A METHOD FOR CONSTRUCTING GROUPS OF PERMUTATION POLYNOMIALS AND ITS APPLICATION TO PROJECTIVE GEOMETRY

by

Chris Castillo

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Summer 2015

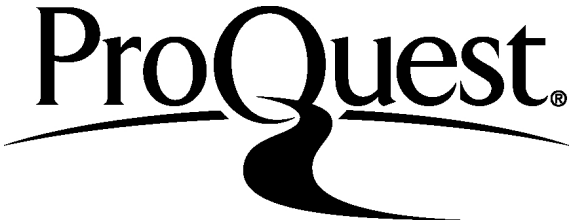
© 2015 Chris Castillo
All Rights Reserved

ProQuest Number: 3730194

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.



ProQuest 3730194

Published by ProQuest LLC (2015). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

A METHOD FOR CONSTRUCTING GROUPS OF PERMUTATION POLYNOMIALS AND ITS APPLICATION TO PROJECTIVE GEOMETRY

by

Chris Castillo

Approved: _____

Louis F. Rossi, Ph.D.
Chair of the Department of Mathematical Sciences

Approved: _____

George Watson, Ph.D.
Dean of the College of Arts and Sciences

Approved: _____

James G. Richards, Ph.D.
Vice Provost for Graduate and Professional Education

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Robert S. Coulter, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Pamela Kosick, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Felix Lazebnik, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: _____

Qing Xiang, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

I have had the kind and generous support of many individuals throughout my time as a graduate student, and it is my pleasure to acknowledge them for the contributions they have made to my personal and professional development.

First, my advisor, Dr. Robert Coulter, who I thank for his encouragement, advice, and patience. I was very lucky to find a topic that was enjoyable to work on with a mentor who was a pleasure to work with.

The members of my committee, Dr. Felix Lazebnik, Dr. Qing Xiang, and Dr. Pam Kosick, for their careful reading of this dissertation and the helpful feedback they provided.

My parents, Lenore and Don Murphy, and my grandparents, Bill and Ada DeAngelis, for their love and encouragement.

My friends (in alphabetical order), Alexander Ames, Dr. Emily Bonistall Postel, Joseph Brodie, Dr. Chuck Hague, Isaac Harris, Megan Hutchins, Mary Korch, Dr. Brian Kronenthal, Dr. Bryan Petrak, Dr. Steven Senger, and Dr. Wiseley Wong, for helping my six years in Newark pass a bit more pleasantly.

Finally, Dr. Mary Martin and Dr. Jim Richards, who were both very generous with their time and advice during my tenure as Graduate Student Government President. I would not have been successful without their confidence and support. Graduate students at the University of Delaware are truly fortunate to have them as advocates for graduate education and staunch supporters of "graduate student life".

DEDICATION

To Robert Clary,
who first showed me the beauty of polynomials
and who challenged me to be a better mathematician,
with my deep appreciation and respect.

TABLE OF CONTENTS

ABSTRACT . . . . . **viii**

Chapter

1 INTRODUCTION **1**

1.1 Overview 1
1.2 Background on Finite Fields and Polynomials 3
1.3 Background on Group Actions and Representations 5
1.4 Background on Projective Planes and Planar Ternary Rings 6
1.5 Background on Loops 8
1.6 Historical Context 9
1.7 Useful Lemmas 11

2 INTERPOLATION IN FINITE FIELDS **14**

2.1 Interpolation Methods 14
2.2 Indicator Functions 16
2.3 Application of Indicator Functions to Produce Representation Polynomials 19

3 THE THEORY OF CONSTRUCTING GROUPS OF PERMUTATION POLYNOMIALS **25**

3.1 Constructing Polynomial Representations of Groups 25
3.2 The Preserved Subgroup and Its Properties 28
3.3 Preserving Group Structure in Field Structure 33
3.4 Equivalence of Representations 34

4 EXAMPLES OF ADDITIVE REPRESENTATIONS **41**

4.1 Preliminaries on the Representation of Direct Products of Cyclic p-groups 41

4.2 Representation of the Cyclic p-Groups 45
4.3 Representation of the Cyclic Group of Order p^2 51

5 EXAMPLES OF MULTIPLICATIVE REPRESENTATIONS . . 57

5.1 Representation of Certain Dihedral Groups 57
5.2 Representation of Certain Hamiltonian Groups 61
5.3 Representation of the Cyclic Group of Order p 66
5.4 Representation of the Cyclic Group of Order q 68

6 THE THEORY OF BIVARIATE POLYNOMIAL REPRESENTATIONS 73

6.1 Construction of Bivariate Representations 73
6.2 Equivalence of Bivariate Representations 74
6.3 Application to the Coordinatization of Finite Projective Planes . . . 76

7 FUTURE WORK & OPEN PROBLEMS 81

BIBLIOGRAPHY 83

Appendix

A SUMMARY OF NOTATION 85

A.1 Algebraic Structures 85
A.2 Representation Polynomials and Polynomial Operations 86
A.3 Groups and Their Presentations 86

B INDEX 87

ABSTRACT

This dissertation presents original work on permutation polynomials over finite fields. From a consideration of the proof of Cayley's theorem, it is clear that any finite group can be represented as a group of permutation polynomials (via interpolation) using the left regular action of the group on itself. The goal is to produce new families of permutation polynomials with particularly simple coefficients or relatively few terms. Central to the construction method is the choice of injective function from the group into a finite field, and a number of results are stated describing the relationship between the chosen injection and the resulting form of the representation polynomials. The construction method is then generalized to produce a single bivariate polynomial representing a given group, and several analogs of the univariate structure theorems are proved for the bivariate case. As applications of the method, we produce families of permutation polynomials representing various groups, several of which are new, and we use the bivariate representation to obtain new results on the construction of planar ternary rings coordinatizing finite Lenz-Barlotti type II.2 planes.

Chapter 1

INTRODUCTION

1.1 Overview

This dissertation is motivated by two problems concerning permutation polynomials over finite fields. The first is very general: constructing new families of permutation polynomials (problem P2 of Lidl and Mullen [13]). The second is more specific: represent given groups of order at most q by permutation polynomials over the finite field $\mathbb{F}_q$. We develop a method to address the second question, which produces answers to the first question as a pleasant byproduct. In particular, we focus on the question of whether some groups can be represented by permutation polynomials that are aesthetically pleasing in some way. For example, the elementary abelian group of order q can be represented by the set of (permutation) polynomials $\{X + a : a \in \mathbb{F}_q\}$, while the cyclic group of order $q - 1$ can be represented by $\{aX : a \in \mathbb{F}_q \setminus \{0\}\}$. These linear polynomials are as simple as can possibly be achieved; in general, the form of the permutation polynomials representing a given group will be significantly more complicated.

After preliminary work on interpolation over finite fields in Chapter 2, which yields our first examples of polynomials which represent specific groups in Section 2.3, we describe a method for constructing a set of polynomials that is (group-)isomorphic to a given finite group G in Chapter 3. This method is based on the proof of Cayley's Theorem, which allows us to represent a group G as the group of (left) regular actions of G on itself; an assignation σ between elements of G and the elements of $\mathbb{F}_q$ then provides the translation, via interpolation, to permutation polynomials, as desired. Generally speaking, one can make this assignment arbitrarily, and using interpolation produce

many groups of permutation polynomials representing G. However, almost certainly a random assignation will result in unpredictable forms for the representation polynomials, lacking any sort of aesthetic. Our approach to producing permutation polynomials with a better aesthetic, that is, with relatively few terms or easily-described coefficients, is to preserve as much of the structure of G as possible in the assignation; we introduce the notions of "preserved subgroup" and "hemimorphism" to make more precise this concept of preservation of structure. In particular, we prove in Theorem 3.2.4 that the restriction of σ to the preserved subgroup is a group homomorphism. One interesting property of our method is that in the case when $|G| = q$, all permutation polynomials not representing the identity are fixed point free; we know of no other method for constructing permutation polynomials where this is guaranteed. Chapter 3 also addresses, via the notion of quasiequivalence of representations, when two groups of permutation polynomials produced by this method are essentially the same.

As applications of the general theory, we represent several families of groups by polynomials. Representations of groups which preserve some of the group structure in the additive group of $\mathbb{F}_q$ are considered in Chapter 4, and representations of groups which preserve some of the group structure in the multiplicative group $\mathbb{F}_q^\times$ are considered in Chapter 5. New classes of permutation polynomials produced by our approach are given in Theorems 2.3.1, 2.3.2, 2.3.3, 4.2.2, 4.3.1, 5.3.1, 5.4.1, and 5.4.2, and Corollary 4.3.3. Theorems 5.1.1 and 5.2.1 exhibit families of permutation polynomials which, while already known, are shown to possess a nice group structure. In most cases, the forms obtained look somewhat complicated. However, they still have either relatively few non-zero terms or a very simple description of the coefficients of each term; for example, we obtain permutation binomials for the Hamiltonian groups we consider. We also determine a new set of polynomial generators for $GL(\mathbb{F}_{p^2})$ in Theorem 4.3.5.

In Chapter 6, we extend the theory of (univariate) polynomial representations developed in Chapter 3 to construct a single bivariate polynomial representing the regular action of G on itself. The bivariate representation is a generalization of the previous

univariate construction, although Theorem 6.2.1 shows an unexpected relationship between univariate quasiequivalence and bivariate equivalence. This construction finds application in projective geometry, where we show in Section 6.3 that finite, prime-power order projective planes of Lenz-Barlotti type II.2 may be coordinatized by such bivariate polynomials.

This dissertation concludes with several open problems and directions for future work, building on the theory of polynomial representations, in Chapter 7.

Parts of this work have already been published or accepted for publication in the following papers:

1. C. Castillo, R.S. Coulter, and S. Smith, *A note on interpolation of permutations of a subset of a finite field*, Bull. Aus. Math. Soc. **90** (2014), 213–219.
2. C. Castillo and R.S. Coulter, *A general theory for constructing groups of permutation polynomials*, Finite Fields Appl. **35** (2015), 172–203.

The former paper covers roughly the material of Section 2.3 from Theorem 2.3.3 onward, while the latter paper covers all of Chapter 3 except for Theorem 3.2.5, Section 4.2 through Corollary 4.2.3 and Section 4.3 from Chapter 4, and all of Chapter 5.

1.2 Background on Finite Fields and Polynomials

Throughout, we will let $q = p^n$ for some prime p and let $\mathbb{F}_q$ denote the finite field of order q. We will write $\mathbb{F}_q^+$ for the additive group of $\mathbb{F}_q$ and $\mathbb{F}_q^\times$ for the multiplicative group of $\mathbb{F}_q$. The additive group $\mathbb{F}_q^+$ is an elementary abelian p-group, and hence is isomorphic to the vector space of dimension n over $\mathbb{F}_p$; accordingly, we will denote a (fixed but arbitrary) basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ by $[\beta_i] = [\beta_0, \beta_1, \ldots, \beta_{n-1}]$. The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$, and will be denoted $\mathbb{F}_q^\times = \langle \zeta \rangle$ for some (fixed but arbitrary) primitive element ζ of $\mathbb{F}_q$.

We will be concerned with elements of $\mathbb{F}_q[X]$, the ring of polynomials over $\mathbb{F}_q$ in the indeterminate X. A nonzero polynomial $f(X) = \sum_{i \geq 0} a_i X^i \in \mathbb{F}_q[X]$ has *degree* d, where d is the largest index i such that $a_i \neq 0$, and $f(X)$ is said to be *reduced* if its degree is less than q. Two reduced polynomials $f(X), g(X) \in \mathbb{F}_q[X]$ are equal if and

only if $f(x) = g(x)$ for all $x \in \mathbb{F}_q$; more generally, for two (not necessarily reduced) polynomials $f(X), g(X) \in \mathbb{F}_q[X]$, we have $f(X) \equiv g(X) \pmod{X^q - X}$ if and only if $f(x) = g(x)$ for all $x \in \mathbb{F}_q$ (see Lemma 7.2 of Lidl and Niederreiter [14]). If, under evaluation, a polynomial $f(X) \in \mathbb{F}_q[X]$ induces a bijection on $\mathbb{F}_q$, then we call $f(X)$ a *permutation polynomial* over $\mathbb{F}_q$. A permutation polynomial $f(X)$ such that $f(X)+X$ is also a permutation polynomial is called a *complete mapping*. It is well known that permutation polynomials over $\mathbb{F}_q$ have degree at most $q-2$, and a result of Niederreiter and Robinson [19] shows that complete mappings have degree at most $q-3$.

Note that since we can consider $\mathbb{F}_q^+$ as a vector space over $\mathbb{F}_p$, we have $\mathrm{Aut}(\mathbb{F}_q^+) \cong GL(\mathbb{F}_q)$, so every automorphism of $\mathbb{F}_q^+$ can be represented by an $\mathbb{F}_p$-linear map. Polynomials of the form

$$L(X) = \sum_{i=0}^{n-1} \ell_i X^{p^i}$$

where $\ell_i \in \mathbb{F}_q$ are called *linearized*, following the terminology introduced in Chapter 11 of Berlekamp [2]. It is an easy exercise to show that they indeed behave linearly over $\mathbb{F}_p$, that is

$$L(aX + b) = aL(X) + L(b)$$

for any $a \in \mathbb{F}_p$ and any $b \in \mathbb{F}_q$. Vaughan [24] showed that the algebra of linear transformations of $\mathbb{F}_q$ (considered as a vector space over $\mathbb{F}_p$) is isomorphic to the algebra of all linearized polynomials in $\mathbb{F}_q[X]$. For our purposes, we only require the fact, established by Dickson [8], that the elements from the set of *invertible* linear transformations of $\mathbb{F}_q$ (i.e. from the general linear group $GL(\mathbb{F}_q)$) are in bijective correspondence with elements from the set of reduced linearized permutation polynomials satisfying one of the following equivalent conditions:

1. $$\begin{vmatrix} \ell_0 & \ell_{n-1}^{p} & \ell_{n-2}^{p^2} & \cdots & \ell_1^{p^{n-1}} \\ \ell_1 & \ell_0^{p} & \ell_{n-1}^{p^2} & \cdots & \ell_2^{p^{n-1}} \\ \ell_2 & \ell_1^{p} & \ell_0^{p^2} & \cdots & \ell_3^{p^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \ell_{n-1} & \ell_{n-2}^{p} & \ell_{n-3}^{p^2} & \cdots & \ell_0^{p^{n-1}} \end{vmatrix} \neq 0;$$
2. The unique root of $L(X)$ in $\mathbb{F}_q$ is 0.

(Bottema [3] and Carlitz [6] showed *a fortiori* that $GL(\mathbb{F}_q)$ is isomorphic to the group of invertible linearized polynomials over $\mathbb{F}_q$; see page 382 of [14] for further historical information.) Therefore each element of the general linear group $GL(\mathbb{F}_q)$ can be represented by a unique (reduced) linearized (permutation) polynomial $L(X) \in \mathbb{F}_q[X]$.

The standard reference for finite fields is Lidl and Niederreiter [14]. Chapters 1 and 2 of [14] contain more information on finite fields in general, while Chapter 7 addresses permutation polynomials in particular.

1.3 Background on Group Actions and Representations

A *group action* of a group G on a set S is a binary operation $*\colon G \times S \to S$ satisfying the following properties for all $s \in S$:

1. $g_1 * (g_2 * s) = (g_1 g_2) * s$ for all $g_1, g_2 \in G$, and
2. $e * s = s$, where e is the identity element of G.

The action of a particular group element $g \in G$ defines a set map $\theta_g\colon S \to S$ via $\theta_g(s) = g * s$. Each function θ_g is a bijection, since

$$\theta_{g^{-1}}(\theta_g(s)) = g^{-1} * (g * s) = (g^{-1}g) * s = e * s = s$$

shows that $\theta_{g^{-1}}$ is the inverse map to θ_g. Letting $\mathrm{Sym}(S)$ denote the group of bijective functions on S, we have shown that the action of G on S determines a function $\Theta\colon G \to \mathrm{Sym}(S)$ via $\Theta(g) = \theta_g$. In fact, Θ is a group homomorphism, since

$$\Theta(g_1 g_1)(s) = \theta_{g_1 g_2}(s) = (g_1 g_2) * s = g_1 * (g_2 * s) = \theta_{g_1}(\theta_{g_2}(s)) = (\Theta(g_1) \circ \Theta(g_2))\,(s)$$

for any $s \in S$ and any $g_1, g_2 \in G$. Such a homomorphism $G \to \mathrm{Sym}(S)$ is called a *representation*, and hence it is clear that a group action gives rise to a representation of G as a group of functions defined on the set S. One particular representation that we will make use of later is the (left) *regular representation*, which arises from the action of left-multiplication of a group G on itself.

We will be interested in knowing when various representations of a given group are essentially the same; that is, when they act in the same way on the underlying

set. We use two similar, but distinct, notions to make this precise. The first notion enables us to compare the actions of two different groups. Let S and S' be finite sets and suppose $\Theta\colon G \to \mathrm{Sym}(S)$ and $\Theta'\colon G' \to \mathrm{Sym}(S')$ are representations. We say that the groups G and G' are *permutation isomorphic* if there exists a bijection $\alpha\colon S \to S'$ and a group isomorphism $\psi\colon G \to G'$ such that

$$\alpha\left(g * s\right) = \psi(g) * \alpha(s)$$

for all $x \in S$ and $g \in G$, where the action on the left is of G on S (corresponding to Θ) and the action on the right is of G' on S' (corresponding to Θ').

The second notion enables us to compare two actions of the same group. Now suppose S is a finite group, and let $\Theta, \Theta'\colon G \to \mathrm{Sym}(S)$ be two representations of G (here we are still considering $\mathrm{Sym}(S)$ as a set of bijections on the underlying set of S). We say that the two representations Θ and Θ' are *quasiequivalent* if there exist group automorphisms $\psi\colon G \to G$ and $\alpha\colon S \to S$ such that

$$\alpha\left(g * s\right) = \psi(g) * \alpha(s)$$

for all $x \in S$ and $g \in G$, where the action on the left corresponds to Θ and the action on the right corresponds to Θ'. If ψ is the identity automorphism of G, then Θ and Θ' are said to be *equivalent*. We remark that our definition follows page 9 of Aschbacher [1], which requires that α be an isomorphism in the category containing the structure on which the group G acts. Thus we require that α be a *group isomorphism* of S; a more general definition used elsewhere in the literature (cf. page 17 of Dixon and Mortimer [9]) requires only that α be a *bijection* of S.

See Chapter 1 of [9] or Sections 4 and 5 of [1] for more information on group actions and (permutation) representations.

1.4 Background on Projective Planes and Planar Ternary Rings

A *projective plane* $\mathscr{P}$ is a combinatorial incidence structure consisting of a set of points, a set of lines, and an incidence relation I between points and lines, which satisfies the following axioms:

1. Any two points are incident with a unique line.
2. Any two lines are incident with a unique point.
3. There exist four points, no three of which are collinear.

A finite projective plane has a well-defined *order* q, such that $\mathscr{P}$ has q^2+q+1 points and q^2+q+1 lines.

The notion of automorphism of a projective plane $\mathscr{P}$ that we will be interested in is *collineation*, an incidence-preserving bijective mapping of points of $\mathscr{P}$ to points of $\mathscr{P}$ and lines of $\mathscr{P}$ to lines of $\mathscr{P}$. In this dissertation, we will only consider those collineations which fix a line ℓ and all the points on it, or equivalently (by Theorem 4.9 of Hughes and Piper [11]), fix a point P and all the lines through it. Such a collineation is called a *central collineation* with *axis* ℓ and *centre* P. A central collineation whose axis and centre are incident is called an *elation*, and one whose axis and centre are non-incident is called a *homology*. A projective plane is (P,ℓ)-*transitive* if it satisfies the following property: for any distinct points A and B, collinear with P but incident with neither P nor ℓ, there exists a central collineation with axis ℓ and centre P that maps A to B.

In Section 6.3, we will have need to reference the Lenz-Barlotti classification, which enumerates all possible sets of (P,ℓ)-transitivities that a projective plane may possess. Type II.1 planes possess a (P,ℓ)-transitivity, where $P \mathrel{\mathrm{I}} \ell$, and no other transitivities; type II.2 planes possess two transitivities, (P,ℓ) and (P',ℓ') with $P \neq P'$ and $\ell \neq \ell'$, satisfying the conditions $P \mathrel{\mathrm{I}} \ell$, $P \mathrel{\mathrm{I}} \ell'$, $P' \mathrel{\mathrm{I}} \ell$, and $P' \not\mathrel{\mathrm{I}} \ell'$. For our purposes, it will suffice to consider type II.1 planes as possessing an $((\infty),[\infty])$-transitivity and type II.2 planes as possessing both an $((\infty),[\infty])$-transitivity and a $((0),[0])$-transitivity. See Theorem 3.1.20 of Dembowski [7] for a complete description of the Lenz-Barlotti classification.

A *planar ternary ring* (PTR) is a set R, containing 0 and 1, equipped with a ternary operation T satisfying the following axioms:

(A) $T(a,0,c) = T(0,b,c) = c$ for all $a,b,c \in R$.

(B) $T(a,1,0) = T(1,a,0) = a$ for all $a \in R$.

(C) For all $a,b,c,d \in R$ with $a \neq c$, there exists a unique $x \in R$ such that $T(x,a,b) = T(x,c,d)$.

(D) For all $a,b,c \in R$, there exists a unique $x \in R$ such that $T(a,b,x) = c$.

(E) For all $a,b,c,d \in R$ with $a \neq c$, there exist unique $x,y \in R$ such that $T(a,x,y) = b$ and $T(c,x,y) = d$.

Letting (x,y) denote (affine) points of $\mathscr{P}$ and $[m,k]$ denote lines, a planar ternary ring can be used to construct (a particular coordinatization of) a projective plane $\mathscr{P}$ by defining $(x,y)\,\mathrm{I}\,[m,k]$ if and only if $T(m,x,y) = k$ (Theorem 5.2 of [11]), and conversely any coordinatization of $\mathscr{P}$ gives rise to a planar ternary ring (Theorem 5.1 of [11]). It is known that a finite ternary ring satisfies conditions (C) and (D) if and only if it satisfies conditions (D) and (E) (Theorem 5.4 of [11]). We can define "addition" and "multiplication" in the PTR by $x \oplus y := T(1,x,y)$ and $x \otimes y := T(x,y,0)$, respectively. A planar ternary ring is *linear* if $T(x,y,z) = (x \otimes y) \oplus z$; that is, the PTR is linear when knowing addition and multiplication (separately) is equivalent to knowing the ternary operation.

Both Hughes and Piper [11] and Dembowski [7] are standard references for projective geometry. See Chapters 5 and 6 of [11] or Chapters 3 and 4 of [7] for more information about planar ternary rings and the coordinatization of projective planes.

1.5 Background on Loops

A *loop* is defined as a set closed under a binary operation, with an identity element, and where each element possesses left- and right-inverses (which need not necessarily coincide); it is often convenient to think of a loop as a group that is not necessarily associative. A Latin square is equivalent to the multiplication table of a loop (see Section 1.1 of Smith [22]).

In any planar ternary ring R, both the additive and multiplicative structures form loops (Theorem 5.3 of [11]). The plane $\mathscr{P}$ being $((\infty),[\infty])$-transitive or $((0),[0])$-transitive corresponds to the additive loop (Theorem 6.2 of [11]) or multiplicative loop

(Theorem 6.5 of [11]), respectively, actually being a group. Thus, coordinatized in an appropriate way, in type II.1 planes the additive loop is a group, and in type II.2 planes both the additive and multiplicative loops are groups.

In addition to the usual notion of homomorphism, there is also the notion of homotopy, which turns out to be more useful for comparing the structure of two loops. For two loops L_1 and L_2, a *homotopy* is an ordered triple (f_1, f_2, f_3) of maps $f_1, f_2, f_3 \colon L_1 \to L_2$ such that

$$f_1(x) \,\square\, f_2(y) = f_3(xy)$$

for all $x, y \in L_1$, where $\square$ is the operation in L_2 and adjunction is the operation in L_1. A loop *homomorphism* is therefore a homotopy with $f_1 = f_2 = f_3$. A homotopy where f_1, f_2, and f_3 are bijections is called an *isotopy*; moreover, when $L_1 = L_2$, an isotopy (f_1, f_2, id) is called a *principal isotopy*. An *isomorphism* of loops is a homotopy that is both an isotopy and a homomorphism.

An isotopy (f_1, f_2, f_3) describes a permutation of the rows (by f_1) and columns (by f_2) and a relabeling of the entries (by f_3) of the multiplication table of a loop, and is therefore the correct structure-preserving map for comparing the additive or multiplicative loops of two planar ternary rings. There are two important facts about loops that we will make use of. First, it is clear that any isotopy (f_1, f_2, f_3) factors as a product of a principal isotopy and an isomorphism:

$$(f_1, f_2, f_3) = (f_1 f_3^{-1}, f_2 f_3^{-1}, \mathrm{id})(f_3, f_3, f_3).$$

Second, an isotopy between a loop and a group is in fact an isomorphism, and in particular, two groups that are isotopic are isomorphic (Proposition 1.4 of [22]). See Chapter 1 of Smith [22] for additional details about the structure of loops.

1.6 Historical Context

Permutation polynomials are a central object of study in finite field theory, and determining whether a given polynomial is a permutation polynomial is a non-trivial

task. Hermite [10] proved the initial results over prime fields, introducing the criterion that now bears his name, and Dickson [8] expanded these to arbitrary finite fields. While it is a simple exercise to show that the monomial X^k is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$, much less simple is the result by Matthews [17] that the "all-ones" polynomial $h_k(X) = 1 + X + X^2 + \cdots + X^k$ is a permutation polynomial over odd-order $\mathbb{F}_q$ if and only if $k \equiv 1 \pmod{p(q-1)}$. Chapter 7 of [14] is a thorough introduction to the basic theory of permutation polynomials.

There are several results describing families of permutation polynomials which possess a group structure under the operation of composition and reduction modulo $X^q - X$. For example, the linearized polynomials over $\mathbb{F}_q$ (from Section 1.2) form a group, called the Betti-Mathieu group, which we saw is isomorphic to $GL(\mathbb{F}_q)$. In another early result, Carlitz [5] showed the full symmetric group S_q on q letters can be generated by X^{q-2} and all linear polynomials in $\mathbb{F}_q[X]$, while Wells [27] later determined polynomial generators for several small-index subgroups of S_q. More recently, Stafford [23] showed that the set of linear polynomials $\tau_{a,b}(X) = aX + b$ with $a, b \in \mathbb{F}_q$ and $a \neq 0$ forms the affine general linear group, and determined the structure of the group generated by the set of $\tau_{a,b}$ polynomials and the k-th-power map.

Nöbauer [20] showed that for fixed $a \in \{-1, 0, 1\}$, Dickson polynomials of the first kind,

$$g_k(X, a) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j X^{k-2j},$$

form (abelian) groups (see also Theorems 7.22 and 7.23 of [14]). Wan and Lidl [25], in the course of proving when polynomials of the form $X^r f(X^{(q-1)/d})$ were permutation polynomials, also determined that they have the group structure of a generalized wreath product, extending the work of Wells [26]. Additionally, Mullen and Niederreiter [18] showed that the permutation polynomials of the form $aX^{\frac{q+1}{2}} + bX$ for $a, b \in \mathbb{F}_q$ form a group isomorphic to the wreath product $C_{\frac{q-1}{2}} \wr C_2$. Finally, we note that Wells [28] determined polynomials representing transpositions and 3-cycles, although the forms

of his polynomials are different from those in Theorems 2.3.3 and 2.3.5, and his proofs are not constructive.

1.7 Useful Lemmas

Before developing the theory, we state several formulae which we will use in subsequent sections to simplify computations. We begin with Lucas' Theorem, which will only be used in the proof of Lemma 1.7.2. See Lucas [16] for the original result, and page 28 of Cameron [4] or page 55 of van Lint [15] for a modern proof.

Lemma 1.7.1 (Lucas' Theorem)**.** *Given $m, d \in \mathbb{N}$ with $m \geq d$, let $m = \sum_{i=0}^{k} \mu_i p^i$ and $d = \sum_{i=0}^{k} \delta_i p^i$ be the p-adic expansions of m and d, respectively. Then*

$$\binom{m}{d} \equiv \prod_{i=0}^{k} \binom{\mu_i}{\delta_i} \pmod{p}.$$

Lemma 1.7.2. *For $0 \leq d \leq q-1$, we have*

$$\binom{q-1}{d} \equiv (-1)^d \pmod{p}.$$

Proof. The statement certainly holds when $d = 0$ since $\binom{q-1}{d} = 1 = (-1)^0$, so for the remainder of the proof we will assume that $1 \leq d \leq q-1$. A standard identity for binomial coefficients gives

$$\binom{q-1}{d} + \binom{q-1}{d-1} = \binom{q}{d},$$

and applying Lucas' Theorem we observe that $\binom{q}{d} \equiv 0 \pmod{p}$ for all $0 < d < q$. For $d = 1$, we have

$$\binom{q-1}{1} + 1 \equiv 0 \pmod{p},$$

and hence $\binom{q-1}{1} \equiv (-1)^1 \pmod{p}$. The lemma now follows inductively for all $d \leq q-1$. □

Next, we state Kummer's Theorem, which we will use to prove Lemma 1.7.4. See Kummer [12] for the original result.

Lemma 1.7.3 (Kummer's Theorem)**.** *Let $m, d \in \mathbb{N}$ with $m \geq d$. Then largest power of p dividing the binomial coefficient $\binom{m}{d}$ is the number of carries in the p-adic sum of d and $m - d$.*

Lemma 1.7.4. *Let $d, N \in \mathbb{N}$ and choose nonnegative integers $d_0, d_1, \ldots, d_{N-1}$ such that $d = d_0 + d_1 + \cdots + d_{N-1}$. Then the multinomial coefficient*

$$\binom{d}{d_0, d_1, \ldots, d_{N-1}} \not\equiv 0 \pmod{p}$$

if and only if there are no carries in the p-adic sum $d_0 + d_1 + \cdots + d_{N-1}$.

Proof. Note that since $d > 0$ by assumption, $\binom{d}{d_0, d_1, \ldots, d_{N-1}} \neq 0$. Using a standard identity for multinomial coefficients, we may write

$$\binom{d}{d_0, d_1, \ldots, d_{N-1}} = \binom{d_0}{d_0}\binom{d_0 + d_1}{d_1} \cdots \binom{d_0 + d_1 + \cdots + d_{N-1}}{d_{N-1}}.$$

By Kummer's Theorem, the largest power of p dividing $\binom{d_0 + d_1 + \cdots + d_\ell}{d_\ell}$, for $0 \leq \ell \leq N-1$, is the number of carries when adding d_ℓ to $d_0 + d_1 + \cdots + d_{\ell-1}$ p-adically, and hence the largest power of p dividing $\binom{d}{d_0, d_1, \ldots, d_{N-1}}$ is precisely the number of carries when adding d_0, d_1, $\ldots$, d_{N-1} p-adically. In particular, no positive power of p divides $\binom{d}{d_0, d_1, \ldots, d_{N-1}}$ if and only if there are no carries in the p-adic sum $d_0 + d_1 + \cdots + d_{N-1}$. □

The following lemma is standard; see Lemma 6.3 of [14] for a proof.

Lemma 1.7.5. *Let $x \in \mathbb{F}_q$. Then*

$$\sum_{x \in \mathbb{F}_q} x^d = \begin{cases} 0, & \text{if } d = 0 \text{ or } (q-1) \nmid d, \\ -1, & \text{if } d \neq 0 \text{ and } (q-1) \mid d. \end{cases}$$

Finally, we state and prove two lemmas that will be of use in later computations.

Lemma 1.7.6. *Let $x \in \mathbb{F}_q^\times$, and recall that $h_k(X) = 1 + X + X^2 + \cdots X^k$. Then*

$$(X - x)^{q-1} = X^{q-1} + h_{q-2}(x^{-1}X).$$

Proof. From the Binomial Theorem and the previous lemma, we have

$$\begin{aligned}(X-x)^{q-1} &= \sum_{k=0}^{q-1}\binom{q-1}{k}X^k(-x)^{q-1-k} = \sum_{k=0}^{q-1}(-1)^k X^k(-1)^{q-1-k}x^{q-1-k} \\ &= \sum_{k=0}^{q-1}(-1)^{q-1}X^k x^{-k} = \sum_{k=0}^{q-1}(x^{-1}X)^k = X^{q-1} + h_{q-2}(x^{-1}X). \qquad \square\end{aligned}$$

Lemma 1.7.7. *Let $x \in \mathbb{F}_q$ and let $r, t \in \{1, 2, \ldots, q-1\}$ such that $(q-1) \mid rt$. Then*

$$\sum_{s=0}^{t-1}(\zeta^r)^s = \begin{cases} t, & \zeta^r = 1, \\ 0, & \zeta^r \neq 1. \end{cases}$$

Proof. If $\zeta^r = 1$, then

$$\sum_{s=0}^{t-1}(\zeta^r)^s = \sum_{s=0}^{t-1}(1)^s = \sum_{s=0}^{t-1}1 = t.$$

Now suppose that $\zeta^r \neq 1$. Using the formula for the sum of a geometric series, we obtain

$$\sum_{s=0}^{t-1}(\zeta^r)^s = \frac{\zeta^{rt}-1}{\zeta^r - 1} = \frac{\zeta^{(q-1)\frac{rt}{q-1}}-1}{\zeta^r-1} = \frac{1^{\frac{rt}{q-1}}-1}{\zeta^r-1} = \frac{1-1}{\zeta^r-1} = 0. \qquad \square$$

Chapter 2

INTERPOLATION IN FINITE FIELDS

This chapter provides necessary background for later computations. In particular, we will use the Interpolation Formula (Lemma 2.1.2) extensively to construct polynomials in subsequent chapters. The statements (and proofs) of the first two lemmas in Section 2.1 are not original, though the remainder of this chapter is.

2.1 Interpolation Methods

Let $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ be a partial function; that is, given a subset $\{x_1, \ldots, x_k\}$ of $\mathbb{F}_q$, φ is a function $\{x_1, \ldots, x_k\} \to \mathbb{F}_q$. There are two standard methods to interpolate φ to a polynomial $f(X)$ over a finite field such that

$$f(x_i) = \varphi(x_i)$$

for all $1 \leq i \leq k$. The first is the classical Lagrange Interpolation, which is also applicable outside the setting of finite fields (for a proof, see Theorem 1.71 of [14]); the second formula is specific to finite fields (equation (7.1) of [14]).

Lemma 2.1.1 (Lagrange Interpolation)**.** *The partial function* $\varphi\colon \{x_1, \ldots, x_k\} \to \mathbb{F}_q$ *is represented by the polynomial*

$$f(X) = \sum_{i=1}^{k} \left(\prod_{j \neq i} \frac{X - x_j}{x_i - x_j} \right) \varphi(x_i).$$

Lemma 2.1.2 (Interpolation Formula)**.** *The partial function* $\varphi\colon \{x_1, \ldots, x_k\} \to \mathbb{F}_q$ *is represented by the polynomial*

$$f(X) = \sum_{i=1}^{k} \left(1 - (X - x_i)^{q-1}\right) \varphi(x_i).$$

Proof. For want of a proof in [14], we give a sketch here. First note that $x^{q-1} = 1$ for any $x \in \mathbb{F}_q^\times$. Then $1 - (x - x_i)^{q-1}$ is nonzero (and equal to 1) only in the case when $x = x_i$; hence $f(x_i) = \varphi(x_i)$ for all $1 \leq i \leq k$ and $f(x) = 0$ for any $x \in \mathbb{F}_q \setminus \{x_1, \ldots, x_k\}$. □

The distinction between Lagrange Interpolation in Lemma 2.1.1 and the unfortunately (un-)named Interpolation Formula in Lemma 2.1.2 is in how they treat the elements of $\mathbb{F}_q$ not specified by the function φ. Lagrange Interpolation produces a polynomial of degree at most k, but there is no control over the images of the elements of $\mathbb{F}_q \setminus \{x_1, \ldots, x_k\}$ not specified by φ. The Interpolation Formula, on the other hand, effectively extends φ to a function defined on all of $\mathbb{F}_q$ by mapping every element of $\mathbb{F}_q \setminus \{x_1, \ldots, x_k\}$ to 0 (or, with obvious modification, to any specified value), at the expense of losing inherent control over the degree of f. When φ is a function defined on all of $\mathbb{F}_q$, then the polynomials from both interpolations are equal. We will find that using the Interpolation Formula is better suited to the computations we will perform.

The Interpolation Formula in Lemma 2.1.2 has the additional advantage that it extends naturally to produce a bivariate polynomial in $\mathbb{F}_q[X, Y]$ that represents a bivariate (partial) function $\varphi\colon \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_q$.

Lemma 2.1.3 (Bivariate Interpolation)**.** *Let $S \subseteq \mathbb{F}_q \times \mathbb{F}_q$. Then the partial function $\varphi\colon S \to \mathbb{F}_q$ is represented by the polynomial*

$$f(X, Y) = \sum_{(x,y)\in S} \left(1 - (X - x)^{q-1}\right)\left(1 - (Y - y)^{q-1}\right)\varphi(x, y).$$

Proof. Let (x, y) be an element of S, the domain of φ. Then as in the proof of Lemma 2.1.2,

$$\left(1 - (z - x)^{q-1}\right)\left(1 - (w - y)^{q-1}\right)$$

is nonzero, and equal to 1, precisely when $(z, w) = (x, y)$, and hence $f(x, y) = \varphi(x, y)$. For any point (x, y) not in the domain of φ, we have $f(x, y) = 0$, completing the proof. □

2.2 Indicator Functions

An *indicator function* for a subset $S \subseteq \mathbb{F}_q$ is a function $\iota_S \colon \mathbb{F}_q \to \mathbb{F}_q$ satisfying

$$\iota_S(x) = \begin{cases} 1, & x \in S, \\ 0, & x \notin S. \end{cases}$$

In fact, the two Interpolation Theorems furnish our first polynomial indicator function.

Corollary 2.2.1. *A polynomial indicator function for $\{\xi\} \subseteq \mathbb{F}_q$ is given by*

$$\iota_{\{\xi\}}(X) = 1 - (X - \xi)^{q-1}.$$

In particular, a polynomial indicator function for 0 is given by

$$\iota_{\{0\}}(X) = 1 - X^{q-1}.$$

In this section, we will make extensive use of the "all ones" polynomial

$$h_k(X) = 1 + X + X^2 + \cdots + X^k \in \mathbb{F}_q[X]$$

to construct polynomial indicator functions. Note that for $x \neq 1$, we may use the formula for the sum of a geometric series to write

$$h_k(x) = \frac{x^{k+1} - 1}{x - 1}.$$

For instance, choosing $k = q - 1$, we find that

$$h_{q-1}(x) = \frac{x^q - 1}{x - 1} = \frac{x - 1}{x - 1} = 1$$

for all $x \neq 1$ and $h_{q-1}(1) = q \cdot 1 = 0$; thus, $h_{q-1}(X)$ is a polynomial indicator function for $\mathbb{F}_q \setminus \{1\}$.

We will now construct polynomial indicator functions for several substructures of $\mathbb{F}_q$, beginning with a subgroup of $\mathbb{F}_q^+$ of order p.

Theorem 2.2.2 (Indicator Function for a Subgroup of $\mathbb{F}_q^+$ of Order p)**.** *Let $\beta \in \mathbb{F}_q^\times$. A polynomial indicator function for the cyclic subgroup $\langle \beta \rangle \leq \mathbb{F}_q^+$ of order p generated by β is given by*

$$\iota_{\langle \beta \rangle}(X) = h_{\frac{q-p}{p-1}}\left((\beta^{-1}X)^{p-1}\right).$$

Proof. First, observe that $h_{\frac{q-p}{p-1}}\left((\beta^{-1}0)^{p-1}\right) = h_{\frac{q-p}{p-1}}(0) = 1$. For the rest of the proof we will assume that $x \neq 0$. Now $x \in \langle\beta\rangle$ if and only if $x = k\beta$ for some $k \in \mathbb{F}_p^*$, or equivalently, $x \in \langle\beta\rangle$ if and only if

$$(\beta^{-1}x)^{p-1} = (\beta^{-1}(k\beta))^{p-1} = k^{p-1} = 1.$$

Then $x \in \langle\beta\rangle$ implies

$$h_{\frac{q-p}{p-1}}\left((\beta^{-1}x)^{p-1}\right) = h_{\frac{q-p}{p-1}}(1) = \frac{q-p}{p-1} + 1 = \frac{q-1}{p-1} = 1,$$

and $x \notin \langle\beta\rangle$ implies

$$h_{\frac{q-p}{p-1}}\left((\beta^{-1}x)^{p-1}\right) = \frac{((\beta^{-1}x)^{p-1})^{\frac{q-p}{p-1}+1} - 1}{(\beta^{-1}x)^{p-1} - 1} = \frac{(\beta^{-1}x)^{q-1}}{(\beta^{-1}x)^{p-1} - 1} = \frac{1-1}{(\beta^{-1}x)^{p-1} - 1} = 0. \quad \square$$

Next, we will construct a polynomial indicator function for a coset of a subgroup of $\mathbb{F}_q^\times$.

Theorem 2.2.3 (Indicator Function for a Multiplicative Coset in $\mathbb{F}_q^\times$)**.** *Let $m \mid (q-1)$. A polynomial indicator function for the multiplicative coset $\zeta^a\langle\zeta^{\frac{q-1}{m}}\rangle \subseteq \mathbb{F}_q^\times$ is given by*

$$\iota_{\zeta^a\langle\zeta^{(q-1)/m}\rangle}(X) = -m\left(h_{\frac{q-1}{m}}\left((\zeta^{-a}X)^m\right) - 1\right).$$

Proof. Consider the sum

$$S := \sum_{t=0}^{k}(x^m)^t = h_k(x^m).$$

When $x^m = 1$, we have

$$S = \sum_{t=0}^{k} 1 = k + 1,$$

and when $x^m \neq 1$, we can use the geometric series summation to obtain

$$S = \frac{x^{m(k+1)} - 1}{x^m - 1}.$$

First, suppose $x \in \zeta^a\langle\zeta^{\frac{q-1}{m}}\rangle$, so that $\zeta^{-a}x \in \langle\zeta^{\frac{q-1}{m}}\rangle$ and $(\zeta^{-a}x)^m = 1$. Then $h_{\frac{q-1}{m}}\left((\zeta^{-a}x)^m\right) = \frac{q-1}{m} + 1$ by the above formula, and hence

$$-m\left(h_{\frac{q-1}{m}}\left((\zeta^{-a}x)^m\right) - 1\right) = -m\left(\frac{q-1}{m} + 1 - 1\right) = -(q-1) = 1.$$

On the other hand, when $x \notin \zeta^a \langle \zeta^{\frac{q-1}{m}} \rangle$, we have that $(\zeta^{-a}x)^m \neq 1$. Then, again using the geometric series summation, we have

$$h_{\frac{q-1}{m}}\left((\zeta^{-a}x)^m\right) = \frac{x^{m(\frac{q-1}{m}+1)}-1}{x^m-1} = \frac{x^{q-1+m}-1}{x^m-1} = \frac{x^m-1}{x^m-1} = 1.$$

Thus, in this case

$$-m\left(h_{\frac{q-1}{m}}\left((\zeta^{-a}x)^m\right)-1\right) = -m\,(1-1) = 0,$$

and the theorem is proved. □

As an easy corollary, we obtain another indicator function for any nonzero element of $\mathbb{F}_q$ (cf. Corollary 2.2.1).

Corollary 2.2.4 (Indicator Function for a Nonzero Element of $\mathbb{F}_q$)**.** *Let $\xi \in \mathbb{F}_q^\times$. A polynomial indicator function for $\{\xi\}$ is given by*

$$\iota_{\{\xi\}}(X) = 1 - h_{q-1}(\xi^{-1}X).$$

Proof. Take $m = 1$ and $\zeta^a = \xi$ in the above theorem, so that

$$\zeta^a\langle\zeta^{\frac{q-1}{m}}\rangle = \xi\langle\zeta^{q-1}\rangle = \xi\langle 1\rangle = \xi.$$ □

Finally, we obtain an indicator function for an arbitrary element of $\mathbb{F}_q$ in terms of an "all ones"-polynomial. This result will prove very useful in later computations.

Corollary 2.2.5 (Indicator Function for an Element of $\mathbb{F}_q$)**.** *Let $\xi \in \mathbb{F}_q$. A polynomial indicator function for $\{\xi\}$ is given by*

$$\iota_{\{\xi\}}(X) = 1 - X^{q-1} - \xi^{q-1}h_{q-2}(\xi^{q-2}X).$$

Proof. If $\xi \neq 0$, then noting $\xi^{q-1} = 1$, we have

$$\begin{aligned}\iota_{\{\xi\}}(X) &= 1 - h_{q-1}(\xi^{-1}X)\\ &= 1 - (\xi^{-1}X)^{q-1} - h_{q-2}(\xi^{-1}X)\\ &= 1 - X^{q-1} - \xi^{q-1}h_{q-2}(\xi^{q-2}X),\end{aligned}$$

from the previous corollary. This last line is also an indicator function for $\{0\}$, since

$$1 - X^{q-1} - 0^{q-1}h_{q-2}(0^{q-2}X) = 1 - X^{q-1} = \iota_{\{0\}}(X)$$

agrees with Corollary 2.2.1. □

2.3 Application of Indicator Functions to Produce Representation Polynomials

We can use the polynomial indicator functions of the previous section to construct our first polynomial group representations, which arise naturally as representations of substructures in a finite field. We begin by constructing polynomials forming cyclic groups of order p and order m (for $m \mid (q-1)$) using Theorems 2.2.2 and 2.2.3, respectively, which exploit the group structure of $\mathbb{F}_q^+$ and $\mathbb{F}_q^\times$, respectively. Then we use Corollary 2.2.5 to construct polynomials representing transpositions and general cycles. In each of these representations save the last one, we will fix every element of $\mathbb{F}_q$ not in the associated substructure, so that (in anticipation of the construction method of the next chapter) the resulting representation polynomials are permutation polynomials.

Consider first the cycle in $\mathbb{F}_q^+$ generated by a nonzero element β:

$$\langle\beta\rangle = \{k\beta : k \in \mathbb{F}_p\} = \{\beta, 2\beta, \ldots, (p-1)\beta, p\beta = 0\}.$$

This cycle describes a subgroup isomorphic to $C_p \leq \mathbb{F}_q^+$, so we can apply Theorem 2.2.2 to construct a polynomial representing it.

Theorem 2.3.1. *Let $\beta \in \mathbb{F}_q^\times$. Then the polynomial representing the element $k\beta$ of $\langle\beta\rangle \cong C_p \leq \mathbb{F}_q^+$ is*

$$f_{k\beta}(X) = X + k\beta h_{\frac{q-p}{p-1}}\left((\beta^{-1}X)^{p-1}\right).$$

Proof. The action of $k\beta$ on $\mathbb{F}_q$ should fix any element of $\mathbb{F}_q$ not in $\langle\beta\rangle$ and should add $k\beta$ otherwise. Theorem 2.2.2 then shows that the polynomial

$$f_{k\beta}(X) = X + (k\beta)\cdot\iota_{\langle\beta\rangle}(X) = X + k\beta h_{\frac{q-p}{p-1}}\left((\beta^{-1}X)^{p-1}\right)$$

performs the desired action. □

Next, let $mm' = q-1$ and choose $z \in \{1, 2, \ldots, m-1\}$ such that $(z, m) = 1$. Recalling that $\mathbb{F}_q^\times = \langle \zeta \rangle$, define $\xi = (\zeta^{m'})^z$ and consider the following cycle in $\mathbb{F}_q^\times$:

$$\langle \xi \rangle = \left\{ \xi^k : k \in \{1, 2, \ldots, m\} \right\} = \left\{ \zeta^{m'z}, \zeta^{2m'z}, \ldots, \zeta^{(m-1)m'z}, \zeta^{mm'z} = 1 \right\}.$$

This cycle describes a subgroup isomorphic to $C_m \leq \mathbb{F}_q^\times$, so we can apply Theorem 2.2.3 to construct a polynomial representing it.

Theorem 2.3.2. *Suppose $m \mid (q-1)$, let $z \in \{1, 2, \ldots, m-1\}$ such that $(z, m) = 1$, and define $\xi = \left(\zeta^{\frac{q-1}{m}}\right)^z$. Then the polynomial representing the element ξ^k of $\langle \xi \rangle \cong C_m \leq \mathbb{F}_q^\times$ is*

$$f_{\xi^k}(X) = X + m(1 - \xi^k) X h_{\frac{q-1}{m}-1}(X^m).$$

Proof. The action of ξ^k on $\mathbb{F}_q$ should fix any element of $\mathbb{F}_q$ not in $\langle \xi \rangle$ and should multiply by ξ^k otherwise. Theorem 2.2.3 then shows that the polynomial

$$f_{\xi^k}(X) = X + (\xi^k X - X) \cdot \iota_{\langle \xi \rangle}(X) = X - m(\xi^k - 1) X \left(h_{\frac{q-1}{m}}(X^m) - 1 \right)$$

performs the desired action. Simplifying, we obtain

$$\begin{aligned}
f_{\xi^k}(X) &= X + m(1 - \xi^k) \sum_{i=1}^{\frac{q-1}{m}} X^{mi+1} \\
&= X + m(1 - \xi^k) \left(X^q + \sum_{i=1}^{\frac{q-1}{m}-1} X^{mi+1} \right) \\
&= X + m(1 - \xi^k) \left(X + X \sum_{i=1}^{\frac{q-1}{m}-1} X^{mi} \right) \\
&= X + m(1 - \xi^k) X \sum_{i=0}^{\frac{q-1}{m}-1} X^{mi} \\
&= X + m(1 - \xi^k) X h_{\frac{q-1}{m}-1}(X^m).
\end{aligned}$$

□

For the remainder of this section, we consider polynomials representing more-general permutations of $\mathbb{F}_q$.

Theorem 2.3.3. *Let $a, b \in \mathbb{F}_q^\times$. The polynomial representing the transposition (a, b) is given by*

$$f_{(a,b)}(X) = X + (a-b)h_{q-2}(a^{-1}X) + (b-a)h_{q-2}(b^{-1}X),$$

and the polynomial representing the transposition $(0, a)$ is given by

$$f_{(0,a)}(X) = X + ah_{q-2}(a^{-1}X).$$

Proof. We will use Corollary 2.2.5 to construct a polynomial representing the transposition (a, b) for distinct $a, b \in \mathbb{F}_q$. Such a polynomial should fix each element of $\mathbb{F}_q$ not equal to either a or b, should take the value b at a, and should take the value a at b. Since the polynomial X fixes $\mathbb{F}_q$ pointwise under evaluation, we have that

$$\begin{aligned} f_{(a,b)}(X) &= X + (b-a)\iota_{\{a\}}(X) + (a-b)\iota_{\{b\}}(X) \\ &= X + (b-a)\left(1 - X^{q-1} - a^{q-1}h_{q-2}(a^{q-2}X)\right) \\ &\qquad + (a-b)\left(1 - X^{q-1} - b^{q-1}h_{q-2}(b^{q-2}X)\right), \end{aligned}$$

where the $(b-a)$ and $(a-b)$ factors on the second and third terms, respectively, compensate for the extra summand of a or b, respectively, from the first (X) term.

When $ab \neq 0$, we have that $a^{q-1} = b^{q-1} = 1$, and upon opening parentheses, we notice that the leading and constant terms cancel. Thus

$$f_{(a,b)}(X) = X + (a-b)h_{q-2}(a^{-1}X) + (b-a)h_{q-2}(b^{-1}X),$$

as desired.

When $b = 0$, the last term simplifies as follows:

$$f_{(0,a)}(X) = X + (0-a)\left(1 - X^{q-1} - a^{q-1}h_{q-2}(a^{q-2}X)\right) + (a-0)\left(1 - X^{q-1}\right).$$

Opening parentheses, we again notice that the leading and constant terms cancel, leaving

$$f_{(0,a)}(X) = X + ah_{q-2}(a^{-1}X). \qquad \square$$

Corollary 2.3.4. *Let $a \in \mathbb{F}_q^\times$, where q is odd. The polynomial representing the transposition $(a, -a)$ is given by*

$$f_{(a,-a)}(X) = X - 4Xh_{\frac{q-3}{2}}\left((a^{-1}X)^2\right).$$

Proof. From the previous theorem, we know that

$$f_{(a,-a)}(X) = X + (-a-a)h_{q-2}(a^{-1}X) + (a-(-a))h_{q-2}(-a^{-1}X).$$

Expanding the h-polynomials, we obtain

$$\begin{aligned} f_{(a,-a)}(X) &= X - 2a\left(\sum_{k=0}^{q-2}(a^{-1})^k X^k\right) + 2a\left(\sum_{k=0}^{q-2}(-1)^k(a^{-1})^l X^k\right) \\ &= X + 2a\sum_{k=0}^{q-2}\left(-1+(-1)^k\right)(a^{-1})^k X^k. \end{aligned}$$

Note that $(-1)^k$ equals 1 or -1 according to whether k is odd or even, respectively; then $-1+(-1)^k$ is -2 for k odd and 0 for k even. Using this to simplify the polynomial above, we obtain

$$\begin{aligned} f_{(a,-a)}(X) &= X + 2a\sum_{k=0}^{\frac{q-3}{2}}(-2)(a^{-1}X)^{2k+1} \\ &= X - 4a(a^{-1}X)h_{\frac{q-2}{2}}\left((a^{-1}X)^2\right) \\ &= X - 4Xh_{\frac{q-3}{2}}\left((a^{-1}X)^2\right). \end{aligned}$$

□

Theorem 2.3.5. *Let π be the permutation of $\mathbb{F}_q$ represented as the product of disjoint (possibly trivial) cycles as*

$$\pi = (a_{11}, a_{12}, \ldots, a_{1m_1})(a_{21}, a_{22}, \ldots, a_{2m_2})\cdots(a_{k1}, a_{k2}, \ldots, a_{km_k}).$$

Then the polynomial representing π is given by

$$f_\pi(X) = X + \sum_{i=1}^{k}\sum_{j=1}^{m_i} a_{ij}^{q-1} h_{q-2}\left(a_{ij}^{q-2}X\right)(a_{ij} - a_{i(j+1)}),$$

where the subscript j in a_{ij} is read modulo m_i.

Proof. We follow the same approach as in the proof of Theorem 2.3.3, using Corollary 2.2.5 to build the polynomial representing π. Such a polynomial should fix each element of $\mathbb{F}_q$ not involved in a cycle of π, and should take a_{ij} to $a_{i(j+1)}$, where the subscript j is read modulo m_i. Since the polynomial X fixes $\mathbb{F}_q$ pointwise under evaluation, we have that

$$\begin{aligned} f_\pi(X) &= X + \sum_{i=1}^{k}\sum_{j=1}^{m_i}(a_{i(j+1)} - a_{ij})\iota_{\{a_{ij}\}}(X) \\ &= X + \sum_{i=1}^{k}\sum_{j=1}^{m_i}(a_{i(j+1)} - a_{ij})\left(1 - X^{q-1} - a_{ij}^{q-1}h_{q-2}(a_{ij}^{q-2}X)\right), \end{aligned}$$

where the $(a_{i(j+1)} - a_{ij})$ factors compensate for the extra summand of a_{ij} provided by the initial X term.

Breaking up the double sum as follows:

$$f_\pi(X) = X + \sum_{i=1}^{k}\sum_{j=1}^{m_i}(a_{i(j+1)} - a_{ij})\left(1 - X^{q-1}\right) - \sum_{i=1}^{k}\sum_{j=1}^{m_i}(a_{i(j+1)} - a_{ij})a_{ij}^{q-1}h_{q-2}(a_{ij}^{q-2}X),$$

we notice that the first double sum telescopes, and we are left with

$$f_\pi(X) = X + \sum_{i=1}^{k}\sum_{j=1}^{m_i} a_{ij}^{q-1}h_{q-2}\left(a_{ij}^{q-2}X\right)(a_{ij} - a_{i(j+1)}),$$

as desired. □

We remark that Theorem 2.3.3 follows as a corollary of the previous theorem. However, the construction we used for both proofs is particularly transparent for a transposition, so it is hoped that the proof of the former helps to illuminate the proof of the latter.

We conclude this section by describing a second polynomial function representing the cycle π. In contradistinction to the polynomial in the previous theorem, the following representation polynomial acts as a constant on the non-specified elements and hence is the only polynomial in this dissertation that is constructed to *not* be a permutation polynomial.

Theorem 2.3.6. *Let π be a permutation of some subset $S \subseteq \mathbb{F}_q$, represented as the product of disjoint (possibly trivial) cycles as*

$$\pi = (a_{11}, a_{12}, \ldots, a_{1m_1})(a_{21}, a_{22}, \ldots, a_{2m_2}) \cdots (a_{k1}, a_{k2}, \ldots, a_{km_k}).$$

Then the polynomial representing the permutation π on S while mapping all elements of $\mathbb{F}_q \setminus S$ to some fixed $c \in \mathbb{F}_q$ is given by

$$f(X) = c + \sum_{i=1}^{k} \sum_{j=1}^{m_i} (a_{i(j+1)} - c) \left(1 - (X - a_{ij})^{q-1}\right).$$

Proof. We reprise the same method of proof once again, but using Corollary 2.2.1 instead to build the representation polynomial since the double sum over the leading and constant terms will not (in general) telescope.

The desired polynomial should map each element of $\mathbb{F}_q \setminus S$ to c, and should take a_{ij} to $a_{i(j+1)}$, where the subscript j is read modulo m_i. Thus

$$\begin{aligned} f_\pi(X) &= c + \sum_{i=1}^{k} \sum_{j=1}^{m_i} (a_{i(j+1)} - c) \iota_{\{a_{ij}\}}(X) \\ &= c + \sum_{i=1}^{k} \sum_{j=1}^{m_i} (a_{i(j+1)} - a_{ij}) \left(1 - (X - a_{ij})^{q-1}\right), \end{aligned}$$

where the $(a_{i(j+1)} - c)$ factors compensate for the extra summand provided by the initial term. □

Chapter 3

THE THEORY OF CONSTRUCTING GROUPS OF PERMUTATION POLYNOMIALS

3.1 Constructing Polynomial Representations of Groups

We begin by describing a new method for constructing groups of permutation polynomials. Let G be a group of order $|G| \leq q$ and associate elements of G with elements of $\mathbb{F}_q$ according to an injective function $\sigma\colon G \hookrightarrow \mathbb{F}_q$. In general, we choose σ to preserve some of the group structure, though this is not necessary for the basic theory. Define the binary operation $*\colon G \times \mathbb{F}_q \to \mathbb{F}_q$ by

$$g * x := \begin{cases} \sigma\big(g \cdot \sigma^{-1}(x)\big), & x \in \mathrm{Im}(\sigma), \\ x, & x \notin \mathrm{Im}(\sigma), \end{cases}$$

for all $g \in G$ and all $x \in \mathbb{F}_q$.

Theorem 3.1.1. *The binary operation $*$ defines an action of G on $\mathbb{F}_q$, and the group G under this action is permutation isomorphic to the left regular representation of G.*

Proof. Let $g_1, g_2 \in G$ and $x \in \mathbb{F}_q$, and let e denote the identity of G. Then $e * x = x$ for $x \notin \mathrm{Im}(\sigma)$ and

$$e * x = \sigma(e \cdot \sigma^{-1}(x)) = \sigma(\sigma^{-1}(x)) = x$$

for $x \in \mathrm{Im}(\sigma)$, so the identity of G fixes every element of $\mathbb{F}_q$. Moreover, $g_1 * (g_2 * x) = g_1 * (x) = x$ for $x \notin \mathrm{Im}(\sigma)$ and

$$\begin{aligned} g_1 * (g_2 * x) &= g_1 * \sigma(g_2 \cdot \sigma^{-1}(x)) \\ &= \sigma(g_1 \cdot \sigma^{-1}(\sigma(g_2 \cdot \sigma^{-1}(x)))) \\ &= \sigma(g_1 \cdot (g_2 \cdot \sigma^{-1}(x))) \end{aligned}$$

$$= \sigma((g_1 g_2) \cdot \sigma^{-1}(x))$$
$$= (g_1 g_2) * x$$

for $x \in \mathrm{Im}(\sigma)$ shows that $*$ satisfies the associativity condition of a group action.

To see that G under the action $*$ is permutation isomorphic to the left regular action of G, take $\psi\colon G \to G$ to be the identity map and define $\alpha\colon G \to \sigma(G) \subseteq \mathbb{F}_q$ by $\alpha = \sigma$. Writing $x = \sigma(s) \in \mathbb{F}_q$ for a fixed, but arbitrary, $s \in G$, we have

$$\alpha\left(g \cdot s\right) = \sigma\left(g \cdot \sigma^{-1}(x)\right) = g * x = \psi(g) * \sigma\left(\sigma^{-1}(x)\right) = \psi(g) \cdot \alpha(s)$$

for all $g \in G$ and $s \in G$. Indeed, this shows that we first relabel the group according to σ so that G then acts naturally on itself by left-multiplication. □

The action of each $g \in G$ on $\mathbb{F}_q$ defines a permutation θ_g of $\mathbb{F}_q$. Interpolating will thus produce a reduced (permutation) polynomial $f_g(X) \in \mathbb{F}_q[X]$ which represents θ_g and hence also represents the action of g on $\mathbb{F}_q$. Explicitly, we compute $f_g(X)$ according to the Interpolation Formula (Lemma 2.1.2):

$$f_g(X) = \sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right)(g * x).$$

Often the representation will rely on a collection Z of parameters, and we will write $f_g^{[Z]}(X)$ as an indication of the dependence of the representation on these parameters. For $g \in G$, we call the permutation polynomial $f_g(X)$ (or $f_g^{[Z]}(X)$) the *representation polynomial* of g as it represents the left regular action of G on itself, under composition modulo $X^q - X$. We shall prove this claim forthwith after noting some properties of representation polynomials. In computations, we will denote the composition of a polynomial $f(X)$ with itself k times, reduced modulo $X^q - X$, by $f(X)^{[k]}$.

Lemma 3.1.2. *Representation polynomials are permutation polynomials which possess the following properties.*

1. *The composition of two representation polynomials, reduced modulo $X^q - X$, is again a representation polynomial. In fact,*

$$\left(f_{g_1} \circ f_{g_2}\right)(X) = f_{g_1 g_2}(X).$$

2. *The composition of the representation of g with itself k times, reduced modulo $X^q - X$, is the representation of g^k. Explicitly,*

$$f_g(X)^{[k]} = f_{g^k}(X),$$

and in particular, $\big(f_g(X)\big)^{[-1]} = f_{g^{-1}}(X)$.

3. *If $g \neq e$, then $f_g(X)$ fixes precisely the elements of $\mathbb{F}_q \setminus \mathrm{Im}(\sigma)$. In particular, f_g fixes no point of $\mathbb{F}_q$ when $|G| = q$.*

4. *The constant term of $f_g(X)$ is $g * 0$. In particular, the constant term is $\sigma(g)$ when $\sigma(0) = e$.*

Proof. Let $x \in \mathbb{F}_q$ and $g_1, g_2 \in G$. Then $g_1 * (g_2 * x) = (g_1 g_2) * x$ since $*$ defines a group action, so $f_{g_1}(f_{g_2}(x)) = f_{g_1 g_2}(x)$. Interpolation yields the first statement, and applying induction easily gives the second.

It follows immediately from the definition of the action $*$ that every element of G fixes $\mathbb{F}_q \setminus \mathrm{Im}(\sigma)$ pointwise. If the action of some $g \in G$ fixed an element $x \in \mathrm{Im}(\sigma)$, then we would have

$$x = g * x = \sigma(g \cdot \sigma^{-1}(x)),$$

and applying σ^{-1} to both sides yields $\sigma^{-1}(x) = g \cdot \sigma^{-1}(x)$. Since σ is injective, the element g acts as the identity of G, hence must be the identity of G, proving the third statement.

To prove the fourth statement, note first that for a fixed $x \in \mathbb{F}_q$ and any $y \in \mathbb{F}_q$,

$$(y - x)^{q-1} = \begin{cases} 1, & y \neq x, \\ 0, & y = x, \end{cases}$$

and hence $1 - (y - x)^{q-1}$ is nonzero precisely when $y = x$. Thus,

$$f_g(0) = \sum_{x \in \mathbb{F}_q} \left(1 - (0 - x)^{q-1}\right)(g * x) = \left(1 - (0 - 0)^{q-1}\right)(g * 0) = g * 0.$$

Moreover, when $\sigma(e) = 0$ we have

$$g * 0 = \sigma\left(g \cdot \sigma^{-1}(0)\right) = \sigma(g \cdot e) = \sigma(g). \qquad \square$$

Note that statement 1 above shows that the map defined by $g \mapsto f_g$ is a homomorphism, that is, representation polynomials indeed describe the representation

$$G \to \mathrm{Sym}(\mathbb{F}_q) \hookrightarrow \mathbb{F}_q[X]/(X^q - X).$$

Moreover, this representation is faithful since distinct group elements produce distinct permutations of $\mathbb{F}_q$, and hence distinct representation polynomials. We shall denote the set of representation polynomials of G by $\Gamma = \{f_g(X) : g \in G\}$; when the representation polynomials depend on a parameter set Z, we will accordingly denote the set of representation polynomials by $\Gamma^{[Z]}$.

Theorem 3.1.3. *The set Γ of representation polynomials of a group G forms a group isomorphic to G under composition modulo $X^q - X$.*

Proof. We claim $f_e(X)$ acts as the identity for Γ. Indeed, since $*$ is a group action, we have $e * x = x$ for all $x \in \mathbb{F}_q$. Thus $f_e(X) = X$ as desired, and we conclude that Γ is a group since the first two statements of Lemma 3.1.2 show that Γ is closed and possesses multiplicative inverses. As noted above, the first statement in Lemma 3.1.2 shows that Γ behaves under composition and reduction precisely as the group G itself does, hence $\Gamma \cong G$. □

3.2 The Preserved Subgroup and Its Properties

The motivation for developing the method just described is to produce new families of permutation polynomials (which happen to be endowed with a group structure inherited from the construction). The previous theorem guarantees that we indeed produce groups of permutation polynomials, but it is not clear whether they will come from families of permutation polynomials which are already known. Our intuition is that choosing σ to preserve some of the group structure will lead to the most visually appealing families of permutation polynomials, that is those with simply-described coefficients, relatively few terms, etc. We make this precise as follows.

Typically, we construct σ so that the images of some of the group elements in the field maintain their group structure even under the field arithmetic; that is, by

"preserving structure" we mean that σ restricts to a homomorphism on some subset of G. The requirement that σ be injective means that σ can be a homomorphism only if G is an elementary abelian p-group (for a representation into the additive group of $\mathbb{F}_q$) or a cyclic group of order dividing $q-1$ (for a representation into the multiplicative group of $\mathbb{F}_q$). Thus, we do not expect σ to be a homomorphism itself, but rather to behave like a homomorphism only on some portion of the group G.

It will often be convenient to treat the theory for both $\mathbb{F}_q^+$ and $\mathbb{F}_q^\times$ at once, so we will write $\star$ to represent the appropriate group operation in computations. Accordingly, for any $a_1, \ldots, a_k \in \mathbb{F}_q$ and any nonnegative integers $\delta_1, \ldots, \delta_k$ we define

$$\bigstar_{i=1}^{k} a_i \delta_i := \underbrace{\left(a_1 \star a_1 \star \cdots \star a_1\right)}_{\delta_1 \text{ times}} \star \cdots \star \underbrace{\left(a_k \star a_k \star \cdots \star a_k\right)}_{\delta_k \text{ times}},$$

and we let $\mathrm{id}^\star$ denote the identity of $\mathbb{F}_q^\star$, so that $\mathrm{id}^+ = 0$ and $\mathrm{id}^\times = 1$. In what follows, we consider only functions σ which satisfy $\sigma(e) = \mathrm{id}^\star$, and we will call σ and its corresponding representation *additive* (respectively, *multiplicative*) if $\sigma(e) = 0$ (respectively, if $\sigma(e) = 1$). In either case, we refer to such a function σ as an *assignation*; we will only consider representations for which σ is an assignation. Note that an assignation cannot simultaneously be both additive and multiplicative, so we will restrict ourselves to considering only the appropriate operation as being denoted by $\star$ instead of both operations simultaneously.

By itself, an assignation indicates that a small amount of structure has already been preserved, namely, that there is a natural algebraic correspondence between the identities of the group and the field. We think of this as a sort of local preservation of structure; the following theorem tells us something about the structure preserved at a global level.

Lemma 3.2.1. *Let σ and σ' be two assignations of a group G. If $\sigma(G)$ and $\sigma'(G)$ are both subgroups of $\mathbb{F}_q^\star$, then $\sigma(G) \cong \sigma'(G)$.*

Proof. Since the assignations are injective by definition, we have that $|\sigma(G)| = |\sigma'(G)| = |G|$.

Suppose first that σ and σ' are additive assignations. The subgroups of $\mathbb{F}_q^+$ are elementary abelian p-groups, and since $|\sigma(G)| = |\sigma'(G)|$, $\sigma(G)$ and $\sigma'(G)$ are elementary abelian p-groups of the same order. Therefore they are isomorphic.

If σ and σ' are multiplicative assignations, then $\sigma(G) \cong C_{|G|}$ and $\sigma'(G) \cong C_{|G|}$ since the cyclic group C_m has a unique (cyclic) subgroup C_d for each divisor d of m. Thus $\sigma(G)$ and $\sigma'(G)$ are isomorphic in this case as well. □

It will prove useful to define a measure of how much structure an assignation preserves. Given an assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\star$, we call the set

$$P^\star(G,\sigma) = \{g \in G : \forall\ x \in \sigma(G),\ g * x = \sigma(g) \star x\}$$

the *preserved subset* of the assignation. We remark that since $g * x = \sigma\left(g \cdot \sigma^{-1}(x)\right)$, for $g \in P^\star(G,\sigma)$ we have

$$\sigma\left(g \cdot \sigma^{-1}(x)\right) = \sigma(g) \star x = \sigma(g) \star \sigma\left(\sigma^{-1}(x)\right)$$

for all $x \in \sigma(G)$, that is, σ behaves like a homomorphism on the preserved subset. We will see shortly that this is, in fact, the case: the preserved subset $P^\star(G,\sigma)$ is a group and the restriction of σ to $P^\star(G,\sigma)$ is indeed a homomorphism from $P^\star(G,\sigma)$ into $\mathbb{F}_q^\star$.

Lemma 3.2.2. *Let $g \in G$ and let $\sigma\colon G \hookrightarrow \mathbb{F}_q^\star$ be an assignation. Then for some $c \in \mathbb{F}_q$ and all $x \in \sigma(G)$, $g * x = c \star x$ if and only if $c = \sigma(g)$ and $g \in P^\star(G,\sigma)$.*

Proof. Suppose $g * x = c \star x$ for some $c \in \mathbb{F}_q$ and all $x \in \sigma(G)$. Then in particular, $g * \mathrm{id}^\star = c \star \mathrm{id}^\star = c$. Since

$$g * \mathrm{id}^\star = \sigma\left(g \cdot \sigma^{-1}(\mathrm{id}^\star)\right) = \sigma(g \cdot e) = \sigma(g),$$

we have that $c = \sigma(g)$. Thus $g * x = \sigma(g) \star x$ for all $x \in \sigma(G)$, and hence $g \in P^\star(G,\sigma)$.

On the other hand, for $g \in P^\star(G,\sigma)$ we have $g * x = \sigma(g) \star x$ for all $x \in \sigma(G)$ by definition. Taking $c = \sigma(g)$ completes the proof. □

Corollary 3.2.3. *Let $\sigma\colon G \hookrightarrow \mathbb{F}_q$ be an assignation and suppose $\sigma(G) = \mathbb{F}_q^\star$. Then the linear polynomial $c \star X$ is a representation polynomial if and only if $c = \sigma(g)$ for some $g \in P^\star(G,\sigma)$.*

Proof. This is simply a rephrasing of the previous lemma in the language of representation polynomials. □

From the above corollary, we see that there is a correspondence, via linear representation polynomials, between group elements on which σ behaves like a homomorphism and linear representation polynomials. This correspondence indicates that the preserved subset is indeed a decent measure of the amount of structure preserved by the assignation; the next two results will make this statement precise.

Theorem 3.2.4. *Let $\sigma\colon G \hookrightarrow \mathbb{F}_q^\star$ be an assignation. Then the preserved subset $P^\star(G,\sigma)$ is an abelian subgroup of G, and the restriction of σ to the preserved subgroup,*

$$\sigma\big|_{P^\star(G,\sigma)}\colon P^\star(G,\sigma) \hookrightarrow \mathbb{F}_q^\star,$$

is a homomorphism.

Proof. Let $g, h \in P^\star(G,\sigma)$. Since $*$ defines a group action, for all $x \in \sigma(G)$ we have

$$gh * x = g * (h * x) = \sigma(g) \star (\sigma(h) \star x) = (\sigma(g) \star \sigma(h)) \star x.$$

In particular, taking $x = \mathrm{id}^\star$ yields $gh * \mathrm{id}^\star = (\sigma(g) \star \sigma(h)) \star \mathrm{id}^\star = \sigma(g) \star \sigma(h)$. But we also have

$$gh * \mathrm{id}^\star = \sigma\left(gh \cdot \sigma^{-1}(\mathrm{id}^\star)\right) = \sigma(gh \cdot e) = \sigma(gh),$$

and hence $\sigma(gh) = \sigma(g) \star \sigma(h)$ for all $g, h \in P^\star(G,\sigma)$. Then for any $x \in \sigma(G)$, we now have

$$gh * x = (\sigma(g) \star \sigma(h)) \star x = \sigma(gh) \star x,$$

which shows that $gh \in P^\star(G,\sigma)$. Therefore $P^\star(G,\sigma)$ is closed. Moreover, for all $x \in \sigma(G)$,

$$e * x = x = \mathrm{id}^\star \star x = \sigma(e) \star x$$

shows that $e \in P^\star(G,\sigma)$, and hence $P^\star(G,\sigma)$ is indeed a group.

That $P^\star(G,\sigma)$ is abelian follows immediately from the commutativity of $\mathbb{F}_q^\star$ since

$$\sigma(gh) = \sigma(g) \star \sigma(h) = \sigma(h) \star \sigma(g) = \sigma(hg)$$

for all $g, h \in P^\star(G, \sigma)$. $\square$

In light of the first statement of the theorem, we shall refer to $P^\star(G, \sigma)$ as the *preserved subgroup* from now on. In addition to indicating local structure of the assignation, i.e. where σ is a homomorphism, the preserved subgroup also has global control over the resulting representation polynomials. Let $H \leq G$, and let $\{g_i\}$ be a set of coset representatives for G/H, the set of right cosets of H in G. (Note that we do not require that H be a normal subgroup of G, so G/H is not, in general, a group.) Now let $hg_i \in G$ and construct σ according to the rule

$$\sigma(hg_i) = \sigma(h) \star \sigma(g_i),$$

with the conditions that σ restricted to H, $\sigma\big|_H \colon H \hookrightarrow \mathbb{F}_q^\star$, is an injective homomorphism and that $\{\sigma(g_i)\}$ is a set of coset representatives for $\sigma(G)/\sigma(H)$. We call this construction of the assignation σ *construction by cosets*.

Certainly for any subgroup $H \leq G$, any injective homomorphism $\sigma\big|_H \colon H \hookrightarrow \mathbb{F}_q$, and any choice of coset representatives $\{\sigma(g_i)\}$ of $\sigma(G)/\sigma(H)$, we can construct an assignation. Conversely, it is also true that every assignation arises from this construction.

Theorem 3.2.5. *Every assignation $\sigma \colon G \hookrightarrow \mathbb{F}_q^\star$ occurs as a coset construction of the subgroup $H = P^\star(G, \sigma)$.*

Proof. Let $h \in P^\star(G, \sigma)$ and $g \in G/P^\star(G, \sigma)$. Then

$$\begin{aligned} hg * x &= \sigma\left(hg \cdot \sigma^{-1}(x)\right) \\ &= \sigma\left(h \cdot \left(g \cdot \sigma^{-1}(x)\right)\right) \\ &= \sigma\left(h \cdot \sigma^{-1}\left(\sigma\left(g \cdot \sigma^{-1}(x)\right)\right)\right) \\ &= \sigma(h) \star \sigma\left(g \cdot \sigma^{-1}(x)\right) \end{aligned}$$

holds for all $x \in \sigma(G)$ by the definition of $P^\star(G, \sigma)$. Specially, for $x = \mathrm{id}^\star$ we have

$$\sigma(hg) = hg * \mathrm{id}^\star = \sigma(h) \star \sigma\left(g \cdot \sigma^{-1}(\mathrm{id}^\star)\right) = \sigma(h) \star \sigma(g \cdot e) = \sigma(h) \star \sigma(g).$$

Since every element of G may be written as hg_j for some $h \in H$ and some element g_j of a set $\{g_i\}$ of coset representatives for G/H, it follows that

$$\left\{\sigma(hg_j) = \sigma(h) \star \sigma(g_j) : h \in H \text{ and } g_j \in \{g_i\}\right\} = \sigma(G).$$

Thus $\{\sigma(g_i)\}$ must be a system of coset representatives for $\sigma(G)/\sigma(H)$, showing that the assignation σ can be constructed by cosets. □

3.3 Preserving Group Structure in Field Structure

Since the restriction of an assignation is a homomorphism on the preserved subgroup, we can preserve the most group structure by constructing assignations which are homomorphisms on large subgroups of G; that is, those for which many representation polynomials are linear (by Corollary 3.2.3). The intuition is that by preserving more structure, the remaining representation polynomials will also have a relatively nice form.

One very strong way to preserve structure is by defining the assignation as follows. Fix a presentation $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j \rangle$ with generators $a_1, \ldots, a_k$ and relations $R_1, \ldots, R_j$. We say that an assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\star$ is a *hemimorphism* if for all $g = \prod_{i=1}^k a_i^{\delta_i} \in G$, we have

$$\sigma(g) = \sigma\left(\prod_{i=1}^{k} a_i^{\delta_i}\right) = \bigstar_{i=1}^{k} \sigma(a_i)\delta_i.$$

In general, σ is a hemimorphism if each element of $\sigma(G)$ is uniquely representable as a sum or product (as appropriate to the type of assignation) of images of generators of G. Thus a hemimorphism behaves like a homomorphism with respect to a product of generators of G, though not (in general) with respect to products of arbitrary elements of G.

In addition to representations which are hemimorphisms, we will also be interested in multiplicative representations of cyclic groups which are nearly hemimorphisms, in the following sense. For a cyclic group $G = \langle g \rangle$ such that $(|G| - 1) \mid (q - 1)$, we say that a multiplicative assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$ *preserves a long cycle* if $\sigma(g)$ is

a generator of the subgroup of $\mathbb{F}_q^\times$ of order $\frac{q-1}{|G|-1}$ and $g * x = \sigma(g)\, x$ for all but two values of $x \in \sigma(G)$. Note that this is a weakening of the condition from the definition of preserved subgroup, which requires that $g * x = \sigma(g)\, x$ for *all* $x \in \sigma(G)$. The "long cycle" that is preserved is the cyclic group $\langle \sigma(g) \rangle \leq \mathbb{F}_q^\times$ of order $|G| - 1$, with the element 0 inserted to extend it artificially to a cycle of length $|G|$. In computations, the exceptional elements will be indicated by the parameter z, so that $g * \sigma(g^{z-1}) = 0$ and $g * 0 = \sigma(g^z)$. Thus the action of g on $\mathbb{F}_q^\times$ is described by the cycle

$$\left(\sigma(g), \sigma(g^2), \ldots, \sigma(g^{z-1}), 0, \sigma(g^z), \ldots, \sigma(g^{|G|-1})\right).$$

Note that when σ preserves a long cycle, the preserved subgroup $P^\times(g, \sigma)$ is necessarily trivial.

3.4 Equivalence of Representations

We now prove a very useful result giving a necessary and sufficient condition for two representations to be quasiequivalent. For a given group G, suppose the assignations σ and σ' are either both additive or both multiplicative, and let their corresponding groups of representation polynomials be denoted $\Gamma = \{f_g(X) : g \in G\}$ and $\Gamma' = \{f'_g(X) : g \in G\}$, respectively. Recall from Section 1.3 that Γ and Γ' are *quasiequivalent* if there exist group automorphisms $\psi \colon G \to G$ and $\alpha \colon \mathbb{F}_q^\star \to \mathbb{F}_q^\star$ such that

$$f_g(X) = (\alpha^{-1} \circ f'_{\psi(g)} \circ \alpha)(X)$$

for all $g \in G$; if ψ is the identity then Γ and Γ' are *equivalent*. Note that any $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ is given by a function $\alpha(x) = x^a$ for some $(a, q-1) = 1$, and hence we can naturally consider α to be defined on $\mathbb{F}_q$ by specifying $\alpha(0) = 0$.

Theorem 3.4.1. *Let $\sigma \colon G \hookrightarrow \mathbb{F}_q^\star$ and $\sigma' \colon G \hookrightarrow \mathbb{F}_q^\star$ be two assignations. The representations Γ and Γ' corresponding to σ and σ', respectively, are quasiequivalent if and only if there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$.*

Proof. Suppose Γ and Γ' are equivalent. Then there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $f_g(x) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right)$ for all $g \in G$ and all $x \in \mathbb{F}_q$. In particular, taking $x = \mathrm{id}^\star \in \sigma(G)$, we obtain

$$f_g(x) = f_g(\mathrm{id}^\star) = \sigma\left(g \cdot \sigma^{-1}(\mathrm{id}^\star)\right) = \sigma(g \cdot e) = \sigma(g)$$

on the one hand, and

$$\begin{aligned}
\alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right) &= \alpha^{-1}\left(f'_{\psi(g)}(\alpha(\mathrm{id}^\star))\right) \\
&= \alpha^{-1}\left(f'_{\psi(g)}(\mathrm{id}^\star)\right) \\
&= \alpha^{-1}\left(\sigma'\left(\psi(g) \cdot (\sigma')^{-1}(\mathrm{id}^\star)\right)\right) \\
&= \alpha^{-1}\left(\sigma'(\psi(g) \cdot e)\right) \\
&= \alpha^{-1}\left(\sigma'(\psi(g))\right)
\end{aligned}$$

on the other. Thus, $\sigma(g) = (\alpha^{-1} \circ \sigma' \circ \psi)(g)$ for all $g \in G$, and we see that $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$.

Now suppose that there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ satisfying $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$. If $x \in \sigma(G)$, then for all $g \in G$ we have

$$\begin{aligned}
f_g(x) &= \sigma\left(g \cdot \sigma^{-1}(x)\right) \\
&= \alpha^{-1}\left(\sigma'\left(\psi\left(g \cdot \psi^{-1}\left((\sigma')^{-1}(\alpha(x))\right)\right)\right)\right) \\
&= \alpha^{-1}\left(\sigma'\left(\psi(g) \cdot \psi\left(\psi^{-1}\left((\sigma')^{-1}(\alpha(x))\right)\right)\right)\right) \\
&= \alpha^{-1}\left(\sigma'\left(\psi(g) \cdot (\sigma')^{-1}(\alpha(x))\right)\right) \\
&= \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right).
\end{aligned}$$

Now let $x \in \mathbb{F}_q \setminus \sigma(G)$ so that $f_g(x) = x$. If $\alpha(x) \in \sigma'(G)$, then $\alpha(x) = \sigma'(g)$ for some $g \in G$. Writing $g' = \psi^{-1}(g)$, we have

$$x = \alpha^{-1}\left(\sigma'(g)\right) = \alpha^{-1}\left(\sigma'(\psi(g'))\right) = \sigma(g'),$$

a contradiction. Thus $\alpha(x) \notin \sigma'(G)$ whenever $x \notin \sigma(G)$. Then

$$\alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right) = \alpha^{-1}\left(\alpha(x)\right) = x,$$

and hence $f_g(x) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(x))\right)$ for all $x \notin \sigma(G)$. We conclude that $f_g(X) = \alpha^{-1}\left(f'_{\psi(g)}(\alpha(X))\right)$, so that Γ and Γ' are quasiequivalent. $\square$

For hemimorphisms, we can significantly strengthen the statement of the previous theorem.

Theorem 3.4.2. *Let $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j \rangle$ be a group with two hemimorphisms σ and σ'. The representations Γ and Γ' corresponding to σ and σ', respectively, are quasiequivalent if and only if there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $\sigma(a_i) = \alpha^{-1}(\sigma'(\psi(a_i)))$ for each $1 \leq i \leq k$.*

Proof. If Γ and Γ' are quasiequivalent, then $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$ for some $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ by the previous theorem, so certainly $\sigma(a_i) = \alpha^{-1}(\sigma'(\psi(a_i)))$ for all $1 \leq i \leq k$.

Now suppose there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\star)$ and $\psi \in \mathrm{Aut}(G)$ such that $\sigma(a_i) = \alpha^{-1}(\sigma'(\psi(a_i)))$ for each $1 \leq i \leq k$. By the previous theorem, to prove that Γ and Γ' are quasiequivalent it will suffice to show that $\sigma = \alpha^{-1} \circ \sigma' \circ \psi$, or equivalently, that $\alpha(\sigma(g)) = \sigma'(\psi(g))$ for all $g \in G$. To that end, let $g = \prod_{i=1}^{k} a_i^{\delta_i} \in G$. Then

$$\begin{aligned}
\alpha(\sigma(g)) &= \alpha\left(\sigma\left(\prod_{i=1}^{k} a_i^{\delta_i}\right)\right) \\
&= \alpha\left(\bigstar_{i=1}^{k} \sigma(a_i)\delta_i\right) \\
&= \bigstar_{i=1}^{k} \alpha(\sigma(a_i))\delta_i \\
&= \bigstar_{i=1}^{k} \sigma'(\psi(a_i))\delta_i \\
&= \sigma'\left(\prod_{i=1}^{k} \psi(a_i)^{\delta_i}\right) \\
&= \sigma'\left(\psi\left(\prod_{i=1}^{k} a_i^{\delta_i}\right)\right) \\
&= \sigma'(\psi(g))
\end{aligned}$$

as desired, where the second and fifth lines follow from the fact that σ and σ', respectively, are hemimorphisms. □

We actually know more about additive hemimorphisms, as demonstrated by the next two corollaries. Recall that $\mathbb{F}_q^+$, as an elementary abelian p-group, can be considered as an n-dimension vector space over $\mathbb{F}_p$.

Corollary 3.4.3. *Let $G = \langle a_1, \ldots, a_k \mid R_1, \ldots, R_j \rangle$ be a group with two additive hemimorphisms σ and σ', and suppose $\sigma(G)$ and $\sigma'(G)$ are both k-dimensional vector subspaces of $\mathbb{F}_q$ with bases $\{\sigma(a_1), \ldots, \sigma(a_k)\}$ and $\{\sigma'(a_1), \ldots, \sigma'(a_k)\}$, respectively. Then the representations Γ and Γ' corresponding to σ and σ', respectively, are equivalent.*

Proof. Set $\beta_i = \sigma(a_i)$ and $\beta_i' = \sigma'(a_i)$ and extend $\{\beta_1, \ldots, \beta_k\}$ and $\{\gamma_1, \ldots, \gamma_k\}$ to bases $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$, respectively, of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then there exists a linear transformation $\alpha \in GL(\mathbb{F}_q)$ which maps the first basis to the second one, satisfying the hypotheses of Theorem 3.4.2, and hence the corresponding representations are equivalent. □

Recall from Section 1.2 that we can describe $GL(\mathbb{F}_q)$ by the set of all reduced linearized permutation polynomials.

Corollary 3.4.4. *Let $L(X) \in \mathbb{F}_q[X]$ denote the polynomial representation of the element of $GL(\mathbb{F}_q)$ which corresponds to the change of basis of $\mathbb{F}_q$ from $[\gamma_i]$ to $[\beta_i]$. Then the following formula holds:*

$$f_g^{[\gamma_i]}(X) = L(X)^{[-1]} \circ f_g^{[\beta_i]}(X) \circ L(X);$$

that is, conjugation of the representation polynomial $f_g^{[\beta_i]}(X) \in \mathbb{F}_q[X]/(X^q - X)$ by the linearized polynomial $L(X)$ gives the representation polynomial $f_g^{[\gamma_i]}(X)$.

Proof. This is simply a restatement of Corollary 3.4.3, taking the representations σ and σ' to be defined in terms of the bases $[\gamma_i]$ and $[\beta_i]$, respectively, of $\mathbb{F}_q^+$ over $\mathbb{F}_p$. □

Unlike the additive representation of cyclic groups where all polynomial representations are equivalent (see Chapter 4), in general there are several inequivalent multiplicative representations of cyclic groups among assignations which preserve a

long cycle. Explicitly, consider a cyclic group $G = \langle g \rangle$ with $(|G| - 1) \mid (q - 1)$. Let $z \in \{1, 2, \ldots, |G| - 1\}$ and choose a generator ξ of $\langle \sigma(g) \rangle \leq \mathbb{F}_q^\times$. Define $\sigma \colon G \hookrightarrow \mathbb{F}_q$ by $\sigma(g^d) = \xi^d$ for $z - (|G| - 1) \leq d \leq z - 1$ and $\sigma(g^z) = 0$ so that σ preserves a long cycle and the action of g describes the cycle $(\xi, \xi^2, \ldots, \xi^{z-1}, 0, \xi^z, \ldots, \xi^{|G|-1})$ in $\mathbb{F}_q$. The representation group will be denoted $\Gamma^{[\xi;z]}$ to emphasize the dependence of the representation on both ξ and z. For more detail on the computations in the proof below, see the representations of C_p and C_q in Sections 5.3 and 5.4, respectively.

In what follows, given $\alpha_a \in \mathrm{Aut}(\mathbb{F}_q^\times)$ we will consider $1 \leq a \leq q - 1$ to be the representative of the corresponding residue class modulo $q - 1$, so that the condition $(a, q - 1) = 1$ means that a^{-1} is well-defined as the multiplicative inverse of a in the ring $\mathbb{Z}/(q - 1)\mathbb{Z}$. Similarly, any automorphism of G is of the form $\psi_j(x) = x^j$ for j satisfying $(j, |G|) = 1$, since G is cyclic.

Theorem 3.4.5. *Let G be a cyclic group such that $(|G| - 1)m = q - 1$ for some integer m, and consider assignations that preserve a long cycle, as described above. Then for $a, a' \in \{1, 2, \ldots, q - 1 : (a, q - 1) = 1\}$ and $z, z' \in \{1, 2, \ldots, |G| - 1\}$, the polynomial representations $\Gamma^{[\zeta^{ma};z]}$ and $\Gamma^{[\zeta^{ma'};z']}$ of G are:*

1. *equivalent for $z = z'$ and any a and a';*
2. *quasiequivalent whenever $z' \equiv 1 - z \pmod{|G| - 1}$; or*
3. *not quasiequivalent whenever $z' \not\equiv 1 - z \pmod{|G| - 1}$.*

Proof. We begin by proving the equivalence statement. Let $z \in \{1, 2, \ldots, |G| - 1\}$ and $\alpha_a \in \mathrm{Aut}(\mathbb{F}_q^\times)$, and note that $\alpha_a^{-1} = \alpha_{a^{-1}}$. That $\Gamma^{[\zeta^m;z]}$ and $\Gamma^{[\zeta^{ma};z]}$ are equivalent follows immediately since direct calculation shows

$$f_{g^j}^{[\zeta^m;z]}(x) = f_g^{[\zeta^m;z]}(x)^{[j]} = (\alpha_a^{-1} \circ f_g^{[(\zeta^m)^a;z]} \circ \alpha_a)(x)^{[j]} = (\alpha_a^{-1} \circ f_{g^j}^{[\zeta^{ma};z]} \circ \alpha_a)(x)$$

for each $x \in \mathbb{F}_q$ and each $j \in \{1, 2, \ldots, |G|\}$.

Now let $z, z' \in \{1, 2, \ldots, |G| - 1\}$ and consider two representations of G with distinct parameters z and z'. In light of the equivalence statement just proved, it will suffice to consider representations which both use the fixed parameter $\xi = \zeta^m$. Suppose

the representations $f_g^{[\xi;z]}(X)$ and $f_{g^j}^{[\xi;z']}(X)$ are quasiequivalent so that $f_g^{[\xi;z]}(X) = (\alpha_a^{-1} \circ f_{g^j}^{[\xi;z']} \circ \alpha_a)(X)$ for some $\alpha_a \in \mathrm{Aut}(\mathbb{F}_q^\times)$ and $\psi_j \in \mathrm{Aut}(G)$. We will show that $\Gamma^{[\xi^a;z]}$ and $\Gamma^{[\xi^{a'};z']}$ are quasiequivalent only when $z' \equiv z \pmod{|G|-1}$ by determining several conditions that a and j must satisfy.

First, $f_g^{[\xi;z]}(0) = \xi^z$, and

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}(\alpha_a(0))\right) = \alpha_{a^{-1}}\left(f_{g^j}^{[\xi;z']}(0)\right) = \alpha_{a^{-1}}\left(\xi^{z'+j-1}\right) = \xi^{a^{-1}(z'+j-1)},$$

so we must have $z \equiv a^{-1}(z'+j-1) \pmod{\frac{q-1}{m}}$, or equivalently,

$$z' \equiv az - j + 1 \pmod{\tfrac{q-1}{m}}. \tag{3.1}$$

Next, $f_g^{[\xi;z]}(\xi^{z-1}) = 0$, and

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}\left(\alpha_a(\xi^{a^{-1}(z'-j)})\right)\right) = \alpha_{a^{-1}}\left(f_{g^j}^{[\xi;z']}(\zeta^{z'-j})\right) = \alpha_{a^{-1}}(0) = 0,$$

so we must also have $z - 1 \equiv a^{-1}(z'-j) \pmod{\frac{q-1}{m}}$, or equivalently,

$$z' \equiv az - a + j \pmod{\tfrac{q-1}{m}}. \tag{3.2}$$

Subtracting congruences (3.1) from congruence (3.2) gives the condition

$$a + 1 \equiv 2j \pmod{\tfrac{q-1}{m}}. \tag{3.3}$$

Continuing, $f_g^{[\xi;z]}(1) = \xi$, and

$$f_{g^j}^{[\xi;z']}(1) = \begin{cases} \xi^j, & j \le z'-1, \\ 0, & j = z', \\ \xi^{j-1}, & j \ge z'+1. \end{cases}$$

Since $\alpha_a(1) = 1$, we also have

$$\alpha_a^{-1}\left(f_{g^j}^{[\xi;z']}(\alpha_a(1))\right) = \begin{cases} \xi^{ja^{-1}}, & j \le z'-1, \\ 0, & j = z', \\ \xi^{(j-1)a^{-1}}, & j \ge z'+1. \end{cases}$$

This leads to three cases: $j = z'$, $j \leq z' - 1$, and $j \geq z' + 1$. In the first case, when $j = z'$, we must have $\xi = 0$, which is impossible since $\xi = \zeta^m \in \mathbb{F}_q^\times$.

The second case $j \leq z' - 1$ implies $\xi = \xi^{ja^{-1}}$, or $a \equiv j \pmod{\frac{q-1}{m}}$. Substituting this into congruence (3.3), we obtain $a+1 \equiv 2a \pmod{\frac{q-1}{m}}$, or $a \equiv 1 \pmod{\frac{q-1}{m}}$. Thus $j \equiv 1 \pmod{\frac{q-1}{m}}$ as well, and hence $z \equiv z' \pmod{\frac{q-1}{m}}$ follows from congruence (3.1). But this means $z = z'$, contradicting the assumption that z and z' are distinct.

Finally, when $j \geq z' + 1$, we must have $\xi = \xi^{(j-1)a^{-1}}$, or equivalently, $a \equiv j - 1 \pmod{\frac{q-1}{m}}$. Substituting this expression into congruence (3.3), we obtain the congruence $(j-1) + 1 \equiv 2j \pmod{\frac{q-1}{m}}$, or $j \equiv 0 \pmod{|G| - 1}$. Since $j \in \{1, 2, \ldots, |G|\}$, this means $j = |G| - 1$ and $a \equiv (|G| - 1) - 1 \equiv -1 \pmod{|G| - 1}$. Substituting back into (3.1), we find that $z' \equiv 1 - z \pmod{|G| - 1}$, proving case (2) and completing the proof. $\square$

Chapter 4

EXAMPLES OF ADDITIVE REPRESENTATIONS

Our goal in this chapter is to build an additive representation of direct products of cyclic p-groups. Preliminary results and background will be given in Section 4.1, and we specialize to cyclic p-groups in Section 4.2. We then use our results from the latter section to describe representations of direct products of cyclic p-groups in general. Much more can be said about representations of C_{p^2} in $\mathbb{F}_{p^2}^+$, which we describe in Section 4.3. Since the images of the groups will always be subgroups of $\mathbb{F}_q^+$, all of the representations in this chapter for a given group will be equivalent by Corollary 3.4.3.

4.1 Preliminaries on the Representation of Direct Products of Cyclic p-groups

We begin with a partition of $\mathbb{F}_q = \mathbb{F}_{p^n}$, as follows. Given $N \in \mathbb{N}$ such that $N \leq n$, write $n = \sum_{i=1}^{N} n_i$ where $n_i \geq 1$ for all $1 \leq i \leq N$, and let

$$[\beta] = [\beta_{1,0}, \beta_{1,1}, \ldots, \beta_{1,n_1-1}, \beta_{2,0}, \beta_{2,1}, \ldots, \beta_{2,n_2-1}, \ldots, \beta_{N,0}, \beta_{N,1}, \ldots, \beta_{N,n_N-1}]$$

be a fixed (but arbitrary) basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. We will be interested in representations of the group

$$G = C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_N}} = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_N \rangle,$$

where a general element $g \in G$ has the form $g = g_1^{k_1} g_2^{k_2} \ldots g_N^{k_N}$. Define the assignation $\sigma \colon G \hookrightarrow \mathbb{F}_q^+$ by

$$\sigma(g) = \sigma\left(\prod_{i=1}^{N} g_i^{k_i}\right) = \sum_{i=1}^{N} \sum_{\ell=0}^{n_i-1} \kappa_{i,\ell} \beta_{i,\ell},$$

where $k_i = \sum_{\ell=0}^{n_i-1} \kappa_{i,\ell} p^\ell$ is the p-adic representation of k_i.

Now fix one index $1 \leq i \leq N$ and for simplicity of notation, denote $n' = n_i$, $C_{p^{n'}} = C_{p^{n_i}}$, $k' = k_i$, $\kappa'_\ell = \kappa_{i,\ell}$ and

$$[\beta'] = [\beta_{i,0}, \beta_{i,1}, \ldots, \beta_{i,n_i-1}].$$

Then it is clear that the restriction $\sigma\big|_{C_{p^{n'}}} : C_{p^{n'}} \hookrightarrow \mathbb{F}_q^+$ of σ to $C_{p^{n'}}$ is itself an assignation which fixes every element of $\mathbb{F}_q^+$ outside of the vector subspace of dimension n' generated by $[\beta']$. By abuse of notation, we will denote the $\mathbb{F}_p$-span of $[\beta']$ by $\mathbb{F}^+_{p^{n'}}$, so that $[\beta']$ is a basis of the vector subspace $\mathbb{F}^+_{p^{n'}}$ and $\mathbb{F}^+_{p^{n'}}$ is the image of $C_{p^{n'}}$ under the assignation σ. Thus, to determine the structure of the representation of G in $\mathbb{F}_q^+$, it will suffice to consider the representation of $C_{p^{n'}}$ in $\mathbb{F}_q^+$. (Note that, in general, $\mathbb{F}_{p^{n'}}$ is *not* a subfield of $\mathbb{F}_q$.)

Returning to the assignation σ, it will be convenient to think about $\sigma\big|_{C_{p^{n'}}}$ as follows: we rewrite the exponent k' of an element $g_{n'}^{k'} \in C_{p^{n'}}$ p-adically, and then assign the digit in the ℓ-th position as the coefficient of the ℓ-th element of $[\beta']$. As we will see, the form of the representation polynomial of $g_{n'}^{k'}$ reflects where there are carries in a p-adic sum involving k'. To be precise, we say there is a *carry* at p^j, or in the j-th position, if the coefficient of p^j is augmented by one due to a carry from a lower position. Thus it will be convenient to define the sets

$$\mathcal{F}_j^{[\beta']}(k') = \left\{ \sum_{\ell=0}^{n'-1} \lambda_\ell \beta_\ell \in \mathbb{F}^+_{p^{n'}} : \sum_{\ell=0}^{n'-1} \lambda_\ell p^\ell + \sum_{\ell=0}^{n'-1} \kappa'_\ell p^\ell \text{ has a base-}p \text{ carry at } p^j \right\}$$

for $1 \leq j \leq n' - 1$, which will correspond to where these carries occur. The fact about these sets that will be of greatest importance to us is that their order is always divisible by p.

Lemma 4.1.1. *The set $\mathcal{F}_j^{[\beta']}(k')$ has the following properties:*

1. *If $1 \leq j \leq n' - \log_p(o(g_{n'}^{k'}))$, then $\mathcal{F}_j^{[\beta']}(k') = \emptyset$.*
2. *If $n' - \log_p(o(g_{n'}^{k'})) + 1 \leq j \leq n' - 1$, then $\mathcal{F}_j^{[\beta']}(k')$ has cardinality at least $p^{n'-j}$ and is a disjoint union of affine linear subspaces of $\mathbb{F}^+_{p^{n'}}$, considered as a vector space over $\mathbb{F}_p$.*

In particular, the cardinality of $\mathcal{F}_j^{[\beta']}(k')$ is always divisible by p.

Proof. Let $1 \leq j \leq n'-1$ and $1 \leq k' \leq p^{n'}-1$ be fixed, but arbitrary, and write k' p-adically as $k' = \sum_{\ell=0}^{n'-1} \kappa'_\ell p^\ell$. Define $I(k')$ to be the minimum index ℓ such that $\kappa'_\ell \neq 0$. Note that $o(g_{n'}^{k'}) = p^{n'-I(k')}$ since $k' \neq 0$ by assumption; equivalently, solving for $I(k')$, we have that $I(k') = n' - \log_p(o(g_{n'}^{k'}))$.

If $j \leq I(k)$, then no index less than j produces a carry in the j-th place, and therefore $\mathcal{F}_j^{[\beta_i]}(k) = \emptyset$.

Now suppose that $j > I(k)$, so that there exists at least one $x = \sum_{\ell=0}^{n'-1} \lambda_\ell \beta_\ell \in \mathbb{F}_{p^{n'}}^+$ which produces a carry in the p-adic sum

$$\sum_{\ell=0}^{n'-1} \lambda_\ell p^\ell + \sum_{\ell=0}^{n'-1} \kappa_\ell p^\ell.$$

Without loss of generality, we may assume $x = \sum_{\ell=0}^{j-1} \lambda_\ell \beta_\ell$. Then all of the elements of the set

$$\mathcal{F}(x) = \left\{ \sum_{\ell=0}^{j-1} \lambda_\ell \beta_\ell + \sum_{\ell=j}^{n'-1} \lambda'_\ell \beta_\ell : \lambda'_\ell \in \mathbb{F}_p \right\}$$

also produce a carry, and it is clear that this set is an affine subspace of $\mathbb{F}_{p^{n'}}^+$. Any other element $y = \sum_{\ell=0}^{j-1} \mu_\ell \beta_\ell \in \mathbb{F}_{p^{n'}}^+$, where $\mu_\ell \neq \lambda_\ell$ for some index $0 \leq \ell \leq j-1$, which also produces a carry will yield another affine subspace $\mathcal{F}(y)$ that is disjoint from $\mathcal{F}(x)$. Thus $\mathcal{F}_j^{[\beta']}(k')$ is a disjoint union of the sets $\mathcal{F}(x)$, where x is an element of the set

$$\left\{ \sum_{\ell=0}^{j-1} \lambda_\ell \beta_\ell : \sum_{\ell=0}^{j-1} \lambda_\ell p^\ell + \sum_{\ell=0}^{n'-1} \kappa_\ell p^\ell \text{ has a base-}p \text{ carry at } p^j \right\}.$$

Finally, noting that each set $\mathcal{F}(x)$ has cardinality $p^{n'-j}$ completes the proof. □

We also state and prove one more lemma, which we will use to bound the degree of the representation polynomial $f_{g^{k'}}^{[\beta']}(X)$.

Lemma 4.1.2. *Let $d, m \in \mathbb{N}$ and consider the multinomial coefficient $\binom{d}{d_0, d_1, \ldots, d_m}$, where $d_0, d_1, \ldots, d_m$ are nonnegative integers satisfying the following conditions:*

1. $d = d_0 + d_1 + \cdots + d_m$,

2. $d_i > 0$ *for all* $0 \leq i \leq m-1$, *and*

3. $(p-1) \mid d_i$ *for all* $0 \leq i \leq m-1$.

Then whenever $d < p^m - 1$, *we have*

$$\binom{d}{d_0, d_1, \ldots, d_m} \equiv 0 \pmod{p}.$$

Proof. Suppose $d < p^m - 1$ and let the p-adic expansions of d and d_i be written as $d = \sum_{j=0}^{m-1} \delta_j p^j$ and $d_i = \sum_{j=0}^{m-1} \delta_{i,j} p^j$, respectively. Without loss of generality, we may assume that there are no carries in the p-adic sum $\sum_{i=0}^{m} d_i$, for if there were, then Lemma 1.7.4 already shows that $\binom{d}{d_0, d_1, \ldots, d_m} \equiv 0 \pmod{p}$. Note that

$$\delta_j = \sum_{i=0}^{m} \delta_{i,j}$$

for each $0 \leq j \leq m$ since there are no carries in the sum $d = \sum_{i=0}^{m} d_i$. In what follows, we will ignore the d_m term, so that any reference to the index i is for i restricted to $0 \leq i \leq m-1$.

Now $(p-1) \mid d_i$ implies that

$$0 \equiv \sum_{j=0}^{m-1} \delta_{i,j} p^j \equiv \sum_{j=0}^{m-1} \delta_{i,j} \cdot (1)^j \equiv \sum_{j=0}^{m-1} \delta_{i,j} \pmod{p-1};$$

that is, $p-1$ divides $\sum_{j=0}^{m-1} \delta_{i,j}$ for each i. Since $d_i \neq 0$, we also have

$$\sum_{j=0}^{m-1} \delta_{i,j} \geq p-1.$$

Thus, we obtain the estimate

$$\sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \delta_{i,j} \geq \sum_{i=0}^{m-1} (p-1) = m(p-1).$$

Since $d < p^m - 1$ by assumption, we have

$$d < p^m - 1 = (p-1)(p^{m-1} + \cdots + p + 1) = \sum_{j=0}^{m-1} (p-1) p^j,$$

and hence certainly $\delta_j < p-1$ for some index $0 \leq j \leq m-1$. Then it follows that

$$\sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\delta_{i,j} = \sum_{j=0}^{m-1}\delta_j < m(p-1),$$

which is a contradiction. Therefore $\sum_{i=0}^{m} d_i$ must always have a p-adic carry whenever $d < p^m - 1$, and we conclude from Lemma 1.7.4 that $\binom{d}{d_0,d_1,\ldots,d_m} \equiv 0 \pmod{p}$. □

4.2 Representation of the Cyclic p-Groups

Let us consider representations of C_q in $\mathbb{F}_q^+$, so that the notation of the previous section becomes considerably simpler; this case will easily generalize to representations of $C_{p^{n'}}$ in $\mathbb{F}_q^+$. Let $C_q = \langle g \rangle$ and fix a basis $[\beta_i] = [\beta_0, \beta_1, \ldots, \beta_{n-1}]$ of $\mathbb{F}_q$ over $\mathbb{F}_p$, so that the assignation $\sigma\colon C_q \hookrightarrow \mathbb{F}_q$ is given by

$$\sigma(g^k) = \sigma\left(g^{\sum_{i=0}^{n-1}\kappa_i p^i}\right) = \sum_{i=0}^{n-1}\kappa_i\beta_i.$$

While the above form of assignation will be most useful in the following computations, it will be easier to see that σ is a hemimorphism if we consider a slight variation. To that end, let C_q have the presentation

$$\langle a_1, \ldots, a_n \mid a_i a_j = a_j a_i \text{ for all } i, a_i^p = a_{i+1} \text{ for } i \leq n-1, a_n^p = 1\rangle.$$

By taking $a_i = g^{p^{i-1}}$, we see that this presentation in fact describes C_q. The assignation σ then becomes

$$\sigma(g^k) = \sigma\left(g^{\sum_{i=0}^{n-1}\kappa_i p^i}\right) = \sigma\left(\prod_{i=0}^{n-1}\left(g^{p^i}\right)^{\kappa_i}\right) = \sigma\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right) = \sum_{i=0}^{n-1}\kappa_i\beta_i.$$

Using this second form of the assignation, it is clear that σ is a hemimorphism.

Lemma 4.2.1. *We have $P^+(C_q,\sigma) = \langle a_n\rangle = \langle g^{p^{n-1}}\rangle$, and $P^+(C_q,\sigma)$ is represented by the linear polynomials $X + \kappa_{n-1}\beta_{n-1}$ for $\kappa_{n-1} \in \mathbb{F}_p$.*

Proof. Let $k = \sum_{i=0}^{n-1}\kappa_i p^i \in \{0,1,\ldots,q-1\}$ and let $x = \sum_{i=0}^{n-1}\lambda_i\beta_i \in \mathbb{F}_q$. The elements of $P^+(C_q,\sigma)$ will be precisely those elements $g^k \in C_q$ for which $g^k * x = \sigma(g^k) + x$ for all $x \in \mathbb{F}_q$. Using the above computations, we have

$$g^k * x = \sigma(g \cdot \sigma^{-1}(x))$$

$$= \sigma\left(\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right) \cdot \sigma^{-1}\left(\sum_{i=0}^{n-1} \lambda_i\beta_i\right)\right)$$
$$= \sigma\left(\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right) \cdot \left(\prod_{i=0}^{n-1} a_{i+1}^{\lambda_i}\right)\right),$$

and

$$\begin{aligned}\sigma(g^k) + x &= \left(\sum_{i=0}^{n-1} \kappa_i\beta_i\right) + \left(\sum_{i=0}^{n-1} \lambda_i\beta_i\right) \\ &= \sum_{i=0}^{n-1} (\kappa_i + \lambda_i)\beta_i \\ &= \sigma\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i+\lambda_i}\right).\end{aligned}$$

Thus $g^k * x = \sigma(g^k) + x$ if and only if $\left(\prod_{i=0}^{n-1} a_{i+1}^{\kappa_i}\right) \cdot \left(\prod_{i=0}^{n-1} a_{i+1}^{\lambda_i}\right) = \prod_{i=0}^{n-1} a_{i+1}^{\kappa_i+\lambda_i}$. The latter statement occurs if and only if there are no p-adic carries when adding $\sum_{i=0}^{n-1} \kappa_i p^i$ and $\sum_{i=0}^{n-1} \lambda_i p^i$ for any $x \in \mathbb{F}_q$; that is, when $\kappa_i + \lambda_i \leq p-1$ for all $0 \leq i \leq n-2$ and any choice of λ_i. In particular, we may choose $x = \sum_{i=0}^{n-1}(p-1)\beta_i$, and hence it is clear that we must have $\kappa_i = 0$ for all $0 \leq i \leq n-2$. Therefore,

$$P^+(C_q, \sigma) = \{g^{\kappa_{n-1}p^{n-1}} : \kappa_{n-1} \in \mathbb{F}_p\} = \langle g^{p^{n-1}} \rangle = \langle a_n \rangle,$$

proving the first claim, and by Corollary 3.2.3, we have

$$f^{[\beta_i]}_{g^{\kappa_{n-1}p^{n-1}}}(X) = \sigma(g^{\kappa_{n-1}p^{n-1}}) + X = X + \kappa_{n-1}\beta_{n-1},$$

proving the second. □

Now we determine the polynomial representing an element of C_q. Recall that σ is a hemimorphism, so from Corollary 3.4.3 we know that all polynomial representations from the following theorem are equivalent.

Theorem 4.2.2. *The permutation polynomial representing the action of $g^k \in C_q$ on $\mathbb{F}_q$, where $k = \sum_{i=0}^{n-1} \kappa_i p^i$ is the p-adic expansion of k, is given by*

$$f^{[\beta_i]}_{g^k}(X) = X + \sum_{i=0}^{n-1} \kappa_i\beta_i - \sum_{j=1}^{n-1}\left(\sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} h_{q-2}(x^{-1}X)\right)\beta_j.$$

Proof. For an element $x \in \mathbb{F}_q$, we will write $x = \sum_{i=0}^{n-1} \lambda_i \beta_i$. The action of g^k on x is

$$\begin{aligned} g^k * x &= \sigma\left(g^k \cdot \sigma^{-1}\left(\sum_{i=0}^{n-1} \lambda_i \beta_i\right)\right) \\ &= \sigma\left(g^{\sum_{i=0}^{n-1} \kappa_i p^i} \cdot g^{\sum_{i=0}^{n-1} \lambda_i p^i}\right) \\ &= \sigma\left(g^{\sum_{i=0}^{n-1} (\kappa_i + \lambda_i) p^i}\right) \\ &= \left(\sum_{i=0}^{n-1} (\kappa_i + \lambda_i)\beta_i\right) + \left(\sum_{j \in J(x;k)} \beta_j\right), \end{aligned}$$

where the set $J(x;k)$ is defined to be those indices $1 \leq j \leq n-1$ where there is a carry at p^j in the p-adic sum $\sum_{i=0}^{n-1}(\kappa_i + \lambda_i)p^i$. Thus the second sum in the fourth line is necessary since we read $\sum(\kappa_i + \lambda_i)$ as a p-adic sum (i.e. with carries) in the third line and as a sum of elements of $\mathbb{F}_q$ in the fourth line, and it explicitly accounts for where the p-adic carries are located when adding k and the exponent of $\sigma^{-1}(x)$. Continuing, we can open parentheses in the first sum on the last line to obtain

$$\begin{aligned} g^k * x &= \sum_{i=0}^{n-1} \lambda_i \beta_i + \sum_{i=0}^{n-1} \kappa_i \beta_i + \sum_{j \in J(x;k)} \beta_j \\ &= x + \sum_{i=0}^{n-1} \kappa_i \beta_i + \sum_{j \in J(x;k)} \beta_j. \end{aligned}$$

Interpolating, we obtain

$$\begin{aligned} f_{g^k}^{[\beta_i]}(X) &= \sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right)(g * x) \\ &= \sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right)\left(x + \sum_{i=0}^{n-1} \kappa_i \beta_i + \sum_{x \in \mathbb{F}_q} \sum_{j \in J(x;k)} \beta_j\right) \\ &= \left(\sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right)\left(x + \sum_{i=0}^{n-1} \kappa_i \beta_i\right)\right) \\ &\qquad + \left(\sum_{x \in \mathbb{F}_q} \left(1 - (X - x)^{q-1}\right) \sum_{j \in J(x;k)} \beta_j\right) \\ &= X + \sum_{i=0}^{n-1} \kappa_i \beta_i + \sum_{j=1}^{n-1} \left(\sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} \left(1 - X^{q-1} - h_{q-2}(x^{-1}X)\right)\right) \beta_j \end{aligned}$$

$$= X + \sum_{i=0}^{n-1} \kappa_i \beta_i + (1 - X^{q-1}) \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} \beta_j - \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} h_{q-2}(x^{-1}X),$$

where the inner quantity in the double sum on the penultimate line follows from Corollary 2.2.5 ($0 \notin \mathcal{F}_j^{[\beta_i]}(k)$ for any $1 \leq j \leq n-1$ since adding 0 never produces a carry), and the first double sum in the final line drops out since we are summing β_j a multiple of p times. □

Corollary 4.2.3. *Let $1 \leq \ell \leq q-2$. Then the coefficient of the X^ℓ term of $f_{g^k}^{[\beta_i]}(X)$ is*

$$-\sum_{j=1}^{n-1} \beta_j \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} x^{q-1-\ell}.$$

Proof. Indeed, from the previous theorem it is clear that the X^ℓ term of $f_{g^k}^{[\beta_i]}(X)$ appears inside the double sum as the X^ℓ term of $h_{q-2}(x^{-1}X)$. □

Theorem 4.2.4. *The polynomial $f_{g^k}^{[\beta_i]}(X)$ representing the action of $g^k \in C_q$ on $\mathbb{F}_q^+$ has degree at most $q\left(1 - \frac{p}{o(g^k)}\right) = p^n - \frac{p^{n+1}}{o(g^k)}$ when $o(g^k) > p$.*

Proof. From Theorem 4.2.2, the polynomial representing $f_{g^k}^{[\beta_i]}(X)$ is

$$X + \sum_{i=0}^{n-1} \kappa_i \beta_i - \sum_{j=1}^{n-1} \left(\sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} h_{q-2}(x^{-1}X) \right) \beta_j.$$

Applying Lemma 1.7.6 and simplifying, we obtain

$$\begin{aligned} f_{g^k}^{[\beta_i]}(X) &= X + \sum_{i=0}^{n-1} \kappa_i \beta_i - \sum_{j=1}^{n-1} \left(\sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} \left(-X^{q-1} + (X-x)^{q-1}\right) \right) \beta_j \\ &= X + \sum_{i=0}^{n-1} \kappa_i \beta_i + \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} X^{q-1} \\ &\qquad - \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} \sum_{\ell=0}^{q-1} \binom{q-1}{\ell} X^\ell (-1)^{q-1-\ell} x^{q-1-\ell} \\ &= X + \sum_{i=0}^{n-1} \kappa_i \beta_i + 0 - \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} \sum_{\ell=0}^{q-1} (-1)^\ell X^\ell (-1)^{q-1-\ell} x^{q-1-\ell} \end{aligned} \tag{4.1}$$

$$= X + \sum_{i=0}^{n-1} \kappa_i \beta_i + 0 - \sum_{\ell=0}^{q-1} X^\ell \sum_{j=1}^{n-1} \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} x^{q-1-\ell},$$

where the double sum in line (4.1) equals 0 by Lemma 4.1.1. We will focus our attention on the inner-most sum on the last line:

$$S(j, q-1-\ell) := \sum_{x \in \mathcal{F}_j^{[\beta_i]}(k)} x^{q-1-\ell}.$$

To that end, write $d = q-1-\ell$ for some fixed (but arbitrary) value of ℓ and let m be a fixed (but arbitrary) value of the index j greater than $n - \log_p(o(g^k))$. The latter condition is justified since the sum $S(j,d)$ equals 0 whenever $j \leq n - \log_p(o(g^k))$ by part 1 of Lemma 4.1.1.

For any $x = \sum_{\ell=0}^{n-1} \lambda_\ell \beta_\ell \in \mathcal{F}_m^{[\beta_i]}(k)$, we also have that $\sum_{\ell=0}^{m-1} \mu_\ell \beta_\ell + \sum_{\ell=m}^{n-1} \lambda_\ell \beta_\ell \in \mathcal{F}_m^{[\beta_i]}(k)$ for any $\mu_\ell \in \mathbb{F}_p$ where $0 \leq \ell \leq m-1$. Thus we can decompose the sum $S(m,d)$ into a collection of sums of the form

$$\sum_{\mu_0=0}^{p-1} \cdots \sum_{\mu_{m-1}=0}^{p-1} \left(\sum_{\ell=0}^{m-1} \mu_\ell \beta_\ell + \sum_{\ell=m}^{n-1} \lambda_\ell \beta_\ell \right)^d.$$

Writing d as a sum $d = d_0 + \cdots + d_m$ of $m+1$ nonnegative integers d_ℓ for $0 \leq \ell \leq m$, we may expand the above sum as follows:

$$\sum_{\mu_0=0}^{p-1} \cdots \sum_{\mu_{m-1}=0}^{p-1} \sum_{d=d_0+d_1+\cdots+d_m} \binom{d}{d_0, d_1, \ldots, d_m} \left(\prod_{\ell=0}^{m-1} (\mu_\ell \beta_\ell)^{d_\ell} \right) \left(\sum_{\ell=m}^{n-1} \lambda_\ell \beta_\ell \right)^{d_m}$$
$$= \sum_{d=d_0+d_1+\cdots+d_m} \binom{d}{d_0, d_1, \ldots, d_m} \left(\sum_{\ell=m}^{n-1} \lambda_\ell \beta_\ell \right)^{d_m} \cdot \prod_{\ell=0}^{m-1} \left(\sum_{\mu_\ell=0}^{p-1} \mu_\ell^{d_\ell} \right) \beta_\ell^{d_\ell}.$$

By Lemma 1.7.5, the sum $\sum_{\mu_\ell=0}^{p-1} \mu_\ell^{d_\ell} = 0$ unless $d_\ell > 0$ and $(p-1) \mid d_\ell$, in which case it equals -1. Therefore, we may restrict ourselves to the case where $d_\ell > 0$ and $(p-1) \mid d_\ell$ for all $0 \leq \ell \leq m-1$. Now Lemma 4.1.2 applies, and we have that the multinomial coefficient $\binom{d}{d_0, d_1, \ldots, d_m} = 0$ whenever $d < p^m - 1$. Unpacking this result, we see that the sum $S(m,d)$ is 0 for $d < p^m - 1$, i.e. the coefficient of the X^ℓ term of $f_{g^k}^{[\beta_i]}(X)$ is 0 for $\ell = q-1-d > q-1-(p^m-1) = q-p^m$.

We can now obtain an upper bound on the degree of $f_{g^k}^{[\beta_i]}(X)$ from the smallest possible value of m, or equivalently, of j. By assumption, this value is $m = n - \log_p(o(g^k)) + 1$. Observing that

$$p^m = p^{n-\log_p(o(g^k))+1} = \frac{p^{n+1}}{o(g^k)}$$

completes the proof. □

Corollary 4.2.5. *The polynomial $f_{g^{k'}}^{[\beta']}(X)$ representing the action of $g^{k'} \in C_{p^{n'}}$ on $\mathbb{F}_q^+$ has degree at most $q\left(1 - \frac{p}{o(g^{k'})}\right) = p^n - \frac{p^{n+1}}{o(g^{k'})}$ when $o(g^{k'}) > p$. In particular, the polynomial $f_g^{[\beta]}(X)$ representing the action of $g = g_1^{k_1} g_2^{k_2} \dots g_N^{k_N} \in C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_N}}$ on $\mathbb{F}_q^+$ has degree at most $q\left(1 - \frac{p}{o(g)}\right) = p^n - \frac{p^{n+1}}{o(g)}$ when $o(g) > p$.*

Proof. We will sketch a proof. As in Section 4.1, we will fix an arbitrary index i and use the $'$ symbol to identify elements corresponding to this particular cyclic subgroup and its image in $\mathbb{F}_q^+$. Let m' denote a fixed (but arbitrary) value of the index j greater than $n' - \log_p(o(g_{n'}^{k'}))$.

For any $x = \sum_{\ell=0}^{n'-1} \lambda'_\ell \beta'_\ell \in \mathcal{F}_{m'}^{[\beta']}(k')$, we have that the elements

$$\sum_{n_i \neq n'} \sum_{\ell=0}^{n_i-1} \mu_{i,\ell}\beta_{i,\ell} + \sum_{\ell=0}^{m'-1} \mu'_\ell \beta'_\ell + \sum_{\ell=m'}^{n'-1} \lambda'_\ell \beta_\ell \in \mathbb{F}_q^+$$

also produce a p-adic carry for all $\mu_{i,\ell}, \mu'_\ell \in \mathbb{F}_p$. Decomposing sums of d-th powers of these elements, we obtain multinomial coefficients with $(n - n') + m' + 1$ terms, and hence the multinomial coefficient is zero whenever $d < p^{n-n'+m'} - 1$. When the index i is fixed, the smallest value of m' is $n' - \log_p(o(g_{n'}^{k'})) + 1$, and the degree of $f_{g_{n'}^{k'}}^{[\beta']}(X)$ is at most

$$q - 1 - d = q - p^{n-n'+m'} = q - p^{n+\log_p(o(g_{n'}^{k'}))+1} = q - \frac{p^{n+1}}{o(g_{n'}^{k'})}.$$

Considering all indices i, the greatest upper bound on the degree of $f_g^{[\beta]}(X)$ comes from the smallest value of m_i, or equivalently, from an element $g_{n_i}^{k_i}$ of greatest order. We finish by observing that the order of such an element is the order of g. □

Conjecture 1. *The polynomial $f_g^{[\beta]}(X)$ representing the action of $g = g_1^{k_1} g_2^{k_2} \dots g_N^{k_N} \in C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_N}}$ on $\mathbb{F}_q^+$ has degree equal to $q\left(1 - \frac{p}{o(g)}\right) = p^n - \frac{p^{n+1}}{o(g)}$ when $o(g) > p$.*

4.3 Representation of the Cyclic Group of Order p^2

For C_{p^2}, there is only one carry to keep track of, and hence we can explicitly compute the form of the representation polynomial of any element of C_{p^2}. Since Lemma 4.2.1 gives the form of representation polynomial for elements of the subgroup of C_{p^2} of order p, with the following theorem we have described the entire group $\Gamma^{[\beta_0,\beta_1]}$ of representation polynomials of C_{p^2}.

Theorem 4.3.1. *The representation polynomial of $g^{\kappa_0+\kappa_1 p}$ for $\kappa_0 \neq 0$ is given by*

$$f_{g^{\kappa_0+\kappa_1 p}}^{[\beta_0,\beta_1]}(X) = X + \kappa_0\beta_0 + \kappa_1\beta_1 - \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} h_{p^2-2}\left((\lambda_0\beta_0 + \lambda_1\beta_1)^{-1}X\right).$$

Proof. Let $x = \lambda_0\beta_0 + \lambda_1\beta_1 \in \mathbb{F}_{p^2}$. From Theorem 4.2.2 with $k = \kappa_0 + \kappa_1 p$, it will suffice to show that

$$\sum_{x \in \mathcal{F}_1^{[\beta_0,\beta_1]}(k)} h_{q-2}(x^{-1}X)\beta_1 = \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} h_{p^2-2}\left((\lambda_0\beta_0 + \lambda_1\beta_1)^{-1}X\right).$$

Indeed, $\mathcal{F}_1^{[\beta_0,\beta_1]}(k)$ is the set of elements $x = \lambda_0\beta_0 + \lambda_1\beta_1 \in \mathbb{F}_{p^2}$ such that there is a carry (from the units place to the tens place) when adding $\lambda_0 + \lambda_1 p$ and $\kappa_0 + \kappa_1 p$ p-adically. There is such a carry whenever $\lambda_0 + \kappa_0 \geq p$, that is, for all $\lambda_0 \geq p - \kappa_0$ and for all λ_1. □

Lemma 4.3.2. *The leading term of $f_{g^{\kappa_0+\kappa_1 p}}^{[\beta_0,\beta_1]}(X)$ is $\kappa_0\beta_1^p X^{p^2-p}$ when $\kappa_0 \neq 0$.*

Proof. By Theorem 4.2.4, the degree of $f_{g^{\kappa_0+\kappa_1 p}}^{[\beta_0,\beta_1]}(X)$ is at most

$$p^2 - \frac{p^{2+1}}{o(g^{\kappa_0+\kappa_1 p})} = p^2 - \frac{p^3}{p^2} = p^2 - p.$$

Furthermore, we know that the coefficient of the X^{p^2-p} term of $f_{g^{\kappa_0+\kappa_1 p}}^{[\beta_0,\beta_1]}(X)$ is

$$-\beta_1 \sum_{x \in \mathcal{F}_1^{[\beta_0,\beta_1]}(\kappa_0+\kappa_1 p)} x^{p^2-1-(p^2-p)} = -\beta_1 \sum_{x \in \mathcal{F}_1^{[\beta_0,\beta_1]}(\kappa_0+\kappa_1 p)} x^{p-1}$$

from Lemma 4.2.3. Simplifying, we obtain

$$\begin{aligned}
-\beta_1 \sum_{x \in \mathcal{F}_1^{[\beta_0,\beta_1]}(\kappa_0+\kappa_1 p)} x^{p-1} &= -\beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} (\lambda_0\beta_0 + \lambda_1\beta_1)^{p-1} \\
&= -\beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} \sum_{\ell=0}^{p-1} \binom{p-1}{\ell} (\lambda_0\beta_0)^{\ell} (\lambda_1\beta_1)^{p-1-\ell} \\
&= -\beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\ell=0}^{p-1} (-1)^{\ell} (\lambda_0\beta_0)^{\ell} \beta_1^{p-1-\ell} \sum_{\lambda_1=0}^{p-1} \lambda_1^{p-1-\ell}.
\end{aligned}$$

The inner-most sum on the last line is 0 unless $\ell = 0$ (in which case it equals -1) according to Lemma 1.7.5, hence the coefficient of the X^{p^2-p} term is

$$-\beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} (-1)^0 (\lambda_0\beta_0)^0 \beta_1^{p-1-0}(-1) = \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \beta_1^{p-1} = \kappa_0 \beta_1^p. \qquad \square$$

Corollary 4.3.3. *The polynomials $X \pm X^{p-1} h_{p-1}(X^{p-1})$ are permutation polynomials over $\mathbb{F}_{p^2}$.*

Proof. Recall that the composition of permutation polynomials is again a permutation polynomial. We will establish that

$$f_{g^{(p-1)+\kappa_1 p}}^{[\beta_0,\beta_1]}(X) = X - \beta_0 + \kappa_1\beta_1 - \beta_1(\beta_1^{-1}X)^{p-1} h_{p-1}\big((\beta_1^{-1}X)^{p-1}\big),$$

from which it follows that

$$(X+\beta_0) \circ f_{g^{p-1}}^{[\beta_0,1]}(X) = X - X^{p-1} h_{p-1}(X^{p-1})$$

and

$$(X+\beta_0) \circ f_{g^{p-1}}^{[\beta_0,-1]}(X) = X + X^{p-1} h_{p-1}(X^{p-1})$$

are also permutation polynomials.

By Theorem 4.3.1, the representation polynomial of $g^{(p-1)+\kappa_1 p}$ is

$$\begin{aligned}
f_{g^{(p-1)+\kappa_1 p}}^{[\beta_0,\beta_1]}(X) &= X + (p-1)\beta_0 + \kappa_1\beta_1 - \beta_1 \sum_{\lambda_0=1}^{p-1} \sum_{\lambda_1=0}^{p-1} h_{p^2-2}((\lambda_0\beta_0 + \lambda_1\beta_1)^{-1}X) \\
&= X - \beta_0 + \kappa_1\beta_1
\end{aligned}$$

$$
\begin{aligned}
&\quad - \beta_1 \sum_{\lambda_0=1}^{p-1} \sum_{\lambda_1=0}^{p-1} \left(-X^{p^2-1} + (X - (\lambda_0\beta_0 + \lambda_1\beta_1))^{p^2-1} \right) \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 \sum_{\lambda_0=1}^{p-1} \sum_{\lambda_1=0}^{p-1} X^{p^2-1} \\
&\quad - \beta_1 \sum_{\lambda_0=0}^{p-1} \sum_{\lambda_1=0}^{p-1} (X - (\lambda_0\beta_0 + \lambda_1\beta_1))^{p^2-1} \qquad (4.2) \\
&\quad + \beta_1 \sum_{\lambda_1=0}^{p-1} (X - \lambda_1\beta_1)^{p^2-1} \\
&= X - \beta_0 + \kappa_1\beta_1 + 0 - (-\beta_1) \\
&\quad + \beta_1 \sum_{\lambda_1=0}^{p-1} \sum_{\ell=0}^{p^2-1} \binom{p^2-1}{\ell} X^\ell (-1)^{p^2-1-\ell} (\lambda_1\beta_1)^{p^2-1-\ell} \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 \\
&\quad + \beta_1 \sum_{\ell=0}^{p^2-1} (-1)^\ell X^\ell (-1)^{p^2-1-\ell} \beta_1^{-\ell} \sum_{\lambda_1=0}^{p-1} \lambda_1^{p^2-1-\ell} \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 + \beta_1 \sum_{\substack{0 \le \ell < p^2-1 \\ p-1 \mid \ell}} X^\ell \beta_1^{-\ell} (-1) \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 - \beta_1 \sum_{\ell=0}^{p} (\beta_1^{-1}X)^{(p-1)\ell} \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 - \beta_1(\beta_1^{-1}X)^0 - \beta_1 \sum_{\ell=1}^{p} (\beta_1^{-1}X)^{(p-1)\ell} \\
&= X - \beta_0 + \kappa_1\beta_1 + \beta_1 - \beta_1(1) - \beta_1(\beta_1^{-1}X)^{p-1} \sum_{\ell=0}^{p-1} \left((\beta_1^{-1}X)^{(p-1)} \right)^k \\
&= X - \beta_0 + \kappa_1\beta_1 - \beta_1(\beta_1^{-1}X)^{p-1} h_{p-1}(\beta_1^{-1}X)^{(p-1)}),
\end{aligned}
$$

where the double sum in line (4.2) simplifies according to Lemma 1.7.7. □

We remark that this lemma may be proved directly, independent of the fact that

these polynomials arise as representation polynomials of a particular group. Indeed,

$$x + ax^{p-1}h_{p-1}(x^{p-1}) = \begin{cases} x, & x \in \mathbb{F}_p, \\ x - a, & x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p, \end{cases}$$

which shows that $X + aX^{p-1}h_{p-1}(x^{p-1})$ is a permutation polynomial for any $a \in \mathbb{F}_p$.

Lemma 4.3.4. *The representation polynomial $f_g^{[\beta_0,\beta_1]}(X)$ is conjugate to*

1. *$f_g^{[r\beta_0,r\beta_1]}(X)$ by rX for any $r \in \mathbb{F}_{p^2}^\times$;*
2. *$f_g^{[\beta_0+s\beta_1,\beta_1]}(X)$ by $M_s(X) = \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_1^2X^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - s\beta_1^{p+1})X\right)$ for any $s \in \mathbb{F}_p$;*
3. *$f_g^{[t\beta_0,\beta_1]}(X)$ by $N_t(X) = \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}}\left((t-1)X^p + (\beta_0^{p-1} - t\beta_1^{p-1})X\right)$ for any $t \in \mathbb{F}_p^\times$.*

Proof. It follows from Corollary 3.4.4 that to show

$$L(X)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ L(X) = f_g^{[\gamma_0,\gamma_1]}(X)$$

for a linearized polynomial $L(X)$, it will suffice to verify that $L(\beta_0) = \gamma_0$ and $L(\beta_1) = \gamma_1$. Thus (1) follows immediately. For (2), let $s \in \mathbb{F}_p$. Then

$$\begin{aligned} M_s(\beta_0) &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_1^2\beta_0^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - s\beta_1^{p+1})\beta_0\right) \\ &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_0^p\beta_1^2 + \beta_0^{p+1}\beta_1 - \beta_0^2\beta_1^p - s\beta_0\beta_1^{p+1}\right) \\ &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(\beta_0(\beta_0^p\beta_1 - \beta_0\beta_1^p) + s\beta_1(\beta_0^p\beta_1 - \beta_0\beta_1^p)\right) = \beta_0 + s\beta_1 \end{aligned}$$

and

$$\begin{aligned} M_s(\beta_1) &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_1^2\beta_1^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - s\beta_1^{p+1})\beta_1\right) \\ &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_1^{p+2} + \beta_0^p\beta_1^2 - \beta_0\beta_1^{p+1} - s\beta_1^{p+2}\right) \\ &= \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(\beta_1(\beta_0^p\beta_1 - \beta_0\beta_1^p)\right) = \beta_1, \end{aligned}$$

as desired. Finally, for (3), let $t \in \mathbb{F}_p^\times$. Then

$$N_t(\beta_0) = \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}}\left((t-1)\beta_0^p + (\beta_0^{p-1} - t\beta_1^{p-1})\beta_0\right)$$

$$= \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}} \left((t-1)\beta_0^p + \beta_0^p - t\beta_0\beta_1^{p-1}\right)$$
$$= \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}} \left(t\beta_0(\beta_0^{p-1} - \beta_1^{p-1})\right) = t\beta_0$$

and

$$N_t(\beta_1) = \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}} \left((t-1)\beta_1^p + (\beta_0^{p-1} - t\beta_1^{p-1})\beta_1\right)$$
$$= \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}} \left(t\beta_1^p - \beta_1^p + \beta_0^{p-1}\beta_1 - t\beta_1^p\right)$$
$$= \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}} \left(\beta_1(\beta_0^{p-1} - \beta_1^{p-1})\right) = \beta_1,$$

completing the proof. □

Theorem 4.3.5. *Let $\rho \in \mathbb{F}_{p^2}^\times$ be primitive and let $\psi, \tau \in \mathbb{F}_p$ with τ nonzero. Then the polynomials ρX, $M_\psi(X)$, and $N_\tau(X)$ (as defined in Lemma 4.3.4) generate a group of permutation polynomials isomorphic to $GL(\mathbb{F}_{p^2})$.*

Proof. Recall that the elements of the group $GL(\mathbb{F}_{p^2})$ are precisely the linearized polynomials which produce a change of basis of $f_g^{[\beta_0,\beta_1]}(X)$ upon conjugation. We will show that any change of basis can be accomplished by composition of (conjugations by) ρX, $M_\psi(X)$, and $N_\tau(X)$, demonstrating that they indeed generate a group of polynomials under composition modulo $X^q - X$ which is isomorphic to $GL(\mathbb{F}_{p^2})$.

Let the basis $[\beta_0, \beta_1]$ be fixed and the basis $[\gamma_0, \gamma_1]$ be arbitrary. We first show that there are unique $r \in \mathbb{F}_{p^2}^\times$, $s \in \mathbb{F}_p$, and $t \in \mathbb{F}_p^\times$ for which the basis $[\gamma_0, \gamma_1]$ can be rewritten as $[r(t\beta_0 + s\beta_1), r\beta_1]$. Since we must have $r\beta_1 = \gamma_1$, r is uniquely determined. That there are unique s and t for which $t\beta_0 + s\beta_1 = r^{-1}\gamma_0$ follows at once since the right-hand side may be written as a unique linear $\mathbb{F}_p$-combination of the basis elements β_0 and β_1. Thus the bases $[r(t\beta_0 + s\beta_1), r\beta_1]$ and $[\gamma_0, \gamma_1]$ are the same.

Now write $r = \rho^{\kappa_1}$, $s = \kappa_2\psi$, and $t = \tau^{\kappa_3}$. Then

$$(\rho X)^{[-\kappa_1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ (\rho X)^{[\kappa_1]} = (\rho X)^{[-(\kappa_1-1)]} \circ f_g^{[\rho\beta_0,\rho\beta_1]}(X) \circ (\rho X)^{[\kappa_1-1]},$$

and inductively, we have

$$(\rho X)^{[-\kappa_1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ (\rho X)^{[\kappa_1]} = f_g^{[\rho^{\kappa_1}\beta_0,\rho^{\kappa_1}\beta_1]}(X) = f_g^{[r\beta_0,r\beta_1]}(X).$$

Thus conjugation by $(\rho X)^{[\kappa_1]}$ changes the basis of representation from $[\beta_0, \beta_1]$ to $[r\beta_0, r\beta_1]$. This change of basis is accomplished by a unique (reduced) linearized polynomial, so we conclude that $(\rho X)^{[\kappa_1]} = rX$. It follows similarly that $M_\psi(X)^{[\kappa_2]} = M_s(X)$ and $N_\tau(X)^{[\kappa_3]} = N_t(X)$.

Finally, the computation

$$\begin{aligned}(rX)^{[-1]} \circ M_s(X)^{[-1]} \circ N_t(X)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ N_t(X) \circ M_s(X) \circ (rX) \\ &= (rX)^{[-1]} \circ M_s(X)^{[-1]} \circ f_g^{[t\beta_0,\beta_1]}(X) \circ M_s(X) \circ (rX) \\ &= (rX)^{[-1]} \circ f_g^{[t\beta_0+s\beta_1,\beta_1]}(X) \circ (rX) \\ &= f_g^{[r(t\beta_0+s\beta_1),r(\beta_1)]}(X) \\ &= f_g^{[\gamma_0,\gamma_1]}(X)\end{aligned}$$

shows that conjugation by $L_{r,s,t}(X) = N_t(X) \circ M_s(X) \circ (rX)$ changes the basis of the representation from $[\beta_0, \beta_1]$ to $[r(t\beta_0 + s\beta_1), r\beta_1]$. As r, s, and t vary, the latter basis runs over all bases of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$, and hence the set $\{L_{r,s,t}(X) : r \in \mathbb{F}_{p^2}^\times, s \in \mathbb{F}_p, t \in \mathbb{F}_p^\times\}$ produces all changes of basis of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$; that is, this set is in fact a group isomorphic to $GL(\mathbb{F}_{p^2})$. □

Corollary 4.3.6. *Let $[\beta_0, \beta_1]$ and $[\gamma_0, \gamma_1]$ be two bases of $\mathbb{F}_{p^2}^+$ over $\mathbb{F}_p$. Then there exist unique $r \in \mathbb{F}_{p^2}^\times$, $s \in \mathbb{F}_p$, and $t \in \mathbb{F}_p^\times$ such that*

$$f_g^{[\gamma_0,\gamma_1]}(X) = L(X)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ L(X),$$

where $L(X) = L_{r,s,t}(X) = N_t(X) \circ M_s(rX)$.

Chapter 5

EXAMPLES OF MULTIPLICATIVE REPRESENTATIONS

5.1 Representation of Certain Dihedral Groups

We begin by considering hemimorphism representations of certain dihedral groups. Suppose $q-1=2m$ for some $m \in \mathbb{N}$ and consider the dihedral group of order $2m$ with presentation

$$D_{2m} = \left\langle r, t \mid r^m = t^2 = (rt)^2 = 1 \right\rangle.$$

Let ρ be a generator of $\langle \zeta^2 \rangle$, let τ be a generator of $\langle \zeta \rangle = \mathbb{F}_q^\times$, and define the assignation $\sigma \colon D_{2m} \hookrightarrow \mathbb{F}_q$ by $\sigma(r^k t^\varepsilon) = \rho^k \tau^\varepsilon$ for all $k \in \{0, 1, \ldots, m-1\}$ and all $\varepsilon \in \{0, 1\}$. By construction, σ is a hemimorphism.

Let $x = \rho^\ell \tau^\varepsilon \in \mathbb{F}_q^\times$. Then the action of r^k on x is

$$\begin{aligned} r^k * x &= \sigma\left(r^k \cdot \sigma^{-1}(\rho^\ell \tau^\varepsilon)\right) = \sigma\left(r^k \cdot r^\ell t^\varepsilon\right) = \sigma\left(r^{k+\ell} t^\varepsilon\right) \\ &= \rho^{k+\ell}\tau^\varepsilon = \rho^k \cdot \rho^\ell \tau^\varepsilon = \rho^k x = \sigma(r^k) x, \end{aligned}$$

which shows that $\langle r \rangle \leq P^\times(D_{2m}, \sigma)$. In fact, we have $P^\times(D_{2m}, \sigma) = \langle r \rangle$ since $\langle r \rangle \cong C_m$ is a maximal cyclic subgroup of D_{2m}.

Theorem 5.1.1. *The polynomial representing r^k is*

$$f_{r^k}^{[\rho,\tau]}(X) = \rho^k X,$$

and the polynomial representing t is

$$f_t^{[\rho,\tau]} = \tau X^{q-2}.$$

Proof. By Corollary 3.2.3, it is clear that $f_{r^k}^{[\rho,\tau]}(X) = \sigma(r^k)X = \rho^k X$.

Note that $t^{\varepsilon} = t^{-\varepsilon}$, so that the action of t on $x = \rho^{\ell}\tau^{\varepsilon}$ is

$$t * x = \sigma\left(t \cdot \sigma^{-1}(\rho^{\ell}\tau^{\varepsilon})\right) = \sigma\left(t \cdot r^{\ell}t^{\varepsilon}\right) = \sigma\left(r^{-\ell}t \cdot t^{-\varepsilon}\right) = \sigma\left(r^{-\ell}t^{1-\varepsilon}\right) = \rho^{-\ell}\tau^{1-\varepsilon}.$$

We interpolate to obtain

$$\begin{aligned}
f_t^{[\rho,\tau]}(X) &= \sum_{x\in\mathbb{F}_q^{\times}} \left(1-(X-x)^{q-1}\right)(t*x) \\
&= \sum_{\ell=0}^{m-1}\Big(\left(1-(X-\rho^{\ell})^{q-1}\right)(\rho^{-\ell}\tau) + \left(1-(X-\rho^{\ell}\tau)^{q-1}\right)(\rho^{-\ell})\Big) \\
&= \sum_{\ell=0}^{m-1}\Big(\left(1-X^{q-1}-h_{q-2}\left((\rho^{\ell})^{-1}X\right)\right)\rho^{-\ell}\tau + \left(1-X^{q-1}-h_{q-2}\left((\rho^{\ell}\tau)^{-1}X\right)\right)\rho^{-\ell}\Big) \\
&= \left(\sum_{\ell=0}^{m-1}(1-X^{q-1})(\rho^{-\ell}+\rho^{-\ell}\tau)\right) - \left(\sum_{\ell=0}^{m-1}\rho^{-\ell}\Big(\tau h_{q-2}(\rho^{-\ell}X) + h_{q-2}(\rho^{-\ell}\tau^{-1}X)\Big)\right) \\
&= \left((1-X^{q-1})\sum_{x\in\mathbb{F}_q^{\times}} x\right) - \left(\sum_{\ell=0}^{m-1}\rho^{-\ell}\sum_{k=0}^{q-2}\Big(\tau(\rho^{-\ell})^k + (\rho^{-\ell}\tau^{-1})^k\Big)X^k\right) \\
&= 0 - \sum_{\ell=0}^{m-1}\rho^{-\ell}\sum_{k=0}^{q-2}\rho^{-\ell k}(\tau+\tau^{-k})X^k \\
&= -\sum_{k=0}^{q-2}(\tau+\tau^{-k})X^k\sum_{\ell=0}^{m-1}\rho^{-\ell(k+1)},
\end{aligned}$$

where the third line follows from Lemma 1.7.6. The innermost sum on the last line simplifies to

$$\sum_{\ell=0}^{m-1}\left(\rho^{-(k+1)}\right)^{\ell} = \begin{cases} m, & \rho^{-(k+1)} = 1, \\ 0, & \rho^{-(k+1)} \neq 1, \end{cases}$$

by Lemma 1.7.7. Since $o(\rho) = m$, we have $\rho^{-(k+1)} = 1$ when $m \mid (k+1)$, and hence either $k = m-1$ or $k = 2m-1$ as $0 \leq k \leq q-2 = 2m-1$.

It will be helpful at this point to perform several auxiliary computations. Since $2m = q-1$, we have that $\tau^{-m} = \tau^{m}$. Thus $o(\tau^{m}) = 2$ shows that τ^{m} is the unique element of $\mathbb{F}_q^{\times}$ of order 2, that is, $\tau^{-m} = -1$. Additionally, $\tau^{-2m} = (\tau^{-1})^{q-1} = 1$.

Continuing the computation of $f_t^{[\rho,\tau]}(X)$, we have

$$f_t^{[\rho,\tau]}(X) = -\sum_{k=0}^{q-2}(\tau+\tau^{-k})X^k\sum_{\ell=0}^{m-1}\rho^{-\ell(k+1)}$$

$$
\begin{aligned}
&= -m(\tau + \tau^{1-m})X^{m-1} - m(\tau + \tau^{1-2m})X^{2m-1} \\
&= -m\tau\Big((1 + \tau^{-m})X^{m-1} + (1 + \tau^{-2m})X^{2m-1}\Big) \\
&= -m\tau\Big((1 + (-1))X^{m-1} + (1 + 1)X^{2m-1}\Big) \\
&= -2m\tau X^{2m-1}.
\end{aligned}
$$

Since $2m = q - 1 \equiv -1 \pmod{p}$, we conclude that $f_t^{[\rho,\tau]}(X) = \tau X^{q-2}$. □

Corollary 5.1.2. *The polynomial representing $r^k t^\varepsilon \in D_{2m}$ is*

$$
f_{r^k t^\varepsilon}^{[\rho,\tau]}(X) = \begin{cases} \rho^k X, & \text{when } \varepsilon = 0, \\ \rho^k \tau X^{q-2}, & \text{when } \varepsilon = 1. \end{cases}
$$

Proof. Noting that $f_{r^k t^\varepsilon}^{[\rho,\tau]}(X) = f_{r^k}^{[\rho,\tau]}(f_{t^\varepsilon}^{[\rho,\tau]}(X))$ by Lemma 3.1.2, the result follows immediately from the previous theorem. □

Theorem 5.1.3. *Any two hemimorphisms representing D_{2m} are quasiequivalent. If we let σ and σ' be two such hemimorphisms with parameters ρ, τ and ρ', τ', respectively, then writing $\rho = \tau^d$ and $\rho' = (\tau')^{d'}$, we have that σ and σ' are equivalent if and only if $d = d'$.*

Proof. Without loss of generality, we may fix the assignation σ to be

$$
\sigma(r) = \rho = \zeta^2, \quad \sigma(t) = \tau = \zeta.
$$

Now let σ' be defined by

$$
\sigma'(r) = \rho' = (\zeta^y)^2, \quad \sigma'(t) = \tau' = \zeta^z
$$

for some $(y, 2m) = (z, 2m) = 1$ (so that ζ^y and ζ^z are generators of $\mathbb{F}_q^\times$). By Theorem 3.4.2, to prove that σ and σ' are quasiequivalent, it will suffice to show that there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ and $\psi \in \mathrm{Aut}(D_{2m})$ such that

$$
\sigma(r) = \alpha^{-1}\left(\sigma'(\psi(r))\right), \quad \sigma(t) = \alpha^{-1}\left(\sigma'(\psi(t))\right).
$$

To this end, define the number s to be the least positive integer satisfying $s \equiv y^{-1}z \pmod{2m}$; we know that y is invertible modulo $2m$ since $(y, 2m) = 1$. Note that s is also invertible modulo $2m$, since y and z are, and hence that s is odd. We claim that the functions α and ψ defined by $\alpha(x) = x^z$ and $\psi(x) = x^s$, respectively, satisfy the above equations.

First, we verify that α and ψ are automorphisms of the appropriate groups. That $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ is clear since $(z, 2m) = (z, q-1) = 1$. Thus if we can show that $\psi(r)$ and $\psi(t)$ satisfy the same relations as r and t, respectively, then $\psi(r)$ and $\psi(t)$ will be generators for a group isomorphic to D_{2m}; that is, ψ will be an automorphism of D_{2m}.

Since s is invertible modulo $2m$, it is also invertible modulo m. Hence $\psi(r) = r^s$ is also a generator of $\langle r \rangle$, and so has order m. Moreover, $\psi(t)$ has order two since $\psi(t) = t^s = t$ as s is odd. Finally,

$$\psi(r)\psi(t)\psi(r)\psi(t) = r^s t^s r^s t^s = r^s(tr^s t) = r^s(r^{-s}) = 1$$

shows that $\psi(t)$ and $\psi(r)$ satisfy all the necessary relations, so $\psi \in \mathrm{Aut}(D_{2m})$.

Now it remains to verify that the conditions of Theorem 3.4.2 are satisfied. Note that

$$ysz^{-1} \equiv y(y^{-1}z)z^{-1} \equiv 1 \pmod{2m}$$

and $\alpha^{-1}(x) = \alpha(x)^{[-1]} = x^{z^{-1}}$. Then

$$\alpha^{-1}\left(\sigma'(\psi(r))\right) = \alpha^{-1}\left(\sigma'(r^s)\right) = \left((\zeta^{2y})^s\right)^{z^{-1}} = \zeta^2 = \sigma(r)$$

and

$$\alpha^{-1}\left(\sigma'(\psi(t))\right) = \alpha^{-1}\left(\sigma'(t)\right) = (\zeta^z)^{z^{-1}} = \zeta = \sigma(t),$$

as desired.

For the assignations σ and σ' to be equivalent, we require that we can choose ψ to be the identity, that is, $s = 1$. Consider the more general case where σ is defined by

$$\sigma(r) = \rho = \tau^d, \quad \sigma(t) = \tau,$$

and σ' is defined by

$$\sigma'(r) = \rho' = (\tau')^{d'} = \tau^{zd'}, \quad \sigma'(t) = \tau' = \tau^z.$$

Let $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ be defined by $\alpha(x) = x^a$. In order to satisfy the conditions of Theorem 3.4.2, we require that

$$\tau = \sigma(t) = \alpha^{-1}\left(\sigma'(t)\right) = \alpha^{-1}\left(\tau^z\right) = \tau^{za^{-1}},$$

which shows that we must have $a \equiv z \pmod{2m}$. Thus $\alpha(x) = x^z$, and indeed $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ since $(z, 2m) = 1$. Furthermore, the theorem also requires that

$$\tau^d = \sigma(r) = \alpha^{-1}\left(\sigma'(r)\right) = \alpha^{-1}\left(\tau^{zd'}\right) = \tau^{zd'z^{-1}} = \tau^{d'}.$$

Therefore σ and σ' define equivalent representations if and only if $d = d'$. □

5.2 Representation of Certain Hamiltonian Groups

Hamiltonian groups are defined to be those nonabelian groups in which every subgroup is normal. A finite Hamiltonian group must be isomorphic to a direct product of a quaternion group of order 8, an elementary abelian 2-group, and an abelian group of odd order; see pages 143–145 of Robinson [21] for a proof. We will not consider the representation of Hamiltonian groups generally, but rather those of the following type.

Suppose $q - 1 = 8m$ for some odd $m \in \mathbb{N}$ and let H_{8m} be the Hamiltonian group of order $8m$ which is a direct product of the quaternion group and a cyclic group of odd order with presentation

$$H_{8m} = Q \times O = \left\langle i, j \mid i^2 = j^2 = (ij)^2 = -1 \right\rangle \times \left\langle g \mid g^m = 1 \right\rangle.$$

Let ρ be a generator of $\langle \zeta^2 \rangle$, let τ be a generator of $\langle \zeta \rangle$, and define the assignation $\sigma\colon H_{8m} \hookrightarrow \mathbb{F}_q$ by $\sigma(i^\delta j^\varepsilon g^k) = \rho^{m\delta+4k}\tau^\varepsilon$ for all $\delta \in \{0,1,2,3\}$, all $\varepsilon \in \{0,1\}$, and all $k \in \{0, 1, \ldots, m-1\}$. By construction, σ is a hemimorphism.

Let $x = \rho^{m\gamma+4\ell}\tau^\varepsilon \in \mathbb{F}_q^\times$. Then the action of $i^\delta g^k$ on x is

$$i^\delta g^k * x = \sigma\left(i^\delta g^k \cdot \sigma^{-1}(\rho^{m\gamma+4\ell}\tau^\varepsilon)\right) = \sigma\left(i^\delta g^k \cdot i^\gamma j^\varepsilon g^\ell\right) = \sigma\left(i^{\delta+\gamma} j^\varepsilon g^{k+\ell}\right)$$

$$= \rho^{m(\delta+\gamma)+4(k+\ell)}\tau^{\varepsilon} = \rho^{m\delta+4k} \cdot \rho^{m\gamma+4\ell}\tau^{\varepsilon} = \rho^{m\delta+4k}x = \sigma(i^{\delta}g^{k})x,$$

which shows that $\langle i, g\rangle \leq P^{\times}(H_{8m}, \sigma)$. In fact, we have $P^{\times}(H_{8m}, \sigma) = \langle i, g\rangle$ since $\langle i, g\rangle \cong C_{4m}$ is a maximal cyclic subgroup of H_{8m}.

Theorem 5.2.1. *The polynomial representing $i^{\delta}g^{k}$ is*

$$f_{i^{\delta}g^{k}}^{[\rho,\tau]}(X) = \rho^{m\delta+4k}X,$$

and the polynomial representing j is

$$f_{j}^{[\rho,\tau]}(X) = 2^{-1}\tau\Big((1-\tau^{-2-2m})X^{2m+1} + (1+\tau^{-2-2m})X^{6m+1}\Big).$$

Proof. By Corollary 3.2.3, it is clear that $f_{i^{\delta}g^{k}}^{[\rho,\tau]}(X) = \sigma(i^{\delta}g^{k})X = \rho^{m\delta+4k}X$.

The action of j on $x = \rho^{m\gamma+4\ell}\tau^{\varepsilon}$ is

$$\begin{aligned} j * \rho^{m\gamma+4\ell}\tau^{\varepsilon} &= \sigma\left(j \cdot \sigma^{-1}(\rho^{m\gamma+4\ell}\tau^{\varepsilon})\right) = \sigma\left(j \cdot i^{\gamma}j^{\varepsilon}g^{\ell}\right) \\ &= \begin{cases} \sigma\left(i^{-\gamma}jg^{\ell}\right), & \varepsilon = 0, \\ \sigma\left(i^{2-\gamma}g^{\ell}\right), & \varepsilon = 1, \end{cases} \\ &= \begin{cases} \rho^{-m\gamma+4\ell}\tau, & \varepsilon = 0, \\ \rho^{m(2-\gamma)+4\ell}, & \varepsilon = 1. \end{cases} \end{aligned}$$

Interpolating, we obtain

$$\begin{aligned} f_{j}^{[\rho,\tau]}(X) &= \sum_{x\in\mathbb{F}_q^{\times}} \left(1-(X-x)^{q-1}\right)(j*x) \\ &= \left(\sum_{\ell=0}^{m-1}\sum_{\gamma=0}^{3}\left(1-(X-\rho^{m\gamma+4\ell})^{q-1}\right)(\rho^{-m\gamma+4\ell}\tau)\right) \\ &\qquad + \left(\sum_{\ell=0}^{m-1}\sum_{\gamma=0}^{3}\left(1-(X-\rho^{m\gamma+4\ell}\tau)^{q-1}\right)(\rho^{m(2-\gamma)+4\ell})\right) \\ &= \left(\sum_{\ell=0}^{m-1}\sum_{\gamma=0}^{3}\left(1-X^{q-1}-h_{q-2}(\rho^{-m\gamma-4\ell}X)\right)(\rho^{-m\gamma+4\ell}\tau)\right) \\ &\qquad + \left(\sum_{\ell=0}^{m-1}\sum_{\gamma=0}^{3}\left(1-X^{q-1}-h_{q-2}(\rho^{-m\gamma-4\ell}\tau^{-1}X)\right)(\rho^{m(2-\gamma)+4\ell})\right) \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{\ell=0}^{m-1} \sum_{\gamma=0}^{3} (1 - X^{q-1})(\rho^{-m\gamma+4\ell}\tau + \rho^{m(2-\gamma)+4\ell}) \right) \\
&\qquad - \left(\sum_{\ell=0}^{m-1} \sum_{\gamma=0}^{3} \rho^{-m\gamma+4\ell} \Big(\tau h_{q-2}(\rho^{-m\gamma-4\ell}X) + \rho^{2m} h_{q-2}(\rho^{-m\gamma-4\ell}\tau^{-1}X) \Big) \right) \\
&= \left((1 - X^{q-1}) \sum_{x \in \mathbb{F}_q^\times} x \right) \\
&\qquad - \left(\sum_{\ell=0}^{m-1} \sum_{\gamma=0}^{3} \rho^{-m\gamma+4\ell} \sum_{k=0}^{q-2} \Big(\tau(\rho^{-m\gamma-4\ell})^k + \rho^{2m}(\rho^{-m\gamma-4\ell}\tau^{-1})^k \Big) X^k \right) \\
&= 0 - \sum_{\ell=0}^{m-1} \sum_{\gamma=0}^{3} \rho^{-m\gamma+4\ell} \sum_{k=0}^{q-2} (\rho^{-m\gamma-4\ell})^k \Big(\tau + \rho^{2m}\tau^{-k} \Big) X^k \\
&= -\sum_{k=0}^{q-2} (\tau + \rho^{2m}\tau^{-k}) X^k \sum_{\ell=0}^{m-1} \rho^{-4\ell(k-1)} \sum_{\gamma=0}^{3} \rho^{-m\gamma(k+1)},
\end{aligned}
$$

where the third line follows from Lemma 1.7.6. The inner two sums on the last line simplify to

$$
\sum_{\ell=0}^{m-1} \left(\rho^{-4(k-1)}\right)^{\ell} = \begin{cases} m, & \rho^{-4(k-1)} = 1, \\ 0, & \rho^{-4(k-1)} \neq 1, \end{cases}
$$

and

$$
\sum_{\gamma=0}^{3} \left(\rho^{-m(k+1)}\right)^{\gamma} = \begin{cases} 4, & \rho^{-m(k+1)} = 1, \\ 0, & \rho^{-m(k+1)} \neq 1, \end{cases}
$$

by Lemma 1.7.7.

Since $o(\rho) = 4m$, we have $\rho^{-4(k-1)} = 1$ when $4m \mid 4(k-1)$, or equivalently, when $m \mid (k-1)$. Similarly, $\rho^{-m(k+1)} = 1$ when $4m \mid m(k+1)$, or when $4 \mid (k+1)$. Thus $k \equiv 1 \pmod{m}$ and $k \equiv -1 \equiv 3 \pmod{4}$, and since m is odd by definition, it is easily verified that $k \equiv 2m + 1 \pmod{4m}$.

It will be helpful at this point to perform several auxiliary computations. Since $o(\rho) = 4m$, we have that $o(\rho^{2m}) = 2$, so that ρ^{2m} is the unique element of $\mathbb{F}_q^\times$ of order 2. Thus $\rho^{2m} = -1$. Similarly, $\tau^{-4m} = \tau^{4m} = -1$ since $o(\tau) = 8m$. Moreover, $8m = q - 1$ implies $4m = 2^{-1}(q-1) = -2^{-1}$ in $\mathbb{F}_q$.

Continuing the computation of $f_j^{[\rho,\tau]}(X)$, we have

$$\begin{aligned} f_j^{[\rho,\tau]}(X) &= -\sum_{k=0}^{q-2}(\tau+\rho^{2m}\tau^{-k})X^k\sum_{\ell=0}^{m-1}\rho^{-4\ell(k-1)}\sum_{\gamma=0}^{3}\rho^{-m\gamma(k+1)} \\ &= -(\tau-\tau^{-(2m+1)})X^{2m+1}\cdot 4m-(\tau-\tau^{-(6m+1)})X^{6m+1}\cdot 4m \\ &= -4m\tau\Big((1-\tau^{-2-2m})X^{2m+1}+(1-\tau^{-2-6m})X^{6m+1}\Big) \\ &= 2^{-1}\tau\Big((1-\tau^{-2-2m})X^{2m+1}+(1+\tau^{-2-2m})X^{6m+1}\Big). \end{aligned}$$

□

Corollary 5.2.2. *The polynomial representing $i^\delta j^\varepsilon g^k \in H_{8m}$ is*

$$f_{i^\delta j^\varepsilon g^k}^{[\rho,\tau]}(X) = \begin{cases} \rho^{m\delta+4k}X, & \text{when } \varepsilon=0, \\ 2^{-1}\rho^{m\delta+4k}\tau\Big((1-\tau^{-2-2m})X^{2m+1}+(1+\tau^{-2-2m})X^{6m+1}\Big), & \text{when } \varepsilon=1. \end{cases}$$

Proof. Noting that $f_{i^\delta j^\varepsilon g^k}^{[\rho,\tau]}(X) = f_{i^\delta g^k j^\varepsilon}^{[\rho,\tau]}(X) = f_{i^\delta g^k}^{[\rho,\tau]}(f_{j^\varepsilon}^{[\rho,\tau]}(X))$ by Lemma 3.1.2, the result follows immediately from the previous theorem. □

Theorem 5.2.3. *Any two hemimorphisms representing H_{8m} are quasiequivalent. If we let σ and σ' be two such hemimorphisms with parameters ρ, τ and ρ', τ', respectively, then writing $\rho=\tau^d$ and $\rho'=(\tau')^{d'}$, we have that σ and σ' are equivalent if and only if $d \equiv d' \pmod{4m}$.*

Proof. Without loss of generality, we may fix the assignation σ to be

$$\sigma(i)=\rho^m=\zeta^{2m}, \quad \sigma(j)=\tau=\zeta, \quad \sigma(g)=\rho^4=\zeta^8.$$

Now let σ' be defined by

$$\sigma'(i)=(\rho')^m=(\zeta^y)^{2m}, \quad \sigma'(j)=\tau'=\zeta^z, \quad \sigma'(g)=(\rho')^4=(\zeta^y)^8$$

for some $(y,8m)=(z,8m)=1$ (so that ζ^y and ζ^z are generators of $\mathbb{F}_q^\times$). By Theorem 3.4.2, to prove that σ and σ' are quasiequivalent, it will suffice to show that there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ and $\psi \in \mathrm{Aut}(D_{2m})$ such that

$$\sigma(i)=\alpha^{-1}\left(\sigma'(\psi(i))\right), \quad \sigma(j)=\alpha^{-1}\left(\sigma'(\psi(j))\right), \quad \sigma(g)=\alpha^{-1}\left(\sigma'(\psi(g))\right).$$

We claim that the functions α and ψ, defined as follows, satisfy the above equations. Define the function α by $\alpha(x) = x^z$. Let s be the least positive integer satisfying $s \equiv y^{-1}z \pmod{8m}$; we know that y is invertible modulo $8m$ since $(y, 8m) = 1$. Now let ψ to be the homomorphism defined by $\psi(i) = i^s$, $\psi(j) = j$, and $\psi(g) = g^s$.

First, we verify that α and ψ are automorphisms of the appropriate structures. That $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ is clear since $(z, 8m) = (z, q-1) = 1$. Note that s is invertible modulo $8m$ since $(y, 8m) = (z, 8m) = 1$. Thus, in particular, s is invertible modulo m and modulo 4, and hence $\psi(i)$ and $\psi(g)$ are generators of $\langle i \rangle$ and $\langle g \rangle = O$, respectively. Certainly ψ induces an automorphism of O, and moreover, ψ also induces an automorphism of Q since $\mathrm{Aut}(Q) \cong S_4$, and hence there exists an automorphism of Q which maps i to $i^s = i^{\pm 1}$ and fixes j. Therefore $\psi \in \mathrm{Aut}(H_{8m})$.

It remains to verify that the conditions of Theorem 3.4.2 are satisfied. Note that

$$ysz^{-1} \equiv y(y^{-1}z)z^{-1} \equiv 1 \pmod{8m}$$

and $\alpha^{-1}(x) = \alpha(x)^{[-1]} = x^{z^{-1}}$. Then

$$\alpha^{-1}\left(\sigma'(\psi(i))\right) = \alpha^{-1}\left(\sigma'(i^s)\right) = \left((\zeta^{2my})^s\right)^{z^{-1}} = \zeta^{2m} = \sigma(i),$$

$$\alpha^{-1}\left(\sigma'(\psi(j))\right) = \alpha^{-1}\left(\sigma'(j)\right) = (\zeta^z)^{z^{-1}} = \zeta = \sigma(j),$$

and

$$\alpha^{-1}\left(\sigma'(\psi(g))\right) = \alpha^{-1}\left(\sigma'(g^s)\right) = \left((\zeta^{8y})^s\right)^{z^{-1}} = \zeta^8 = \sigma(g),$$

as desired.

For the assignations σ and σ' to be equivalent, we require that we can choose ψ to be the identity, that is, $s = 1$. Consider the more general case where σ is defined by

$$\sigma(i) = \rho^m = \tau^{md}, \quad \sigma(j) = \tau, \quad \sigma(g) = \rho^4 = z^{4d},$$

and σ' is defined by

$$\sigma'(i) = (\rho')^m = \left((\tau')^{d'}\right)^m = \tau^{md'z}, \quad \sigma'(j) = \tau' = \tau^z, \quad \sigma(g) = (\rho')^4 = \left((\tau')^{d'}\right) = \tau^{4d'z}.$$

Let $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ be defined by $\alpha(x) = x^a$. In order to satisfy the conditions of Theorem 3.4.2, we require that

$$\tau = \sigma(t) = \alpha^{-1}\left(\sigma'(t)\right) = \alpha^{-1}\left(\tau^z\right) = \tau^{za^{-1}},$$

which shows that we must have $a \equiv z \pmod{8m}$. Thus $\alpha(x) = x^z$, and indeed $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ since $(z, 8m) = 1$. Furthermore, the theorem also requires that

$$\tau^{md} = \sigma(i) = \alpha^{-1}\left(\sigma'(i)\right) = \alpha^{-1}\left(\tau^{md'z}\right) = \tau^{md'zz^{-1}} = \tau^{md'}$$

and

$$\tau^{4d} = \sigma(g) = \alpha^{-1}\left(\sigma'(g)\right) = \alpha^{-1}\left(\tau^{4d'z}\right) = \tau^{4d'zz^{-1}} = \tau^{4d'}.$$

From the first equation, we have $md \equiv md' \pmod 4$, and hence $d \equiv d' \pmod 4$ (since m is odd); similarly, we have $d \equiv d' \pmod m$ since the second equation implies $4d \equiv 4d' \pmod m$. Thus we conclude that σ and σ' define equivalent representations if and only if $d \equiv d' \pmod{4m}$. □

5.3 Representation of the Cyclic Group of Order p

We now consider representations of the cyclic group C_p in $\mathbb{F}_q^\times$ that preserve a long cycle. Let $C_p = \langle g \rangle$ and choose $z \in \{1, 2, \ldots, p-1\}$. Writing $\xi = \zeta^{\frac{q-1}{p-1}}$, define $\sigma\colon C_p \hookrightarrow \mathbb{F}_q$ by

$$\sigma(g^k) = \begin{cases} \xi^k, & 1 \le k \le z-1, \\ 0, & k = z, \\ \xi^{k-1}, & z+1 \le k \le p, \end{cases}$$

so that the action of g describes the cycle $(\xi, \xi^2, \ldots, \xi^{z-1}, 0, \xi^z, \ldots, \xi^{p-1})$ in $\mathbb{F}_q$. Theorem 3.4.5 shows that all representations of C_p preserving a long cycle with a fixed value of the parameter z are equivalent, while those with differing values of z are quasiequivalent if those z-values sum to 1 modulo $p-1$ and not quasiequivalent otherwise.

Theorem 5.3.1. *Let $z \in \{1, 2, \ldots, p-1\}$ and define $\xi = \zeta^{\frac{q-1}{p-1}}$. Then the polynomial representing the generator g of C_p in $\mathbb{F}_q^\times$ is*

$$f_g^{[\xi;z]}(X) = X + (\xi - 1)Xh_{\lfloor \frac{q-2}{p-1} \rfloor}(X^{p-1}) + \xi^z h_{q-2}(\xi^{1-z}X).$$

Proof. The action of g on $x \in \mathbb{F}_q$ is

$$g * x = \begin{cases} x, & x \notin \langle \xi \rangle \cup \{0\}, \\ 0, & x = \xi^{z-1}, \\ \xi^z, & x = 0, \\ \xi x, & x \in \langle \xi \rangle \setminus \{\xi^{z-1}\}. \end{cases}$$

Interpolating, we obtain

$$\begin{aligned}
f_g^{[\xi;z]}(X) &= \sum_{x \in \mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)(g * x) \\
&= \left(\sum_{x \in \mathbb{F}_q^\times \setminus \langle \xi \rangle} \left(1 - (X-x)^{q-1}\right)(x) \right) + \left(1 - (X - \xi^{z-1})^{q-1}\right)(0) \\
&\qquad + \left(1 - (X-0)^{q-1}\right)(\xi^z) + \left(\sum_{x \in \langle \xi \rangle \setminus \{\xi^{z-1}\}} \left(1 - (X-x)^{q-1}\right)(\xi x) \right) \\
&= \left(\sum_{x \in \mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)(x) \right) - \left(\sum_{x \in \langle \xi \rangle} \left(1 - (X-x)^{q-1}\right)(x) \right) \\
&\qquad + (1 - X^{q-1})(\xi^z) + \left(\sum_{x \in \langle \xi \rangle} \left(1 - (X-x)^{q-1}\right)(\xi x) \right) \\
&\qquad - \left(1 - (X - \xi^{z-1})^{q-1}\right)(\xi^z) \\
&= X + \left((\xi - 1) \sum_{x \in \langle \xi \rangle} \left(1 - (X-x)^{q-1}\right)(x) \right) + \xi^z \left(-X^{q-1} + (X - \xi^{z-1})^{q-1} \right) \\
&= X + \left((\xi - 1) \sum_{j=0}^{p-1} \left(1 - (X - \xi^j)^{q-1}\right)(\xi^j) \right) + \xi^z \left(-X^{q-1} + X^{q-1} + h_{q-2}(\xi^{1-z} X) \right) \\
&= X + \left((\xi - 1) \sum_{j=0}^{p-1} \left(1 - X^{q-1} - h_{q-2}(\xi^{-j} X)\right)(\xi^j) \right) + \xi^z h_{q-2}(\xi^{1-z} X) \\
&= X + \left((\xi - 1) \sum_{j=0}^{p-1} (1 - X^{q-1}) \right) - \left((\xi - 1) \sum_{j=0}^{p-1} \xi^j \sum_{i=0}^{q-2} \xi^{-ij} X^i \right) + \xi^z h_{q-2}(\xi^{1-z} X) \\
&= X + 0 - \left((\xi - 1) \sum_{i=0}^{q-2} X^i \sum_{j=0}^{p-1} \xi^{-(i-1)j} \right) + \xi^z h_{q-2}(\xi^{1-z} X)
\end{aligned}$$

$$= X - \left((\xi - 1) \sum_{i=0}^{\lfloor \frac{q-2}{p-1} \rfloor} X^{(p-1)i+1}(-1) \right) + \xi^z h_{q-2}(\xi^{1-z} X)$$

$$= X + (\xi - 1) X h_{\lfloor \frac{q-2}{p-1} \rfloor}(X^{p-1}) + \xi^z h_{q-2}(\xi^{1-z} X). \qquad \square$$

5.4 Representation of the Cyclic Group of Order q

Finally, we consider representations of the cyclic group C_q in $\mathbb{F}_q^\times$ which preserve a long cycle. Let $C_q = \langle g \rangle$, choose a generator ξ of $\mathbb{F}_q^\times$, and choose $z \in \{1, 2, \ldots, q-1\}$. Define the bijection $\sigma \colon C_q \hookrightarrow \mathbb{F}_q$ by

$$\sigma\left(g^k\right) = \begin{cases} \xi^k, & 1 \le k \le z-1, \\ 0, & k = z, \\ \xi^{k-1}, & z+1 \le k \le q. \end{cases}$$

For $z + 1 \le k \le q$, we have $g^{k-q} = g^k$, hence

$$\sigma\left(g^{k-q}\right) = \sigma\left(g^k\right) = \xi^{k-1} = \xi^{k-1-(q-1)} = \xi^{k-q};$$

that is, $\sigma\left(g^k\right) = \xi^k$ for $z + 1 - q \le k \le 0$. Therefore, we can rewrite the bijection as

$$\sigma\left(g^k\right) = \begin{cases} \xi^k, & z+1-q \le k \le z-1, \\ 0, & k = z, \end{cases}$$

and it is clear that σ preserves a long cycle. As for the representation of C_p above, all representations of C_q fixing a long cycle with a fixed value of the parameter z are equivalent, while those with differing values of z are quasiequivalent if those z-values sum to 1 modulo $q - 1$ and not quasiequivalent otherwise by Theorem 3.4.5.

We first determine the polynomial representing the action of a generator.

Theorem 5.4.1. *Let $z \in \{1, 2, \ldots, q-1\}$ and let ξ be a generator of $\mathbb{F}_q^\times$. Then the polynomial representing the generator of g on $\mathbb{F}_q$ is*

$$f_g^{[\xi;z]}(X) = \xi X + \xi^z h_{q-2}(\xi^{1-z} X).$$

Proof. The action of g on $0 \in \mathbb{F}_q$ is

$$g * 0 = \sigma\left(g \cdot \sigma^{-1}(0)\right) = \sigma\left(g \cdot g^z\right) = \sigma\left(g^{z+1}\right) = \sigma\left(g^{z+1-q}\right) = \xi^{z+1-q},$$

while for $z + 1 - q \leq \ell \leq z - 1$,

$$g * \xi^\ell = \sigma\left(g \cdot \sigma^{-1}(\xi^\ell)\right) = \sigma\left(g \cdot g^\ell\right) = \sigma\left(g^{\ell+1}\right) = \begin{cases} \xi^{\ell+1}, & z+1-q \leq \ell \leq z-2, \\ 0, & \ell = z-1. \end{cases}$$

Interpolating, we obtain

$$\begin{aligned} f_g^{[\xi;z]}(X) &= \sum_{x \in \mathbb{F}_q} \left(1 - (X-x)^{q-1}\right)(g * x) \\ &= \left(\sum_{i=z+1-q}^{z-2} \left(1 - (X-\xi^i)^{q-1}\right)(\xi^{i+1})\right) \\ &\qquad + \left(1 - (X - \xi^{z-1})^{q-1}\right)(0) + \left(1 - (X-0)^{q-1}\right)(\xi^z) \\ &= \xi\left(\sum_{i=z+1-q}^{z-1} \left(1 - (X-\xi^i)^{q-1}\right)\xi^i\right) \\ &\qquad - \xi\left(1 - (X - \xi^{z-1})^{q-1}\right)\xi^{z-1} + (1 - X^{q-1})\xi^z \\ &= \xi X - \xi^z + \xi^z\left(X^{q-1} + h_{q-2}(\xi^{1-z}X)\right) + \xi^z - \xi^z X^{q-1} \\ &= \xi X + \xi^z h_{q-2}(\xi^{1-z}X), \end{aligned}$$

where the third term in the fourth line follows from Lemma 1.7.6. □

We remark that it is straightforward to prove directly that each representation polynomial $f_g^{[\xi;z]}(X) = \xi X + \xi^z h_{q-2}(\xi^{1-z}X)$ is in fact a permutation polynomial. First, observe that

$$h_{q-2}(x) = \begin{cases} 1, & x = 0, \\ -1, & x = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Consequently, it can be seen that

$$f_g^{[\xi;z]}(x) = \begin{cases} \xi^z, & x = 0, \\ 0, & x = \xi^{z-1}, \\ \xi x, & \text{otherwise}, \end{cases}$$

from which the permutation behavior of $f_g^{[\xi;z]}(X)$ is clear.

Now we establish the form of the representation polynomial of a general element of C_q.

Theorem 5.4.2. *Let $z \in \{1, 2, \ldots, q-1\}$ and let ξ be a generator of $\mathbb{F}_q^\times$. Then the polynomial representing the action of g^k on $\mathbb{F}_q$ for $2 \leq k \leq q-1$ is*

$$f_{g^k}^{[\xi;z]}(X) = \xi^k X + \xi^z h_{q-2}(\xi^{k-z}X) + (\xi^k - \xi^{k-1}) \sum_{i=1}^{k-1} h_{q-2}(\xi^{k-z}X)\xi^{z-i}.$$

Proof. For $2 \leq k \leq q-1$, the action of g^k on $\mathbb{F}_q$ is

$$g^k * 0 = \sigma\left(g^k \cdot \sigma^{-1}(0)\right) = \sigma\left(g^k \cdot g^z\right) = \sigma\left(g^{z+k}\right) = \sigma\left(g^{z+k-q}\right) = \xi^{z+k-q} = \xi^{z+k-1},$$

while for $1 \leq k + \ell \leq q-1$,

$$\begin{aligned} g^k * \xi^\ell &= \sigma\left(g^k \cdot \sigma^{-1}(\xi^\ell)\right) = \sigma\left(g^k \cdot g^\ell\right) = \sigma\left(g^{k+\ell}\right) \\ &= \begin{cases} \xi^{k+\ell}, & 1 \leq k+\ell \leq z-1, \\ 0, & k+\ell = z, \\ \xi^{k+\ell-1}, & z+1 \leq k+\ell \leq q-1, \end{cases} \\ &= \begin{cases} \xi^{k+\ell}, & 1-k \leq \ell \leq z-k-1, \\ 0, & \ell = z-k, \\ \xi^{k+\ell-1}, & z-k+1 \leq \ell \leq q-1-k. \end{cases} \end{aligned}$$

But for $z \leq \ell \leq q-1-k$, we have

$$\sigma\left(g^{k+\ell-q}\right) = \sigma\left(g^{k+\ell}\right) = \xi^{k+\ell-1} = \xi^{k+\ell-1-(q-1)} = \xi^{k+\ell-q},$$

so $g^k * \xi^\ell = \xi^{k+\ell}$ when $z-(q-1) \le \ell \le -k$. Therefore,

$$g^k * \xi^\ell = \begin{cases} \xi^{k+\ell}, & z+1-q \le \ell \le z-k-1, \\ 0, & \ell = z-k, \\ \xi^{k+\ell-1}, & z-k+1 \le \ell \le z-1. \end{cases}$$

Interpolating, we obtain

$$\begin{aligned}
f_{g^k}^{[\xi;z]}(X) &= \sum_{x \in \mathbb{F}_q} \left(1-(X-x)^{q-1}\right)(g^k * x) \\
&= \left(\sum_{i=z+1-q}^{z-k-1} \left(1-(X-\xi^i)^{q-1}\right)(\xi^{i+k})\right) + \left(1-(X-\xi^{z-k})^{q-1}\right)(0) \\
&\qquad + \left(\sum_{i=z-k+1}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)(\xi^{i+k-1})\right) + \left(1-(X-0)^{q-1}\right)(\xi^{z+k-1}) \\
&= \xi^k \left(\sum_{i=z+1-q}^{z-k-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) + \xi^k \left(\sum_{i=z-k}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) \\
&\qquad - \xi^k \left(1-(X-\xi^{z-k})^{q-1}\right)\xi^{z-k} - \xi^k \left(\sum_{i=z-k+1}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) \\
&\qquad + \xi^{k-1} \left(\sum_{i=z-k+1}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) + \left(1-X^{q-1}\right)\xi^{z+k-1} \\
&= \xi^k \left(\sum_{i=z-1-q}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) - \xi^z + \xi^z (X-\xi^{z-k})^{q-1} \\
&\qquad + \xi^{k-1}(1-\xi) \left(\sum_{i=z-k+1}^{z-1} \left(1-(X-\xi^i)^{q-1}\right)\xi^i\right) + \xi^{z+k-1} - \xi^{z+k-1} X^{q-1} \\
&= \xi^k X - \xi^z + \xi^z \left(X^{q-1} + h_{q-2}(\xi^{k-z} X)\right) + \xi^{k-1}(1-\xi) \left(\sum_{i=z-k+1}^{z-1} \xi^i\right) \\
&\qquad - \xi^{k-1}(1-\xi) \left(\sum_{i=z-k+1}^{z-1} \left(X^{q-1} + h_{q-2}(\xi^{-i} X)\right)\xi^i\right) + \xi^{z+k-1} - \xi^{z+k-1} X^{q-1},
\end{aligned}$$

where the last step follows from Lemma 1.7.6. Continuing, we have

$$f_{g^k}^{[\xi;z]}(X) = \xi^k X - \xi^z + \xi^z X^{q-1} + \xi^z h_{q-2}(\xi^{k-z} X) + \xi^{k-1}(1-\xi) \left(\sum_{i=z-k+1}^{z-1} \xi^i\right)$$

$$
\begin{aligned}
&\quad - \xi^{k-1}(1-\xi)X^{q-1}\left(\sum_{i=z-k+1}^{z-1}\xi^i\right) - \xi^{k-1}(1-\xi)\left(\sum_{i=z-k+1}^{z-1}h_{q-2}(\xi^{-i}X)\xi^i\right)\\
&\quad + \xi^{z+k-1} - \xi^{z+k-1}X^{q-1}\\
&= \xi^k X - \xi^z + \xi^z X^{q-1} + \xi^z h_{q-2}(\xi^{k-z}X) + \xi^{k-1}(\xi^{z-k+1} - \xi^z)\\
&\quad - \xi^{k-1}(\xi^{z-k+1} - \xi^z)X^{q-1} - \xi^{k-1}(1-\xi)\left(\sum_{i=z-k+1}^{z-1}h_{q-2}(\xi^{-i}X)\xi^i\right)\\
&\quad + \xi^{z+k-1} - \xi^{z+k-1}X^{q-1}\\
&= \xi^k X - \xi^z + \xi^z X^{q-1} + \xi^z h_{q-2}(\xi^{k-z}X) + \xi^z - \xi^{z+k-1} - \xi^z X^{q-1} + \xi^{z+k-1}X^{q-1}\\
&\quad + (\xi^k - \xi^{k-1})\left(\sum_{i=z-k+1}^{z-1}h_{q-2}(\xi^{-i}X)\xi^i\right) + \xi^{z+k-1} - \xi^{z+k-1}X^{q-1}\\
&= \xi^k X + \xi^z h_{q-2}(\xi^{k-z}X) + (\xi^k - \xi^{k-1})\sum_{i=1}^{k-1}h_{q-2}(\xi^{i-z}X)\xi^{z-i}. \qquad \square
\end{aligned}
$$

Chapter 6

THE THEORY OF BIVARIATE POLYNOMIAL REPRESENTATIONS

6.1 Construction of Bivariate Representations

We will be interested in consolidating the set Γ of polynomials representing a group G into a single polynomial representing the group. Appealing to the Bivariate Interpolation Formula (Lemma 2.1.3), we will define the *bivariate representation* of G to be the polynomial

$$M(X,Y) = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(1-(X-x)^{q-1}\right)\left(1-(Y-y)^{q-1}\right)(x*y) \in \mathbb{F}_q[X,Y],$$

where

$$x*y = \begin{cases} \sigma\left(\sigma^{-1}(x)\cdot\sigma^{-1}(y)\right), & x,y\in\sigma(G), \\ y, & \text{otherwise,} \end{cases}$$

for an additive assignation $\sigma\colon G\hookrightarrow\mathbb{F}_q^+$, and where

$$x*y = \begin{cases} \sigma\left(\sigma^{-1}(x)\cdot\sigma^{-1}(y)\right), & x,y\in\sigma(G), \\ 0, & xy=0, \\ y, & \text{otherwise,} \end{cases}$$

for a multiplicative assignation $\sigma\colon G\hookrightarrow\mathbb{F}_q^\times$.

For a fixed (but arbitrary) $x\in\sigma(G)$, it is easy to see that the bivariate representation reduces to the univariate representation from Chapter 3 for any $y\in\mathbb{F}_q$. The bivariate representation therefore extends the univariate representation by using the same assignation function σ to translate the element $g\in G$ indexing the representation polynomial $f_g(X)$ to the X coordinate of $M(X,Y)$. The specification that $0*x = x*0 = 0$ for a multiplicative representation will be necessary in Section 6.3.

6.2 Equivalence of Bivariate Representations

We define bivariate equivalence for multiplicative representations as follows; recall that we will consider a group homomorphism $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ as a function on $\mathbb{F}_q$ by defining it to fix 0. We say that two bivariate multiplicative representations M and M' are *equivalent* if there exists $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ such that $M(x,y) = \alpha\left(M'(\alpha^{-1}(x), \alpha^{-1}(y))\right)$ for all $x, y \in \mathbb{F}_q$. We will see that this definition is analogous to the (usual) univariate case of polynomial representations when $\sigma(G) = \mathbb{F}_q^\times$ by taking ψ to be the identity automorphism of G in the proof of Theorem 6.2.1.

Theorem 6.2.1. *Let M and M' be bivariate representation polynomials arising from multiplicative assignations σ and σ', respectively, and suppose that $\sigma(G) = \sigma'(G) = \mathbb{F}_q^\times$. Then quasiequivalence of σ and σ' is sufficient for equivalence of M and M'.*

To prove this theorem, we require two technical lemmas.

Lemma 6.2.2. *Let $\alpha \in \mathbb{F}_q^\times$. Then for any $x \in \mathbb{F}_q$, we have*

$$1 - (X - x)^{q-1} = \alpha^{-1}\left(1 - (\alpha(X) - \alpha(x))^{q-1}\right).$$

Proof. Let $x, y \in \mathbb{F}_q$, and note that $1 - (y-x)^{q-1}$ is 0 or 1 according to whether $x \neq y$ or $x = y$, respectively. Then we have

$$1 - (y-x)^{q-1} = \alpha^{-1}\left(\alpha\left(1 - (y-x)^{q-1}\right)\right) = \alpha^{-1}\left(\alpha(1) - \alpha\left((y-x)^{q-1}\right)\right)$$

since α must fix 0 and 1. Moreover, $x = y$ if and only if $\alpha(x) = \alpha(y)$, hence

$$1 - (y-x)^{q-1} = \alpha^{-1}\left(1 - (\alpha(y) - \alpha(x))^{q-1}\right).$$

Interpolating over y now yields the desired result. □

Lemma 6.2.3. *Let $\alpha \in \mathbb{F}_q^\times$ and let $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ be an arbitrary function. Then we have*

$$\sum_{x \in \mathbb{F}_q} \alpha^{-1}\Big(\left(1 - (X-x)^{q-1}\right)\varphi(x)\Big) = \alpha^{-1}\left(\sum_{x \in \mathbb{F}_q}\left(1 - (X-x)^{q-1}\right)\varphi(x)\right).$$

Proof. Let $y \in \mathbb{F}_q$ and consider the sum

$$S := \sum_{x \in \mathbb{F}_q} \alpha^{-1}\Big(\big(1-(y-x)^{q-1}\big)\,\varphi(x)\Big).$$

Recalling the fact from the previous lemma that for any $x, y \in \mathbb{F}_q$ we have $1-(y-x)^{q-1}$ is 0 or 1 according to whether $x \neq y$ or $x = y$, respectively, it follows that

$$\alpha^{-1}\Big(\big(1-(y-x)^{q-1}\big)\,\varphi(x)\Big) = \begin{cases} \alpha^{-1}\left(\varphi(y)\right), & x = y, \\ 0, & x \neq y. \end{cases}$$

Thus, for a fixed $y \in \mathbb{F}_q$, the only term of the sum S that is nonzero is the term where $x = y$, and this term is $\alpha^{-1}(\varphi(y))$. In other words,

$$S = \sum_{x \in \mathbb{F}_q} \alpha^{-1}\Big(\big(1-(y-x)^{q-1}\big)\,\varphi(x)\Big) = \alpha^{-1}\big(\varphi(y)\big) = \alpha^{-1}\left(\sum_{x \in \mathbb{F}_q} \big(1-(y-x)^{q-1}\big)\,\varphi(x)\right)$$

for each $y \in \mathbb{F}_q$. Interpolating over y concludes the proof. □

Proof of Theorem 6.2.1. Let σ and σ' be quasiequivalent multiplicative assignations and define

$$\begin{aligned} M(X,Y) &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \big(1-(X-x)^{q-1}\big)\big(1-(Y-y)^{q-1}\big)\,\sigma\left(\sigma^{-1}(x)\cdot\sigma^{-1}(y)\right), \\ M'(X,Y) &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \big(1-(X-x)^{q-1}\big)\big(1-(Y-y)^{q-1}\big)\,\sigma'\left((\sigma')^{-1}(x)\cdot(\sigma')^{-1}(y)\right). \end{aligned}$$

Recall from the univariate theory that since σ and σ' are quasiequivalent, there exist $\alpha \in \mathrm{Aut}(\mathbb{F}_q^\times)$ and $\psi \in \mathrm{Aut}(G)$ such that $\sigma = \alpha \circ \sigma' \circ \psi$. Equivalently, we also have $\sigma' = \alpha^{-1} \circ \sigma \circ \psi^{-1}$ and $(\sigma')^{-1} = \psi \circ \sigma^{-1} \circ \alpha$. Thus

$$\begin{aligned} M'(X,Y) &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \big(1-(X-x)^{q-1}\big)\big(1-(Y-y)^{q-1}\big)\,\sigma'\left((\sigma')^{-1}(x)\cdot(\sigma')^{-1}(y)\right) \\ &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \big(1-(X-x)^{q-1}\big)\big(1-(Y-y)^{q-1}\big) \\ &\qquad \cdot (\alpha^{-1} \circ \sigma \circ \psi^{-1})\left((\psi \circ \sigma^{-1} \circ \alpha)(x)\cdot(\psi \circ \sigma^{-1} \circ \alpha)(y)\right) \\ &= \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_q} \big(1-(X-x)^{q-1}\big)\big(1-(Y-y)^{q-1}\big)\,\alpha^{-1}\Big(\sigma\left(\sigma^{-1}(\alpha(x))\cdot\sigma^{-1}(\alpha(y))\right)\Big) \end{aligned}$$

where ψ and ψ^{-1} cancel since ψ is necessarily a group homomorphism. Applying Lemma 6.2.2 and noting that α is a homomorphism of $\mathbb{F}_q^\times$, we obtain

$$\begin{aligned}
M'(X,Y) &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \alpha^{-1}\left(1-(\alpha(X)-\alpha(x))^{q-1}\right)\alpha^{-1}\left(1-(\alpha(Y)-\alpha(y))^{q-1}\right) \\
&\qquad\qquad \cdot\alpha^{-1}\Big(\sigma\left(\sigma^{-1}(\alpha(x))\cdot\sigma^{-1}(\alpha(y))\right)\Big) \\
&= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \alpha^{-1}\Big(\left(1-(\alpha(X)-\alpha(x))^{q-1}\right)\left(1-(\alpha(Y)-\alpha(y))^{q-1}\right) \\
&\qquad\qquad \cdot\sigma\left(\sigma^{-1}(\alpha(x))\cdot\sigma^{-1}(\alpha(y))\right)\Big) \\
&= \sum_{\alpha(x)\in\mathbb{F}_q}\sum_{\alpha(y)\in\mathbb{F}_q} \alpha^{-1}\Big(\left(1-(\alpha(X)-\alpha(x))^{q-1}\right)\left(1-(\alpha(Y)-\alpha(y))^{q-1}\right) \\
&\qquad\qquad \cdot\sigma\left(\sigma^{-1}(\alpha(x))\cdot\sigma^{-1}(\alpha(y))\right)\Big).
\end{aligned}$$

We conclude by applying Lemma 6.2.3 and performing a change of variables:

$$\begin{aligned}
M'(X,Y) &= \alpha^{-1}\left(\sum_{\alpha(x)\in\mathbb{F}_q}\sum_{\alpha(y)\in\mathbb{F}_q}\left(1-(\alpha(X)-\alpha(x))^{q-1}\right)\left(1-(\alpha(Y)-\alpha(y))^{q-1}\right)\right. \\
&\qquad\qquad \left.\cdot\sigma\left(\sigma^{-1}(\alpha(x))\cdot\sigma^{-1}(\alpha(y))\right)\right) \\
&= \alpha^{-1}\left(\sum_{x'\in\mathbb{F}_q}\sum_{y'\in\mathbb{F}_q}\left(1-(\alpha(X)-x')^{q-1}\right)\left(1-(\alpha(Y)-y')^{q-1}\right)\right. \\
&\qquad\qquad \left.\cdot\sigma\left(\sigma^{-1}(x')\cdot\sigma^{-1}(y')\right)\right) \\
&= \alpha^{-1}\left(M(\alpha(X),\alpha(Y))\right). \qquad \square
\end{aligned}$$

6.3 Application to the Coordinatization of Finite Projective Planes

Our goal is to construct a planar ternary ring coordinatizing a finite projective planes of Lenz-Barlotti type "at least" II.2. When coordinatized optimally, these planes are $((\infty),[\infty])$- and $((0),[0])$-transitive, so that the planary ternary rings coordinatizing them are linear with additive and multiplicative structures that are groups.

We will narrow our focus as follows. Consider a planar ternary ring R, with $\mathbb{F}_q$ as its coordinatizing set, possessing the following properties:

1. R has prime-power order;
2. R is a group under addition isomorphic to $\mathbb{F}_q^+$;
3. R is a group G under multiplication;
4. R is linear, so we can write $T(X, Y, Z) = M(X, Y) + Z$.

Theorem 6.3.1. *Let R be a planar ternary ring coordinatized by a finite field $\mathbb{F}_q$ and satisfying the properties above, and denote multiplication in R by $M(X, Y)$. Then $M(X, Y)$ arises from interpolation of an assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$ as*

$$M(x, y) = \begin{cases} \sigma\left(\sigma^{-1}(x) \cdot \sigma^{-1}(y)\right), & xy \neq 0, \\ 0, & xy = 0. \end{cases}$$

Proof. Recall from Section 1.5 that if two groups are isotopic then they are, in fact, isomorphic. Since the multiplicative group of R, with operation $M(X, Y)$, is isomorphic to the group G, there exists a bijection $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$ satisfying

$$M\left(\sigma(g_1), \sigma(g_2)\right) = \sigma(g_1 \cdot g_2)$$

for $g_1, g_2 \in G$. Writing $x_1 = \sigma(g_1)$ and $x_2 = \sigma(g_2)$, we have

$$M(x_1, x_2) = \sigma\left(\sigma^{-1}(x_1) \cdot \sigma^{-1}(x_2)\right).$$

By defining $M(x_1, 0) = M(0, x_2) = M(0, 0) = 0$, it follows by interpolation that the polynomial function $M(X, Y)$ has the claimed form. It remains to show that $\sigma(e) = 1$, that is, σ is an assignation.

By PTR property (B), we have that $M(1, x) = x$ for any $x \in \mathbb{F}_q$; without loss of generality, we may assume that $x \in \mathbb{F}_q^\times$. Translating to an equation in terms of σ, we obtain

$$\sigma\left(\sigma^{-1}(1) \cdot \sigma^{-1}(x)\right) = x.$$

Since σ is injective and $x \in \mathbb{F}_q^\times = \sigma(G)$, we may apply σ^{-1} to both sides:

$$\sigma^{-1}(1) \cdot \sigma^{-1}(x) = \sigma^{-1}(x).$$

Since the equation is now an equation in the group G, we may cancel $\sigma^{-1}(x)$ from both sides, leaving

$$\sigma^{-1}(1) = e,$$

as desired. □

Corollary 6.3.2. *A finite Lenz-Barlotti II.2 plane of prime order may be coordinatized by a multiplicative assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$.*

Proof. Indeed, a Lenz-Barlotti II.2 plane $\mathscr{P}$ of prime order may be coordinatized by the prime field $\mathbb{F}_p$, and since addition in the planar ternary ring coordinatizing $\mathscr{P}$ forms a group of order p, it is indeed the addition of $\mathbb{F}_p$. Letting G denote the group of $((0),[0])$-transitivities of $\mathscr{P}$, the previous theorem then guarantees that multiplication arises from an assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$. □

Theorem 6.3.3. *The bivariate representation polynomial $M(X,Y)$ arising from an assignation $\sigma\colon G \hookrightarrow \mathbb{F}_q^\times$ as the interpolation of*

$$M(x,y) = \begin{cases} \sigma\left(\sigma^{-1}(x) \cdot \sigma^{-1}(y)\right), & xy \neq 0, \\ 0, & xy = 0, \end{cases}$$

coordinatizes a linear planar ternary ring if and only if $M(X,Y)$ satisfied PTR property (C).

Proof. The representation polynomial $M(X,Y)$ satisfies PTR property (A) by construction and property (D) since the planar ternary ring is assumed to be linear. Moreover, property (B) holds because $\sigma(e) = 1$:

$$M(x,1) = \sigma\left(\sigma^{-1}(x) \cdot \sigma^{-1}(1)\right) = \sigma\left(\sigma^{-1}(x) \cdot e\right) = \sigma\left(\sigma^{-1}(x)\right) = x$$

for all $x \in \mathbb{F}_q^\times$, and $M(1,x) = x$ follows similarly.

Now we will show that the unique solution x of equation (6.1) is a translation of PTR condition (C). Throughout, we will let $a, b, c, d \in \mathbb{F}_q$ such that $a \neq c$. First, assume that property (C) holds, so that $x \in \mathbb{F}_q$ is the unique solution of $M(x,a)+b = M(x,c)+d$, or equivalently, $M(x,a)-M(x,c) = d-b$. Now suppose that $d'-b' = d-b$ for some $b', d' \in \mathbb{F}_q$. Then there is a unique $x' \in \mathbb{F}_q$ such that

$$M(x',a) - M(x',c) = d' - b' = d - b,$$

which shows, by property (C), that we actually have $x = x'$. Taking $z = d - b$, we see that equation (6.1) holds. On the other hand, suppose (6.1) holds, and write $z = d-b$. Then

$$M(x,a) - M(x,c) = z = d - b$$

has a unique solution $x \in \mathbb{F}_q$, and hence property (C) holds. □

We conclude by stating an equivalent condition for when the bivariate representation polynomial $M(X,Y)$ coordinatizes a finite projective plane.

Corollary 6.3.4. *The bivariate representation polynomial $M(X,Y)$ satisfies PTR property (C) if and only if for all $a, c, z \in \mathbb{F}_q^\times$ such that $a \neq c$, there exists a unique $x \in \mathbb{F}_q^\times$ such that*

$$M(x,a) - M(x,c) = z. \tag{6.1}$$

Proof. From Theorem 6.3.3, it remains to show that we can restrict a, c, z to $\mathbb{F}_q^\times$. First, note that $x = 0$ is the unique solution of (6.1) when $z = 0$ since $a \neq c$, so we may take $z \neq 0$ from now on without loss of generality. Suppose $c = 0$, so that we wish to show there is a unique solution $x \in \mathbb{F}_q$ for

$$M(x,a) = z.$$

Translating to an equation in terms of σ, we have

$$\sigma\left(\sigma^{-1}(x) \cdot \sigma^{-1}(a)\right) = z,$$

which we can solve to obtain

$$x = \sigma\left(\sigma^{-1}(z) \cdot (\sigma^{-1}(a))^{-1}\right).$$

Thus there is a unique solution when $c = 0$. Similarly,

$$x = \sigma\left(\sigma^{-1}(-z) \cdot (\sigma^{-1}(c))^{-1}\right)$$

is the unique solution of $-M(x, c) = z$ when $a = 0$, and the proof is complete. □

Chapter 7

FUTURE WORK & OPEN PROBLEMS

Question 1. In Theorem 2.2.2, we found a polynomial indicator function for the cyclic subgroup C_p of $\mathbb{F}_q^+$. Find a polynomial indicator function for a general subgroup of $\mathbb{F}_q^+$; that is, a polynomial indicator function for a vector subspace of $\mathbb{F}_q^+$.

Question 2. Suppose $|G| = |\mathbb{F}_q^\star|$. Then we know from Corollary 3.2.3 that the polynomials representing elements of $P^\star(G, \sigma)$ are linear, and for multiplicative representations they are moreover linear monomials. Is there a subgroup of G or condition on the elements of G which produce monomial representation polynomials?

Question 3. Is there any relationship between the amount of structure preserved by an assignation and the degree of the representation polynomial? Can we determine what the degree must be? Can we count the number of nonzero terms? Do we always get polynomials of the shape $X^r f(X^s)$ (i.e. Wan-Lidl polynomials, see [25]) from multiplicative hemimorphisms?

Question 4. Prove Conjecture 1: The polynomial $f_g^{[\beta]}(X)$ representing the action of $g = g_1^{k_1} g_2^{k_2} \dots g_N^{k_N} \in C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_N}}$ on $\mathbb{F}_q^+$ has degree equal to $q\left(1 - \frac{p}{o(g)}\right) = p^n - \frac{p^{n+1}}{o(g)}$ when $o(g) > p$.

Question 5. What is the appropriate analogue of the preserved subgroup $P^\star(G, \sigma)$ for a bivariate representation? What properties does this subgroup have?

Question 6. Consider a bivariate representation polynomial $M(X, Y)$ (as in Chapter 6); the planar ternary ring axioms (A), (B), and (D) are satisfied automatically by the construction. What algebraic condition (e.g. equivalence, isotopy) preserves PTR

property (C) for $M(X, Y)$? More generally, What algebraic condition on planar ternary rings coordinatized by bivariate polynomials guarantees that the resulting planes are isomorphic?

Question 7. Consider a planar ternary ring with multiplication given by the polynomial $M(X, Y)$ (as in Chapter 6.3). By PTR property (C), we have that

$$M(a, X) + M(1, X) = M(a, X) + X$$

is a permutation polynomial for all $a \in \mathbb{F}_q \setminus \{0, 1\}$; that is, $M(a, X)$ is a complete polynomial. From Theorem 1 of [19], we know that a complete polynomial has reduced degree at most $q - 3$. Can we determine the coefficient

$$\sum_{x \in \mathbb{F}_q} x \, \sigma\left(g \cdot \sigma^{-1}(x)\right)$$

of X^{q-2} in $M(a, X)$?

Question 8. Is it possible to narrow the search space for polynomials coordinatizing planar ternary rings of Lenz-Barlotti II.2 planes enough that an exhaustive search is feasible, for example, over $\mathbb{F}_{17}$ or $\mathbb{F}_{41}$?

Question 9. Extend the construction of the bivariate representation of a group to produce a bivariate construction of a loop. What properties carry over to this representation, and which properties arise from the group structure (i.e. from associativity)?

BIBLIOGRAPHY

[1] M. Aschbacher, *Finite Group Theory*, second edition, Cambridge: Cambridge University Press, 2000.

[2] E.R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw Hill, 1968.

[3] O. Bottema, *On the Betti-Mattieu group*, Nieuw Arch. Wisk. (2)**16** no. 4 (1930), 46–50.

[4] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge: Cambridge University Press, 1994.

[5] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc. **4** (1953), 538.

[6] ———, *A note on the Betti-Mattieu group*, Portugal. Math. **22** (1963), 121–125.

[7] P. Dembowski, *Finite Geometries*, New York: Springer, 1968.

[8] L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.

[9] J.D. Dixon and B. Mortimer, *Permutation Groups*, New York: Springer, 1996.

[10] C. Hermite, *Sur les fonctions de sept lettres*, C.R. Acad. Sci. Paris **57** (1863), 750–757.

[11] D. R. Hughes and F. C. Piper, *Projective Planes*, New York: Springer, 1973.

[12] E.E. Kummer, *Über die ergänzungssätze zu den allgemeinen reciprocitätsgesetzen*, J. reine angew. Math. **44** (1852), 93–146.

[13] R. Lidl and G.L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95** (1988), 243–246.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge: Cambridge University Press, 1997.

[15] J.H. Van Lint, *Introduction to Coding Theory*, third edition, New York: Springer, 1999.

[16] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.

[17] R. Matthews, *Permutation properties of the polynomials* $1 + x + \cdots + x^k$ *over a finite field*, Proc. Amer. Math. Soc. **120** (1994), 47–51.

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

[19] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. (series A) **33** (1982), 197–212.

[20] W. Nöbauer, *Über eine klasse von permutationspolynomen und die dadurch dargestellten gruppen*, J. reine agnew. Math. **231** (1968), 215–219.

[21] D.J.S. Robinson, *A Course in the Theory of Groups*, second edition, New York: Springer, 1996.

[22] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Boca Raton: Chapman & Hall/CRC, 2007.

[23] R. M. Stafford, *Groups of permutation polynomials over finite fields*, Finite Fields Appl. **4** (1998), 450–452.

[24] T.P. Vaughan, *Polynomials and linear transformations over finite fields*, J. reine angew. Math. **262** (1974), 179–206.

[25] D. Wan and R. Lidl, *Permutation polynomials of the form* $x^r f(x^{(q-1)/d})$ *and their group structure*, Mh. Math. **112** (1991), 149–163.

[26] C. Wells, *Groups of permutation polynomials*, Monatsh. Math. **71** (1967), 248–262.

[27] C. Wells, *Generators for groups of permutation polynomials over finite fields*, Acta Sci. Math. Szeged **29** (1968), 167–176.

[28] C. Wells, *The degrees of permutation polynomials over finite fields*, J. Comb. Theory **7** (1969), 49–55.

Appendix A

SUMMARY OF NOTATION

A.1 Algebraic Structures

Structure	Symbol	Identity Element	Typical Elements	Operation(s)
Loop	L	e	ℓ, ℓ_1, ℓ_2	$\ell_1 \,\square\, \ell_2$
Group	G	e	g, g_1, g_2	$g_1 \cdot g_2$
Subgroup	$H \leq G$	e	h, h_1, h_2	$h_1 \cdot h_2$
Finite field of order $q = p^n$	$\mathbb{F}_q = \mathbb{F}_{p^n}$	0, 1	x, y	$x + y$, xy
Subfield (for $e \mid n$)	$\mathbb{F}_{p^e}$	0, 1	x, y	$x + y$, xy
Additive group of $\mathbb{F}_q$ with basis $[\beta_i]$	$\mathbb{F}_q^+$	0	$x = \sum_{i=0}^{n-1} \xi_i \beta_i$	$x + y$
Multiplicative group of $\mathbb{F}_q$ with generator ζ	$\mathbb{F}_q^\times$	1	$\xi = \zeta^i$, ξ_1, ξ_2	$\xi_1 \xi_2$
Group of $\mathbb{F}_q$ (either $\mathbb{F}_q^+$ or $\mathbb{F}_q^\times$)	$\mathbb{F}_q^\star$	$\mathrm{id}^\star$	x, y	$x \star y$
Preserved subgroup	$P^\star(G, \sigma)$			
Polynomial ring over $\mathbb{F}_q$	$\mathbb{F}_q[X]$	X	$f(X)$, $g(X)$	$f(g(X)) \pmod{X^q - X}$
Planar ternary ring	R	0, 1	x, y, z	$T(x, y, z)$
	$(R, \oplus)$	0		$T(x, 1, y) = x \oplus y$
	$(R, \otimes)$	1		$T(x, y, 0) = x \otimes y$

A.2 Representation Polynomials and Polynomial Operations

Operation	Notation
"All-ones" polynomial	$h_k(X) = \sum_{i=0}^{k} X^i$
Indicator polynomial for $S \subseteq \mathbb{F}_q$	$\iota_S(X)$
Assignation	$\sigma \colon G \hookrightarrow \mathbb{F}_q$
Action of $g \in G$ on $x \in \mathbb{F}_q$	$g * x = \sigma\left(g \cdot \sigma^{-1}(x)\right)$
Representation polynomial of $g \in G$	$f_g(X)$
with parameter set Z	$f_g^{[Z]}(X)$
set of representation polynomials	$\Gamma = \{f_g(X) : g \in G\}$
Bivariate representation of G	$M(X, Y)$
Composition of polynomials $f(X)$ and $g(X)$	$(f \circ g)(X) = f(g(X)) \pmod{X^q - X}$
k-fold composition of $f(X)$ with itself	$f(X)^{[k]} \pmod{X^q - X}$
compositional inverse of $f(X)$	$f(X)^{[-1]}$

A.3 Groups and Their Presentations

Group	Notation	Presentation
Automorphism group of G	$\mathrm{Aut}(G)$	—
Cyclic group of order m	C_m	$\langle g \mid g^m = 1 \rangle$
Dihedral groups	D_{2m}	$\langle r, t \mid r^m = t^2 = (rt)^2 = 1 \rangle$
General linear group of $\mathbb{F}_q$	$GL(\mathbb{F}_q)$	—
Hamiltonian groups (m odd)	H_{8m}	$Q \times O = \langle i, j \mid i^2 = j^2 = (ij)^2 = -1 \rangle \times \langle g \mid g^m = 1 \rangle$
Symmetric group on the set S	$\mathrm{Sym}(S)$	—

Index

assignation, 29
  construction by cosets, 32
  hemimorphism, 33
  preserving a long cycle, 33
axis, 7

bivariate representation, 73
  equivalent, 74

carry, 42
centre, 7
collineation, 7
  central, 7
  elation, 7
  homology, 7
complete mapping, 4
construction by cosets, 32

elation, 7

group action, 5

hemimorphism, 33
homology, 7
homotopy, 9

indicator function, 16
interpolation formula, 14
isotopy, 9
  principal, 9

loop, 8
  homomorphism, 9
  homotopy, 9
  isomorphism, 9
  isotopy, 9
  principal isotopy, 9

permutation isomorphic, 6
planar ternary ring, 7
  linear, 8
polynomial
  complete mapping, 4
  degree, 3
  linearized, 4
  permutation, 4
  reduced, 3
  representation, 26
preserved subgroup, 30, 32
preserving a long cycle, 33
projective plane, 6
  order, 7
  transitive, 7

representation, 5
additive, 29
bivariate, 73
equivalent, 6, 34, 74
multiplicative, 29
quasiequivalent, 6, 34
regular, 5
representation polynomial, 26