INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

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

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI®

DISSERTATION

CYCLOTOMIC COSET ASSOCIATION SCHEMES

Submitted by

Ann Cushman

Department of Mathematics

In partial fulfillment of the requirements

for the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2001

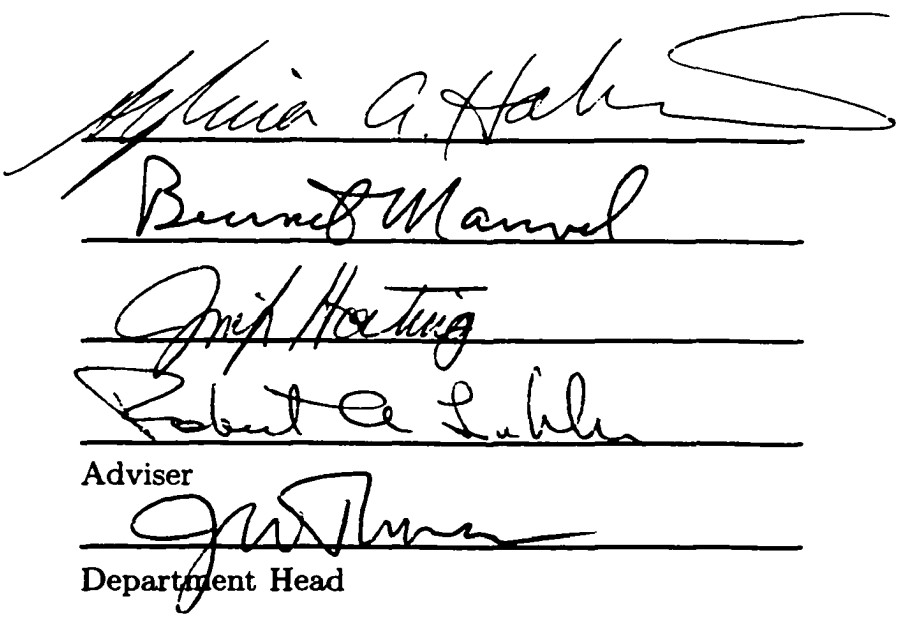
ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

COLORADO STATE UNIVERSITY

June 26, 2001

WE HEREBY RECOMMEND THAT THE DISSERTATION PREPARED UNDER OUR SUPERVISION BY ANN CUSHMAN ENTITLED "CYCLOTOMIC COSET ASSOCIATION SCHEMES" BE ACCEPTED AS FULFILLING IN PART REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY.

Committee on Graduate Work



Adviser

Department Head

ABSTRACT

CYCLOTOMIC COSET ASSOCIATION SCHEMES

For any abelian group G and subgroup Λ of $Aut(G)$, let $\{C_i\}$ be the Λ-orbits in G. The cyclotomic coset scheme is the commutative, non-symmetric association scheme with point set G and i^{th} relation $\{(x, y) : xy^{-1}$ is in $C_i\}$. This scheme admits the semidirect product of G by Λ as a group of automorphisms and is a generalization of cyclotomic association schemes.

We develop the theory of the cyclotomic coset scheme with particular attention to its character table. We give constructions for the character table and a formula for its inverse. If Λ contains the p^{th} power map for a prime p not dividing $|G|$ then the character table is integral modulo powers of prime ideals π over (p). The mod π^t character table is used to construct all factors modulo p^t of scheme elements. We use the mod π character table to link the set-ness property of scheme elements to their character values.

We show that the techniques for the study of difference sets and related structures persist in this new context. Cyclotomic coset schemes provide new tools to exploit the faithful spectrum. We apply this theory to a conjecture of John Dillon on cyclic difference sets with classical parameters. We also compute and use faithful idempotents modulo 2 to prove that a counter example to Dillon's conjecture must be a mod 2 sum of cosets of nontrivial subgroups of G.

Ann Cushman
Department of Mathematics
Colorado State University
Fort Collins, Colorado 80523
Summer 2001

ACKNOWLEDGEMENTS

I am most grateful to Dr. Robert Liebler, my adviser, for all of his help, guidance, patience, and encouragement. Without his support, this paper would be unthinkable. To Mark, my gratutude is beyond expression.

Contents

1 Introduction

The study of combinatorics is, at its heart, an integral study. In combinatorics we consider structures like sets (difference sets, codes), arrangements of sets (designs, association schemes), and so on. These combinatorial objects are described using the language of algebra (groups, vector spaces, matrix algebras), and studied using the tools of algebra.

The dilemma is that the farther one ventures into the algebraic realm and the use of fields, on the one hand, the more powerful the tools are and the easier solutions to the corresponding equations become. On the other hand, for combinatorial applications we require not just integrality, but 'set-ness' of solutions. We seem to be poised between $\mathbb{C}$ and its simplified algebra and $\mathbb{Z}$ and its combinatorial applicability.

This dissertation is motivated by the need to find a computational context in which the tools of algebra (group theory, complex characters, finite field theory) can be applied to combinatorial structures while maintaining as much control of integrality as possible.

In our study of abelian difference sets it became clear that the use of a multiplier group Λ is critical and should be applied as early in the process as possible. In this way, we restrict our attention from the beginning to group ring elements fixed by the multiplier group. The natural way to do this is to pass from group elements to orbit sums under Λ as our basis elements. Thus we are led to consider an association scheme based on G and Λ.

This dissertation is in three parts. Following preliminary material in chapter 2, the first part (chapter 3) gives the combinatorial setting for the association scheme $\mathcal{C}(G, \Lambda)$. In the first part we give definitions of difference sets and related structures

and multipliers, then discuss standard techniques used to study abelian difference sets. These include in particular: group homomorphic images, complex characters, and the embedding of a cyclic group in a quotient of finite fields. These are powerful and fruitful techniques.

On the other hand, we consider difficulties caused by using these techniques when we try to maintain integrality or 'set-ness' through the solution process. We also bring up in this context some conjectures of Dillon [Di], Pott [Pott], and Hamada (cf. [Xi]) about difference sets which are examples of these difficulties.

As a final illustration we describe a difference set context for the factorization of certain group ring elements and discuss problems that arise when using algebraic techniques to find such factorizations.

In the second part of the dissertation (chapter 4) we define the cyclotomic coset association scheme $\mathcal{C}(G, \Lambda)$ as a subalgebra of the integral group ring $\mathbb{Z}G$ with basis consisting of 'orbit sums' of elements of G under a subgroup Λ of $Aut(G)$. The association scheme $\mathcal{C}(G, \Lambda)$ is the setting in which we will connect the algebraic and combinatorial properties of the group ring elements we wish to study.

$\mathcal{C}(G, \Lambda)$ is shown (Theorem 4.45) to be a generalization of cyclotomic association schemes (the case that G is the additive group of a finite field). We work out some basic properties of these schemes as G and Λ vary, and especially of their character tables. The character table $P(G, \Lambda)$ of the scheme $\mathcal{C}(G, \Lambda)$ is the link between the combinatorial structures (defined as integral group ring elements fixed by a multiplier group) and the algebraic techniques (character and field methods).

We show that this character table is invertible (Corollary 4.39) and give a formula for its inverse. We also show (Theorem 4.29) that in an important special case the entries of $P(G, \Lambda)$ are actually integral modulo the powers of certain prime

ideals. (Later we will see that these prime ideals are the only relevant ideals when considering these special cases (Definition 5.42).) We also discuss properties of these character tables we can use in recursive constructions and illustrate these properties by computing specific examples.

The last part (chapter 5) is where we return to the question of abelian difference sets (and their relatives), and place them in the context of the cyclotomic coset association scheme. We show that the algebraic tools are preserved by translating them into the scheme context. In particular, the scheme builds in the multiplier, group homomorphic image techniques have their analogues (Theorem 5.3), the group character values are given by the spectrum (defined in section 5.1), the trace function is computable (Theorem 5.7) directly from the character table P, and the larger field context in at least one very general case is shown to be inessential (Theorem 5.13).

We translate the conjectures from chapter 3 into the language of the scheme and see that their key features are highlighted in that context. In particular the tricky set-ness condition of Dillon's conjecture can be brought into play within the scheme (Proposition 5.37). We compute faithful idempotents mod 2 and use these to give necessary and sufficient conditions (Theorems 5.29, 5.35) for counter examples to Dillon's conjecture. The third part concludes with a return to the factorization question. We consider in some detail the key algebraic issues that make this a difficult problem in the number ring and give an explicit algorithm for finding all mod p^k factors of a scheme element (Theorem 5.48).

2 Preliminaries

2.1 Association Schemes

In chapter 4 we define a specific class of association schemes which can be applied to certain combinatorial questions. In this section we give the basic definitions and theorems for general association schemes and their character tables that we will need. The standard reference is the 1984 text by Bannai and Ito [BI]. Brouwer, Cohen and Neumaier [BCN] (1989) also have many fundamental results on association schemes, though they concentrate on the symmetric case. Where the terminology in this subject varies we will follow Bannai and Ito.

Definition 2.1 *[BI, p.52] Let X be a set of size v, and define relations $\mathcal{R}_i : 0 \leq i \leq d$ as subsets of $X \times X$. Then $(X, \{\mathcal{R}_i\})$ is a d-class* **association scheme** *if and only if the following conditions are satisfied:*

1. $\mathcal{R}_0 = \{(x, x) \mid x \in X\}$
2. *The disjoint union $\cup_{i=0}^{d} \mathcal{R}_i$ is $X \times X$*
3. $(x, y) \in \mathcal{R}_i$ *if and only if* $(y, x) \in \mathcal{R}_{i'}$ *for some* i'
4. *For $(x, y) \in \mathcal{R}_k$, the size of the set $\{z \in X \mid (x, z) \in \mathcal{R}_i, (z, y) \in \mathcal{R}_j\}$ is constant, independent of the choice of (x, y). Denote this constant by p_{ij}^k. (The integers p_{ij}^k are called the* **structure constants** *of the scheme.)*

The scheme is **commutative** *if $p_{ij}^k = p_{ji}^k$ for all i, j, and k, and* **symmetric** *if in property 3, $\mathcal{R}_i = \mathcal{R}_{i'}$ for all i.*

It is convenient to replace the relations $\mathcal{R}_i$ with their matrices:

Definition 2.2 *Define the* i^{th} **adjacency matrix** A_i *of the scheme* $(X, \{\mathcal{R}_i\})$ *by*

$$(A_i)_{(x,y)} = \begin{cases} 1 & \text{if } (x,y) \in \mathcal{R}_i \\ 0 & \text{else.} \end{cases}$$

Using the adjacency matrices we get an equivalent matrix definition of the scheme.

Lemma 2.3 *[BI, p.53] Let* $A_0, \ldots A_d$ *be a set of* $v \times v$ $(0,1)-$*matrices. Then the set* $\{A_i\}$ *are adjacency matrices for an association scheme if and only if the following matrix conditions are satisfied:*

1. $A_0 = I$
2. $\sum_{i=0}^{d} A_i = J$ *(the all one's matrix)*
3. $A_i^T = A_{i'}$
4. $A_i A_j = \sum_{i=0}^{d} p_{ij}^k A_k$

The scheme is commutative if and only if $A_i A_j = A_j A_i$ *for all* i *and* j*, and symmetric if and only if* $A_i^T = A_i$ *for all* i*.*

We will also use the notation $(X, \{A_i\})$ for a scheme defined by adjacency matrices. The lemma above implies that the adjacency matrices A_i generate a matrix algebra (called the **Bose-Mesner** algebra if the scheme is symmetric), which is a $(d+1)$ dimensional subalgebra of $Mat_v(\mathbb{C})$.

We will be especially interested in the character table of certain commutative association schemes. We define the character table as in [BI, Ch. 2].

Since the matrices A_i are a set of commuting, normal matrices, they can be simultaneously diagonalized (by a unitary matrix). This gives a decomposition $\mathbb{C}^v = \bigoplus_{i=0}^{r} V_i$ into common eigenspaces V_i of $A_0, \ldots A_d$. Choose the V_i to be maximal so that if $i \neq j$ then the eigenvalue of A_k on V_i is different from the eigenvalue of A_k on V_j for some k. Then:

Lemma 2.4 *[BI, p.59]* $r = d$.

Definition 2.5 *The* **character table P** *of the association scheme* $(X, \{A_i\})$ *is the* $(d+1) \times (d+1)$ *matrix with* (i,j)*-entry defined to be the eigenvalue of* A_j *on* V_i.

Remark *The character table* P *is also sometimes called the first eigenmatrix of the scheme. Also, some authors define the* (i,j)*-entry of* P *to be the eigenvalue of* A_i *on* V_j.

Definition 2.6 *Define the* **valencies** k_i *of the scheme to be* $k_i := p^0_{ii}$. k_i *is the number of* $y \in X$ *such that* $(x,y) \in \mathcal{R}_i$ *for fixed* $x \in X$.
Define the **multiplicities** *of the scheme to be* $m_i := dim(V_i)$.

Note that $|X| = \sum k_i = \sum m_i$.

Proposition 2.7 *[BI, p.62]*
$P_{(i,0)} = 1$, *and* $P_{(0,i)} = k_i$.

Proposition 2.8 *[BI, p.63]*

1. *(First Orthogonality Relation)*

$$\sum_{t=0}^{d} \frac{1}{k_t} P_{(i,t)} \overline{P}_{(j,t)} = \frac{|X|}{m_i} \delta_{ij}$$

2. *(Second Orthogonality Relation)*

$$\sum_{t=0}^{d} m_t P_{(t,i)} \overline{P}_{(t,j)} = |X| k_i \delta_{ij}$$

Proposition 2.9 *Let $(X_1, \{B_i\})$ be an association scheme with adjacency matrices B_i, and $(X_2, \{\hat{B}_i\})$ be an association scheme with adjacency matrices $\hat{B}_i$. Denote the Kronecker product of matrices by $\otimes$. Then $(X_1 \times X_2, \{B_i \otimes B_j\})$ is an association scheme, called the* **product scheme**.

Proof: Check the matrix properties in Lemma 2.3. The first three properties are clear, and the fourth follows from the relation $(M_1 \otimes M_2)(M_3 \otimes M_4) = M_1 M_3 \otimes M_2 M_4$ for $\otimes$. ■

The direct product scheme is commutative (resp. symmetric) if and only if the original schemes are commutative (resp. symmetric).

2.2 Character Theory

Group character theory is a powerful technique for the study of combinatiorial structures including association schemes (chapter 4) and difference sets (chapters 3 and 5). This section contains the notation, definitions and results that we will apply in future sections. The material is taken from [CR, Sections 10 & 31], except where otherwise noted.

In what follows, G is a finite group, written multiplicatively, and K is a field.

A **K-representation of G** with representation space M is a homomorphism $T : g \mapsto T(g)$ into $GL(M)$. T has **character** χ defined by $\chi(g) = tr(T(g))$. Two representations with representation spaces M and M' are **equivalent** if $M \cong M'$ as G-spaces. Equivalent representations afford the same character. The representation (and its corresponding character) is **complex** if $K \leq \mathbb{C}$. In this case, $M = \mathbb{C}^n$ for some n, and χ maps $G \mapsto \mathbb{C}$. The representation (and its corresponding character) is **irreducible** if M has no nontrivial G-invariant subspace. We will denote the irreducible characters of G by $Irr(G)$.

A representation is **faithful** if $T(g) = T(1)$ implies $g = 1$. The **trivial** or **principal** representation maps $g \mapsto 1$ for all $g \in G$.

The **regular representation** of G maps g to a permutation matrix $T(g)$ having a 1 in row i and column j if $gg_i = g_j$ and zero otherwise.

The **group ring** KG is the set of all formal sums $\sum_{g \in G} a_g g$ where $a_g \in K$, with multiplication defined by extending the group multiplication linearly to all of KG.

The basic facts about characters which we will need are collected below. These are taken from [CR, Section 31] unless otherwise noted.

Lemma 2.10 *[CR, p.221-222] Let χ be a complex character of G. Then:*

1. $\chi(g^{-1}) = \overline{\chi(g)}$.

2. *If χ is an irreducible character, so is $\overline{\chi}$ defined by $\overline{\chi}(g) = \overline{\chi(g)}$*

We will be working primarily with abelian groups so we define the character table of a group as follows:

Definition 2.11 *[CR, p.225] The* **character table** $\chi(G)$ *of a group G is an array with rows indexed by the distinct irreducible characters χ_i of G and columns by elements g_j of G. The (χ_i, g_j) entry is $\chi_i(g_j)$.*

Theorem 2.12 *[CR, p.222](Character Orthogonality)*

1. *For χ_i, χ_j irreducible characters,*

$$\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = |G|\delta_{ij}$$

2.

$$\sum_{\chi \in Irr(G)} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{else} \end{cases}$$

Using this theorem it is easy to show:

Corollary 2.13 *(Inversion Formula)(cf. [Pott, p.17])*
Let G be an abelian group and $A = \sum_{g \in G} a_g g \in \mathbb{C}G$. Then

$$a_g = \frac{1}{|G|} \sum_{\chi \in Irr(G)} \chi(A)\chi(g^{-1})$$

Corollary 2.14 *Let χ and φ be irreducible characters and define*

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} g\chi(g^{-1})$$

Then:

$$\varphi(e_\chi) = \begin{cases} 1 & \text{if } \varphi = \chi \\ 0 & \text{else} \end{cases}$$

Definition 2.15 *Define the* **faithful character** e_F *to be $e_F := \sum e_\chi$ over all faithful irreducible characters χ.*

Lemma 2.16 *If $G = Z_v$ the cyclic group of order v, then $e_F = \sum_{g \in G} f_g g$ with*

$$f_g = \frac{1}{v} \frac{\phi(v)}{\phi(o(g))} \mu(o(g)).$$

Here ϕ is the Euler ϕ-function, μ is the Möbius μ-function, and $o(g)$ is the order of g in G.

Proof: The inversion formula implies that $e_F = \sum_{g \in G} a_g g$ with $a_g = \frac{1}{v} \sum \chi(g^{-1})$ where the sum is over all the faithful characters χ of G. Let $s(w)$ be the sum of all the primitive w^{th} roots of unity. Then since G is cyclic, $a_{g^{-1}} = \frac{1}{v} \frac{\phi(v)}{\phi(w)} s(w)$, for $w = o(g)$. Möbius inversion gives the sum of the roots of unity and we get the statement in the Lemma. ∎

Definition 2.17 *[Is, p.23] Let χ be a character of G. Then*

$ker(\chi) := \{g \in G \mid \chi(g) = \chi(1)\}$

Lemma 2.18 *[Is, p.24]*

If $N \trianglelefteq G$, then the irreducible characters of G/N are in one-to-one correspondance with the irreducible characters of G which are trivial on N. Explicitly, if χ is a character of G and $N \subseteq ker(\chi)$ then χ is constant on cosets of N in G and the function $\hat{\chi}$ on G/N defined by $\hat{\chi}(gN) = \chi(g)$ is a character of G/N. $\chi \in Irr(G)$ if and only if $\hat{\chi} \in Irr(G/N)$.

Lemma 2.19 *[CR, p. 266] Let χ be a character of H for $H \trianglelefteq G$. Let*

$$\chi^G(\alpha) = \frac{1}{|H|} \sum_{y \in G} \tilde{\chi}\,(y^{-1}\alpha y)$$

for α in G where

$$\tilde{\chi}\,(\beta) = \begin{cases} \chi(\beta) & \text{if } \beta \in H \\ 0 & \text{else.} \end{cases}$$

Then χ^G is a character of G called the **induced character**.

Lemma 2.20 *[Is, p.16,30]*

1. *G is abelian if and only if all irreducible representations are* **linear** *(having representation space $M = \mathbb{C}$).*

2. *Let G be abelian and let $G^* = Irr(G)$. Then G^* is an abelian group under function composition and $G \cong G^*$.*

The first statement in the lemma above allows us to identify irreducible representations with their characters when the group is abelian.

Definition 2.21 *[CR, p.37] For a finite group G the smallest integer v satisfying $g^v = 1$ for all $g \in G$ is called the* **exponent of** *G and will be denoted $exp(G)$.*

Lemma 2.22 *[CR, p.37] Let G be abelian, with $exp(G) = v$, and let χ be any irreducible complex character of G. Then $\chi(g) = \zeta_v$ where ζ_v is a v^{th} root of unity.*

A complex character χ of G is extended to the integral group ring $\mathbb{Z}G$ by $\chi(\sum a_g f) = \sum a_g \chi(g)$. In case G is abelian of exponent v, the complex character value of any $A \in \mathbb{Z}G$ is in the number ring $\mathbb{Z}[\zeta_v]$ where ζ_v is a v^{th} root of unity. In the next section we will summarize some basic results about this number ring.

2.3 Number Theory

In this section we collect the notations, definitions and results from algebraic number theory that will be needed in future sections. All material in this section is taken from Ireland and Rosen [IR] unless otherwise noted.

We begin with finite fields.

Let $GF(q)$ denote the finite field with $q = p^e$ elements for some prime p, and let $GF(q)^*$ denote its multiplicative group.

Theorem 2.23 *[IR, p.80] $GF(q)^*$ is a cyclic group of size $q - 1$.*

We will call α a **primitive element** of $GF(q)$ if $GF(q)^* = < \alpha >$.
The **trace function** from $GF(q^n)$ to $GF(q)$ will be denoted $tr_q^{q^n}$ and is defined by: $tr_q^{q^n}(\alpha) = \alpha + \alpha^q + \ldots \alpha^{q^{n-1}}$ for all $\alpha \in GF(q^n)$.

Proposition 2.24 *[IR, p.158-159] Let $\alpha \in GF(q^n)$, and $a \in GF(q)$.*

1. $tr_q^{q^n}(\alpha) \in GF(q)$.
2. $tr_q^{q^n}(a\alpha) = a(tr_q^{q^n}(\alpha))$.

We will always take ζ_v to be a primitive v^{th} root of unity. We will use several facts about the number ring $D := \mathbb{Z}[\zeta_v]$ which we summarize below.

Theorem 2.25 *[IR, p.177] Every prime ideal of D is maximal.*

Theorem 2.26 *[IR, p.180] Every nonzero ideal in D can be written uniquely as a product of prime ideals.*

If an ideal π is a factor of an ideal I in the sense of Theorem 2.26 we say π **lies above** I.

Theorem 2.27 *[IR, p.196] Let let $gcd(v,p) = 1$, let σ_p be the map $x \mapsto x^p$, and let π be a prime ideal of $\mathbb{Z}[\zeta_v]$ containing p. Then $\sigma_p(\pi) = \pi$.*

Definition 2.28 *[IR, p. 194] The v^{th}* **cyclotomic polynomial** *$\Phi_v(x)$ is $\Pi(x - \zeta_v^a)$ where the product is taken over all a such that $1 \leq a \leq v$ and $gcd(a,v) = 1$.*

Theorem 2.29 *[IR, p.194] $\Phi_v(x) \in \mathbb{Z}[x]$.*

We plan to use powers of the prime ideals π lying above (p) in $\mathbb{Z}[\zeta_v]$ for the case $gcd(v,p) = 1$. Calderbank and Sloane [CS] give a nice exposition of this topic which we summarize below.

Theorem 2.30 *[CS] Let p be a prime not dividing v. Then the ideal (p) factors into prime ideals as $(p) = \pi_1\pi_2 \ldots \pi_g$ in $\mathbb{Z}[\zeta_v]$. The π_i are $(f_i(\zeta_v), p)$ for the g distinct irreducible divisors $f_i(x)$ of $\Phi_v(x)$ in $\mathbb{Z}/(p)[x]$.*

We can consider $(x^v - 1)$ as an element of $\mathbb{Z}/(p)[x]$ and also of $\mathbb{Z}/(p^e)[x]$. The monic irreducible divisors of $(x^v - 1)$ in $\mathbb{Z}/(p)[x]$ are in one to one correspondance with the monic irreducible divisors of $(x^v - 1)$ in $\mathbb{Z}/(p^e)[x]$. Explicitly:

Theorem 2.31 *[CS, Theorem 1] If $f(x)$ is a monic irreducible divisor of $x^v - 1$ in $\mathbb{Z}/(p)[x]$, then there is a unique irreducible polynomial $f^{(e)}(x)$ (the e^{th}* **hensel lift of** *f) which divides $x^v - 1$ in $\mathbb{Z}/(p^e)$ and which is congruent to $f(x)$ modulo p.*

Theorem 2.32 *[CS, Theorem 4] Let p be a prime not dividing v. Let f be a factor of $\Phi_v(x)$ mod p, so that $\pi = (f(\zeta_v), p)$ is a prime ideal above (p) in $\mathbb{Z}[\zeta_v]$. Then $\pi^e = (f^{(e)}(\zeta_v), p)$.*

The binomial theorem implies that $(f(x))^p = f(x^p) + p\,h(x)$. We can use this to recursively compute the e^{th} hensel lift from the $(e-1)^{st}$.

Lemma 2.33 *Let $f(x)$ be a divisor of $x^v - 1$ mod p and let $j(x) = f^{(e-1)}(x)$.*
Let $s = p^{-1}$ mod v and define $h(x) = \frac{1}{p}((j(x))^p - j(x^p))$.
Let $g(x) = j(x) + p(h(x^s) \bmod (j, p^{e-1})$. Then $g(x) = f^{(e)}(x)$

Proof: Computing, we get $g(x) \equiv f(x) \bmod p$, and if $j(\alpha) \equiv 0 \bmod p^{e-1}$, then $g(\alpha^p) \equiv 0 \bmod p^e$. So g divides $x^v - 1 \bmod p^e$ ■

3 Combinatorial Context

In this chapter we describe the combinatorial setting for the association schemes that we introduce in chapter 4. That setting is the study of elements of the group ring RG with 'nice' combinatorial properties. In particular the elements we wish to study correspond to subsets (or multi-sets) of the group G and hence will have $(0,1)$- (or at least positive integer)- coefficients. They also satisfy certain group ring equations. In section 3.1 we define difference sets and related structures and give some basic theorems about them. The multiplier conjecture and Theorem 3.14 motivate our study of cyclotomic coset association schemes in chapter 4, since every equivalence class of a difference set in G fixed by a multiplier group Λ must have a member in the scheme $\mathcal{C}(G,\Lambda)$.

In section 3.2 we consider some of the standard techniques used to study abelian difference sets. These include in particular: group homomorphic images, group character methods, and constructions involving finite fields. We discuss a recent paper of Gaal and Golomb [GG] in this context, and give a general theorem of No about finite field constructions [No] in some detail.

In section 3.3 we describe problems that arise when using algebraic techniques to study combinatorial structures. The difficulty is that our combinatorial structures are usually defined as sets, yet the most powerful algebraic techniques do not maintain even integrality.

Finally in section 4, we discuss some open questions in this area (in particular a conjecture of Dillon) that highlight the interplay between the algebra and the combinatorics. We also discuss the combinatorial context for the factorization of certain group ring elements. The Gordon Mills Welch construction gives a key example of this kind of factorization.

In chapter 5 we revisit the techniques from section 2 and the problems from sections 3 and 4 in the context of the cyclotomic coset association schemes.

3.1 Difference Sets and Related Structures

We now focus on elements of the integral group ring whose combinatorial properties force them to satisfy certain group ring equations. Our primary examples are difference sets. In this section we summarize some basic definitions and results about difference sets (and similar objects). These can be found in any standard reference on the subject. We use [Pott] whenever possible. (There are more comprehensive references (eg. [BJL]), but the monograph by Pott is the most recent.)

Definition 3.1 *[Pott, p.11] Let G be a group of order v, written multiplicatively. Then a (v, k, λ)* **difference set** *is a k-element subset D of G satisfying the 'difference condition': For each non-identity element $g \in G$, there are exactly λ representations $g = xy^{-1}$ for $x,\ y \in D$. It is usual to define the additional parameter $n := k - \lambda$. Difference sets with $n = 0$ or $n = 1$ are called* **trivial**. *A difference set is also called* **abelian** *(resp.* **non-abelian**, *or* **cyclic**) *if the group G is abelian (resp. non-abelian or cyclic).*

Remark *The definition together with a simple count implies that the relation $k(k-1) = \lambda(v-1)$ must hold among the parameters of a difference set.*

The formal sum $\sum_{d \in D} d$ is an element of the integral group ring $\mathbb{Z}G$. We follow the standard conventions:

1. For any subset $S \subset G$, write $S = \sum_{s \in S} s$ as an element of $\mathbb{Z}G$.
2. For an element $A = \sum a_g g \in \mathbb{Z}G$, define $A^{(t)} = \sum a_g g^t$.
   (More generally, if σ is any map on G write $A^\sigma = \sum a_g \sigma(g)$.)

This allows us to write the equivalent group ring definition:

Lemma 3.2 *[Pott, p.10] If $D \in \mathbb{Z}G$ represents a k-element subset of G then D is a (v, k, λ) difference set if and only if D satisfies the difference set equation in $\mathbb{Z}G$:*

$$DD^{(-1)} = n\,1_G + \lambda G \tag{3.3}$$

The group ring formulation makes it easier to define structures related to difference sets by simply giving the group ring equation the structure must satisfy. We list two additional such definitions below for future use. These and similar examples can be found in [Pott, ch 1].

Definition 3.4 *R is an (m, n, k, λ)-***relative difference set** *in G relative to the normal subgroup N of G, if and only if R corresponds to a k-set and satisfies the integral group ring equation*

$$RR^{(-1)} = k\,1_G + \lambda(G - N) \tag{3.5}$$

where $m = |G/N|$ and $n = |N|$.

Definition 3.6 *R is an $(m, n, k, \lambda_1, \lambda_2)$* **divisible difference set** *in G, relative to a normal subgroup N of G, if and only if R corresponds to a k-set and satisfies the integral group ring equation:*

$$RR^{(-1)} = (k - \lambda_1)\,1_G + (\lambda_1 - \lambda_2)N + \lambda_2 G \tag{3.7}$$

where $m = |G/N|$ and $n = |N|$.

If D is a (v, k, λ) difference set, then so is any shift gD for any $g \in G$ and any automorphic image $\tau(D)$ for any $\tau \in \mathrm{Aut}(G)$. Difference sets obtained in this way from D are said to be **equivalent** to D.

Remark *If D is a (v, k, λ) difference set in G, then the complement $G - D$ is a $(v, v-k, v-2k+\lambda)$ difference set.*

There is a connection between difference sets and designs:

Definition 3.8 *A* **symmetric (v, k, λ)-design** *is an incidence structure with a set of v points and v blocks of size k, such that any two distinct points lie in exactly λ common blocks.*

Lemma 3.9 *(cf. [Pott, p.13].) The set of points given by G, and the set of blocks given by $\{ gD \mid g \in G\}$ is a symmetric (v, k, λ)-design with G acting transitively on the blocks if an only if D is a (v, k, λ) difference set in G.*

Definition 3.10 *[Pott, p.27] A* **multiplier** *of a difference set D is a group automorphism τ which satisfies $\tau(D) = gD$ for some $g \in G$. (That is, the automorphism acts as a shift on the difference set.) If in addition, $\tau(D) = D^{(t)}$ for some t, then we say τ (or sometimes just t) is a* **numerical multiplier**. *The set of multipliers of a difference set D forms a group under function composition, called the* **multiplier group** *of D.*

Multipliers are tremendously useful in the study of difference sets. A key reason for this is contained in the theorem below.

Theorem 3.11 *[Pott, p.31] If a difference set D has a multiplier τ, then there is at least one translate Dg of D such that $\tau(Dg) = Dg$.*

In fact, it has been shown (cf [Pott] p.31) that if $gcd(v, k) = 1$ then there is some shift gD of an abelian (v, k, λ) difference set D fixed by all multipliers.

Since we study difference sets only up to equivalence, without loss we only consider sets fixed by the multiplier group. This is the inspiration for the automorphism group Λ in the definition of cyclotomic coset association schemes given in chapter 4.

There are several 'multiplier theorems' which give multipliers of abelian difference sets in terms of their parameters (v, k, λ). Many of these multiplier theorems are attempts to prove the famous 'multiplier conjecture' :

Conjecture 3.12 *(Hall)(cf. [Pott, p.29]) Every divisor of $n = k - \lambda$ which is relatively prime to v is a (numerical) multiplier of any abelian (v, k, λ) difference set.*

The first multiplier theorem is due to Hall and Ryser (1951).

Theorem 3.13 *(cf. [Bau, p.8]). If p is a prime dividing n and $gcd(p, v) = 1$, and if $p > \lambda$ then p is a numerical multiplier of any abelian (v, k, λ) difference set.*

The additional multiplier theorems attempt to weaken the condition that $p > \lambda$. The one we will use is due to Marshall Hall:

Theorem 3.14 *(cf. [Bau] p.54) Let D be a (v, k, λ) difference set in an abelian group G. Let n_o be a divisor of n satisfying $gcd(n_o, v) = 1$ with $n_o > \lambda$. If, for every prime p dividing n_o there is an integer j_p with $p^{j_p} \equiv t$ modulo v, then t is a (numerical) multiplier of D.*

Example 3.15 *Let $v = 2^d - 1$, $k = 2^{d-1}$, and $\lambda = 2^{d-2}$ for $d > 2$, so that $n = 2^{d-2}$. Then use $n_o = n$ in Theorem 3.14 to get $t = 2$ as a numerical multiplier.*
This means any $(2^d - 1, 2^{d-1}, 2^{d-2})$ difference set in an abelian group G has an element D of its equivalence class fixed by the multiplier group $\Lambda =< \sigma : \sigma(x) = x^2 >$. Hence D is in the cyclotomic coset association scheme $\mathcal{C}(G, \Lambda)$ defined in chapter 4.

The difference-set-like structures mentioned above have their own multiplier theorems very similar to those for difference sets.

Finally, we note that while there are families of (v, k, λ) difference sets with $gcd(v, n) > 1$ there are no multiplier theorems for these sets. For this reason we concentrate on the case $gcd(v, n) = 1$.

3.2 Established Techniques

In this section we describe standard general techniques used to study abelian difference sets, focusing on the case $gcd(v, n) = 1$. In addition to group homomorphic images, classical cyclotomy and character methods, we describe a tool introduced by Gaal and Golomb [GG] that we will reconsider in chapter 5. Construction techniques involving finite fields whose multiplicative group has G as a homomorphic image are also summarized. In chapter 5 we show that this larger field context is inessential.

The most basic technique for studying difference sets is simply 'brute force.' If we are looking for (v, k, λ) difference sets in some group G, we test all k-subsets in G for the property and study those. This approach is refined using multiplier theorems.

If it is known that some group automorphism τ is a multiplier of a difference set, we only consider members of the equivalence class fixed by τ so we need only test k-subsets that are unions of orbits under τ (or show that there are none such). This approach alone is sufficient to rule out parameter sets, or even to construct all (equivalence classes of) difference sets when the order of τ is large relative to v.

The next refinement is to study all possible group homomorphic images of a difference set in G under maps from G to its quotient groups G/H. Homomorphisms of groups naturally extend to homomorphisms of the corresponding group rings. Applying such a homomorphism τ of G to the group ring equation (3.3), we obtain:

$$\tau(D)\tau(D^{(-1)}) = n \cdot 1_G + \lambda \cdot (\tau(G)) \tag{3.16}$$

So group homomorphic images of difference sets satisfy group ring equations in

the (quotient) group ring similar to (3.3).

(Some authors ([BJL]) use the term 'difference list' for a group ring element satisfying 3.16 since these group ring elements are not required to represent sets.

Example 3.17 *As an illustration of this technique we summarize Baumert's exposition [Bau, III.C] of this technique for cyclic groups.*

In case $G = Z_v =< x \mid x^v = 1 >$, $G/H \cong Z_w$, *solving (3.16) amounts to finding all solutions to the system of diophantine equations:*

$$\begin{aligned} \sum_{i=0}^{w-1} b_i &= k \\ \sum_{i=0}^{w-1} b_i^2 &= n + \frac{\lambda v}{w} \\ \sum_{i=0}^{w-1} b_i b_{i-j} &= \frac{\lambda v}{w} \quad j = 1 \ldots w-1. \end{aligned}$$

This is done for each $w \mid v$, *in order to find the possible homomorphic images*

$$D_w := \sum_{i=0}^{w-1} b_i x^{\frac{v}{w}}$$

of D *into the various quotient groups* Z_w *of* Z_v.

The typical strategy in both exhaustive searches and non-existence proofs for a given G and parameter set (v, k, λ) is to solve the difference list equation (3.16) for (all) possible homomorphisms τ and then to search the intersection of the pre-images of these solutions for difference sets in G, or to show that the intersection of such pre-images is the empty set.

This is an extremely common technique because it is so useful. Group homomorphic images were used as early as 1955 by Bruck [BJL, VI.6] and also by Turyn [Tur]. For current applications of this technique see for example Smith [DS] (and also Bacher [Bac]) in exhaustive enumerations of $(511, 256, 128)$ difference sets, Iiams (1999) [Ii]

in settling some open cases for (non)-existence, and Gaal and Golomb (2000) [GG] in an exhaustive ennumeration of $(1027, 512, 256)$ cyclic difference sets.

The next general technique is to apply group representations. If G is abelian, all representations are linear, and are therefore group characters. The systematic use of group characters in the study of abelian difference sets goes back at least to the key paper by Turyn (1965) [Tur]. The general idea is contained in the following well-known lemma, which follows from the fact that group characters extend to group-ring homomorphisms.

Lemma 3.18 *Let G be abelian with $exp(G) = v$. Suppose $D \in \mathbb{Z}G$ satisfies (3.3). Suppose $\alpha = \chi(D) := \sum_{d \in D} \chi(d)$, where χ is any nontrivial irreducible character of G. Then if $\overline{\alpha}$ is the complex conjugate of α, $\alpha \in \mathbb{Z}[\zeta_v]$ satisfies $\alpha\bar{\alpha} = n$.*

Lemma 3.18 is used with results from algebraic number theory to prove various multiplier theorems, to rule out certain parameter sets, and in exhaustive enumerations and constructions.

A major drawback of this technique is the required knowledge of all number ring elements of given absolute value $\sqrt{n}$. Turyn, for example required the following 'self-conjugacy' condition where one can find all α satisfying $\alpha\bar{\alpha} = n$.

Definition 3.19 *An integer $n \in \mathbb{Z}$ is* **self-conjugate** *modulo v if all prime ideals above n in $\mathbb{Z}[\zeta_v]$ are invariant under complex conjugation.*

Under this condition Turyn showed that the group character approach could be used quite successfully. The condition of self conjugacy, however is a strong condition on v and n which rules out many interesting parameter sets. As recently as 1999, Schmidt [Sc, p.32] discusses this problem and notes that "the probability that n is

self-conjugate modulo v decreases exponentially fast in the number of distinct prime divisors of n and of v."

Along these lines, Gaal and Golomb [GG] recently used a discrete Fourier transform in their exhaustive search for cyclic $(2^{10}-1, 2^9, 2^8)$-difference sets. After solving the difference set equation in all group homomorphic images (to quotient groups of order 3, 11, 31, and using these to quotient groups of order 33, 93, and 341), their next step was to test the intersection of the pre-images of these solutions for the difference set condition. In their case, the difficulty was that the usual tests for the difference set property are prohibitively time consuming for a group of this size.

Gaal and Golomb applied the following additional test: For each pre-image sequence $\{a_i\}_{i=0}^{v-1}$, they computed a 'single Discrete Fourier Transform Value'

$$A = \sum_{j=0}^{v-1} a_i e^{-\sqrt{-1}j\frac{2\pi}{v}} \tag{3.20}$$

as a complex number. They then checked (using floating point computation with tolerance) whether its $\mathbb{C}$-norm $A\overline{A}$ was $\sqrt{n}$.

Under the expectation that "non-difference set candidates fail this test with high probability" the number of sequences which must be further tested was considerably reduced, enough so that they were able to exhaustively ennumerate all $(2^{10}-1, 2^9, 2^8)$ cyclic difference sets. A sharpened variation of this idea is presented in section 5.2.

Next we consider a series of difference set construction techniques based on finite fields.

An early approach to difference set construction was "cyclotomy." The set of all N^{th}- power residues in $GF(q)$ was examined for the difference set condition for various N and q. This was inspired by the best known example - due to Payley (1933) where $N = 2$ and q is a prime conjugate to 3 mod 4.

Theorem 3.21 *(cf. [Pott, p.39]) Let $v = 4n - 1$ be prime. Then the set of quadratic residues modulo v form a $(4n - 1, 2n - 1, n - 1)$ difference set in Z_v.*

Example 3.22 *Let $n = 2$ in the theorem above. The set of squares mod 7 are $\{1, 2, 4\}$. These form a $(7, 3, 1)$ difference set in Z_7 (written additively).*

There are several theorems on cyclotomic difference sets in finite fields dating from the 1960's. The 1965 monograph by Storer [St] is the standard reference. The cyclotomy approach has likely been exhausted however, and most researchers in the subject have abandoned cyclotomy in favor of the approaches described below.

Let q be a power of a prime. Whenever $v = (q^n - 1)/(q - 1)$, one can realize the cyclic group Z_v as a quotient group $Z_v \cong GF(q^n)^*/GF(q)^*$ and use the finite field to construct difference sets with the **classical parameters**:

$$\left(\frac{q^d - 1}{q - 1}, \frac{q^{d-1} - 1}{q - 1}, \frac{q^{d-2} - 1}{q - 1}\right) \tag{3.23}$$

These constructions follow a couple of similar patterns. In the first, one finds a map from $GF(q^n)$ to $GF(q)$ with certain specified properties. Then the kernel of the map is shown to be a (cyclic) difference set with the parameters (3.23) above.

The oldest such construction is due to Singer(1938):

Theorem 3.24 *(cf. [Pott, p.36].) Let α be a primitive element of $GF(q^n)$. Then the set $D = \{\alpha^t : f(\alpha^t) = 0, \text{for } 0 \leq t < \frac{q^n - 1}{q - 1}\}$ is a union of $GF(q)^*$ cosets in $GF(q^n)$ that form a cyclic difference set with parameters (3.23).*

Difference sets constructed this way are called **Singer difference sets.**

In 1962, Gordon, Mills and Welch gave a structure theorem for Singer difference sets which resulted in the construction of a new infinite family of difference sets with the classical parameters (3.23). A different formulation appears in section 3.4: here, we use the 'twisted trace' form.

Theorem 3.25 *(Gordon-Mills-Welch) [Pott, p.79]. Let α be a primitive element of $GF(q^n)$, let $s \mid d$ and let r be such that $gcd(q^s - 1, r) = 1$. Then the set:*

$$\{\alpha^t : tr_q^{q^s}(tr_{q^s}^{q^d}(\alpha^t)^r) = 0,\ 0 \leq i \leq (q^d - 1)/(q - 1)\}$$

is a union of $GF(q)^*$ - cosets of $GF(q^n)$ that form a cyclic difference set with parameters (3.23).

These basic constructions have been successively generalized. For example we have the 'cascaded GMW-sequences given by Klapper (cf. [No]) defined in a similar way by the maps

$$f(a^t) = tr_q^{q^k}\{tr_{q^k}^{q^m}[(tr_{q^m}^{q^n}(\alpha^t))^r]^u\}$$

for $k \mid m,\ m \mid n,\ 1 \leq u \leq q^k - 1,\ 1 \leq r \leq q-2,\ gcd(u, q^k - 1) = 1,\ gcd(r, q^m - 1) = 1,$ and α a primitive element of $GF(q^n)$.

The second pattern in these construction techniques is to find a map from $GF(q^n)$ to itself. Recently, several authors (Maschietti [MA], Xiang [Xi], Dillon and Dobbertin [Xi], and others) have had some success in showing that the images of certain q-to-1 maps on $GF(q^d)$ are difference sets with the classical parameters (or their complementary parameters.)

Definition 3.26 *A* **q-to-1 map** *τ is a map from $GF(q^n)$ to $GF(q^n)$ where the preimage of any element in $Im(\tau)$ has exactly q elements.*

This approach was inspired by the paper by Maschietti [MA] which gave a connection between cyclic difference sets with the classical parameters (for $q = 2$) and geometric constructions which can be described by such maps.

As an example of such a construction:

Theorem 3.27 *(Dillon and Dobberton) [Xi]*

Let k be a positive integer with $k < n$ and $gcd(k, n) = 1$. Then the nonzero elements

in the image of $GF(2^n)$ *under the map* $x \mapsto x^e + (x+1)^e + 1$ where $e = 2^{2k} - 2^k + 1$ *form a difference set with parameters (3.23) in* $GF(2^n)^*$.

We finish off this section by giving the most recent and very general theorem due to No [No]. This follows the first of the two patterns given above, and requires a few definitions:

Definition 3.28 *A function* $f : GF(q^n) \to GF(q)$ *is* **d-homogeneous** *if* $f(yx) = y^d f(x)$ *for all* $x \in GF(q^n)$, $y \in GF(q)$.

Definition 3.29 *A function* $f : GF(q^n) \to GF(q)$ *is* **balanced** *if* $|f^{-1}(0)| = |f^{-1}(x)| - 1$ *for all* $x \in GF(q)^*$.

Definition 3.30 *A function* $f : GF(q^n) \to GF(q)$ *is* **difference-balanced** *if the function* $g_\tau(\alpha^t) := f(\alpha^{t+\tau}) - f(\alpha^t)$ *is balanced for all* $1 \leq \tau \leq q^n - 2$ *(where* α *is a primitive element in* $GF(q^n)$*.)*

No proved the following as his Main Theorem:

Theorem 3.31 *[No] Let* f *be a d-homogeneous function mapping* $GF(q^n) \to GF(q)$ *for* $gcd(d, q-1) = 1$. *If* f *is difference balanced, then the set of integers defined by*

$$D = \{t \mid f(\alpha^t) = 0,\ 0 \leq t < \frac{q^n - 1}{q - 1}\}$$

form a cyclic difference set with parameters (3.23)

No observes that the maps used for the Singer, Gordon-Mills-Welch, and cascaded GMW sequences mentioned above are d-homogeneous and difference balanced (using heavily the fact that the trace function itself has these properties) and then finds other such maps leading to a new infinite family of cyclic difference sets with parameters (3.23). We show in chapter 5 that the larger field context of $GF(q^n)$ in No's Theorem is inessential.

3.3 Algebraic Methods vs. Combinatorial Requirements

Certain difficulties repeatedly arise in the study of group ring elements such as difference sets. These difficulties are primarily due to the interplay between the combinatorial description of the objects and the algebraic methods used to study them.

In this section and the next, we highlight some of these difficulties. First we note that staying close to the combinatorial context often leads to a proliferation of cases: a 'combinatorial explosion.' In the remainder of the section we discuss the delicate balance between the powerful algebraic character techniques and the subtle combinatorial requirements of integrality and set-ness.

The algebraic tools useful to the study of abelian difference sets fall into two broad classes: the use of group homomorphic images (this includes the finite field approaches) and the application of complex group characters.

First consider the group homomorphic image approach, which is the more combinatorial of the two classes. The typical use of group homomorphic images was described in the last section. Note that this approach essentially amounts to computing possible distributions of a difference set in a group G among the cosets gH: a counting problem. Integrality (and set-ness) can be preserved during this process. The difficulty in group homomorphic image techniques is with the 'combinatorial explosion.' One is often overwhelmed by the number of cases to consider and by the requirement that pre-images of solutions arising from different subgroups H of G fit together as a set in the larger context of $\mathbb{Z}G$.

The more algebraic of the two methods is the use of complex group characters. As mentioned in the last section the idea is to apply a group character to a group ring equation like 3.3 and then solve the resulting equation ($\delta\overline{\delta} = n$).

If we apply a complex character and work in the algebraically closed field $\mathbb{C}$ the

algebraic problem is completely solved, but we also completely lose track of integrality and thus also set-ness.

The usual solution is to stay closer to the combinatorial context and work in the number ring $\mathbb{Z}[\zeta_v]$ where $v = exp(G)$. This makes sense, since for all A in $\mathbb{Z}G$ and any complex character χ of G, the character value $\chi(A)$ is in $\mathbb{Z}[\zeta_v]$.

There are still problems with the number ring approach however. In the number ring for example, solutions δ to $\delta\overline{\delta} = n$, viewed as character values, have pre-images in $(\frac{1}{v}\mathbb{Z}[\zeta_v])G$ by the inversion formula (Corollary 2.13). Thus, coefficients are not just 0 and 1 and so the set-ness problem is not completely solved.

Other problems lie with the number ring itself. $\mathbb{Z}[\zeta_v]$ is not a UFD in general, so when solving problems that are essentially factorizations (like $\delta\overline{\delta} = n$) we must work with ideals and not with elements. But combinatorial questions require discussion of specific elements. On this issue, Schmidt [Sc] observes 'the required complete knowledge of cyclotomic integers of prescribed absolute value ... is a problem of algebraic number theory far beyond the scope of our present knowledge.'

Attempts to deal with these issues often lead to restrictive conditions on the parameters of the difference sets that can be studied. As we saw in section 3.2, for example, Turyn used the self-conjugacy requirement to avoid the difficulties of working in $\mathbb{Z}[\zeta_v]$ in the general case.

In section 5.4 we will see specific difficulties that arise when we attempt to use the number ring to factor certain group ring elements.

The overall problem is this: The closer we stay to integrality and the combinatorial context the more intractible the computations become. On the other hand, the closer we move toward the algebraic realm (and $\mathbb{C}$) the more difficult it is to retain integrality and set-ness.

3.4 Problems

In this section we present some conjectures that are still outstanding, followed by a discussion of the difference set context for factoring certain group ring elements. We also introduce some of the difficulties encountered when trying to factor in the number ring.

The conjectures below share two critical features. First, their statements link specifically algebraic properties to purely combinatorial objects, and second, they do not seem to be particularly amenable to the established techniques - in particular neither can be settled by group homomorphic image techniques.

The first is a conjecture of John Dillon. This conjecture is an especially good illustration of the difficulties encountered in passing information between the algebraic and combinatorial realms. On the one hand, if you drop the combinatorial condition of set-ness (or even of set size) there are counter-examples. On the other hand the usual character techniques don't clearly distinguish between faithful and nonfaithful characters as this conjecture requires.

Conjecture 3.32 *(Dillon) [Di]*
Let D be any $(2^m - 1, 2^{m-1}, 2^{m-2})$ cyclic difference set. (These are the classical parameters (3.23) with $q = 2$). Let $Z_v =< x >$. Identify the group ring $\mathbb{Z}/(2)$ with polynomials mod $(x^v - 1)$, so that D is a polynomial in x. Then the minimal degree annihilator of the polynomial D in R (the **check polynomial** *) has a primitive polynomial of degree m over $\mathbb{Z}/(2)$ as a factor.*

Equivalently, by Theorem 2.30 there is a faithful representation φ such that $\varphi(D) \not\equiv 0 \bmod \pi$ where π is a prime ideal above (2) in $\mathbb{Z}[\zeta_v]$.

From the second statement, it is clear that Dillon's conjecture cannot be settled using either group homomorphic image techniques (since the characters of interest

are faithful), or by complex characters (since we are to work modulo a prime ideal over (2)).

A second conjecture relates directly to the p-rank of difference sets and is due to Hamada. We first need to define p-rank of a group ring element:

Definition 3.33 *Let A be any element of the group ring RG and let $\Psi(A)$ be the image of A under the regular representation (so that $\Psi(A)$ is a (0,1)-matrix). Then the* **p-rank of** *A is the rank of the matrix $\Psi(A)$ over the field $GF(p)$.*

If A corresponds to a difference set, then the image of A under Ψ is the incidence matrix of the symmetric design obtained from A. Thus the definition above corresponds to the more usual definition of p-rank for a difference set as the p-rank of the incidence matrix of the design.

Conjecture 3.34 *(Hamada, 1973)(cf [Xi]) Let D be a difference set with parameters (3.23) where $q = p^e$. Then the p-rank of D is at least $(\frac{p+n-2}{n-1})^e + 1$ with equality if and only if D is a 'Singer' difference set.*

For $q = 2$ this conjecture was proven by Hamada and Ohmori in 1975.

The p-rank is of combinatorial interest for several reasons. For example, since the p-rank of an element is fixed under shifts and automorphisms of the group, the p-rank can be used to show that difference sets given by different constructions are inequivalent.

We will note in chapter 5 that the p-rank of an element D can easily be computed if the value of $\varphi(D)$ is known modulo a prime ideal π over (p) for all representations φ of Z_v. As with Dillon's conjecture, this information is lost under homomorphic images.

Our next conjecture stems from an observation of Pott. Pott observed [Pott, p. 75] that while there are some examples of non-abelian difference sets with the classical parameters (3.23), there is **no** abelian, non-cyclic example known. The field approach described in section 3.2 only gives constructions for difference sets in **cyclic** groups, or (in the case of cyclotomy) in the additive group of $GF(q)$. (There are other constructions for difference sets in abelian, non-cyclic groups (in particular for elementary abelian groups) but these constructions are for the case that $gcd(v, n) > 1$ which fails for the classical parameters.)

Conjecture 3.35 *There are non-cyclic difference sets with parameters(3.23).*

Given the number of open questions about difference sets with parameters (3.23), along with the relative abundance and usefulness of these sets, there is great interest in knowing all difference sets (up to equivalence) with these parameters. A classification would be ideal, but seems to be a long way off. Exhaustive ennumerations have been done for $v = 2^t - 1$ for all $2 \leq t \leq 10$ with little use of the faithful characters. Searches for $t > 10$ will likely require far more information from the faithful characters.

Conjecture 3.36 *No efficient method for exhaustively enumerating (cyclic) difference sets with perscribed parameter set can ignore the faithful characters.*

In the remainder of this section we discuss a combinatorial context for the factorization of group ring elements.

Example 3.37 *The difference set equation* $DD^{(-1)} = (k-\lambda)1_G + \lambda G$ *displays* D *and* $D^{(-1)}$ *as factors of the group ring element* $(n-\lambda)1_G + \lambda G$.

Product constructions can be viewed as factorizations of the object constructed. For example Ionin [Io] gives conditions on the parameters of a relative difference set

R in G (relative to a subgroup N), and a difference set D in N so that the group ring product RD is a divisible difference set in G relative to N.

An even more striking example is the Gordon-Mills-Welch Theorem. We saw this construction in section 3.2 as a composition of twisted trace functions. The formulation below is (largely) due to Pott [Pott, p.75]. Instead of using the trace trace map, this version emphasizes the factorization of the Singer difference set into the product of a relative difference set and a difference set in a subgroup of G.

Theorem 3.38 *(Gordon Mills Welch) Let $t = sr$, $v = 2^t - 1$ and $w = 2^s - 1$. Then:*

1. *Any Singer $(2^t - 1, 2^{t-1} - 1, 2^{t-2} - 1)$ difference set can be expressed in the group ring $\mathbb{Z}Z_v$ in factored form as*

$$D_v = D_w R.$$

D_w is a Singer $(2^s - 1, 2^{s-1} - 1, 2^{s-2} - 1)$ difference set and R is a relative $(v/w, w, 2^{st-t}, 2^{st-2t})$ difference set.

2. *If $\hat{D}_w$ is any $(2^s - 1, 2^{s-1} - 1, 2^{s-2} - 1)$ difference set, then $\hat{D}_v$ defined by*

$$\hat{D}_v = \hat{D}_w R$$

for R as above is <u>also</u> a $(2^t - 1, 2^{t-1} - 1, 2^{t-2} - 1)$ difference set. Furthermore, $\hat{D}_v$ is equivalent to D_v if and only if $\hat{D}_w$ is a cyclic shift of D_w.

Note a few key properties in the examples above:

- Each factor satisfies some group ring equation. For these examples the product of an element and its image under the automorphism $x \mapsto x^{-1}$ is specified.
- The factors (and their products) are integral. They are also fixed by a multiplier group. For combinatorial applications the factors represent sets.

- At least one of the factors may be supported entirely in a subgroup of G. (This can be used to ensure the set-ness of the product.)

One approach to this problem is to use group characters and try to find factorizations of elements $\delta = \chi(D)$ in the number ring $\mathbb{Z}[\zeta_v]$. The difficulty we encounter is with divisibility in $\mathbb{Z}[\zeta_v]$. The number ring is a Dedekind domain, not a UFD, and so we can uniquely factor the ideal (δ) but not the element δ itself.

Using the ideal factorization approach, we suppose that $(\delta) = I_1 I_2 \ldots I_t$ for some prime ideals I_k in $\mathbb{Z}[\zeta_v]$. Then we seek an ideal I which is a product of some subset of $\{I_1, I_2, \ldots I_t\}$ and which is also principal (thus corresponding to a group ring element). This is not an easy problem in general.

In chapter 5 we will return to this question, using special properties of the group ring element to be factored in order to find further conditions on the possible ideals considered. We will also give an algorithm to find all factors of the element modulo some power of a prime p, avoiding the complications of the number ring completely.

4 The Association Scheme $\mathcal{C}(G, \Lambda)$

In this chapter we define the cyclotomic coset association schemes $\mathcal{C}(G, \Lambda)$ constructed from an abelian group G and a subgroup Λ of the automorphism group of G. These schemes are a generalization of both cyclotomic association schemes (as defined by [BM], etc.) and of the cyclotomy methods of Storer [St]. These schemes also build in certain combinatorial conditions. In particular, Λ can be viewed as the multiplier group of a difference set. Any difference set satisfying the multiplier conjecture must have a member of its equivalence class in the scheme $\mathcal{C}(G, \Lambda)$ where Λ is generated by the multiplier(s).

In section 1 we define the scheme $\mathcal{C}(G, \Lambda)$, first as a matrix algebra (as in chapter 2), and then as a subalgebra of the integral group ring $\mathbb{Z}G$. We also define cyclotomic and translation schemes in this context. We also give a basic construction of the character table $P(G, \Lambda)$ of the scheme.

In section 4.2 we work out some properties of these schemes, concentrating on those which will be useful for applications to combinatorics. The semidirect product group $G \rtimes \Lambda$ of G with Λ is used to help interpret how changes in G and in Λ affect the scheme $\mathcal{C}(G, \Lambda)$ and its character table.

Section 4.3 contains properties of the character tables $P(G, \Lambda)$ of $\mathcal{C}(G, \Lambda)$ over $\mathbb{Z}[\zeta_v]$ and also modulo certain prime ideals. One aim is efficient computation of the character table for applications. A formula for the inverse of P is also given.

In section 4.4 we describe special cases for G and for Λ: in particular the cyclotomic association scheme case (where G is the additive group of $GF(q)$) and the integral group ring case (where Λ is the identity). We apply properties from this chapter to the example $\mathcal{C}(Z_v, \Lambda)$ where $v = 2^{11} - 1$ and Λ is the multiplier group $< \sigma : x \mapsto x^2 >$.

4.1 Definition of $\mathcal{C}(G, \Lambda)$ and $P(G, \Lambda)$

Let G be any finite abelian group and let Λ be a subgroup of $Aut(G)$. Then Λ acts on G as a group of permutations. Label the orbits of this action $C_0 = \{1_G\}, C_1, \ldots, C_d$. We call these orbits the **Λ-cyclotomic cosets** of the scheme. We generally suppress the Λ when it is clear from the context and simply refer to the **cyclotomic cosets** of the scheme. (The term cyclotomic coset is taken from the difference set context.)

Lemma 4.1 *Define relations $\mathcal{R}_i$ for $0 \leq i \leq d$ by*

$$\mathcal{R}_i = \{(\alpha, \beta) \mid \alpha, \beta \in G, \alpha\beta^{-1} \in C_i\}$$

Define the matrices A_i for $0 \leq i \leq d$ with rows and columns indexed by a given ordering of the elements of G by:

$$(A_i)_{(\alpha,\beta)} = \begin{cases} 1 & \text{if } \alpha\beta^{-1} \in C_i \\ 0 & \text{else.} \end{cases}$$

Then the relations $\mathcal{R}_i$ (and thus also the matrices A_i) satisfy the conditions given in chapter 2 for a commutative association scheme.

Proof:

- $\alpha\mathcal{R}_0\alpha$ for all $\alpha \in G$ since $\alpha\beta^{-1} = 1_G$ if and only if $\alpha = \beta$.
- The disjoint union $\cup_{i=0}^{d}\mathcal{R}_i = G \times G$ since the C_i partition the elements of G.
- To see that $\alpha\mathcal{R}_i\beta$ if and only if $\beta\mathcal{R}_{i'}\alpha$ for some i', note that the automorphism $\tau : x \mapsto x^{-1}$ permutes the cyclotomic cosets so that $\alpha\beta^{-1} \in C_i$ if and only if $\beta\alpha^{-1} \in \tau(C_i) = C_{i'}$.
- For the fourth property, we need to show that the number of $g \in G$ such that $\alpha g^{-1} \in C_i$ and $g\beta^{-1} \in C_j$ is constant for $\alpha\beta^{-1} \in C_k$ (and then we may denote

this constant p_{ij}^k.)

To check this note that $\alpha\beta^{-1} \in C_k$ if and only if $\alpha\beta^{-1} = c$ for some $c \in C_k$. This happens if and only if $\alpha g^{-1} g\beta^{-1} = c$ for all $g \in G$. So the number of $g \in G$ with $\alpha g^{-1} \in C_i$ and $g^{-1}\beta \in C_j$ is the number of solutions to $c = c_i c_j$ for fixed $c \in C_k$, and any $c_i \in C_i$, $c_j \in C_j$. This number is independent of the choice of α and β.

- and finally, $p_{ij}^k = p_{ji}^k$ since G is commutative. ∎

Definition 4.2 *Define the* **cyclotomic coset association scheme** $\mathcal{C}(G, \Lambda)$ *to be the scheme defined in Lemma 4.1.*

$\mathcal{C}(G, \Lambda)$ is defined for abelian groups G and any subgroup Λ of $Aut(G)$. If G were not abelian, all that would be lost in the above is commutativity. For non-abelian groups there is the related construction of the **class algebra** in which the automorphism group Λ is the set of all inner automorphisms of G (those given by group conjugation).

We also note that 'cyclotomic coset scheme' is our terminology and should not be confused with the special case of cyclotomic association schemes (cf. [BCN], [BM], [GC]) described below.

Remark *The third property in Lemma 2.3 implies that the scheme $\mathcal{C}(G, \Lambda)$ is only symmetric when the automorphism $x \mapsto x^{-1}$ is in Λ. (This condition restricts character values of elements of such a scheme to numbers satisfying Turyn's definition of self-conjugacy given in chapter 3.) Since cyclic difference sets never have -1 as a multiplier (cf. [Bau, p.60]), the schemes for such applications are never symmetric.*

We must also point out here that the cyclotomic cosets C_i of $\mathcal{C}(G, \Lambda)$ are formal sums of orbits under Λ and always have $(0, 1)$-coefficients when viewed as elements of

the integral group ring $\mathbb{Z}G$. Orbit sizes may vary among divisors of $|\Lambda|$. This is one property that distinguishes $\mathcal{C}(G, \Lambda)$ from cyclotomic association schemes.

$\mathcal{C}(G, \Lambda)$ has been defined as an association scheme and thus via Lemma 2.3 as a subalgebra of $\mathrm{Mat}_v(\mathbb{Z})$. We usually prefer to view $\mathcal{C}(G, \Lambda)$ as a subalgebra of the group ring $\mathbb{Z}G$ generated by the cyclotomic cosets. In particular, the structure constants p_{ij}^k of the scheme have a nice interpretation in the group ring.

Proposition 4.3 *$\mathcal{C}(G, \Lambda)$ is isomorphic to the subalgebra of $\mathbb{Z}G$ generated by the cyclotomic cosets C_i. The structure constants p_{ij}^k are the coefficients of C_k in the group ring product C_iC_j.*

Proof: Using the conventions from chapter 3, for any subset $S \subseteq G$ let S also denote the formal sum in the group ring of the elements of S. Then each cyclotomic coset C_i is fixed in $\mathbb{Z}G$ under the automorphism group Λ, as is any product of the C_i: therefore, $C_iC_j = \sum_{k=0}^{d} a_{ij}^k C_k$. Let these C_i generate a subalgebra of $\mathbb{Z}G$. Under the mapping $C_i \leftrightarrow A_i$; this subalgebra is (additively) isomorphic to the matrix algebra $\mathcal{C}(G, \Lambda)$, and since $p_{ij}^k = a_{ij}^k =$ the number of solutions to $c = c_ic_j$ for fixed $c \in C_k$, any $c_i \in C_i$, $c_j \in C_j$, this is also an algebra isomorphism. In addition, the argument above shows that the structure constants p_{ij}^k are the coefficients of C_k in the group ring product C_iC_j. ∎

In what follows, when we view $\mathcal{C}$ as a subalgebra of $\mathbb{Z}G$, we will refer to the formal orbit sums C_i as elements of the scheme.

Next we place $\mathcal{C}(G, \Lambda)$ in the context of cyclotomic association schemes and translation schemes.

Definition 4.4 *(cf. [BCN, p.65]) An association scheme defined on a set X of points and a set of relations $\{R_i\}$ is called a* **translation association scheme** *if X has*

the structure of an abelian group and the elements of the scheme satisfy the condition $xR_iy \Rightarrow xzR_iyz$ *for all* $z \in X$.

Lemma 4.5 $\mathcal{C}(G, \Lambda)$ *is a translation scheme.*

Proof: In $\mathcal{C}(G, \Lambda)$ the definition of a translation scheme is simply the condition that $\alpha\beta^{-1} \in C_i \Rightarrow (\alpha\gamma)(\beta\gamma)^{-1} \in C_i$ for all $\gamma \in G$. ■

The term " cyclotomic scheme" has already been used (cf. [BCN], [GC], [BM]), for the special case that G is the additive group of $GF(q)$: The definition below is from [BM]:

Definition 4.6 *Let* q *be a prime power,* e *a divisor of* $(q-1)$ *and* α *a primitive root in* $GF(q)$. *Define relations* $R_0 = \{(x, x)\ x \in GF(q)\}$ *and*

$$R_i = \{(x, y) \mid x, y \in GF(q), x - y \in < \alpha^e > \alpha^{i-1}\} \text{ for } 1 \leq i \leq e$$

The association scheme $(GF(q), \{R_i\})$ *is called the* **cyclotomic scheme of class e on** $GF(q)$.

In some of the literature (eg. [GC]) on cyclotomic schemes it is also noted that more generally, the orbits of a group under an automorphism group form a scheme. However, the focus in these papers is the special case of the cyclotomic association scheme.

Brauer, Cohen and Neumaier give the following connection between translation schemes and cyclotomic schemes:

Theorem 4.7 *[BCN, p.66]*
Any translation association scheme with a prime number of points is a cyclotomic association scheme.

We make the connection between a cyclotomic coset scheme with a prime number of points and a cyclotomic scheme on $GF(p)$ explicit since we will use the character table construction from [BM] in section 4. The subgroup $< \alpha^e >$ in Bannai and Munemasa's definition has index e in $GF(p)^*$ and therefore order $f = (p-1)/e$.

Lemma 4.8 *Let p be prime, and let Λ be the unique automorphism group of order $f = (p-1)/e$ the additive group of $GF(p)$. Then the cyclotomic association scheme of class e on $GF(p)$* **is** *$C(Z_p, \Lambda)$.*

We will see in the last section of this chapter that in general, cyclotomic schemes for any $GF(q)$ are a special case of cyclotomic coset schemes where G is the elementary abelian group of the additive structure of $GF(q)$.

The character table for the scheme $C(G, \Lambda)$ is of particular interest and will be denoted $P(G, \Lambda)$, or just P when G and Λ are clear from the context. The general definition of the character table of an association scheme given in chapter 2 is somewhat unwieldy for our purposes. There are, however, several alternate constructions of $P(G, \Lambda)$ in our case which we can use instead. The first requires a lemma:

Lemma 4.9 *Fix an irreducible character χ of G and form the vector $\underline{\chi}$ by $(\underline{\chi})_g := \chi(g)$ using the same ordering as the indices in the adjacency matrices A_j. Then the vector $\underline{\chi}$ is an eigenvector for each A_j with eigenvalue $\chi(C_j) := \sum_{\gamma \in C_j} \chi(\gamma)$.*

Proof: Let $\beta = \alpha\gamma$. The α-th row of A_j has a 1 exactly at positions labelled by $\{\alpha\gamma \mid \gamma^{-1} \in C_j\}$ (since β runs over G if and only if $\alpha\gamma$ runs over G, and $\alpha\beta^{-1} \in C_j$ if and only if $\alpha(\alpha\gamma)^{-1} \in C_j$ if and only if $\gamma^{-1} \in C_j$.) This means the matrix product $A_j\underline{\chi}$ has α-th entry

$$\sum_{\gamma \in C_{j'}} \chi(\alpha)\chi(\gamma) = \chi(\alpha)(\sum_{\gamma \in C_{j'}} \chi(\gamma))$$

(since $\gamma^{-1} \in C_j \Leftrightarrow \gamma \in C_{j'}$.)

$\chi(\alpha)$ is the α-th entry of the vector $\underline{\chi}$ and the sum $\sum_{\gamma \in C_{j'}} \chi(\gamma)$ is the corresponding eigenvalue. ■

Recall that the (i,j)-entry of the matrix P was defined in chapter 2 to be the eigenvalue of the matrix A_j on the maximal common eigenspace V_i.

Lemma 4.10 *Label the columns of P by the cyclotomic cosets C_j of $\mathcal{C}(G,\Lambda)$. The i^{th} eigenspace V_i may be represented by some irreducible character χ_i of G and the (i,j)-entry of P is $\chi_i(C_{j'})$.*

Proof: The character table of G gives us $|G|$ linearly independent eigenvectors. We group these into the maximal common eigenspaces V_i. (Two irreducible characters χ and $\hat{\chi}$ are in the same eigenspace if and only if $\chi(C) = \hat{\chi}(C)$ for all cyclotomic cosets C in $\mathcal{C}$). The eigenvalue of A_j on V_i will be $\sum_{\gamma \in C_{j'}} \chi_i(\gamma) = \chi_i(C_{j'})$ by Lemma 4.9. Therefore, $(P)_{ij} = \chi_i(C_{j'})$. ■

Example 4.11 *Let G be the cyclic group $Z_{23} =< x \mid x^{23} = 1 >$ and let*
$\Lambda_{23} =< \sigma \mid \sigma(x) = x^2 >$.
For this example, we can compute
$Aut(G) = \Lambda_{23} \times \Theta_{23}$ *where* Θ_{23} *is* $< \tau_{23} \mid \tau_{23}(x) = x^{-1} >$.
Since Θ_{23} permutes the non-identity cyclotomic cosets under Λ transitively, the orbit sums of G under Λ can be written as

$$\begin{aligned} C_0 &= 1 \\ C_1 &= x + x^2 + x^4 + x^8 + x^{16} + x^9 + x^{18} + x^{13} + x^3 + x^6 + x^{12} \\ C_{-1} &= \tau_{23}(C_1) \end{aligned}$$

(Here we follow the standard difference-set practice of labelling cyclotomic cosets

by an element of the coset. For cyclic groups an exponent of the generator is used. In this example they are chosen to reflect the action of τ.)

There are $d+1 = 3$ maximal common eigenspaces. The trivial eigenspace represented by $\chi_0 : x \mapsto 1$ has eigenvalue $|C_j|$ on each A_j. We next choose (somewhat arbitrarily) $\chi_1 : x \mapsto \zeta_{23}$ as a representative for the eigenspace V_1. χ_1 has character values $\chi_1(1) = 1$, $\chi_1(C_1) = \alpha = \zeta_{23} + \zeta_{23}^2 + \ldots + \zeta_{23}^{12}$, and $\chi_1(C_{-1}) = \overline{\alpha}$, where $\overline{\alpha}$ is the complex conjugate of α.

The automorphism which interchanges C_1 and C_{-1} also acts to swap the two non-trivial eigenspaces. We choose the character $\chi_{-1} : x \mapsto \zeta_{23}^{-1}$ to represent the last eigenspace. Then

$$P(Z_{23}, \Lambda_{23}) = \begin{array}{c|ccc} & C_0 & C_{-1} & C_1 \\ \hline \chi_0 & 1 & 11 & 11 \\ \chi_1 & 1 & \alpha & \overline{\alpha} \\ \chi_{-1} & 1 & \overline{\alpha} & \alpha \end{array}$$

Since we will use this example again, we note here that $\alpha + \overline{\alpha} = -1$, and $\alpha\overline{\alpha} = 6$. Another feature of this particular example should be pointed out. The orbits of G under Λ partition the non-identity elements of Z_{23} into the set of squares and the set of non-squares. Since $23 \equiv 3 \bmod 4$, C_1 (the set of squares) is a $(23, 11, 5)$-Payley difference set (see Theorem 3.21), with $n = \alpha\overline{\alpha} = 6$.

As a contrast to the N^{th}-power construction exemplified above, and also because we will need this character table in a future example, we include the following:

Example 4.12 *Let $G = Z_{89} =< y \mid y^{89} = 1 >$ and let $\Lambda_{89} =< \sigma \mid \sigma(y) = y^2 >$.*
As in example 4.11, we seek an automorphism group which will permute the (non-identity) cyclotomic cosets. $Aut(Z_{89}) \cong Z_{88}$ and $|\Lambda|$ has order 11, so we seek an automorphism of order 8. Let $\Theta_{89} =< \tau \mid \tau(y) = y^{12} >$. Then we can check that $Aut(G) = \Lambda_{89} \times \Theta_{89}$. As in the first example, Θ_{89} permutes the non-identity cyclotomic

cosets under Λ_{89} *transitively, so the orbit sums of* G *under* Λ_{89} *can be written as images of* C_1 *under* Θ_{89}. *Let* $\Delta := y+y^2+y^4+y^8+y^{16}+y^{32}+y^{64}+y^{39}+y^{78}+y^{67}+y^{45}$. *Then* $C_0 = 1$ *and*

$$\begin{array}{ll} C_1 = \Delta & C_{-1} = \tau^4(\Delta) \\ C_3 = \tau(\Delta) & C_{-3} = \tau^5(\Delta) \\ C_9 = \tau^2(\Delta) & C_{-9} = \tau^6(\Delta) \\ C_{27} = \tau^3(\Delta) & C_{-27} = \tau^7(\Delta) \end{array}$$

Choose a representative χ_i *for each* V_j *as in the first example to get* $P(Z_{89}, \Lambda_{89}) =$

	1	C_{-1}	C_{-3}	C_{-9}	C_{-27}	C_1	C_3	C_9	C_{27}
χ_0	1	11	11	11	11	11	11	11	11
χ_1	1	β	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$
χ_3	1	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$	β
χ_9	1	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$	β	$\tau(\beta)$
χ_{27}	1	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$	β	$\tau(\beta)$	$\tau^2(\beta)$
χ_{-1}	1	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$	β	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$
χ_{-3}	1	$\tau^5(\beta)$	$\tau^6(\beta)$	$\tau^7(\beta)$	β	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$
χ_{-9}	1	$\tau^6(\beta)$	$\tau^7(\beta)$	β	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$
χ_{-27}	1	$\tau^7(\beta)$	β	$\tau(\beta)$	$\tau^2(\beta)$	$\tau^3(\beta)$	$\tau^4(\beta)$	$\tau^5(\beta)$	$\tau^6(\beta)$

where $\beta = \chi_1(C_1)$ *and* $\tau(\beta)$ *denotes the Galois map* $\zeta_{89} \mapsto \zeta_{89}^{12}$ *applied to* β.

Both of the examples above illustrate the (particularly nice) case that $G = Z_p$ for p prime. Recall that for this case $\mathcal{C}(G, \Lambda)$ is a cyclotomic association scheme. A special construction for P in this situation is given in [BM] and appears in section 4.4. Note especially that all the non-identity cyclotomic cosets are the same size in this special case. We will include an example which is not a cyclotomic scheme below.

Another view of this construction of P will be useful. We can get from a character table $\chi(G)$ of G to a character table for the scheme $\mathcal{C}(G, \Lambda)$ by taking row sums of an appropriate block matrix.

Arrange the columns of a character table $\chi(G)$ for G into blocks corresponding to orbits under the automorphism group Λ. Form the $(d+1) \times |G|$ matrix by taking row

sums of the blocked matrix. The above lemmas show that there will be only $(d+1)$ distinct rows in this matrix, and these $(d+1)$ rows can be taken to be the matrix P.

Example 4.13 *As a contrast to the cyclotomic case we include the small example* $P(Z_{15}, \Lambda)$ *where* $\Lambda =< \sigma : x \mapsto x^2 >$. *The cyclotomic cosets are:*

$C_0 = 1,$

$C_5 = x^5 + x^{10}$

$C_3 = x^3 + x^6 + x^{12} + x^9$

$C_1 = x + x^2 + x^4 + x^8$

$C_{-1} = x^{14} + x^{13} + x^{11} + x^7$

Using the construction discussed above, we find the $d+1$ *distinct rows of the* 5×15 *matrix described above and compute the* (χ_i, C_j)*-entry of* P *as* $\chi_i(C_{j-1})$

$$P(Z_{15}, \Lambda) = \begin{array}{c|ccccc} & 1 & C_5 & C_3 & C_{-1} & C_1 \\ \hline \chi_0 & 1 & 2 & 4 & 4 & 4 \\ \chi_5 & 1 & -1 & 4 & -2 & -2 \\ \chi_3 & 1 & 2 & -1 & -1 & -1 \\ \chi_1 & 1 & -1 & -1 & \gamma & \bar{\gamma} \\ \chi_{-1} & 1 & -1 & -1 & \bar{\gamma} & \gamma \end{array}$$

where $\gamma = \zeta_{15} + \zeta_{15}^2 + \zeta_{15}^4 + \zeta_{15}^8$. *(Note the orbit of size* 2. *This is not a cyclotomic association scheme.)*

In the next section we will see the action of Λ on the character group G^* of G which groups characters into orbits corresponding to the maximal common eigenspaces of the A_i.

4.2 Properties of $\mathcal{C}(G, \Lambda)$ and $P(G, \Lambda)$

In this section we work out some properties of $\mathcal{C}(G, \Lambda)$ as G and Λ vary, and the corresponding properties of its character table P.

To make this second task easier we first show that the character table $P(G,\Lambda)$ is embedded in the group character table of the semi-direct product group $\mathcal{G} = G \rtimes \Lambda$ of G with Λ. This gives an additional construction for $P(G,\Lambda)$.

Recall that for $\Lambda \leq Aut(G)$ we define

$$\mathcal{G} := G \rtimes \Lambda =< g\lambda \,:\, g \in G,\ \lambda \in \Lambda,\ \lambda^{-1}g\lambda = \lambda(g) > .$$

Since G is normal in $\mathcal{G}$, G is a union of conjugacy classes in $\mathcal{G}$. The definition implies that the conjugacy classes comprising G in $\mathcal{G}$ are exactly the orbits of G under the automorphism group Λ.

Theorem 4.14 *Let $\mathcal{G} = G \rtimes \Lambda$, let χ be an irreducible character of G and let $g \in G$. Let C_g be the cyclotomic coset containing g in $\mathcal{C}(G,\Lambda)$. Then the induced character $\chi^{\mathcal{G}}$ satisfies:*

$$\chi^{\mathcal{G}}(g) = (|\Lambda|/|C_g|)\chi(C_g).$$

(and thus the $(\chi, C_{g'})$ entry $\chi(C_g)$ of P is $(|C_g|/|\Lambda|)\chi^{\mathcal{G}}(g)$).

Proof:

The induced character is defined (Lemma 2.19) as:

$$\chi^{\mathcal{G}}(\alpha) = \frac{1}{|G|}\sum_{y\in\mathcal{G}} \tilde{\chi}\,(y^{-1}\alpha y) \text{ where } \tilde{\chi}\,(\beta) = \begin{cases} \chi(\beta) & \text{if } \beta \in G \\ 0 & \text{else.} \end{cases}$$

for α in $\mathcal{G}$

Since G is normal in $\mathcal{G}$, for $g \in G$ we have $y^{-1}gy \in G$ for all $y \in \mathcal{G}$. Also, if y and y_1 are in the same coset of $\mathcal{G}/G$ then $y^{-1}gy = y_1^{-1}gy_1$. Because $\mathcal{G}/G \cong \Lambda$ we can choose elements of Λ as a transversal for $\mathcal{G}/G$. Then we may compute

$$\chi^{\mathcal{G}}(g) = \frac{1}{|G|}|G|\sum_{\lambda\in\Lambda}\chi(\lambda^{-1}g\lambda) = \sum_{\lambda\in\Lambda}\chi(\lambda(g)).$$

Since this is a sum over the whole group Λ we get $\chi^{\mathcal{G}}(g) = \chi(|\Lambda|/|C_g| \cdot C_g) = (|\Lambda|/|C_g|)\chi(C_g)$. ∎

Remark $\chi^{\mathcal{G}}(1) = |\Lambda|$ *for any irreducible character* χ *of* G.

The semidirect product construction gives us an action of Λ on the character group G^* of G that is compatible with the action of Λ on G:

Lemma 4.15 *[Is, p. 78] Let* χ *be an irreducible character of* G *and* γ *be an element of* $\mathcal{G}$. *Define* χ^γ *to be the map* $\chi^\gamma(\alpha) = \chi(\gamma\alpha\gamma^{-1})$ *for* $\alpha \in G$. *Then:*

1. χ^γ *is also an irreducible character of* G.
2. $(\chi^{\gamma_1})^{\gamma_2} = \chi^{\gamma_1\gamma_2}$, *and*
3. $\mathcal{G}$ *permutes the irreducible characters of* G *by* $\chi \mapsto \chi^\gamma$ *with* G *acting trivially: so* $\Lambda \cong \mathcal{G}/G$ *permutes the irreducible characters of* G.

Note that the definition of $\mathcal{G}$ implies that $\chi^\lambda(g) = \chi(\lambda^{-1}(g))$ for $g \in G$.

Definition 4.16 *Let* χ *be an irreducible character of* G. *Define the* **inertia group of** χ **in** $\mathcal{G}$ *to be* $I_{\mathcal{G}}(\chi) := \{\gamma \in \mathcal{G} \mid \chi^\gamma = \chi\}$

Lemma 4.17 *[Is, p.82]* $I_{\mathcal{G}}(\chi)$ *is a subgroup of* $\mathcal{G}$ *containing* G.

To see how $P(G, \Lambda)$ is embedded in the character table $\chi(\mathcal{G})$ for $\mathcal{G} = G \rtimes \Lambda$ we need to know when the induced character $\chi^{\mathcal{G}}$ is irreducible. Then we have the (χ, C_g^{-1}) entry of P given by a multiple of an irreducible character of $\mathcal{G}$.

Lemma 4.18 *[Is, p.95] If* χ *is an irreducible representation for* G, *then* $\chi^{\mathcal{G}}$ *is irreducible if and only if* $I_{\mathcal{G}}(\chi) = G$

Since G is abelian, G is isomorphic to its character group G^* by some isomorphism $\chi \mapsto g_\chi$. Then there is a stabilizer in Λ of χ if and only if there is a stabilizer in Λ of g_χ if and only if $|C_{g_\chi}| < |\Lambda|$.

Explicitly, $Stab_\Lambda(\chi) := \{\lambda \in \Lambda \mid \chi^\lambda = \chi\}$ is isomorphic to $Stab_\Lambda(g_\lambda)$. Thus:

Corollary 4.19 *Let χ be an irreducible character of G. Then χ^G is irreducible if and only if $|C_{g_\chi}| = |\Lambda|$*

Next we consider what happens to the scheme $\mathcal{C}(G, \Lambda)$ and more importantly, to its character table $P(G, \Lambda)$ when we pass from G to the quotient group G/H.

Let $H \leq G$ with $\Lambda(H) = H$. (This is always the case when Λ is generated by numerical multipliers.) Then, since Λ acts on G, Λ also acts on G/H by $\lambda(gH) = \lambda(g)H$. The condition $\Lambda(H) = H$ ensures that $H \trianglelefteq G \rtimes \Lambda$ and that the map is well defined.

Theorem 4.20 *Let $H \leq G$ with $\Lambda(H) = H$. Let η be the natural map $\eta : G \mapsto G/H$. Then a cyclotomic coset C in $\mathcal{C}(G, \Lambda)$ maps under η to a cyclotomic coset in $\mathcal{C}(G/H, \Lambda)$ and the character table $P(G/H, \Lambda)$ is embedded in the character table $P(G, \Lambda)$.*

Proof: g and g' are in the same cyclotomic coset in $\mathcal{C}(G, \Lambda)$ if and only if there is a $\lambda \in \Lambda$ with $g' = \lambda(g)$. Then $g'H = \eta(g') = \eta(\lambda(g)) = \lambda(g)H = \lambda(gH)$ so that $g'H$ and gH are in the same cyclotomic coset in $\mathcal{C}(G/H, \Lambda)$

Since $H \leq G$, representations of G/H are representations of G that are trivial on H. Thus the character table of $P(G/H, \Lambda)$ is embedded in the character table of $P(G, \Lambda)$ just as the group character table for G/H is embedded in the group character table for G. ■

Example 4.21 *For G the cyclic group Z_{15}, $H = Z_3$, and $\Lambda =< x \mapsto x^2 >$ we have the character table*

$$P(G/H, \Lambda) = \begin{array}{c|cc} & C_0 & C_1 \\ \hline \chi_0 & 1 & 4 \\ \chi_1 & 1 & -1 \end{array}$$

Compare this to the character table in example 4.13 and its characters χ_0 and χ_3 which are both trivial on $H \cong 1 \cup C_5$

Remark *Theorem 4.20 can also be seen as a consequence of the embedding of $P(G, H)$ in the character table of the semidirect product group $\mathcal{G}$ since $(G \rtimes \Lambda)/H \cong (G/H) \rtimes \Lambda$*

Also note that if $H \leq G$ with $\Lambda(H) = H$, the scheme $\mathcal{C}(H, \Lambda|_H)$ is a **subscheme** of $\mathcal{C}(G, \Lambda)$: The relations are a subset of the relations $\mathcal{R}_i$ for the full scheme. The character table for the subscheme is also embedded in the character table of the full scheme.

Example 4.22 *Again consider example 4.13, and $H = Z_5 \cong 1 \cup C_3$.*
The character table $P(Z_5, \Lambda|_H)$ is in the example just above. Compare to the result of deleting the columns in example 4.13 corresponding to C_5, C_{-1}, and C_1.

We will also need to take direct products:

Theorem 4.23 *For G, K abelian groups and Λ, Γ subgroups of $Aut(G)$ and $Aut(K)$ respectively, the product scheme:*
$\mathcal{C}(G, \Lambda) \times \mathcal{C}(K, \Gamma)$ is the scheme $\mathcal{C}(G \times K, \Lambda \times \Gamma)$.
The character table $P(G \times K, \Lambda \times \Gamma)$ of the product scheme is the Kronecker product $P(G, \Lambda) \otimes P(K, \Gamma)$.

Proof: The direct product of association schemes is an association scheme by Proposition 2.9. For this particular product, the Kronecker products of the adjacency matrices A_i from the scheme $\mathcal{C}(G, \Lambda)$ with those from $\mathcal{C}(K, \Gamma)$ are indexed by elements of $G \times K$ grouped into orbits formed by the automorphism group $\Lambda \times \Gamma$ under the action $(\lambda, \gamma)((g, k)) = (\lambda(g), \gamma(k))$. ∎

Example 4.24 *Let* $G = Z_{23} \times Z_{89} =< x, y \mid x^{23} = y^{89} = 1 >$,

$\Lambda_{23} =< \hat{\sigma} \mid x \mapsto x^2,\ y \mapsto y >$, *and*

$\Lambda_{89} =< \sigma \mid x \mapsto x,\ y \mapsto y^2 >$.

We computed $P_{23} = P(Z_{23}, \Lambda_{23})$ *in example 4.11, and* $P_{89} = P(Z_{89}, \Lambda_{89})$ *in example 4.12.*

$P(Z_{23} \times Z_{89}, \Lambda_{23} \times \Lambda_{89})$ *is the* 27×27 *Kronecker product of these matrices.*

$$\left(\begin{array}{c|c|c} P_{89} & 11P_{89} & 11P_{89} \\ \hline P_{89} & \alpha P_{89} & \overline{\alpha} P_{89} \\ \hline P_{89} & \overline{\alpha} P_{89} & \alpha P_{89} \end{array}\right)$$

We will work with this example again so we give the column labels explicitly. The column labels are orbits of $x^i y^j$ under the automorphism group $\Lambda_{23} \times \Lambda_{89}$. The vertical bars below show the blocks from the Kronecker product. In terms of the map $\tau : y \mapsto y^{12}$ from example 4.12, these labels are:

$$1 \quad y \quad \tau(y) \quad \ldots \quad \tau^7(y) \mid x \quad xy \quad \tau(xy) \quad \ldots \quad \tau^7(xy) \mid x^{-1} \quad x^{-1}y \quad \tau(x^{-1}y) \quad \ldots \quad \tau^7(x^{-1}y)$$

For the rest of this section we consider the effect of enlarging or shrinking the automorphism group Λ.

If Λ is a subgroup of some larger subgroup Γ of $Aut(G)$, then the scheme $\mathcal{C}(G,\Gamma)$ can be thought of as "those elements of $\mathcal{C}(G,\Lambda)$ which satisfy further restrictions imposed by the additional automorphisms in Γ." In the difference set context, Λ might be the standard multiplier group, while Γ represents the inclusion of an additional 'extraneous' multiplier.

Lemma 4.25 *If $\Gamma \leq \Lambda$, then $\mathcal{C}(G,\Lambda)$ is the result of fusing classes from $\mathcal{C}(G,\Gamma)$.*

Proof: This is just since G (and G^*) split into fewer orbits under the larger automorphism group Λ. ■ Such a scheme is called a **fusion scheme**.

Remark *Here we are viewing $\mathcal{C}(G,\Lambda)$ as a subalgebra of $\mathbb{Z}G$. In the matrix version of the scheme, the fusion of classes C_i and C_j is equivalent to summing the corresponding adjacency matrices A_i and A_j.*

Example 4.26 *Return to the situation of example 4.12 and let Λ' be the product $\Lambda_{89} \times < \tau^4 : y \mapsto y^{-1} >$. The nine $\Lambda_{89}-$cyclotomic cosets condense to five $\Lambda'-$cosets with the character table below. (We have replaced $\tau_i(\beta)$ by β_i.)*

$P(Z_{89},\Lambda') =$

	1	C_1	C_3	C_9	C_{27}
χ_0	1	22	22	22	22
χ_1	1	$\beta+\beta^{-1}$	$\beta_1+\beta_1^{-1}$	$\beta_2+\beta_2^{-1}$	$\beta_3+\beta_3^{-1}$
χ_3	1	$\beta_1+\beta_1^{-1}$	$\beta_2+\beta_2^{-1}$	$\beta_3+\beta_3^{-1}$	$\beta+\beta^{-1}$
χ_9	1	$\beta_2+\beta_2^{-1}$	$\beta_3+\beta_3^{-1}$	$\beta+\beta^{-1}$	$\beta_1+\beta_1^{-1}$
χ_{27}	1	$\beta_3+\beta_3^{-1}$	$\beta+\beta^{-1}$	$\beta_1+\beta_1^{-1}$	$\beta_2+\beta_2^{-1}$

We can get from $P(Z_{89},\Lambda_{89})$ to $P(Z_{89},\Lambda')$ by summing columns corresponding to the fused classes. (Also, note that since the automorphism $y \mapsto y^{-1}$ is in Λ' all entries in P are real.)

In the example above, we moved from one automorphism group (Λ_{89}) to a larger one (Λ'). More often, for applications we do the opposite. We want to build up schemes $\mathcal{C}(G, \Lambda)$ from 'smaller' schemes $\mathcal{C}(H_i, \Gamma_i)$, and while we may have $G = H_1 \times \cdots \times H_s$, the automorphism group Λ we really need in the application is a proper subgroup of $\Gamma_1 \times \cdots \times \Gamma_s$.

For $\Gamma \leq \Lambda$ the above lemma shows that $\mathcal{C}(G, \Gamma)$ is a refinement of $\mathcal{C}(G, \Lambda)$, also known as a **fission scheme**. A given cyclotomic coset C from $\mathcal{C}(G, \Lambda)$ splits into some number $t(C)$ cyclotomic cosets in $\mathcal{C}(G, \Gamma)$ We can compute this number.

Theorem 4.27 *Let $\Gamma \trianglelefteq \Lambda$. Then the cyclotomic coset C in $\mathcal{C}(G, \Lambda)$ splits into $t(C)$ cyclotomic cosets $C_1, \ldots C_{t(C)}$ of equal size in $\mathcal{C}(G, \Gamma)$. $t(C) = [\Lambda : \mathrm{Stab}_\Lambda(\alpha)]/[\Gamma : \mathrm{Stab}_\Gamma(\alpha)]$ for any fixed $\alpha \in C$.*

Proof: C is a conjugacy class in the semidirect product group $G \rtimes \Lambda$ with size $|C| = [G \rtimes \Lambda : \mathrm{Stab}_{G \rtimes \Lambda}(\alpha)] = [\Lambda : \mathrm{Stab}_\Lambda(\alpha)]$ (since G acts trivially by conjugation on elements of G in $G \rtimes \Lambda$). Let C_1 be the orbit of α under the subgroup Γ and let $C_1, \ldots C_t$ be the orbit of C_1 under Λ. Since these orbits C_i are conjugate under Λ they all have the same size and so $t(C) = |C|/|C_1|$ where $|C_1| = [\Gamma : \mathrm{Stab}_\Gamma(\alpha)]$. ∎

Example 4.28 *Returning to the context of example 4.24, let $G = Z_{23} \times Z_{89}$, $\Lambda = \Lambda_{23} \times \Lambda_{89}$ and now let $\Gamma =< \gamma : \gamma(xy) = (xy)^2 >$. Then $\Gamma \trianglelefteq \Lambda$.*
Consider the $\Gamma-$cyclotomic coset C_{xy} containing (xy). The element xy is stabilized only by the identity in both Λ and Γ so $t(C_{xy}) = 11^2/11 = 11$. This implies that the column labelled by $C_{(xy)}$ in example 4.24 will split into 11 columns whose sum is the original column.

On the other hand, the element y is stabilized by Λ_{23} in Λ and the identity in Γ so $t(C_y) = 11/11 = 1$ so this column will not split.

Continuing in this way, we see that only the columns labelled by $\tau^i(xy)$ *and* $\tau^i(x^{-1}y)$ *will split (each into 11 columns). The final matrix* $P(G,\Gamma)$ *will thus have* $(16)(11)+11 = 187$ *columns (and* 187 *rows.)*

The isomorphism of G *with* G^* *and the action of* Λ *of* G^* *given in Lemmas 4.35 and 4.15 give us a similar splitting for the rows of* P*.*

We will compute this example modulo a power of a prime ideal in section 4.4.

4.3 Computations with $P(G,\Lambda)$

In this section we work out some properties of the matrix $P(G,\Lambda)$ which are useful in computations and combinatorial applications. There are two main ideas in this section. First we consider a situation where the entries of P are integral. Secondly we work out a formula for the inverse of P.

In general, we expect the entries of $P(G,\Lambda)$ to be in $\mathbb{Z}[\zeta_v]$ where v is the exponent of the abelian group G, since these entries are characters of G applied to formal sums of elements of G. These entries, in fact, turn out to be integral modulo powers of certain prime ideals in $\mathbb{Z}[\zeta_v]$.

Theorem 4.29 *Let* $v = \exp(G)$*. Let* p *be a prime not dividing* v*, and let* π *be a prime ideal lying above* (p) *in* $\mathbb{Z}[\zeta_v]$*. Suppose* Λ *contains the automorphism* σ *where* $\sigma(g) = g^p$ for all $g \in G$*. Then entries in* $P(G,\Lambda)$ *are integral modulo any positive power of* π*.*

Proof: Since every character χ maps g to a v^{th} root of unity, $\chi(C_i)$ is a sum of v^{th} roots of unity, and this sum is fixed by the map σ. This means each entry p_{ij} of P is fixed by σ acting on $\mathbb{Z}[\zeta_v]$ by $\zeta_v \mapsto \zeta_v^p$. So p_{ij} is in the fixed ring of the subgroup of the Galois group of $\mathbb{Z}[\zeta_v]$ that fixes all prime ideals π dividing (p) (and any power

of those prime ideals). Therefore mod π^k, p_{ij} is actually in the subring $\mathbb{Z}/(p^k)$ of $\mathbb{Z}[\zeta_v]/\pi^k$. ■

Definition 4.30 *Let $\mathbf{P}_{\pi^k}$ denote the matrix P with entries taken modulo π^k.*

Example 4.31 *We compute the matrix from example 4.11 modulo π^{11}, where π is a prime ideal over (2) in $\mathbb{Z}[\zeta_{23}]$. By Theorem 2.30, the ideal (2) factors into the prime ideals $\pi_1\pi_2$ in $\mathbb{Z}[\zeta_{23}]$. We compute $\pi = \pi_1 = (f(\zeta_v), 2)$ where $f(x)$ is the factor $x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$ of $\Phi_{23}(x)$ mod 2.*

By Theorem 2.32, the ideal π^{11} is generated by $(f^{(11)}(\zeta_v), 2^{11})$ where $f^{(11)}$ is the hensel lift of f from $\mathbb{Z}/(2)$ to $\mathbb{Z}/(2^{11})$.
We compute $f^{(11)}(x) = x^{11} + 1559x^{10} + 1556x^9 + 2044x^8 + 486x^7977x^6 + 981x^5$ $+493x^4 + 4x^3 + 1561x^2 + 1558x + 2047$. The element α from example 4.11 is fixed by the map $\zeta_{23} \mapsto \zeta_{23}^2$. Modulo π^{11}, $\alpha = 489$ and $\overline{\alpha} = -490$ (both in $\mathbb{Z}/(2^{11})$). We get:

$$P_{\pi^{11}}(Z_{23}, \Lambda_{23}) =$$

	C_0	C_{-1}	C_1
χ_0	1	11	11
χ_1	1	489	−490
χ_{-1}	1	−490	489

Note that modulo 2^{11}, $\alpha + \overline{\alpha} = -1$, and $\alpha\overline{\alpha} = 6$ as expected.

A similar computation can be easily done for the matrix $P(Z_{89}, \Lambda_{89})$ where $Z_{89} =< y >$, and $\Lambda_{89} =< y \mapsto y^2 >$. The first 'faithful' row of $P(Z_{89}, \Lambda_{89})$ is:

$$[1, \beta, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7] =$$

$$[1, -544, -111, 323, -161, 91, -620, 84, 937]$$

The numbers $\alpha, \overline{\alpha}$ and the β_i can now be substituted into example 4.24 to get the character table $P_{\pi^{11}}(Z_{(23\times 89)}, \Lambda_{23} \times \Lambda_{89})$.

One advantage of working modulo a power of a prime π over (p) is that we may now do integer arithmetic (modulo p^k), and avoid the difficulties of working in $\mathbb{Z}[\zeta_v]$. We will see applications for this in chapter 5.

The second key property of $P(G, \Lambda)$ we consider is the invertibility of P over $\frac{1}{|G|}\mathbb{Z}[\zeta_v]$ where $v = exp(G)$. The proof is collected in a few lemmas:

Definition 4.32 *Let $\overline{P}$ be the matrix P with all entries replaced by their complex conjugates.*

Lemma 4.33 *$\overline{P} = \hat{M}P$ for some permutation matrix $\hat{M}$.*

Proof: Recall from chapter 2 that if φ is any irreducible character of the abelian group G, then the character $\overline{\varphi}(g) = \overline{\varphi(g)}$ is another irreducible character. To get from P to $\overline{P}$ we swap the rows of P corresponding to φ and $\overline{\varphi}$. ∎

Example 4.34 *This is visible in all the character tables given so far.*

Now we show that the automorphism group Λ groups the characters of G into the maximal common eigenspaces V_i used in the definition of the matrix P. The action of Λ on G^* is determined by the action of Λ on characters of G in the group $G \rtimes \Lambda$.

Lemma 4.35 *Let Λ act on the character group G^* of G by $\chi^\lambda(g) = \chi(\lambda^{-1}(g))$ as in Lemma 4.15. Then χ and $\hat{\chi}$ are in the same Λ-orbit if and only if χ and $\hat{\chi}$ have the same eigenvalue on each adjacency matrix A of $C(G, \Lambda)$.*

Proof: Suppose there is a λ in Λ such that $\hat{\chi} = \chi^\lambda$. Then $\chi(C) = \chi(\lambda^{-1}(C)) = \chi^\lambda(C) = \hat{\chi}(C)$ for all cyclotomic cosets C in $\mathcal{C}$. Then χ and $\hat{\chi}$ have the same eigenvalues on all the adjacency matrices of the scheme.

On the other hand, suppose there is no such λ. Define

$$\chi_1 := \sum_{\lambda \in \Lambda} \chi^\lambda \text{ and } \hat{\chi}_1 := \sum_{\lambda \in \Lambda} \hat{\chi}^\lambda$$

$\chi_1 \neq \hat{\chi}_1$. Let $g \in G$. Then $g \in C$ for some cyclotomic coset C.

$$\chi_1(g) = \sum_{\lambda \in \Lambda} \chi^\lambda(g) = \sum_{\lambda \in \Lambda} \chi(\lambda^{-1}(g)) = \frac{|\Lambda|}{|C|}\chi(C)$$

$$\hat{\chi}_1(g) = \sum_{\lambda \in \Lambda} \hat{\chi}^\lambda(g) = \sum_{\lambda \in \Lambda} \hat{\chi}(\lambda^{-1}(g)) = \frac{|\Lambda|}{|C|}\hat{\chi}(C)$$

Since $\chi(C) = \chi(\hat{C})$ for all cyclotomic cosets C, $\chi_1(g) = \hat{\chi}_1(g)$ for all g, a contradiction.

■

Remark *The 'twist' $\chi^\lambda(g) = \chi(\lambda^{-1}(g))$ was required for the relation $(\chi^{\lambda_1})^{\lambda_2} = \chi^{\lambda_1\lambda_2}$ so that characters are in the same Λ-orbit in G^* if and only if they are conjugate in $\mathcal{G}$ under this action.*

Recall from section 2.1 that $m_i := \dim V_i$, the dimension of the i^{th} eigenspace V_i, so that m_i is the number of characters in the i^{th} eigenspace.

Corollary 4.36 *There is a permutation of the list m_i so that $m_i = |C_i|$.*

Proof: Lemma 4.35 gives a mapping of the C_i to the eigenspaces V_i ■

Corollary 4.37 *Let D_V be the diagonal matrix with i^{th} entry m_i and let D be the diagonal matrix with i^{th} entry $|C_i|$.*
Then $P^T D_V \overline{P} = |G|D$

Proof: Apply the Second Orthogonality Relation (Theorem 2.8) to $\mathcal{C}(G, \Lambda)$ with $k_i = |C_i|$. ■

Corollary 4.38 *There are permutation matrices M and $\hat{M}$ so that* $P^T M D \hat{M} P = |G|D$

Proof: Corollary 4.36 implies that there is a permutation matrix M such that $D_V = MD$ ■

Corollary 4.39 *P is invertible over $\mathbb{C}$ with inverse $\frac{1}{|G|} D^{-1} P^T M D \hat{M}$.*

Proof: D is a diagonal matrix with non-zero entries. ■

Remark *Taking determinants in the formula $P^T M D \hat{M} P = |G|D$, we see that the only denominator required to find the inverse of P is $|G|$. In key applications we work with the matrix P modulo ideals above a prime not dividing $|G|$. In those cases P remains invertible.*

4.4 Special Cases and Some Character Tables

In this section we discuss the computation of the matrix $P(G, \Lambda)$ in some special circumstances. We begin with the extremal cases for Λ.

Lemma 4.40 *If Λ contains only the identity automorphism, then $P(G, \Lambda) = \chi(G)$: the group character table for G.*

Proof: Just use the construction in section 4.1. All orbits under Λ consist of single elements of G. ■

Lemma 4.41 *If $\Lambda = Aut(G)$ then $P(G, \Lambda)$ has integer entries.*

Proof: Let $v = exp(G)$. Then for $A \in \mathbb{Z}G$ and χ any irreducible character of G, $\chi(A) \in \mathbb{Z}[\zeta_v]$. On the other hand, if A is fixed by Λ then $\chi(A)$ is fixed by every element of $Gal_{\mathbb{Q}}(\mathbb{Q}(\zeta_v))$. Therefore, $\chi(A) \in \mathbb{Z}[\zeta_v] \cap \mathbb{Q} = \mathbb{Z}$. ■

Example 4.42 *An easy example here is:*

$$P(Z_{23}, Aut(Z_{23})) = \begin{array}{c|cc} & 1 & C_1 \\ \hline \chi_0 & 1 & 22 \\ \chi_1 & 1 & -1 \end{array}$$

which is a fusion scheme of the scheme in example 4.11.

The next examples relate to the special case of a cyclotomic association scheme of class e on $GF(q)$ as defined by [BM] and others.

The definition and the first case (for q prime) was given in section 4.1. The cyclotomic association scheme of class e of $GF(p)$ is $\mathcal{C}(Z_p, \Lambda)$ where Λ is generated by the automorphism corresponding to multiplication by the e^{th} power of a primitive element of $GF(p)$.

In this case the character table has a particularly nice form. Bannai and Munemasa give the following theorem (restated in terms of $\mathcal{C}(G, \Lambda)$):

Theorem 4.43 *[BM] If $G = Z_p$ and Λ is the subgroup of $Aut(Z_p)$ of index e (and size $f = (p-1)/e$), then the character table of the scheme is*

$$P(G, \Lambda) = \begin{pmatrix} 1 & f & f & \cdots & f \\ 1 & & & & \\ \vdots & & P_0 & & \\ 1 & & & & \end{pmatrix}.$$

P_0 is an $e \times e$ circulant matrix called the **principal part** *of P with first row $[\eta_0, \eta_1, \ldots \eta_{e-1}]$. The η_i are 'Gaussian periods' defined by the equation:*

$$\eta_i = \sum_{\beta \in <\alpha^e> \alpha^{i-1}} \chi(\beta)$$

for χ an irreducible character of Z_p.

Remark *Let $Aut(Z_p) = \Lambda \times \Gamma$. Γ must be cyclic, generated by some γ, so we can write $\eta_i = \gamma^i(\eta_0)$*

Example 4.44 *The character tables in examples 4.11 and 4.12 both have this form.*

In the more general case:

Proposition 4.45 *Let p be prime and $q = p^t$. Let α be a primitive element of $GF(q)$ and let λ be the automorphism of the additive structure of $GF(q)$ given by $x \mapsto x\alpha^e$. Let $\Lambda =< \lambda >$. Then the cyclotomic association scheme of class e on $GF(q)$ is $\mathcal{C}(Z_p^t, \Lambda)$.*

Proof: Since the additive structure of $GF(q)$ is isomorphic to Z_p^t, multiplication by α^e gives an automorphism τ of order $f = (p^t - 1)/e$. Λ is the subgroup of $Aut(Z_p^t)$ generated by τ. This gives the correspondance between cosets of $< \alpha^e >$ in $GF(q)$ and orbits of Λ on Z_p^t. The subgroup coset $< \alpha^e > \alpha^i$ in $GF(q)$ corresponds to the cyclotomic coset generated by α^i under Λ in $\mathcal{C}(Z_p^t, \Lambda)$. ■

Bannai and Munemasa give a nice connection between the character tables of class e on $GF(q)$ and on $GF(q^s)$:

Theorem 4.46 *[BM] The character table for the cyclotomic association scheme of class e on $GF(q^s)$ is*

$$\begin{pmatrix} 1 & f' & f' & \cdots & f' \\ 1 & & & & \\ \vdots & & \hat{P}_0 & & \\ 1 & & & & \end{pmatrix}$$

with principal part $\hat{P}_0 = (-1)^{s-1} P_0^s$, where P_0 is the principal part of the character table of class e on $GF(q)$ (and $f' = (q^s - 1)/e$).

Example 4.47 *Example 4.11 is a cyclotomic scheme of order 11 on $GF(23)$. Now let $G = Z_{23}^2$ and $\Lambda =< \lambda : \lambda(a, b) = (-3a + b, -5a + 2b) >$. It is easy to check that Λ has order 48 as an automorphism of G so $\mathcal{C}(G, \Lambda)$ is the cyclotomic association*

scheme of class $e = 11$ *on* $GF(23^2)$ *with character table:*

$$\begin{pmatrix} 1 & 48 & 48 \\ 1 & -11 & 12 \\ 1 & 12 & -11 \end{pmatrix}$$

Comparing the principal part of this matrix with the principal part of the matrix in example 4.11 and using the relations $\alpha\overline{\alpha} = 6$ *and* $\alpha + \overline{\alpha} = -1$, *we note:*

$$\begin{pmatrix} -11 & 12 \\ 12 & -11 \end{pmatrix} = (-1)\begin{pmatrix} \alpha & \overline{\alpha} \\ \overline{\alpha} & \alpha \end{pmatrix}^2$$

as in the theorem above.

Now we put the machinery of this chapter to work to finish building the character table $P(G, \Lambda)$ modulo π^{11} where G is the cyclic group of order $v = 2^{11} - 1$ generated by z, Λ is the automorphism group $< \sigma : \sigma(z) = z^2 >$, and π is a prime ideal over (2) in $\mathbb{Z}[\zeta_v]$.

We computed in previous examples the character table

$\hat{P} = P(Z_{(23\times 89)}, \Lambda_{23} \times \Lambda_{89})$ modulo π^{11} where $\pi = (f(\zeta_{2047}), 2)$.

Here we collect the relevant notation:

$G = Z_{(23\times 89)} =< x, y : x^{23} = y^{89} = 1,\ z = xy = yx >$

$\Lambda_{23} =< x \mapsto x^2,\ y \mapsto y >$

$\Lambda_{89} =< x \mapsto x,\ y \mapsto y^2 >$

$Aut(Z_{23}) = \Lambda_{23} \times \Delta$ where $\Delta =< x \mapsto x^{-1} >$, Λ_{23} has order 11 and Δ has order 2,

$Aut(Z_{89}) = \Lambda_{89} \times \Gamma$ where $\Gamma =< \tau : y \mapsto y^{12} >$, Λ_{89} has order 11 and τ has order 8.

In example 4.24, we computed the column labels of $\hat{P}$ in terms of τ:

$$1 \quad y \quad \tau(y) \quad \ldots \quad \tau^7(y) \mid x \quad xy \quad \tau(xy) \quad \ldots \quad \tau^7(xy) \mid x^{-1} \quad x^{-1}y \quad \tau(x^{-1}y) \quad \ldots \quad \tau^7(x^{-1}y)$$

The 16 cyclotomic cosets given by $\tau^i(xy)$ and $\tau^i(x^{-1}y)$ each split (as in example 4.28) into 11 cyclotomic cosets under Λ. These 11 cyclotomic cosets are in all cases cyclically

permuted by the automorphism $\gamma : (xy) \mapsto (xy)^{1428}$. (The remaining cosets do not split.) The rows of $\hat{P}$ have labels similar to those of the columns, split in the same way and are also permuted in the same way by the automorphisms τ, γ, and $x \mapsto x^{-1}$. (To see this, replace x by $\chi_x : (x \mapsto \zeta_{23},\ y \mapsto 1)$ and y by $\chi_y : (x \mapsto 1,\ y \mapsto \zeta_{89})$.)

In practice, we compute an entire row of P mod π^{11} and use the automorphisms γ, τ, and $x \mapsto x^{-1}$ to compute the remaining rows. Here as an illustration, we give the first row of the circulant 11×11 matrix corresponding to the (xy) column and $\chi_x\chi_y$ row of $\hat{P}$ to be:

$$[143, 517, 916, 1005, 300, -375, 496, 347, 779, 117, 75].$$

The row sum of this matrix is $(489)(-544)$ mod 2^{11} as expected.

5 The Cyclotomic Scheme in the Combinatorial Context

Returning to the topic of chapter 3, suppose our goal is to study group ring elements like difference sets with certain specified combinatorial properties. Now we may use the tools from a cyclotomic coset association scheme. Further, we change emphasis and start by formulating desired properties algebraically. Then we work back to group ring elements, and finally to subsets of G.

In section 5.1 we define the spectrum of an element A of a cyclotomic coset scheme. This spectrum will be a vector with coordinates in a number ring R, and carry all the character information necessary to determine A. In section 5.2 we translate the methods from chapter 3 into the association scheme framework and see that none of the standard techniques are lost. In particular, the multiplier group of a difference set is built in from the very outset, group homomorphic image techniques have their analogues, and all the character information is available. We also see from the translation of No's theorem that the overlying field in some constructions is not essential. In section 5.3 we show how working modulo π^t for some prime ideal π of R can help resolve some of the conflicts caused by using algebraic techniques to study sets. We show that if two sets have the same representations modulo π they are, in fact the same set.

Finally, in section 4, we restate conjectures from chapter 3 in the cyclotomic coset scheme context. The factorization underlying the Gordon Mills Welch construction has a very satisfying theory mod π. We will give an algorithm to find all factors of a given subset of a cyclotomic coset association scheme into sets. An additional advantage is that this algorithm completely avoids the difficulties associated with working in the number ring.

5.1 Spectrum

In this section we define the spectrum $\mathcal{S}(A)$ for any element of the cyclotomic coset scheme $\mathcal{C}(G, \Lambda)$. We will view $\mathcal{C}(G, \Lambda)$ as a subalebra of $\mathbb{Z}G$. In this case, scheme elements are $\mathbb{Z}$-linear combinations of the cyclotomic cosets of $\mathcal{C}$.

Let $A \in \mathcal{C}(G, \lambda)$ and let χ and $\hat{\chi}$ be irreducible characters of G. We saw in lemma 4.35 that $\chi(A) = \hat{\chi}(A)$ whenever χ and $\hat{\chi}$ are in the same Λ-orbit. Hence the set $\{\chi(A)\}$ where χ runs over all the orbit representatives of G^* under Λ is a complete set of irreducible characters of the group ring element A.

By the inversion formula (Corollary 2.13), the original group ring element A is recoverable from this set of data.

Given an element A of the scheme, let $\mathbf{A}$ be the characteristic vector of A under the same labelling as that used in the character table P of $\mathcal{C}$, so that $\mathbf{A}$ gives the coefficients of the cosets C_i for A. Then if we replace A by its characteristic vector the matrix product $P \cdot \mathbf{A}$ gives this complete set of irreducible characters as an ordered list in vector form.

Definition 5.1 *The* **exact spectrum** $\mathcal{S}(A)$ *(relative to the matrix P) of A is defined to be the vector $P\mathbf{A}$*

Example 5.2 *The exact spectrum of any cyclotomic coset C_g is the column of P labelled by C_g.*

In corollary 4.39 we saw that the matrix P is invertible over $\mathbb{C}$ so the element A is recoverable from its exact spectrum by matrix multiplication. This essentially restates the inversion formula in matrix form, so we view P as a transition matrix between group ring elements fixed by Λ and their set of values on all the irreducible characters of G.

It is useful to divide the exact spectrum of a group ring element into two parts: the faithful and the non-faithful.

Recall that a group character χ of G is **faithful** if $\chi(g) = \chi(1)$ implies that $g = 1$. Since $\lambda(1) = 1$ for all $\lambda \in \Lambda$, faithful characters are mapped to faithful characters under the action of Λ on characters of G. Therefore the matrix P can be divided into rows labelled by faithful characters (the faithful part P_F of P) and rows labelled by non-faithful characters (the non-faithful part P_C of P).

This means that the spectrum of any element of the scheme can also be divided into two pieces: the faithful part $\mathcal{S}_F$ and the non-faithful part $\mathcal{S}_C$.

The main reason we make this distinction is that we can compute the non-faithful part $\mathcal{S}_C(A)$ of the spectrum of A corresponding to a subgroup H fixed by Λ from knowledge of its homomorphic image into G/H. This is formalized in the lemma below. The condition $\Lambda(H) = H$ is satisfied whenever Λ is generated by numerical multipliers. On the other hand, homomorphic image information tells us nothing about the faithful part of the spectrum.

Lemma 5.3 *If $H \leq G$ with $\Lambda(H) = H$, then the non-faithful portion of the spectrum corresponding to H can be computed entirely within the homomorphic image $\mathcal{C}(G/H, \Lambda)$.*

Proof: Suppose γ is an entry in $\mathcal{S}_C(A)$. Then $\gamma = \chi(A)$ where χ is some non-faithful character of G. Since χ is non-faithful, it is trivial on some subgroup H of G. If the subgroup H satisfies $\Lambda(H) = H$ we can apply Theorem 4.20. Let η map $G \mapsto G/H$ in the usual way. Then $\chi(A) = \chi(\eta(A))$. Note particularly that $\eta(A)$ is in the smaller scheme $\mathcal{C}(G/H, \Lambda)$. ∎

A primary use of the exact spectrum is to examine algebraic properties of a group

ring object A in an organized way. We consider some properties which can be checked using the exact spectrum below.

Group ring equation: Since group characters extend to group ring homomorphisms, when we apply an irreducible complex character φ of G to equations such as (3.3) and (3.5) we obtain a condition on the $\mathbb{C}$- norm of the image of the group ring object. For example, the difference set equation (3.3) becomes

$$\varphi(D)\varphi(D^{(-1)}) = \varphi(D)\overline{\varphi(D)} = n + \lambda(\varphi(G)) = n$$

(when φ is not the trivial character). Given an exact spectrum $\mathcal{S}$ we can easily compute the $\mathbb{C}$-norm of all its entries. This means that if D is a k-set, then D is a (v, k, λ)- difference set if and only if $\alpha\overline{\alpha} = n$ for all entries α in the spectrum.

Equivalence: Recall that a difference set D is defined to be equivalent to a set $\hat{D}$ if $\hat{D} = g \cdot \tau(D)$ where τ is an automorphism of G, and $g \in G$. These equivalence relations are more easily recognized in the exact spectrum $\mathcal{S}(\mathbf{D})$ than in the original group ring context.

In particular, if τ is an automorphism of G, then τ permutes the cyclotomic cosets of G as well as the orbit classes in G^*. In this case, the ordered entries of $P(\tau(\mathbf{D}))$ will be the corresponding permutation of the entries of $\mathcal{S} = P\mathbf{D}$. Further, since we are considering only elements of the group ring fixed by the automorphism group Λ, shifts gD of G are irrelevant.

Additional symmetry: An element A of $\mathcal{C}(G, \Lambda)$ may be fixed by automorphisms outside the (multiplier) group Λ. This symmetry will be reflected in the fact that A is an element of the fusion scheme $\mathcal{C}(G, \Gamma)$ where Λ is a subgroup of Γ.

Striking examples of this are the Payley difference sets described in chapter 3 which are known to have a large multiplier group. Here we give the general theorem

for N^{th}-power residue difference sets due to Lehmer:

Theorem 5.4 *([Bau, p.125])*
The N^{th} power residues themselves are (the only) multipliers of a non-trivial N^{th} power residue difference set.

This means that in the case of a Payley difference set D (where $N = 2$ and G is the cyclic group of prime order $4n - 1$), D is fixed by every automorphism in $Aut(G)$ except the map $x \mapsto x^{-1}$.

Thus the non-trivial spectrum of a Payley difference set is two-valued, visibly reflecting this symmetry.

The second (and perhaps more interesting) major use for the spectrum is to encode partial algebraic information about a desired element of $\mathcal{C}$ and then use P^{-1} to examine the set of elements in $\mathcal{C}$ having this property. We will have more to say about this in the last two sections of this chapter.

Finally, it is important to stress that the exact spectrum of an element A as a vector over $\mathbb{Z}[\zeta_v]$ uniquely determines an element in the group ring. Under certain conditions we will see that much less information is needed.

5.2 Established Techniques Revisited in $\mathcal{C}$

We now reconsider the basic techniques for the study of abelian difference sets discussed in section 3.2, using the machinery we have built up: namely the cyclotomic coset scheme and the spectrum.

The first thing to note (and a key point) is that the association scheme builds in the multiplier of a difference set. Only sets fixed by Λ come under consideration, and character values in $\mathbb{Z}[\zeta_v]$ are also fixed by Λ (viewed as a subgroup of $Gal_{\mathbb{Q}}(\mathbb{Q}[\zeta_v])$.) This actually forces the character values into a smaller number ring than $\mathbb{Z}[\zeta_v]$.

The lowest level technique for studying difference sets mentioned in section 3.2 was the brute force method in which one searches among subsets of G for (all) those with the required combinatorial property. The analog of brute force from the spectral point of view is to search among $P^{-1}\mathcal{S}$ over (all) possible exact spectra $\mathcal{S}$ with the required algebraic properties (eg. $\mathbb{C}$ - norms) for group ring elements corresponding to sets. This turns the problem into one of linear algebra over a number ring. We give a small example to illustrate this.

Example 5.5 *Let* $G = Z_5$, $\Lambda_5 =< x \mapsto x^2 >$. *Suppose we seek all multisets* A *in* $\mathcal{C}(G, \Lambda_5)$ *satisfying the group ring equation* $AA^{(-1)} = 4 + 12G$ *(an example of the difference list equation(3.16)). The character table* $P(Z_5, \Lambda_5)$ *appears in example 4.21. Since* A *is integral, so are* $\chi_0(A)$ *and* $\chi_1(A)$. $\chi_0(A) = \sqrt{4 + 12(5)} = 8$ *(since* χ_0 *must be positive), and* $\chi_1(A) = \pm\sqrt{4} = \pm 2$. *Computing* $\mathbf{A} = P^{-1}\mathcal{S}(A)$ *we see that* A *is integral if and only if* $\chi_1(A) = -2$ *so we have the unique solution* $A = 2(x + x^2)$.

The group homomorphic image approach described in chapter 3 translates very well into the cyclotomic coset scheme. Recall in that approach, one first computes all possible images $\tau(D)$ of a difference set D with given parameters into the quotient group G/H for all normal subgroups H of G. One then attempts to lift these solutions to a solution of the difference set equation in $\mathbb{Z}G$.

The hardest part of this approach is in the lifting. If there are several homomorphic images any lift must be compatible with all the images simultaneously.

In the cyclotomic coset scheme context, we first solve the homomorphic image equation $\tau(D)\tau(D^{(-1)}) = n + \lambda(\tau(G))$ in the (smaller) schemes $\mathcal{C}(G/H, \Lambda)$ for all $H \leq G$ which satisfy $\Lambda(H) = H$. By Lemma 5.3 each such homomorphic image fills in the portion of the non-faithful spectrum of D in $\mathcal{C}(G, \Lambda)$ corresponding to G/H.

If Λ is generated by a numerical multiplier then the condition $\Lambda(H) = H$ is satisfied for all $H \leq G$ and so the entire non-faithful spectrum can be generated in this way.

Example 5.6 *Let D be a $(15, 8, 4)$ cyclic difference set. D has multiplier group Λ_{15} generated by the map $x \mapsto x^2$ by example 3.15. This means D is in $\mathcal{C}(Z_{15}, \Lambda_{15})$ with character table given in example 4.13.*
$\mathcal{S}(D) = [\chi_0(D), \chi_5(D), \chi_3(D), \chi_1(D), \chi_{-1}(D)]^T$.
In the example just above we found $\chi_0 = 8$ and $\chi_3 = -2$. Similarly we can find $\chi_5 = 2$. This fills in the non- faithful portion of $\mathcal{S}(D)$.

The spectral data generated from group homomorphic images can be used with linear algebra to avoid the bookkeeping problems associated with keeping track of the intersections of the pre-images of the solutions for each $H \leq G$.

Note that the faithful spectrum carries all the information that is inaccessible from group homomorphic images. In the example above, $\chi_1(D)$ and $\chi_{-1}(D)$ cannot be computed using group homomorphic images.

The next technique from section 3.2 (and perhaps the most general and powerful) is the application of group representations. This is exactly the point of the spectrum. The spectrum displays all the relevant character information simultaneously, and turns computations such as character inversion into linear algebra.

Gaal and Golomb's search for $(1023, 512, 256)$ -cyclic difference sets was described in section 3.2. After finding all possible homomorphic images, (in our context, the non-faithful spectrum), the size of the resulting search space forced them to use additional character information. Their discrete Fourier transform (equation 3.20), is really the evaluation of a faithful character of the cyclic group $< x >$ applied to the group ring element $\sum a_i x^i$. This is a single entry in the (faithful) spectrum of

$\sum a_i x^i$. We can compute this transform by taking the dot-product of a single row of the character table P with the characteristic vector $\mathbf{A}$ of each case $\sum a_i x^i$.

Gaal and Golomb evaluated the $\mathbb{C}$-norm of their discrete Fourier transforms using floating point computation with tolerance. But floating point computation can be slow. Section 5.4 shows how to replace it in this instance with computation modulo p^e. Moreover, e may be chosen interactively to reduce the number of extraneous solutions produced.

Next we address constructions involving the tower of finite fields

$$K_n := GF(q^n) \subseteq K := GF(q) \subseteq := GF(p)$$

where p is prime and $q = p^e$.

In section 3.2 we described the technique of realizing the cyclic group Z_v as a quotient group K_n^*/K^* when $v = (q^n - 1)/(q - 1)$. In the field context, one then uses well known properties of the trace map (and generalizations of the trace map) to construct difference sets. The trace map can be computed in the scheme.

The matrix $P(Z_v, < x \mapsto x^p >)$ taken modulo any prime ideal π over (p) does give the (absolute) trace of elements of K_n as we will see below, but only of those elements belonging to the subgroup Z_v of K_n^*.

We can, however, retrieve the complete trace map from K_n to K in this context if we move to the larger scheme $\mathcal{C}(Z_{v'}, \Lambda')$ where $v' = q^n - 1$ and Λ' is the subgroup of $Aut(Z_{v'})$ generated by the map $x \mapsto x^q$.

Theorem 5.7 *Let* $\Lambda =< \sigma \mid \sigma(x) = x^q >$ *be a subgroup of* $Aut(Z_{v'})$ *for* $q = p^e$ *and* $v' = q^n - 1$. *Let* χ *be a faithful representation of* $Z_{v'}$ *Fix* $\beta \in GF(q^n)^*$. *Then*

$$tr_q^{q^n}(\beta) = \frac{n}{|C|}(P_\pi)_{(\chi,C)}$$

where C is the cyclotomic coset in $\mathcal{C}$ containing the image of β under the correspondance $GF(q)^* \cong Z_{v'}$.

Proof: The faithful representation χ of $Z_{v'}$ maps the generator x of $Z_{v'}$ to some ζ satisfying $\zeta^{v'} - 1 = 0$. The prime ideal π is $(f(\zeta), p)$ where f is a (primitive) irreducible polynomial of degree $e \times n$ over $GF(p)$. Let α be a root of $f(x)$ mod p. Without loss of generality, we may let $GF(q^n)^* =< \alpha >$. Then $\beta = \alpha^i$.

Let $Z_{v'} =< x >$ so that $x^{v'} - 1 = 0$. Let C be the cyclotomic coset containing x^i, and let k be the order of σ on the subgroup of $Z_{v'}$ generated by x^i so that $(x^i)^{q^k} = x^i$. Then we have $C = x^i + (x^i)^q + \ldots + (x^i)^{q^{k-1}}$. (Note that $|C|$ divides n.)

Computed modulo π, $\chi(C) = \alpha^i + (\alpha^i)^q + \ldots + (\alpha^i)^{q^{k-1}} = (P_\pi)_{(\chi,C)}$.
On the other hand, $tr_q^{q^n}(\alpha^i) = \alpha^i + \alpha^{iq} + \ldots + \alpha^{iq^{n-1}}$. This implies
$tr_q^{q^n} = \frac{n}{k}(\alpha^i + \alpha^{iq} + \ldots + \alpha^{iq^{k-1}}) = \frac{n}{|C|} \cdot (P_\pi)_{(\chi,C)}$ ■

We will discuss more applications for the matrix P taken modulo π in the next section.

Next we translate the recent theorem by No described in chapter 3 into the context of $\mathcal{C}(Z_v, \Lambda)$ for $v = (q^n - 1)/(q - 1)$. This translation will imply that the larger field context is not essential to the constructions.

So let $v = (q^n - 1)/(q - 1)$, and let $K_n = GF(q^n)$, as above. Let $K_n^* =< z >$. Then we have $< z^v >= K^*$ (and $< z^{p-1} >= Z_v$ as a subgroup of K_n^*).
This gives us a cannonical representation of the elements in K_n^*/K^*:
$z^i = z^{jv+k} = z^{jv}z^k$ for $0 \leq k \leq v - 1$, and $0 \leq j \leq q - 2$.
We take the set of z^k as (cannonical) coset representatives of K_n^*/K^*.

Lemma 5.8 *d-homogeneous functions $f : K_n \rightarrow K$ correspond to functions $\hat{f} : Z_v \rightarrow K$.*

Proof: Let $f : K_n \rightarrow K$ be d-homogeneous, and write $f(z^i) = f(z^{jv}z^k) = z^{jvd}f(z^k)$. Define $\hat{f} : Z_v \rightarrow K$ by $\hat{f}(z^k) = f(z^k)$. Similarly, given $\hat{f} : Z_v \rightarrow K$ and any natural number d, we can extend $\hat{f}$ to f by defining $f(z^{jv}z^k) = z^{jvd}\hat{f}(z^k)$. ■

Definition 5.9 *A function $\hat{f} : Z_v \rightarrow K$ is* **v-balanced** *if*
$(q-1)|\hat{f}^{-1}(0)| = |\hat{f}^{-1}(K^*)| - 1$.

Lemma 5.10 *$f : K_n \rightarrow K$ is d-homogeneous and balanced if and only if its restriction $\hat{f}$ is v-balanced.*

Proof: Since f is d- homogeneous, $f(z^i) = f(z^{jv}z^k) = z^{jvd}f(z^k) = \hat{f}(z^k)$.
This means that $f(z^i) = 0$ if and only if $\hat{f}(z^k) = 0$. In this case,
$|f^{-1}(0)| = |\hat{f}^{-1}(0)|(q-1)$, since $0 \leq j \leq q-2$.

Now fix $\alpha \in K^*$. Then $z^{jv+k} \in f^{-1}(\alpha)$ if and only if $z^{jvd}f(z^k) = \alpha$. Since $z^{jvd} \in K^*$, this happens if and only if $f(z^k) = (\alpha)(z^{jvd})$. This is if and only if $\hat{f}(z^k) \neq 0$ and $\hat{f}(z^k) \neq 0$ if and only if $z^k \in \hat{f}^{-1}(K^*)$. So $|f^{-1}(\alpha)| = |\hat{f}^{-1}(K^*)|$. Then since f is balanced, the condition $|f^{-1}(0)| = |f^{-1}(\alpha)| - 1$ forces $(q-1)|\hat{f}^{-1}(0)| = |\hat{f}^{-1}(K^*)| - 1$.
■

Definition 5.11 *Let $Z_v =< x >$. A function $\hat{f} : Z_v \rightarrow K$ is* **v-difference balanced** *if $\hat{g}_\tau(x^i) := \hat{f}(x^{i+\tau}) - \hat{f}(x^i)$ is v-balanced for all τ with $1 \leq \tau \leq v-1$.*

Lemma 5.12 *A function $f : K_n \rightarrow K$ is d-homogeneous and difference balanced if and only if the corresponding $\hat{f}$ is v-difference balanced.*

Proof: Fix τ and i. Then $g_\tau(x^i) = f(x^{i+\tau}) - f(x^i) = x^{jvd}[f(x^{k+\tau}) - f(x^k)]$ So g_τ is d-homogeneous and difference balanced if and only if $\hat{g}_\tau$ is v-difference balanced. ■

Putting all this together we get a translation of No's Theorem:

Theorem 5.13 *[No]*

Let $v = (q^n - 1)/(q-1)$, *and* $K = GF(q)$. *If* $\hat{f}$ *is a* v*-difference balanced function from* Z_v *to* K, *then the set* $D = \{t \mid f(x^t) = 0,\ 0 \leq t \leq v-1\}$ *is a cyclic difference set with the classical parameters (3.23).*

In his paper, No uses the trace function as the prototypical d-homogeneous difference- balanced function. (The kernel of the trace map gives the Singer difference sets.) He then uses various twists and sums of trace maps to write other d-homogeneous difference balanced functions and therefore some new difference sets.

The translation of his theorem into the cyclotomic coset scheme for the cyclic group Z_v implies that the use of the field $GF(q^n)$ is not nessesarily essential to the construction.

Remark *A method to construct a* $v-$*difference balanced function for any cyclic difference set with the classical parameters would give a unified construction for these difference sets.*

5.3 $P(G, \Lambda)$ and Sets

In this section we return to the issues raised in section 3.3, now viewing them in terms of the cyclotomic coset association scheme $\mathcal{C}$. In the next section we will apply results from this section to the questions raised in section 3.4.

We begin by considering conditions on the exact spectrum of an element of $\mathcal{C}(G, \Lambda)$ that we can use to reduce the amount of spectral information needed to uniquely determine scheme elements.

The idea is this: Suppose we are given some vector $\mathcal{A} = (\alpha_1, \alpha_2, \ldots, \alpha_s)^T$ with $\alpha_i \in \mathbb{Z}[\zeta_v]$. (s is the number of cyclotomic cosets in the scheme). We want to answer the question: When is $\mathcal{A}$ a spectrum of some (integral) $A \in \mathcal{C}(G, \Lambda)$?

The easiest statement is that $\mathcal{A}$ is a spectrum if and only if $\mathcal{A}$ is in the $\mathbb{Z}$- column span of $P(G,\Lambda)$.

We can push this a little further in some cases. First, suppose Λ contains an automorphism σ which corresponds to a numerical multiplier $\sigma(g) = g^t$ for all g. Then character values must also be fixed by σ. Thus:

Proposition 5.14 *Let $A \in \mathcal{C}(G,\Lambda)$. If the map $g \mapsto g^t \in \Lambda$, then all entries α_i in the spectrum of A must be fixed by the map $\zeta_v \mapsto \zeta_v^t$ in $\mathbb{Z}[\zeta_v]$*

Now, let $G =< x >$ be cyclic and let $\gamma \in Aut(G)$. Then γ must map $x \mapsto x^i$ for some i and γ acts on $\mathbb{Z}[\zeta_v]$ in the same way: $\gamma(\zeta_v) = \zeta_v^i$. Thus, γ also permutes the rows of the matrix P. Let the action on the rows be described by the equation

$$\gamma(p_{i,j}) = p_{\gamma(i),j}$$

If $\mathcal{A}$ is a spectrum, then γ must act on $\mathcal{A}$ exactly as it acts on the rows of P. Specifically:

Definition 5.15 *Let G be cyclic. $\mathcal{A} = (\alpha_1, \alpha_2, \ldots, \alpha_s)^T \in (\mathbb{Z}[\zeta_v])^s$ satisfies the* **spin condition** *(relative to P) if and only if $\gamma(\alpha_i) = \alpha_{\gamma(i)}$ for all $\gamma \in Aut(G)$.*

Lemma 5.16 *Let G be cyclic and let $\mathcal{A} = (\alpha_1, \alpha_2, \ldots, \alpha_s)^T \in (\mathbb{Z}[\zeta_v])^s$. If $\mathcal{A}$ is the spectrum of an integral element of $\mathcal{C}(G,\Lambda)$ for a cyclic group G, then $\mathcal{A}$ must satisfy the spin condition relative to P.*

Proof: If $\mathcal{A}$ is a spectrum then $\mathcal{A} = P\mathbf{A}$ where A is an integral vector. Then γ acts on $P\mathbf{A}$ exactly as it does on P, so $\mathcal{A}$ must satisfy the spin condition. ∎

Remark *The lemma above is not an 'if and only if' condition since the formula for P^{-1} also involves inverting $|G|$. The point of the lemma is that we can recover an*

(integral) element A of C from minimal information about its complex representations together with the spin condition.

Example 5.17 *As an illustration, let $G = Z_{89}$ and consider the matrix P given in example 4.11. The exact spectrum of an element of $\mathcal{C}(Z_{89}, \Lambda_{89})$ contains nine character values. We can reconstruct an (integral) element of the associated scheme with just two: one from each orbit of Γ on rows of P.*

There is a second way to address integrality questions. This technique avoids the difficulties of working in $\mathbb{Z}[\zeta_v]$, at the expense of introducing extraneous solutions to equations such as (3.3). The idea is to use Theorem 4.29 (on the integrality of P_{π^t}), and work modulo π^t for an appropriate prime ideal π in $\mathbb{Z}[\zeta_v]$.

We need to make two additional definitions regarding the spectrum of an element in $\mathcal{C}$. As in Theorem 4.29 in what follows let $v = exp(G)$, let p be a prime not dividing v, and suppose Λ contains the p^{th} power map $\sigma(g) = g^p$.

In section 5.1 we defined the spectrum $\mathcal{S}(D)$ of an element $D \in \mathcal{C}(G, \Lambda)$ to be $\mathcal{S}(D) = P \cdot \mathbf{D}$. Just as in Theorem 4.29, if we take any character value of D in $\mathcal{S}(D)$ modulo π^t for any prime ideal π above p in $\mathbb{Z}[\zeta_v]$, the result is an integer modulo p^t. This is easily computed for all characters at once by the matrix computation $P_{\pi^t}\mathbf{D}$.

Definition 5.18 *The* **mod π^t spectrum $\mathcal{S}_{\pi^t}(D)$ of** *D is defined to be*
$\mathcal{S}_{\pi^t}(D) := P_{\pi^t}\mathbf{D}$.

Definition 5.19 *Given $P_{\pi^t}\mathbf{D}$, replace each entry of the mod π^t spectrum $\mathcal{S}_{\pi^t}(D)$ by its valuation over π (as an entry between 0 and t). The result is the* **valuation vector** $\nu_{\pi^t}(D)$.

We must note here that the valuation of some character values of D over π in $\mathbb{Z}[\zeta_v]$ may in fact be greater than t, but we will be working only modulo π^t.

The mod π^t spectrum makes it easy to prove the statement below: one of the few tools we have that combines algebra with integrality ($a_i \in \mathbb{Z}$) and bounded coefficients (set-ness if the bound is $0 \leq a_i \leq 1$).

Theorem 5.20 *Let $v = exp(G)$, let p be a prime not dividing v, and let t be an integer with $p^t > M$. Let Λ contain the map $\sigma : g \mapsto g^p$ for all $g \in G$. Then any element of the $\mathbb{Z}$-scheme $\mathcal{C}(G, \Lambda)$ with coefficients bounded by $0 \leq a_i \leq M$ is completely determined by its mod π^t spectrum.*

Proof: The formula in chapter 4 implies that the inverse of P exists mod π^t whenever p does not divide $|G|$. Let $D \in \mathcal{C}$ with coefficients $0 \leq a_i \leq p^t - 1$.
Then (D mod p^t) = D. Let $\circ$ denotes the matrix product modulo p^t. Since D has integral coefficients, D mod $p^t = D$ mod $\pi^t = P_{\pi^t}^{-1} \circ (\mathcal{S}_{\pi^t}(D))$ ■

Corollary 5.21 *Let $\mathcal{C}$ satisfy the conditions in Theorem 5.20. Then any set in $\mathcal{C}$ is completely determined by its mod π spectrum. If $p = 2$ each mod π spectrum corresponds to exactly one set. In particular, difference sets are determined by their mod π spectra.*

Remark *The case $p = 2$ is an important special case of the classical parameters, in particular, it is the case for Dillon's conjecture.*

Corollary 5.22 *Let $\mathcal{C}$ satisfy the conditions in Theorem 5.20 for $p = 2$. Then if D_1 and D_2 are sets in $\mathcal{C}$ with $\nu_\pi(D_1) = \nu_\pi(D_2)$ for all primes π over (p) then $D_1 = D_2$. Hence, any set is determined by its valuation vector $\nu_\pi(D)$.*

Corollary 5.23 *Let $\mathcal{C}$ satisfy the conditions in Theorem 5.20 for $p = 2$. If D is a set in $\mathcal{C}$ with the faithful portion of $\nu_\pi(D) \equiv 0$ mod π then D is completely determined by its valuations mod π on the non-faithful representations.*

There are many advantages of working modulo π^t. One is that we can avoid the problems associated with solving $\delta\bar{\delta} = n$ in the number ring $\mathbb{Z}[\zeta_v]$. It is easy to write down all solutions to $\delta\bar{\delta} = n$ modulo π^t since δ and $\bar{\delta}$ are integers mod π^t, and as long as we are looking for sets we will not lose any solutions. The downside is that we will introduce extraneous solutions which are not $\mathbb{Z}$-solutions, but solutions only modulo p^t. Finding these solutions is easier though, because the matrix P_{π^t} is also an integer matrix with an integral inverse whenever $gcd(|G|, p) = 1$.

We will apply the ideas from this section in the next:

5.4 Problems Revisited

In this section we return to the open questions mentioned in chapter 3 and examine them in the context of the cyclotomic coset association scheme.

The conjecture of Dillon (Conjecture 3.32) can be re-stated in the context of the scheme $\mathcal{C}(G, \Lambda)$ where G is the cyclic group $Z_v =< x >$, $v = 2^t - 1$, and where Λ is the multiplier group $< \sigma : x \mapsto x^2 >$ given by Theorem 3.14 for $(2^d - 1, 2^{d-1}, 2^{d-2})$ difference sets.

The conjecture (3.32) is that there is no $(2^t - 1, 2^{t-1}, 2^{t-2})$ difference set D such that $\varphi(D) \equiv 0 \bmod \pi$ for every faithful representation φ of Z_v (and any fixed prime π over (2) in $\mathbb{Z}[\zeta_v]$).

We can choose D from its equivalence class so that $\sigma(D) = D$. Then a counter-example to Dillon's conjecture would be an element D of the scheme $\mathcal{C}$ whose mod π spectrum $\mathcal{S}_\pi(D)$ is 0 on all faithful representations φ of $\mathcal{C}$. Note that since $p = 2$ and $\mathcal{S}_\pi(D)$ is integral, for this case $\mathcal{S}_\pi(D)$ is a $(0, 1)$-vector.

Dillon's conjecture has been verified for all values of t from 3 to 10 by exhaustive enumeration. (The case $t = 8$ was done by Cheng [Ch] in 1986, $t = 9$ was done by Smith [DS] and also Bacher [Bac] in 1994, and the case $t = 10$ by Gaal and

Golomb [GG] in 2000.)

Example 5.24 *Consider $t = 5$. There are only two equivalence classes of $(31, 16, 8)$ difference sets, Singer and Payley (cf. [Pott, p.92]). The spectrum of these difference sets have one non-faithful character (the trivial character) and six faithful characters. Their mod π spectra are:*

$$\begin{array}{lc|cccccc} \text{Singer}: & [\ 0 & 1 & 0 & 0 & 0 & 0 & 0\ ] \\ \text{Payley}: & [\ 0 & 1 & 0 & 1 & 0 & 1 & 0\ ] \end{array}$$

Neither spectrum is 0 on all the faithfuls. (Note also the extra symmetry in the Payley spectrum.)

Since Dillon's conjecture is concerned with elements having faithful character values congruent to 0 mod π, a counter- example must be in the mod 2 kernel of the idempotent e_F of Definition 2.15. We compute this idempotent mod 2:

Definition 5.25 *Let $v = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Define the* **square free part** v_0 **of** v *to be* $v_0 = p_1 p_2 \cdots p_s$.

Definition 5.26 *Let G be an abelian group of order v and let $o(g)$ be the order of g in G. Define $F_G^{\cdot} := \{g \in G \mid o(g) = v_0\}$*

Theorem 5.27 *Let G be cyclic, of odd order v. Let $e = \sum_{g \in F_G} g$.*
Then mod 2, $e_F \equiv e$.

Proof: In Lemma 2.16 we had $e_F = \sum a_g g$ where

$$a_g = \frac{1}{v} \frac{\phi(v)}{\phi(o(g))} \mu(o(g)).$$

We first note that $\mu(o(g))$ is zero unless $o(g)$ is square free. Then, since v is odd, $\phi(v)/\phi(o(g))$ is even unless the factorization of $o(g)$ contains every prime dividing v. So the coefficient of g is odd if and only if $o(g) = v_0$. ∎

Lemma 5.28 *Let B be in the integral group ring $\mathbb{Z}G$ for G cyclic of odd order v, and let π be a prime ideal over (2) in $\mathbb{Z}[\zeta_v]$. $\chi(B) \equiv 0 \mod \pi$ for all faithful characters χ of G if and only if $Be \equiv 0 \mod 2$.*

Proof: The product Be is in the integral group ring, with $\chi(Be) \equiv \chi(B) \mod 2$ for all faithful characters. ■

Theorem 5.29 *Let $D \in \mathbb{Z}G$ for G cyclic of odd order v, and let π be a prime ideal over (2) in $\mathbb{Z}[\zeta_v]$. Then $\chi(D) \equiv 0 \mod \pi$ for all faithful characters χ of G if and only if for all $g \in G$ the size of the set*
$\mathcal{D}_g = \{h \in F_G \mid h = d^{-1}g$ for some $d \in D\}$ is even.

Proof: The coefficient of g in the group ring product De is the number of solutions to $g = hd$ for $h \in F_G, d \in D$. ■

Corollary 5.30 *If D is a counter example to Dillons conjecture, then*
$|D \cap F_G| \equiv 0 \mod 2$.

Proof: Since $D \cap F_G = D^{(-1)} \cap F_G$, this is just the theorem above for $g = 1$. ■

There is a second formulation for the mod 2 idempotent which will give us another necessary and sufficient condition for a difference set to be a counter example to Dillon's conjecture.

Definition 5.31 *Let G be cyclic of odd order $v = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. Let A_i be the subgroup generated by elements of order p_i. Define $E := \prod(p_i - A_i) \in \mathbb{Z}G$.*

Lemma 5.32 *E is a faithful eigenpotent. That is:*

1. *$E^2 = v_0 E$ where $v_0 = \prod p_i$ as above.*

2. $\chi(E) = 0$ *if and only if* χ *is a non-faithful character.*

Proof: For (1), compute $(p_i - A_i)^2 = p_i(p_i - A_i)$ in the group ring.
For (2), since A_i are cyclic, if χ is faithful then $\chi(A_i) = 0$ for all i. If χ is non-faithful, there is some A_i in the kernel of χ so that for this i, $\chi(A_i) = p_i$. Thus

$$\chi(E) = \prod \chi(p_i - A_i) = \begin{cases} v_0 & \text{if } \chi \text{ is faithful} \\ 0 & \text{if } \chi \text{ is non-faithful} \end{cases}$$ ■

So just as with the idempotent e_F we have:

Lemma 5.33 *Let B be in the integral group ring $\mathbb{Z}G$ for G cyclic of odd order v, and let π be a prime ideal over (2) in $\mathbb{Z}[\zeta_v]$. $\chi(B) \equiv 0 \bmod \pi$ for all faithful characters χ of G if and only if $BE \equiv 0 \bmod 2$.*

Lemma 5.34 $E = v_0 + \sum S_i A_i$ *for* $S_i \in \mathbb{Z}G$.

Proof: $E = \prod(p_i - A_i)$. Multiplying this out we get

$$E = v_0 + \sum_{T \subseteq \{1 \ldots t\}} (-1)^{|T|} \prod_{i \in T, j \in T^c} p_i A_j$$

Also, since the A_i are subgroups, $\prod_{i \in I} A_i = S A_{i_1}$ for some $S \in \mathbb{Z}G$. ■

Theorem 5.35 *Let $D \in \mathbb{Z}G$ for G cyclic of odd order v, and let π be a prime ideal over (2) in $\mathbb{Z}[\zeta_v]$. Then $\chi(D) \equiv 0 \bmod \pi$ for all faithful characters χ of G if and only if D is a mod 2 sum of A_i cosets.*

Proof: $DE \equiv 0 \bmod 2$ if and only if $D \equiv D(\sum S_i A_i) \equiv \sum B_i A_i \bmod 2$ by the above lemma for some $B_i \in \mathbb{Z}G$. $\sum B_i A_i$ is visibly a sum of A_i-cosets. ■

Corollary 5.36 *A $(2^d - 1, 2^{d-1}, 2^{d-2})$ cyclic difference set D is a counter-example to Dillon's conjecture if and only if D is a mod 2 sum of A_i cosets.*

What makes proving Dillon's conjecture hard is the importance of the setness (and set-size) requirements. As a trivial example, any group ring element divisible by 2 has zero spectrum mod π for any prime π over (2).

On the other hand, the setness theorem 5.20 in section 5.3 allows us to say a few things.

Proposition 5.37 *A counter-example to Dillon's conjecture is completely determined by its character values mod π on homomorphic images.*

Proof: We know from Theorem 5.20 that any set is completely determined by its mod π spectrum. We also know from Proposition 4.20 that the entire non-faithful spectrum can be generated from group homomorphic images into G/H for subgroups H of G. ■

Remark *A counter example to Dillon's conjecture would be in the kernel of the faithful part P_F of the matrix P_π over $GF(2)$. Since sets in this context are determined by their mod π spectrum, understanding this kernel should be enough.*

Remark *Dillon's conjecture is true in case all the nontrivial divisors w of v are self-conjugate, since then the non-faithful spectrum of D is also forced to be 0 mod π which would imply $D = 0$.*

Next we restate the question of p-rank of difference sets in terms of C.

A theorem of MacWilliams and Mann gives the K-rank of the group ring element A (where the K-rank of A is defined as the dimension of the ideal generated by A in KG).

Theorem 5.38 *(MacWilliams and Mann, 1968)(cf. [Pott, p.25]) Let G be an abelian group of order v and K a field of characteristic p not dividing v, and containing v^{th}*

roots of unity. Then the K-rank of A is the number of characters χ of G such that $\chi(A) \neq 0$.

For $K = GF(p)$, this rank is clearly visible in the mod π spectrum $\mathcal{S}_\pi(A)$ where π is any prime ideal over (p). Since $(\mathcal{S}_\pi(A))_i = \chi_i(A) \bmod \pi$ as χ_i runs over orbit representatives of G^* under Λ,
to compute this rank we sum up the orbit size of χ_i for all i such that
$(\mathcal{S}_\pi(A))_i \neq 0$. (These orbit sizes are given by the first row of P.) Thus, questions about the p-rank of group ring elements can be restated as questions about the kernel of P_π over $GF(p)$. The p^t-rank is given in the same way by the $\mathcal{S}_{\pi^t}$ for any t, so the mod π^t spectrum actually carries much more information than the p-rank.

Recall from chapter 3 that Pott noted that among difference sets with the classical parameters (3.23), no abelian but non-cyclic example is known. One reason for this lack of knowledge is that the technique used to study difference sets with parameters (3.23) is to focus on the quotient $GF(q^n)^*/GF(q)^*$ which restricts attention to this (cyclic) group. On the other hand, the cyclotomic coset scheme $\mathcal{C}(G, \Lambda)$ and its matrix P can be built for any abelian group G and automorphism group Λ, hence the techniques involving the cyclotomic coset scheme do not limit us to the study of cyclic groups. The classical parameters come with a numerical multiplier so the Λ is given to us in the non-cyclic context as well.

Also mentioned in section 3.4 was the exhaustive ennumeration of (cyclic) difference sets with given parameter set - especially for those with parameters $(2^t - 1, 2^{t-1}, 2^{t-2})$. All the searches done for $2 \leq t \leq 10$ made extensive use of homomorphic images, and little to no use of faithful characters. The matrix P_F on the other hand, can be used to thoroughly investigate the faithful characters.

For the rest of this section we return to the question of factorization raised in

chapter 3. We will confine ourselves to factorizations in the scheme $\mathcal{C}(G, \Lambda)$. From the difference set perspective we are just asking that the factors be fixed by the same multiplier as the difference set. This property is obeyed by all the factorizations mentioned in section 3.4. We begin by formally defining divisibility:

Definition 5.39 *Let $D \in \mathcal{C}(G, \Lambda)$. Then we say $A|D$ in $\mathcal{C}$ if (and only if) $D = AB$ for $A, B \in \mathcal{C}$.*

Remark *Implicit in the definition is that the factors must be integral.*

There seem to be two avenues to approach questions of factorization in $\mathcal{C}(G, \Lambda)$. Both approaches involve some serious difficulties. The first approach is to transform questions about factorization in the scheme $\mathcal{C}$ to questions about factorizations of ideals in $\mathbb{Z}[\zeta_v]$.

The second approach is to find elements of $\mathcal{C}$ that are factors of the given element only 'mod p^e' for an appropriate prime p. This avoids the number ring difficulties of the first approach, but at the expense of finding 'extraneous' factors that aren't factors over $\mathbb{Z}$.

The following simple lemma follows from the definition, the fact that group characters extend to group ring homomorphisms and the inversion formula:

Lemma 5.40 *If D, A, and $B \in \mathcal{C}(G, \Lambda)$ then $D = AB$ if and only if $\varphi(D) = \varphi(A)\varphi(B)$ for all representations φ of $\mathcal{C}(G, \Lambda)$.*

The lemma illustrates one difficulty with factoring arbitrary elements $\mathcal{C}(G, \Lambda)$. If $\varphi(D) = 0$ for some representation φ of $C_R(G, H)$ then $\varphi(A)$ is left unconstrained by this condition. This is illustrated in the example below.

Example 5.41 *In $\mathbb{Z}Z_2$ let $D = (1 + x)$. The representation $\varphi : x \mapsto -1$ has $\varphi(D) = 0$. Let $A = (t + 1 - tx)$. One can check that $(-D)A = D$ so we have $A|D$ for any $t \in \mathbb{Z}$. The representation with zero value on D allows us to find divisors of D with arbitrarily large coefficients; a situation we naturally wish to avoid.*

Now suppose that we are given $D \in \mathcal{C}(G, \Lambda)$ satisfying a group ring equation like (3.3), where $\varphi(D)$ is nonzero for all representations φ of $\mathcal{C}$, and that we seek some (or all) factors A of D in $\mathcal{C}(G, \Lambda)$.

Using the number ring approach, suppose that $\varphi(D) = \beta$ for some irreducible character φ of $\mathcal{C}(G, \Lambda)$. We seek $\alpha \in \mathbb{Z}[\zeta_v]$ with $\alpha \mid \beta$ in $\mathbb{Z}[\zeta_v]$. Since $\mathbb{Z}[\zeta_v]$ isn't a UFD in general, we work with ideals. As ideals of $\mathbb{Z}[\zeta_v]$, $(\beta) = I_1^{k_1} I_2^{k_2} \cdots I_s^{k_s}$ where the ideals I_i are maximal. The condition α divides β forces $(\alpha) = I_1^{j_1} I_2^{j_2} \cdots I_s^{j_s}$ with $j_i \leq k_i$ for all i.

In the applications we are particularly interested in (difference sets with the classical parameters(3.23)), the number ring elements $\beta = \varphi(D)$ we wish to factor satisfy $\beta\overline{\beta} = p^e$ for some prime p not dividing v and $e \geq 1$. We will take this simplifying assumption.

Definition 5.42 *An ideal $I \subseteq \mathbb{Z}[\zeta_v]$ is* **strictly over** (p) *(or SOp) if for any prime ideal π in $\mathbb{Z}[\zeta_v]$, whenever $\pi | I$, then $\pi | (p)$.*
We will say an element $\alpha \in \mathbb{Z}[\zeta_v]$ is SOp if the principal ideal (α) is SOp.

Proposition 5.43 *An ideal I of $\mathbb{Z}[\zeta_v]$ is SOp if and only if I is the product $\prod_{i=1}^{s} \pi_i^{e_i}$ where the π_i are the prime ideals lying above (p) in $\mathbb{Z}[\zeta_v]$ and $e_i \geq 0$.*

Proof: Since $\mathbb{Z}[\zeta_v]$ is a Dedekind domain any ideal I factors completely into a product of powers of prime ideals. The definition forces these ideals to be the prime ideals over (p). ■

Proposition 5.44 *$\alpha \in \mathbb{Z}[\zeta_v]$ is SOp if and only if $\prod g(\alpha) = \pm p^t$ for some positive integer t , where the product is taken over all $g \in \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_v))$*

Proof: For any $\alpha \in \mathbb{Z}[\zeta_v]$, the product $\prod g(\alpha) = m$, an integer.
So if an ideal π divides (α) then the ideal $\mathbb{Z} \cap (\alpha)$ divides (m). ∎

Corollary 5.45 *If $\beta\overline{\beta} = p^e$ then β is SOp.*

To summarize the above discussion, we seek ideals I which are

1. *SOp.*
2. Principal, so that $I = (\alpha)$ corresponds to a single element.
3. Have valuation $\nu_{\pi_i}(I) \leq \nu_{\pi_i}((\beta))$ for all i.

We will discuss each of these properties below. We start with *SOp*:

We have criteria above for an ideal to be *SOp*. However, the first doesn't guarantee principal ideals, and the second requires generating the entire Galois group. It is possible to check this property using a matrix model that doesn't require explicitly generating the Galois group:

The map $\zeta_v \mapsto M_v :=$ (the companion matrix of Φ_v) is an isomorphism of $\mathbb{Z}[\zeta_v]$ into $\mathrm{Mat}_{\phi(v)}\mathbb{Z}[\zeta_v]$ (where ϕ is the Euler ϕ-function). If we map an element
$\alpha = \sum a_i(\zeta_v^i) \mapsto \sum a_i M_v^i =: M(\alpha)$
then the principal ideal (α) is the column space (over $\mathbb{Z}$) of $M(\alpha)$.

Remark *More generally, if $I =< \alpha_1, \ldots, \alpha_t >$, then I can be represented as the column space of the augmented matrix $M(I) := [M(\alpha_1)|M(\alpha_2)\cdots|M(\alpha_t)]$*

Theorem 5.46 *An ideal I of $\mathbb{Z}[\zeta_v]$ is SOp if and only if the invariant factors of $M(I)$ consist only of powers of p.*

Proof: The diagonal form of $M(I)$ displays the $\mathbb{Z}$-module corresponding to I as a direct sum of cyclic modules. ∎

Remark *We already know the maximal (prime) ideals π_i above (p) in $\mathbb{Z}[\zeta_v]$ from Theorem 2.30. They are given by $\pi_i = (f_i(\zeta_v), p)$ where $f_i(x)$ is a factor of $\Phi_v(x)$ over $GF(p)$. These ideals are not principal in general, however. When π_i is not principal, the principal ideal $(f_i(\zeta_v))$ will not be SOp.*

Next we discuss principality and valuations:

It is a result of number theory that given v, there is some integer $h(v)$, $1 \leq h(v) < \infty$ (called the 'class number' of $\mathbb{Z}[\zeta_v]$), such that, for any ideal $I \subseteq \mathbb{Z}[\zeta_v]$, the ideal $I^{h(v)}$ is guaranteed to be principal. Also, if $(p) = \prod \pi_i$ then $\prod \pi_i^{k_i}$ is principal for $k_i = 1$ for all i.

If D is a group ring element element satisfying the difference set equation (3.23), then $(\beta) = (\varphi(D))$ is principal. If β is *SOp* then $(\beta) = \prod \pi_i^{k_i}$. This is where the valuations enter the picture. The divisibility question becomes: Find $k_i' \leq k_i$ so that the product ideal $\prod \pi_i^{k_i'}$ is (still) principal.

Question 5.47 *Let p be prime, not dividing v. What are (minimal) sets $\{k_1', k_2', \ldots k_s'\}$ of integers for which the product $\prod \pi_i^{k_i}$ is principal in $\mathbb{Z}[\zeta_v]$*

The remarks above imply that the set $k_i = 1$ for all i gives a principal ideal. Also, note that the Singer difference sets give us a set with some $k_i = 0$, and that Dillon's conjecture is relevant to this question.

We get a more satisfying answer to the factorization questions if we shift to the second approach to factoring in $\mathcal{C}(G, \Lambda)$. By working modulo π^t, we can find all the candidates for factors with bounded coeffiecients. First we give the algorithm for

finding all factors of a scheme element modulo p^t. (The algorithm appears in the proof.)

Theorem 5.48 *Let $D \in C(G, \Lambda)$ where $exp(G) = v$, p is a prime not dividing v, and Λ contains the map $\sigma : g \mapsto g^p$ for all $g \in G$. Suppose D has valuation vector $\nu_{\pi^t}(D) = (d_1, d_2, \ldots d_s)^T$. Then any element A of C with valuation vector $\nu_{\pi^t}(A) = (a_1, a_2, \ldots a_s)^T$ with $0 \leq a_i \leq d_i$ is a divisor of D mod p^t.*

Proof: If D has the given valuation vector, then the mod π^t spectrum of D is $\mathcal{S}_{\pi^t}(D) = (u_1 p^{d_1}, u_2 p^{d_2} \ldots u_s p^{d_s})$ where the u_i are units mod p^t for all i. Similarly the mod π^t-spectrum of A is given by $\mathcal{S}_{\pi^t}(A) = (u'_1 p^{a_1}, u'_2 p^{a_2} \ldots u'_s p^{a_s})$ where u'_i are units mod p^t and $a_i \leq d_i$ for all i.
Then one complementary factor is B defined by

$$\mathcal{S}_{\pi^t}(B) = (u_1 (u'_1)^{-1} p^{d_1 - a_1}, u_2 (u'_2)^{-1} p^{d_2 - a_2} \ldots u_t (u'_t)^{-1} p^{d_s - a_s}).$$

Since P is invertible (and integral) mod π^t we have that $A := P_{\pi^t}^{-1} \circ \mathcal{S}_{\pi^t}(A)$ and $B := P_{\pi^t}^{-1} \circ \mathcal{S}_{\pi^t}(B)$ (where $\circ$ represents matrix multiplication modulo p^t). Both A and B have integral entries and hence are elements of the scheme C. Also, since $\varphi(D) = \varphi(A)\varphi(B)$ for all representations φ of $C(G, \Lambda)$ we may apply Lemma 5.40 and we are done. ∎

For combinatorial applications, we may wish to find all factorizations over the integers of a given element where the factors arise from SETS, or, more generally, we may wish to find all factors A having bounded coefficients $0 \leq a_i \leq M$ (hence arising from multisets). A factor of D having these bounded coefficients must appear as a factor of D modulo p^t where $p^t \leq M$.

Example 5.49 *Let D be the $(15, 8, 4)$ difference set $C_3 + C_1$ (see example 4.13). D has mod π valuation vector $\nu_\pi(D) = [1, 1, 1, 0, 1]^T$ for a prime π over (2) in $\mathbb{Z}[\zeta_{15}]$.*

Any scheme element A with valuation vector $\nu_\pi(A) = [a_1, a_2, a_3, 0, a_4]^T$ where the a_i are all 0 or 1 will be a divisor of D mod 2. There are 16 such divisors.

We test each of these 16 mod 2 factors to see whether it divides D over $\mathbb{Z}$. There were 4 survivors, corresponding to $1, D, C_5, and C_{-1}$. Therefore, these are the only $\mathbb{Z}$- factors corresponding to sets. The factorization $D = C_5 C_{-1}$ is the Gordon Mills Welch factorization.

6 Looking Further

In this dissertation we have seen that the cyclotomic coset association scheme is a valuable tool for the study of abelian difference sets and similar structures having a multiplier group. In particular:

- The multiplier is built into the scheme, so less information is required. Characters in the same Λ- orbit are redundant.

- The primary algebraic tool for working in the scheme (the character table P) is reasonably easy to compute in the number ring $\mathbb{Z}[\zeta_v]$ and especially modulo π^t when π is a prime ideal above any prime p not dividing v whenever the automorphism taking group elements to their p^{th} powers is in Λ.

- The standard techniques are still available to us:
  Group homomorphic images, complex characters and field techniques all have their analogues in the scheme $\mathcal{C}$.
  In particular, the trace function $tr_q^{q^n}$ is easily computed from the character table $P(G, \Lambda)$ where $G = GF(q^n)^*$ and Λ is generated by the automorphism $x \mapsto x^q$.

- The larger field $GF(q^n)$ in trace based constructions is inessential.

- In some special (but not rare!) cases we get additional tools for handling the tricky combinatorial issues of integrality with bounded coefficients and set-ness. In particular we can reconstruct sets from mod π information alone.

- There is an easy algorithm for finding (all) factors of a given element of the scheme mod p^k.

The methods discussed in this dissertation thus have applications to the study of abelian difference sets and also open up some new avenues for discussion. Issues we would particularly like to resolve (and for which the scheme may be the best approach) include:

- Given any cyclic difference set with the classical parameters, find a v-difference balanced function.
- Give conditions on the character values of integral elements in the $\mathbb{Z}$- column space of the matrix $P(G, \Lambda)$. Give conditions on the character values of sets using the matrix P_π.
- Settle Dillon's conjecture.
- Find non-cyclic difference sets with the classical parameters.
- Use the mod p^t factorization with the SOp property answer the ideal factorization question posed in section 5.4.
- Decide whether the only integer factorization of a Singer difference set into a product of sets is given by the Gordon Mills Welch factorization.

References

[Bac] R. Bacher: Cyclic Difference Sets With Parameters $(511, 255, 127)$ *L'Enseignement Mathematique*, Vol. 40, 1994, 187-192.

[Bau] L.D. Baumert: *Cyclic Difference Sets.* Springer-Verlag, Berlin, 1971.

[BI] E. Bannai and T. Ito: *Algebraic Combinatorics I: Association Schemes.* Benjamin/Cummings, Menlo Park, CA, 1984.

[BM] E. Bannai and A. Munemasa: Davenport-Hasse Theorem and Cyclotomic Schemas. *Manuscript* (1990).

[BJL] T. Beth, D. Jungnickel, and H. Lenz: *Design Theory* . Cambridge University Press, Cambridge, 1986.

[BCN] A.E.Brouwer, A.M. Cohen, and A. Neumaier: *Distance - Regular Graphs.* Springer-Verlag, Berlin,1989.

[CS] A. Calderbank and N. Sloane: Modular and p-adic Cyclic Codes. *Designs, Codes, and Cryptography*, Vol. 6, No. 1, 1995, 21-35.

[Ch] U. Cheng: Exhaustive Construction of $(255, 127, 63)$-Cyclic Difference Sets. *J. Combinatorial Theory (Series A)*, Vol. 35, 1983, 115-125.

[CR] C. Curtis and I. Reiner: *Representation Theory of Finite Groups and Associative Algebras* . John Wiley & Sons, New York, 1988.

[CR2] C. Curtis and I. Reiner: *Methods of Representation Theory Vol. 1.* John Wiley & Sons, New York, 1981.

[Di] J. Dillon: Cyclic Difference Sets and Primitive Polynomials *Finite Fields, Coding Theory, and Advances in Communications and Computing* G. Mullen and P. Shiue (eds) Marcel Dekker, New York, 1993.

[DS] R. Drier and K. Smith: Exhaustive Determination of (511,255,127) Cyclic Difference Sets *Unpublished*, (1991).

[GG] P. Gaal and S. Golomb: Exhaustive Determination of (1023, 511, 255)-Cyclic Difference Sets. *Mathematics of Computation*, Vol. 70, No. 233, 2000, 357-366.

[GC] R. Goldbach and H. Clasen: Cyclotomic Schemes Over Finite Rings. *Indagationes Mathematicae*, Vol. 3, No. 3, 1992, 301-312.

[GC2] R. Goldbach and H. Clasen: Cyclotomic Schemes Over Finite, Commutative, Admissible Rings. *Indagationes Mathematicae*, Vol. 3, No. 3, 1992, 277-299.

[Ii] J.E. Iiams: Lander's Tables Are Complete! *Difference Sets, Sequences, and their Correlation Properties* A. Pott et al. (eds) Kluwer Academic Publishers, Netherlands, 1999.

[IR] K. Ireland and M. Rosen: *A Classical Introduction to Modern Number Theory* 2nd Ed., Springer-Verlag, New York, 1990.

[Is] I. Isaacs: *Character Theory of Finite Groups.* Academic Press, New York, 1976.

[Io] Y. J. Ionin: A Technique for Constructing Divisible Difference Sets. *Journal of Geometry*, Vol.67, 2000, 164-172.

[MA] A. Maschietti: Difference Sets and Hyperovals. *Designs, Codes, and Cryptography*, Vol. 14, 1998, 89-98.

[No] Jong-Seon No: New Cyclic Difference Sets with Singer Parameters Constructed from d-Homogeneous Functions. *Designs, Codes, and Cryptography*, to appear.

[Pott] A. Pott: *Finite Geometry and Character Theory.* Springer-Verlag, Berlin, 1995.

[Sc] B. Schmidt: Cyclotomic Integers and Finite Geometry. *Journal of the American Mathematical Society.* Vol. 12, No. 4, 1999, 929-952.

[St] T. Storer: *Cyclotomy and Difference Sets.* Markham Publishing Company, Chicago, 1967.

[Tur] R.J.Turyn: Character Sums and Difference Sets. *Pacific Journal of Mathematics*, Vol. 15, No. 1, 1965, 319-346.

[Xi] Q. Xiang: Recent Results on Difference Sets with Classical Parameters. *Difference Sets, Sequences, and their Correlation Properties* A. Pott et al. (eds) Kluwer Academic Publishers, Netherlands, 1999.