 1)/(p-1)} \cdot \prod_{k=q}^{m} \left(1 - \frac{1}{p^k} \right)^{\pi(k)}, \text{ and}$$

$$\text{(iii)} \prod_{k=1}^{m} k^{\pi(k)} \pi(k)! \cdot \prod_{k=1}^{[m/2]} \left(\left(p^k - 1 \right) \cdot \left(p^{k \cdot ([m/k]-2)} \right) \right)^{\pi(k)} \times \qquad (n \geq 3)$$

$$p^{2p \cdot (p^m - 1)/(p-1)} \cdot \prod_{k=q}^{m} \left(1 - \frac{1}{p^k} \right)^{\pi(k)} \times \prod_{k=3}^{n} p^{\kappa_m(p^n)}.$$

Proof:

Follows from (3.6), (3.7), and (3.8). □

In order to give a sense of concreteness to the above formulas, I will give, on the following page, the actual numbers involved for small values of the parameters. Appendix B contains the values of the special functions used. See also Appendix C.

Table 3.2

Order of $PP_m(\mathbf{Z}_n)$.

m	2	3	4	5
1	2	6	8	120
2	4	$2^8 3^2$	$2^{12} 3^1$	$2^{31} 3^5 5^3 7^1$
3	$2^5 3^2$	$2^{15} 3^{15} 5^1 7^1$	$2^{25} 3^3 7^2$	$2^{49} 3^{23} 5^{12} 7^6 11^3 13^3 \cdot 17^2 19^2 23^1 29^1 31^1 37^1$
4	$2^{14} 3^4$	$2^{76} 3^{26} 5^4 7^3 \cdot 11^1 13^1 17^1$	$2^{54} 3^8 5^3 7^2$	$5! \cdot 10! \cdot 40! \cdot 150! \cdot 2^{350} 3^{50} 5^{10}$

Chapter 4

Applications and Topics for Future Work.

§0 Introduction and Summary.

This chapter is a potpourri of results related to the main results of my thesis and a few applications of results, particularly Lemma 1.2. In Section 1 I will compute the permutation polynomials of the p-adic integers with p-adic coefficients. In Section 2, I will compute the compositional attractors associated with the group algebras of finite fields over finite abelian groups. In Section 3 I will define multidimensional compositional attractors and give a list of topics for additional consideration.

§1 The Permutation Polynomials of the p-adic Integers.

In this section $\mathbf{Z}_p$ will denote the p-adic integers and $\mathbf{Z}/n$ will denote the integers modulo n. The p-adic integers are the set of all series $\{a_k : k \geq 1\}$ so that

$$a_k \in \mathbf{Z}/p^k, \text{ and} \tag{4.1}$$

$$a_{k+1} \equiv a_k \pmod{p^k}. \tag{4.2}$$

They are given the structure of a ring by

$$\{a_k\}+\{b_k\} = \{a_k+b_k\}, \text{ and}$$

$$\{a_k\}\times\{b_k\} = \{a_k \times b_k\}.$$

Denote by π_m the natural projection homomorphism from $\mathbf{Z}_p$ to $\mathbf{Z}/p^m$ given by $\{a_k\} \mapsto a_m$. Let π_m^* be the extension of π_m to polynomials. With these definitions we may characterize the p-adic permutation polynomials of the p-adic integers.

Theorem 4.1. Let $S=\mathbf{Z}/p^2$, $R = \mathbf{Z}_p$. Then $f(x) \in PP_R(R)$ iff $f(x)\pi_2^* \in PP_S(S)$.

Proof:

($\Rightarrow$) Suppose that $f(x) \in PP_R(R)$. Then the function $r \mapsto f(r)$ is 1:1 on R and hence $s \mapsto f(x)\pi_2^*(s)$ is 1:1 on $S = R\pi_2$. Thus $f(x)\pi_2^* \in PP_S(S)$.

($\Leftarrow$) Suppose that $f(x)\pi_2^* \in PP_S(S)$. Then Corollary 3.1 says that $f(x)\pi_m^* \in PP_{R\pi_m}(R\pi_m)$ for all $m \geq 2$. Assume then by way of contradiction that for $r, s \in R$, $r \neq s$ but that $f(r) = f(s)$. Since $r \neq s$, there is some m so that $\forall\, l \geq m$, $r\pi_l \neq s\pi_l$, but for each such l, $f(r)\pi_l = f(s)\pi_l$, which contradicts the information yielded by Corollary 3.1. □

§2 Permutation Polynomials of Abelian Group Algebras over Finite Fields.

In this section $F = GF(q)$, $q = p^n$, G is a finite abelian group, and $R = F[G]$, the group algebra of F over G. As in Chapter 2, $\pi(n)$ will denote the number of irreducibles of degree n in $F[x]$. I will compute the compositional attractor I_F^R and from it the size of $PP_F(R)$. When the exponent on G and p are relatively prime, I will also give the isomorphism type of the group.

Theorem 4.2. Suppose that $G = <\sigma>$ is a cyclic group of order $m = p^k \cdot s$, where s, and p are relatively prime. Set $R = F[G]$ and let r be the order of q (mod s). Then

$$I_F^R = <\left(x^{q^r} - x\right)^{p^k}>.$$

Proof:

Let $f(x) = x^{q^r} - x$; let

$$\alpha = \sum_{i=0}^{m-1} f_i \sigma^i$$

be an arbitrary element of R, and take $g(x)$ to be the generator of I_F^R. Since $q^r \equiv 1 \pmod{s}$, there is some t so that $q^r = st+1$. Then a short computation shows that

$$f(\alpha) = \sum_{i=0}^{m-1} f_i \left(\sigma^{(st+1)\cdot i} - \sigma^i\right).$$

If we then compute the p^kth power of $f(\alpha)$, we find that

$$f(\alpha)^{p^k} = \sum_{i=0}^{m-1} (f_i)^{p^k} \left(\sigma^{p^k \cdot (st+1)\cdot i} - \sigma^{p^k \cdot i}\right).$$

Since the two powers of σ in each term of the sum differ by a multiple of the order of σ, we see that the sum is zero; hence $g(x) \mid f(x)^{p^k}$. It remains to show that $f(x)^{p^k} \mid g(x)$.

First consider the case $k=0$. It follows from Corollary 2.1 that $g(x) = x^{q^l} - x$ for some divisor l of r. A quick computation shows that $1 \cdot \sigma \in R$ satisfies $x^{q^l} - x$ only when

$l = r$, so $g(x)$ has the specified form when $k = 0$.

Consider the case $k>0$. Notice that if H is a subgroup of G, then F[H] is a subalgebra of R. From this we may deduce that

$$I_F^{F[H]} \subseteq I_F^R. \tag{4.3}$$

From this we may deduce that $g(x)$ is in fact a multiple of $f(x)$, as σ^{p^k} generates a subgroup of G of order s; hence R has a subalgebra of the type treated in the case $k=0$, whose F-zeroing polynomials are generated by $f(x)$. From the theory of finite fields we know that each irreducible divisor of $f(x)$ has multiplicity 1, so from Corollary 2.1 we deduce that $g(x)$ is in fact a power of $f(x)$. Finally, a computation shows that $1\cdot\sigma$ fails to satisfy $f(x)^{p^k-1}$; hence $f(x)^{p^k} \mid g(x)$. □

Corollary 4.1. Let $G = C_{n_1} \times C_{n_2} \times C_{n_e}$ be a direct product decomposition of a finite abelian group into cyclic groups of order $n_1, n_2, \ldots, n_e$, let $n_i = s_i \cdot p^{k_i}$ where $p \nmid s_i$, let r_i be the order of q mod s_i, and set $R = F[G]$. Then

$$I_F^R = \mathrm{LCM}\left\{\left(x^{q^{r_i}} - x\right)^{p^{k_i}} : i = 1, 2, \ldots, e\right\}.$$

Proof:

Notice that R is the direct product of $C_{n_1}, C_{n_2}, \ldots, C_{n_e}$, apply Theorem 4.2 to each component of the direct product, and apply Lemma 1.4 (iii), recalling that in F[x] the generator of the intersection of ideals is the least common multiple of the generators of the ideals.

Corollary 4.2. Assume the hypotheses of Corollary 4.1 and let $k_1 = k_2 = \cdots = k_e = 0$. Then

(i) $PP_F(R) \cong \prod_{s \mid \text{some } r_i} C_s \text{ wr } S_{\pi(s)}$, and

(ii) $\left|PP_F(R)\right| = \prod_{s \mid \text{some } r_i} s^{\pi(s)} \cdot \pi(s)!$

Proof:

Use Corollary 4.1 to obtain I_F^R. Lemma 1.2 then says that Corollary 2.4 may be applied to obtain the formulas given.

Corollary 4.3. Assume the hypotheses of Corollary 4.1, let S be the set of all divisors of any r_i, let T be those members of S dividing an r_i for which $k_i>0$, and let

$$d_s = \max\left\{p^{k_i} : s \mid r_i\right\}.$$

Then

$$\left|PP_F(R)\right| = \prod_{s \,\varepsilon\, S} s^{\pi(s)} \cdot \pi(s)! \cdot \prod_{s \varepsilon T} \left(\left(q^s - 1\right) \cdot \left(q^{s \cdot (d_s - 2)}\right)\right)^{\pi(s)}.$$

Proof:

Use Corollary 4.1 to compute I_F^R, and use Lemma 1.2 to allow you to apply Theorem 2.3.

Example 4.1. Let $F = GF(2)$, $G = C_3$, the cyclic group of order 3, and set $R = F[G]$. Then Theorem 4.2 says that

$$I_F^R = \langle x^4 - x \rangle, \text{ and}$$

Corollary 4.2 says that

$$PP_F(R) \cong C_2 \times C_2,$$

the Klein-4 group. In fact,

$$PP_F(R) = \left\{x,\ x+1,\ x^2, \text{ and } x^2+1\right\}.$$

Example 4.2 . Let F = GF(3), G = C_6, and set R = F[G]. Then Theorem 4.2 says that

$$I_F^R = \langle x^9 - x^3 \rangle, \text{ and}$$

Corollary 4.3 says that

$$|PP_F(R)| = 1296 = 6^4.$$

§3 Questions for further study.

Multivariate Compositional Attractors.

A question I am asked virtually every time I mention compositional attractors is "What happens when you use more variables?" My answer typically has been that things get messy, so I haven't checked. The question, however, is a good one and in this section I will extend the definition of compositional attractors to multivariable polynomial rings.

A *multivariate compositional attractor* of the polynomial ring $S[x_1, x_2, \ldots, x_n]$ is an ideal I with the additional property that for $f \in I$ and for $g_1, g_2, \ldots, g_n$ we have that $f(g_1, g_2, \ldots, g_n) \in I$.

Compositional Attractors of the Integers.

Something on my wish list is a classification of the compositional attractors of $\mathbb{Z}[x]$. The techniques used to compute the compositional attractors for matrices over $\mathbb{Z}_n$ generalize to $\mathbf{Z}_n$ algebras that have the property that every possible monic polynomial, up to some fixed degree, is a least degree monic polynomial satisfied by some member of the algebra. Algebras that do not have this property exist. To see this, notice that Corollary 2.6 suggests a means of constructing them. Lacking some additional insight, I do not at present have the tools to classify such compositional attractors.

Public Key Cryptosystems.

The second topic I would like to study is the computational complexity of decomposing long period permutation polynomials into short period permutation

polynomials. If the computational complexity of this process is high then the material from the first three sections of Chapter 3 may be used to construct a public key cryptosystem. One would design the permutation polynomial separately mod each p, p^2, p^3, etc. dividing n to obtain a long period permutation without any short cycles in its cycle decomposition. Locally, that is modulo each p^k, one would invert the polynomial and then compose the inverses to obtain the secret decoding key.

In conjunction with this it would be nice to see if the number of nonzero coefficients of a permutation polynomial of $\mathbf{Z}_n$ can be controlled "locally." For permutation polynomials over finite fields locating permutation polynomials with few nonzero coefficients is difficult[7].

Compositional Attractors of Nonabelian Group Rings.

One of the nice things about the theory of compositional attractors presented herein is that it lets computations on nonabelian algebras take place in equivalent abelian settings. It would be nice, then, to be able to find which compositional attractors go with the various nonabelian group algebras.

Factorization Theorems.

One of the consequences of the material presented in Chapter 2 is a large number of global factorization properties of composed polynomials over finite fields. It would be nice to see if any additional juice could be squeezed out of this.

Appendix A

Explicit Examples of Polynomial Groups

The Group Sym(GF(5)) Realized as Polynomials.

Permutation	Polynomial	Permutation	Polynomial
()	x	(3 4)	x^3+2x^2+3x
(2 3)	x^3	(2 4)	$4x^3+4x^2+3x$
(1 2)	x^3+3x^2+3x	(1 3)	$4x^3+x^2+3x$
(1 4)	$4x^3$	(0 1)	x^3+x^2+2x+1
(0 2)	$4x^3+3x^2+2x+2$	(0 3)	$4x^3+2x^2+2x+3$
(0 4)	x^3+4x^2+2x+4	(1 2)(3 4)	$2x^3$
(1 3)(2 4)	$3x^3$	(1 4)(2 3)	$4x$
(0 1)(3 4)	$2x^3+3x^2+4x+1$	(0 1)(2 3)	$2x^3+x^2+x+1$
(0 1)(2 4)	$4x+1$	(0 2)(3 4)	$4x+2$
(0 2)(1 3)	$3x^3+4x^2+4x+2$	(0 2)(1 4)	$3x^3+3x^2+x+2$
(0 3)(2 4)	$3x^3+x^2+4x+3$	(0 3)(1 2)	$4x+3$
(0 3)(1 4)	$3x^3+2x^2+x+3$	(0 4)(2 3)	$2x^3+4x^2+x+4$
(0 4)(1 2)	$2x^3+2x^2+4x+4$	(0 4)(1 3)	$4x+4$
(2 3 4)	$3x^3+4x^2+4x$	(2 4 3)	$3x^3+2x^2+x$
(1 2 3)	$3x^3+3x^2+x$	(1 2 4)	$2x^3+4x^2+x$
(1 3 2)	$3x^3+x^2+4x$	(1 3 4)	$2x^3+2x^2+4x$
(1 4 2)	$2x^3+3x^2+4x$	(1 4 3)	$2x^3+x^2+x$
(0 1 2)	$3x^3+2x^2+x+1$	(0 1 3)	$2x^3+1$
(0 1 4)	$3x^3+x^2+4x+1$	(0 2 1)	$3x^3+2$
(0 2 3)	$2x^3+3x^2+4x+2$	(0 2 4)	$2x^3+x^2+x+2$
(0 3 1)	$2x^3+4x^2+x+3$	(0 3 2)	$2x^3+2x^2+4x+3$
(0 3 4)	$3x^3+3$	(0 4 1)	$3x^3+4x^2+4x+4$
(0 4 2)	$2x^3+4$	(0 4 3)	$3x^3+3x^2+x+4$

Permutation	Polynomial	Permutation	Polynomial
(0 1)(2 3 4)	$4x^3+1$	(0 1)(2 4 3)	$4x^3+3x^2+2x+1$
(0 1 2)(3 4)	$4x^3+4x^2+3x+1$	(0 1 3)(2 4)	x^3+4x^2+2x+1
(0 1 4)(2 3)	$4x^3+x^2+3x+1$	(0 2 1)(3 4)	$4x^3+2x^2+2x+2$
(0 2)(1 3 4)	x^3+2	(0 2 4)(1 3)	x^3+2x^2+3x+2
(0 2)(1 4 3)	x^3+4x^2+2x+2	(0 2 3)(1 4)	x^3+3x^2+3x+2
(0 3 1)(2 4)	x^3+3x^2+3x+3	(0 3 4)(1 2)	$4x^3+3x^2+2x+3$
(0 3)(1 2 4)	x^3+x^2+2x+3	(0 3 2)(1 4)	x^3+2x^2+3x+3
(0 3)(1 4 2)	x^3+3	(0 4 1)(2 3)	$4x^3+4x^2+3x+4$
(0 4 3)(1 2)	$4x^3+x^2+3x+4$	(0 4)(1 2 3)	$4x^3+2x^2+2x+4$
(0 4 2)(1 3)	x^3+x^2+2x+4	(0 4)(1 3 2)	$4x^3+4$
(1 2 3 4)	x^3+4x^2+2x	(1 2 4 3)	$2x$
(1 3 4 2)	$3x$	(1 3 2 4)	$4x^3+2x^2+2x$
(1 4 3 2)	x^3+x^2+2x	(1 4 2 3)	$4x^3+3x^2+2x$
(0 1 2 3)	x^3+2x^2+3x+1	(0 1 2 4)	x^3+1
(0 1 3 2)	$2x+1$	(0 1 3 4)	x^3+3x^2+3x+1
(0 1 4 2)	$4x^3+2x^2+2x+1$	(0 1 4 3)	$3x+1$
(0 2 3 1)	$3x+2$	(0 2 4 1)	$4x^3+x^2+3x+2$
(0 2 3 4)	x^3+x^2+2x+2	(0 2 4 3)	$4x^3+2$
(0 2 1 3)	$4x^3+4x^2+3x+2$	(0 2 1 4)	$2x+2$
(0 3 2 1)	x^3+4x^2+2x+3	(0 3 4 1)	$2x+3$
(0 3 4 2)	$4x^3+x^2+3x+3$	(0 3 2 4)	$3x+3$
(0 3 1 2)	$4x^3+3$	(0 3 1 4)	$4x^3+4x^2+3x+3$
(0 4 2 1)	x^3+2x^2+3x+4	(0 4 3 1)	x^3+4
(0 4 3 2)	x^3+3x^2+3x+4	(0 4 2 3)	$2x+4$
(0 4 1 2)	$3x+4$	(0 4 1 3)	$4x^3+3x^2+2x+4$

Permutation	Polynomial	Permutation	Polynomial
(0 1 2 3 4)	$x+1$	(0 1 2 4 3)	$3x^3+4x^2+4x+1$
(0 1 3 4 2)	$2x^3+4x^2+x+1$	(0 1 3 2 4)	$3x^3+3x^2+x+1$
(0 1 4 3 2)	$3x^3+1$	(0 1 4 2 3)	$2x^3+2x^2+4x+1$
(0 2 3 4 1)	$3x^3+x^2+4x+2$	(0 2 4 3 1)	$2x^3+2x^2+4x+2$
(0 2 1 3 4)	$3x^3+2x^2+x+2$	(0 2 4 1 3)	$x+2$
(0 2 1 4 3)	$2x^3+4x^2+x+2$	(0 2 3 1 4)	$2x^3+2$
(0 3 4 2 1)	$3x^3+3x^2+x+3$	(0 3 2 4 1)	$2x^3+3$
(0 3 4 1 2)	$2x^3+x^2+x+3$	(0 3 1 2 4)	$2x^3+3x^2+4x+3$
(0 3 1 4 2)	$x+3$	(0 3 2 1 4)	$3x^3+4x^2+4x+3$
(0 4 3 2 1)	$x+4$	(0 4 2 3 1)	$3x^3+2x^2+x+4$
(0 4 3 1 2)	$3x^3+x^2+4x+4$	(0 4 1 2 3)	$3x^3+4$
(0 4 1 3 2)	$2x^3+3x^2+4x+4$	(0 4 2 1 3)	$2x^3+x^2+x+4$

The Stabilizer of 0 in $PP(\mathbf{Z}_9)$.

Permutation	Polynomial	Permutation	Polynomial
identity	x	(1 7)	$x^5+x^4+2x^3+2x^2+x$
(2 8)	$x^5+2x^4+2x^3+4x^2+x$	(5 8)	$x^5+2x^4+2x^3+x^2+4x$
(1 4)	$x^5+x^4+2x^3+5x^2+4x$	(2 5)	$x^5+2x^4+2x^3+7x^2+7x$
(4 7)	$x^5+x^4+2x^3+8x^2+7x$	(3 6)	x^5+x^3+8x
(1 4)(5 8)	$2x^5+x^3+x$	(1 7)(2 5)	$2x^5+x^3+3x^2+x$
(2 8)(4 7)	$2x^5+x^3+6x^2+x$	(1 7)(3 6)	$2x^5+x^4+2x^2+2x$
(2 8)(3 6)	$2x^5+2x^4+4x^2+2x$	(1 7)(2 8)	$2x^5+x^3+4x$
(4 7)(5 8)	$2x^5+x^3+3x^2+4x$	(1 4)(2 5)	$2x^5+x^3+6x^2+4x$
(3 6)(5 8)	$2x^5+2x^4+x^2+5x$	(1 4)(3 6)	$2x^5+x^4+5x^2+5x$
(2 5)(4 7)	$2x^5+x^3+7x$	(1 4)(2 8)	$2x^5+x^3+3x^2+7x$
(1 7)(5 8)	$2x^5+x^3+6x^2+7x$	(2 5)(3 6)	$2x^5+2x^4+7x^2+8x$
(3 6)(4 7)	$2x^5+x^4+8x^2+8x$	(1 2)(4 5)(7 8)	x^3+x
(1 4)(3 6)(5 8)	$2x^3+2x$	(1 7)(2 5)(3 6)	$2x^3+3x^2+2x$
(2 8)(3 6)(4 7)	$2x^3+6x^2+2x$	(1 5)(2 7)(4 8)	x^3+4x
(1 8)(2 7)(4 5)	$2x^5+2x^3+4x$	(1 2)(4 8)(5 7)	$2x^5+2x^3+3x^2+4x$
(1 5)(2 4)(7 8)	$2x^5+2x^3+6x^2+4x$	(1 7)(2 8)(3 6)	$2x^3+5x$
(3 6)(4 7)(5 8)	$2x^3+3x^2+5x$	(1 4)(2 5)(3 6)	$2x^3+6x^2+5x$
(1 8)(2 4)(5 7)	x^3+7x	(2 5)(3 6)(4 7)	$2x^3+8x$
(1 4)(2 8)(3 6)	$2x^3+3x^2+8x$	(1 7)(3 6)(5 8)	$2x^3+6x^2+8x$
(1 5)(2 7)(3 6)(4 8)	x^5+2x^3+2x	(1 8)(2 4)(3 6)(5 7)	x^5+2x^3+5x
(1 8)(2 7)(3 6)(4 5)	$8x$	(1 2)(3 6)(4 5)(7 8)	x^5+2x^3+8x
(1 2)(3 6)(4 8)(5 7)	$3x^2+8x$	(1 5)(2 4)(3 6)(7 8)	$6x^2+8x$
(1 7 4)	$3x^2+4x$	(2 5 8)	$6x^2+4x$
(2 8 5)	$3x^2+7x$	(1 4 7)	$6x^2+7x$
(1 7 4)(2 5)	$x^5+2x^4+2x^3+x^2+x$	(2 5 8)(4 7)	$x^5+x^4+2x^3+5x^2+x$
(1 4 7)(5 8)	$x^5+2x^4+2x^3+7x^2+x$	(1 4)(2 8 5)	$x^5+x^4+2x^3+8x^2+x$
(1 7 4)(3 6)	$x^5+x^3+3x^2+2x$	(2 5 8)(3 6)	$x^5+x^3+6x^2+2x$
(2 8 5)(4 7)	$x^5+x^4+2x^3+2x^2+4x$	(1 4 7)(2 5)	$x^5+2x^4+2x^3+4x^2+4x$
(1 7 4)(2 8)	$x^5+2x^4+2x^3+7x^2+4x$	(1 7)(2 5 8)	$x^5+x^4+2x^3+8x^2+4x$
(2 8 5)(3 6)	$x^5+x^3+3x^2+5x$	(1 4 7)(3 6)	$x^5+x^3+6x^2+5x$
(1 4 7)(2 8)	$x^5+2x^4+2x^3+x^2+7x$	(1 4)(2 5 8)	$x^5+x^4+2x^3+2x^2+7x$
(1 7 4)(5 8)	$x^5+2x^4+2x^3+4x^2+7x$	(1 7)(2 8 5)	$x^5+x^4+2x^3+5x^2+7x$

Permutation	Polynomial	Permutation	Polynomial
(1 7 4)(2 5)(3 6)	$2x^5+2x^4+x^2+2x$	(2 5 8)(3 6)(4 7)	$2x^5+x^4+5x^2+2x$
(1 4 7)(3 6)(5 8)	$2x^5+2x^4+7x^2+2x$	(1 4)(2 8 5)(3 6)	$2x^5+x^4+8x^2+2x$
(2 8 5)(3 6)(4 7)	$2x^5+x^4+2x^2+5x$	(1 4 7)(2 5)(3 6)	$2x^5+2x^4+4x^2+5x$
(1 7 4)(2 8)(3 6)	$2x^5+2x^4+7x^2+5x$	(1 7)(2 5 8)(3 6)	$2x^5+x^4+8x^2+5x$
(1 4 7)(2 8)(3 6)	$2x^5+2x^4+x^2+8x$	(1 4)(2 5 8)(3 6)	$2x^5+x^4+2x^2+8x$
(1 7 4)(3 6)(5 8)	$2x^5+2x^4+4x^2+8x$	(1 7)(2 8 5)(3 6)	$2x^5+x^4+5x^2+8x$
(1 4 7)(2 5 8)	$3x^2+x$	(1 7 4)(2 8 5)	$6x^2+x$
(1 4 7)(2 8 5)	$4x$	(1 7 4)(2 5 8)	$7x$
(1 4 7)(2 8 5)(3 6)	x^5+x^3+2x	(1 7 4)(2 5 8)(3 6)	x^5+x^3+5x
(1 4 7)(2 5 8)(3 6)	$x^5+x^3+3x^2+8x$	(1 7 4)(2 8 5)(3 6)	$x^5+x^3+6x^2+8x$
(1 5 4 8)(2 7)	$x^5+2x^4+x^2+x$	(1 5 7 8)(2 4)	$x^5+x^4+2x^2+x$
(1 8 4 2)(5 7)	$x^5+2x^4+4x^2+x$	(1 8 4 5)(2 7)	$x^5+x^4+5x^2+x$
(1 2 4 5)(7 8)	$x^5+2x^4+7x^2+x$	(1 2)(4 8 7 5)	$x^5+x^4+8x^2+x$
(1 8 7 5)(2 4)	$x^5+2x^4+x^2+4x$	(1 8 7 2)(4 5)	$x^5+x^4+2x^2+4x$
(1 2 7 8)(4 5)	$x^5+2x^4+4x^2+4x$	(1 2 4 8)(5 7)	$x^5+x^4+5x^2+4x$
(1 5 7 2)(4 8)	$x^5+2x^4+7x^2+4x$	(1 5)(2 7 8 4)	$x^5+x^4+8x^2+4x$
(1 2)(4 5 7 8)	$x^5+2x^4+x^2+7x$	(1 2 7 5)(4 8)	$x^5+x^4+2x^2+7x$
(1 5)(2 4 8 7)	$x^5+2x^4+4x^2+7x$	(1 5 4 2)(7 8)	$x^5+x^4+5x^2+7x$
(1 8)(2 7 5 4)	$x^5+2x^4+7x^2+7x$	(1 8)(2 4 5 7)	$x^5+x^4+8x^2+7x$
(1 8 7 5)(2 4)(3 6)	$2x^5+2x^4+x^3+x^2+2x$	(1 8 7 2)(3 6)(4 5)	$2x^5+x^4+x^3+2x^2+2x$
(1 2 7 8)(3 6)(4 5)	$2x^5+2x^4+x^3+4x^2+2x$	(1 2 4 8)(3 6)(5 7)	$2x^5+x^4+x^3+5x^2+2x$
(1 5 7 2)(3 6)(4 8)	$2x^5+2x^4+x^3+7x^2+2x$	(1 5)(2 7 8 4)(3 6)	$2x^5+x^4+x^3+8x^2+2x$
(1 2)(3 6)(4 5 7 8)	$2x^5+2x^4+x^3+x^2+5x$	(1 2 7 5)(3 6)(4 8)	$2x^5+x^4+x^3+2x^2+5x$
(1 5)(2 4 8 7)(3 6)	$2x^5+2x^4+x^3+4x^2+5x$	(1 5 4 2)(3 6)(7 8)	$2x^5+x^4+x^3+5x^2+5x$
(1 8)(2 7 5 4)(3 6)	$2x^5+2x^4+x^3+7x^2+5x$	(1 8)(2 4 5 7)(3 6)	$2x^5+x^4+x^3+8x^2+5x$
(1 5 4 8)(2 7)(3 6)	$2x^5+2x^4+x^3+x^2+8x$	(1 5 7 8)(2 4)(3 6)	$2x^5+x^4+x^3+2x^2+8x$
(1 8 4 2)(3 6)(5 7)	$2x^5+2x^4+x^3+4x^2+8x$	(1 8 4 5)(2 7)(3 6)	$2x^5+x^4+x^3+5x^2+8x$
(1 2 4 5)(3 6)(7 8)	$2x^5+2x^4+x^3+7x^2+8x$	(1 2)(3 6)(4 8 7 5)	$2x^5+x^4+x^3+8x^2+8x$

Permutation	Polynomial	Permutation	Polynomial
(1 5 7 8 4 2)	$2x^5+2x^3+x$	(1 5 7 2 4 8)	x^3+3x^2+x
(1 8 7 2 4 5)	$2x^5+2x^3+3x^2+x$	(1 8 4 2 7 5)	x^3+6x^2+x
(1 2 7 5 4 8)	$2x^5+2x^3+6x^2+x$	(1 8 7 5 4 2)	x^3+3x^2+4x
(1 2 4 5 7 8)	x^3+6x^2+4x	(1 2 4 8 7 5)	$2x^5+2x^3+7x$
(1 2 7 8 4 5)	x^3+3x^2+7x	(1 5 4 2 7 8)	$2x^5+2x^3+3x^2+7x$
(1 5 4 8 7 2)	x^3+6x^2+7x	(1 8 4 5 7 2)	$2x^5+2x^3+6x^2+7x$
(1 2 4 8 7 5)(3 6)	$2x$	(1 5 4 2 7 8)(3 6)	$3x^2+2x$
(1 8 7 5 4 2)(3 6)	$x^5+2x^3+3x^2+2x$	(1 8 4 5 7 2)(3 6)	$6x^2+2x$
(1 2 4 5 7 8)(3 6)	$x^5+2x^3+6x^2+2x$	(1 5 7 8 4 2)(3 6)	$5x$
(1 8 7 2 4 5)(3 6)	$3x^2+5x$	(1 2 7 8 4 5)(3 6)	$x^5+2x^3+3x^2+5x$
(1 2 7 5 4 8)(3 6)	$6x^2+5x$	(1 5 4 8 7 2)(3 6)	$x^5+2x^3+6x^2+5x$
(1 5 7 2 4 8)(3 6)	$x^5+2x^3+3x^2+8x$	(1 8 4 2 7 5)(3 6)	$x^5+2x^3+6x^2+8x$

Appendix B

Tables of special functions.

The function $\pi(d)$ is used to denote the number of irreducibles of degree d in GF(q). There is a well known formula for $\pi(d)$,

$$\pi(d) = \frac{1}{d} \cdot \sum_{k \mid d} \mu(k) \cdot q^{d/k},$$

where $\mu(k)$ is the Möbius function. A table of values for small values is given below.

	d						
q	1	2	3	4	5	6	7
2	2	1	2	3	6	9	18
3	3	3	8	18	48	116	312
4	4	6	20	60	204	670	2340
5	5	10	40	150	624	2580	11160
7	7	21	112	588	3360	19544	117684
8	8	28	168	1008	6552	43596	299592
9	9	36	240	1620	11808	88440	683280
11	11	55	440	3630	32208	295020	2783880
13	13	78	728	7098	74256	804076	8964072
16	16	120	1360	16320	209712	2795480	38347920

Table 3.1 gives several values for $\kappa(n)$, the least degree of an n-ish monic polynomial in $\mathbb{Z}[x]$. Below, values are given for $\kappa_m(n)$, the least degree of an m-matrix n-ish polynomial.

$\kappa_m(n)$

n

m	2	3	4	5	6	7	8	9
1	2	3	4	5	3	7	4	6
2	6	12	12	30	12	56	18	24
3	14	39	28	155	39	399	42	78
4	30	120	60	780	120	2800	90	240

m	10	11	12	13	14	15	16	17
1	5	11	4	13	7	5	6	17
2	30	132	12	182	56	30	24	306
3	155	1463	39	2379	399	155	56	5219
4	780	16104	120	30940	2800	780	120	88740

m	18	19	20	21	22	23	24	25
1	6	19	5	7	11	23	4	10
2	24	380	30	56	132	552	18	60
3	78	7239	155	399	1463	12689	42	310
4	240	137560	780	2800	16104	292530	120	1560

m	26	27	28	29	30	31	32	33
1	13	9	7	29	5	31	8	11
2	182	36	56	870	30	992	24	132
3	2379	117	399	25259	155	30783	70	1463
4	30940	360	2800	732540	780	954304	150	16104

Appendix C

Certain Permutation Polynomial Groups

In this appendix I want to include some information about particular groups of permutation polynomials that I have uncovered. Since the members of $PP_{\mathbf{Z}_n}(\mathbf{Z}_n)$ are polynomials of $\mathbf{Z}_n$, they preserve equivalence classes mod each divisor of n. If $n = p^k$ is a prime power, this means that they live inside a group isomorphic to S_p wr S_p wr $\cdots$ wr S_p, the k-fold wreath product of the symmetric group on p letters. This pins down the structure of $G = PP_{\mathbf{Z}_8}(\mathbf{Z}_8)$. Theorem 3.4 says that the size of G is 128, exactly the size of $\mathbf{Z}_2$ wr $\mathbf{Z}_2$ wr $\mathbf{Z}_2$, which itself contains a copy of G.

Table 3.2 tells us that $PP_2(\mathbf{Z}_2)$ has size four. Pencil-and-paper examination of its action on the matrices reveals that it has the structure of a Klein 4 group. This fact was known to Brawley[8].

References

[1] G. Boole, A Treatise on the Calculus of Finite Differences, Macmillan and co., London, 1872.

[2] K. Miller, An Introduction to the Calculus of Finite Differences and Difference Equasions, Dover Books, New York, 1960.

[3] M. Aschbacher, Finite Group Theory, Cambridge University Press, Cambridge, 1986.

[4] D. Singmaster, On Polynomial Functions (mod m), *Journal of Number Theory* 6 (1974), 345-352.

[5] A. J. Kempner, Polynomials and their Residue Systems, *Transactions of the American Mathematical Society* 22 (1925), 240-266, 267-288.

[6] I. Niven and L. J. Warren, A Generalization of Fermat's Theorem, *Proceedings of the American Mathematical Society* 8(1957), 306-313.

[7] R. Lidl and H. Niederreiter, Finite Fields, Ency. of Mathematics 20, Cambridge University Press, Cambridge, 1984.

[8] J. V. Brawley, The Number of Polynomial Functions that Permute the Matrices Over a Finite Field, *Journal of Combinatorial Theory(A)* 21 (1976), 147-153.

[9] L. Carlitz and D. R. Hayes, Permutations with Coefficients in a Subfield, *Acta Arithmetica* XXI (1972), 131-135.

[10] J. V. Brawley, Polynomials Over a Ring That Permute the Matrices Over That Ring, *Journal of Algebra*, 38 (1976), 93-99.

[11] J. V. Brawley, L. Carlitz, and Jack Levine, Scalar Polynomial Functions on the nxn Matrices over a Finite Field, *Linear Algebra and its Applications* 10, (1975) 199-217.

[12] Hans Lausch, Winfried B. Müller, und Wilfried Nöbauer, Über die Struktur einer durch Dicksonpolynome dargestellten Permutationsgruppe des Restklassenringes modulo n, *J. Reine Agnew Math.* 261 : (1973) 88-99.

[13] Wilfried Nöbauer, Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen, *Monatsh. f. Math. (Vienna)* 69 : (1965) 230-238.