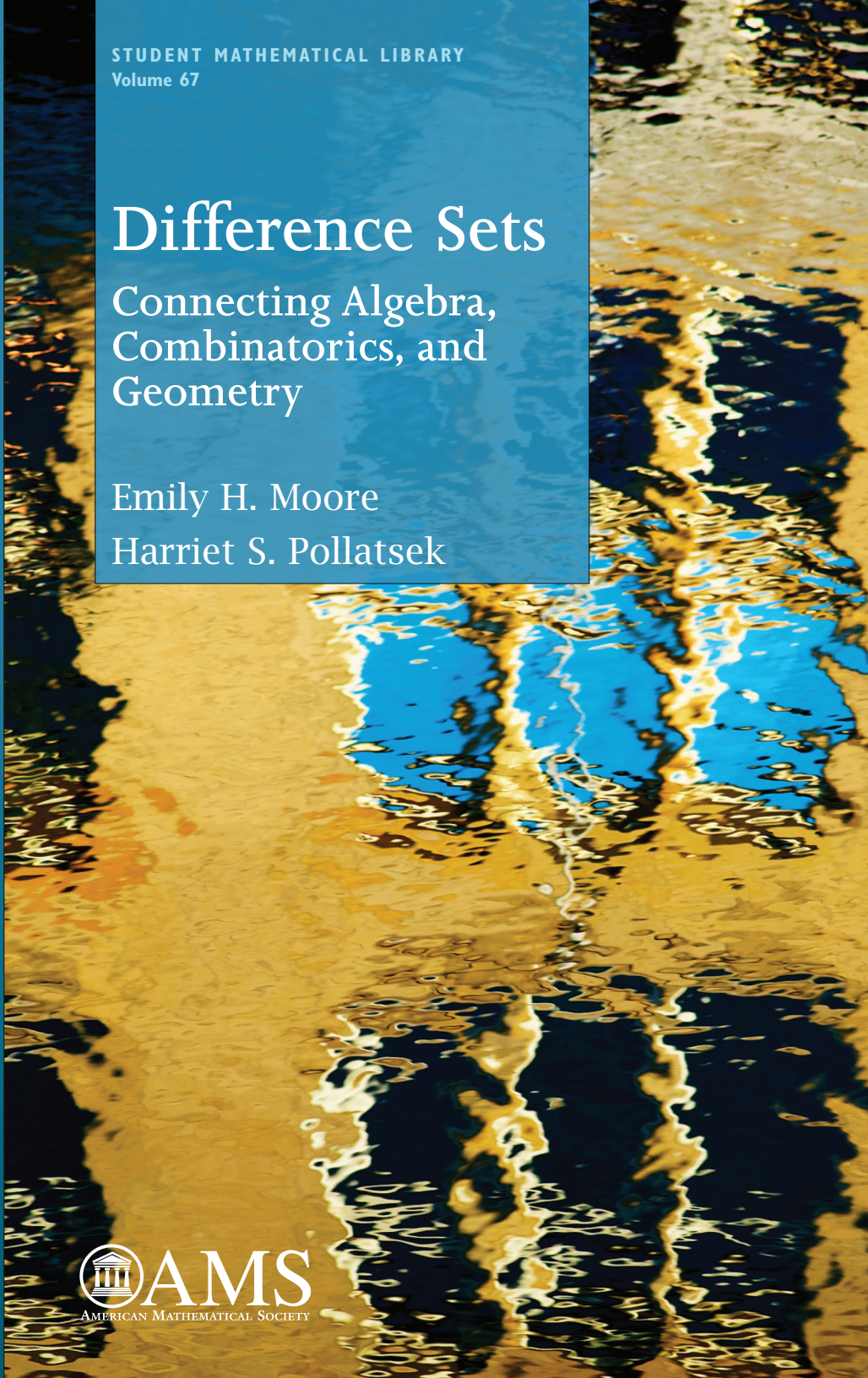
STUDENT MATHEMATICAL LIBRARY
Volume 67

Difference Sets

Connecting Algebra, Combinatorics, and Geometry

Emily H. Moore
Harriet S. Pollatsek



AMS
American Mathematical Society

Difference Sets

Connecting Algebra, Combinatorics, and Geometry

STUDENT MATHEMATICAL LIBRARY
Volume 67

Difference Sets

Connecting Algebra, Combinatorics, and Geometry

Emily H. Moore
Harriet S. Pollatsek

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 05B10, 05B20, 05B25, 11R04, 20C15, 51E15.

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-67

Library of Congress Cataloging-in-Publication Data

Moore, Emily H., 1948–
Difference sets : connecting algebra, combinatorics, and geometry / Emily H. Moore, Harriet S. Pollatsek.
pages cm. — (Student mathematical library ; volume 67)
Includes bibliographical references and indexes.
ISBN 978-0-8218-9176-6 (alk. paper)
1. Difference sets. 2. Combinatorial geometry. I. Pollatsek, Harriet Suzanne Katcher. II. Title.

QA166.25.M66 2013
511′.6—dc23 2013006295

10 9 8 7 6 5 4 3 2 1 18 17 16 15 14 13

To Jack, Edie, and Ian Broadmoore

and to the memory of

David Pollatsek and Robert Liebler

Contents

Preface

We are drawn to the study of difference sets because this topic "belongs both to group theory and to combinatorics and ... uses tools from these areas as well as from geometry, number theory, and representation theory" (quoting from the opening of Chapter 1). Each of us has supervised undergraduate research on difference sets. Our original goal in writing this book was to collect in one place the material beyond a one-semester abstract algebra course required to prepare our students for these research projects. However, the links to many parts of mathematics led to our current, broader aim: not only to serve prospective undergraduate researchers but also to provide a rich text for a senior seminar or capstone course in mathematics. With this expanded goal in mind, we highlight these mathematical interconnections.

We never intended our book to be a comprehensive survey of difference sets. However, we hope it will encourage students to explore the literature on difference sets and give them a solid foundation so they can do so successfully.

We assume student readers have taken an abstract algebra course.[1] We show them concrete examples of some algebraic ideas they studied there, and we apply and extend these concrete instances in a variety

[1] Appendix A includes the background we need from prior courses, and specific results are cited using the notation A.x.

of settings. Some of our exposition, especially in earlier chapters, is very thorough, with reasoning fully explained. The proofs of some theorems are explicitly left for the exercises, and some of these exercises offer the student considerable guidance. For other theorems we may give rather terse proofs, more like what a student would encounter in a journal article. Normally we expect the reader to fill in any omitted arguments, so we don't write "see the exercises" for each instance. In a few cases we quote theorems without proof, but always with a reference, and often with a comment on the accessibility of the proof given in the cited source.

Almost every section of the book ends with exercises. Some exercises aim to check the reader's understanding of a definition or a proof. Some ask for proofs (with or without guidance). Some are puzzles to be solved. Some invite the student to explore ideas and examples, sometimes with the aid of a computer (and so indicated). All of these kinds of exercises vary from straightforward to challenging. Appendix C includes hints for exercises marked Ⓗ and solutions to selected exercises marked Ⓢ.[2] Every chapter except the first and the last ends with a brief *Coda*[3] highlighting the main ideas and emphasizing mathematical connections.

Examples and exercises are numbered consecutively within chapters with, for example, Exercise 5 within a chapter and Exercise 7.5 for a reference to Exercise 5 in Chapter 7 made in a different chapter. Theorems are also numbered consecutively within chapters and are always referred to with both a chapter label and a theorem label, as, for example, Theorem 7.5 both within and outside of Chapter 7.

After the Introduction, Chapters 2–4 comprise the core of the book. We then see two kinds of selective paths through the rest. One would focus on representation theory and its applications. It would include Section 7.1 on intersection numbers, the constructions of difference sets in Chapters 8–9, Chapters 10–12, and Section 13.4. Another path would focus on the existence question for difference sets. It would include Chapters 5–9. Even if Chapters 10–12 are not

[2]Complete solutions are available electronically for instructors; please send email to textbooks@ams.org for more information. Some helpful computer programs are available at `http://www.ams.org/publications/authors/books/stml-67`.

[3]We borrow the term "coda" in this context from Jennifer Quinn.

covered, Sections 10.4 and 11.4 give a taste of the use of representation theory and characters in the study of difference sets. The applications in Sections 13.1–13.3 are suitable for readers following either path.

Acknowledgements.

We wish to thank the senior seminar and research students at Grinnell College and the REU students at Mount Holyoke College. Their enthusiasm inspired us, and their questions and reactions helped us shape this text. Mark Krusemeyer allowed us to borrow ideas and exercises from his Spring 2004 course on representation theory at Carleton College; we appreciate his generosity. We thank Robert McFarland for his sympathetic interest. John Polhill read several chapters and James A. Davis used parts of an early draft with an independent student; we thank them both for their encouragement. We owe a particular debt to Ken W. Smith, who read and commented on drafts of several chapters. We thank an anonymous reviewer for valuable advice on our treatment of the integral group ring. We are responsible for any errors or infelicities that remain. We are grateful for our support from the AMS: especially to Barbara Beeton for her unstinting technical assistance, to Thomas Costa for his careful and thoughtful copy-editing, and to Ina Mette for her interest and encouragement from the early days of our writing project. Finally, we thank Tom and Sandy for their love, support and many delicious dinners.

Emily Moore
Grinnell College

Harriet Pollatsek
Mount Holyoke College

Chapter 1

Introduction

Here we introduce some of the topics in this book—briefly, but we hope invitingly. The ideas will be developed more fully and their inter-relations more thoroughly examined in the chapters that follow.

This book has two over-arching themes. One is that different parts of mathematics can and do come together in surprising and illuminating ways: suggesting questions, providing tools, and generating examples. The other is the idea of a difference set—a special subset of a group. It exemplifies the first theme, since it belongs both to group theory and to combinatorics, and the study of difference sets uses tools from these areas as well as from geometry, number theory, and representation theory.

A group is often useful when it acts on a set or a structure. As we shall explain, a group contains a difference set if and only if it acts in a particular way on a nice structure called a symmetric design. Thus finding a difference set is equivalent to finding an interesting group action. Also, difference sets are of intrinsic interest because they yield applications in communications and other areas.

So what is a difference set? If a finite group G is written additively, a non-empty proper subset D of G is a (v, k, λ)-*difference set* if $|G| = v$, $|D| = k$ and there is an integer λ such that each non-identity element of G can be expressed in exactly λ ways as a difference $d_1 - d_2$ of elements of D. Equivalently, we require that

each non-identity group element appears λ times in the *multiset*

$$\Delta = \{d_1 - d_2 \,|\, d_1, d_2 \in D, d_1 \neq d_2\}.$$

(The word "multiset" means that elements may be listed more than once.)

Example 1. Choose

$$G_1 = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\},$$

the additive group of integers modulo 7, and choose

$$D_1 = \{1, 2, 4\}.$$

To check that D_1 is a $(7, 3, 1)$-difference set in G_1, it is convenient to organize our work in a table.

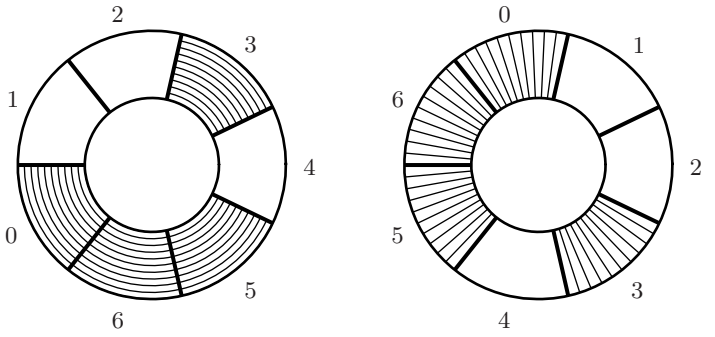
$-$	1	2	4
1	0	$-1 = 6$	$-3 = 4$
2	$2 - 1 = 1$	0	$-2 = 5$
4	$4 - 1 = 3$	$4 - 2 = 2$	0

Each of $1, 2, 3, 4, 5, 6$ appears exactly once in the table, confirming that D_1 is a $(7, 3, 1)$-difference set. $\diamond$

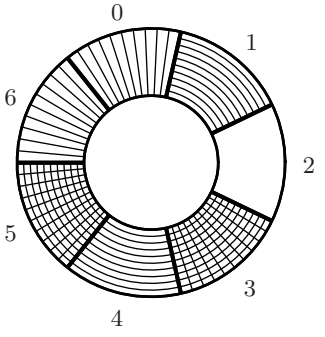
We can use the difference set of Example 1 to glimpse one of the applications of difference sets. We might want to robotically align a cylindrical nozzle within a circular opening without deforming either the nozzle or the opening. Example 2 illustrates the general idea. We say more about this application in Chapter 13.

Example 2. The context here is refueling an airplane. Suppose that to optimize the refueling, the cylindrical nozzle on the fuel hose has to be aligned just right within the circular opening of the fuel tank. Imagine that the tank opening is surrounded by a circular ring divided into 7 cells numbered $0, 1, 2, \ldots, 6$. The cells numbered 1, 2 and 4 emit light and the others do not. A second similarly-patterned ring is on the nozzle, backed up by a light detector. The cells numbered 1, 2, 4 on the nozzle ring are transparent to light; the others are opaque. When the two rings are perfectly aligned, the maximum amount of light is detected. When they are out of alignment by as few as 1 or 2 cells, the amount of light detected is much less. In Figure 1.1, the

ring in (a) surrounds the opening of the tank, and the ring in (b), on the nozzle, has been rotated clockwise by 2 cells. The ring in (c) shows the light reaching the detector on the nozzle. (See Figure 13.1 for a graph of the amount of light detected when the nozzle is in various positions.) A robot can adjust the nozzle to maximize the light reaching its detector and thereby position it correctly. ◇



(a) tank opening **(b)** nozzle shifted by 2



(c) light detector

Figure 1.1. Alignment model for Example 2

Now we return to Example 1. Since $\mathbb{Z}_7$ is also a ring, we can multiply as well as add. Notice that the elements of D_1 are the nonzero squares in $\mathbb{Z}_7$. As we see later, this example can be generalized. We

take a partial step toward that generalization, but first we need to do some counting.

Suppose D is a (v, k, λ)-difference set. There are $k(k-1)$ ordered pairs (d_1, d_2), with d_1, d_2 distinct elements of D, and therefore $k(k-1)$ differences $d_1 - d_2$ in the multiset Δ. However, because D is a difference set, each of the $v-1$ non-identity elements of G appears exactly λ times among the elements listed in Δ. We have proved the following theorem.

Theorem 1.1. *Assume D is a (v, k, λ)-difference set. Then*

$$k(k-1) = \lambda(v-1).$$

We use this theorem to help us determine a necessary condition for the generalization of Example 1.

Theorem 1.2. *Let p be an odd prime, and let D be the set of nonzero squares in $\mathbb{Z}_p$. If D is a difference set in the additive group $\mathbb{Z}_p$, then $p \equiv 3$ (mod 4).*

Proof. Assume D is a difference set in $\mathbb{Z}_p$. We know $v = p$, and we want to determine $k = |D|$. Since p is prime, the $p-1$ nonzero elements of $\mathbb{Z}_p$ form a group under multiplication. We denote this multiplicative group by $\mathbb{Z}_p^*$. Consider the function mapping each element of $\mathbb{Z}_p^*$ to its square. This is a homomorphism onto D. Because p is an odd prime, $x^2 = 1$ implies $x = \pm 1$, so the kernel of this homomorphism has size 2. Therefore, there are exactly $(p-1)/2$ nonzero squares in $\mathbb{Z}_p$, and $k = (p-1)/2$. Now Theorem 1.1 tells us that $\lambda = k(k-1)/(v-1) = (p-3)/4$. But λ must be an integer, so $p \equiv 3 \pmod 4$. □

The idea of a difference set first appeared in the 1938 paper, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," by James Singer [**62**]. Where is the geometry in our example of a $(7, 3, 1)$-difference set?

We create a geometry by specifying *points* and special sets of points called *blocks*. The points are the 7 elements of G_1, and the blocks are D_1 together with its 6 translates $a+D_1 = \{a+1, a+2, a+4\}$

for $a \in G_1$, $a \neq 0$. The 7 blocks are:

$$\{1,2,4\}\ \{2,3,5\}\ \{3,4,6\}\ \{4,5,0\}\ \{5,6,1\}\ \{6,0,2\}\ \{0,1,3\}.$$

Note that two distinct points appear together in exactly one block and that two distinct blocks have exactly one point in common. If we call blocks "lines," we say informally that two points determine a line and two lines determine a point; there are no parallel lines. This example meets the non-degeneracy conditions that there are at least three points in each block and at least two blocks. Thus we have an example of a non-Euclidean geometry called a finite *projective plane*.

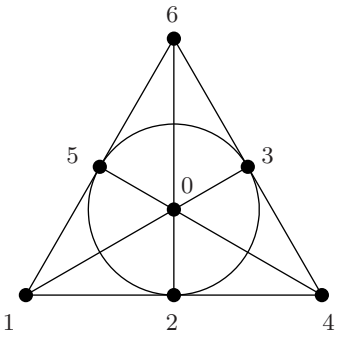


Figure 1.2. The Fano plane

More generally, a set of v *points* and v sets of points called *block*s form a *symmetric design* with parameters (v, k, λ) if every block contains k points, every point belongs to k blocks, two distinct points occur together in λ blocks, and two distinct blocks intersect in λ points. Our geometry is thus a symmetric design[1] with parameters $(7, 3, 1)$. This specific geometric structure is often called the *Fano plane*; see Figure 1.2 for a picture. In this picture, most blocks are represented by line segments; the block $\{2, 3, 5\}$ is represented by a circle.

Now we show how G_1 acts on this structure. Each element of the group G_1 can be regarded as a function taking points to points: the group element a takes the point b to the point $a + b$. Indeed, since

[1] We study designs, including symmetric designs, in Chapter 2.

distinct points go to distinct points, this function is a *permutation* of the points. This function can also be applied to blocks: it takes the block $B = m + D_1$ to the block $a + B = (a + m) + D_1$. Again, distinct blocks go to distinct blocks, so it is a permutation of the blocks. If point x is in block B, then the point $a + x$ is in the block $a + B$. This means that the elements of G_1 act as *automorphisms* of the geometry.

These permutations are special. We can see that G_1 acts *transitively* on the set of 7 points: given any two points b and c, there is a permutation (i.e., an element a of G_1) taking b to c, namely $a = c - b$. Similarly, G_1 acts transitively on the set of 7 blocks: given any two blocks $b + D_1$ and $c + D_1$, there is a permutation taking $b + D_1$ to $c + D_1$, namely $a = c - b$ again. Of course the identity $a = 0$ fixes every point and every block. But the converse is true too. If $a + b = b$ then a must be 0; and similarly (but less obviously) for blocks, if $a + B = B$ then $a = 0$.

We summarize these properties by saying G_1 acts as a *regular* group of automorphisms of the geometry we have defined. In fact, as we prove in Chapter 4, a finite group G contains a (v, k, λ)-difference set if and only if G acts as a regular group of automorphisms of a symmetric (v, k, λ) design.

We have used the group and the difference set to construct the design. How do symmetric designs arise "in nature"? Here is a construction that will take us back to the Fano plane. Choose the field $\mathbb{Z}_2 = \{0, 1\}$, with arithmetic modulo 2. Let V be the 3-dimensional vector space $(\mathbb{Z}_2)^3$. The vector space V contains exactly 2^3 vectors and thus 7 nonzero vectors. Since 1 is the only nonzero scalar, V also contains exactly 7 one-dimensional subspaces. Call these 1-spaces *points*.

Further consequences of the fact that 1 is the only nonzero scalar are

- distinct nonzero vectors are linearly independent, and
- a two-dimensional subspace of V contains exactly 3 nonzero vectors.

In particular, notice that for distinct nonzero vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$, $\{\mathbf{0}, \mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a 2-space if and only if $\mathbf{u} + \mathbf{v} + \mathbf{w} = \mathbf{0}$. Call a triple of

points contained in a single 2-space a *block*. Each block thus contains 3 points. There are exactly 7 2-spaces of V and therefore exactly 7 blocks. We list them below (writing xyz instead of (x, y, z) for each vector and omitting curly braces):

$$\begin{array}{l} 100,\ 010,\ 110 \\ 100,\ 001,\ 101 \\ 100,\ 111,\ 011 \\ 010,\ 001,\ 011 \\ 010,\ 111,\ 101 \\ 001,\ 111,\ 110 \\ 011,\ 110,\ 101. \end{array}$$

Consulting the preceding list we see that two distinct points appear together in exactly one block, and two distinct blocks intersect in exactly one point.

Where is the group? Consider the linear transformation $T : V \to V$ with matrix

$$M = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

with respect to the standard basis.[2] We write transformations on the left, so a vector $\mathbf{v}$ is written as a column in calculating $T(\mathbf{v}) = M\mathbf{v}$. The matrix M^7 is the identity matrix, so T^7 is the identity function fixing every vector in V. From linear algebra we know that invertible linear transformations map 1-spaces to 1-spaces and 2-spaces to 2-spaces. Thus the elements of the group

$$G_2 = \{T, T^2, T^3, T^4, T^5, T^6, T^7 = I\}$$

map points to points and blocks to blocks. Indeed we can check that G_2 acts regularly on the points and on the blocks.

Since we are writing the group operation multiplicatively, we replace the difference $d_i - d_j$ by $d_i\, d_j^{-1}$ in the definition of a difference set. Now we see that the subset

$$D_2 = \{T, T^2, T^4\}$$

[2] Admittedly, this transformation appears to come out of the blue. We motivate it when we discuss Singer's work in Chapter 8.

is a $(7,3,1)$-difference set in G_2. (In fact, the obvious group isomorphism from G_1 to G_2 takes D_1 to D_2.)

In his 1938 paper, Singer constructed symmetric designs slightly differently, identifying the vector space V with a finite field containing 8 elements. His construction and analysis generalize to finite projective geometries obtained from higher-dimensional vector spaces over arbitrary finite fields. Other constructions of difference sets require even more ideas from finite geometry, and we will explore them in Chapter 8.

Now we have seen the $(7,3,1)$-difference set twice.[3] But how would we find this difference set if we did not know it was there? Or, how could we prove a particular group does *not* contain a difference set? To glimpse one strategy, we rewrite the group of order 7 one more time, this time as a subgroup of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers,

$$G_3 = \{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$$

for $\omega = \cos(2\pi/7) + i\sin(2\pi/7)$. We can add complex numbers, even though addition is not the group operation in this case. Observe what happens if we multiply the sum of the elements of the difference set

$$D_3 = \{\omega, \omega^2, \omega^4\}$$

by the sum of the inverses of those three elements in G_3:

$$\begin{aligned}(\omega + \omega^2 + \omega^4)(\omega^6 + \omega^5 + \omega^3) \\ &= 1 + \omega^6 + \omega^4 + \omega + 1 + \omega^5 + \omega^3 + \omega^2 + 1 \\ &= (1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6) + 2 \cdot 1.\end{aligned}$$

However, $1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = (1 - \omega^7)/(1 - \omega) = 0$, so we have

$$(\omega + \omega^2 + \omega^4)(\omega^6 + \omega^5 + \omega^3) = 2.$$

In other words, we have factored 2 in the ring $\mathbb{Z}[\omega]$ of integer linear combinations of powers of ω. Notice that $2 = k - \lambda$ in this example. This difference is important enough to get its own name. The quantity $n = k - \lambda$ is the *order* of a (v,k,λ)-difference set or symmetric design. Looking for factorizations of n in the ring $\mathbb{Z}[\eta]$ (where, in general, η

[3] Some of the ideas in this introduction appear in [**9**].

is an mth root of unity for some m dividing v) is a way to search for difference sets, or to prove they do not exist. However, $\mathbb{Z}[\eta]$ need not be a unique factorization domain, so this analysis requires some algebraic number theory. We develop these ideas in Chapter 12.

The group G_3 is actually the image of G_2 under the *representation* (i.e., group homomorphism) $\rho : G_2 \to \mathbb{C}^*$ defined by $\rho(T) = \omega$, and D_3 is the image of D_2. It is the representation ρ that gives us access to the factorization of n in $\mathbb{Z}[\omega]$. To pursue this line of investigation we need to study some representation theory. We offer a primer on representations and characters of finite groups in Chapters 10 and 11.

We now embark on our study, beginning first with designs, then moving on to difference sets. We hope this introduction has given some idea of the diversity and richness of the mathematical ideas we will encounter.

Chapter 2

Designs

In this chapter we introduce designs. Our ultimate goal is to study symmetric designs and their relationship to difference sets. Along the way we also introduce more general designs. Concepts of existence and equivalence that appear here will be mirrored in our study of difference sets.

Design theory is an area of combinatorics that was originally studied for its connections to statistics and the design of experiments. This study has found use in other areas of mathematics including geometry, coding theory, finite group theory, and difference sets. So the study of designs is a good place to start our exploration of the connections among these different algebraic and combinatorial structures.

2.1. Incidence structures

We start with the general notion of an incidence structure.

Definition. An incidence structure is an ordered triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ where

$\mathcal{P}$ is a set of points,

$\mathcal{B}$ is a set of blocks,

$\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is an incidence relation between $\mathcal{P}$ and $\mathcal{B}$.

If (p, B) is in $\mathcal{I}$, we say that p and B are incident.

A block is said to be "repeated" if it and another block are incident with precisely the same set of points. Repeated blocks can be useful in statistical designs. An incidence structure is known as simple if it has no repeated blocks. The incidence structures we will study are simple, so we can regard a block as a subset of points. If the point p and block B are incident with each other we say that $p \in B$. With blocks described as subsets of $\mathcal{P}$, we often drop the more formal notation for an incidence structure and simply write $(\mathcal{P}, \mathcal{B})$.

The concept of an incidence structure is so general it may seem at first not to be useful. However, it can be found in several places.

Example 1. In the Euclidian plane, we may take $\mathcal{P}$ to be the set of points, and $\mathcal{B}$ the set of lines. ◇

Example 2. We wish to run a statistical experiment to compare varieties of corn in various soils. In the design of the statistical experiment, we take the points to be the *varieties* of corn and the blocks to be the subsets of the varieties planted on particular plots. The different plots are more generally called *treatments*. ◇

Example 3. Represent a set of three people as $\mathcal{P} = \{a, b, c\}$ and specify four committees by $\mathcal{B} = \Big\{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\Big\}$. Person a is in all four committees, person b is in committees 2 and 4, and person c is in committees 3 and 4. ◇

In Example 1 the sets of points and blocks are infinite; in Examples 2 and 3 these sets are finite. Example 1 has the regularity condition that any two points are incident with exactly one block, since any two points determine a line. Example 3 has no such regularity. Even the blocks are of different sizes. In this book we will study mainly finite incidence structures.

Any finite incidence structure can be represented by an incidence matrix M where the columns represent points and the rows represent blocks,[1] and

$$m_{ij} = \begin{cases} 1 & \text{if } p_j \in B_i \\ 0 & \text{otherwise.} \end{cases}$$

[1] Note that some authors use the transpose of this matrix. Here we follow the convention in Lander[**43**], and Hall and Ryser[**29**].

Example 4. The following is the incidence matrix of the incidence structure in Example 3, with point set $\mathcal{P} = \{a, b, c\}$ and block set $\mathcal{B} = \Big\{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\Big\}$:

$$M \quad = \quad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} .$$

◇

An incidence matrix is not only a compact way to represent an incidence structure. Sometimes matrix multiplication gives us a tool for studying the incidence structure. For instance, we can multiply an incidence matrix by a permutation matrix to reorder the blocks or the points to check whether two incidence structures are essentially the same.

Definition. Two simple incidence structures $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ are isomorphic if there is a one-to-one mapping from $\mathcal{P}$ onto $\mathcal{P}'$ that maps $\mathcal{B}$ onto $\mathcal{B}'$.

The mapping must preserve the incidence structure. That is, if p maps to p' and B maps to B', then (p, B) is in $\mathcal{I}$ if and only if (p', B') is in $\mathcal{I}'$. As a consequence of this definition, simple incidence structures $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $(\mathcal{P}', \mathcal{B}', \mathcal{I}')$ are isomorphic if and only if we can permute the rows and columns of the incidence matrix of one to get the incidence matrix of the other. That is,

$$PMQ = M'$$

for permutation matrices P and Q. Note that P permutes the rows (blocks); Q permutes the columns (points).

In the exercises we will also explore what the calculations $M^T M$ and MM^T yield, where M^T is the transpose of M.

Exercises

1. For the incidence matrix given in Example 4,

(a) find a permutation matrix P that switches blocks (rows) 1 and 3. That is, PM is the matrix M but with rows 1 and 3 switched. Ⓢ

(b) find a permutation matrix Q so that MQ is the matrix M but with points (columns) 2 and 3 switched.

2. For the incidence matrix given in Example 4,

(a) compute MM^T. What do the entries of this product represent?

(b) compute M^TM. What do the entries of this product represent?

3. Construct an incidence matrix for the Fano plane in Chapter 1. Order the points and blocks so that each row is a circular shift to the right of the previous row. Compute MM^T and M^TM and explain the entries.

2.2. t-Designs

Designs are incidence structures on which some conditions of regularity are imposed. For instance, we might require that all blocks contain the same number of points, and that any two points be in a fixed number of blocks. The first type of design we will study is a t-design.

Definition. Let t be a non-negative integer.[2] A t-design is an incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ in which

(i) Each block contains k points, and

(ii) Each subset of t points is completely contained in exactly λ blocks for some $\lambda \geq 1$.

Since we will often talk about subsets of $\mathcal{P}$ of a particular size, we adopt the term s-set for a set of s points. Thus for a t-design, every t-set is in λ blocks. As an extreme case, a 0-set is the empty set, so

[2] Some authors (e.g., [**8**]) require that $t > 0$; others (e.g., [**70**]) require only that $t \geq 0$. We will adopt this latter restriction.

every incidence structure with constant block size is a 0-design with λ equal to the number of blocks.

If we let $v = |\mathcal{P}|$, then any t-design with these parameters is known as a t-(v, k, λ) design.[3]

Statisticians use 2-designs, called *block designs*, in designing experiments. The points (e.g., varieties of corn) are to be compared under various sets of conditions (blocks). The 2-design allows exactly λ head-to-head comparisons of any two points. A design is called *complete* if the set of blocks contains all the k-sets for some $k \leq v$. An experiment will be more efficient if we can get the information we need without including all the k-sets. Block designs that do not include all k-sets as blocks are known as *balanced incomplete block designs (BIBD)*.

Let us look at a few examples of t-designs. The first two get their structure from the patterns in complete graphs;[4] the next two from the structure of vector spaces over finite fields.

Example 5. Let $\mathcal{P}$ be the set of edges of K_6, the complete graph on six vertices. Define two types of blocks: (i) the three edges of a triangle, and (ii) the three edges of a complete matching (that is, three edges no two of which share a vertex). This is a 2-design since any two edges are in exactly one block. ◇

Example 6. Let $\mathcal{P}$ be the set of edges of K_5, and define three types of blocks: (i) the four edges incident with a single vertex (these edges form a *claw*), (ii) the three edges of a triangle together with the one edge disjoint from these, (iii) the four edges of a 4-cycle. This is a 3-design. ◇

Example 7. Consider the 4-dimensional vector space over the finite field $\mathbb{Z}_2$, denoted $(\mathbb{Z}_2)^4$. Let $\mathcal{P}$ be the set of all nonzero vectors, and let the blocks be sets of three vectors $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ so that $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$ in the vector space. For instance, $\{\,(1,0,1,1),\ (1,0,0,0),\ (0,0,1,1)\,\}$ is a block since the sum of these vectors (mod 2) is the zero vector. This is a 2-design. ◇

[3] Some authors (e.g., [**7**]) use the notation $S_\lambda(t, k, v)$ for a t-design. As a special case, a *Steiner system* is a t-design with $\lambda = 1$, and is often denoted simply as $S(t, k, v)$.

[4] The complete graph K_m has m vertices and an edge between every pair of vertices.

Example 8. Again consider the vector space $(\mathbb{Z}_2)^4$. This time let $\mathcal{P}$ be the set of all vectors, including the zero vector, and let the blocks be sets of four vectors $\{\mathbf{w}, \mathbf{x}, \mathbf{y}, \mathbf{z}\}$ with $\mathbf{w} + \mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. This is a 3-design. ◇

We now look at theorems that give relationships among the parameters of a t-design. The proofs require counting arguments and are left as exercises. Our first theorem shows how the parameters can be used to determine the number of blocks in a t-design.

Theorem 2.1. *The number of blocks in a t-(v, k, λ) design is*

$$b = \lambda \binom{v}{t} \Big/ \binom{k}{t}.$$

The next theorem tells us that every t-design is also an s-design for any s such that $0 \le s \le t$. Specifically, given any s-set S, this theorem gives a way to calculate λ_s, the number of blocks that contain S.

Theorem 2.2. *Let $\mathcal{D}$ be a t-(v, k, λ) design, and let S be an s-set of points with $0 \le s \le t$. Then the number of blocks that contain S is*

$$\lambda_s = \lambda \binom{v-s}{t-s} \Big/ \binom{k-s}{t-s}.$$

We note that if $s = t$, then $\lambda_s = \lambda$. At the other extreme, if $s = 0$ then λ_0 is the total number of blocks. And if $s = 1$, λ_1 gives the number of blocks incident with a given point. This quantity is often denoted by r (for replications in statistical designs). In summary, the parameters for a t-(v, k, λ) design are:

v = number of points (varieties, in statistical designs),

b = number of blocks,

k = number of points incident with each block,

r = number of blocks incident with each point (replications),

λ = number of blocks containing any given set of t points.

In Theorem 2.2 if we choose $t = 2$ and $s = 1$ we get a relation between parameters that we will see reflected often in our study of difference sets:

Corollary 2.3. *If $\mathcal{D}$ is a 2-design, then*

$$r(k-1) = \lambda(v-1).$$

Another fundamental relation exists between the first four parameters in our list above:

Theorem 2.4. *For a t-(v,k,λ) design, $vr = bk$.*

Once we have a t-design, we can construct a new design called the complement design.

Definition. Given a t-design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, the design $\overline{\mathcal{D}}$ with point set $\overline{\mathcal{P}} = \mathcal{P}$ and block set $\overline{\mathcal{B}} = \{\mathcal{P} \setminus B \mid B \in \mathcal{B}\}$ is called the complement design. Note that the blocks in $\overline{\mathcal{D}}$ are the complements of the blocks in $\mathcal{D}$.

To prove that this is indeed an s-design, and to find the largest s for which this is true, we will first need to establish that the number of blocks in the original t-design *disjoint* from a fixed s-set, is the same for any s-set. We use λ^s to denote this number.[5]

Of course if the s-set is too large there may be no blocks disjoint from our s-set. To avoid this trivial case, we will require that $s \leq v-k$.

Theorem 2.5. *Let $\mathcal{D}$ be a t-(v,k,λ) design, and let S be an s-set of points with $0 \leq s \leq t$ and $s \leq v-k$. Then the number of blocks of $\mathcal{D}$ disjoint from S is independent of the choice of s-set and equals*

$$\lambda^s = \lambda \binom{v-s}{k} \Big/ \binom{v-t}{k-t}.$$

Proof. First we argue that the value of λ^s is independent of our choice of s-set. By inclusion/exclusion (see A.20)

$$\begin{aligned} \lambda^s &= b - \binom{s}{1}\lambda_1 + \binom{s}{2}\lambda_2 - \cdots + (-1)^s \binom{s}{s}\lambda_s \\ &= \sum_{i=0}^{s} (-1)^i \binom{s}{i} \lambda_i. \end{aligned}$$

[5] Here s is part of the notation and is not an exponent. In this section λ_s is the number of blocks containing a fixed s-set, and λ^s is the number of blocks disjoint from a fixed s-set.

We could use binomial identities to simplify this sum and get our result. But since the above calculation shows that λ^s is the same for each s-set, it is both easier and more illuminating to proceed using a simple counting argument. We count the number of ordered pairs (B, S) with B a block and S an s-set disjoint from B. On the one hand, we can choose B from b blocks, and then choose an s-set S disjoint from B in $\binom{v-k}{s}$ ways. On the other hand, we can choose the s-set first, in $\binom{v}{s}$ ways, and then choose a block disjoint from the s-set in λ^s ways. So

$$\lambda^s \binom{v}{s} = b \binom{v-k}{s}.$$

Substituting $b = \lambda\binom{v}{t}/\binom{k}{t}$ and simplifying gives our result. □

Now we can use Theorem 2.5 to show that complement designs are s-designs.

Corollary 2.6. *Let $\mathcal{D}$ be a t-(v, k, λ) design. Then $\overline{\mathcal{D}}$, the complement design, is an s-design for $s = \min(t, v - k)$.*

A fundamental question in design theory concerns existence: For which triples (v, k, λ) does a t-design exist? The corollary above says that every design has a complement design. Therefore, to answer this question it is enough to find only those designs for which $k \leq v/2$, since any design for which $k > v/2$ has a complement design with $k < v/2$.

Exercises

4. Use the incidence matrix from Exercise 3 to show that the Fano plane is a 2-design.

5. For Example 5 find the numbers of blocks of each of the two types. Show that this is a 2-design by verifying that any two points (i.e., edges of the complete graph) are contained in exactly one block. Find the parameters of this design and verify that the total number of blocks agrees with Theorem 2.1. Ⓢ

6. For Example 6 find the numbers of blocks of each of the three types. What is the total number of blocks? Show that this is a 3-design, and find its parameters.

7. Show that Example 7 is a 2-design, and find its parameters.

8. What is $M^T M$ for the 2-design in Example 7? In general, what is $M^T M$ for a 2-design with parameters 2-(v, k, λ)? Write your answer using scalars times the matrices I (the $v \times v$ identity matrix) and J (the $v \times v$ matrix with all 1's).

9. What is $M^T M$ for a 3-design with parameters 3-$(10, 4, 1)$? In general, what is $M^T M$ for a 3-design with parameters 3-(v, k, λ)?

10. Prove that Examples 5 and 7 are isomorphic by giving a one-to-one correspondence between the vectors in Example 7 and the edges of K_6 in Example 5 that preserves the blocks.

11. Show that Example 8 is a 3-design, and find its parameters.

12. Show that Example 8 is also a 2-design by showing that any two points are contained in a fixed number of blocks. Use a combinatorial argument to find λ_2.

13. Prove Theorem 2.1. Ⓗ

14. Prove Theorem 2.2. Be careful not to assume that for every s-set there must be the same fixed number of blocks containing the s-set.

15. Prove Theorem 2.4 by showing that both vr and bk count the set of ordered pairs (p, B) with $p \in B$.

16. Prove Corollary 2.6 and find the parameters of the complement of a t-(v, k, λ) design.

2.3. Affine planes

Geometry—literally speaking—means "earth measure." Euclidean geometry with its infinite number of points and its definition of distance fits our literal interpretation of geometry. However, in this book we will look at different types of geometries. Most of our geometries will have finite numbers of points and lines, and we will drop any notion of a metric. What remains is a highly structured design with geometric points for its points, and lines or other substructures for its blocks. The structure is imposed on our geometries by a set of axioms. We are most interested in finite geometries that can be coordinatized.

In this section we define an affine plane and show that a finite coordinatized affine plane is a 2-design. In Section 5 we study finite projective geometries. These geometries provide a rich source for the symmetric designs we define in Section 4 and for constructing difference sets.

First we take the approach of synthetic geometry and define an affine plane as a set of points and lines that obey a set of axioms:

Definition. An affine plane is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

A1. Each pair of points is in a unique line.

A2. If ℓ is a line and P is a point not in ℓ, then there is a unique line ℓ' that contains P and does not intersect ℓ.

A3. There are at least two points in each line, and at least two lines in the plane.

We say that lines ℓ and ℓ' are parallel if either $\ell = \ell'$ or $\ell \cap \ell' = \emptyset$.

A1 is common to many geometries; it is often stated as "two points determine a line." A2 is one formulation of the parallel postulate, and is the key feature that distinguishes the Euclidean plane from infinite non-Euclidean planes. A3 eliminates trivial cases.

The well-known Euclidean plane is an example of an affine plane. The next example is the smallest affine plane allowed by our system of axioms.

Example 9. Let $\mathcal{P}$ be the set of points $\{A, B, C, D\}$ in Figure 2.1, and let $\mathcal{L}$ be the set of all 2-subsets of $\mathcal{P}$. The line segments connecting pairs of points represent the lines.

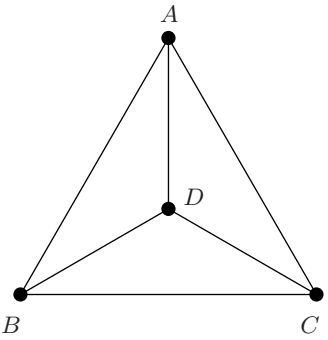


Figure 2.1. Affine plane with four points

If we label the columns A, B, C, D, then an incidence matrix for this affine plane is:

$$M \quad = \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

The rows correspond to the six lines in Figure 2.1. ◇

From this simple set of axioms it is possible to derive many properties of affine planes. While we will not pursue these results in detail, we list some of the numeric properties of finite affine planes derivable simply from these axioms. The parameter n in the theorem is the order of the affine plane. (See [**6**], p. 26, for a proof.)

Theorem 2.7. *Let $(\mathcal{P}, \mathcal{L})$ be a finite affine plane. Then for some integer $n \geq 2$:*

(i) Each line has n points.

(ii) Each point is incident with $n+1$ lines.

(iii) There are n^2 points.

(iv) There are $n(n+1)$ lines.

(v) The lines form $n+1$ classes, each with n mutually parallel lines.

Often we identify the points of the Euclidean plane with ordered pairs from $\mathbb{R}\times\mathbb{R}$, and describe a line as a set of points (x, y) that obey a linear equation $ax + by = c$, where $a, b, c \in \mathbb{R}$ and a and b are not both 0. In this way we *coordinatize* the plane. This coordinate system gives us analytical tools to work with the plane. For instance, we can judge whether two lines are parallel by comparing their slopes. For two lines that are not parallel, we can find the point of intersection by finding the solution common to their two equations.

In a similar way we can coordinatize a finite affine plane.

Example 10. Consider the four-point affine plane, and label the points using coordinate pairs from $\mathbb{Z}_2 \times \mathbb{Z}_2$. The equations that determine the six lines are: $x = 0$, $x = 1$, $y = 0$, $y = 1$, $y = x$, and $y = x + 1 \bmod 2$. See Figure 2.2. ⋄

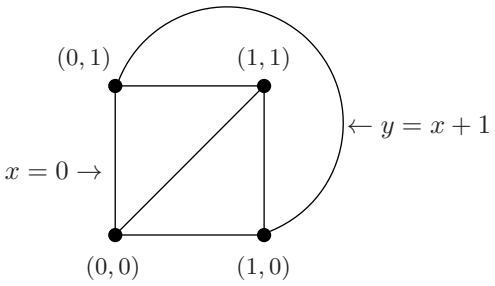


Figure 2.2. Coordinatized affine plane with four points

In general we start with any field $\mathbb{F}$ and use elements from $\mathbb{F} \times \mathbb{F}$ as coordinates of the points in an affine plane. We take as lines the solution sets of linear equations $ax + by = c$ for $a, b, c \in \mathbb{F}$ with a and

b not both zero. Notice that for any nonzero $u \in \mathbb{F}$, the equations $ax + by = c$ and $uax + uby = uc$ have the same solution set.

We define the slope of a line with equation $ax+by = c$ as follows. If $b = 0$, the slope is infinite (and the line is "vertical"). If $b \neq 0$, the slope is $m = -a/b \in \mathbb{F}$. Using algebra, we can verify that distinct lines with the same slope are parallel. Also suppose (x_1, y_1) and (x_2, y_2) are two points on a line. If $x_1 = x_2$, then the line has infinite slope. If $x_1 \neq x_2$, we calculate the slope as $m = (y_2 - y_1)/(x_2 - x_1)$.

This structure does indeed satisfy the axioms of an affine plane. We call this the coordinatized affine plane, denoted by $AG(2, \mathbb{F})$. If $\mathbb{F}$ has q elements, we denote this plane by $AG(2, q)$.

Theorem 2.8. *Let $\mathbb{F}$ be a field. Let $\mathcal{P} = \mathbb{F} \times \mathbb{F}$, and let $\mathcal{L}$ be the collection of lines defined as the solution sets to linear equations $ax + by = c$, for $a, b, c \in \mathbb{F}$, with a and b not both equal to 0. Then $(\mathcal{P}, \mathcal{L})$ is an affine plane.*

Proof. To show that two points determine a line, we consider the points (x_1, y_1) and (x_2, y_2). If $x_1 = x_2$, the line determined by these two points is the set of solutions to the equation $x = x_1$, a vertical line with infinite slope. If $x_1 \neq x_2$, then the line determined by the two points is the set of solutions to the equation $y - y_1 = m(x - x_1)$.

To show this line is unique, we suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax+by = c$ and $a'x+b'y = c'$. We want to show there is a nonzero $u \in \mathbb{F}$ with $a' = ua, b' = bu, c' = cu$. We leave the two special cases $x_1 = x_2$ and $y_1 = y_2$ to the exercises and assume $x_1 \neq x_2$ and $y_1 \neq y_2$, so $m = (y_2 - y_1)/(x_2 - x_1) \neq 0$. Subtracting $ax_2 + by_2 = c$ from $ax_1 + by_1 = c$ we get $a(x_1 - x_2) = b(y_2 - y_1)$, from which it follows that both a and b must be nonzero and $a = b(-m)$. It follows that $c = b(y_1 - mx_1)$. Similarly, both a' and b' are nonzero, $a' = b'(-m)$ and $c' = b'(y_1 - mx_1)$. Now, choose $u = b'/b$ to see that $a' = ua$, $b' = ub$ and $c' = uc$, so the line is unique.

To prove axiom A2, the parallel postulate, we show that given a line ℓ and a point P not on ℓ, we can find a line parallel to ℓ and through P. Let P have coordinates (x_1, y_1). If ℓ has no slope (that is, if ℓ is a vertical line), its equation is of the form $x = x_0$ for some $x_0 \neq x_1$. Then the line with equation $x = x_1$ contains P and is

parallel to ℓ. It is clearly unique. Otherwise let ℓ have slope m. Then the line through P and parallel to ℓ has equation $y - y_1 = m(x - x_1)$. We can rearrange this equation as $mx - y = mx_1 - y_1$, that is $a = m$, $b = -1$ and $c = mx_1 - y_1$. We see the ratio $a/b = m$, agreeing with the slope of ℓ. If $m = 0$ the equation is $by = c$ and we easily check that this line is unique. If $m \neq 0$ we can adapt the proof of uniqueness above for axiom A1.

Clearly if $\mathbb{F}$ is infinite, then the affine plane has infinitely many points and lines, and so satisfies axiom A3. We leave the finite case to the exercises. □

The above theorem guarantees the existence of a finite affine plane of order n for any n a prime power. It is not known whether other affine planes exist with other orders. It is relatively easy to show that we cannot construct an affine plane of order 6 using coordinates $\mathbb{Z}_6 \times \mathbb{Z}_6$. However, a proof that no order-6 affine plane exists cannot assume this coordinatization. It has now been shown that no affine planes of orders 6 or 10 exist [**42**]. The next open case is $n = 12$.

Finally we note the connection between affine planes and t-designs. Every finite affine plane is a t-design for $t = 2$ and $\lambda = 1$. This simply reflects the fact that any two points determine a line, and that every line contains the same number of points. Thus for any q a power of a prime, the coordinatized affine plane built on the field $GF(q)$ gives us a 2-$(q^2, q, 1)$ design.

Exercises

17. Consider the finite coordinatized plane $AG(2, 3)$.

(a) List the equations $ax + by = c$ corresponding to distinct solution sets by completing the following table. (The first row is done as a sample.)

a	b	c	slope	points
1	0	0	∞	$(0,0), (0,1), (0,2)$

(b) Draw the 3×3 array of points (x, y) where $x, y \in \mathbb{Z}_3$. Connect sets of points when they lie together on a line.

(c) How many lines are there? How many points per line? What is the order n of this plane? What are the parameters of this plane as a 2-design? Ⓢ

(d) What is $M^T M$? Explain its entries geometrically.

(e) What is MM^T? Explain its entries geometrically.

18. Show that distinct lines of $AG(2, \mathbb{F})$ with the same slope are parallel. Specifically, suppose a, b, a', b' are elements of $\mathbb{F}$ and $ax + by = c$ and $a'x + b'y = c'$ are distinct lines with the same slope. Show that these two lines have no points in common by considering these two cases.

(a) Suppose $b = b' = 0$ (i.e., both lines have infinite slope).

(b) Suppose $b \neq 0$, $b' \neq 0$, and $m = -a/b = -a'/b'$.

The next two exercises complete the proof of Theorem 2.8.

19. Consider the coordinatized plane $AG(2, \mathbb{F})$.

(a) Suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax + by = c$ and $a'x + b'y = c'$, with $x_1 = x_2$ and $y_1 \neq y_2$. Show that the solution sets of these two linear equations are the same.

(b) Suppose that (x_1, y_1) and (x_2, y_2) are solutions of both $ax + by = c$ and $a'x + b'y = c'$, with $x_1 \neq x_2$ and $y_1 = y_2$. Show that the solution sets of these two linear equations are the same.

(c) Suppose ℓ is a line of slope 0 and $P = (x_1, y_1)$ is not on ℓ but is on the line with equation $by = c$. Show that this is the unique line of slope 0 containing P.

(d) Assume ℓ is a line of slope $m \neq 0$, and $P = (x_1, y_1)$ is a point not on ℓ. Show that $y - y_1 = m(x - x_1)$ is the unique line through P having slope m.

20. Let $\mathbb{F}$ be the finite field $GF(q)$ for $q = p^m$ where p is a prime and m is a positive integer.

(a) Calculate the numbers of points and lines in $AG(2, \mathbb{F})$.

(b) Calculate the number of points on a line in $AG(2, \mathbb{F})$.

21. For Example 9 compute $M^T M$. Use the result to show that this is a 2-design, and find its parameters. Now compute MM^T. Explain the diagonal elements. Then explain the 0's and 1's in the off-diagonal positions in terms of the geometry (using 'points' and 'lines').

22. It is known that there is no finite affine plane of order 6. If we try to coordinatize a 6×6 grid using $\mathbb{Z}_6$, several things go wrong. Using the definition of a line as the solution set to a linear equation, and calling two lines parallel if they have no points in common, show that there would be at least two lines through the point $(1, 3)$ and parallel to the line $y = 0$.

23. Show that the set of points $\mathbb{Z}_{12} \times \mathbb{Z}_{12}$, with lines defined as the solution sets to linear equations, is not an affine plane.

2.4. Symmetric designs

We have seen that for 2-designs, while $M^T M$ has a constant value λ in all the off-diagonal positions, the product MM^T may have different values in its off-diagonal positions. These products show that, while pairs of points are incident with a constant number of blocks, pairs of blocks can be incident with different numbers of points. Symmetric designs place more restrictions on the design to exclude this.

Definition. A symmetric (v, k, λ) design is an incidence structure $(\mathcal{P}, \mathcal{B}, I)$ in which $0 < k < v$ and the following hold:

(i) $|\mathcal{P}| = v$.

(ii) $|\mathcal{B}| = v$.

(iii) Each point is incident with k blocks.

(iv) Each block is incident with k points.

(v) Each pair of points is incident with λ blocks.

(vi) Each pair of blocks is incident with λ points.

To avoid problems with degenerate cases we require that $0 < k < v$. We will call symmetric designs with $\lambda = 0$ or $k-1$ trivial symmetric designs.[6] The value $n = k - \lambda$ is called the order of the symmetric design.

These axioms are redundant. If a structure obeys axioms (i)–(iv), then (v) and (vi) are equivalent. (See Exercise 32.)

An immediate consequence of the definition is the following theorem.

Theorem 2.9. *Let A be a $v \times v$ matrix of 0's and 1's. Then A is the incidence matrix of a symmetric (v, k, λ) design if and only if*

$$AA^T \quad = \quad A^T A \quad = \quad nI + \lambda J.$$

Corollary 2.10. *The incidence matrix A of a symmetric design is invertible.*

Example 11. Consider a 4×4 board of squares. The 16 individual squares form the points of the design. The block T_j is the set of all squares in the row and the column of square j except the square j itself. Thus every block contains 6 squares. For instance, if we label the squares as shown in Figure 2.3, then block T_7 consists of squares 3, 5, 6, 8, 11, 15. This construction forms a symmetric $(16, 6, 2)$ design. ◇

Example 12. Let $p = 11$, and let $\mathcal{P} = \mathbb{Z}_{11}$. Let D be the set of all nonzero squares mod 11, and let $\mathcal{B}$ be the blocks $\{D,\ 1 + D,\ 2 + D, \cdots,\ 10 + D\}$, where addition is mod 11. Then these points and blocks form a symmetric design. The nonzero squares mod p are called the quadratic residues mod p. ◇

In Section 2.2 we saw relations among the parameters for t-designs. The following theorem shows how the parameters of a symmetric design are related.

Theorem 2.11. *For a symmetric (v, k, λ) design, $(v-1)\lambda = k(k-1)$.*

[6] Some authors define symmetric designs as special 2-designs, which would exclude what we call trivial symmetric designs. We retain trivial designs because they correspond to trivial difference sets.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Figure 2.3. Design from 4×4 grid in Example 11; T_7 is shaded

As with t-designs, we define the complement of a symmetric design to have the same point set and to have blocks defined as the complements of the blocks in the original design.

Theorem 2.12. *The complement of a symmetric (v, k, λ) design is a symmetric design with parameters $(v, v-k, v-2k+\lambda)$.*

The following theorem generalizes Example 12 and the Fano plane example.

Theorem 2.13. *Let p be a prime such that $p \equiv 3 \pmod 4$, and let $\mathcal{P} = \{0, 1, \ldots, p-1\}$. Let D be the set of quadratic residues mod p, and let $\mathcal{B} = \{i + D \mid i \in \mathcal{P}\}$, where addition is mod p. Then $(\mathcal{P}, \mathcal{B})$ is a symmetric design.*

We explore examples of this construction in the exercises, and prove a more general result in Chapter 4.

A fundamental question is for which triples (v, k, λ) do symmetric (v, k, λ) designs exist. A partial answer comes from the infinite family of designs given in Theorem 2.13. We encounter other infinite families as we study projective geometries. The general existence question remains open.

There are many tantalizing questions about the triples of parameters for symmetric designs. According to Lander ([**43**], p. 44), "For each $\lambda > 1$, only finitely many symmetric (v, k, λ) designs are known." Most nontrivial symmetric designs have $v \leq \lambda^2(\lambda + 2)$. The

only known exceptions are designs that have parameters $(37, 9, 2)$, $(56, 11, 2)$, $(79, 13, 2)$, and $(71, 15, 3)$. For each prime power λ, Lander gives a symmetric design that attains the bound $v = \lambda^2(\lambda + 2)$.

Exercises

24. Show that Example 11 is a symmetric $(16, 6, 2)$ design. Ⓢ

25. Show that Example 12 is a symmetric design and give its parameters.

26. Prove Theorem 2.11. Then compare this result with Corollary 2.3.

27. Prove Theorem 2.12: the complement of a symmetric (v, k, λ) design is a symmetric design. Explain why the parameters of the complement design are $(v, v - k, v - 2k + \lambda)$.

28. Using the construction in Theorem 2.13, what is the set D in $\mathbb{Z}_{19}$? What are the parameters for the symmetric design?

29. Show that the construction in Theorem 2.13 with $p = 5$ does not give a symmetric design. What goes wrong?

30. Nontrivial symmetric designs as 2-designs

(a) Which of the six axioms in the definition of a symmetric design are needed to make the structure a 2-design?

(b) Assume that an incidence structure is a 2-design with equal numbers of points and blocks. Prove that r, the number of blocks incident with a particular point, is equal to k.

31. Prove Corollary 2.10 as follows. Parts (b–d) assume a symmetric design with parameters (v, k, λ) and incidence matrix A.

(a) Let B be a $v \times v$ matrix with $B = aI + bJ$. Show that $\det B = (a + vb)a^{v-1}$ by finding $v - 1$ linearly independent

eigenvectors for B with eigenvalue a and one independent of these with eigenvalue $a + vb$.

(b) Show that $\det(nI + \lambda J) = k^2 n^{v-1} \neq 0$.

(c) Explain why $AA^T = nI + \lambda J$.

(d) Prove that A is invertible.

32. Assume an incidence structure obeys axioms (i)–(iv) of a symmetric design, and let A be the incidence matrix for this structure.

(a) Show that $AJ = JA$.

(b) Assume axiom (vi) and deduce axiom (v). Ⓗ

(c) Assume axiom (v) and deduce axiom (vi).

2.5. Projective geometry

We return in this section to geometries—this time to projective geometries—to look for examples of symmetric designs. As with the affine planes of Section 3, we look first at the axiomatic definition of a projective plane. We then construct a coordinatized projective plane $PG(2, q)$ starting with a vector space over $GF(q)$. We also study projective geometries of dimension higher than two.

Definition. A projective plane is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

P1. Each pair of points is in a unique line.

P2. Each pair of lines intersects.

P3. Each line contains at least three points; the plane contains at least two lines.

Note that the parallel postulate from the definition of an affine plane is replaced by axiom P2 stating that any two lines intersect. Combining axioms P1 and P2 shows that any two lines intersect in exactly one point. From the axioms it is also possible to prove that each point is incident with at least three lines, and that the plane contains at least two points. An important property that comes from these axioms is that any true statement that can be derived from these axioms about points and lines remains true if the words “points” and

"lines" are interchanged. This is known as the property of duality. We see this in the next theorem.

As with finite affine planes, the axioms for a projective plane give us enough information to prove that each line in a finite projective plane must have the same number of points. We can also prove other numerical results, as summarized in this theorem. (See [**6**], p. 4.)

Theorem 2.14. *Let $(\mathcal{P}, \mathcal{L})$ be a finite projective plane. Then for some integer $n \geq 2$*

(i) Each line has $n + 1$ points.

(ii) Each point is incident with $n + 1$ lines.

(iii) There are $n^2 + n + 1$ points.

(iv) There are $n^2 + n + 1$ lines.

The number n is called the order of the projective plane. The smallest finite projective plane is the order-2 Fano plane, with seven points and seven lines, each line containing three points. (See Figure 1.2 on page 5.)

So far we have talked about the synthetic approach. Just as we did with affine planes, we now restrict our attention to the class of coordinatized projective planes that are constructed starting with a vector space—in this case, a 3-dimensional vector space $\mathbb{F}^3$. Before we look at this construction in general, we introduce it using the field $\mathbb{R}$.

Example 13. Let $\mathbb{F} = \mathbb{R}$ and let $V = \mathbb{R}^3$, the familiar 3-space. The 1-spaces in V are the ordinary lines through the origin, and these will be our "points". The 2-spaces are the ordinary planes through the origin, and these will be our "lines". Then two 1-spaces ("points") span a unique 2-space ("line"). Two 2-spaces ("lines") meet in a 1-space ("point"). ◇

Theorem 2.15. *Let $\mathbb{F}$ be a field and let V be a vector space of dimension three over $\mathbb{F}$. Let $\mathcal{P}$ be the collection of 1-spaces of V, and let $\mathcal{L}$ be the collection of 2-spaces of V. Then $(\mathcal{P}, \mathcal{L})$ is a projective plane.*

A projective plane constructed in this fashion is denoted $PG(2, \mathbb{F})$. When $\mathbb{F}$ has q elements, we write $PG(2, q)$.

Example 14. The finite projective plane $PG(2, 3)$ is constructed starting with the vector space $V = (\mathbb{Z}_3)^3$. There are $3^3 - 1 = 26$ nonzero vectors, with (x_1, x_2, x_3) and $2(x_1, x_2, x_3)$ in the same 1-space (together with the zero vector). So there are 26/2 projective points. ◇

We can define coordinates for $PG(2, \mathbb{F})$ and use analytical techniques to study these geometries. Clearly we cannot simply label a projective point with the components of a single vector in the related 1-space, since that would give several labels for one point. But since all the nonzero vectors in a 1-space are nonzero multiples of each other, we do something quite close to this.

On the set of nonzero ordered triples $(x, y, z) \in \mathbb{F}^3 \setminus (0, 0, 0)$ we define an equivalence relation $(x, y, z) \sim (x', y', z')$ if and only if $(x', y', z') = s(x, y, z)$ for some nonzero scalar s. We use square brackets for the equivalence class $[x, y, z]$ of all triples equivalent to (x, y, z), and we use these equivalence classes to label the projective points.

Any 2-space of V can be described as the solution set of a linear equation $ax + by + cz = 0$ with a, b, and c not all 0. Given this, the projective line identified with this 2-space can be described as the set of projective points $[x, y, z]$ so that $ax+by+cz = 0$. We note that any vector equivalent to (a, b, c) gives the same projective line. So we use an equivalence class $[a, b, c]$ to describe a particular projective line. We thus naturally call $PG(2, \mathbb{F})$ the coordinatized projective plane .

Example 15. Consider the projective plane $PG(2, 3)$. The points $[2, 1, 0]$ and $[1, 0, 1]$ are different since $(2, 1, 0) \not\sim (1, 0, 1)$. Given this, there must be a projective line through these points. This line must have coordinates $[a, b, c]$ so that $2a + b = 0$ and $a + c = 0$ in $\mathbb{Z}_3$. If we choose $a = 1$, then $b = -2 = 1$ and $c = -1 = 2$. Other choices for a will give other triples in the equivalence class $[1, 1, 2]$. ◇

Projective spaces of higher dimensions. If we increase the dimension, there is enough room in projective space for lines that do

not intersect. In the definition of a projective space we replace axiom P2 with one that basically says any two lines in a planar subspace must intersect.

Definition. A projective space is a non-empty set $\mathcal{P}$ of points and a non-empty set $\mathcal{L}$ of subsets of $\mathcal{P}$ called lines, so that

P1. Each pair of points is in a unique line. (We write $\ell(A, B)$ for the unique line on points A and B.)

P2′. (The Pasch Axiom) If A, B, C, and D are distinct points such that there is a point E in the intersection of lines $\ell(A, B)$ and $\ell(C, D)$, then there is a point F in the intersection of lines $\ell(A, C)$ and $\ell(B, D)$.

P3′. Each line contains at least three points; the projective space contains at least two lines.

Extending our construction to projective spaces of higher dimensions, we construct $PG(d, q)$ starting with the vector space $V = \mathbb{F}^{d+1}$ for $\mathbb{F}$ the field $GF(q)$. Again, the points of the projective space are the 1-spaces of V; the lines are the 2-spaces; the planes are the 3-spaces; and so forth.

In a finite projective space of dimension greater than two, there are not equal numbers of points and lines, so we cannot find a symmetric design using the lines as blocks. However there are equal numbers of 1-spaces and d-spaces in $V = \mathbb{F}^{d+1}$. We call these d-spaces hyperplanes, and we have the following theorem.

Theorem 2.16. *Let $\mathbb{F} = GF(q)$ and let V be a $(d+1)$-dimensional vector space over $\mathbb{F}$ for $d \geq 2$. Let $\mathcal{P}$ be the set of 1-spaces of V, and let $\mathcal{B}$ be the set of hyperplanes. Then $(\mathcal{P}, \mathcal{B})$ is a symmetric design with parameters*

$$v = \frac{q^{d+1} - 1}{q - 1}, \quad k = \frac{q^d - 1}{q - 1}, \quad \lambda = \frac{q^{d-1} - 1}{q - 1}.$$

Proof. We leave for the exercises the verification that v is the number of 1-spaces in V. Now we count the number of hyperplanes.[7] To

[7] It is true that the 1-spaces and hyperplanes of a finite-dimensional vector space are in a one-to-one correspondence. (See A.4.) For vector spaces over a finite field, a direct count of the hyperplanes is interesting.

begin, we count the number of ways to choose d linearly independent vectors in V. There are $q^{d+1}-1$ choices for the first nonzero vector. Then there are $q^{d+1}-q$ choices for a second vector independent of the first. Similarly there are $q^{d+1}-q^2$ ways to choose a third vector not in the span of the first two. Proceeding in this way, the total number of choices is

$$(q^{d+1}-1)(q^{d+1}-q)(q^{d+1}-q^2)\dots(q^{d+1}-q^{d-1}).$$

But a hyperplane has many bases. The number of bases of a fixed hyperplane (d-space) is $(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-1})$. Therefore the number of hyperplanes is

$$\frac{(q^{d+1}-1)(q^{d+1}-q)(q^{d+1}-q^2)\dots(q^{d+1}-q^{d-1})}{(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-1})}.$$

Factor a q from all but the first binomial in the numerator for a leading factor of q^{d-1}. Now factoring q^{d-1} from the last binomial in the denominator gives:

$$\frac{q^{d-1}(q^{d+1}-1)(q^d-1)(q^d-q)\dots(q^d-q^{d-2})}{q^{d-1}(q^d-1)(q^d-q)(q^d-q^2)\dots(q^d-q^{d-2})(q-1)}.$$

Cancel factors in common to get:

$$\frac{q^{d+1}-1}{q-1}.$$

We leave for the exercises the proof that k is also the number of 1-spaces in a hyperplane.

Next we show that the number r of hyperplanes containing a 1-space is independent of the particular 1-space. Suppose $\mathbf{u},\mathbf{w}\in V$ are two nonzero vectors. We can define an invertible linear transformation $T:V\to V$ with $T(\mathbf{u})=\mathbf{w}$. Then T permutes the hyperplanes of V, so H is a hyperplane containing $\mathbf{u}$ if and only if $T(H)$ is a hyperplane of V containing $\mathbf{w}$.

Finally, two hyperplanes meet in λ 1-spaces. □

Exercises

33. Let $\mathbb{F}=GF(5)$

(a) How many nonzero vectors are there in $\mathbb{F}^3$?

(b) Explain how to calculate the number of points and lines in $PG(2, 5)$.

34. Prove Theorem 2.15. Be sure to verify axiom P3 in the finite case.

35. What goes wrong with the construction in Theorem 2.15 if we start with $V = \mathbb{Z}^3$?

36. Consider the projective plane $PG(2, 5)$.

(a) Let [0,1,3] and [2,1,1] be two projective points. Find the coordinates for the line through these points. Ⓢ

(b) Let [0,1,3] and [2,1,1] be two projective lines. Find the coordinates for the point in the intersection of these two lines.

(c) Write a general statement about the principal of duality that you see in parts (a) and (b).

37. Let $V = \mathbb{Z}_5^4$, the vector space of dimension 4 over $\mathbb{Z}_5$. Find an equation for the hyperplane (here, a 3-space) containing vectors $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, and $(1, 1, 1, 1)$.

38. Consider the projective space $PG(3, 5)$.

(a) Find the numbers of points, lines, and planes in this projective space.

(b) Show that the incidence structure with $\mathcal{P}$ the set of projective points and $\mathcal{B}$ the set of projective planes is a symmetric design. Find its parameters.

39. Complete the proof of Theorem 2.16 as follows:

(a) Show that v is the number of 1-spaces in V.

(b) Show that k is the number of 1-spaces in a hyperplane of V.

(c) Explain why $r = k$.

(d) Fix two hyperplanes. Show that λ is the number of 1-spaces in the intersection of the hyperplanes.

Coda

Design theory is mathematically rich and very useful. It belongs to combinatorics and is strongly linked to geometry and algebra. Designs arose in statistics as designs of experiments (and this statistical origin shows in the standard notation v for the number of points in a design). A statistics text that highlights designs is [**14**]; it is very applied but also imbued with the spirit of abstract designs. Another important application of designs is to coding theory. See for example [**12**]. Also see the section on codes in Chapter 13.

The treatment of designs in this chapter is somewhat more general than required for our study of difference sets, but we wanted to place the designs we need in a wider context. Our main focus is on symmetric designs because they are intimately connected to difference sets in finite groups. Chapter 3 introduces groups via automorphisms of designs, and Chapter 4 makes the explicit link between symmetric designs and difference sets.

Finite geometries often play a key role in constructions of difference sets. Here we have treated affine and projective geometries in two parallel sections (forgive the pun). In each section, we begin synthetically, with a list of axioms. Adding the assumption of finiteness to the axioms determines many parameters of the geometry. We then narrow our focus to the coordinatized geometries, since these are most useful to us.

Chapter 3

Automorphisms of Designs

In Section 2.1 we defined two incidence structures to be isomorphic if there is a way to map the points of one to the points of the other that preserves the blocks. We want to extend the notion of permuting points and blocks of a design by discussing more formally the group of automorphisms of a symmetric design. Before we do that, we need the concept of a group acting on a set.

3.1. Group actions

Many examples of groups arise naturally as sets of functions mapping a set X to itself. We have groups of invertible linear transformations $V \to V$ for some vector space V; or symmetries of polygons thought of as groups of invertible functions $\mathbb{R}^2 \to \mathbb{R}^2$; or subgroups of $\mathcal{S}(X)$, the symmetric group consisting of all permutations of a set X. It is useful to be able to regard an abstract group G as a set of functions $X \to X$ for a suitably chosen set X of "objects." More formally:

Definition. Let G be a group and X a set. We say that G acts on X if there is a function $F : G \times X \to X$ with the following properties.

(i) The identity 1_G of G satisfies $F(1_G, x) = x$ for all x in X.

(ii) For all $g, h \in G$ and $x \in X$, $F(gh, x) = F(g, F(h, x))$.

You can think of the preceding definition as the bare minimum of what is required for elements of a group G to act on a set in a way that respects the structure of G. This minimum actually suffices to give the following theorem.

Theorem 3.1. *Let G be a group acting on a set X via the function $F : G \times X \to X$. For $g \in G$ and $x \in X$, write $\pi_g(x) = F(g, x)$. Then π_g is a permutation of X and $g \mapsto \pi_g$ is a homomorphism from G to $\mathcal{S}(X)$.*[1]

The following three examples show groups acting on sets of objects. In the second and third, the group acts on itself.

Example 1. Let G be the group of the 24 rotation symmetries of a cube, and let X be the set of eight vertices. Then each $g \in G$ permutes the set X and the identity of G fixes each vertex. Further, for any $g, h \in G$, $\pi_g(\pi_h(x)) = \pi_{gh}(x)$. Alternatively we might let X be the set of 12 edges and view each $g \in G$ as a permutation of these edges. $\diamond$

Example 2. Let G be a group. We define a group action on the set of elements of G by left multiplication. If $g \in G$, then multiplication on the left by g permutes the elements of G with $\pi_g(h) = gh$. $\diamond$

Example 3. As with Example 2 we define a group action with G acting upon itself, though in this example the action is conjugation. Let $g \in G$. Then for all $h \in G$, π_g maps h to ghg^{-1}. Notice that the π_g are homomorphisms of G. (This is not true in Example 2.) $\diamond$

We need some terminology to describe how G acts on X:

Definition. Let G be a group acting on the set X. Define an equivalence relation on X by $x \sim y$ if $y = \pi_g(x)$ for some $g \in G$. The equivalence classes are called the orbits of G on X. For $x \in X$ the orbit of x under G, denoted $\mathrm{orb}_G(x)$, is the equivalence class containing x. The subset $\mathrm{stab}_G(x) = \{g \in G \mid \pi_g(x) = x\}$ is called the stabilizer of x.

[1] This is called a permutation representation of the group G, and is closely allied to the linear representations in Chapter 10.

In Example 1, if we let X be the set of 8 vertices of the cube then the orbit of any one vertex is all of X. The stabilizer of any vertex is the set of all 3 rotations of the cube about an axis through that vertex and the one diagonally opposite. Suppose instead we let X be the set of $\binom{8}{2} = 28$ pairs of vertices and choose for x a pair of vertices connected by an edge of the cube. Then the orbit of x consists of the 12 pairs of vertices determined by the 12 edges. The stabilizer of x consists of the 2 rotations about an axis through the midpoints of the edge determined by x and the opposite edge. The numbers in these examples might lead you to conjecture the following theorem. The proof depends on the fact that $\text{stab}_G(x)$ is a subgroup of G.

Theorem 3.2. *(Orbit-stabilizer theorem) Assume the finite group G acts on a set X, and let $x \in X$. Then $|G| = |stab_G(x)|\,|orb_G(x)|$.*

When we turn our attention to groups acting on symmetric designs, we need some additional language.

Definition. If there is only one orbit of G on X, we say G acts transitively on X. Further, G acts regularly on X if G acts transitively on X and the stabilizer $\text{stab}_G(x) = \{1_G\}$ for all $x \in X$. (When this happens, if G is finite then $|G| = |X|$.)

In Example 1, if we let X be the set of vertices of the cube then G acts transitively on X. But G does not act regularly on X since there are three rotation symmetries that take any vertex to itself. On the other hand, if we let X be the set of pairs of vertices, then G does not act transitively on X. In Example 2 the action of G on itself is regular.[2] In Example 3, if G is nontrivial, the action is not transitive. (What is the orbit of 1_G?)

In the next section we need one more result about orbits of a group acting on a set, often called Burnside's Lemma.[3] The proof is found in many abstract algebra texts, for example the one by Gallian [**23**].

[2]This is the left regular representation of G discussed in Chapter 10. It gets its name from acting "regularly" on the elements of G.

[3]Lander [**43**] calls this the Cauchy-Frobenius lemma; other texts call it Burnside's Theorem or the Polya-Burnside Lemma.

Lemma 3.3. *(Burnside's Lemma) Assume the group G acts on a set X. For $g \in G$, let* $\mathrm{Fix}(g)$ *be the set of elements of X fixed by π_g. Then*

$$\text{Number of orbits of } G \text{ on } X = \frac{1}{|G|} \sum_{g \in G} \big|\, \mathrm{Fix}(g) \big|.$$

Exercises

1. Prove Theorem 3.1.

2. Let G be the dihedral group of order 8, and let G act on itself by conjugation. Find the G-orbits. Ⓢ

3. Let G be a group acting on a set X, and consider the relation on X defined by $x \sim y$ if $y = \pi_g(x)$ for some $g \in G$. Prove that this is an equivalence relation.

4. Prove Theorem 3.2. Ⓗ

The next two exercises revisit some theorems you may have seen in abstract algebra.

5. Cayley's theorem says that every group G is isomorphic to a subgroup of $\mathcal{S}(G)$. Use Example 2 to prove Cayley's theorem.

6. Prove the following statements:

(a) A group G is partitioned into its conjugacy classes.

(b) For any $a \in G$, the size of the conjugacy class of a in G is the index in G of the subgroup $C_G(a) = \{g \in G \,|\, ga = ag\}$, the centralizer of a.

3.2. Automorphisms of symmetric designs

We now look specifically at groups acting on the points and simultaneously on the blocks of a symmetric design.

Definition. Let $\mathcal{D}$ be a symmetric design with point set $\mathcal{P}$ and block set $\mathcal{B}$. An automorphism of $\mathcal{D}$ is a permutation of $\mathcal{P}$ that preserves

the set of blocks. Consequently the automorphism also acts as a permutation of $\mathcal{B}$.

Theorem 3.4. *The set of all automorphisms of a symmetric design is a group under the operation of composition of functions. This is called the group of automorphisms of the design.*

Example 4. An example that is easy to picture is the automorphism of the Fano plane in Figure 3.1 that rotates the figure 120 degrees counterclockwise.

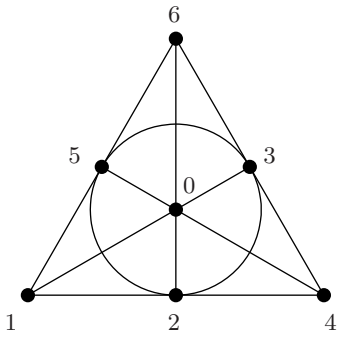


Figure 3.1. The Fano plane

The permutations on the points and on the blocks are

$$\begin{array}{ll} (0)(146)(235) & \text{on points} \\ (\ell_2)(\ell_1\,\ell_3\,\ell_5)(\ell_0\,\ell_4\,\ell_6) & \text{on blocks} \end{array}$$

where $\ell_1 = 124$, $\ell_2 = 235$, $\ell_3 = 346$, $\ell_4 = 450$, $\ell_5 = 561$, $\ell_6 = 602$, $\ell_0 = 013$. ◇

In our example the cycle structures of the permutation of the points and the permutation of the blocks are the same. This is no accident. For any automorphism of a symmetric design, the cycle structures of the corresponding permutations of the points and blocks are always the same ([**43**], p. 78). For our purposes the important link between these two permutations is Corollary 3.7. This result is vital to our work on difference sets in Chapters 4, 6, and 8.

The first theorem below concerns the numbers of fixed points for the permutations of the points and blocks caused by an automorphism.

Theorem 3.5. *An automorphism of a symmetric design fixes the same number of blocks as points.*

Proof. Let A be the incidence matrix of the symmetric design. Let Q be a permutation matrix that permutes the points according to the automorphism. Then AQ is the incidence matrix for the symmetric design but with the points permuted. Since an automorphism of a block design is a permutation of the points of the design that permutes the blocks, there is a permutation matrix P so that $PA = AQ$.

Corollary 2.10 tells us that A is invertible. So $P = AQA^{-1}$, making P and Q similar. Therefore P and Q have the same trace. Since the trace of a permutation matrix is the number of objects fixed by that permutation, we have our result. □

The next theorem and its corollary compare the actions of a group of automorphisms of a design on the point set and on the block set. The proof requires Burnside's Lemma 3.3.

Theorem 3.6. *A group of automorphisms of a symmetric design has as many orbits on points as it does on blocks. In particular, it is transitive on points if and only if it is transitive on blocks.*

Proof. From Theorem 3.5 we know that an automorphism of a symmetric design $\mathcal{D}$ fixes the same number of points as blocks. In other words, the value of $\left|\operatorname{Fix}(g)\right|$ is the same for $X = \mathcal{P}$ as for $X = \mathcal{B}$. Now apply Burnside's Lemma with G the group of automorphisms to see that the number of orbits of G on $\mathcal{P}$ is the same as the number of orbits of G on $\mathcal{B}$. □

The following corollary pulls together the information in Theorems 3.5 and 3.6 and is the key result referred to above.

Corollary 3.7. *Let $\mathcal{D}$ be a symmetric design with point set $\mathcal{P}$ and block set $\mathcal{B}$, and let G be a group of automorphisms of $\mathcal{D}$. Then G acts regularly on $\mathcal{P}$ if and only if G acts regularly on $\mathcal{B}$.*

Exercises

7. In Example 4 consider the automorphism of the Fano plane that reflects our figure about the vertical line of symmetry. Write in cycle form the resulting permutations on the set of points and the set of lines. Ⓢ

8. What is the full group of automorphisms of the Fano plane? Ⓗ

9. Prove Theorem 3.4.

10. Prove Corollary 3.7.

Coda

There are two important ideas in this chapter: the general concept of a group acting on an arbitrary set, and the specific case of a group of automorphisms of a symmetric design. An automorphism of a symmetric design is a permutation of its points and of its blocks that "preserves its structure." By saying a mapping preserves the structure of the design we mean that if a point P belongs to a block B of the design, then the image of P under the mapping belongs to the image of B.

The concept of a group G acting on a set X as a set of mappings $X \to X$ is a major theme in group theory. If the set X has additional structure—whether algebraic or geometric or physical—we may restrict attention to group actions that preserve the structure. Thus group actions can lead to a host of applications by using symmetry groups to analyze such things as crystals or atoms or networks. Group actions also supply a unifying thread in proofs of major results about groups, such as Cayley's theorem, the Sylow theorems, and the class equation.

Automorphisms of a symmetric design provide the link to difference sets. As we prove in Chapter 4, a group acts regularly on the

points and on the blocks of a symmetric (v, k, λ) design if and only if the group contains a (v, k, λ)-difference set.

Chapter 4

Introducing Difference Sets

As we noted in Chapter 1, many authors trace difference sets to the 1938 paper of Singer ([**62**]). Although Singer does formulate the definition of a difference set, his main theorem is about an automorphism of a design. Singer also frames the theorem's important consequences as descriptions of the points and blocks of the design. The systematic study of difference sets themselves goes back at least to Hall's work in the late 1940's. Ideas from combinatorics, geometry and algebra were ingredients in all of these early papers. The use of algebraic methods has grown steadily as the subject has developed.

In this chapter we introduce difference sets and some of the mathematical tools used to construct them and to explore their properties. We begin in Section 1 with the definition and examples. We describe in Section 2 how a difference set can be used to produce a symmetric design and thus how it provides a compact description of the design it yields. An important algebraic tool for the study of difference sets is the integral group ring, the topic of Section 3. Finally, in Section 4 we define what it means for two difference sets to be equivalent.

4.1. Definition and examples

Throughout, we restrict our attention to *finite* groups. If G is a cyclic group of order v, we will usually identify G with $\mathbb{Z}_v = \{0, 1, \ldots, v-1\}$, the group of integers under addition modulo v. (Later we use $\mathbb{Z}_m$ to denote the ring of integers modulo m, relying on context to make clear whether $\mathbb{Z}_m$ refers to the group or the ring.)

Difference sets were first defined in abelian groups in which the operation is written as addition and the identity is denoted by zero. A difference set D is a non-empty proper subset of a group G with the property that every nonzero element in G can be expressed in exactly the same number of ways as the difference of two elements in D. Another way to say this is to consider the *multiset* of differences

$$\Delta = \{\, d_1 - d_2 \mid d_1, d_2 \in D, d_1 \neq d_2 \,\}.$$

Then D is a difference set if every nonzero element of G appears the same number of times in Δ.

It is usual to use multiplication as a generic group operation, and to write 1, or sometimes 1_G, for the identity. (This is particularly useful for the study of difference sets because the symbol for addition is then available for another purpose, as in Section 3.) In the language of multiplicative groups, subtraction becomes multiplication by the inverse. So the multiset is

$$\Delta = \{\, d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2 \,\},$$

and we write the definition as follows.

Definition. A difference set D in a group G is a non-empty proper subset[1] of G such that any non-identity element of G can be written in exactly λ ways as $d_1 d_2^{-1}$ where d_1 and d_2 are in D. We say the difference set is cyclic or abelian if G is.

We freely apply this definition to groups written additively, and use the term "difference" when we talk about $d_1 d_2^{-1}$. However, we usually use multiplicative notation when speaking generally about

[1]Some authors include $\emptyset$ and G as trivial difference sets. In his definition ([**43**], p. 120) Lander requires $|D| > \lambda$, which we shall see is equivalent to our restriction. Notice that λ can be zero in one of our trivial cases, as Example 1 shows.

difference sets. (By Theorem 4.9, it doesn't matter, even in non-abelian groups, whether we define the multiplicative "difference" by $d_1 d_2^{-1}$ as above or with the inverse on the other side, as $d_1^{-1} d_2$.)

The following example shows that every finite group with at least two elements contains certain difference sets.

Example 1. Let G be a finite group and $g \in G$. If G contains at least two elements, then $\{g\}$ and $G \setminus \{g\}$ are difference sets. These are called trivial difference sets. ◇

The next two examples are cyclic difference sets. They are members of families of difference sets introduced later in this section.

Example 2. In the (additive) group $\mathbb{Z}_{11}$, $D = \{1, 3, 4, 5, 9\}$, the set of nonzero squares in $\mathbb{Z}_{11}$, is a difference set. ◇

Example 3. In the (additive) group $\mathbb{Z}_{15}$, $D = \{0, 1, 2, 4, 5, 8, 10\}$ is a difference set. ◇

Just as with designs, important parameters are associated with difference sets. We use the following letters to denote these parameters:

v = $|G|$,
k = $|D|$,
λ = the number of ways a non-identity element of G can be represented as a difference of two elements in D,
n = $k - \lambda$ is known as the order of the difference set.

We write that D is a (v, k, λ)-difference set. In the next section we describe the connection to designs that this notation suggests. Of course, the difference set parameters are related to each other. Notice that $0 < k < v$ together with the relation in the following theorem implies that $\lambda < k$, so the order of a difference set is a positive integer.

Theorem 4.1. *Let $D \subset G$ be a (v, k, λ)-difference set. Then $k(k-1) = \lambda(v-1)$. Equivalently, $n = k^2 - v\lambda$.*

The next example is taken from Lander ([**43**], p. 123), who rightly describes it as "elegant." It is a member of a family of difference sets first studied by Menon in 1962 ([**55**]). (We study this family of difference sets in Chapter 9.)

Example 4. The following elements of the additive group $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ form a $(36, 15, 6)$-difference set:

$$\begin{array}{lllll} (1,1) & (2,2) & (3,3) & (4,4) & (5,5) \\ (0,1) & (0,2) & (0,3) & (0,4) & (0,5) \\ (1,0) & (2,0) & (3,0) & (4,0) & (5,0). \end{array} \quad \diamond$$

So far we have looked exclusively at difference sets in abelian groups. Any finite abelian group is isomorphic to a direct product[2] of cyclic groups $\mathbb{Z}_m$. Non-abelian groups cannot be characterized as simply. However, any finite group can be defined by specifying the elements that generate the group and the fundamental relations the generators satisfy.

Definition. A group presentation for the group G is a minimal set S of elements that generate G and a set R of relations that determine how these elements interact. We write $G = \langle S \mid R \rangle$.

If G is the cyclic group of order 7, we write $G = \langle a \mid a^7 = 1 \rangle$. All other relations among elements of G are consequences of $a^7 = 1$. If G is the abelian group of order 10, it must be cyclic and can be presented with one generator: $G = \langle a \mid a^{10} = 1 \rangle$. It may also be presented with two generators of orders 5 and 2, and with an additional relation that shows the two generators commute: $G = \langle b, c \mid b^5 = c^2 = 1,\ bc = cb \rangle$.

Definition. The dihedral group of order $2m$, which we denote[3] D_m, can be presented with two generators: a of order m, and b of order 2. A third relation shows how the two generators interact

$$D_m = \langle a, b \mid a^m = b^2 = 1,\ ba = a^{-1}b \rangle.$$

The third relation is also frequently written $bab^{-1} = a^{-1}$. In words, conjugation by b maps a to its inverse.

You may expect that, after the definition of the dihedral groups, the next order of business ought to be an example of a difference set in

[2] We could say *sum* instead of *product*. Indeed, we will usually write $G_1 \oplus G_2$ when the group operations are written additively and $G_1 \times G_2$ when they are written multiplicatively. Other authors, for example Gallian, write $G_1 \oplus G_2$ for the external direct sum/product of groups G_1 and G_2 and $H_1 \times H_2$ for the internal direct product of normal subgroups H_1, H_2 of some group G.

[3] Some authors use D_{2m} to denote the dihedral group of order 2m.

a dihedral group. We have none to offer. Indeed, it is conjectured that a difference set *cannot* exist in a dihedral group. However, difference sets *do* exist in non-abelian groups, as the next example shows. It is from Kibler's very useful catalog of non-cyclic difference sets with $k < 20$ [**40**].

Example 5. Let $G = \langle a, b \mid a^7 = b^3 = 1, ba = a^2b \rangle$. Then the set $D = \{1, a, a^3, b, a^2b^2\}$ is a $(21, 5, 1)$-difference set in G. $\diamond$

Once we find a difference set, we can find several other related difference sets. The following theorem gives us some of them.

Theorem 4.2. *Let $D \subset G$ be a (v, k, λ)-difference set.*

(i) For $g \in G$, both gD and Dg are (v, k, λ)-difference sets.

(ii) Let α be an automorphism of G. Then $\alpha(D)$ is a (v, k, λ)-difference set.

When G is written additively, the difference sets in (i) are written $g + D$ and $D + g$, which motivates calling these new difference sets (in either notation) translates or shifts of D. Sometimes we refer to the element g as the offset of the translate $g + D$.

Various infinite families of difference sets are known to exist. The first family we describe consists of the nonzero squares (quadratic residues) in $\mathbb{Z}_p$ when $p \equiv 3 \pmod 4$. In fact, the next theorem shows that this example can be generalized to nonzero squares in the finite field $GF(q)$ where q, the number of elements, is a power of a prime. Its proof requires the fact that the element -1 in the field $GF(q)$ is a square if and only if $q \equiv 1 \pmod 4$. (See A.17.) The difference sets in Theorem 4.3 are often called Paley difference sets.

Theorem 4.3. *Let q be a power of a prime, $q \equiv 3 \,(mod\, 4)$, and let G be the (additive) group of the finite field $GF(q)$. Let D be the set of nonzero squares in $GF(q)$. Then D is a difference set with parameters $(q, (q-1)/2, (q-3)/4)$.*

Proof. Notice that while we use multiplication to determine the elements of D, the group operation is addition. The set D of nonzero squares is a subgroup of the multiplicative group $GF(q)^*$ of nonzero

elements, and the map $a \mapsto a^2$ is a group homomorphism from $GF(q)^*$ onto D with kernel $\{+1, -1\}$. Since q is odd, $+1 \neq -1$. Therefore $|D| = (q-1)/2$. We also note that $q \equiv 3 \pmod 4$ implies -1 is a non-square, and therefore $a \in GF(q)^*$ is a square if and only if $-a$ is a non-square.

Now we show D is a difference set. Choose $a \in GF(q)$, $a \neq 0$. First consider the case when a is a square. Observe that for $s \in D$

$$a = d - d' \text{ with } d, d' \in D \quad \Leftrightarrow \quad sa = sd - sd' \text{ with } sd, sd' \in D.$$

This tells us that every nonzero square appears exactly the same number of times in the multiset $\Delta = \{d - d' \mid d, d' \in D, d \neq d'\}$. Next we consider the case when a is a non-square. Note that $-a$ is thus a square. Note also that

$$a = d - d' \text{ with } d, d' \in D \quad \Leftrightarrow \quad -a = d' - d \text{ with } d, d' \in D.$$

This tells us that every non-square appears exactly the same number of times in Δ as every square does. Finally, we can find the value of λ by solving $k(k-1) = \lambda(v-1)$ for λ. Since $v = q$ and $k = (q-1)/2$, we obtain $\lambda = (q-3)/4$. □

In the proof we used $q \equiv 3 \pmod 4$ to conclude -1 is a non-square. Also notice that since λ is an integer, $\lambda = (q-3)/4$ only makes sense when $q \equiv 3 \pmod 4$.

Two other families of difference sets can be constructed in some groups $\mathbb{Z}_p$ using fourth powers (quartic residues). We state the theorems here without proof.[4]

Theorem 4.4. *Let p be a prime of the form $p = 4x^2 + 1$, where x is an odd integer, and let $G = \mathbb{Z}_p$. Then the set D of all nonzero fourth powers of elements in G is a difference set.*

Theorem 4.5. *Let p be a prime of the form $p = 4x^2 + 9$, where x is an odd integer, and let $G = \mathbb{Z}_p$. Then the set D of all fourth powers of elements in G including 0 is a difference set.*

[4]Proofs of Theorems 4.4 and 4.5 are given by Lehmer in [**44**] and depend upon her lemma which appears in this text as Lemma 9.6. (See [**8**], p. 357.)

The last family of difference sets we introduce here is the family of twin prime difference sets. Twin primes are primes that differ by 2. The smallest example is the pair $\{3, 5\}$. The difference set in $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$ in Example 3 is the smallest in the family of "twin prime" difference sets. The following theorem describes a general procedure for constructing difference sets in $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ when p and $p + 2$ are primes. A more general version is Theorem 9.4, where the proof is given.

Theorem 4.6. *Let $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$ where p and $p + 2$ are primes. Let D be the subset of G consisting of elements (a, b) such that one of the following statements is true:*

$b = 0$,

a and b are both nonzero squares in their respective fields,

a and b are both non-squares in their respective fields.

Then D is a difference set.

Exercises

1. Verify the following examples in this section, and determine the parameters for each difference set.

(a) Example 1.

(b) Example 2.

(c) Example 3.

(d) Example 4.

2. Let $D = \{1, 2, 4\} \subset \mathbb{Z}_7$, and show that $\overline{D} = \{0, 3, 5, 6\}$ is a difference set in $\mathbb{Z}_7$. What are its parameters? (In Section 3 we will prove that the complement of a difference set is always a difference set.)

3. This exercise concerns the parameters v, k, λ of a difference set.

(a) Prove Theorem 4.1. Ⓢ

(b) Deduce that $0 < k < v$ implies $\lambda < k$.

(c) Can it happen that a difference set consists of exactly half the elements of a group? If so, under what circumstances?

(d) Show that if $k \leq v/2$ then $\lambda < n$. Ⓗ

4. Prove Theorem 4.2.

5. In the dihedral group D_8 every element may be written in standard form $a^i b^j$ where $0 \leq i \leq 7$ and $0 \leq j \leq 1$. Write $(a^3b)(a^2)$ in standard form.

6. In the group $G = \langle a, b \mid a^7 = b^3 = 1,\ ba = a^2b \rangle$, each element can be written in standard form $a^i b^j$ where $0 \leq i \leq 6$ and $0 \leq j \leq 2$. What is the order of G? Write ba^5 and $(a^5b^2)^{-1}$ in standard form.

7. The following is *not* a consistent presentation for a group: $\langle a, b \mid a^7 = b^3 = 1,\ ba = a^3b \rangle$. Explain why.

8. What restrictions on j are necessary for the relations in the presentation $\langle a, b \mid a^7 = b^3 = 1, ba = a^j b \rangle$ to be consistent? Justify your answer. Ⓗ

9. Similar difference sets in two different groups.

(a) Let $G = \langle a, b \mid a^7 = b^3 = 1,\ ab = ba \rangle$ and let $D = \{a, a^2, a^4, b, b^2\}$. Verify that D is a difference set in G.

(b) Let $G' = \langle c, d \mid c^7 = d^3 = 1,\ dc = c^2 d \rangle$ and let $D' = \{c, c^2, c^4, d, d^2\}$. Verify that D' is a difference set in G'.

10. Verify Example 5.

11. Fill in the details in the proof of Theorem 4.3 as follows.

(a) Verify that D is a subgroup of $GF(q)^*$.

(b) Verify that the mapping $a \mapsto a^2$ is a group homomorphism from $GF(q)^*$ onto D with kernel $\{+1, -1\}$.

(c) Solve $k(k-1) = \lambda(v-1)$ for λ in terms of q.

12. This exercise introduces computation in the field $GF(q)$ when q is not a prime. Specifically, we construct a difference set in the additive group $GF(27)$. We use the multiplication in $GF(27)$ to determine membership in our difference set. View $GF(27)$ as $\mathbb{Z}_3[x]/\langle p(x)\rangle$ where $p(x) = x^3 + 2x + 1$, a cubic polynomial that is irreducible in $\mathbb{Z}_3[x]$. The polynomials $ax^2 + bx + c$ in $\mathbb{Z}_3[x]$ form a complete set of coset representatives for $\mathbb{Z}_3[x]/\langle p(x)\rangle$. Identify an element of $GF(27)$ with its coset representative.

(a) Show that x in $GF(27)$ has multiplicative order 26 by expressing $x^3, x^4, \ldots$ as quadratic polynomials in x. Represent $ax^2 + bx + c$ by the triple (a, b, c).

(b) List the triples corresponding to the nonzero squares in $GF(27)$. (This is the $(27, 13, 6)$-difference set promised in Theorem 4.3.)

13. Use Theorems 4.4 and 4.5 to find difference sets in $\mathbb{Z}_{37}$ and $\mathbb{Z}_{13}$. In each theorem, what are the parameters of the difference sets constructed from the fourth powers of elements in Z_p in terms of the prime p?

14. Using Theorem 4.6, construct a twin primes difference set in $\mathbb{Z}_3 \oplus \mathbb{Z}_5$. Then using $\mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15}$ with $(1, 1)$ mapped to generator 1, find the corresponding difference set in $\mathbb{Z}_{15}$. Compare your results to the difference set in $\mathbb{Z}_{15}$ in Example 3. Using this same technique, construct a difference set in $\mathbb{Z}_{35}$.

15. For all parts of this exercise assume G is an abelian group under addition. Call a subset $S \subseteq G$ <u>normalized</u> if $\sum_{s \in S} s = 0$ in G.

(a) Find a normalized difference set in $\mathbb{Z}_7$ that is a translate of $\{0, 1, 3\}$.

(b) Find a normalized difference set in $\mathbb{Z}_{11}$ that is a translate of $\{1, 4, 6, 7, 8\}$.

(c) Find a normalized difference set in $\mathbb{Z}_{13}$ that is a translate of $\{3, 4, 6, 12\}$.

(d) Let q be a power of a prime, $q \equiv 3 \pmod 4$, $q > 3$, and let $G = GF(q)$. Let D be the set of nonzero squares in G. Show D is normalized.

16. Assume G is an abelian group under addition. Further assume $|G| = v$, $D \subset G$, $|D| = k$ and $\gcd(k, v) = 1$. Show that D has a unique translate that is normalized. Also show that the total number of (v, k, λ)-difference sets in G is equal to v times the number of normalized (v, k, λ)-difference sets.

4.2. Difference sets and designs

In Theorem 2.13 we stated that if $p \equiv 3 \pmod 4$ is a prime, and D is the set of nonzero squares in $\mathbb{Z}_p$ (which we now know to be a difference set), then we have a symmetric design whose points are the elements of $\mathbb{Z}_p$ and whose blocks are the translates $a + D$ as a varies through the additive group $\mathbb{Z}_p$. The parameters of the design are $\big(p,\ (p-1)/2,\ (p-3)/4\big)$, the same as the parameters of the difference set. These examples are instances of a general phenomenon. We state it in multiplicative notation where the translates have the form aD.

Definition. Given a difference set $D \subset G$, the development of D, denoted dev$D$, is the incidence structure whose points are the elements of G and whose blocks are the (left) translates of the difference set

$$\mathcal{B} = \{aD \mid a \in G\}.$$

Theorem 4.7. *Let $D \subset G$ be a (v, k, λ)-difference set. Then devD is a symmetric (v, k, λ) design.*

Proof. We refer to the numbering of the properties in the definition of a symmetric design in Chapter 2, page 26. Clearly the number of points of dev$D$ equals v, and the number of points per block is equal to $|D| = k$, so properties (i) and (iv) hold. Because it will be useful in verifying the other properties for a symmetric design, we next show that for $a, b \in G$ with $a \neq b$, we have $|aD \cap bD| = \lambda$. Fix the distinct group elements a, b and suppose $g \in aD \cap bD$. Then $g = ad_1 = bd_2$ for d_1, d_2 in D if and only if $a^{-1}b = d_1 d_2^{-1}$. Because D is a difference set and $a^{-1}b \neq 1$, there are exactly λ such choices of d_1, d_2.

Since we know $\lambda < k$, $|aD \cap bD| = \lambda$ tells us that distinct group elements a and b give distinct blocks aD and bD, so the number of blocks of dev$D$ equals v; this is property (ii). We also know that two distinct blocks have exactly λ points in common; this is property (vi). To count the number of blocks on a point, fix $g \in G$ and observe that $g \in aD$ if and only if $a = gd^{-1}$ for some $d \in D$. Since there are k choices for $d \in D$, there are k choices for a and thus k choices for the block aD on g; this is axiom (iii). From Exercise 2.32, we know that the five properties for a symmetric design which we have verified thus far imply property (v): that two distinct points appear together in exactly λ blocks. □

The relationship between a difference set $D \subset G$ and its development is stronger than just the fact that dev$D$ is a symmetric design. The design also bears a special relationship to the group G. If the group operation is written multiplicatively, we can identify each element $g \in G$ with the function $\pi_g : x \mapsto gx$. Since left multiplication by g takes blocks to blocks, G is a group of automorphisms of the design dev$D$. We will see that G acts regularly on the points and the blocks of dev$D$.

In fact, the relationship goes the other way too. If a group acts regularly on the points and blocks of a symmetric design, then it contains a difference set with the parameters of the symmetric design. Indeed, this is what Singer did in his seminal 1938 paper: he constructed a cyclic group acting regularly on a particular symmetric design, and used this to construct a difference set. The following theorem is the formal statement.

Theorem 4.8. *Let G be a finite group of order v. Then G acts regularly on the points and on the blocks of a symmetric (v, k, λ) design if and only if G contains a (v, k, λ)-difference set.*

Proof. First, assume G contains a (v, k, λ)-difference set D. We already know dev$D$ is a symmetric (v, k, λ) design. We write G multiplicatively, so for $g \in G$ and x a point of dev$D$, $\pi_g(x) = gx$. We have observed that G is a group of automorphisms of the design dev$D$. We claim G acts regularly on the points of dev$D$. By Corollary 3.7 it

follows that G acts regularly on the blocks of dev$D$. (For details see Exercise 17.)

Now assume G acts regularly on a symmetric (v, k, λ) design $\mathcal{D}$ with point set $\mathcal{P}$ and block set $\mathcal{B}$. Choose a point $P_0 \in \mathcal{P}$ and a block $B_0 \in \mathcal{B}$. Because G acts transitively on $\mathcal{P}$, for each $P \in \mathcal{P}$ there is $g \in G$ with $g(P_0) = P$. Because only the identity fixes a point, g must be the unique group element mapping P_0 to P. Identify the point P with the group element g. Notice that P_0 is identified with the identity 1_G. Similarly, because G acts regularly on blocks, for each $B \in \mathcal{B}$, there is a unique $g \in G$ with $g(B_0) = B$. Let $D = \{g \in G \mid g(P_0) \in B_0\}$; in other words, D is the set of group elements identified with the points in the block B_0.

Set up notation with $B_0 = \{P_1, \ldots, P_k\}$ and $D = \{d_1, \ldots, d_k\}$ with $P_j = d_j(P_0)$. Notice that if B is any block, $B = g(B_0) = \{g(P_1), \ldots, g(P_k)\} = \{gd_1(P_0), \ldots, gd_k(P_0)\}$ for a unique $g \in G$, and B is identified with the set of group elements in gD.

Now we show D is a (v, k, λ)-difference set in G. Since B_0 contains k points, D contains k group elements. Choose $x \in G$, $x \neq 1_G$, and write $x = h^{-1}g$ for a fixed choice of $g \neq h$ in G. The blocks $g(B_0)$ and $h(B_0)$ are distinct and so have exactly λ points in common. A common point corresponds to a choice of (i, j) with $gd_i(P_0) = hd_j(P_0)$. Because G acts regularly on points, we must have $gd_i = hd_j$ and $x = h^{-1}g = d_j d_i^{-1}$. Conversely, writing $x = d_j d_i^{-1}$ for $d_i, d_j \in D$ produces a point common to the blocks $g(B_0)$ and $h(B_0)$ (where, as before, $x = h^{-1}g$). Therefore x can be written in exactly λ ways as a "difference" $d_j d_i^{-1}$ for $d_i, d_j \in D$. □

Note that implicit in the proof of Theorem 4.8 is the fact that the symmetric design $\mathcal{D}$ on which G is assumed to act regularly is equivalent to the constructed design dev$D$, where D is the difference set defined by means of the chosen point $P_0 \in \mathcal{P}$ and the chosen block $B_0 \in \mathcal{B}$.

We have left dangling the assertion that it does not matter in our definition of a (v, k, λ)-difference set whether we write the differences of elements of D as $d_1 d_2^{-1}$ or as $d_1^{-1} d_2$. The following indirect approach to the proof of this fact is due to Bruck in [**10**]. A more direct

approach, due to Bruck in the same paper, is in the exercises for the next section. (See Exercise 29.)

Theorem 4.9. *Let D be a non-empty proper subset of a finite group G. Let $v = |G|$ and $k = |D|$, and assume λ is a fixed integer. The following are equivalent:*

(i) If $g \in G$, $g \neq 1_G$, there are exactly λ pairs $d_1, d_2 \in D$ with $d_1 d_2^{-1} = g$.

(ii) If $g \in G$, $g \neq 1_G$, there are exactly λ pairs $d_1, d_2 \in D$ with $d_1^{-1} d_2 = g$.

Proof. Assume condition (i) holds, so D is a difference set. By Theorem 3.7, dev$D$ is a symmetric design. In particular, two distinct points appear together in exactly λ blocks. Let g be a non-identity element of G, and let $h = 1_G$. Then g and h lie in exactly λ blocks aD. This means that there exist $d_1,\ d_2 \in D$ with $g = ad_2$ and $h = ad_1$. Solving for a we get $a = gd_2^{-1} = hd_1^{-1}$. So $g = h^{-1}g = d_1^{-1}d_2$. Thus, every block aD that contains both g and h gives a representation of g as $d_1^{-1}d_2$. So there are at least λ representations of g as $d_1^{-1}d_2$, and this is true for every non-identity element g. We already know $k(k-1) = \lambda(v-1)$, so the $k(k-1)$ differences $d_1^{-1}d_2$ cannot represent g more than λ times.

An argument similar to the proof of Theorem 3.7 shows that condition (ii) guarantees that the incidence structure with blocks Da for $a \in G$ is a symmetric (v, k, λ) design, and this in turn implies condition (i). □

Exercises

17. Assume that $D \subset G$ is a difference set. Identify $g \in G$ with the function $\pi_g : G \to G$, with $\pi_g(x) = gx$. Complete the proof of Theorem 4.8 by showing that:

(a) Each π_g is an automorphism of the design dev$D$.

(b) G acts regularly on the points of dev$D$.

18. Complete the proof of Theorem 4.9 by showing that condition (ii) implies condition (i).

19. Recall Example 2.11, the symmetric $(16, 6, 2)$ design whose points are the 16 individual squares of a 4×4 grid and whose blocks consist of the six points in the row and column of a fixed square, not including the square itself. Label the points as indicated in Figure 4.1.

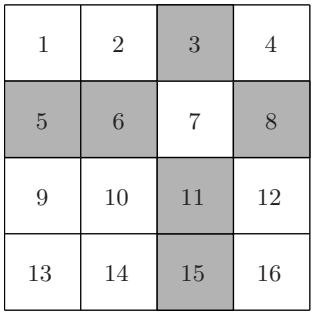


Figure 4.1. Design from 4×4 grid; block T_7 is shaded

Let T_j be the block determined by point j; for example, the block $T_7 = \{3, 5, 6, 8, 11, 15\}$.

(a) Show that the incidence matrix of this design is given by

$$A = \begin{bmatrix} M & I & I & I \\ I & M & I & I \\ I & I & M & I \\ I & I & I & M \end{bmatrix}$$

where I is the 4×4 identity matrix and

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

(b) Define permutations α and β of the 16 points by

$$\alpha = (1\,2\,3\,4)(5\,6\,7\,8)(9\,10\,11\,12)(13\,14\,15\,16) \quad \text{and}$$
$$\beta = (1\,5\,9\,13)(2\,6\,10\,14)(3\,7\,11\,15)(4\,8\,12\,16).$$

Explain why α and β are automorphisms of the design.

(c) Show that $\alpha\beta = \beta\alpha$ and $G = \langle \alpha, \beta \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

(d) Show that $G = \langle \alpha, \beta \rangle$ acts regularly on the points and blocks of this design.

(e) Choose $P_0 = 1$ and $B_0 = T_1 = \{2, 3, 4, 5, 9, 13\}$. What is the corresponding set $D \subset G$ as in the proof of Theorem 4.8? Ⓢ

(f) Verify that D is a $(16, 6, 2)$-difference set in G.

4.3. Integral group ring

In this section we introduce an algebraic tool that is particularly useful for studying finite groups and difference sets. We start with a finite multiplicative group G. The elements of the integral group ring $\mathbb{Z}G$ are formal sums of integers times group elements. For instance, if $g_1, g_2 \in G$, then $2g_1 - 5g_2$ is an element of the integral group ring. When all the integer coefficients are non-negative we can think of an element in $\mathbb{Z}G$ as a multiset of elements of G. From this point of view, $3g_1 + 4g_2$ is 3 copies of g_1 and 4 copies of g_2. The elements of $\mathbb{Z}G$ are called *formal* sums since the addition of group elements is not defined within the group; for example, $g_1 + g_2$ is not a group element. Addition and multiplication of elements in this ring are similar to addition and multiplication of polynomials.

Definition. Let G be a finite multiplicative group. The integral group ring $\mathbb{Z}G$ consists of formal sums $\sum_{g \in G} a_g g$ where $a_g \in \mathbb{Z}$. Addition and multiplication are defined as follows:

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

$$\left(\sum_{f \in G} a_f f \right) \left(\sum_{g \in G} b_g g \right) = \sum_{h \in G} \left(\sum_{fg = h} a_f \, b_g \right) h.$$

The zero element of the ring is the sum $\sum_g 0g$ having all coefficients equal to zero. Part of what we mean by calling the elements of $\mathbb{Z}G$ "formal sums" is that the *only* way the sum $\sum_g a_g g$ can be zero in $\mathbb{Z}G$ is if $a_g = 0$ for each g in G. We write $0g = 0$ for the product of the integer 0 and the group element g, and $1g = g$ for $1 \in \mathbb{Z}$ and $g \in G$. To distinguish the integer 1 from the group identity in this

setting, we write 1_G for the identity in G.[5] It follows that $\mathbb{Z}G$ is a ring with identity 1_G. Further, the ring $\mathbb{Z}G$ is commutative if and only if the group G is abelian.

Remark: Replacing $\mathbb{Z}$ by any commutative ring R with identity also gives a ring RG with identity, and RG is commutative if and only if G is abelian. We use the ring $\mathbb{Q}G$ in the exercises at the end of this section. Indeed, Theorem 4.10 below remains true in the group ring RG provided the characteristic of R is zero ([**8**], p. 312).

In $\mathbb{Z}G$, if $A = \sum a_g g$ and t is an integer, we denote by $A^{(t)}$ the element $\sum a_g g^t$. In particular, $A^{(-1)}$ is the element $\sum a_g g^{-1}$. We may consider any subset S of G as an element of the integral group ring by identifying S with the formal sum $\sum_{g\in S} g$. Using this notation we can restate the condition that makes D a difference set in G.

Theorem 4.10. *Let D be a non-empty proper subset of a group G with $|D| = k$ and $|G| = v$. Then D is a (v, k, λ)-difference set if and only if*

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

holds in the integral group ring $\mathbb{Z}G$.

The following theorem gives us another way to use one difference set to construct another. It parallels what we saw in Chapter 2, namely that the complement of a symmetric design is again a symmetric design.

Theorem 4.11. *Let D be a (v, k, λ)-difference set in G. Then its complement $\overline{D} = G \setminus D$ is a difference set in G.*

Remark: When the multiplicative group G is a subset of a ring, the addition of group elements is defined in the ring, and that can be confusing. For example, consider the group $G = \{1, \omega, \omega^2, \ldots, \omega^6\} \subset \mathbb{C}$ for $\omega = \cos(2\pi/7) + i\sin(2\pi/7)$. As we saw in Chapter 1, as a sum of complex numbers $1 + \omega + \cdots + \omega^6 = 0$ in $\mathbb{C}$, but the "formal sum" $\sum \omega^j$ is *not* the zero element of the ring $\mathbb{Z}G$. To avoid this

[5] Many authors don't make this distinction and write $m \in \mathbb{Z}G$ where we write $m1_G$.

possible confusion, another way to define $\mathbb{Z}G$ is as the set of all integer-valued functions on G. From this point of view, the element $\sum_g a_g g$ is replaced by the function $F : G \to \mathbb{Z}$ with $F(g) = a_g$. Then, for the example above, $1 + \omega + \cdots + \omega^6 \in \mathbb{Z}G$ corresponds to the function F_1 with $F_1(g) = 1$ for all g in G, but $0 \in \mathbb{Z}G$ corresponds to the function F_2 with $F_2(g) = 0$ for all g in G. The addition of elements of $\mathbb{Z}G$ in this formulation is easy to describe: if $F_1(g) = a_g$ and $F_2(g) = b_g$, then $(F_1 + F_2)(g) = a_g + b_g$. Multiplication is more complicated to describe: $(F_1F_2)(h) = \sum_{fg=h} a_f b_g$. Exercise 26 gives some practice with this alternative definition. Also see the exercises on the Hall polynomial for yet another representation of the integral group ring for the special case of an additive group.

For now, we leave our discussion of the integral group ring here. It will be used heavily in later chapters.

Exercises

20. Let G be a finite group.

(a) Verify that $\mathbb{Z}G$ is a ring with identity 1_G.

(b) Show that the ring $\mathbb{Z}G$ is commutative if and only if the group G is abelian.

21. We know that the set of nonzero squares $\{1, 3, 4, 5, 9\}$ in $\mathbb{Z}_{11}$ is an $(11, 5, 2)$-difference set. Switch to multiplicative notation and let G be the abelian cyclic group $\langle a \mid a^{11} = 1\rangle$, and let $D = \{a, a^3, a^4, a^5, a^9\}$. Compute $GG^{(-1)}$ and $DD^{(-1)}$ in $\mathbb{Z}G$ by explicitly multiplying out the sums.

22. Let $G = \langle a \mid a^{11} = 1\rangle$.

(a) Let $S = \{1, a, a^2, a^4, a^7\}$. Compute $SS^{(-1)}$ in $\mathbb{Z}G$.

(b) Let $T = \{1, a, a^2, a^5, a^7\}$. Compute $TT^{(-1)}$ in $\mathbb{Z}G$.

(c) Based on your calculations above, which of S and T is a difference set? Explain.

23. Assume $S \subseteq G$ and $s \in S$.

(a) Calculating in the integral group ring $\mathbb{Z}G$, find SG, and GS. Ⓢ

(b) What element of $\mathbb{Z}G$ corresponds to $G \setminus S$?

(c) Let $A, B \in \mathbb{Z}G$. Explain why $(A+B)^{(-1)} = A^{(-1)} + B^{(-1)}$.

(d) Explain why $G^{(-1)} = G$.

24. Prove Theorem 4.10.

25. Use the integral group ring $\mathbb{Z}G$ to prove Theorem 4.11 and find the parameters of the difference set $\overline{D} = G \setminus D$.

26. In this exercise you will explore the alternative definition of $\mathbb{Z}G$ as the set of all integer-valued functions on G. From this point of view, the element $\sum_g a_g g$ is replaced by the function $F : G \to \mathbb{Z}$ with $F(g) = a_g$.

(a) Let $G = \langle a, b \,|\, a^2 = b^2 = 1_G, ab = ba \rangle$. What is the function $F_1 : G \to \mathbb{Z}$ associated with the sum $3a - 5b + ab$ in $\mathbb{Z}G$?

(b) Continue with G as in part (a). What is the element in $\mathbb{Z}G$ associated with the function F_2 for which $F_2(1_G) = 2$, $F_2(a) = 0$, $F_2(b) = 7$, $F_2(ab) = -4$?

(c) What is the sum function $F_1 + F_2$ on G? What is the product function $F_1 F_2$?

(d) Let $H = \langle a \,|\, a^4 = 1_H \rangle$. What function $F : H \to \mathbb{Z}$ is associated with the formal sum $a + a^3$ in $\mathbb{Z}H$?

(e) Let $K = \{1, i, -1, -i\} \subset \mathbb{C}^*$. What function $F : K \to \mathbb{Z}$ is associated with the formal sum $i + (-i)$ in $\mathbb{Z}K$? What is the value of the "actual" sum $i + (-i)$ in $\mathbb{C}$?

The next two exercises involve computations in the more general ring $\mathbb{Q}G$. They are needed for Bruck's direct proof that it does not matter in the definition of a difference set whether we write inverses on the left or on the right. (See Exercise 29.)

27. Show that $x, y \in \mathbb{Q}$ implies that $x1_G + yG$ commutes with all elements of $\mathbb{Q}G$.

28. Suppose A and B are elements of the group ring $\mathbb{Q}G$. Show that $AB = 1_G$ implies $BA = 1_G$. Ⓗ

29. This result is from ([**10**], p. 468). Let D be a non-empty proper subset of a group G and assume that the equation $DD^{(-1)} = n1_G + \lambda G$ holds in the integral group ring $\mathbb{Z}G$. Write $C = n1_G + \lambda G$.

(a) Show that there is an element $C' \in \mathbb{Q}G$ of the form $a1_G + b\,G$ satisfying $C'C = CC' = 1_G$; in other words C is an invertible element of the ring $\mathbb{Q}G$.

(b) Show that D is invertible in $\mathbb{Q}G$.

(c) Show that D and $D^{(-1)}$ commute. This, along with Theorem 4.10, gives a direct proof that conditions (i) and (ii) in Theorem 4.9 are equivalent.

The next three exercises introduce the use of polynomials as an alternative representation of elements of $\mathbb{Z}G$ for G an *additive* group. This representation leads to an alternative characterization of a difference set D in G. Hall used this strategy in his work on difference sets and it can also be found in his influential book *Combinatorial Theory* [**28**]. The polynomial $D(x)$ in Exercise 31 is sometimes called the Hall polynomial of the difference set D.

30. In $G = \mathbb{Z}_7 = \{0, 1, \ldots, 6\}$ let $D = \{1, 2, 4\}$. Represent the set $S \subseteq G$ by the polynomial $S(x) = \sum_{g \in S} x^g$.

(a) Find $D(x)$ and $D(x^{-1})$, computing exponents mod 7.

(b) What is $G(x)$?

(c) Compute the product of polynomials $D(x)D(x^{-1})$, reducing exponents mod 7.

31. Let G be an additive abelian group, and let

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g\, x^g \mid a_g \in \mathbb{Z} \right\}.$$

The "indeterminate" x is essentially a place-holder. Addition in $\mathbb{Z}[G]$ is defined by $\sum a_g\, x^g + \sum b_g\, x^g = \sum (a_g + b_g)\, x^g$. Multiplication is

defined via $x^f x^g = x^{f+g}$, where $f+g$ is defined in G, as follows.

$$\left(\sum_{f\in G} a_f\, x^f\right)\left(\sum_{g\in G} b_g\, x^g\right) = \sum_{h\in G}\left(\sum_{f+g=h} a_f\, b_g\right) x^h.$$

(a) Let $A \subseteq G$. Writing the group operation additively, A determines the polynomial $A(x) = \sum_{g\in A} x^g$ in $\mathbb{Z}[G]$, corresponding to what we write as A in $\mathbb{Z}G$ when we write the operation multiplicatively. Explain why $A(x^{-1})$ corresponds to what we call $A^{(-1)}$ in $\mathbb{Z}G$. Also explain why the k-set D in G of order v is a (v,k,λ)-difference set in G if and only if $D(x)D(x^{-1}) = n + \lambda G(x)$ in $\mathbb{Z}[G]$.

(b) Show that if the additive group G is cyclic of order v, say $G = \mathbb{Z}_v$, the polynomial ring $\mathbb{Z}[G]$ is isomorphic (as a ring) to $\mathbb{Z}[x]/\langle x^v - 1\rangle$.

32. (Prop 28.1 in [**70**]) Continuing the notation of the previous exercise, assume v, k, λ are positive integers satisfying $k(k-1) = \lambda(v-1)$ and G is abelian of order v. Suppose $A(x) = \sum a_g x^g$ satisfies

$$A(x)A(x^{-1}) = n + \lambda G(x).$$

Show that there exists $B(x) = \sum b_g x^g$ with $b_g \in \{0,1\}$ and $B(x)B(x^{-1}) = n + \lambda G(x)$. Ⓗ

The results of the next three exercises are used later: the first two for the proof of Theorem 6.2, and all three for the proof of Theorem 9.5, specifically for the proof of Lemma 9.6.

33. Assume G is an abelian group and p is a prime. For $A, B \in \mathbb{Z}G$ say $A \equiv B \pmod p$ if all the integer coefficients of $A - B$ are divisible by p. Let $S \in \mathbb{Z}G$. Show $S^p \equiv S^{(p)} \pmod p$. Ⓗ

34. Assume G is an abelian group of order v and p is a prime not dividing v. Let $A \in \mathbb{Z}G$ and suppose $A^m \equiv 0 \pmod p$ for some positive integer m. Then $A \equiv 0 \pmod p$. Ⓗ

35. Assume G is abelian and D is a nontrivial (v, k, λ)-difference set in G (i.e., $1 < k < v - 1$). Suppose further that $D^{(-1)} = D$. Show that v must be even. Ⓗ

4.4. Equivalence

When should we regard two difference sets as "the same"? A reasonable answer is that two difference sets are equivalent if it is possible to transform one to the other by repeated applications of Theorem 4.2. More formally:

Definition. Difference sets D_1 and D_2 in a group G are equivalent if for some $g \in G$ and for some automorphism α of G, $D_2 = g\alpha(D_1)$. (If the group is written additively, this condition is written as $D_2 = g + \alpha(D_1)$.)

Note that we use subscripts to distinguish difference sets in this section. Context should make clear that there is no reference here to dihedral groups. Kibler [**40**] lists all of the non-cyclic difference sets (up to equivalence) for $k < 20$. When we refer to difference sets on this list, we use as the subscript the number of the difference set in the appropriate table from that paper.

Example 6. In the abelian group $G = \langle a, b \mid a^4 = b^4 = 1 \rangle$, Kibler gives the $(16, 6, 2)$-difference set $D_4 = \{1, a, a^2, b, b^3, a^3b^2\}$. We can define an automorphism α of G by setting $\alpha(a) = b$ and $\alpha(b) = ab$. Then $ab\,\alpha(D_4) = \{ab, ab^2, ab^3, a^2b^2, 1, a^3b^2\}$ is a difference set in G equivalent to D_4. ◇

Example 7. Example 5 in Section 1 is another from Kibler, where $G = \langle a, b \mid a^7 = b^3 = 1, ba = a^2b \rangle$ contains the $(21, 5, 1)$-difference set $D_1 = \{1, a, a^3, b, a^2b^2\}$. Kibler claims that all difference sets in this group are equivalent to this one. We may check that $D' = \{a, a^2, a^4, b, b^2\}$ is also a difference set in G, so we try to find an automorphism α of G and an element $g \in G$ with $D' = g\alpha(D_1)$. To figure this out, first observe that $a^6D' = \{1, a, a^3, a^6b, a^6b^2\}$ has 3 elements in common with D_1. This suggests we might look for an automorphism of G that takes D_1 to a^6D'. We try α defined by $\alpha(a) = a$ and $\alpha(b) = a^6b$. Since a^6b is an element of order 3

and satisfies $(a^6b)a = a^2(a^6b)$, α is in fact an automorphism. Also $\alpha(a^2b^2) = a^6b^2$ so $\alpha(D_1) = a^6D'$, and this tells us that $D' = a\,\alpha(D_1)$. Thus D_1 and D' are indeed equivalent. $\diamond$

Example 8. Let $G = \langle a, b \mid a^8 = b^2 = 1,\ ab = ba\rangle$.

Kibler lists two $(16, 6, 2)$-difference sets in G:

$$\begin{aligned} D_1 &= \{1, a, a^2, a^4, ab, a^6b\} \text{ and} \\ D_2 &= \{1, a, a^2, a^5, b, a^6b\}. \end{aligned}$$

He claims these are not equivalent. How does he know? Suppose that D_1 and D_2 are equivalent and that $g(\alpha(D_1)) = D_2$ for some $g \in G$ and some automorphism α. We show that this leads to a contradiction.

Since $g(\alpha(D_1)) = D_2$, we know that $\alpha(D_1) = g^{-1}D_2$. First we limit the values of g that are possible. Since $1 \in D_1$, 1 is also in $\alpha(D_1)$. So 1 must be in $g^{-1}D_2$. This means that g must be in D_2. We look at all the shifts of D_2 by inverses of elements in D_2:

$$\begin{aligned} 1D_2 &= \{1, a, a^2, a^5, b, a^6b\} \\ a^{-1}D_2 &= \{a^7, 1, a, a^4, a^7b, a^5b\} \\ a^{-2}D_2 &= \{a^6, a^7, 1, a^3, a^6b, a^4b\} \\ a^{-5}D_2 &= \{a^3, a^4, a^5, 1, a^3b, ab\} \\ b^{-1}D_2 &= \{b, ab, a^2b, a^5b, 1, a^6\} \\ (a^6b)^{-1}D_2 &= \{a^2b, a^3b, a^4b, a^7b, a^2, 1\}. \end{aligned}$$

To limit further the possible values of g, we look at the orders of the elements in these shifts of D_2. Since the orders of the elements in D_1 are $\{1, 8, 4, 2, 8, 4\}$, and α preserves the orders of elements, these are also the orders of $\alpha(D_1)$, and therefore must be the orders of the elements in $g^{-1}D_2$. Note that in the list above, $a^{-1}D_2$ and $a^{-5}D_2$ each have four elements of order 8, so a and a^5 are eliminated as candidates for g. The only remaining possible values for g are 1, a^2, b, and a^6b.

Finally we look at the element $a^4 \in D_1$ and its image under α. Since a^4 has order 2, its image must be a^4, b, or a^4b. If we let $\alpha(a) = a^ib^j$, then $\alpha(a^4) = a^{4i}b^{4j}$. Since b has order 2, $b^{4j} = 1$. This forces $\alpha(a^4) = a^4$. But now we note that a^4 is not in $g^{-1}D_2$ for any

of the four remaining values for g. So we have a contradiction. We conclude that D_1 and D_2 are not equivalent. $\diamond$

Recall from Chapter 2 that two incidence structures are isomorphic if there is a one-to-one, onto correspondence between their point sets that maps blocks to blocks and preserves incidence. It is reasonable to wonder whether equivalent difference sets produce isomorphic designs. Indeed they do.

Theorem 4.12. *Assume D and D' are equivalent difference sets in the group G. Then the designs dev$D$ and devD' are isomorphic.*

There are many cases known of inequivalent difference sets with the same parameters. Example 8 gives one instance. Here is a preview of another example. We know from Theorem 4.3 that the nonzero squares in $\mathbb{Z}_{31}$ form a $(31, 15, 7)$-difference set. In Chapter 8 we will study the family of cyclic difference sets discovered by Singer in his 1938 paper. The parameters of these Singer difference sets are

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = \frac{q^m - 1}{q - 1}, \quad \lambda = \frac{q^{m-1} - 1}{q - 1},$$

where q can be any prime power and m is an integer greater than 1. When $q = 2$ and $m = 4$ we get a $(31, 15, 7)$-difference set in $\mathbb{Z}_{31}$. We will see in Chapter 9 that the development of Singer's $(31, 15, 7)$-difference set is not isomorphic to the development of the $(31, 15, 7)$-difference set of nonzero squares. It then follows from Theorem 4.12 that these difference sets are not equivalent.

Exercises

36. Show that equivalence of difference sets is an equivalence relation.

37. Prove that if D_1 and D_2 are equivalent difference sets in a group G, then their complements are equivalent difference sets in G.

38. In this exercise you will find all difference sets in $G = \mathbb{Z}_7$ that are equivalent to $D = \{1, 2, 4\}$.

(a) Find all difference sets equivalent to D by a shift.

(b) How many group automorphisms does G have?

(c) Now find all the subsets of G that are equivalent to the difference set $D = \{1, 2, 4\}$. Ⓢ

39. Show that if $\mathbb{Z}_m$ contains an (m, k, λ)-difference set, then it contains an (m, k, λ)-difference set D with $0, 1 \in D$.

40. Let G be the abelian group $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $G = \langle\, a, b, c \mid a^4 = b^2 = c^2 = 1 \rangle$. For this group Kibler [**40**] lists two difference sets: $D_6 = \{1, a, a^2, b, c, a^3bc\}$ and $D_7 = \{1, a, a^2, ab, ac, a^3bc\}$. Show that these are not equivalent. Ⓗ

41. Kibler [**40**] gives three difference sets in the group $\langle\, a, b \mid a^4 = b^4 = 1,\ ab = ba \,\rangle$. They are

$$\begin{aligned} D_3 &= \{1,\ a,\ a^2,\ b,\ ab^2,\ a^2b^3\}, \\ D_4 &= \{1,\ a,\ a^2,\ b,\ b^3,\ a^3b^2\}, \\ D_5 &= \{1,\ a,\ b,\ a^2b,\ ab^2,\ a^2b^2\}. \end{aligned}$$

Which of Kibler's three examples is equivalent to the difference set in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ of Exercise 19 on page 58? How do you know?

42. Prove that in $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ the difference sets

$$\{1,\ a,\ b,\ c,\ d,\ abcd\} \quad \text{and} \quad \{a,\ b,\ c,\ d,\ ab,\ cd\}$$

are equivalent. (The first is in Kibler's paper [**40**]; the second is in Baumert ([**5**], p. 10).)

43. Show that up to equivalence there is only one $(16, 6, 2)$-difference set in $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Ⓗ

44. Prove Theorem 4.12.

Coda

The fundamental problem in the study of difference sets is the existence question:

Given a group, does it contain a difference set?

In particular, can we construct one? Can we prove one cannot exist?

Difference sets bridge group theory and design theory, since a group contains a difference set if and only if the group acts regularly on the points and on the blocks of a symmetric design. Groups, designs and existence are three of our mathematical threads. We describe briefly how these and others weave through the book.

The definition of a difference set is combinatorial, so it is natural that counting plays an important role. Counting leads immediately to the fundamental equation $\lambda(v-1) = k(k-1)$ satisfied by the parameters of a (v, k, λ)-difference set. This is the first necessary condition for existence. We will see other necessary conditions in Chapters 5–7.

Many of the examples of difference sets we have seen thus far come from number theory: squares, fourth powers, twin primes. We use methods from algebra, combinatorics and geometry to construct families of difference sets in Chapters 8 and 9.

We translate the criterion for being a difference set into an equation in the integral group ring $\mathbb{Z}G$. This group ring equation opens the door to the use of other algebraic tools to address the existence question, and we develop these topics in Chapters 10–12.

Chapter 5

Bruck-Ryser-Chowla Theorem

The Bruck-Ryser-Chowla Theorem (BRC) is one of the most important tools for proving that difference sets with particular parameters cannot exist. It gives necessary conditions on the parameters (v, k, λ) for the existence of a symmetric (v, k, λ) design. Since the development of a difference set is a symmetric design, this theorem places restrictions on the parameters of a difference set in a group of order v.

In Section 1 we present the BRC Theorem and look at a number of applications of the theorem. In Section 2 we look at the details of the proof. This will lead us through interesting arguments from number theory and from linear algebra. It will also explain how the existence of a solution to a diophantine equation could have any bearing on the existence of a symmetric design.

The Bruck-Ryser-Chowla Theorem gets its name from the work by Bruck and Ryser [**11**] and by Chowla and Ryser [**13**]. In the first paper the authors prove the theorem in the case $\lambda = 1$. The second paper extends the result to any positive integer λ. Ryser's later paper [**61**] gives a much simplified proof. We look at this proof in some detail in Section 2.

5.1. The BRC Theorem

The Bruck-Ryser-Chowla Theorem gives necessary conditions for the existence of a symmetric (v, k, λ) design, and thus necessary conditions for a (v, k, λ)-difference set in a group G. Since this test is independent of the structure of G, it provides us with a test that is easily applied.

Theorem 5.1. *(Bruck-Ryser-Chowla, 1949, 1950) Assume the existence of a symmetric (v, k, λ) design.*

(i) If v is even, then $n = k - \lambda$ is a perfect square.

(ii) If v is odd, then the diophantine equation

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a nonzero solution in integers x, y, z.

In the case v is even, both the statement and the proof are straightforward. (See Exercise 4.) The statement in the case v is odd may seem unusual. Its proof is based on equivalence of matrices, and will lead us through some interesting arguments from number theory and linear algebra. Before we embark on the proof, let us look at some examples of how this theorem is used to rule out difference sets with specific parameters. The parameters we consider in these examples already meet the basic test that $k(k-1) = \lambda(v-1)$.

Example 1. Consider the parameters $(22, 7, 2)$. Since v is even, n would have to be a perfect square. But $n = 7 - 2 = 5$, so there is no symmetric design, and therefore no difference set with these parameters. ◇

Example 2. Consider the parameters $(49, 16, 5)$. Could there be a difference set with these parameters? Since $v = 49$ is odd, we look at the diophantine equation $x^2 = 11y^2 + 5z^2$. Since $(x, y, z) = (4, 1, 1)$ is a nonzero solution, BRC cannot rule out the possibility of a difference set with these parameters. (We will examine these parameters using multipliers in Chapter 6.) ◇

In Example 2 it was relatively easy find a nonzero solution for the diophantine equation. It is more difficult to show that a diophantine

equation has no solution. We introduce Legendre's Theorem[1] to help us answer the question of existence of solutions. Here the symbol $s\,R\,t$ means that s is a square modulo $|t|$.

Theorem 5.2. *(Legendre's Theorem, 1785) Let a and b be nonzero, square-free*[2] *integers with at least one positive, and let $d = gcd(a, b)$. Then $x^2 = ay^2 + bz^2$ has a nonzero integer solution if and only if the following three conditions are satisfied:*

(i) $a\,R\,b$,

(ii) $b\,R\,a$, *and*

(iii) $-(ab/d^2)\,R\,d$.

Example 3. Consider the parameters $(43, 15, 5)$. If there were a difference set with these parameters, BRC says that the diophantine equation $x^2 = 10y^2 - 5z^2$ must have a nonzero integer solution. We use Legendre's Theorem to check. For this equation, $a = 10$, $b = -5$, and $d = \gcd(a, b) = 5$. We find that $-ab/d^2 = 2$ is not a square mod 5. So this equation does not have a nonzero integer solution. We conclude that there is no symmetric design, and therefore no difference set, with parameters $(43, 15, 5)$. ◇

It is important to pay attention to the hypotheses of Legendre's Theorem. This next example shows that failing to do so leads to a false conclusion.

Example 4. Consider the parameters $(343, 19, 1)$. The equation is $x^2 = 18y^2 - z^2$. This does have the solution $(3, 1, 3)$. If we didn't happen to notice this, we might try to use Legendre's Theorem. We note that $-1 \equiv 17 \pmod{18}$ is not a square. This would seem to indicate that there is no solution. But since 18 is not square-free, the equation does not meet the hypotheses of the theorem. Try substituting $u = 3y$ to get the equation $x^2 = 2u^2 - z^2$. This equation passes Legendre's test. Note that it has the integer solution $(1, 1, 1)$. If we let $y = u/3$ we get the rational solution $(1, 1/3, 1)$ to the original equation. We can multiply this by 3 to clear the denominators and get the integer solution $(3, 1, 3)$. ◇

[1] For a proof see [**32**], Section 17.3.

[2] A *square-free integer* is an integer not divisible by the square of any prime.

The projective planes discussed in Chapter 2 are symmetric designs with parameters $(v, k, \lambda) = (n^2+n+1,\ n+1,\ 1)$. The parameter n is the order of the projective plane. From Theorem 2.15 we know how to construct the coordinatized projective plane $PG(2, q)$ of order q a power of a prime. In our next two examples we use BRC to explore the existence question for projective planes of order n not a power of a prime. Along the way we learn that the converse of BRC does not hold.

Example 5. If there were a projective plane of order $n = 6$, it would be a symmetric design with parameters $(v, k, \lambda) = (43, 7, 1)$. BRC says that if there were such a design, then the diophantine equation $x^2 = 6y^2 - z^2$ must have a nonzero integer solution. Legendre's Theorem states that for there to be a solution, -1 must be a square modulo 6. Since it is not, the diophantine equation has no nonzero solution. Therefore there is no projective plane of order 6. ◇

In the 1980s it was thought that the converse of BRC might be true; that is, if parameters (v, k, λ) satisfy BRC and also $k(k-1) = \lambda(v-1)$, then a symmetric design with those parameters exists. (See Ryser [**61**] and Lander [**43**], p. 44.) But in 1989, Lam proved that there is no projective plane of order 10. (See the expository paper [**42**].) The resulting example shows that the converse of BRC is false.

Example 6. If there were a projective plane with order $n = 10$, it would be a symmetric design with parameters $(n^2+n+1, n+1, 1) = (111, 11, 1)$. It was a long-standing question whether a projective plane of order 10 existed. These parameters do pass the BRC test: $v = 111$ is odd, and the diophantine equation $x^2 = 10y^2 - z^2$ has the nonzero solution $(x, y, z) = (1, 1, 3)$. But since there is no projective plane of order 10, this example serves to show that passing the BRC test is not sufficient to guarantee the existence of a symmetric design. ◇

Exercises

1. Test whether the following sets of parameters meet the necessary condition given in the Bruck-Ryser-Chowla Theorem for the existence of a symmetric design:

(a) $(16, 6, 2)$.

(b) $(67, 12, 2)$. Ⓢ

(c) $(71, 15, 3)$.

(d) $(93, 24, 6)$.

(e) $(51, 25, 12)$.

(f) $(25, 9, 3)$.

2. This exercise is an opportunity for you to put into your own words two simple but fundamental ideas:

(a) Is it possible to have parameters (v, k, λ) pass the BRC test and still have no (v, k, λ)-difference set in a group G of order v? Explain.

(b) Is it possible to have a (v, k, λ)-difference set in a group of order v if the parameters do not pass BRC? Explain.

3. Explore the use of BRC to eliminate possible projective planes of orders n not a prime power (6, 10, 12, 14, 15, 18, 20, ...).

(a) Which planes are eliminated?

(b) Describe any patterns you see.

4. Prove BRC for the case v is even. Ⓗ

5. (Alternative statement of Legendre's Theorem) The following is often given as the statement of Legendre's Theorem. The appeal is that its symmetry may make it easier to remember. Prove that the alternative statement implies Theorem 5.2.

> **Theorem**. Let a, b, and c be nonzero, square-free integers that are pairwise relatively prime and not all of the same sign. Then $ax^2 + by^2 + cz^2 = 0$ has a nonzero solution if and only if the following three conditions are satisfied:
>
> (i) $-ab\,R\,c$,
>
> (ii) $-ac\,R\,b$, and
>
> (iii) $-bc\,R\,a$.

6. Computer exercises:

(a) Write a function that accepts two integer values s and t and tests whether s is a square mod $|t|$.

(b) Write a computer program that accepts integer values for v, k, and λ and tests whether these parameters pass the fundamental identity that $k(k-1) = \lambda(v-1)$ and also pass BRC.

5.2. Proof of BRC for v odd

The proof of the Bruck-Ryser-Chowla Theorem that we present here is from Ryser's paper [**61**]. It will introduce us to classical results in both number theory and linear algebra. In the *Preliminaries* we prove Lagrange's theorem that any positive integer can be written as a sum of four squares. We then turn to linear algebra and define what it means for two square matrices with rational entries to be equivalent over the field of rationals. ($A \cong B$ if there exists an invertible, rational matrix S so that $S^T AS = B$.) We use the four-squares theorem to show that I_4 is equivalent to nI_4, and we use linear algebra to prove basic theorems about equivalence of matrices, including Witt's Cancellation Theorem.

With this background we present *The Main Argument*, showing that if there exists a symmetric (v, k, λ) design then, starting with its $v \times v$ incidence matrix, ultimately two 2×2 matrices involving parameters n and λ are equivalent. From this, we get our nonzero integer solution to the diophantine equation $x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$.

While the details of this proof are not needed later in this text, we include them because the proof illustrates one of our themes: there is power in combining ideas from different parts of mathematics. For a first reading of this section you may wish to skim the Main Argument to get an overview, and then come back to study the Preliminaries.

Preliminaries:

We start with a lemma used in the proof of the four-squares theorem.

Lemma 5.3. *Let p be an odd prime. Then there are integers m, x and y so that $mp = x^2 + y^2 + 1$ with $1 \leq m < p$.*

Proof. Consider the set of values x^2 modulo p for $0 \leq x \leq (p-1)/2$. We claim that no two of these values are equal. Therefore this set contains $(p+1)/2$ different residues. Now consider a second set of all values $-y^2 - 1$ modulo p for $0 \leq y \leq (p-1)/2$. Again, there are $(p+1)/2$ different residues. Since there are only p different residues modulo p, the two sets must share a value. Choose an x and y for which $x^2 \equiv -y^2 - 1 \pmod{p}$. Then $x^2 + y^2 + 1 \equiv 0 \pmod{p}$, so $x^2 + y^2 + 1 = mp$ for some positive integer m. Further, since $0 \leq x, y \leq (p-1)/2$, we have

$$x^2 + y^2 + 1 \quad = \quad mp \quad \leq \quad \frac{(p-1)^2}{4} + \frac{(p-1)^2}{4} + 1 \quad < \quad p^2.$$

We conclude that $mp = x^2 + y^2 + 1$ with $1 \leq m < p$. □

Theorem 5.4. *(Lagrange, 1770) Every positive integer can be written as the sum of four squares of integers.*

Proof. If two integers can each be written as sums of four squares, then so can their product. (See Exercise 8.) So it is enough to prove the result for every prime.

For the prime $p = 2$ we have $2 = 1^2 + 1^2 + 0^2 + 0^2$. Now assume p is an odd prime. By Lemma 5.3 there is an integer m with $1 \leq m < p$ so that $mp = x^2 + y^2 + 1$. This specific form shows that we can express mp as the sum of four squares:

$$mp = a^2 + b^2 + c^2 + d^2, \quad \text{with } 1 \leq m < p. \tag{1}$$

We choose m to be the smallest integer so that mp is the sum of four squares, and we show that $m = 1$.[3] Assume that $m > 1$, and choose integers A, B, C, D so that $a \equiv A,\ b \equiv B,\ c \equiv C,\ d \equiv D \pmod{m}$, and $-m/2 < A, B, C, D \leq m/2$. Then $A^2 + B^2 + C^2 + D^2 \equiv 0 \pmod{m}$. So there is an integer $r \geq 0$ so that

$$rm = A^2 + B^2 + C^2 + D^2. \tag{2}$$

[3]Here we phrase the argument as a proof by contradiction. In Exercise 9 we explore a slightly different constructive argument.

Also $0 \leq A^2 + B^2 + C^2 + D^2 \leq 4(\frac{m}{2})^2 = m^2$, so $0 \leq r \leq m$. We claim that $0 < r < m$. If $r = 0$, then each of A, B, C, D is 0. But this means that m divides each of a, b, c, d, so m^2 divides $a^2 + b^2 + c^2 + d^2 = mp$, and m divides p. Since p is prime and $1 < m < p$, this is a contradiction.

At the other extreme, if $r = m$, then each of A, B, C, D would equal $m/2$. This in turn would force each of a, b, c, d to be an odd multiple of $m/2$, so that m^2 would divide $a^2 + b^2 + c^2 + d^2$. Again, this is a contradiction.

We now multiply Equations (1) and (2) to get

$$(mp)(rm) \quad = \quad (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2). \qquad (3)$$

By Exercise 8 we can write the right-hand side as a sum of four squares:

$$\begin{aligned} rpm^2 \quad = \quad & (aA + bB + cC + dD)^2 + (aB - bA + cD - dC)^2 \qquad (4) \\ & + (aC - bD - cA + dB)^2 + (aD + bC - cB - dA)^2. \end{aligned}$$

Each of the four expressions in parentheses is congruent to 0 modulo m, so each term on the right side of Equation (4) has the form $(u_j m)^2$ for some integer u_j. (See Exercise 10.) Dividing both sides of Equation (4) by m^2 leaves rp as a sum of four squares for $0 < r < m$. However, this is a contradiction since m was chosen as the smallest integer multiple of p expressible as a sum of four squares. Therefore $m = 1$ and we can express $1 \cdot p = p$ as a sum of four squares. □

We now look at our definition of equivalence of matrices and some basic facts about equivalence. This concept of equivalence comes from the study of quadratic forms. While we do not use the language of quadratic forms, many proofs of BRC couch their arguments more explicitly in this language.

Definition. Let A and B be square matrices of the same size with entries in the field $\mathbb{K}$. Then A is equivalent over $\mathbb{K}$ to B if there exists an invertible matrix S with entries in $\mathbb{K}$ so that $S^T AS = B$. We say that S transforms A into B.

This is indeed an equivalence relation. We note that if $\det(B)$ is nonzero then S is necessarily invertible.

Since our aim is to prove the existence of an integer solution to a diophantine equation, from this point in this section we assume that $\mathbb{K} = \mathbb{Q}$ and use the notation $A \cong B$ to mean that A and B are equivalent over the rational numbers. First we use Lagrange's four-squares theorem to prove that $I_4 \cong nI_4$ for n a positive integer.

Theorem 5.5. *Let n be a positive integer. Then*

$$diag(n,n,n,n) \cong diag(1,1,1,1) = I_4.$$

Proof. To prove this we exhibit a matrix S that transforms I_4 into nI_4. Using the four-squares theorem we write n as the sum of four integers squared: $n = a^2+b^2+c^2+d^2$. We use these integers to form the matrix:

$$S = \begin{bmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{bmatrix}.$$

Then $S^T I_4 S = nI_4$. Note that S is invertible and that the entries of S are integers, so certainly they are in $\mathbb{Q}$. □

To continue our proof of BRC, we need these basic facts about the equivalence of matrices. Proofs of the lemmas are left to the exercises.

Lemma 5.6. *Let A be a $v \times v$ matrix, and let B be matrix A but with row i switched with row j and column i switched with column j, for some $i \neq j$. Then $A \cong B$.*

Lemma 5.7. *Let A be a $v \times v$ matrix, and let $c \in \mathbb{Q}$. Let B be the matrix A but with $c \times$ row i added to row j and $c \times$ column i added to column j for some $i \neq j$. Then $A \cong B$.*

Lemma 5.8. *Any symmetric matrix with rational entries is equivalent over the rationals to a diagonal matrix.*

Lemma 5.9. *Let A, B, and C be square matrices, with A and B the same size.*

$$\text{If } A \cong B \quad \text{then } \begin{bmatrix} C & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} C & 0 \\ 0 & B \end{bmatrix},$$

where we write 0 *for the zero matrix of the appropriate size.*

The following theorem is a partial converse of Lemma 5.9. It is trickier to prove. Our proof comes from Jones [**34**].

Theorem 5.10. *(Witt's Cancellation Theorem, 1937) Let A and B be invertible $m \times m$ matrices, and $c \in \mathbb{Q}$.*

$$\text{If } \begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} c & 0 \\ 0 & B \end{bmatrix} \quad \text{then } A \cong B.$$

Proof. We assume that the $(m+1) \times (m+1)$ matrices are equivalent and find a rational matrix S that transforms A into B. Since we assume A and B are invertible, such an S must be invertible.

Given that $\begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} c & 0 \\ 0 & B \end{bmatrix}$ there exists a $W = \begin{bmatrix} t & \mathbf{u}^T \\ \mathbf{v} & M \end{bmatrix}$ so that

$$W^T \begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} W = \begin{bmatrix} t & \mathbf{v}^T \\ \mathbf{u} & M^T \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & A \end{bmatrix} \begin{bmatrix} t & \mathbf{u}^T \\ \mathbf{v} & M \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & B \end{bmatrix}.$$

Multiplying these matrices and equating corresponding blocks gives:

$$\begin{aligned} t^2c + \mathbf{v}^T A\mathbf{v} &= c, \\ tc\mathbf{u}^T + \mathbf{v}^T AM &= 0, \\ tc\mathbf{u} + M^T A\mathbf{v} &= 0, \\ c\mathbf{u}\mathbf{u}^T + M^T AM &= B. \end{aligned} \tag{5}$$

Next choose the sign in the expression $t \pm 1$ so that it is not zero, and let $d = 1/(t \pm 1)$. Let matrix $S = M - d\mathbf{v}\mathbf{u}^T$. We claim that $S^T AS = B$.

First we calculate

$$\begin{aligned} S^T AS &= \left(M^T - d\mathbf{u}\mathbf{v}^T\right) A \left(M - d\mathbf{v}\mathbf{u}^T\right) \\ &= M^T AM - dM^T A\mathbf{v}\mathbf{u}^T - d\mathbf{u}\mathbf{v}^T AM + d^2\mathbf{u}\mathbf{v}^T A\mathbf{v}\mathbf{u}^T. \end{aligned}$$

Using the equations in (5) above we substitute to get:

$$\begin{aligned} S^T AS &= M^T AM + cdt\mathbf{u}\mathbf{u}^T + cdt\mathbf{u}\mathbf{u}^T - d^2c\mathbf{u}(t^2-1)\mathbf{u}^T \\ &= M^T AM + cd\big(2t - d(t^2-1)\big)\mathbf{u}\mathbf{u}^T \\ &= M^T AM + c\mathbf{u}\mathbf{u}^T \\ &= B. \end{aligned}$$

Therefore $A \cong B$. □

The Main Argument:

We are now ready to present Ryser's proof [**61**] of BRC for v odd: If $\mathcal{D}$ is a symmetric (v, k, λ) design with v odd, then the diophantine equation

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a nonzero solution (x, y, z) in integers.

Proof. Assume that a symmetric (v, k, λ) design exists, and that N is the $v \times v$ incidence matrix for this design. Then $N^T N = nI + \lambda J$. By Exercise 12 we can assume that $\lambda > 0$. We define the following $(v+1) \times (v+1)$ matrices

$$A = \begin{bmatrix} & & & 1 \\ & N & & \vdots \\ & & & 1 \\ 1 & \dots & 1 & k/\lambda \end{bmatrix}$$

$$D = \operatorname{diag}[1, \dots, 1, -\lambda], \quad E = \operatorname{diag}[n, \dots, n, -n/\lambda].$$

Then $A^T D A = E$. Since D and E are invertible, it follows that $D \cong E$. (See Exercise 17.)

Case 1: Assume that $v \equiv 1 \pmod 4$, so $(v-1)/2$ is even. Then repeatedly using Theorem 5.5 to replace $v-1$ of the ns in E with 1s, we have that E is equivalent to the diagonal matrix $\operatorname{diag}[1, \dots 1, n, -n/\lambda]$. Since the matrices involved are diagonal and easily seen to be invertible, we can use Witt's cancellation theorem to cancel the $v-1$ 1s that D and this new matrix have in common. We get:

$$\begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} \cong \begin{bmatrix} n & 0 \\ 0 & -n/\lambda \end{bmatrix}.$$

Let $M = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ be the matrix that transforms the first into the second. So

$$M^T \begin{bmatrix} 1 & 0 \\ 0 & -\lambda \end{bmatrix} M = \begin{bmatrix} n & 0 \\ 0 & -n/\lambda \end{bmatrix}.$$

Equating the (1,1) entries gives $a^2 - b^2\lambda = n$. Rearranging this equation to $a^2 = n + \lambda b^2$ reveals a nontrivial rational solution to the diophantine equation with $(x, y, z) = (a, 1, b)$. If necessary, multiply this triple by an integer to get an integer solution.

Case 2: Assume that $v \equiv 3 \pmod 4$, so $(v-1)/2$ is odd. Again we start with $D \cong E$. Using Lemma 5.9 and then Lemma 5.6, we insert an n into each and shift this n to position $(v-1)$ to get $(v+2)\times(v+2)$ matrices:

$$\text{diag}[1, \ldots, 1, n, -\lambda] \quad \cong \quad \text{diag}[n, \ldots, n, n, -n/\lambda].$$

Then using Theorem 5.5 we change $v+1$ of the ns in the second matrix to 1s:

$$\text{diag}[1, \ldots, 1, n, -\lambda] \quad \cong \quad \text{diag}[1, \ldots, 1, 1, -n/\lambda].$$

Finally we use Witt's cancellation theorem to get:

$$\begin{bmatrix} n & 0 \\ 0 & -\lambda \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & -n/\lambda \end{bmatrix}.$$

Again the equivalence of these 2×2 matrices gives us an equality; in this case $a^2 n - b^2\lambda = 1$. Rearranging this equation to $1^2 = na^2 - \lambda b^2$ shows a rational solution to the diophantine equation with $(x, y, z) = (1, a, b)$. Clear any denominators to get an integer solution. □

Exercises

7. Verify the claim in the proof of Lemma 5.3 that if $0 \le a < b \le (p-1)/2$ then $a^2 \not\equiv b^2 \pmod p$.

8. Prove that the product of two sums of four squares is equal to a sum of four squares by showing that:

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + u^2) \; = \\ (ar + bs + ct + du)^2 \; + \; (as - br + cu - dt)^2 \; + \\ (at - bu - cr + ds)^2 \; + \; (au + bt - cs - dr)^2.\end{aligned}$$

9. In this section we used Lagrange's theorem simply to establish that each positive integer *can* be written as the sum of four squares. So

a proof by contradiction was satisfactory for our purpose. If instead we needed to actually express an integer as a sum of four squares, we would prefer a constructive proof. This exercise provides one. Start with $mp = a^2 + b^2 + c^2 + d^2$. If $m = 1$ we are done. If not, use the algorithm in the proof to calculate r. We now have $1 \leq r < m$, with rp the sum of four squares. If $r = 1$, we are done. If not, substitute r for m and repeat the algorithm. This process is known as "descent."

(a) Why is this process guaranteed to stop?

(b) Start with $p = 11$, $m = 9$ and $99 = 3^2 + 4^2 + 5^2 + 7^2$. Note that $m < p$ as required by the algorithm. Iterate the algorithm until it gives $p = 11$ as a sum of four squares.

10. Show that the expressions in parentheses in Equation (4) are each congruent to 0 modulo m. Thus dividing the right hand side by m^2 leaves a sum of four squares of integers. Ⓢ

11. Prove that the relation of square matrices being equivalent over a field $\mathbb{K}$ is an equivalence relation.

12. Recall that we allow $\lambda = 0$ for a trivial symmetric design. Prove Theorem 5.1 for the case v is odd and $\lambda = 0$.

13. Prove Lemma 5.6.

14. Prove Lemma 5.7.

15. Prove Lemma 5.8. Ⓗ

16. Prove Lemma 5.9.

17. Confirm that $A^T DA = E$ in the proof of BRC.

18. Extending Witt's Cancellation Theorem. Prove that if A and B are invertible $m \times m$ matrices, and C is a symmetric matrix, all with entries in a field $\mathbb{Q}$, and

$$\text{if } \begin{bmatrix} C & 0 \\ 0 & A \end{bmatrix} \cong \begin{bmatrix} C & 0 \\ 0 & B \end{bmatrix}, \text{ then } A \cong B. \qquad \text{Ⓗ}$$

5.3. Partial converse and extension of BRC

It turns out that a partial converse to BRC is true. While the conditions do not guarantee the existence of a design, they do guarantee the existence of a matrix with some of the same properties as that of an incidence matrix of a design, though the entries need not be 0s and 1s. (See [**8**], p. 96.)

Theorem 5.11. *If parameters (v, k, λ) obey the equation $k(k-1) = \lambda(v-1)$ and if*

(i) for v even, n is a square,

(ii) for v odd, the equation $x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$ has a solution in integers x, y, z not all zero,

then there exists a rational matrix A with $A^TA = nI + \lambda J$.

Work extending BRC has been used to eliminate other triples as parameters of difference sets. Here we state (without proof) one of these extensions for cyclic groups and present an example where it proves useful.

Theorem 5.12. *(Hall and Ryser* [**29**]*) If there is a nontrivial (v, k, λ) cyclic difference set for odd v, then for every divisor w of v, the equation $x^2 = ny^2 + (-1)^{(w-1)/2}wz^2$ has a solution in integers, not all 0.*

Example 7. The parameters $(39, 19, 9)$ pass the BRC test, but by the extension given in Theorem 5.12 there is no *cyclic* difference set with these parameters. (Since there is a non-abelian group of order 39, this theorem does not rule out a $(39, 19, 9)$-difference set in that group.) ◇

In his survey of cyclic difference sets for $k \leq 50$, Hall [**27**] reported that 268 sets of parameters passed the initial test that $k(k-1) = \lambda(v-1)$. Of these, 101 failed the BRC test, leaving 167 possible. By the time Hall published his paper, difference sets had been found in 46 cases, and other methods had been used to rule out difference sets in 109 cases; twelve cases remained. Later Baumert [**5**] reported that all twelve cases had been settled in the negative. In the following

chapters we will explore other necessary conditions for the existence of difference sets.

Exercises

19. Verify that in Example 7 the parameters pass the BRC test, but fail the test in Theorem 5.12.

Coda

The centuries-long quest for a proof of Fermat's Last Theorem reminds us that proving non-existence is often very hard. The Bruck-Ryser-Chowla Theorem (BRC) can tell us when a (v, k, λ) design does not exist and thus when a (v, k, λ)-difference set does not exist.

The proof of BRC uses the incidence matrix N of the design. For v even, we only need the determinant of $N^T N$. For v odd, the argument is more intricate. Many proofs explicitly require background knowledge of quadratic forms. We have chosen a more elementary approach that uses matrix algebra. Even if you did not follow all the details of this long argument, you should work to appreciate the source of this surprising number-theoretic condition required for the existence of a symmetric design.

Chapter 6

Multipliers

A multiplier for difference set $D \subseteq G$ is an automorphism of G that maps D to a translate of D. Hall [**26**] introduced the concept of multipliers in cyclic difference sets. Since then multipliers have been studied and theorems proved for abelian difference sets and, to some extent, for non-abelian difference sets. For the latter much less is known. For abelian difference sets, multipliers have proved an important tool for showing difference sets in certain groups cannot exist. Unlike the BRC, multipliers also provide an important tool for finding difference sets when they do exist, and for answering questions of equivalence of difference sets.

Section 1 introduces multipliers. In Section 2 we look at theorems that guarantee the existence of numerical multipliers. Section 3 shows that there must be a difference set that is fixed by a multiplier. This is a key to the use of multipliers for finding difference sets. In Sections 4 and 5 we look at specific examples of the use of multipliers.

6.1. Definition and examples

We begin with a discussion of certain automorphisms of abelian groups. Let G be an abelian group of order v written additively, and let t be a positive integer relatively prime to v. Then ϕ_t is an automorphism

of G where

$$\phi_t : a \mapsto ta.$$

We learned in Chapter 4 that if D is a difference set in G, then its image under any automorphism is also a difference set. What is interesting is that sometimes ϕ_t maps the difference set to itself, or at least to a shift of itself. For instance, in $\mathbb{Z}_{13}$ the set $D = \{0, 1, 3, 9\}$ is a difference set, and $\phi_3(D) = \{0, 3, 9, 1\} = D$. We may think of the automorphism ϕ_t as a permutation of the group elements. It is then clear that if $\phi_t(D) = D$, then D must be the union of one or more orbits[1] of ϕ_t. It is this fact that we use both to find difference sets in some abelian groups, and to prove that other groups cannot contain difference sets with particular parameters.

While the automorphisms ϕ_t motivate the term "multiplier," a multiplier for a difference set is any automorphism of the group that maps the difference set to a shift of itself.

In Chapter 4 with the introduction of the integral group ring, we found it helpful to use multiplication for the general group operation and to reserve the plus sign for addition within the integral group ring. So from this point we use multiplication for the group operation unless a particular group (e.g., $\mathbb{Z}_m$) is an additive group. For multiplicative groups, the automorphism ϕ_t is defined:

$$\phi_t : a \mapsto a^t.$$

As a consequence, in multiplicative notation

$$\phi_t(D) = D^{(t)} = \{d^t \mid d \in D\}.$$

Also, a "left shift" of D by the element g is gD.

Definition. Let D be a difference set in G. Then an automorphism α of G is called a multiplier for D if α maps D to aDb for some elements $a, b \in G$. If $b = 1$ so that $\alpha(D) = aD$, then α is a left multiplier.

Note that if G is abelian, then any multiplier is a left multiplier. Multipliers of the form ϕ_t are most helpful in our study, and are given a special name.

[1] By an orbit of ϕ_t we mean an orbit of the group $\langle \phi_t \rangle$ acting on G.

Definition. Let G be an abelian group, t an integer relatively prime to the order of G, and D a difference set in G. Then ϕ_t is a numerical multiplier if for some $h \in G$, $\phi_t(D) = hD$. It is common practice to abuse terminology and call the integer t itself a numerical multiplier.

Since any automorphism of a cyclic group is of the form ϕ_t for some t relatively prime to the order of the group, a multiplier for a cyclic difference set is necessarily a numerical multiplier. Let us look at some examples of multipliers in abelian groups.

Example 1. Let $G = \mathbb{Z}_{13}$ and let $D = \{2, 3, 5, 11\}$. Then ϕ_3 is a numerical multiplier for D since $\phi_3(D) = 3D = \{6, 9, 2, 7\}$, which is $4 + D$. ◇

It may be instructive to consider this "same" difference set in the cyclic group of order 13 written multiplicatively.

Example 2. Let $G = \langle a \mid a^{13} = 1\rangle$ and let $D = \{a^2, a^3, a^5, a^{11}\}$. Then ϕ_3 is a numerical multiplier for D since $\phi_3(D) = D^{(3)} = \{a^6, a^9, a^2, a^7\} = a^4 D$. ◇

Example 3. Let p be a prime, $p \equiv 3 \pmod 4$, $G = \mathbb{Z}_p$, and D be the set of quadratic residues mod p. We know from Theorem 4.3 that D is a difference set in G. Since D is a subgroup of the multiplicative group ${\mathbb{Z}_p}^*$, each element of D is a multiplier of D that fixes D. ◇

Example 4. Let $G = \langle a, b, c, d \mid a^2 = b^2 = c^2 = d^2 = 1\rangle$, an elementary abelian 2-group, and let $D = \{1, a, b, c, d, abcd\}$. Consider the two automorphisms defined by their action on the generators:

$$\alpha : a \mapsto b \mapsto c \mapsto d \mapsto a$$

$$\beta : a \mapsto abcd, \quad b \mapsto bcd, \quad c \mapsto acd, \quad d \mapsto abd.$$

Note that α maps D to itself, and β maps D to a shift of D, namely $abcdD$. So both automorphisms are (left) multipliers for D, though neither is a numerical multiplier. ◇

With the terminology established, we repeat the outline of this chapter. In Section 2 we introduce the Multiplier Theorems that guarantee the existence of certain numerical multipliers. In Section

3 we show that left multipliers act as automorphisms of the design dev$D$. This leads to theorems that guarantee that certain multipliers fix a difference set. In Section 4 we apply what we have learned to construct difference sets in some groups and to show in others that no nontrivial difference set can exist. Section 5 explores how multipliers can be used in abelian, non-cyclic groups.

Exercises

1. Show that each of these sets of multipliers for a difference set D in a group G is a subgroup of the group of all automorphisms of G.

(a) The set of left multipliers.

(b) The set of numerical multipliers.

2. In $G = \mathbb{Z}_{21}$, the set $D = \{1, 4, 5, 10, 12\}$ is a difference set. Which of the following are numerical multipliers for D? Explain.

(a) ϕ_2. Ⓢ

(b) ϕ_3. Ⓢ

(c) ϕ_4.

(d) ϕ_5.

3. Refer to Exercise 4.9 on page 52.

(a) Show that ϕ_2 is a multiplier for D.

(b) Show that $D'^{(2)} = D'$.

(c) Why is ϕ_2 not a multiplier for D'?

4. Refer to Example 4.

(a) Verify that $\beta(D) = abcdD$.

(b) Since multipliers form a group, β^2 must also be a multiplier for D. Find a group element g so that $\beta^2(D) = gD$. (Careful: g is not $(abcd)^2$.)

6.2. Existence of numerical multipliers

The First Multiplier Theorem guarantees the existence of numerical multipliers for certain abelian difference sets. We state it here without proof.[2]

Theorem 6.1. *(First Multiplier Theorem) Let D be an abelian difference set with parameters (v, k, λ), and let p be a prime that divides n but does not divide v. If $p > \lambda$, then p is a numerical multiplier of D.*

Example 5. In $\mathbb{Z}_{21}$ the set $D = \{1, 3, 13, 16, 17\}$ is a difference set with parameters $(21, 5, 1)$. Then $p = 2$ is a numerical multiplier. $\diamond$

Example 6. Let $G = \mathbb{Z}_{37}$. The parameters $(37, 9, 2)$ pass the test that $k(k-1) = \lambda(v-1)$. Theorem 4.4 gives us the difference set of nonzero fourth powers, and the multiplier theorem guarantees that $t = 7$ is a numerical multiplier for this difference set. $\diamond$

Though the condition that $p > \lambda$ is used in the proof of the First Multiplier Theorem, Jungnickel [**35**] reports that for all known difference sets this condition is not necessary. This leads to the long-standing conjecture:

Conjecture: (Multiplier conjecture) Theorem 6.1 holds without the assumption that $p > \lambda$.

Jungnickel further states that since the First Multiplier Theorem there have been attempts to extend this result to circumvent the suspect condition. The next theorem is one such extension. It was proved by Hall [**26**] for the cyclic case and later proved for all abelian groups.[3]

Theorem 6.2. *(Second Multiplier Theorem). Let D be an abelian (v, k, λ)-difference set in G, and let $m > \lambda$ be a divisor of n which is co-prime with v. Moreover, let t be an integer co-prime with v satisfying the following condition: For every prime p dividing m there exists a non-negative integer f with $t \equiv p^f \pmod{v^*}$, where v^* denotes the exponent of G. Then t is a numerical multiplier for D.*

[2] For a proof of Theorem 6.1 see [**35**], p. 252 in [**19**].
[3] For a proof of Theorem 6.2 see [**8**], pp. 323–326.

The following corollary makes this theorem easy to apply when n is a power of a prime.

Corollary 6.3. [**35**] *Let D be an abelian (v, k, λ)-difference set and assume that $n = k - \lambda$ is a power of a prime p, with $gcd(p, v) = 1$. Then p is a numerical multiplier for D.*

Example 7. Theorem 4.6 shows how to construct a difference set in $\mathbb{Z}_{35}$ with parameters $(35, 17, 8)$ using twin primes. Corollary 6.3 guarantees that $p = 3$ is a numerical multiplier for the difference set. In Exercise 15 we will use this multiplier to find whether there are other inequivalent difference sets in $\mathbb{Z}_{35}$. $\diamond$

We end this section with a short discussion of the mapping ϕ_{-1} that takes a to a^{-1}, and conditions under which this might be a multiplier for a difference set.

First we note that if G is a non-abelian group, then this mapping is not a homomorphism and so cannot be a multiplier. At the other extreme, the least complicated of groups—the cyclic groups—have no nontrivial difference sets with -1 as a multiplier.[4] Even in non-cyclic abelian groups, difference sets with -1 as a multiplier are quite rare.

On the other hand, Lander ([**43**], p. 153) tells us that ϕ_{-1} "plays a special role in ... nonexistence theorems" for difference sets. So while difference sets with multiplier -1 are rare, it is important to study the mapping ϕ_{-1}.

A difference set that admits -1 as a multiplier is called reversible.[5] The $(36, 15, 6)$-difference set in the group $\mathbb{Z}_6 \oplus \mathbb{Z}_6$ in Example 4.4 on page 48 is reversible. In Chapter 8 we will study the construction of McFarland difference sets and will see a reversible $(4000, 775, 150)$-difference set.

Here are two interesting facts about difference sets with multiplier -1. We will look at a proof of the first of these in Exercise 11 in the next section.

[4] A very readable proof is in ([**5**], p. 60) where Baumert writes, "This fact was known for several years prior to any publication of its proof. This accounts for the anomaly that it is often referred to in publications which predate the papers [Johnsen (1964), Brualdi (1965) and Yates (1967)] containing proofs."

[5] Some authors reserve the term reversible for a difference set D that is fixed by multiplier -1.

Theorem 6.4. *([43], p. 154) Let D be a nontrivial (v, k, λ)-difference set in an abelian group G. If -1 is a multiplier of D, then v is even.*

Theorem 6.5. *([43], p. 158) Let D be a nontrivial (v, k, λ)-difference set in an abelian group G. If -1 is a multiplier of D, then so is every integer t relatively prime to v. Moreover, if D happens to be fixed by the multiplier -1, then D is fixed by every numerical multiplier.*

Exercises

5. In Example 5, $p = 2$ is a multiplier for D. Find the element g so that $2D = g + D$.

6. Let D be the $(37, 9, 2)$-difference set determined in Exercise 4.13. We know that 7 is a multiplier for D. Find the element g so that $7D = g + D$.

7. Find numerical multipliers other than 1 for these difference sets, and justify your answers.

(a) $D = \{1, 5, 11, 24, 25, 27\}$ in $\mathbb{Z}_{31}$. Ⓢ

(b) The twin primes difference set in $\mathbb{Z}_{15}$.

(c) The set D of quadratic residues in $\mathbb{Z}_{19}$.

(d) The set D of quadratic residues in $\mathbb{Z}_{23}$.

8. Deduce Corollary 6.3 from Theorem 6.2 by establishing the following:

(a) Suppose α is a multiplier of the abelian difference set D. Show that α is also a multiplier of the complementary difference set $\overline{D}$.

(b) Explain why the result of (a) tells us that in the proof of Corollary 6.3 we may assume $k \leq v/2$.

(c) Apply Theorem 6.2 with $n = m$ to show that the prime p in Corollary 6.3 is a numerical multiplier for D. Ⓗ

6.3. Multipliers fix sD

We seek to show that any left multiplier must fix a difference set. For an automorphism α to qualify as a left multiplier of D it need not fix D, but it must map D to one of the blocks in the design dev$D$. We will study this design to find a difference set fixed by α.

Recall that the development of D, dev$D$, is a symmetric design with $\mathcal{P} = G$ and $\mathcal{B} = \{gD \mid g \in G\}$. Our next theorem states that a left multiplier of D is an automorphism of dev$D$.

Theorem 6.6. *Let G be a group containing a difference set D, and let α be a left multiplier for D. Then α is an automorphism of dev$D$.*

Proof. Since α acts as an automorphism of the group G, it is a one-to-one mapping of points to points. First we claim that α maps blocks to blocks. Since α is a multiplier for D, $\alpha(D)$ is a shift of D. Say $\alpha(D) = hD$. Now consider a general block of the design: gD. Then $\alpha(gD) = \alpha(g)\alpha(D) = (\alpha(g)h)D$, which is a shift of D and so is a block in dev$D$. It follows that α is a 1-to-1 mapping on the set of blocks. Therefore α acting on dev$D$ is an automorphism of the design. □

Having established that a left multiplier is an automorphism of the design dev$D$, we now invoke Theorem 3.5 to prove that every left multiplier must fix at least one difference set.

Theorem 6.7. *Let G be a group containing a difference set D, and let α be a left multiplier for D. Then α fixes at least one of the blocks in dev$D$.*

Proof. By Theorem 6.6, the left multiplier α acts as an automorphism of the design dev$D$. Since α is an automorphism of G, it must map the identity of G to itself. Therefore, as an automorphism of the design, α fixes at least one point. Now Theorem 3.5 says that α fixes equal numbers of points and blocks of the design. Therefore α fixes at least one block of dev$D$. □

In the special case that G is abelian and $\gcd(v, k) = 1$, McFarland and Mann [**53**] proved a stronger result.

Theorem 6.8. *Let G be an abelian group and let D be a (v, k, λ)-difference set in G. If $gcd(v, k) = 1$, then there is an element $b \in G$ so that the difference set bD is fixed by every multiplier of D.*

Proof. Let $D = \{d_1, d_2, \ldots, d_k\}$. Note that $\phi_k : g \mapsto g^k$ is an automorphism of G. So there is exactly one $b \in G$ so that

$$b^k\Big(\prod_{d_i \in D} d_i\Big) = 1.$$

In words, b^k is the inverse of the group element that is the product of the elements in D. For any multiplier α, $\alpha(bD) = cD$ for some $c \in G$. We will show $b = c$, and thus the multiplier α fixes the block bD.

$$1 = \alpha\Big(b^k \prod_{d_i \in D} d_i\Big) = \alpha\Big(\prod_{d_i \in D} bd_i\Big) = \alpha\Big(\prod_{g_i \in bD} g_i\Big)$$

$$= \prod_{h_i \in cD} h_i = \prod_{d_i \in D} cd_i = c^k \prod_{d_i \in D} d_i.$$

We conclude that c^k is the inverse of the group element that is the product of the elements in D. Therefore $b^k = c^k$, and so $b = c$. □

The next two theorems cover other cases and are presented here without proof. If G is an abelian group that contains a difference set, and v and k are not necessarily relatively prime, the following theorem by McFarland and Rice [**54**] guarantees the existence of a difference set fixed by all *numerical* multipliers.

Theorem 6.9. [**54**] *If G is an abelian group that contains a difference set D, then there is a translate of D that is fixed by all of its numerical multipliers.*

The following theorem is not restricted to numerical multipliers, but does have a condition restricting v. It also does not require that G be abelian, so may be of interest in the search for non-abelian difference sets.

Theorem 6.10. *([**35**], p. 248, credited to Lander.) Let D be a (v, k, λ)-difference set in G, let M be a group of multipliers of D, and assume that $gcd(|M|, v) = 1$. Then there exists a translate of D that is fixed by every multiplier in M.*

This next example concerns multipliers that are not numerical multipliers. It serves as a warning for us to carefully read the hypotheses of the theorems in this section.

Example 8. Let $G = \langle a, b, c, d \mid a^2 = b^2 = c^2 = d^2 = 1 \rangle$ and let α and β be the multipliers defined in Example 4. In Exercise 9 you will show that the automorphism group generated by α and β acts transitively on the non-identity elements of G. This means that no translate of D can be fixed by both α and β. $\diamond$

The following theorem gives insight into the interaction of multipliers of a difference set in an abelian group. The proof is quite short and involves showing that ϕ_t and σ commute.

Theorem 6.11. [**53**] *Let G be an abelian group with difference set D. If ϕ_t is a numerical multiplier for D and σ is any multiplier for D, then σ permutes the blocks in devD that are fixed by ϕ_t.*

Exercises

9. Refer to Example 8 and prove that the group of multipliers generated by α and β acts transitively on the non-identity elements of G.

10. Explain why Example 8 does not provide a counterexample to Theorems 6.8 and 6.9.

11. Use Exercise 4.35 and Theorem 6.7 to show that if a nontrivial abelian (v, k, λ)-difference set D has multiplier -1 then v is even. (This is a result in [**52**].)

12. Prove Theorem 6.11.

6.4. Using multipliers

The following fact may be obvious at this point. We state it as a theorem so that it will not be overlooked, and so that we may easily refer to it.

Theorem 6.12. *Let G be a group and let α be a multiplier of a difference set D so that $\alpha(D) = D$. Then D consists of a union of orbits for α as a permutation of elements of G.*

In the following example we use this simple fact to find a difference set.

Example 9. Let $G = \mathbb{Z}_{15}$. We wish to find a nontrivial difference set D in G. With $v = 15$, we discover the only choices for k and λ with $1 < k < v/2$ and $k(k-1) = \lambda(v-1)$ are $(v, k, \lambda) = (15, 7, 3)$. Assume such a difference set exists. Since $n = 4 = 2^2$ and $\gcd(2, 15) = 1$, Corollary 6.3 says that 2 is a numerical multiplier for D. Theorem 6.7 allows us to choose D to be a difference set fixed by multiplication by 2. The orbits[6] for ϕ_2 acting on G are:

$$\begin{array}{lll} (0) & (5, 10) & \\ (1, 2, 4, 8) & (3, 6, 12, 9) & (7, 14, 13, 11). \end{array}$$

Since D must have seven elements and must be the union of some of these orbits, it must contain 0, 5, 10, and the elements of one of the 4-cycles. It turns out that $D = \{0, 5, 10, 1, 2, 4, 8\}$ is indeed a difference set. (This is the twin primes difference set of Example 4.3.) ◇

Next we consider an example where parameters pass the BRC test, but where multipliers show that no difference set exists.

Example 10. We wish to show that there is no $(79, 13, 2)$-difference set.[7] Since 79 is prime, G must be $\mathbb{Z}_{79}$. These parameters do satisfy the basic equation and pass the BRC test. Theorem 6.1 tells us that 11 is a numerical multiplier for any difference set with these parameters. So we seek a difference set that is fixed by ϕ_{11}.

The orbits for ϕ_{11} are (0) and two orbits each of length 39. Since no orbits can be combined to get a set of size 13, there is no fixed difference set with these parameters, and therefore no difference set of size 13 in $\mathbb{Z}_{79}$. ◇

Finally we look at an example in which we can find all the equivalence classes of difference sets using multipliers.

[6] Strictly speaking we write the cycle decomposition of ϕ_t. The orbits are the subsets of elements that are in these cycles.

[7] According to Lander [**43**] there is a symmetric design with these parameters.

Example 11. We wish to find all the difference sets, up to equivalence, in the cyclic group $\mathbb{Z}_{73}$. The only parameters with $1 < k < v/2$ that satisfy the basic equation are $(73, 9, 1)$. Since 2 is a numerical multiplier, we seek difference sets fixed by ϕ_2.

The orbits for ϕ_2 are:

(0)

$(1, 2, 4, 8, 16, 32, 64, 55, 37)$ $\quad$ $(9, 18, 36, 72, 71, 69, 65, 57, 41)$

$(5, 10, 20, 40, 7, 14, 28, 56, 39)$ $\quad$ $(17, 34, 68, 63, 53, 33, 66, 59, 45)$

$(25, 50, 27, 54, 35, 70, 67, 61, 49)$ $\quad$ $(3, 6, 12, 24, 48, 23, 46, 19, 38)$

$(13, 26, 52, 31, 62, 51, 29, 58, 43)$ $\quad$ $(11, 22, 44, 15, 30, 60, 47, 21, 42)$

Any difference set fixed by ϕ_2 must be the elements in one of the orbits of size 9. The set $\{1, 2, 4, 8, 16, 32, 64, 55, 37\}$ is the set of nonzero eighth powers (octic residues), and is a difference set. The other orbits are images of the first under automorphisms (multiplication by powers of 5), so all are equivalent difference sets. Since every difference set must be equivalent to one of these fixed difference sets, there is only one $(73, 9, 1)$-difference set up to equivalence. $\diamond$

Exercises

13. Use multipliers to find a nontrivial difference set in $\mathbb{Z}_{11}$, or to show that none exists. Ⓢ

14. Refer to Example 9. Do any of the other 4-cycles combine with $\{0, 5, 10\}$ to form a difference set? If so, are they images of each other under group automorphisms? Or shifts? Are they equivalent difference sets?

15. The twin prime difference set in $\mathbb{Z}_{35}$ has parameters $(35, 17, 8)$. Use multipliers to see if this difference set is the only one in $\mathbb{Z}_{35}$ with $k < v/2$ up to equivalence.

16. Use multipliers to find a nontrivial difference set in $\mathbb{Z}_{21}$.

17. Use multipliers to find a nontrivial difference set in $\mathbb{Z}_{37}$. Compare this with the difference set constructed using Theorem 4.4, page 50.

18. Prove that $\mathbb{Z}_{49}$ does not contain a nontrivial difference set. (Note: We still have not ruled out a difference set in $\mathbb{Z}_7 \oplus \mathbb{Z}_7$.)

19. Prove that, up to equivalence, $\mathbb{Z}_{43}$ has only two difference sets with $1 < k < v/2$, and that these two have parameters $(43, 21, 10)$.

20. Find all the nontrivial difference sets (up to equivalence) in the cyclic group $\mathbb{Z}_{31}$.

(a) Find all parameters $(31, k, \lambda)$ with $1 < k < v/2$ that satisfy the basic equation $k(k-1) = \lambda(v-1)$.

(b) Which of these triples pass the BRC test?

(c) For each triple of parameters that passes the BRC test, use multipliers to determine the number of equivalence classes of difference sets.

21. Find all the nontrivial difference sets (up to equivalence) in the cyclic group $\mathbb{Z}_{67}$. (Note that 67 is the number of this volume in the AMS STML series.)

(a) Find all parameters $(67, k, \lambda)$ with $1 < k < v/2$ that satisfy the basic equation $k(k-1) = \lambda(v-1)$.

(b) Which of these triples pass the BRC test?

(c) For each triple of parameters that passes the BRC test, use multipliers to determine the number of equivalence classes of difference sets.

22. Write a computer program to calculate the orbits for ϕ_t in the cyclic group $\mathbb{Z}_v$. Allow the user to enter v and t. Your program should check that $\gcd(v, t) = 1$ so that ϕ_t is an automorphism. For output, list the sizes of the orbits and list the orbits themselves.

6.5. Multipliers in non-cyclic groups

To better understand multipliers in the context of abelian non-cyclic difference sets we look at an extended example.

Example 12. Consider the parameters $(99, 49, 24)$. Since $99 = 9\times 11$, we will learn in Chapter 9 that the group $\mathbb{Z}_{11} \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3)$ contains a twin prime powers difference set D. The corollary to the Second Multiplier Theorem guarantees that 5 is a multiplier for any difference set in this group. We will first look at the orbits for ϕ_5. For this we represent group elements as triples $(a; b, c)$, and we multiply by 5 (mod (11, 3, 3)) respectively. For instance

$$(1; 0, 1) \mapsto (5; 0, 2) \mapsto (3; 0, 1) \mapsto (4; 0, 2) \mapsto \dots.$$

This orbit is size 10. In all, we have 1 orbit of size 1, 4 of size 2, 2 of size 5, and 8 of size 10. (See Figure 6.1. The asterisks are explained below.)

$$
\begin{array}{ll}
*_1 & \Big((0;0,0)\Big) \\
*_1 & \Big((0;0,1)\ (0;0,2)\Big) \\
*_1 & \Big((0;1,0)\ (0;2,0)\Big) \\
*_1 & \Big((0;1,1)\ (0;2,2)\Big) \\
*_1 & \Big((0;1,2)\ (0;2,1)\Big) \\
 & \Big((1;0,0)\ (5;0,0)\ (3;0,0)\ (4;0,0)\ (9;0,0)\Big) \\
 & \Big((2;0,0)\ (10;0,0)\ (6;0,0)\ (8;0,0)\ (7;0,0)\Big) \\
*_2 & \Big((1;0,1)\ (5;0,2)\ (3;0,1)\ (4;0,2)\ (9;0,1)\ (1;0,2)\dots\Big) \\
 & \Big((1;1,0)\ (5;2,0)\dots\Big) \\
*_2 & \Big((1;1,1)\ (5;2,2)\dots\Big) \\
 & \Big((1;1,2)\ (5;2,1)\dots\Big) \\
 & \Big((2;0,1)\ (10;0,2)\dots\Big) \\
*_3 & \Big((2;1,0)\ (10;2,0)\dots\Big) \\
 & \Big((2;1,1)\ (10;2,2)\dots\Big) \\
*_3 & \Big((2;1,2)\ (10;2,1)\dots\Big)
\end{array}
$$

Figure 6.1. Orbits for Example 12

Theorem 6.9 says that, since there is a difference set in this group, there must be a difference set fixed by ϕ_5. If we are lucky, the twin prime powers difference set D will be fixed. If not, then a shift of this difference set will be fixed.

All the elements in the orbits of sizes 1 and 2 belong to D since these elements have $\mathbb{Z}_{11}$ component equal to 0.

To find the other elements we need to find the quadratic residues in $\mathbb{Z}_{11} = GF(11)$ and in $GF(9)$. The quadratic residues of $\mathbb{Z}_{11}$ are $\{1, 5, 3, 4, 9\}$. To identify the quadratic residues in $GF(9)$ we need to understand its structure as $\mathbb{Z}_3[x]/\langle p(x)\rangle$.

In $\mathbb{Z}_3[x]$, the polynomial $p(x) = x^2 + 2x + 2$ is irreducible. We construct the field $\mathbb{Z}_3[x]/\langle p(x)\rangle$, and note that the coset represented by x is a generator of the multiplicative group of nonzero elements. (See A.18.) In the table below we show the nonzero elements of $GF(9)$ in their forms as polynomials in x and as ordered pairs from $\mathbb{Z}_3 \oplus \mathbb{Z}_3$:

$$\begin{array}{rcrcl@{\qquad}rcrcl}
1 & = & 1 & = & (0,1) & x & = & x & = & (1,0) \\
x^2 & = & x+1 & = & (1,1) & x^3 & = & 2x+1 & = & (2,1) \\
x^4 & = & 2 & = & (0,2) & x^5 & = & 2x & = & (2,0) \\
x^6 & = & 2x+2 & = & (2,2) & x^7 & = & x+2 & = & (1,2)\ .
\end{array}$$

From this construction the quadratic residues are (0,1), (1,1), (0,2) and (2,2). In the table of orbits, those containing elements with quadratic residues in both $\mathbb{Z}_{11}$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ are marked with $*_2$. Those with quadratic non-residues in both are marked with $*_3$. We conclude that the difference set D consists of the elements in the orbits of ϕ_5 that are marked, and D is indeed fixed by ϕ_5.

Note: This works because in both $\mathbb{Z}_{11}$ and $GF(9)$, 5 is a quadratic residue. (In the second field since $5 \equiv 2 \bmod 3$, we multiply by 2, and $2 = (0,2) = (x^2)^2$.) So multiplying an element by 5 takes squares to squares and non-squares to non-squares in both fields. $\diamond$

Exercises

23. Use multipliers to find a $(49, 16, 5)$-difference set in $\mathbb{Z}_7 \oplus \mathbb{Z}_7$ or to show that none exists. A computer may be useful.

24. With the aid of a computer, use multipliers to explore possible difference sets in the abelian, non-cyclic group $\mathbb{Z}_{23} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$.

Coda

Multipliers have been central to the study of difference sets from the beginning. Marshall Hall began the systematic study of difference sets, and, in particular, he introduced multipliers in 1947. Since then, multipliers have become an important tool for answering the existence question for abelian difference sets and for providing information about equivalence. In this chapter the emphasis is on *using* multipliers for discovery and for proof of non-existence. Hall's first two multiplier theorems are stated without proof. This chapter provides opportunities for the use of the computer as an investigative tool.

Chapter 7

Necessary Group Conditions

Chapters 5 and 6 introduced necessary conditions for the existence of difference sets with certain parameters and in certain groups. Here we continue this discussion with three results that depend on the structure of the group. There are two related topics in Section 1. The first concerns the distribution of the elements of a difference set among the cosets of a normal subgroup of G. The second considers homomorphic images of D in the setting of the integral group ring. In Section 2 we discuss Turyn's "exponent bound". In Section 3 we describe Dillon's "dihedral trick" linking the existence of a difference set in a generalized dihedral group of size $2n$ to a difference set in an abelian group of the same size.

7.1. Intersection numbers

Partitioning D. We start with a group G that contains a difference set D. When G has a normal subgroup N, the cosets mod N partition the elements of G and correspondingly lead to a partition of the elements of D. The main result of this section concerns the possible sizes of these subsets of D. This theorem can be used both to find difference sets and to rule out the existence of difference sets in certain groups.

We start by looking at an example found in Kibler's list of difference sets.

Example 1. Let G be the elementary abelian 3-group of order 27 generated by a, b, and c, and consider the difference set from Kibler [**40**]

$$D = \{1, a, a^2, b, ab, b^2, c, ac, bc, ac^2, a^2bc^2, b^2c^2, a^2b^2c^2\}.$$

If we choose the subgroup $N = \langle a, b\rangle$, then $G = N \cup Nc \cup Nc^2$ and D is partitioned into $D = D_0 \cup D_1 \cup D_2$ where $D_i = D \cap Nc^i$. We find that $D_0 = \{1, a, a^2, b, ab, b^2\}$, $D_1 = \{c, ac, bc\}$, and $D_2 = \{ac^2, a^2bc^2, b^2c^2, a^2b^2c^2\}$. The numbers of elements in these D_i are (respectively) 6, 3, and 4. ◇

Example 2. Let G be the group $\mathbb{Z}_5 \oplus \mathbb{Z}_7$ and let D be the $(35, 17, 8)$-difference set based on the twin primes 5 and 7. (See Theorem 4.6.) Let $N_1 = \{(a, 0) \mid a \in \mathbb{Z}_5\}$ and let $N_2 = \{(0, b) \mid b \in \mathbb{Z}_7\}$. These are normal subgroups in G. Figure 7.1 shows the elements of D and their membership in the various cosets of these normal subgroups. For instance, the second column shows that coset $(0, 1) + N_1$ (denoted by $(*, 1)$ in the table) contains two elements of D, namely $(1, 1)$ and $(4, 1)$. ◇

	$(*,0)$	$(*,1)$	$(*,2)$	$(*,3)$	$(*,4)$	$(*,5)$	$(*,6)$	
$(0,*)$	$(0,0)$							1
$(1,*)$	$(1,0)$	$(1,1)$	$(1,2)$		$(1,4)$			4
$(2,*)$	$(2,0)$			$(2,3)$		$(2,5)$	$(2,6)$	4
$(3,*)$	$(3,0)$			$(3,3)$		$(3,5)$	$(3,6)$	4
$(4,*)$	$(4,0)$	$(4,1)$	$(4,2)$		$(4,4)$			4
	5	2	2	2	2	2	2	17

Figure 7.1. Array showing elements of the twin-prime difference set

The sizes of the intersections of a possible difference set D with the various cosets of a normal subgroup are useful in tackling the existence question.

Definition. Let G be a group and N a normal subgroup of index r. Let $\{g_1, \ldots, g_r\}$ be a complete set of coset representatives for N in G. If D is a difference set in G, then the numbers $n_i = |D \cap g_i N|$ are the intersection numbers for D with respect to N.

For short we sometimes call these the intersection numbers for D mod N. In Figure 7.1 the numbers at the ends of the columns are the intersection numbers mod N_1, and those at the ends of the rows are the intersection numbers mod N_2. It is clear that the sum of the intersection numbers mod N for a (v, k, λ)-difference set must be k. What is less obvious is that the sum of their squares is predictable.

Theorem 7.1. *Let D be a (v, k, λ)-difference set in the group G, and let N be a normal subgroup of index r in G with $|N| = s$. Let $\{g_1, \ldots, g_r\}$ be a complete set of coset representatives, and denote the intersection numbers for D with respect to N by $n_i = |D \cap g_i N|$. Then*

$$\begin{aligned} \sum_{i=1}^{r} n_i &= k \\ \sum_{i=1}^{r} (n_i)^2 &= n + \lambda s. \end{aligned}$$

As illustrations of this theorem, we look again at the examples above.

Example 3. In the $(27, 13, 6)$-difference set of Example 1, we have $s = |\langle a, b \rangle| = 9$, $n = 7$, and

$$6^2 + 3^2 + 4^2 = 61 = 7 + 6 \cdot 9.$$

In the $(35, 17, 8)$-difference set of Example 2, when $s = 5$ we have $n + \lambda s = 9 + 8 \cdot 5 = 49$. We check that $\sum n_i^2 = 5^2 + 6 \cdot 2^2 = 49$. When $s = 7$ we have $n + \lambda s = 9 + 8 \cdot 7 = 65$. We check that $\sum n_i^2 = 1^2 + 4 \cdot 4^2 = 65$. ◇

Our proof of Theorem 7.1 uses the integral group ring introduced in Chapter 4. Recall that if D is a (v, k, λ)-difference set in G, then in the integral group ring $\mathbb{Z}G$ we know that $DD^{(-1)} = n1_G + \lambda G$. Our proof involves summing the coefficients of elements of N on each side of this equation.

Proof. The right hand side of the equation $DD^{(-1)} = n1_G + \lambda G$ may be rewritten as $n1_G + \lambda N + \lambda(G \setminus N)$. So the sum of the coefficients of elements in N is $n + \lambda|N| = n + \lambda s$. For the left hand side we write $D = D_1 + D_2 + \cdots + D_r$ where r is the index of N in G and $D_i = D \cap g_i N$. Then

$$\begin{aligned} DD^{(-1)} &= \Big(D_1 + D_2 + \cdots + D_r\Big)\Big(D_1 + D_2 + \cdots + D_r\Big)^{(-1)} \\ &= \sum_{i \neq j} D_i\, D_j^{(-1)} \;+\; \sum_i D_i\, D_i^{(-1)}. \end{aligned}$$

The terms $D_i\, D_j^{(-1)}$ have nonzero coefficients for elements in the coset $g_i\, g_j^{-1} N$. These elements are in N if and only if $i = j$. So in the expression for $DD^{(-1)}$ the sum of the coefficients of elements in N is the sum of coefficients in $\sum_i D_i\, D_i^{(-1)}$, namely the sum of squares of the intersection numbers. We conclude that

$$\sum_{i=1}^{r} (n_i)^2 = n + \lambda s. \qquad \square$$

Next we look at how this theorem can be used to limit the search for a difference set in a particular group. If we suspect that a group G might have a (v, k, λ)-difference set, we could check each of the $\binom{v}{k}$ subsets of G. This is prohibitively time consuming even for quite small examples. If G contains such a difference set D, we could search for an equivalent difference set $g^{-1}D$ where $g \in D$. This guarantees that 1_G is in $g^{-1}D$, so we only need to examine k-subsets that include 1_G, cutting the brute force search down to $\binom{v-1}{k-1}$. In a similar fashion, if we know a supposed difference set in a group G with normal subgroup N must have certain intersection numbers, we can limit our search based on these numbers.

Example 4. Continuing with Example 1, let $G = \langle a, b, c \mid a^3 = b^3 = c^3 = 1\rangle$ and $N = \langle a, b\rangle$. If we have a $(27, 13, 6)$-difference set D in G, we can show that the only intersection numbers that obey Theorem 7.1 are 3, 4, 6 in some order. Further we can specify the assignment of these numbers to specific cosets by looking at difference sets equivalent to D. Let D be a difference set with intersection numbers $3, 4, 6$. By multiplying D by an appropriate power of c, we

can find a difference set equivalent (by a shift) to one with $|D \cap N| = 6$. Similarly the mapping

$$a \mapsto a, \quad b \mapsto b, \quad c \mapsto c^2$$

is a homomorphism that keeps the coset N fixed and interchanges the cosets Nc and Nc^2. So using this mapping if necessary, we can find an equivalent difference set with $|D \cap Nc| = 4$ and $|D \cap Nc^2| = 3$. Thus, we can limit our search to sets with 6 elements in N, 4 in Nc, and 3 in Nc^2. So we have cut the brute force search from $\binom{27}{13} \approx 20$ million to $\binom{9}{6}\binom{9}{4}\binom{9}{3} = 889,056$. Of course this number is also large, but computers may be able to tackle the smaller search in reasonable time where the larger one may be intractable. ◇

Homomorphisms. To take advantage of the integral group ring as a tool for studying intersection numbers, we start with a group homomorphism $\varphi : G \to H$ and extend it to a mapping $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$. Let N be the kernel of φ, so $H = G/N$. Then this mapping $\widehat{\varphi}$ will give us a slightly different approach to a proof of Theorem 7.1, and will be useful in later chapters.

First we must prove that $\widehat{\varphi}$ is a ring homomorphism.

Theorem 7.2. *Assume G and H are groups and $\varphi : G \to H$ is a group homomorphism. Define $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$ by*

$$\widehat{\varphi}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \, \varphi(g).$$

Then $\widehat{\varphi}$ is a ring homomorphism.

Let us look at some examples.

Example 5. One case of interest is when G is a group, $H = \{1_G\}$, and $\varphi(g) = 1_G$ for all $g \in G$. So $N = G$. Then $\widehat{\varphi}(\sum a_g g) = \sum a_g 1_G$ which we identify with the integer $\sum a_g \in \mathbb{Z}$. By analogy to evaluating a polynomial $f(x) \in \mathbb{Z}[x]$ at $x = 1$, this is sometimes called the *evaluation map.* ◇

Example 6. Let $G = \langle a, b \mid a^7 = b^3 = 1, \ ba = a^2 b \rangle$, and $D = \{1, a, a^3, b, a^2 b^2\}$, a $(21, 5, 1)$-difference set. We define $H = \langle b \rangle$, and

consider the homomorphism φ from G to H defined by $\varphi(a) = 1$, $\varphi(b) = b$. The kernel of φ is $N = \langle a \rangle$. Then $\widehat{\varphi} : \mathbb{Z}G \to \mathbb{Z}H$ with $\widehat{\varphi}(G) = 7H$ and $\widehat{\varphi}(D) = 3 \cdot 1_H + 1 \cdot b + 1 \cdot b^2$. Note that the coefficients in $\widehat{\varphi}(D)$ are the intersection numbers of D mod N. $\diamond$

The following theorem shows the result of applying $\widehat{\varphi}$ to the integral group ring equation for a difference set. Note that it requires that the group homomorphism map G *onto* H.

Theorem 7.3. *Assume D is a (v, k, λ)-difference set in G and $\varphi : G \to H$ is an epimorphism of groups. Then the image $\widehat{D} = \widehat{\varphi}(D)$ satisfies the following equation in $\mathbb{Z}H$:*

$$\widehat{D}\widehat{D}^{(-1)} = n1_H + s\lambda H,$$

where s is the order of $N = Ker\varphi$.

Example 7. This example sets the stage for a slightly different proof of Theorem 7.1 (see Exercise 11). Suppose the group G contains a (v, k, λ)-difference set D. Suppose further that G contains a normal subgroup N and let $\varphi : G \to G/N = H$ be the natural homomorphism. Assume $\{g_1, \ldots, g_r\}$ is a complete set of coset representatives for N in G, and let $n_i = |D \cap g_i N|$. Write $h_i = \varphi(g_i)$. Then

$$\widehat{D} = \widehat{\varphi}(D) = \sum_{i=1}^{r} n_i h_i. \qquad \diamond$$

Difference lists. Motivated by Theorem 7.3, we have the following generalization of a difference set.

Definition. An element $E = \sum_h a_h h$ in the integral group ring $\mathbb{Z}H$ is called a difference list over H with parameters (r, k, s, λ) if s and k are positive integers, λ and the a_h are non-negative, $|H| = r$, $\sum_h a_h = k$, and $EE^{(-1)} = (k - \lambda)1_H + s\lambda H$.

Difference lists were introduced in [**2**]. In that paper, the authors interpreted E as a multiset of elements from H, with $a_h h$ regarded as a_h copies of the element h. In the special case when $s = 1$ and all the coefficients a_h are 0 or 1, E interpreted as a subset of elements of H is an (r, k, λ)-difference set.

Write the image of a group G under a group homomorphism as $H \simeq G/N$. It is then clear that the image of a difference set D

in $\mathbb{Z}G$ under the corresponding ring homomorphism is a difference list $E = \sum_h a_h h$ in $\mathbb{Z}H$. In this case the multiplicity a_h counts the number of elements of D in the coset mod N that corresponds to h. In ([**8**], p. 332) we find the remark that not all difference lists can be obtained in this way. We also find the following interesting theorem, due to Hall and Ryser for cyclic groups and Bruck for general groups ([**10**], p. 469).

Theorem 7.4. *Let E be an (r, k, s, λ)-difference list over H, where r is odd and $n = k - \lambda$. Then the equation*

$$x^2 = ny^2 + (-1)^{(r-1)/2} r z^2$$

has a nontrivial solution in integers x, y, z.

This result is similar to the powerful and useful Bruck-Ryser-Chowla Theorem for symmetric designs (and thereby for difference sets).

Example 8. Can a $(25, 9, 3)$-difference set exist? These parameters satisfy BRC because $x^2 = 6y^2 + 3z^2$ has the solution $x = 3$ and $y = z = 1$. It is a consequence of the class equation (A.10) that every group of order equal to the square of a prime is abelian. Therefore a group of order 25 has a normal subgroup of order 5. It follows that if a difference set with these parameters existed, then a $(5, 9, 5, 3)$-difference list would also exist. Then by Theorem 7.4 the equation $x^2 = 6y^2 + 5z^2$ would have a nontrivial solution. However, by Theorem 5.2, this is impossible. ◇

Exercises

1. Let D be the difference set in Example 1.

(a) Let N be the normal subgroup $\langle a \rangle$. Find the intersection numbers for D with respect to N, and verify that these numbers obey Theorem 7.1.

(b) Show that these nine intersection numbers form a subpartition of the intersection numbers with respect to $\langle a, b \rangle$.

2. Consider the non-abelian group $G = \langle a, b \mid a^9 = b^3 = 1,\ ba = a^4 b\rangle$ with $(27, 13, 6)$-difference set given by Kibler

$$D = \{1, a, a^2, a^4, a^5, a^7, b, ab, a^2 b, a^5 b, a^5 b^2, a^6 b^2, a^8 b^2\}.$$

(a) Check whether the subgroups $\langle a\rangle$ and $\langle b\rangle$ are normal subgroups.

(b) For any normal subgroups found in part (a), find the corresponding intersection numbers and confirm that they satisfy the equations in Theorem 7.1. Ⓢ

3. In this exercise we return to Example 4 to verify the claim that the only intersection numbers for a $(27, 13, 6)$-difference set G satisfying the equations in Theorem 7.1 are $3, 4, 6$. Suppose the intersection numbers, in some order, are the non-negative integers x, y, z.

(a) Explain why, without loss of generality, we may assume $x \leq y \leq z \leq 7$.

(b) By examining cases, complete the verification.

4. In the proof of Theorem 7.1, where do we use the fact that N is a *normal* subgroup of G?

5. Consider the non-abelian group

$$G = \langle a, b \mid a^{19} = b^3 = 1,\ ba = a^7 b\rangle.$$

(a) Show that $N = \langle a\rangle$ is normal in G.

(b) Assume that there is a $(57, 8, 1)$-difference set D in G, and find all possible triples of intersection numbers using Theorem 7.1.

(c) Show that we can assume without loss of generality that $n_0 \geq n_1,\ n_2$, where $n_j = |D \cap b^j N|$.

(d) Show that there is no homomorphism of G that fixes N and interchanges the cosets bN and $b^2 N$. (This means we cannot swap intersection numbers n_1 and n_2 without loss of generality.)

(e) Compare your results above to the two difference sets in G given in Kibler's list for this group [**40**]:
$D_2 = \{1, a, a^3, a^8, b, a^4b, a^{13}b, a^{18}b^2\}$,
$D_3 = \{1, a, a^3, a^8, b, a^5b^2, a^9b^2, a^{18}b^2\}$.

6. Let G be a group of order 39. First look back at Example 5.7 to see what we know so far about the existence of $(39, 19, 9)$-difference sets. Use Theorem 7.1 to show that G cannot contain a $(39, 19, 9)$-difference set. Ⓗ

7. Let G be as in Example 6. Map G onto $H = \langle b \rangle$ by $\varphi(a^ib^j) = b^j$.

(a) Verify that φ is a group homomorphism.

(b) Calculate $\widehat{\varphi}((a^2 + 3ab - 5a^2b)(2a^5 - b))$.

(c) Calculate $\widehat{\varphi}(a^2 + 3ab - 5a^2b)\widehat{\varphi}(2a^5 - b)$.

8. Prove Theorem 7.2.

9. Start with the $(40, 13, 4)$-difference set

$$D = \{1, a, a^2, b, a^3b, ab^2, a^3b^2, a^4b^2, ab^4, ab^5, a^2b^5, ab^6, a^4b^7\}$$

in the group $G = \langle a, b \mid a^5 = b^8 = 1, ba = a^4b \rangle$.

(a) Explain why $N = \langle a \rangle$ is a normal subgroup in G.

(b) Find a complete set of coset representatives of G modulo N.

(c) Let $\varphi : G \to G/N = H$ be the natural homomorphism. Find $\widehat{D} = \widehat{\varphi}(D)$.

(d) How do the coefficients of $\widehat{D}$ in $\mathbb{Z}H$ compare to the intersection numbers for D mod N?

10. Prove Theorem 7.3

11. Using the notation of Example 7, compare the coefficients of 1_H on each side of the $\mathbb{Z}H$ equation in Theorem 7.3 to give another proof of Theorem 7.1

12. Recall from Section 5.1 that no projective plane of order $n = 10$ exists. It follows that no symmetric $(111, 11, 1)$ design exists, even though these parameters satisfy BRC. This fact implies that no difference set with these parameters exists. Using Theorem 7.4, give a direct proof that no $(111, 11, 1)$-difference set exists. Ⓗ

13. This exercise concerns the parameters $(201, 25, 3)$.

(a) Show that these parameters satisfy BRC.

(b) Use Theorem 7.4 to show that no $(201, 25, 3)$-difference set exists.

7.2. Turyn's exponent bound

The aspect of the structure of a group G that is the focus of this section is the exponent[1] of a Sylow p-subgroup of G. We also restrict our attention to abelian groups. The first version of our main theorem further restricts our discussion to difference sets with parameters $(4p^{2a},\ 2p^{2a} - p^a,\ p^{2a} - p^a)$ for a prime p. While this may sound narrow, these difference sets are in the important "Hadamard family" with $v = 4n$. All of these difference sets can be shown to have parameters of the form $(4u^2, 2u^2 - u, u^2 - u)$. We study them in Section 9.3. The second version of Turyn's theorem is more general.

Turyn's paper [**69**] is important not only for his very useful exponent bound, but also for his innovative use of tools from character theory and from algebraic number theory. We give an elementary introduction to some of these methods in Chapters 11 and 12. Here is the first version of Turyn's theorem as it is often given in the literature (for example, in [**8**], p. 414).

Theorem 7.5. *(Turyn's exponent bound, first version) Let p be a prime and assume the existence of a difference set with parameters*

$$(4p^{2a},\ 2p^{2a} - p^a,\ p^{2a} - p^a)$$

[1] See A.8 for the definition of the exponent of a group.

in an abelian group G. Let P be the Sylow p-subgroup of G. Then one has the following bounds on the exponent of P:

$$\begin{aligned} exp(P) &\leq p^a \quad \text{for } p \text{ odd}, \\ exp(P) &\leq 4 \cdot 2^a \quad \text{for } p = 2. \end{aligned}$$

Deducing this theorem from the second version is left as an exercise, and we give a proof of the second version in Chapter 12. For now we concentrate on applying Theorem 7.5, as in the following examples.

Example 9. Consider $G = \mathbb{Z}_{16}$, the cyclic group of order 16. In the notation of the theorem, $|G| = 16 = 4p^{2a} = 4 \cdot 2^2$ with $a = 1$. Since $\exp(P) = \exp(G) = 16$, which exceeds the bound of $4 \cdot 2^1 = 8$, there is no $(16, 6, 2)$-difference set in $\mathbb{Z}_{16}$. ◇

Example 10. Consider an abelian group G of order $100 = 4 \cdot 5^2$, and let P be the Sylow 5-subgroup of G. If G contains a $(100, 45, 20)$-difference set, then by the theorem $\exp(P) \leq 5$, so $P = \mathbb{Z}_5 \oplus \mathbb{Z}_5$ is possible, but $P = \mathbb{Z}_{25}$ is ruled out. ◇

For a cyclic group G of order $4p^{2a}$, if $p = 2$, then $P = G$ and $\exp(P) = v$. Otherwise, the Sylow p-subgroup P has exponent p^{2a}. So in either case, if G is cyclic, then P has the largest possible exponent. For $a = 0$, the parameters in Theorem 7.5 are $(4, 1, 0)$, and the cyclic group with 4 elements does have a (trivial) difference set with these parameters. But for $a \geq 1$ and for any prime p, Turyn's exponent bound rules out difference sets in cyclic groups of order $4p^{2a}$ for all $a \geq 1$ and all primes p. Together with Dillon's "dihedral trick," discussed in the next section, this rules out difference sets in infinitely many dihedral groups.

In 1993 Kraemer[2] showed that for abelian 2-groups, Turyn's exponent bound is not only a necessary but also a sufficient condition for the existence of a difference set [**41**].

Theorem 7.6. *There exists a $(4 \cdot 2^{2a},\ 2 \cdot 2^{2a} - 2^a,\ 2^{2a} - 2^a)$-difference set in an abelian group G if and only if $exp(G) \leq 4 \cdot 2^a$.*

[2]The result is also in Jedwab's 1991 doctoral thesis ([**17**], p. 137).

In the same year, conclusive evidence appeared that non-abelian difference sets are more exotic. Liebler and Smith constructed a non-abelian $(64, 28, 12)$-difference set exceeding Turyn's exponent bound. (See [**47**] in [**37**].) They wrote, "Dillon has raised the question of which 2-groups G admit difference sets, and his question has been settled for all groups of order 64 except [one]." The open case was $G = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$, and Liebler and Smith were actually trying to prove non-existence when they made their surprising discovery. Their work was subsequently generalized by Davis and Smith in [**17**]. Davis and Smith showed that the difference set in [**47**] is a member of an infinite family of difference sets in non-abelian groups of order $4 \cdot 2^{2a}$ with exponent $4 \cdot 2^{a+1}$. We will return to a discussion of these developments in Section 9.3.

The second, more general version of Turyn's exponent bound is given here as stated in ([**8**], p. 440). We first need the definition of a term used in its statement. (The motivation for this notion of *self-conjugacy* comes from algebraic number theory and is discussed in Chapter 12.)

Definition. Let p be a prime, and w an integer. Write $w = p^a w'$ where w' is not divisible by p. Then p is self-conjugate modulo w if there exists a non-negative integer j with $p^j \equiv -1 \pmod{w'}$. An integer ℓ is self-conjugate modulo w if every prime divisor of ℓ is self-conjugate modulo w.

Example 11. Choose $p = 5$. We look at three choices for w. If $w = 85$, then $w' = 13$ and $5^2 \equiv -1 \pmod{13}$, so 5 is self-conjugate modulo 85. If $w = 125$ then $w' = 1$ and $5 \equiv 1 \equiv -1 \pmod{1}$, so 5 is self-conjugate modulo 125. If $w = 20$ then $w' = 4$ and since $5 \equiv 1 \pmod{4}$, no power of 5 can be congruent to -1 mod 4, and 5 is *not* self-conjugate modulo 20. Notice too that for any positive integer a, 5^a is self-conjugate modulo w whenever 5 is. $\diamond$

Now we can state the stronger form of Turyn's exponent bound.

Theorem 7.7. *(Turyn's exponent bound, second version) Assume the existence of a (v, k, λ)-difference set in an abelian group G. Let p be a prime divisor of v and denote the Sylow p-subgroup of G by P. Assume that p^{2a} divides n for some $a \geq 1$. Let U be any subgroup of*

G with $U \cap P = \{1\}$. If p is self-conjugate modulo $e = exp(G/U)$, then

$$exp(P) \leq |U| \frac{|P|}{p^a}.$$

We remark that one way to apply this version of Turyn's exponent bound is to choose $U = \{1\}$.

Exercises

14. List the abelian 2-groups that cannot contain a $(64, 28, 12)$-difference set.

15. Consider abelian groups of order 324.

(a) Find the exponent bound for the Sylow 3-subgroup given in Theorem 7.5. Ⓢ

(b) Using this, list all abelian groups of order 324 that *cannot* contain a $(324, 153, 72)$-difference set.

16. Consider the parameters $(175, 30, 5)$.

(a) List the possible abelian groups of order 175.

(b) Why does Theorem 7.5 not apply in this case?

(c) Based on Theorem 7.7, which of the groups in (a) *cannot* contain a $(175, 30, 5)$-difference set?

17. Consider the parameters $(160, 54, 18)$.

(a) List the possible abelian groups of order 160.

(b) Why does Theorem 7.5 not apply in this case?

(c) Based on Theorem 7.7, which of the groups in (a) *cannot* contain a $(160, 54, 18)$-difference set?

18. In this exercise you will deduce Theorem 7.5 from Theorem 7.7. Assume the abelian group G has a $(4p^{2a}, 2p^{2a} - p^a, p^{2a} - p^a)$-difference set for some prime p and positive integer a. Let P be the Sylow p-subgroup of G.

(a) Assume $p = 2$ and choose $U = \{1\}$. Explain why 2 is self-conjugate modulo $\exp(G/U)$ and deduce $\exp(P) \leq 4p^a$ from Theorem 7.7.

(b) Assume p is odd and choose U to be a subgroup of G of order 2. Explain why p is self-conjugate modulo $\exp(G/U)$ and deduce $\exp(P) \leq p^a$ from Theorem 7.7.

7.3. Dillon's dihedral trick

Dillon [**18**] showed that if there is no cyclic difference set in a group of order $2m$, then there is no difference set in the dihedral group of order $2m$. His theorem is actually more general.

Definition. Let H be an abelian group. The group G is a generalized dihedral extension of H if there is an element $\mathbf{g} \notin H$ such that $G = H + \mathbf{g}H$ in $\mathbb{Z}G$, $\mathbf{g}^2 = 1$, and for all $h \in H$, $\mathbf{g}h\mathbf{g} = h^{-1}$.

Example 12. Let $H = \langle a, b \mid a^6 = b^2 = 1, ab = ba \rangle$, and let $G = \langle a, b, c \mid a^6 = b^2 = c^2 = 1, ab = ba, ac = ca^{-1}, bc = cb \rangle$. Then G is a generalized dihedral extension of H with $\mathbf{g} = c$. $\diamond$

Theorem 7.8. [**18**] *Let H be an abelian group, and let G be a generalized dihedral extension of H. If G contains a difference set, then any abelian group with H as a subgroup of index 2 also contains a difference set.*

The proof of this theorem relies heavily on calculations in the integral group ring, and is a good demonstration of the usefulness of $\mathbb{Z}G$.

Proof. Assume $G = H + \mathbf{g}H$. Let D be a difference set in G, and write $D = X + \mathbf{g}Y$ for X and Y subsets of H. Since D is a difference set, $DD^{(-1)} = n1_G + \lambda G$. We substitute the expression for D in terms of the subsets X and Y to learn more about how these two subsets interact. In this calculation note that $\mathbf{g} = \mathbf{g}^{-1}$. We can freely commute subsets of the abelian group H. However, we must be careful

with $\mathbf{g}$. Specifically $X\mathbf{g} = \mathbf{g}X^{(-1)}$ and $(\mathbf{g}Y)^{(-1)} = Y^{(-1)}\mathbf{g} = \mathbf{g}Y$, so

$$\begin{aligned}(X+\mathbf{g}Y)(X+\mathbf{g}Y)^{(-1)} &= (X+\mathbf{g}Y)(X^{(-1)}+\mathbf{g}Y)\\ &= XX^{(-1)}+YY^{(-1)}+\mathbf{g}YX^{(-1)}+X\mathbf{g}Y\\ &= XX^{(-1)}+YY^{(-1)}+2\mathbf{g}YX^{(-1)}.\end{aligned}$$

Since this must equal $n1_G + \lambda G$, we equate the summands involving elements of H, which gives us Equation (1). Equating the summands involving elements of $\mathbf{g}H$ gives Equation (2). Equation (3) is obtained from (2) via $XY^{(-1)} = (YX^{(-1)})^{(-1)} = (\lambda/2)H^{(-1)} = (\lambda/2)H$.

Thus

$$XX^{(-1)} + YY^{(-1)} = n1_G + \lambda H \quad (1)$$

$$YX^{(-1)} = \frac{\lambda}{2}H \quad (2)$$

$$XY^{(-1)} = \frac{\lambda}{2}H. \quad (3)$$

Now let K be an abelian group with H a subgroup of index 2. We can write $K = H + \mathbf{k}H$ for some element $\mathbf{k} \notin H$. Note here that $\mathbf{k}$ need not have order 2, though $\mathbf{k}^2 \in H$, so $\mathbf{k}^2H = H$. We claim that $C = X + \mathbf{k}Y$ is a difference set in K. Since K is abelian we can freely commute elements in the calculation below:

$$\begin{aligned}CC^{(-1)} &= (X+\mathbf{k}Y)(X+\mathbf{k}Y)^{(-1)}\\ &= (X+\mathbf{k}Y)(X^{(-1)}+\mathbf{k}^{-1}Y^{(-1)})\\ &= XX^{(-1)}+YY^{(-1)}+\mathbf{k}YX^{(-1)}+\mathbf{k}^{-1}XY^{(-1)}.\end{aligned}$$

In this last term we replace $\mathbf{k}^{-1}$ with $\mathbf{k}\mathbf{k}^{-2}$ to get:

$$CC^{(-1)} = XX^{(-1)} + YY^{(-1)} + \mathbf{k}\Big(YX^{(-1)} + \mathbf{k}^{-2}XY^{(-1)}\Big).$$

Then using Equations (1)–(3) we get:

$$\begin{aligned}CC^{(-1)} &= n1_K + \lambda H + \mathbf{k}\left(\frac{\lambda}{2}H + \frac{\lambda}{2}H\right)\\ &= n1_K + \lambda K.\end{aligned}$$

Thus a difference set in the generalized dihedral group G can be used to construct a difference set in the abelian group K. □

Exercises

19. Let $G_1 = \langle a, b, c \,|\, a^4 = b^2 = c^2 = 1, bab = a^3, ac = ca, bc = cb \rangle$ and let $H = \langle a, c \rangle \subset G_1$.

(a) Show that G_1 is a generalized dihedral extension of H.

(b) Give generators and relations for an abelian group G_2 that has H as a subgroup of index 2. (There is more than one way to do this.)

(c) We know from Kibler's list that $D_1 = \{1, a, a^2, b, ac, a^2bc\}$ is a $(16, 6, 2)$-difference set in G_1. Use Dillon's construction to produce a $(16, 6, 2)$-difference set D_2 in your group G_2. Verify that D_2 is a $(16, 6, 2)$-difference set in G_2.

(d) There are 8 difference sets in abelian groups of order 16 in Kibler's catalog [**40**]. They are listed below. (We omit the commutativity of generators from the relations.) Which of these groups is isomorphic to G_2? Show that your difference set D_2 is equivalent to one listed below.

No.	Difference Set	Group
1.	$1, x, x^2, x^4, xy, x^6y$	$\langle x, y \mid x^8 = y^2 = 1 \rangle$
2.	$1, x, x^2, x^5, y, x^6y$	$\langle x, y \mid x^8 = y^2 = 1 \rangle$
3.	$1, x, x^2, y, xy^2, x^2y^3$	$\langle x, y \mid x^4 = y^4 = 1 \rangle$
4.	$1, x, x^2, y, y^3, x^3y^2$	$\langle x, y \mid x^4 = y^4 = 1 \rangle$
5.	$1, x, y, x^2y, xy^2, x^2y^2$	$\langle x, y \mid x^4 = y^4 = 1 \rangle$
6.	$1, x, x^2, y, z, x^3yz$	$\langle x, y, z \mid x^4 = y^2 = z^2 = 1 \rangle$
7.	$1, x, x^2, xy, xz, x^3yz$	$\langle x, y, z \mid x^4 = y^2 = z^2 = 1 \rangle$
8.	$1, x, y, z, w, xyzw$	$\langle x, y, z, w \mid x^2 = y^2 = z^2 = w^2 = 1 \rangle$

20. Consider groups of order 64.

(a) Show that the dihedral group D_{32} cannot contain a difference set with parameters $(64, 28, 12)$.

(b) Write $G_1 = \langle a, b \mid a^{32} = b^2 = 1, ab = ba \rangle$. Give generators and relations for a *non-cyclic* subgroup H of index 2 in G_1.

(c) Specify generators and relations for a generalized dihedral extension G_2 of H that is not isomorphic to D_{32}.

(d) Show that G_2 cannot contain a $(64, 28, 12)$-difference set.

Coda

In this chapter we continue our focus on the existence question for difference sets. Here we ask if a group G contains a difference set D, what does that imply about the structure of G? This emphasis on group structure is in contrast to the emphasis on the parameters (v, k, λ) in the two preceding chapters.

In Section 1 we look at the distribution of elements of a difference set in the cosets of a normal subgroup. A useful strategy is to construct a sieve of smaller and smaller normal subgroups of G, leading to finer and finer constraints on the possible elements of a difference set. Sometimes this strategy by itself suffices to prove non-existence. Sometimes it restricts the possibilities enough to make tractable a computer search that either produces a difference set or shows that none can exist. In this way this sieve strategy is similar to the analysis of unions of orbits of multipliers in Chapter 6.

Section 2 concerns the exponent of the Sylow p-subgroup for a prime p. Turyn's exponent bound may prove non-existence, but it provides no help in constructing a difference set if one is possible. This section focuses on applying Turyn's theorem. The proof uses deep ideas from representation theory and algebraic number theory, and it is our culminating application of these tools in Chapter 12.

Dillon's "dihedral trick" in Section 3 links existence of a difference set in a generalized dihedral extension of an abelian group H to existence in an abelian extension of H. It can be used either to prove non-existence or to produce an abelian difference set if the non-abelian one is known.

Chapters 5–7 contain clear necessary conditions for existence, and the latter two provide methods to narrow the search for a difference

set to the point where a computer search may be feasible. In contrast, the next two chapters give explicit constructions for difference sets.

Chapter 8

Difference Sets from Geometry

In Chapter 2 we introduced finite affine and projective geometries. While we know from Chapter 4 that the existence of a symmetric (v, k, λ) design is necessary for the existence of a (v, k, λ)-difference set, we have not yet explicitly used geometry to produce a difference set. This is the goal of the present chapter. We begin with Singer's construction [**62**] and then describe two more recent constructions due to Turyn [**69**] and McFarland [**50**] respectively. Each of these three authors uses geometry in a different way. Singer begins with a projective geometry and produces a cyclic group acting regularly on the points and blocks of the associated symmetric design, which in turn leads to a difference set. Turyn describes a set algebraically but then uses affine geometry to prove that it is a difference set. McFarland literally uses geometry to construct a difference set.

8.1. Singer difference sets

In this section we look at Singer's construction of the family of cyclic difference sets bearing his name. Following the structure of his paper [**62**], we look first at the $(q^2 + q + 1, q + 1, 1)$-difference set associated with the projective plane $PG(2, q)$, for a prime power q. Toward the end of his paper (page 384), Singer writes, "The preceding concepts

are susceptible of immediate generalization." We also look at this generalization, associating a cyclic (v, k, λ)-difference set with $PG(m, q)$ for $m \geq 2$, with

$$v = \frac{q^{m+1} - 1}{q - 1}, \quad k = \frac{q^m - 1}{q - 1}, \quad \lambda = \frac{q^{m-1} - 1}{q - 1}.$$

The key to both arguments is the vector space isomorphism between a space V of dimension $m + 1$ over $\mathbb{F}_q$ and the finite field $GF(q^{m+1})$.

We know $PG(2, q)$ gives a symmetric design whose points are the projective points and whose blocks are the projective lines. Singer's first theorem is the following (written in our language, not his).

Theorem 8.1. *Let q be a prime power. Then the symmetric design of $PG(2, q)$ has an automorphism τ of order $q^2 + q + 1$. The cyclic group $G = \langle \tau \rangle$ acts regularly on the points of $PG(2, q)$.*

Proof. We know that the multiplicative group of nonzero elements of a finite field is cyclic. The proof of Singer's first theorem depends on the representation of points of $PG(2, q)$ as powers of a generator of $GF(q^3)^*$. We also know that $GF(q^3)$ is a 3-dimensional vector space over the field $\mathbb{F}_q$; we call it V to emphasize this structure. We can construct V as $\mathbb{F}_q[x]/\langle p(x) \rangle$ for an irreducible monic polynomial $p(x) \in \mathbb{F}_q[x]$ of degree 3. In fact, it is always possible to choose $p(x)$ so that the coset represented by x is a generator of the multiplicative group $GF(q^3)^*$. (See A.16 and A.18.)

As we did in Exercise 4.12, we identify the elements of $V = \mathbb{F}_q[x]/\langle p(x) \rangle$ with their quadratic coset representatives. It then follows that every element of V can be written as an $\mathbb{F}_q$-linear combination of x^2, x^1, x^0. Since these three vectors span the 3-dimensional vector space V, they therefore form a basis.

The multiplicative group $\mathbb{F}_q^*$ is the unique subgroup of order $q - 1$ in the cyclic group $\langle x \rangle$ of order $q^3 - 1$, and this subgroup is generated by x^r for $r = (q^3 - 1)/(q - 1) = q^2 + q + 1$. The powers of x which correspond to elements of the ground field $\mathbb{F}_q$ are therefore x^{jr} for $j = 0, 1, \ldots, q - 2$. It follows that x^s and x^t correspond to linearly dependent vectors in V if and only if $x^{s-t} \in \mathbb{F}_q$; in other words, they are linearly dependent vectors if and only if the exponents $s \equiv t \pmod{r}$. However, we know $PG(2, q)$ has exactly r points, so we

may take $x^0, x^1, x^2, \ldots, x^{r-1}$ as the vectors generating them. This is our rationale for denoting the projective point determined by x^s by $s \in \mathbb{Z}_r$. (We write x^1 and x^0 instead of x and 1 to keep the link to this notation clear.)

Next, consider the transformation $T_x : V \to V$ defined by multiplication by x. Thus $T_x(0) = 0$ and $T_x(x^s) = x^{s+1}$. This is in fact a non-singular linear transformation of V and so determines an automorphism τ of $PG(2, q)$. We see that $\tau(s) = s+1$ for $s = 0, \ldots, r-2$ and $\tau(r-1) = 0$. The group $G = \langle\tau\rangle$ thus acts transitively on the r points of $PG(2, q)$. Since $|G|$ also equals r, G acts regularly on the points by the orbit-stabilizer theorem (Theorem 3.2, p. 39). □

Example 1. Choose $q = 4$, so $r = (q^3-1)/(q-1) = q^2+q+1 = 21$. For the ground field we have $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ with $\omega^2 + \omega + 1 = 0$. To construct $GF(64) = \mathbb{F}_4[x]/\langle p(x)\rangle$ we choose $p(x) = x^3+x^2+x+\omega$. Since $p(x)$ has no zeroes in $\mathbb{F}_4$, it is irreducible in $\mathbb{F}_4[x]$. We then have $x^3 = x^2+x^1+\omega x^0$. More generally, the vectors x^2, x^1, x^0 form a basis for the 3-dimensional vector space V. We still need to check that x is a generator for $GF(64)^*$. To do this, we express the other powers of x as linear combinations of the basis vectors. (Note that $x^0 = 1$ is actually in the ground field $\mathbb{F}_4$.) We show one calculation in detail:

$$\begin{aligned} x^4 &= x^3 + x^2 + \omega x^1 \\ &= x^2 + x^1 + \omega x^0 + x^2 + \omega x^1 \\ &= \omega^2 x^1 + \omega x^0. \end{aligned}$$

Similarly, we find that $x^5 = \omega^2 x^2 + \omega x^1$, $x^6 = x^2 + \omega^2 x^1 + x^0$, $x^7 = \omega x^2 + \omega x^0$, ... Checking the exponents that are multiples of 21 we find what we expect: $x^{21} = \omega$, $x^{42} = \omega^2$, and $x^{63} = 1$ are all elements of the base field $\mathbb{F}_4$. We can thus choose $x^0, x^1, \ldots, x^{20}$ as generators of the 21 points of $PG(2, 4)$, and we label the point represented by x^s by s. The points are then denoted $0, 1, \ldots, 20$. Since $x^{21} = \omega x^0$ determines the same projective point as x^0, we see that $\tau(s) = s + 1$, with addition modulo 21, defines a regular action on the 21 points of $PG(2, 4)$. ◇

Singer's theorem tells us that the automorphism group $G = \langle\tau\rangle$ acts regularly on the points of the symmetric design $PG(2, q)$. By

Corollary 3.7, G also acts regularly on the blocks. Now Theorem 4.8 implies that G contains a difference set with the same parameters as the design, namely $(q^2+q+1, q+1, 1)$.

We conclude with the generalization of Theorem 8.1 that yields the cyclic (v,k,λ)-difference set with

$$v = \frac{q^{m+1}-1}{q-1}, \quad k = \frac{q^m-1}{q-1}, \quad \lambda = \frac{q^{m-1}-1}{q-1}.$$

We know $PG(m,q)$ gives a symmetric design whose points are the projective points and whose blocks are the projective $(m-1)$-spaces.

Theorem 8.2. *Let q be a prime power. Then the symmetric design of $PG(m,q)$ has an automorphism τ of order $(q^{m+1}-1)/(q-1)$. The cyclic group $G = \langle\tau\rangle$ acts regularly on the points of $PG(m,q)$.*

The proof is essentially the same as that for Theorem 8.1, and it is left for the exercises.

Exercises

1. Carry out Singer's construction of the $(7,3,1)$-difference set by constructing $GF(8) = \mathbb{F}_2[x]/\langle p(x)\rangle$ using the irreducible polynomial $p(x) = x^3+x+1$.

(a) Find $x^0, x^1, \ldots, x^6$ as linear combinations of x^2, x^1, x^0 with coefficients in $\mathbb{F}_2 = \{0,1\}$. Ⓢ

(b) Write the matrix of T_x with respect to the ordered basis (x^2, x^1, x^0) of V. Compare this to the matrix M in Chapter 1. Ⓢ

(c) Identifying the point represented by x^s with the integer $s \in \mathbb{Z}_7$, find the line $B = \{d_0, d_1, d_2\}$ of $PG(2,2)$ containing $d_0 = 0$ and $d_1 = 1$.

(d) How does the difference set $\{d_0, d_1, d_2\}$ compare to the difference set D_1 in Example 1.1?

2. Construct $GF(27)$ as in Exercise 4.12 using $p(x) = x^3+2x+1$. Repeat the previous exercise for $q = 3$ (omitting the references to Chapter 1). In particular, do the following:

(a) Verify that $x^{13} = 2$ and x has order 26 in the multiplicative group $GF(27)^*$. Find $x^0, x^1, \ldots, x^{12}$ as linear combinations of x^2, x^1, x^0 with coefficients in $\mathbb{F}_3 = \{0, 1, 2\}$.

(b) Find the line $B = \{d_0, d_1, d_2, d_3\}$ of $PG(2, 3)$ containing $d_0 = 0$ and $d_1 = 1$.

(c) Compare the difference set $\{d_0, d_1, d_2, d_3\}$ to the one constructed in $\mathbb{Z}_{13}$ in Exercise 4.13 on page 53.

3. In this exercise you will carry out Singer's construction of a $(15, 7, 3)$-difference set in $\mathbb{Z}_{15}$ using $PG(3, 2)$. Construct $GF(16)$ as $\mathbb{F}_2[x]/\langle p(x)\rangle$ for $p(x) = x^4 + x^3 + 1$. Identify powers of x with their representations $ax^3 + bx^2 + cx^1 + dx^0$ written (a, b, c, d). Let τ be the automorphism of $PG(3, 2)$ determined by the linear transformation T_x, and let $G = \langle\tau\rangle$.

(a) Verify that $p(x) = x^4 + x^3 + 1$ is irreducible over $\mathbb{Z}_2$.

(b) Verify the following:

$$\begin{array}{lcllcl} x^5 &=& (1,0,1,1) & x^{10} &=& (1,0,1,0) \\ x^6 &=& (1,1,1,1) & x^{11} &=& (1,1,0,1) \\ x^7 &=& (0,1,1,1) & x^{12} &=& (0,0,1,1) \\ x^8 &=& (1,1,1,0) & x^{13} &=& (0,1,1,0) \\ x^9 &=& (0,1,0,1) & x^{14} &=& (1,1,0,0). \end{array}$$

(c) Let P be the point (1-space) spanned by $x = (0, 0, 1, 0)$, and choose the block (3-space) B spanned by x^1, x^2, x^3. Find the subset D of G consisting of automorphisms mapping P to a point in B.

(d) Confirm that D is a $(15, 7, 3)$ difference set in G.

4. Prove Theorem 8.2. Use the notation in the proof of Theorem 8.1.

8.2. Turyn's construction

In his 1965 paper ([**69**], p. 336) Turyn gave a construction for difference sets in the additive group $G = GF(q) \oplus GF(q)$ where q is a power of 2. His proof is an appealing tour of some of the geometry of the affine plane $GF(q) \times GF(q)$.

Theorem 8.3. *(Turyn) Let $q = 2^h$ for $h > 1$ and let $G = GF(q) \oplus GF(q)$. Let*

$$D = \{(c_1 + c_2, c_1c_2) \mid c_1, c_2 \in GF(q)\}.$$

Then D is a (v, k, λ)-difference set in G with $v = 4n$ and $n = (2^{h-1})^2$.

From this description, the size of the set D is not immediately apparent. Clearly the element $(c_1 + c_2, c_1c_2)$ is the same when the choices of c_1 and c_2 are interchanged. If these were the only repeats, we would have q elements of D with $c_1 = c_2$ and then $q(q-1)/2$ more elements of D corresponding to unordered pairs $\{c_1, c_2\}$ with $c_1 \neq c_2$, for a total of $q(q+1)/2$. In the next example we determine D for the special case $q = 4$.

Example 2. Choose $q = 4$ and $GF(4) = \{0, 1, \omega, \omega^2\}$ with $\omega^2 + \omega + 1 = 0$. In this case $q(q+1)/2 = 10$. Is this the size of D? We list the elements of D below to check:

c_1	c_2	element in D
0	0	$(0, 0)$
0	1	$(1, 0)$
0	ω	$(\omega, 0)$
0	ω^2	$(\omega^2, 0)$
1	1	$(0, 1)$
1	ω	(ω^2, ω)
1	ω^2	(ω, ω^2)
ω	ω	$(0, \omega^2)$
ω	ω^2	$(1, 1)$
ω^2	ω^2	$(0, \omega)$.

We do find that all 10 choices of c_1, c_2 give distinct elements of D. $\diamond$

The proof that this way of determining $|D|$ works in general is left for the exercises. Turyn himself makes a different argument for the size of D. We outline his entire proof below.

Proof. To begin, note two useful properties of the field $GF(q)$ when q is a power of 2, and thus $GF(q)$ has characteristic 2. First, $-x = x$ for every $x \in GF(q)$. Second, $x \mapsto x^2$ is a field automorphism. (The

lack of these special properties is the obstruction to directly extending this argument to odd values of q.)

Recall from Section 2.3 the following properties of the affine plane $GF(q) \times GF(q)$. (These properties hold for any prime power q.) The plane contains q^2 points (x, y). The lines of this affine plane are the point sets satisfying linear equations. A line of slope m for $m \in GF(q)$ has equation $y = mx + b$ for some $b \in GF(q)$. A line of slope denoted ∞ has equation $x = c$ for some $c \in GF(q)$. Each line contains q points. Distinct lines of the same slope are parallel (i.e., pairwise disjoint). Two lines of different slopes meet at a unique point.

Now we again specialize to the case when q is a power of 2. Select one line from each parallel class as follows:

$$\begin{aligned} &\ell_m \text{ has equation } y = mx + m^2 \quad \text{for } m \in GF(q), \\ &\ell_\infty \text{ has equation } x = 0. \end{aligned}$$

See Figure 8.1 for an illustration of these lines when $q = 4$. Observe that for each $\mu \in GF(q) \cup \{\infty\}$, the points in ℓ_μ are contained in D. Further, each point of D lies on exactly two of the $q+1$ lines ℓ_μ. These two observations tell us that $k = |D| = q(q+1)/2 = 2^{h-1}(2^h + 1)$. (Notice that this agrees with the count preceding Example 2.)

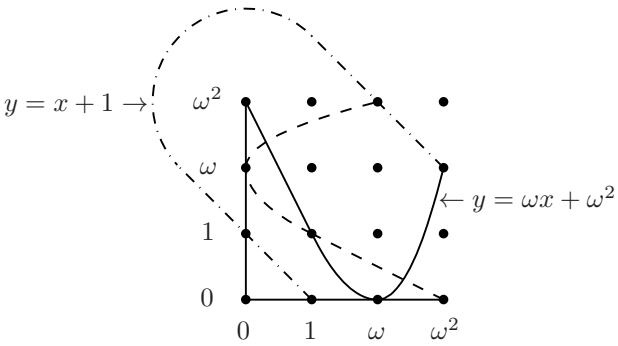


Figure 8.1. Lines from Turyn construction, $q = 4$

We need to show that D is a difference set in G. First observe that for a non-identity element $a \in G$, $a = d_1 - d_2$ for $d_1, d_2 \in D$ if and only if $d_1 = a + d_2 \in D \cap (a + D)$. Therefore, to verify that each

non-identity element of G appears the same number of times in the multiset of differences of distinct elements of D, it is sufficient to show that $|D \cap (a + D)|$ is independent of the choice of the non-identity element $a \in G$. To show this independence, we will make use of the lines in D and calculate $|\ell_\mu \cap (a + \ell_\mu)|$ for each μ.

To make this calculation, it is useful to assign a *slope* to a *point*. We say a point $a = (a_1, a_2) \neq (0, 0)$ has slope m if $a_1 \neq 0$ and $a_2 = ma_1$, and we say it has infinite slope if $a_1 = 0$.

We make the following observations:

(i) If $a \neq (0, 0)$ has slope μ then $a + \ell_\mu = \ell_\mu$.

(ii) For all $a \in G$, $a + \ell_\mu$ is a line of slope μ, but $a + \ell_\mu = \ell_\mu$ for $a \neq (0, 0)$ only if a has slope μ.

(iii) Suppose $a \neq (0, 0)$ is a point of slope not equal to μ. Then ℓ_μ and $a + \ell_\mu$ are disjoint.

Choose $a \in G$, $a \neq (0, 0)$. Suppose a has slope μ. Choose a slope $\gamma \neq \mu$. We know $a + \ell_\gamma$ is a line $\ell'_\gamma \neq \ell_\gamma$ and therefore not equal to any of the selected ℓ_β. We claim ℓ'_γ contains exactly $q/2$ points of D. To see why, first observe that ℓ'_γ intersects ℓ_β for each of the q choices of $\beta \neq \gamma$. Since each point of D lies on *two* of these lines, we get only $q/2$ points of D on ℓ'_γ.

We are ready to count the size of $D \cap (a + D)$. Since a has slope μ, we get q points in the intersection from $a + \ell_\mu = \ell_\mu \subset D$. Now we have q choices for $\gamma \neq \mu$, and each choice of γ gives $q/2$ points of D from $a + \ell_\gamma = \ell'_\gamma$. This gives $q + q(q/2)$ points. However, since each point of D is on *two* of the lines ℓ_β, this double-counts the size of $D \cap (a + D)$. Our conclusion is

$$\Big|D \cap (a + D)\Big| = \left(\frac{1}{2}\right)\left(q + \frac{q^2}{2}\right) = \frac{q^2 + 2q}{4} = 2^{h-1}(2^{h-1} + 1).$$

Since $|D \cap (a + D)|$ is thus independent of the choice of a, our proof is complete. □

Exercises

5. This exercise concerns Turyn's construction for $q = 4$, with $GF(4) = \{0, 1, \omega, \omega^2\}$ where $1 + \omega + \omega^2 = 0$. Refer to Example 2 for a list of the elements of D.

(a) What are the parameters of this difference set?

(b) List the elements of ℓ_m for each $m \in GF(4)$. Also list the elements of ℓ_∞. Ⓢ

(c) Verify that each of these five lines is a subset of D and that each element of D lies on two of these lines.

6. In general, what are the parameters of the difference set in Theorem 8.3 in terms of h?

7. Assume q is a power of 2. Show that if $(c + d, cd) = (a + b, ab)$ for $a, b, c, d \in GF(q)$, then either $c = d = a = b$ or the 2-sets $\{a, b\}$ and $\{c, d\}$ are equal. (This gives another argument for $k = q(q + 1)/2$ in Turyn's construction.)

8. Complete the arguments in the proof of Theorem 8.3 as follows:

(a) Show $\ell_\mu \subset D$ for each $\mu \in GF(q) \cup \{\infty\}$.

(b) Show each point of D is on exactly two lines ℓ_μ.

(c) Verify observation (i).

(d) Verify observation (ii).

(e) Verify observation (iii).

8.3. McFarland difference sets

The first two constructions in this chapter produced difference sets in very specific types of abelian groups. In contrast, this next construction produces difference sets in groups with much less restrictive structure and provides our first family of non-abelian difference sets. McFarland's paper "A Family of Difference Sets in Non-cyclic Groups" [**50**] is exceptionally readable. We follow it closely and even

quote from it. In this paper McFarland constructs difference sets with parameters

$$v = q^{s+1}\left(\frac{q^{s+1}-1}{q-1}+1\right), \quad k = q^s\left(\frac{q^{s+1}-1}{q-1}\right), \quad \lambda = q^s\left(\frac{q^s-1}{q-1}\right).$$

McFarland's construction begins with a vector space V of dimension $s+1$ over a finite field $\mathbb{F} = GF(q)$, where s is a positive integer. Write

$$r = \frac{q^{s+1}-1}{q-1}.$$

We know from Theorem 2.16 that r is both the number of 1-spaces in V and also the number of hyperplanes in V. Let $H_1, \ldots, H_r$ be the hyperplanes of V. Let E denote the additive group of V, and regard each H_j as a subgroup of E. Here is the surprising part: choose for K *any* group of order $r+1$. Let $G = E \times K$. Note that if K is chosen non-abelian, G will be non-abelian.

Now we define $D \subset G$. Choose r distinct elements $k_1, \ldots, k_r$ in K. Choose r not necessarily distinct elements $e_1, \ldots, e_r$ in E. Write $(H_i + e_i, k_i)$ for the coset of $H_i \times 1_K$ in G with coset representative (e_i, k_i). We set D equal to the union of these cosets:

$$D = \bigcup_{i=1}^{r} \{(h + e_i, k_i) \mid h \in H_i\}.$$

Theorem 8.4. *(McFarland,* [**50**]*) Define the group G, the set D, and the parameters v, k, λ as above. Then D is a (v, k, λ)-difference set in G.*

Proof. We will show $D^{(-1)}D = (k-\lambda)1_G + \lambda G$ in $\mathbb{Z}G$.[1] We begin with the following observations about multisets in the group E:

(i) The multiset $H_1 \cup \cdots \cup H_r$ contains the identity of E (i.e., the zero vector of V) exactly r times, and contains each non-identity element of E exactly $(q^s-1)/(q-1)$ times.

(ii) For $i = 1, \ldots, r$, each element of H_i appears q^s times in $H_i + H_i = \{a + b \mid a, b \in H_i\}$.

[1] We write $D^{(-1)}$ on the left because McFarland does. We know from Theorem 4.9 that it doesn't matter which side we put the inverse on.

(iii) If $i \neq j$, then $x \in E$ appears q^{s-1} times in $H_i + H_j = \{a + b \,|\, a \in H_i, b \in H_j\}$.

Now we change notation and write all of our group operations multiplicatively, with identities 1_E, 1_K and 1_G in E, K, G respectively, reserving addition for the integral group ring. In this notation $D \in \mathbb{Z}G$ can be written $D = \sum_i H_i e_i k_i$ and the observations (i)–(iii) above can be rewritten in $\mathbb{Z}E$ as follows:

(i) $$H_1 + \cdots + H_r = r\,1_E + \left(\frac{q^s - 1}{q - 1}\right)(E - 1_E)$$
$$= q^s 1_E + \left(\frac{q^s - 1}{q - 1}\right) E.$$

(ii) $H_i H_i = q^s\, H_i$.

(iii) For $i \neq j$, $H_i H_j = q^{s-1}\, E$.

We depart slightly from McFarland's notation (in order to reserve k for the size of D) and write $K = \{k_0, k_1, \ldots, k_r\}$. However when we sum over i, it is for $i = 1, \ldots, r$. Here is what McFarland writes to complete the argument:

$$\begin{aligned}
\text{“}D^{(-1)}D &= \left(\sum_i H_i\, e_i^{-1} k_i^{-1}\right)\left(\sum_j H_j\, e_j k_j\right) \\
&= \sum_i H_i^2\, 1_K \;+\; \sum_{i \neq j} H_i H_j\, e_i^{-1} e_j k_i^{-1} k_j \\
&= q^s \sum_i H_i\, 1_K \;+\; q^{s-1} \sum_{i \neq j} (E\, e_i^{-1} e_j)(k_i^{-1} k_j) \\
&= q^{2s}\, 1_E\, 1_K \;+\; q^s \left(\frac{q^s - 1}{q - 1}\right) E\, 1_K \\
&\qquad\qquad + \; q^s \left(\frac{q^s - 1}{q - 1}\right) E\,(K - 1_K) \\
&= q^{2s}\, 1_G \;+\; q^s \left(\frac{q^s - 1}{q - 1}\right) G.
\end{aligned}$$

Thus D is a difference set in the group $G = E \times K$ with the parameters [given above]." □

McFarland's paper contains two other interesting results. He shows that when q is odd, his construction produces at least $(q^s+1)/2$ inequivalent difference sets in the same group. He also shows that for $q = 5$ and $s = 2$ he gets a difference set which has minus one as a multiplier. He writes, "this is the first (and so far only) example of a difference set having minus one as a multiplier which is *not* a Hadamard difference set." A Hadamard difference set is one with $v = 4n$; we discuss these in Section 9.3. When $q = 2$, McFarland's construction gives a Hadamard difference set. The Turyn construction in the previous section also gives difference sets in the Hadamard family.

Exercises

9. Verify the first three observations in the proof of Theorem 8.4 as follows:

(a) Verify statement (i). Ⓢ

(b) Verify statement (ii).

(c) Verify statement (iii).

10. Verify that the $\mathbb{Z}E$ versions of the three statements in the preceding exercise are as claimed.

11. Let $K = \{k_0, k_1, \ldots k_r\}$ and $1 \le i, j \le r$, and verify that

$$\sum_{i \neq j} k_i^{-1} k_j = (r-1)(K - 1_K). \qquad \text{Ⓗ}$$

12. Verify the equations quoted on p. 131 from McFarland [**50**].

13. Carry out McFarland's construction with $q = 2$ and $s = 2$ as follows:

(a) Choose K abelian and choose $k_0 = 1_K$.

(b) Choose K non-abelian and choose $k_0 = 1_K$.

14. Carry out McFarland's construction with $q = 5$ and $s = 1$. Choose $k_0 = 1_K$.

15. Look up Dillon's generalization of McFarland's construction [**18**]. Give a specific example of a group to which Dillon's construction applies, but McFarland's does not.

Coda

The three constructions in this chapter use geometry in different ways to produce infinite families of difference sets in groups of varying kinds. Not only do these constructions address the existence question, but they also exemplify the interweaving of group theory, geometry (projective, affine and linear) and combinatorics.

In the first construction, Singer identifies a vector space V of dimension $m+1$ over the finite field $GF(q)$ with the field $GF(q^{m+1})$. He uses this identification to construct a cyclic subgroup of order $(q^{m+1}-1)/(q-1)$ acting regularly on the symmetric design defined by the points and projective $(m-1)$-spaces of the projective space $PG(m,q)$ coming from V. We see the Singer family of cyclic difference sets again in the next chapter because when q is a power of 2, the parameters of the Singer difference set have the special "Paley-Hadamard" relationship $v = 4n-1$. We also see these difference sets in Chapter 13, where they are used to produce binary sequences with useful properties.

Turyn's construction gives a difference set D in the non-cyclic abelian 2-group $GF(q) \oplus GF(q)$ for $q = 2^h$ and $h > 1$. Although Turyn's description of the elements of D is purely algebraic, his proof that D is a difference set involves an analysis of the affine plane $GF(q) \times GF(q)$, including careful counting.

For the third construction, McFarland, like Singer, begins with a vector space V over a finite field. However, McFarland exploits the vector space structure directly, using the r hyperplanes (subspaces) of V to construct a difference set in $G = E \times K$, where E is the additive group of V and K is *any* group of order $r+1$, so G can be

non-abelian. McFarland's construction was subsequently generalized by Dillon in [**18**]. When $q = 2$, the McFarland difference sets have parameters satisfying the special "Hadamard" relationship $v = 4n$, so they reappear in the next chapter.

Chapter 9

Families from Hadamard Matrices

Some important and intriguing families of symmetric designs and difference sets are linked to Hadamard matrices. In Section 1 we introduce Hadamard matrices. In Section 2 we study the family of $(4n-1, 2n-1, n-1)$-difference sets associated with Hadamard matrices, including the quadratic residue sets from Chapter 4. In Section 3 we examine (v, k, λ)-difference sets with $v = 4n$, which are related to special Hadamard matrices. In addition, we briefly revisit constraints on abelian difference sets in this second family and some surprising results in non-abelian groups. In Chapter 13 we see an application of some difference sets from these families.

9.1. Hadamard matrices

Hadamard matrices are special square matrices with entries ± 1. Hadamard originally studied them while trying to find the maximum absolute value for the determinant of a square matrix with complex entries h_{ij} satisfying $|h_{ij}| \leq 1$.

Definition. A Hadamard matrix of order m is an $m \times m$ matrix with entries ± 1 satisfying

$$HH^T = mI_m.$$

An immediate consequence is that $H^T H = mI_m$. The entries along the diagonal of HH^T (and of $H^T H$) are simply sums of m squares 1^2 and $(-1)^2$. The zeroes off the diagonal mean that each pair of rows (and each pair of columns) is orthogonal in $\mathbb{R}^m$ (or in $\mathbb{C}^m$).

Example 1. Here are four small Hadamard matrices:

$$H_1 = [1] \qquad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_3 = \begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad H_4 = \begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix}. \quad \diamond$$

If we permute the rows or columns of a Hadamard matrix, or if we multiply any row or column by -1, we get another Hadamard matrix. By repeatedly applying these operations to any Hadamard matrix, we can obtain one whose first row and first column consist entirely of $+1$'s.

Definition. Two Hadamard matrices are equivalent if we can obtain one from the other by a series of operations of permuting rows or columns or multiplying a row or column by -1. A Hadamard matrix is normalized if it contains only $+1$'s in its first row and first column.

If we choose a positive integer m, does a Hadamard matrix of order m exist? It is relatively easy to prove the following necessary condition on m.

Theorem 9.1. *If H is a Hadamard matrix of order m, then $m = 1$, $m = 2$, or $m \equiv 0 \,(mod\ 4)$.*

It is also believed that these conditions are sufficient.

Conjecture: If $m \equiv 0 \,(\mathrm{mod}\ 4)$, then there exists a Hadamard matrix of order m.

Lander [**43**] reported in 1983 that this conjecture was known to be true for $m \leq 264$; that is, the first unknown case at that time was

$m = 268$. In 1992 VanLint and Wilson [**70**] reported that the first unknown case was $m = 428$.

In trying to prove this conjecture, people have developed techniques for constructing Hadamard matrices. We examine some constructions via difference sets in the next two sections, but for now, we note the following example. In Section 2 we prove that this construction always produces a Hadamard matrix.

Example 2. Our goal is a Hadamard matrix H of order $p+1$ for a prime $p \equiv 3 \pmod 4$. Let D be the difference set of nonzero squares mod p, and let A be the incidence matrix for dev$D$. We replace each zero by -1 to obtain a matrix we call A^*. Label the rows and columns with $0, 1, \cdots p-1$. Then our description of A^* is equivalent to defining its entries by $a_{ij} = +1$ if $j \in i + D$ and -1 otherwise. (Equivalently, $a_{ij} = +1$ if $(j-i) \in D$ and -1 otherwise.) Next we attach a first row and first column of $+1$'s to A^* to produce H. The example below is for $p = 7$ and $D = \{1, 2, 4\}$:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix}. \qquad \diamond$$

To construct larger Hadamard matrices from smaller ones we define the following matrix product.

Definition. Suppose A is an $m \times n$ matrix and B is $r \times c$. The Kronecker product of these matrices, denoted $A \otimes B$, consists of mn blocks, where the i, j block is $a_{ij}B$:

$$A \otimes B \quad = \quad \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}.$$

Example 3. Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Then

$$A \otimes B = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \\ 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & 4 \end{bmatrix}.$$

◇

Theorem 9.2. *If H_1 and H_2 are Hadamard matrices, then $H_1 \otimes H_2$ is a Hadamard matrix.*

In the next two sections we study the close connections between Hadamard matrices and two families of symmetric designs. For the second family we need to limit ourselves to a particular type of Hadamard matrix.

Definition. A regular Hadamard matrix is a Hadamard matrix having all its row and column sums equal.

Of the matrices in Example 1, only H_1 and H_4 are regular. Note that a normalized Hadamard matrix of order greater than 1 is not regular. Indeed, regularity is not preserved by multiplying a row or a column by -1, so the notion of equivalence does not apply to regular Hadamard matrices.

The next two theorems, which are restated as Theorems 9.3 and 9.8 and proved in Sections 2 and 3 respectively, make explicit the link between symmetric designs with special parameters and Hadamard matrices.

Theorem. *A symmetric $(4n-1, 2n-1, n-1)$ design exists if and only if a Hadamard matrix of order $4n$ exists.*

Theorem. *A symmetric (v, k, λ) design with $v = 4n$ exists if and only if a regular Hadamard matrix of order $4n$ exists.*

We say difference sets with parameters $(4n-1, 2n-1, n-1)$ are in the Paley-Hadamard family. We call (v, k, λ)-difference sets with $v = 4n$ Hadamard difference sets.[1]

[1] Some authors use the less confusing name *Menon difference sets* when $v = 4n$. We use the more common, albeit somewhat confusing, name above.

Exercises

1. Prove that if H is an $m \times m$ Hadamard matrix, then $H^T H = mI_m$.

2. Show that matrix H_3 in Example 1 is equivalent to the normalized matrix

$$H_5 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

3. Verify that the 8×8 matrix in Example 2 is a Hadamard matrix.

4. This exercise, based on [**28**], yields a proof that if a Hadamard matrix of order m exists for $m > 2$, then m is a multiple of 4. (Similar arguments are used in the proofs of Theorems 9.3 and 9.8.) Suppose that H is a normalized Hadamard matrix of order $m > 2$. Assume further that the second and third rows of H have $+1$s in the first x columns. Also assume the second row has $+1$s in the next y columns, while the third row has -1s in those y columns, with the reverse in the next z columns: -1s in the second row, $+1$s in the third row. Finally assume both the second and third rows have -1s in the last w columns. Schematically the second and third rows would look like this:

$$\overbrace{+\cdots+}^{x}\overbrace{+\cdots+}^{y}\overbrace{-\cdots-}^{z}\overbrace{-\cdots-}^{w}$$
$$\underbrace{+\cdots+}_{x}\underbrace{-\cdots-}_{y}\underbrace{+\cdots+}_{z}\underbrace{-\cdots-}_{w} \quad .$$

(a) Explain why there is no loss of generality in making the assumptions above.

(b) Explain why x, y, z and w satisfy the following equations:

$$\begin{aligned} x + y + z + w &= m, \\ x + y - z - w &= 0, \\ x - y + z - w &= 0, \\ x - y - z + w &= 0. \end{aligned}$$

Ⓢ

(c) Solve the system of equations in (b) to obtain $x = y = z = w = m/4$.

5. Examine the properties of the Kronecker product. Is it defined for any pair of matrices? Is the operation commutative? associative? Does this operation have an identity? inverses?

6. Verify the following properties of the Kronecker product:

(a) $(aA) \otimes (bB) = ab(A \otimes B)$ for any matrices A, B and any scalars a, b.

(b) $(A \otimes B)^T = A^T \otimes B^T$ for any matrices A, B.

(c) The Kronecker product of identity matrices is again an identity matrix: $I_m \otimes I_n = I_{mn}$.

(d) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$ where matrices A and C are $m \times m$ and B and D are $n \times n$. (Use block multiplication for matrices as follows: if P_{ij} and Q_{ij} are $n \times n$ matrices for $i, j = 1, \ldots, m$ and P and Q are $nm \times nm$ with blocks P_{ij} and Q_{ij} respectively, then PQ is $nm \times nm$ with blocks $\sum_{j=1}^{m} P_{ij}Q_{jk}$.)

7. Let $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Compute $H \otimes H$ and show that this is a Hadamard matrix. Now compute $H \otimes (H \otimes H)$ and show that this is a Hadamard matrix.

8. Prove Theorem 9.2.

9. If H_1 and H_2 are regular Hadamard matrices, is $H_1 \otimes H_2$ a regular Hadamard matrix? If not, give a counter-example. If yes, provide a proof.

10. Assume that H is a regular Hadamard matrix. Show that the number of $+1$s in each row and in each column is a constant.

11. Recall that the original motivation for defining Hadamard matrices was the search for the maximum absolute value of the determinant of a square matrix whose complex entries are in absolute value no greater than 1. What is the determinant of a Hadamard matrix of order m?

12. Trace the progress of the Conjecture on existence of Hadamard matrices. Find a paper after 1983 that improves on the result reported by Lander. Find a more recent result than reported in 1992. Try to find results in refereed journals.

9.2. Paley-Hadamard family: $v = 4n - 1$

In this section we focus on the Paley-Hadamard family of difference sets with the parameters $(4n-1, 2n-1, n-1)$. Baumert ([**5**], p. 90) notes that these difference sets have been extensively studied for reasons including the following:

- They are relatively abundant. (In this section we see four families within this larger family: Paley, Singer for suitable q, twin prime powers, and a family due to Hall.)
- If a nontrivial (v, k, λ)-difference set exists with $k < v/2$, then $1 \leq \lambda \leq (v-3)/4$. "Thus planar difference sets and [Paley-]Hadamard difference sets present the extreme values of λ."
- They have led to several digital communications applications by means of associated "autocorrelation functions". (We discuss these in Chapter 13.)
- The existence of such difference sets casts light on the existence of Hadamard matrices.

We make the link to Hadamard matrices explicit with the following theorem.

Theorem 9.3. *A symmetric* $(4n-1, 2n-1, n-1)$ *design exists if and only if there exists a Hadamard matrix of order* $4n$.

Proof. First, assume H is a Hadamard matrix of order $4n$. Recall that we can multiply a row or a column by -1 without changing the

values of $H^T H$ or HH^T, so we may assume without loss of generality that our matrix has been normalized and the first column and first row of H consist entirely of $+1$s.

Let M be the $(4n-1) \times (4n-1)$ matrix obtained by deleting the first row and first column of H. Let A be the matrix obtained from M by replacing -1 by 0 wherever it occurs. Then A is the incidence matrix of an incidence structure with $+1$ in row i and column j if and only if the ith block contains the jth point. We will show that A is the incidence matrix of a symmetric $(4n-1, 2n-1, n-1)$ design.

Because the rows of H are orthogonal, the number of $+1$s in each row of H after the first must be $2n$, so the number of $+1$s in each row of M must be $2n-1$. By Exercise 1, the number of $+1$s in each column of M is also $2n-1$. Thus the structure with incidence matrix A has $k = 2n-1$ points per block and k blocks per point. Further, because the dot product of two rows of H is 0, the dot product of two rows of M must be -1.

Now consider two rows of M (chosen arbitrarily). We want to show that the number of $+1$s these rows have in common is $n-1$. To do that, we set up notation to count the numbers of columns in which:

x: both rows have $+1$,

y: the first row has $+1$ and the second -1,

z: the first row has -1 and the second $+1$,

w: both rows have -1.

By permuting columns appropriately, we can assume that schematically the two rows look like the following. For economy of notation, we write $+$ and $-$ instead of $+1$ and -1,

$$\begin{array}{cccc} \overbrace{+\cdots+}^{x} & \overbrace{+\cdots+}^{y} & \overbrace{-\cdots-}^{z} & \overbrace{-\cdots-}^{w} \\ \underbrace{+\cdots+}_{x} & \underbrace{-\cdots-}_{y} & \underbrace{+\cdots+}_{z} & \underbrace{-\cdots-}_{w} \end{array} .$$

Using what we know about M, we have the following equations in the variables x, y, z, w:

$$\begin{aligned} x + y + z + w &= 4n - 1, \\ x + y &= 2n - 1, \\ x + z &= 2n - 1, \\ x - y - z + w &= -1. \end{aligned}$$

Solving these equations yields $y = z = w = n$ and $x = n - 1$. In particular, two distinct blocks have exactly $\lambda = n - 1$ points in common. By the redundancy of the axioms for a symmetric design, it follows that A is the incidence matrix of a symmetric $(4n - 1, 2n - 1, n - 1)$ design.

For the converse, assume $\mathcal{D}$ is a symmetric $(4n - 1, 2n - 1, n - 1)$ design and A is its incidence matrix. Let M be the matrix obtained from A by replacing 0s by -1s. Let H be the $4n \times 4n$ matrix obtained from M by adding an initial row and an initial column of $+1$s. We claim H is Hadamard of order $4n$. Choose two rows of M and define x, y, z, w as above. The properties of A imply

$$\begin{aligned} x + y + z + w &= 4n - 1, \\ x &= \lambda = n - 1, \\ x + y &= k = 2n - 1, \quad \text{so } y = n, \\ x + z &= k = 2n - 1, \quad \text{so } z = n. \end{aligned}$$

It follows that $w = n$, so we have

$$x = n - 1 \quad \text{and} \quad y = z = w = n.$$

To find HH^T we need to calculate the dot product of any two rows of H. First we calculate the dot product of the two rows of H described above and for which we have the values:

$$1 + x - y - z + w = 1 + (n - 1) - n - n + n = 0.$$

We also need to find the dot product of one of these rows with the first row of H consisting entirely of $+1$s:

$$1 + x + y - z - w = 0.$$

What about the diagonal entries of HH^T? The square of each entry in H is 1, so the dot product of any row of H with itself is $4n$. Therefore we have $HH^T = 4nI_{4n}$, and H is a Hadamard matrix. □

Remark: The existence of a Hadamard matrix of order $4n$ implies that a symmetric design with parameters $(4n-1, 2n-1, n-1)$ exists. It does not imply that a difference set with these parameters necessarily exists. For example, for $n = 10$ there indeed exists a symmetric design with parameters $(39, 19, 9)$. However, an analysis of possible intersection numbers in Exercise 7.6 shows that a $(39, 19, 9)$-difference set cannot exist.

The Paley family. We know that for q a prime power and $q \equiv 3 \pmod 4$, the nonzero squares in the finite field $GF(q)$ form a difference set in the additive group of $GF(q)$ with parameters $(q, (q-1)/2, (q-3)/4)$. We call these difference sets the Paley family. Since $n = k - \lambda = (q+1)/4$, the parameters of the corresponding symmetric design are $(4n-1, 2n-1, n-1)$. By Theorem 9.3, each Paley difference set leads to a Hadamard matrix of order $4n$. The origin of these ideas, in matrix form, goes back to Paley in 1933 [**57**].[2]

Several authors have studied subsets of a finite field obtained by raising nonzero elements to the eth power,[3] for e having a value other than 2. In certain circumstances fourth powers and eighth powers give difference sets in the additive group of $GF(q)$. See Theorems 4.4 and 4.5 and Example 6.11 for examples with $q \equiv 1 \pmod 4$. Nonzero squares have also been studied in $GF(q)$ for $q \equiv 1 \pmod 4$. The result is a weaker version of a difference set called a partial difference set.

Definition. A subset D of a group G is called a partial difference set with parameters (v, k, λ, μ) if $|G| = v$, $|D| = k$, every non-identity element of D appears λ times in the multiset Δ of "differences" of distinct elements of D, and every non-identity element of $G \setminus D$ appears μ times in Δ. When $\lambda = \mu$, D is a difference set.

[2] The existence of this infinite Paley family is the source of the name Paley-Hadamard for the larger family of all $(4n-1, 2n-1, n-1)$-difference sets.

[3] Difference sets consisting of eth powers of elements of a finite field are sometimes called *cyclotomic* or *residue difference sets*.

When D is the set of nonzero squares in $G = GF(q)$ for $q \equiv 1 \pmod 4$, we find that D is a partial difference set with parameters $v = q$ and $k = (q-1)/2$, $\lambda = (q-5)/4$, and $\mu = (q-1)/4$.

The Singer family. We know that the lines and hyperplanes of a $(m+1)$-dimensional vector space over the finite field $GF(q)$ are the points and blocks of a symmetric (v, k, λ) design where

$$v = \frac{q^{m+1}-1}{q-1}, \quad k = \frac{q^m - 1}{q-1}, \quad \text{and} \quad \lambda = \frac{q^{m-1}-1}{q-1}.$$

From Singer's construction in Chapter 8, we also know that a cyclic group of order v acts regularly on this design, giving us a difference set with these parameters. In the special case when $q = 2$ we have $n = 2^{m-1}$ and thus $v = 4n - 1$, $k = 2n - 1$ and $\lambda = n - 1$.

Note that a Singer difference set gives the same parameters as a quadratic residue difference set in $GF(q')$ if and only if $q' = 2^{m+1} - 1$. In the cyclic case, q' is prime, and primes of this form are called *Mersenne primes*. It can be shown ([**8**], p. 362) that for $m > 2$, the developments of the Singer and the Paley difference sets are not isomorphic designs, so the difference sets themselves are not equivalent. Many authors have studied the construction of difference sets that have the classical Singer parameters but are not equivalent to a Singer difference set. We do not consider this question in generality, but we do examine a special case in Exercise 17.[4]

The twin prime powers family. Whenever q and $q+2$ are odd prime powers, a twin prime powers difference set exists in the additive group G of the ring $R = GF(q) \oplus GF(q+2)$. Note that G is cyclic if and only if q and $q+2$ are primes. We saw a special case of this construction in Chapter 3. Discovery of this family is credited to Stanton and Sprott in 1958 ([**66**]), but Baumert ([**5**], p. 131) says these difference sets were also independently discovered by Menon [**55**], A. Brauer (1953), Chowla (1945), and "perhaps first" by Gruner (1939).

Assume q and $q+2$ are odd prime powers. Let R be the ring

$$R = GF(q) \oplus GF(q+2) = \Big\{ (a, b) \mid a \in GF(q), b \in GF(q+2) \Big\},$$

[4]For a general survey, see [**8**], Section 17 of Chapter VI.

with addition and multiplication defined component-wise:

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2)\\ (a_1, b_1)(a_2, b_2) &= (a_1 a_2, b_1 b_2).\end{aligned}$$

To keep track of squares and non-squares in a field $\mathbb{F}$, we define the function χ on $\mathbb{F}$ by

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0\\ 1 & \text{if } a \text{ is a square in } \mathbb{F}^*\\ -1 & \text{if } a \text{ is a non-square in } \mathbb{F}^*\end{cases}$$

where $\mathbb{F}^*$ is the multiplicative group of nonzero elements of $\mathbb{F}$. The function χ restricted to $\mathbb{F}^*$ defines a homomorphism from $\mathbb{F}^*$ to the subgroup $\{1, -1\}$ of $\mathbb{F}^*$. Thus in a finite field with an odd number of elements, we see again that exactly half the nonzero elements are squares.

We can now state the theorem for twin prime powers difference sets.

Theorem 9.4. *Assume q and $q + 2$ are odd prime powers, and let G be the additive group of the ring $R = GF(q) \oplus GF(q + 2)$. Define $D \subset G$ as follows:*

$$D = \Big\{(a, b) \in G \mid \chi(a)\chi(b) = 1\Big\} \cup \Big\{(a, 0) \mid a \in GF(q)\Big\}.$$

Then D is a $(4n - 1,\, 2n - 1,\, n - 1)$-difference set in G.

Proof. Notice that $q \equiv 1 \pmod 4$ if and only if $q + 2 \equiv 3 \pmod 4$. This tells us two useful things.

- First, $v = q(q+2) \equiv 3 \pmod 4$, so we may write $v = 4N-1$ for some positive integer N.
- Second, -1 is a square in $GF(q)$ if and only if -1 is a non-square in $GF(q + 2)$. (See A.17.)

We see that the cardinality of D is

$$k = \left(\frac{q-1}{2}\right)\left(\frac{q+1}{2}\right) + \left(\frac{q-1}{2}\right)\left(\frac{q+1}{2}\right) + q = \frac{v-1}{2} = 2N - 1.$$

To make the argument that D is a difference set, it is helpful to define the set M,

$$M = \{(a, b) \in D \mid b \neq 0\}.$$

By the second observation above, $(-1, -1)$ is not in M. It is straightforward to check that M is a group under the ring multiplication. Also notice that $MD = D$, where by MD we mean the set of all products mx for $m \in M$ and $x \in D$. Now we use M to define an equivalence relation on G by

$$(a, b) \sim (c, d) \text{ if there exists } m \in M \text{ with } m(a, b) = (c, d).$$

There are five equivalence classes in G:

$$\begin{aligned}
\mathcal{S}_1 &= \{(a, b) \mid \chi(a)\chi(b) = 1\}, \\
\mathcal{S}_2 &= \{(a, b) \mid \chi(a)\chi(b) = -1\}, \\
\mathcal{S}_3 &= \{(a, 0) \mid a \neq 0\}, \\
\mathcal{S}_4 &= \{(0, b) \mid b \neq 0\}, \\
\mathcal{S}_5 &= \{(0, 0)\}.
\end{aligned}$$

We observe that $|\mathcal{S}_1| = |\mathcal{S}_2| = (q - 1)(q + 1)/2$, $|\mathcal{S}_3| = q - 1$, and $|\mathcal{S}_4| = q + 1$. Also notice that $D = \mathcal{S}_1 \cup \mathcal{S}_3 \cup \mathcal{S}_5$.

Let Δ be the multi-set of differences of distinct elements of D. For a non-identity group element (a, b), we have $(a, b) = x_1 - x_2$ for $x_1, x_2 \in D$ if and only if $m(a, b) = mx_1 - mx_2$ for $m \in M$. This tells us that each non-identity group element in class $\mathcal{S}_j$ occurs the same number of times in Δ, say λ_j times, for $j = 1, \ldots, 4$. The heart of the proof is showing $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4$; the common value is λ.

First we show $\lambda_1 = \lambda_2$. Since $(-1, -1) \notin M$, $(a, b) \in \mathcal{S}_1$ if and only if $(-a, -b) \in \mathcal{S}_2$. Since $(a, b) = x_1 - x_2$ exactly when $(-a, -b) = x_2 - x_1$, we conclude that $\lambda_1 = \lambda_2$.

Next we determine λ_3. First we count differences $(a_1, b) - (a_2, b)$ for $a_1 \neq a_2$ and a_1, a_2, b nonzero. There are $q + 1$ choices for $b \in GF(q+2)$, $b \neq 0$; $(q-1)/2$ choices for $a_1 \in GF(q)$ with $\chi(a_1) = \chi(b)$; and $(q - 3)/2$ choices for $a_2 \in GF(q)$ with $\chi(a_2) = \chi(b)$ and $a_2 \neq a_1$. Thus there are $(q+1)(q-1)(q-3)/4$ differences like this. Second we count differences $(a_1, 0) - (a_2, 0)$ with $a_1 \neq a_2$. There are q choices for a_1 and $q - 1$ choices for $a_2 \neq a_1$, so there are $q(q - 1)$ differences

like this. Since there are $q-1$ choices for $(a,0) \in \mathcal{S}_3$, each appearing the same number of times in Δ, we have

$$\lambda_3 = \left(\frac{1}{q-1}\right)\left[\left(\frac{(q+1)(q-1)(q-3)}{4}\right) + q(q-1)\right].$$

This expression for λ_3 can be simplified to give

$$\lambda_3 = \frac{v-3}{4} = N-1.$$

A similar argument shows that $\lambda_4 = N-1 = \lambda_3$.

Since the size of the multiset Δ is $k(k-1)$, we have

$$k(k-1) = \sum_{j=1}^{4} |\mathcal{S}_j|\lambda_j.$$

Using $k = (v-1)/2$ and the sizes noted above for the classes $\mathcal{S}_j$ gives $k(k-1) = ((v-1)/2)((v-3)/2) =$

$$(q-1)\left(\frac{q+1}{2}\right)\lambda_1 + (q-1)\left(\frac{q+1}{2}\right)\lambda_2 + (q-1)\lambda_3 + (q+1)\lambda_4.$$

Because $\lambda_1 = \lambda_2$ and $\lambda_3 = \lambda_4 = (v-3)/4$, when we solve for λ_1 we find λ_1 also equals $(v-3)/4$, so we have $\lambda = (v-3)/4 = N-1$, completing the verification that D is a $(4n-1, 2n-1, n-1)$-difference set in G (with $N = n$). □

The Hall family. In Chapter 6 we found difference sets by forming unions of orbits of multipliers. We now consider some work of Marshall Hall, who constructed difference sets in the additive group of a finite field by using special orbits. The following example introduces some of Hall's ideas.

Example 4. Consider the search for a $(19, 9, 4)$-difference set D in $GF(19)$. By Theorem 6.1, we know that 5 is a numerical multiplier for D. We also know that the multiplicative group $GF(19)^*$ is cyclic, and it is straightforward to check that $\omega = 3$ is a generator and $\omega^4 = 5$. In this language, we say that ω^4 is a multiplier for D; further, each element of the cyclic group $\langle\omega^4\rangle = \{1, \omega^4, \omega^8, \omega^{12}, \omega^{16}, \omega^{20} = \omega^2, \omega^6, \omega^{10}, \omega^{14}\}$ is a multiplier for D. We can also use powers of

ω (and some notation due to Hall) to write out both orbits of the multiplier ω^4 in $GF(19)^*$:

$$\mathcal{C}_0 = \{1, \omega^4, \omega^8, \omega^{12}, \omega^{16}, \omega^{20} = \omega^2, \omega^6, \omega^{10}, \omega^{14}\} \quad \text{(orbit of } \omega^0\text{)},$$
$$\mathcal{C}_1 = \{\omega, \omega^5, \omega^9, \omega^{13}, \omega^{17}, \omega^{21} = \omega^3, \omega^7, \omega^{11}, \omega^{15}\} \quad \text{(orbit of } \omega^1\text{)}.$$

Hall would call these orbits "residues with indices $0, 1 \pmod 2$." (In fact, we see that in this case $\mathcal{C}_0$ is the set of squares and $\mathcal{C}_1$ is the set of non-squares in $GF(19)^*$.) $\diamond$

Hall used similar ideas in a situation with six orbits, so he refers to residues (mod 6). Here is what Hall wrote in his 1956 survey of difference sets ([**27**], p. 979):

> In calculating difference sets of the [Paley-] Hadamard type with $v = 4t - 1,\ k = 2t - 1,\ \lambda = t - 1$, it was found that for $v = 31$ and $v = 43$ not only the quadratic residues but also residues with indices $\equiv 0, 1, 3 \pmod 6$ gave difference sets. On investigation these turned out to be instances of a general theorem.

Hall's proof that his construction gives difference sets is long and intricate, and while we state the first version of his "general theorem" (Theorem 9.5), we do not include a proof.[5] However, we describe some of the ideas he used in his proof of this theorem.

We begin with the finite field $GF(q)$, for an odd prime power q. Let ω be a generator of the cyclic group $GF(q)^*$. Assume $q - 1 = ef$, with neither e nor f equal to 1.

Definition. The cyclotomic classes of order e are the sets

$$\mathcal{C}_i = \{\omega^{es+i} \mid s = 0, \ldots, f-1\}, \quad \text{for } i = 0, \ldots, e-1.$$

In other words, $\mathcal{C}_0 = \{1, \omega^e, \omega^{2e}, \ldots, \omega^{(f-1)e}\} = \langle \omega^e \rangle$, and $\mathcal{C}_i$ is the coset $\omega^i \mathcal{C}_0$ in $GF(q)^*$. We call the elements of $\mathcal{C}_0$ the eth power residues or eth residues. (The elements of $\mathcal{C}_i$ are the residues of index $i \pmod e$ to which Hall was referring in the passage quoted above.)

[5] For a proof, see Hall's book [**28**], pp. 194–195. This may look short, but Hall's argument depends on much of the preceding 20 pages. This proof is for $q = p^a$ a prime power, while his first version, in his 1956 paper, was for $q = p$ prime, but that proof was long too.

Example 5. Suppose $q = 19$, so $q - 1 = 18$ and choose $e = 2$ and $f = 9$. We choose $\omega = 3$ as in Example 4. Then the two cyclotomic classes of order 2 are the orbits $\mathcal{C}_0$ and $\mathcal{C}_1$ listed there. ◇

The next example involves a difference set outside the Paley-Hadamard family. We include it here as an easily accessible use of cyclotomic classes.

Example 6. Suppose $q = 13$, so $q - 1 = 12$, and choose $e = 4$ and $f = 3$. Assume ω is a generator of the cyclic group $GF(13)^*$. Then the cyclotomic classes of order 4 are

$$\begin{aligned} \mathcal{C}_0 &= \{1, \omega^4, \omega^8\}, \\ \mathcal{C}_1 &= \{\omega, \omega^5, \omega^9\}, \\ \mathcal{C}_2 &= \{\omega^2, \omega^6, \omega^{10}\}, \\ \mathcal{C}_3 &= \{\omega^3, \omega^7, \omega^{11}\}. \end{aligned}$$

The field $GF(13)$ is isomorphic to $\mathbb{Z}_{13}$. On page 88 we saw $\mathbb{Z}_{13}$ contains the difference set $D = \{0, 1, 3, 9\}$. If we choose $\omega = 2$, then $\mathcal{C}_0 = \{1, 3, 9\}$ and $D = \{0\} \cup \mathcal{C}_0$. ◇

Example 7. Suppose $q = 31$ and choose $e = 6$ and $f = 5$. Assume ω is a generator of $GF(31)^*$. We list the first two of the six cyclotomic classes of order 6:

$$\begin{aligned} \mathcal{C}_0 &= \{1, \omega^6, \omega^{12}, \omega^{18}, \omega^{24}\}, \\ \mathcal{C}_1 &= \{\omega, \omega^7, \omega^{13}, \omega^{19}, \omega^{25}\}, \\ &\vdots \qquad\qquad\qquad\qquad\qquad . \end{aligned}$$

In this case $D = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_3$ is a difference set in the additive group $GF(31)$. (See Exercise 24.) ◇

The following theorem describes the Hall family of difference sets in $GF(p)$. Example 7 is a difference set in this family.

Theorem 9.5. *(Hall,* [**28**]*, p. 170) Assume p is a prime with $p \equiv 1$ (mod 6) and with $p = 4x^2 + 27$ for some integer x. Choose a generator ω for the multiplicative group $GF(p)^*$ so that $3 = \omega^{6s+1}$ for some integer s. (This can always be done.*[6]*) Now form the cyclotomic*

[6] Hall uses the notation $\mathrm{Ind}_\omega(3)$ for the exponent t so that $\omega^t = 3$. In this notation the condition is written $\mathrm{Ind}_\omega(3) \equiv 1$.

classes of order 6: $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_5$. *Then*

$$D = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_3$$

is a difference set in $GF(p)$.

Notice that the parameters of the Hall difference sets are the same as the parameters of the Paley difference sets.[7]

The proof of Hall's theorem requires the following lemma due to Emma Lehmer ([**44**]).

Lemma 9.6. *(Lehmer) Let* $q = ef + 1$ *be an odd prime power, with* $e \neq 1, f \neq 1$. *If a union of cyclotomic classes of order* e *forms a nontrivial difference set* D *in the additive group of* $GF(q)$, *then* f *is odd and* e *is even.*

Lehmer goes on to prove a theorem giving conditions under which either $\mathcal{C}_0$ or $\mathcal{C}_0 \cup \{0\}$ is a difference set in $GF(q)$. Her theorem then implies theorems Theorems 4.4 and 4.5, the special cases when $\mathcal{C}_0$ is the set of fourth powers.

What is the relationship of Hall's difference sets to Singer difference sets? The only Mersenne primes of the form $4x^2 + 27$ are 31, 127 and 131071, and the Singer and Hall difference sets sharing the same parameters are equivalent only for the case $v = 31$.

It is conjectured that every cyclic difference set which has parameters $(4n - 1, 2n - 1, n - 1)$ has parameters of one of the kinds described above:

v is a prime power and $v \equiv 3 \pmod 4$,

v is a Mersenne prime with $v = 2^{d+1} - 1$,

$v = q(q + 2)$ with q and $q + 2$ odd primes.

The conjecture has been verified for $v < 10,000$, with 17 possible exceptions. This is not to say that every difference set with these parameters is *equivalent* to one given by one of the four constructions

[7] Hall's paper says the Hall and Paley difference sets are "distinct," although his paper does not prove inequivalence. In special cases, for example when $p = 31$, we can say more. See Exercise 17.

above. In fact there are six inequivalent difference sets with $v = 127$, and three of them do *not* arise from the constructions in this section.[8]

Exercises

13. Assume a nontrivial (v, k, λ)-difference set exists with v odd and $k < v/2$. Show that $1 \leq \lambda \leq (v-3)/4$. Ⓢ

14. Although the proof of Theorem 9.3 is complete as written, analyze columns to show directly that in the incidence structure with incidence matrix A, two distinct points appear together in exactly λ blocks.

15. Show that any two Hadamard matrices of order 12 are equivalent. (This challenging exercise is a good one to work on collaboratively.) Ⓗ

16. Assume q is an odd prime power and let D be the set of nonzero squares in $GF(q)$.

(a) Show that D is a $(q, (q-1)/2, \lambda, \mu)$-partial difference set with $\lambda + \mu = (q-3)/2$.

(b) We know that if $q \equiv 3 \pmod 4$, then $\lambda = \mu = (q-3)/4$ and we have a difference set. Assume $q \equiv 1 \pmod 4$. Show $|\lambda - \mu| = 1$ so $\{\lambda, \mu\} = \{(q-5)/4, (q-1)/4\}$.

(c) Assume the following fact from number theory: 2 is a square in $GF(q)$ if and only if $q \equiv \pm 1 \pmod 8$. (See [**20**], p. 58.) Use this fact to show $\lambda = (q-5)/4$ and $\mu = (q-1)/4$.

17. (This argument is due to Hall and appears on page 983 in [**27**].) Let D be the $(31, 15, 7)$-difference set of nonzero squares in $\mathbb{Z}_{31}$. Let D' be a $(31, 15, 7)$-difference set coming from Singer's construction in the vector space $(\mathbb{Z}_2)^5$.

(a) Let $B_0 = D$, $B_1 = 1 + D$ and $B_3 = 3 + D$, blocks of dev$D$. Find $B_0 \cap B_1 \cap B_3$.

[8] Our sources are [**5**], p. 91, and [**8**], p. 355–356, although neither presents a proof.

(b) Recall that the blocks of the Singer design devD' are 4-dimensional subspaces in the vector space $(\mathbb{Z}_2)^5$, and the points are 1-dimensional subspaces. How many points can there be in the intersection of three distinct blocks of devD'? Explain.

(c) Explain why dev$D$ and devD' are not isomorphic designs.

(d) Are D and D' equivalent difference sets? Explain your answer.

18. Assume q and $q+2$ are odd prime powers. Show that the additive group of the ring $GF(q) \oplus GF(q+2)$ is cyclic if and only if q and $q+2$ are primes.

19. In Exercise 8.3 you used the Singer construction to find a cyclic (15, 7, 3)-difference set. Now use the twin primes construction. Are these difference sets equivalent?

Exercises 20–22 fill in some of the details of the proof of Theorem 9.4 on the twin prime powers family.

20. Show that the set M is a group under multiplication. Also verify that $MD = D$.

21. Show that $\sim$ is an equivalence relation on G and that the equivalence classes are as described.

22. Prove that $\lambda_4 = (v-3)/4$.

23. Prove Lehmer's lemma by establishing the following statements. (Note that by Exercise 6.11 we know that if a nontrivial abelian (v, k, λ)-difference set D has multiplier -1 then v is even.)

(a) The translate $\omega^{es}D = D$; that is, the elements of $\mathcal{C}_0$ are multipliers.

(b) If f is even, then $-1 \in \mathcal{C}_0$.

(c) It follows that f is odd and e is even.

24. The field $GF(31)$ is isomorphic to the ring $\mathbb{Z}_{31}$. Using multiplication mod 31, verify that 3 is an element of order 30. In other words, in Example 7 we can choose $\omega = 3$.

(a) Determine the integers (mod 31) in $D = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_3$ and verify that D is a $(31, 15, 7)$-difference set in the additive group $\mathbb{Z}_{31}$.

(b) Compare the cyclotomic classes in (a) with the orbits of the multiplier 2 from Exercise 6.20.

25. In Hall's statement of his Theorem 9.5, he requires $p \equiv 7 \pmod{12}$. (Indeed, in his proof he shows that if $p \equiv 1 \pmod{12}$ then a Hall difference set cannot exist.) Show that if $p \equiv 1 \pmod 6$ and $p = 4x^2 + 27$ for some integer x, then $p \equiv 7 \pmod{12}$.

26. Exercise 17 tells us that the Paley and Singer difference sets in $\mathbb{Z}_{31}$ are not equivalent. From Exercise 6.20 we know $D = \mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_3$ is equivalent to either the Paley or Singer difference set. Which is it? How do you know?

27. This exercise invites you to use the computer to explore difference sets in the field $GF(43) = \mathbb{Z}_{43}$. (We previously considered difference sets in the additive group of this field in Exercise 6.19, but don't look back at that for now.) Find the cyclotomic classes of order 6 in $GF(43)$ for a variety of generators of $GF(43)^*$. For each of your generators:

- Which cyclotomic class contains 3?
- Which unions of cyclotomic classes form difference sets in the additive group of this field? Are the difference sets you obtain of the Hall or Paley type?

Do you see any patterns?

28. This is another invitation to explore using the computer. Choose a prime p with $p - 1 = ef$ for $e = 18$ and $f > 1$ and odd. Find the cyclotomic classes of order 18. Which unions of cyclotomic classes give difference sets in $GF(p)$? Are they of the Hall or Paley type?

9.3. Hadamard family: $v = 4n$

In this section we focus on Hadamard difference sets. These are (v, k, λ)-difference sets satisfying $v = 4n$ for $n = k - \lambda$. They have been and still are much studied. At the end of this section we revisit and extend some constraints on these difference sets in abelian groups, along with some surprising non-abelian results.

We know from the Bruck-Ryser-Chowla Theorem that a symmetric design with $v = 4n$ satisfies $n = u^2$ for some integer u. It turns out that every parameter of such a design can be written in terms of u.

Lemma 9.7. *If a symmetric (v, k, λ) design exists with $v = 4n$, then $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$ for some integer u.*

Difference sets with $v = 4n$ are called Hadamard because of the following theorem. Recall from Section 1 that a Hadamard matrix is regular if all its row and column sums are equal and, as a consequence, each row and column has the same number of $+1$s.

Theorem 9.8. *A symmetric (v, k, λ) design with $v = 4n$ exists if and only if a regular Hadamard matrix of order $4n$ exists.*

Proof. The proof is similar to that of Theorem 9.3, but it is actually easier. First assume H is a regular Hadamard matrix of order $4n$. Let k be the number of $+1$s in each row and each column of H. Create the matrix A from H by replacing each -1 by 0, so A is the incidence matrix of an incidence structure. Choose two rows of H. Let x be the number of columns with $+1$ in both rows and y be the number of columns with -1 in both rows. We know these two rows are orthogonal and $+1$ appears in each row k times. Schematically we represent the two rows as follows, where we write $+$ and $-$ for the entries of H:

$$\begin{array}{cccc}
\overbrace{+\cdots+}^{x} & \overbrace{+\cdots+}^{k-x} & \overbrace{-\cdots-}^{4n-k-y} & \overbrace{-\cdots-}^{y} \\
\underbrace{+\cdots+}_{x} & \underbrace{-\cdots-}_{k-x} & \underbrace{+\cdots+}_{4n-k-y} & \underbrace{-\cdots-}_{y}
\end{array} .$$

Since the number of +1s in the second row is k and the dot product of the rows is 0, we get the following equations:

$$\begin{aligned} x + (4n - k - y) &= k, \\ x - (k - x) - (4n - k - y) + y &= 0. \end{aligned}$$

We find $x = k - n$ and $y = 3n - k$. In other words, two rows of A share the entry 1 in $\lambda = k - n$ positions. (A similar analysis of the columns of H gives the dual conditions.) Thus A is the incidence matrix of a symmetric (v, k, λ) design with $v = 4n$.

For the converse, assume we have a symmetric (v, k, λ) design with $v = 4n$. Let A be the incidence matrix of the design and let H be the matrix obtained from A by replacing zeroes by -1s. Choose two distinct rows of H and count the numbers of columns in which:

x: both rows have $+1$,

y: the first row has $+1$ and the second has -1,

z: the first row has -1 and the second has $+1$, and

w: both rows have -1.

Now the two rows appear as follows:

$$\begin{array}{cccc} \overbrace{+\cdots+}^{x} & \overbrace{+\cdots+}^{y} & \overbrace{-\cdots-}^{z} & \overbrace{-\cdots-}^{w} \\ \underbrace{+\cdots+}_{x} & \underbrace{-\cdots-}_{y} & \underbrace{+\cdots+}_{z} & \underbrace{-\cdots-}_{w} \end{array} .$$

By Lemma 9.7, there is an integer u for which we have the following equations:

$$\begin{aligned} x + y + z + w &= v &&= 4u^2, \\ x + y &= k &&= 2u^2 - u, \\ x + z &= k &&= 2u^2 - u, \\ x &= \lambda &&= u^2 - u. \end{aligned}$$

From this we find that the dot product of the two rows is $x-y-z+w = 0$. Also the dot product of a row with itself is $v = 4u^2$, so we have $HH^T = vI_v$. Further, every row sum equals $x+y-z-w = -2u$, and similarly for columns. Therefore H is a regular Hadamard matrix. □

A much simpler argument, based on calculations in the integral group ring, shows that a (v, k, λ)-difference set gives rise to a Hadamard matrix of order v if and only if $v = 4n$. However, this is a weaker result than Theorem 9.8, since the existence of a difference set implies the existence of a symmetric design with the same parameters, but the converse does not hold.

Small examples. We look first at isolated examples of Hadamard difference sets for small values of u. Normally we restrict our attention to difference sets with $k < v/2$. However, for Hadamard difference sets, the choice of the sign of u is equivalent to the choice of a smaller difference set or its larger complement. In this context, it is usual to include either or both.

Example 8. For $u = 1$, the trivial difference set with parameters $(4, 1, 0)$ exists in both $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. The complementary difference set for $u = -1$ has parameters $(4, 3, 2)$. $\diamond$

Example 9. For $u = 2$, Kibler ([**40**], p. 64) lists 27 inequivalent $(16, 6, 2)$-difference sets which occur in twelve of the fourteen non-isomorphic groups of order 16.[9] Here is one discovered by Kibler in the non-abelian group $G = \langle a, b, c \mid a^4 = b^2 = c^2 = 1,\ ba = a^{-1}b,\ ac = ca,\ bc = cb \rangle$:

$$D_9 = \{1, a, a^2, b, ac, a^2bc\}.$$

(Note that a and b generate a dihedral group of order 8, and G is isomorphic to the direct product of this dihedral group and $\mathbb{Z}_2$.) $\diamond$

Example 10. For $u = 3$, here is an example due to Menon ([**55**], p. 742), who writes (using ℓ instead of u):

> In attempting to discover difference sets corresponding to various values of ℓ, the author has come across one corresponding to $\ell = 3$. It was found almost by accident, by a happy choice of the basic group and a still luckier choice of the elements forming the difference set.

[9] The exceptions are the cyclic group and the dihedral group. In Chapter 7 we see why these exceptions occur.

Menon chose $G = G_1 \times G_2$ where $G_1 = G_2 = \langle\, a, b \mid a^3 = b^2 = 1,\ ba = a^2b \,\rangle$, the dihedral group of order 6. He chose D to be the following set of fifteen elements of G:

$$\begin{array}{lll} (1,1), & (a,a^2), & (a^2,a), \\ (1,b), & (1,ab), & (1,a^2b), \\ (b,1), & (ab,1), & (a^2b,1), \\ (b,ab), & (ab,a^2b), & (a^2b,b), \\ (ab,b), & (a^2b,ab), & (b,a^2b). \end{array}$$

Then D is a $(36, 15, 6)$-difference set in G "as may be easily verified," Menon writes. ◇

Recall from Chapter 4 the conjecture that no dihedral group contains a difference set. However, Examples 9 and 10 show that a difference set *can* exist in a group that has a dihedral group as a homomorphic image. As you might suspect, a group with a dihedral image can contain a difference set only in rather special circumstances. (In Chapter 11 we use representation theory to explore this existence question.)

Infinite families. Now we turn to three infinite families of Hadamard difference sets, two of which we have already seen.

Example 11. Turyn's construction from Chapter 8 gives difference sets in the group $G = GF(q) \oplus GF(q)$ for $q = 2^h$. For these $v = 2^{2h} = 4 \cdot 2^{2h-2}$, so they are Hadamard difference sets with $u = 2^{h-1}$. ◇

Example 12. The McFarland construction of Chapter 8 with $q = 2$ gives difference sets with $v = 2^{2s+2} = 4(2^s)^2$ and $u = 2^s$ for any positive integer s. These difference sets are in groups of the form $G = E \times K$, where K need not be abelian. ◇

Now we consider a new construction, due to Dillon. The following theorem was proved in his 1974 doctoral dissertation.

Theorem 9.9. *(Dillon) Let G be a group of order $4u^2$. Assume G contains u subgroups $K_1, \ldots, K_u$, each of order $2u$ and that $K_i \cap K_j = \{1_G\}$ whenever $i \neq j$. Then the set*

$$D = (K_1 \cup \ldots \cup K_u) \setminus \{1_G\}$$

is a difference set in G.

The proof of Theorem 9.9 is a nice exercise working in the integral group ring $\mathbb{Z}G$. Unfortunately, the range of application of Dillon's construction is narrow. It is restricted to certain groups of order 36, one group of order 64, and any group which is the direct sum of an even number of copies of $\mathbb{Z}_2$. (See [**8**], p. 367.) However, Kantor has shown that in this last category there are exponentially many inequivalent difference sets! (See [**35**], p. 284, and [**38**].)

Menon's construction. In his paper [**55**], Menon proves a composition theorem showing how to construct a Hadamard difference set in $G = G_1 \times G_2$ from Hadamard difference sets in the G_j. Although this is the primary result, Menon actually proves a bit more. He also shows that if his construction gives a difference set in G from difference sets in the G_j, then the difference sets in the G_j must be Hadamard.

Theorem 9.10. *(Menon) For $j = 1, 2$, assume D_j is a (v_j, k_j, λ_j)-difference set in the group G_j. Write $\overline{D}_j$ for the complement of D_j in G_j, so $\overline{D}_j$ is a $(v_j, v_j - k_j, \overline{\lambda}_j)$-difference set in G_j. Let $G = G_1 \times G_2$ and $D = (D_1 \times D_2) \cup (\overline{D}_1 \times \overline{D}_2)$. Then D is a difference set in G if and only if $v_j = 4n_j$ for $j = 1, 2$. Furthermore, when D is a difference set, its parameters satisfy $v = 4n$ for $n = 4n_1n_2$.*

Proof. Write the group operations multiplicatively, and let 1_j be the identity element of G_j, so $1_G = (1_1, 1_2)$. We work in the ring $\mathbb{Z}G$. We follow the usual convention and write S both for a subset of G and for the element of $\mathbb{Z}G$ written $\sum_{s \in S} s$. If $S = X \times Y \subseteq G$ with $X \subseteq G_1$ and $Y \subseteq G_2$, we also write $S = (X, Y) \in \mathbb{Z}G$,

$$(X, Y) = \sum_{x \in X,\ y \in Y} (x, y) = \left(\sum_{x \in X} x,\ \sum_{y \in Y} y \right).$$

This notation can be extended in a natural way to multisets X and Y, or, equivalently, elements of the $\mathbb{Z}G_j$ with non-negative coefficients. Although this notation has to be used with care, the following statements are true for $X, Z \subseteq G_1$ and $Y, W \subseteq G_2$, and for m a positive

integer:

$$\begin{aligned}(X,Y)(Z,W) &= (XZ,YW), &(1)\\ (X+Z,Y) &= (X,Y)+(Z,Y), &(2)\\ (X,Y+W) &= (X,Y)+(X,W),\\ (mX,Y) &= m(X,Y) = (X,mY). &(3)\end{aligned}$$

Since D_j is a difference set in G_j, we know that for $j = 1, 2$

$$\begin{aligned}D_jD_j^{(-1)} &= n_j1_j + \lambda_jG_j, &(4)\\ \overline{D}_j\overline{D}_j^{(-1)} &= n_j1_j + \overline{\lambda}_jG_j,\\ D_j\overline{D}_j^{(-1)} &= D_j(G_j - D_j^{(-1)}) = n_j(G_j - 1_j),\\ \overline{D}_jD_j^{(-1)} &= (G_j - D_j)D_j^{(-1)} = n_j(G_j - 1_j).\end{aligned}$$

In the ring $\mathbb{Z}G$ we have $D = (D_1, D_2) + (\overline{D}_1, \overline{D}_2)$, and therefore $D^{(-1)} = (D_1^{(-1)}, D_2^{(-1)}) + (\overline{D}_1^{(-1)}, \overline{D}_2^{(-1)})$. Multiply out $DD^{(-1)}$ using equations (1) and (4) to obtain equation (5):

$$\begin{aligned}&DD^{(-1)} = &(5)\\ &(n_11_1 + \lambda_1G_1, n_21_2 + \lambda_2G_2) \ + \ (n_1(G_1 - 1_1), n_2(G_2 - 1_2)) \ +\\ &(n_1(G_1 - 1_1), n_2(G_2 - 1_2)) \ + \ (n_11_1 + \overline{\lambda}_1G_1, n_21_2 + \overline{\lambda}_2G_2).\end{aligned}$$

Enumerating terms we see that:

$$(G_1 - 1_1, G_2 - 1_2) \ = \ (G_1, G_2) - (G_1, 1_2) - (1_1, G_2) + (1_1, 1_2). \quad (6)$$

Multiply out the right side of equation (5) using (2), (3) and (6) and then reorganize by collecting the terms involving $(1_1, 1_2)$, $(1_1, G_2)$, $(G_1, 1_2)$, and (G_1, G_2). The result is equation (7):

$$\begin{aligned}&DD^{(-1)} = &(7)\\ &4n_1n_2(1_1, 1_2) \ + \ n_1(\lambda_2 + \overline{\lambda}_2 - 2n_2)(1_1, G_2) \ +\\ &n_2(\lambda_1 + \overline{\lambda}_1 - 2n_1)(G_1, 1_2) \ + \ (2n_1n_2 + \lambda_1\lambda_2 + \overline{\lambda}_1\overline{\lambda}_2)(G_1, G_2).\end{aligned}$$

For our primary result, we assume the D_j are Hadamard difference sets, and we want to show that D is a difference set. To do this, we must show that for appropriate n and λ,

$$DD^{(-1)} = n(1_1, 1_2) + \lambda(G_1, G_2).$$

Since the D_j are Hadamard, we have $v_j = 4n_j$ for $j = 1, 2$. Further, there are integers u_j with $n_j = u_j^2$, $k_j = 2u_j^2 - u_j$, $\lambda_j = u_j^2 - u_j$, and for the complementary cases $\overline{\lambda}_j = u_j^2 + u_j$, so $\lambda_j + \overline{\lambda}_j = 2n_j$. Write $u = 2u_1u_2$; then $v = 4u^2$ and $k = 2u^2 + u$. Substituting these values into equation (7) gives

$$DD^{(-1)} = n(1_1, 1_2) + \lambda(G_1, G_2)$$

for $\lambda = u^2 + u$. In other words, D is a Hadamard difference set in $G = G_1 \times G_2$ with paramaters $(4u^2, 2u^2 + u, u^2 + u)$. Since the integers u_j can each be positive or negative, u can be positive or negative. (This observation means there is no change in the result if one or both of the D_j is replaced by its complement in G_j.)

Conversely, assume D is a difference set in G. This requires the coefficients of $(1_1, G_2)$ and $(G_1, 1_2)$ in equation (7) to be zero. This in turn forces $\lambda_j + \overline{\lambda}_j = 2n_j$ which implies $v_j = 4n_j$, and the D_j are Hadamard difference sets. □

Menon's construction (in [**55**], pp. 741–743) gives the following corollaries.

Corollary 9.11. *The following statements are true:*

(i) If there exists a difference set with parameters (v_0, k_0, λ_0) with $v_0 = 4n_0$ for $n_0 = u_0^2$, then there exists a difference set with parameters (v, k, λ) and $v = 4n$ for $n = u^2$ with $u = 2u_0$.

(ii) If there exists a difference set with parameters (v_0, k_0, λ_0) with $v_0 = 4n_0$ for $n_0 = u_0^2$, then for $r = 1, 2, \ldots$, there exists a difference set with parameters (v, k, λ) and $v = 4n$ for $n = u^2$ with $u = 2^{r-1}u_0^r$.

(iii) There exist difference sets with parameters (v, k, λ) and $v = 4n$ for $n = u^2$ with $u = 2^r$ for all positive integers r.

(iv) There exist difference sets with parameters (v, k, λ) and $v = 4n$ for $n = u^2$ with $u = 2^r 3^s$ for all integers $r \geq s - 1 \geq 0$.

Other results. We conclude with a brief look at some other results about Hadamard difference sets. Turyn's 1965 paper [**69**] is of special importance because of his innovative use of tools from character

theory and algebraic number theory. It contains his useful exponent bound, discussed in Section 7.2. (We give an elementary introduction to some of these methods in Chapters 11 and 12, culminating in a proof of Turyn's exponent bound.) For convenience, we restate Theorem 7.5, the first version of Turyn's result.

Theorem *(Turyn) Let p be a prime and assume G is an abelian group of order $4p^{2a}$. Let P be a Sylow p-subgroup of G. Assume G contains a Hadamard difference set. If $p = 2$, then the exponent of P is at most 2^{a+2}. If p is odd, then the exponent of P is at most p^a.*

We suggest revisiting Section 7.2 for the description of the subsequent work showing that Turyn's bound guarantees the existence of a Hadamard difference set in abelian 2-groups, as well as of other researchers' discoveries of difference sets in non-abelian groups that exceed Turyn's exponent bound.

McFarland extended the work of Turyn and of his own teacher Mann and expanded the use of characters and algebraic number theory in the study of difference sets. In [**51**], a lengthy *tour de force*, McFarland proved the following theorem.

Theorem 9.12. *(McFarland) Assume G is an abelian group of order $4p^2$ for p an odd prime. If G contains a difference set, then $p = 3$.*

Example 13. When $p = 5$, Turyn's exponent bound shows that for any group H of order 4 there is no abelian $(100, 45, 20)$-difference set in $H \oplus \mathbb{Z}_{25}$. McFarland's theorem shows that there is none in $H \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, so there is no abelian $(100, 45, 20)$-difference set of any kind. ◇

Once again, non-abelian groups really are different. In [**65**], Smith constructed a $(100, 45, 20)$-difference set in a non-abelian group. We will look at a portion of Smith's construction in Chapter 11.

The decade of the 1990s was a period of finding (interesting!) non-abelian complexities where there had been simplicities in the abelian case. It was also a period of consolidation and generalization. In particular, Davis and Jedwab [**16**] found a uniform construction for difference sets with $\gcd(v, n) > 1$, including the Hadamard family

along with others. Indeed, they discovered new families of difference sets in the process.

Exercises

29. Prove Lemma 9.7. Also show that the choice of the sign of u corresponds to the choice of the parameters for a difference set or for its complement. Ⓢ

30. In this exercise, use difference sets to construct regular Hadamard matrices.

(a) Write out the regular Hadamard matrices determined by the difference sets in Example 8.

(b) Write out the first five rows of the Hadamard matrix determined by the difference set in Example 9, where the points (elements of G) are in the order:

$$1, a, a^2, a^3, b, ab, a^2b, a^3b, c, ac, a^2c, a^3c, bc, abc, a^2bc, a^3bc,$$

and the first five blocks are D, aD, a^2D, a^3D, bD.

31. Assume D is a (v, k, λ)-difference set. Let G act on itself by left multiplication and write $\pi_g(x) = gx$ for $x, g \in G$. Then π_g is a permutation, and we let $[g]$ be the corresponding $v \times v$ (permutation) matrix of π_g. We know this G-action is regular; equivalently, $\pi_g(x) = \pi_h(x)$ for some $x \in G$ implies $g = h$.

(a) Show that $\varphi(g) = [g]$ defines a group homomorphism from G to the group of invertible $v \times v$ matrices over the real numbers. Also show $[g]^{-1} = [g]^T$ for $g \in G$.

(b) By Theorem 10.11 (p. 192), φ gives a ring homomorphism $\widetilde{\varphi}$ from $\mathbb{Z}G$ to the ring of all $v \times v$ matrices over $\mathbb{R}$ by $\widetilde{\varphi}(\sum a_g g) = \sum a_g \varphi(g)$. Show that $\widetilde{\varphi}(1_G) = I_v$ and $\widetilde{\varphi}(G) = J_v$, the all 1s matrix.

(c) Let $M = \widetilde{\varphi}(G-D) - \widetilde{\varphi}(D)$. Show $MM^T = 4nI_v + (v-4n)J_v$.

(d) Conclude that M is a Hadamard matrix of order $4n$ if and only if $v = 4n$.

32. Prove Theorem 9.9.

33. Theorem 9.9 can be used to construct $(36, 15, 6)$-difference sets in $K \times K$ for K a group of order 6.

(a) Carry out Dillon's construction for $K = \langle a, b \,|\, a^3 = b^2 = 1, bab^{-1} = a^2 \rangle$, the dihedral group of order 6.

(b) Is the difference set constructed in (a) equivalent to Menon's in Example 10 on page 157? Justify your answer.

(c) Now carry out Dillon's construction for $K = \mathbb{Z}_6$.

34. Fill in the missing details in the proof of Theorem 9.10 as follows.

(a) Verify equations (1), (2) and (3).

(b) Verify the equations in (4).

(c) Verify equation (7).

35. Use Theorem 9.10 and Example 8 to construct at least two more specific Hadamard difference sets.

36. Prove Corollary 9.11.

Coda

In 1893, Hadamard gave an upper bound on the determinant of a matrix whose complex entries have absolute value at most 1. When the matrix entries are integers, the upper bound is attained by what are now known as Hadamard matrices. Our interest in these matrices is quite different from Hadamard's. For us, the key facts are the following theorems, and our interest is in the existence or non-existence of corresponding difference sets.

- A Hadamard matrix of order $4n$ exists if and only if a symmetric $(4n - 1, 2n - 1, n - 1)$ design exists.
- A regular Hadamard matrix of order $4n$ exists if and only if a symmetric (v, k, λ) design exists with $v = 4n$.

The Paley-Hadamard family consists of difference sets with parameters $(4n-1, 2n-1, n-1)$. Section 2 describes four subfamilies of this larger family, all abelian and all constructed from finite fields: the Paley family of nonzero squares in $GF(q)$, the Singer family for $q = 2$, the twin prime powers family of difference sets in $GF(q) \oplus GF(q+2)$, and the Hall family of unions of special cyclotomic classes in $GF(p)$ for suitable primes p.

Difference sets in the Hadamard family have parameters with $v = 4n$. Section 3 includes both abelian and non-abelian examples. The McFarland construction (with $q = 2$) and the Turyn construction from Chapter 8 produce difference sets in this family. The main result in this section is Menon's direct product construction, which builds new Hadamard difference sets from smaller ones. Although it is beyond the scope of this book, Davis and Jedwab's unifying construction for all difference sets for which $\gcd(v, n) > 1$ ([**16**]) places Hadamard difference sets in a larger context.

Chapter 10

Representation Theory

Representation theory is an essential tool for the study of algebraic structures, especially groups. We use representations of finite groups to discover and explore difference sets. Recall that in Section 9.3 we mentioned Smith's surprising discovery of a non-abelian $(100, 45, 20)$-difference set. He made substantial use of group representations and characters in his work.

Representation theory has important applications to many areas of mathematics, and to physics and chemistry as well. Because the subject is so beautiful and so widely used, we decided against simply quoting the results we need. Instead, in this chapter and the next we offer a brief primer on representations of finite groups and their characters. As in the proof of the Bruck-Ryser-Chowla Theorem, many of the arguments in these two chapters display the power of linear algebra.

10.1. Definitions and examples

Recall from abstract algebra that $GL(m, \mathbb{K})$, the set of invertible $m \times m$ matrices with elements from the field $\mathbb{K}$, is a group under matrix multiplication. This is known as the general linear group. We may interpret these matrices as invertible linear transformations from $\mathbb{K}^m$ to $\mathbb{K}^m$, where for $A \in GL(m, \mathbb{K})$, each vector $\mathbf{x} \in \mathbb{K}^m$ is mapped to

Ax. The identification of the group $GL(m, \mathbb{K})$ of matrices with the group of invertible linear transformations of an m-dimensional vector space V over $\mathbb{K}$ assumes that we have chosen a basis for V. More generally, if V is an m-dimensional vector space over $\mathbb{K}$, we define $GL(V)$ to be the set of invertible linear transformations from V to V. This set is a group under composition, and it is isomorphic to $GL(m, \mathbb{K})$.

Definition. A linear representation of a group G in a vector space V over a field $\mathbb{K}$ is a group homomorphism $\rho : G \to GL(V)$. The dimension of V is called the degree of the representation. The representation is faithful if the homomorphism is one-to-one (i.e., if the kernel of the representation is $\{1_G\}$).

Throughout this chapter, G is a finite group, V is a vector space of positive finite dimension over $\mathbb{K}$, and $\mathbb{K}$ is either $\mathbb{R}$ or $\mathbb{C}$. Usually we omit the word "linear" and simply refer to a representation of G. Once a basis is chosen for V, we can identify the groups $GL(V)$ and $GL(m, \mathbb{K})$. Therefore, we often think of a representation as a homomorphism from the group G to the group of matrices $GL(m, \mathbb{K})$. In the special case $m = 1$ we identify the matrix $[a]$ and the element $a \in \mathbb{K}$, identifying $GL(1, \mathbb{K})$ and $\mathbb{K}^*$.

Example 1. Let G be the symmetric group S_3 and $V = \mathbb{R}^3$. We use the standard basis vectors $\mathbf{e}_1$, $\mathbf{e}_2$, $\mathbf{e}_3$, so $GL(V) \cong GL(3, \mathbb{R})$. For example, the transformation that swaps vectors $\mathbf{e}_1$ and $\mathbf{e}_2$ and fixes $\mathbf{e}_3$ corresponds to the matrix

$$M \quad = \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

With this understanding, we define the "natural" representation of S_3, mapping a permutation in S_3 to a transformation that permutes the standard basis vectors according to the given permutation,

$$\rho : S_3 \to GL(3, \mathbb{R}), \text{where}$$
$$\rho : \pi \mapsto M_\pi, \text{ the matrix of the transformation } \mathbf{e}_j \mapsto \mathbf{e}_{\pi(j)}.$$

This is indeed a group homomorphism; that is, for all $\pi_1, \pi_2 \in S_3$, $\rho(\pi_1\pi_2) = \rho(\pi_1)\rho(\pi_2)$. It is easiest to show this for the corresponding linear transformations acting on the standard basis vectors, and then to extend this linearly to all of $\mathbb{R}^3$.

Since these six linear transformations simply permute the basis vectors, the matrices are permutation matrices. The complete mapping ρ from S_3 to $GL(3, \mathbb{R})$ is shown here:

$$(1) \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (123) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad (132) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$(12) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (23) \mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad (13) \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \quad \diamond$$

Example 2. Let $G = S_3$ and $V = \mathbb{R}$. Define $\rho(\pi) = 1$ if π is an even permutation and $\rho(\pi) = -1$ if π is an odd permutation. The map ρ is a homomorphism. This representation has degree 1, and it is not faithful. Although by applying ρ we lose much of the group structure, we do retain some information about the group. $\diamond$

Example 3. Let $G = \langle a \mid a^4 = 1 \rangle$ and $V = \mathbb{R}^2$. Define ρ by

$$\rho(a) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Then ρ is a homomorphism. This representation is faithful and has degree 2. Notice that $\rho(a)$ is the matrix of a counter-clockwise rotation of the plane about the origin through 90 degrees. See Figure 10.1. $\diamond$

Example 4. Let G be *any* finite group and let $\mathbb{K}$ be any field. Define $\rho(g) = 1 \in \mathbb{K}$ for all $g \in G$. This is called the trivial representation of G. It has degree 1. If G has more than a single element, the trivial representation is not faithful. $\diamond$

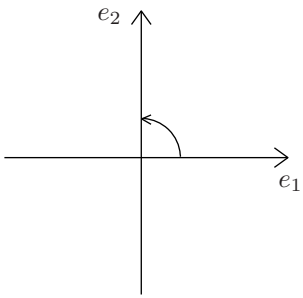


Figure 10.1. Rotate plane through 90 degrees, Example 3

Example 5. Let $G = \langle a \mid a^4 = 1 \rangle$, and let $V = \mathbb{R}^3$ with standard basis $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$. Define $\rho : G \to GL(3, \mathbb{R})$ by

$$\rho(a) = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Then ρ is a homomorphism. The transformation given by $\rho(a)$ rotates 3-space around the axis spanned by $\mathbf{e}_3$. See Figure 10.2. Let W be the subspace spanned by $\mathbf{e}_1$ and $\mathbf{e}_2$. The rotations $\rho(a^j)$ all map W to itself. Notice that the subspace U spanned by $\mathbf{e}_3$ is also mapped to itself by all the $\rho(a^j)$, and that $U = W^\perp$. $\diamond$

The preceding example leads to an important concept.

Definition. An invariant subspace (or stable subspace) of a representation ρ of G in V is a subspace of V that is mapped to itself by all the transformations $\rho(g)$ for $g \in G$. We also use the language G-invariant subspace when it is clear which representation of G is under discussion.

For any representation of a group G, the subspaces $\{\mathbf{0}\}$ and V are always G-invariant. These are called the trivial subspaces. In Example 5 both $W = \text{span}\{\mathbf{e}_1, \mathbf{e}_2\}$ and $U = \text{span}\{\mathbf{e}_3\}$ are G-invariant. In Example 1 where $G = S_3$, each $\rho(g)$ permutes the basis vectors $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$, so the 1-dimensional subspace spanned by their sum

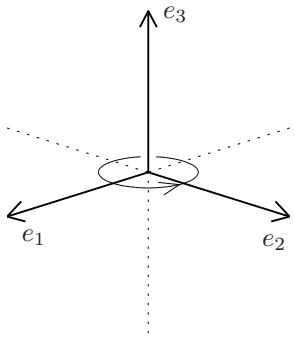


Figure 10.2. Rotate 3-space about the vertical axis 90 degrees, Example 5

$\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ is also G-invariant. In Example 3, there are no nontrivial G-invariant subspaces.

Note that it is not required that individual vectors of a G-invariant subspace are fixed by each $\rho(g)$ for $g \in G$. It is only required that the subspace as a whole is mapped into itself by each $\rho(g)$, as the G-invariant subspace W in Example 5 shows. Indeed, none of the nonzero vectors in W is fixed by all the $\rho(g)$ in that case.

We need one more definition to explain our first main goal.

Definition. An irreducible representation of G in V is a representation whose only G-invariant subspaces are the trivial subspaces V and $\{\mathbf{0}\}$. Otherwise the representation is reducible.

All representations of degree 1 are irreducible because a vector space of dimension 1 has no nontrivial subspaces. The representations in Examples 2, 3 and 4 are irreducible, but those in Examples 1 and 5 are reducible. We look more closely at these reducible examples.

In Example 5, every matrix $\rho(g)$ for $g \in G$ has the form

$$\rho(g) = \begin{bmatrix} A(g) & 0 \\ 0 & 1 \end{bmatrix},$$

where $A(g)$ describes a rotation of the plane spanned by $\mathbf{e}_1$ and $\mathbf{e}_2$. Notice that all the matrices $\rho(g)$ are block diagonal. We can view

the blocks themselves as providing representations of the group G—one of degree 2 in W and one of degree 1 in $U = W^{\perp}$ (the trivial representation).

As in Example 5, the representation in Example 1 is reducible. We know that the span of $\mathbf{v}_1 = \mathbf{e}_1+\mathbf{e}_2+\mathbf{e}_3$ is an invariant subspace. In Exercise 2 we see that the plane orthogonal to $\mathbf{v}_1$ is also an invariant subspace. In Figure 10.3 the vectors $\mathbf{e}_1$, $\mathbf{e}_2$, and $\mathbf{e}_3$ are drawn as edges of a unit cube. The vector $\mathbf{v}_1$ lies along the diagonal of the cube and is shown as a dashed line segment. It is fixed by all the $\rho(g)$, for $g \in S_3$. Let $\mathbf{v}_2$ and $\mathbf{v}_3$ span the plane orthogonal to $\mathbf{v}_1$. With respect to the new basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ for V, the matrix for each transformation $\rho(g)$ for $g \in S_3$ has the form

$$\begin{bmatrix} 1 & 0 \\ 0 & B(g) \end{bmatrix}.$$

Again all the matrices $\rho(g)$ are block diagonal, and the blocks themselves provide representations of the group S_3, one of degree 1 and one of degree 2.

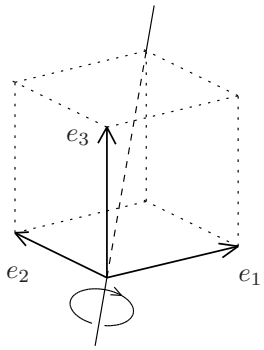


Figure 10.3. Rotate 3-space to cyclically permute e_1, e_2, e_3. Example 1.

In general we seek to *decompose* complex representations into irreducible representations and to study these building blocks. We find that any finite group has a finite number of irreducible representations, and that any of its representations can be decomposed into a

"sum" of irreducible complex representations. The formal statement is Maschke's Theorem.

Before we proceed with our analysis, we expand our library of examples of group representations.

Example 6. We generalize Example 1. Let $G = S_m$ and let V be the vector space $\mathbb{K}^m$ with standard basis $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m\}$. Then the natural representation of S_m in V maps the permutation $\pi \in S_m$ to the representation that permutes the basis vectors according to π; that is:

$$\rho : S_m \to GL(m, \mathbb{K}), \text{ where}$$

$$\rho : \pi \mapsto M_\pi \quad \text{the matrix of the transformation } \mathbf{e}_j \mapsto \mathbf{e}_{\pi(j)}.$$

The map ρ is a group homomorphism. As for the case $m = 3$, it is enough to show that this is true for the basis vectors, and then to extend linearly to all of V. Since the nonzero vector $\sum_j \mathbf{e}_j$ is fixed by $\rho(\pi)$ for all π, this representation is reducible. Since only the identity permutation fixes all the basis vectors, this is a faithful representation. The representation has degree m. ◇

Example 7. Choose $G = \langle a \mid a^5 = 1 \rangle$ and $V = \mathbb{C}$, so $GL(V) \cong GL(1, \mathbb{C}) \cong \mathbb{C}^*$, the multiplicative group of nonzero complex numbers. Define a map $\rho : G \to \mathbb{C}^*$ by

$$\rho(a) = e^{2\pi i/5}.$$

Since $e^{2\pi i/5}$ is of order 5 in $\mathbb{C}^*$, ρ is a group homomorphism. (See A.15 for a review of complex roots of unity.) Since the degree is 1, this is an irreducible representation of G. Also, ρ is faithful. ◇

In the next two examples we consider two representations of the dihedral group D_5, one of degree 1 and one of degree 2.

Example 8. Let $G = \langle a, b \mid a^5 = b^2 = 1, bab^{-1} = a^{-1} \rangle$. Choose $V = \mathbb{C}$ and define

$$\rho(a) = 1 \quad \text{and} \quad \rho(b) = -1.$$

This defines a homomorphism from G to $\mathbb{C}^*$. It is irreducible because it has degree 1; it has kernel $\langle a \rangle$, so it is not faithful. ◇

Example 9. Let G be as in Example 8. Choose $V = \mathbb{C}^2$ and define

$$\rho(a) = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix} \quad \text{and} \quad \rho(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where η is a primitive fifth root of unity (i.e., $\eta = (e^{2\pi i/5})^j$ for some $j \in \{1, 2, 3, 4\}$). This defines a homomorphism from G to $GL(2, \mathbb{C})$. We show that ρ is irreducible. This time V does have nontrivial subspaces, so there is something to check. Suppose that $\mathbf{v} = (x, y)$ spans a nontrivial G-invariant subspace for this representation; we show that this leads to a contradiction. By our assumption $\rho(b)(\mathbf{v}) = s\mathbf{v}$ for some $s \in \mathbb{C}$. Since $\rho(b)$ is invertible, $\mathbf{v} \neq \mathbf{0}$ implies $s \neq 0$. Thus we have $(y, x) = (sx, sy)$, which tells us that $s^2 = 1$ and $y = \pm x$. Similarly, $\rho(a)(\mathbf{v}) = t\mathbf{v}$ for some $t \in \mathbb{C}$, and $t \neq 0$. This tells us that $\eta x = tx$ and $\eta^{-1} y = ty$. Since we are assuming $\mathbf{v} \neq \mathbf{0}$, this tells us $\eta = t = \eta^{-1}$ and $\eta^2 = 1$, which is impossible. Therefore ρ is irreducible. It is also faithful. ◇

The preceding examples generalize.

Example 10. Every cyclic group has a faithful representation of degree 1 generalizing that in Example 7. Let $G = \langle a \mid a^m = 1 \rangle$ and define

$$\rho(a) = e^{2\pi i/m}. \qquad \diamond$$

Example 11. Every dihedral group has representations of degree 2, generalizing those in Example 9. Let

$$G = \langle a, b \mid a^m = b^2 = 1,\ bab^{-1} = a^{-1} \rangle,$$

and let $\eta = (e^{2\pi i/m})^j$ for some integer j. Define

$$\rho(a) = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix} \quad \text{and} \quad \rho(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If m does not divide $2j$ then $\eta^2 \neq 1$ and the representation is irreducible. If $\gcd(j, m) = 1$, this representation is faithful. ◇

We know by Cayley's Theorem that every finite group G is isomorphic to a group of permutations, where we associate $g \in G$ with the function $\pi_g : G \to G$, with $\pi_g(x) = gx$. We find $G \cong H = \{\pi_g \mid g \in G\} \subset S_m$ for $m = |G|$. We now combine this isomorphism with

the natural representation of S_m to get the left regular representation of a group.

Definition. Let G be a finite group of order m. Fix a field $\mathbb{K}$ and let V be a vector space of dimension m over $\mathbb{K}$ with basis $\{\mathbf{e}_h \mid h \in G\}$. We define "the" left regular representation ρ_{reg} of G in V by

$$\rho_{reg}(g) : \mathbf{e}_h \mapsto \mathbf{e}_{gh} \quad \text{for} \quad g \in G.$$

In the definition above, we do not specify the field. There is actually a different left regular representation for each field. We limit our discussion to the left regular representation over the field $\mathbb{C}$, and often simply call this the regular representation.[1]

Example 12. Let $G = \langle a \mid a^5 = 1 \rangle$. Choose $V = \mathbb{C}^5$ with the standard basis $\mathbf{e}_1, \mathbf{e}_a, \mathbf{e}_{a^2}, \mathbf{e}_{a^3}, \mathbf{e}_{a^4}$, so

$$\rho_{reg}(a) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Thus, we have identified the group element a with the permutation $a^j \mapsto a^{j+1}$ of the elements of G and then associated that permutation with the matrix of the linear transformation that maps $\mathbf{e}_j$ to $\mathbf{e}_{j+1}$, where we interpret the subscripts modulo 5. ◇

Exercises

1. Let $G = D_4 = \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_1, F_2\}$. The dihedral group of order 8 is described here as the group of symmetries of a square. The element R_θ is the counterclockwise rotation about the center of the square through θ degrees; F_H, F_V are reflections in horizontal, vertical lines through the center of the square; F_1, F_2 are reflections in the diagonal lines l_1, l_2 where l_1 goes from lower left to upper right. (To rewrite in our usual notation $D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab^{-1} = a^{-1} \rangle$, we can choose $a = R_{90}$ and $b = F_H$.)

[1] The right regular representation is defined in a similar way, but with multiplication on the right by the inverse.

Let ρ be the representation of G in $\mathbb{R}^2$ suggested by the motions of the square centered at the origin. Using the standard basis vectors, find matrices for the transformations $\rho(g)$ for all g in G.

2. In Example 1, determine a basis $\mathbf{v}_2, \mathbf{v}_3$ for the plane orthogonal to the vector $\mathbf{v}_1 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$. Find a matrix A that changes the standard basis to your new basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Then with respect to your new basis, determine the six matrices that realize the six linear transformations in $GL(3, \mathbb{R})$ that are images under ρ of elements in S_3.

3. Assume $m \geq 2$ and let G be the symmetric group S_m acting on $V = \mathbb{C}^m$ by the natural representation ρ. Choose the standard basis $\mathbf{e}_1, \ldots, \mathbf{e}_m$ for V. Define

$$W = \left\{ \sum_j a_j \mathbf{e}_j \;\middle|\; \sum_j a_j = 0 \right\}. \qquad \text{Ⓢ}$$

(a) Show that W is a G-invariant subspace of V.

(b) Give an example of $\mathbf{w} \in W$ and $g \in G$ with $\rho(g)(\mathbf{w}) \neq \mathbf{w}$.

4. Representations of degree 1 over $\mathbb{R}$ and $\mathbb{C}$.

(a) Let G be a finite group of odd order. Show that if $\rho : G \to GL(1, \mathbb{R}) \cong \mathbb{R}^*$ is a representation of degree 1, then ρ must be the trivial representation.

(b) Give an example of a finite group G of odd order and a *nontrivial* representation

$$\rho : G \to GL(1, \mathbb{C}) \cong \mathbb{C}^*.$$

(c) Give an example of a nontrivial representation $\rho : G \to GL(1, \mathbb{R}) \cong \mathbb{R}^*$ for the group $G = \langle a \mid a^4 = 1 \rangle$. Can you find a faithful representation?

(d) Let $G = \langle a \mid a^4 = 1 \rangle$, and give an example of a faithful representation $\rho : G \to GL(1, \mathbb{C}) \cong \mathbb{C}^*$.

10.2. Equivalent representations

The "natural" representation of S_m is in the vector space of dimension m. The left regular representation of S_m is in a vector space of dimension $m!$, the number of elements in the group S_m. So for $m > 1$ these representations are different. Since a group typically has many representations, we need to specify when we regard two representations as "the same."

Definition. Let G be a finite group and let V_1 and V_2 be vector spaces over a field $\mathbb{K}$. Two representations $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ are called equivalent if there exists an invertible (one-to-one, onto) linear transformation $\tau : V_1 \to V_2$ such that

$$\rho_2(g) = \tau\, \rho_1(g)\, \tau^{-1} \text{ for all } g \in G.$$

This last condition can be rewritten as $\rho_2(g)\tau = \tau\rho_1(g)$, for all $g \in G$, although we must require that τ be invertible. Then for every $g \in G$, the following diagram commutes:

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ V_2 & \xrightarrow{\rho_2(g)} & V_2 \end{array}$$

This defines an equivalence relation on the set of representations of G.

Example 13. Choose $G = \langle a \mid a^4 = 1 \rangle$ and let $V = \mathbb{C}^2$ with standard basis $\mathbf{e}_1, \mathbf{e}_2$. We consider two different representations ρ_1 and ρ_2 defined by the following:

$$\rho_1(a): \quad \begin{array}{l} \mathbf{e}_1 \mapsto -\mathbf{e}_2 \\ \mathbf{e}_2 \mapsto \mathbf{e}_1 \end{array} \qquad \rho_2(a): \quad \begin{array}{l} \mathbf{e}_1 \mapsto i\mathbf{e}_1 \\ \mathbf{e}_2 \mapsto -i\mathbf{e}_2. \end{array}$$

These are both faithful representations of G. In fact, they are equivalent. To find the transformation τ that demonstrates the equivalence, we find the eigenvalues of A, the matrix of $\rho_1(a)$ with respect to the

basis $\mathbf{e}_1, \mathbf{e}_2$,

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

The eigenvalues are the zeroes of the characteristic polynomial $\det(A - xI) = x^2 + 1$, namely i and $-i$. If we choose $\mathbf{f}_1$ to be an eigenvector for the eigenvalue i and $\mathbf{f}_2$ for $-i$, then we know $\mathbf{f}_1$ and $\mathbf{f}_2$ are independent, so we can define an invertible linear transformation by $\tau(\mathbf{f}_j) = \mathbf{e}_j$ for $j = 1, 2$. You should check that $\rho_2(a)$ and $\tau\rho_1(a)\tau^{-1}$ have the same effect on $\mathbf{e}_1$ and $\mathbf{e}_2$. Convince yourself that it follows that ρ_1 and ρ_2 are equivalent. ◇

Remark: Note that in general a single representation $G \to GL(V)$ in an m-dimensional $\mathbb{K}$-space V could define different (but equivalent) representations $G \to GL(m, \mathbb{K})$ if the corresponding matrices were written with respect to different bases of V. Since we normally interpret matrices as transformations using the standard basis of V, our convention is that we say two representations of a group G in a space V are equal or equivalent according as the representations $G \to GL(V)$ are equal or equivalent.

Exercises

5. In Example 13, let B be the matrix of $\rho_2(a)$ with respect to the basis $\{\mathbf{e}_1, \mathbf{e}_2\}$. Find a matrix C for τ with respect to this basis, and verify that $B = CAC^{-1}$.

6. Equivalent representations:

(a) Let $\rho_1 : G \to GL(V)$ be any representation of a group G in a vector space V, and let $\tau \in GL(V)$ be a fixed transformation. Define a function $\rho_2 : G \to GL(V)$ by

$$\rho_2(g) = \tau\, \rho_1(g)\, \tau^{-1}$$

for all $g \in G$. Show that ρ_2 is again a representation of G in V.

(b) Let G be any group and let V be any vector space. Define a relation $\sim$ on the set of *all* representations of G in V by

$\rho_1 \sim \rho_2$ if and only if there exists a $\tau \in GL(V)$ such that for all $g \in G$, $\rho_2(g) = \tau\rho_1(g)\tau^{-1}$. Show that $\sim$ is an equivalence relation on the set of all representations of G in V.

7. Let G be the *Klein-four group*: $G = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle$, and let ρ_{reg} be the regular representation of G. Write down the matrices for the different $\rho_{reg}(g)$ with respect to the basis $\{\mathbf{e}_1, \mathbf{e}_a, \mathbf{e}_b, \mathbf{e}_{ab}\}$. (Note that the relation $ab = ba$ is a consequence of $(ab)^2 = 1$.) Ⓢ

8. Let $G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$, and let ρ_{reg} be the regular representation of G.

(a) Write down the matrices for $\rho_{reg}\big((12)\big)$ and $\rho_{reg}\big((13)\big)$ with respect to the basis $\{e_h \mid h \in G\}$. (Use the same order for the basis vectors that was used above in listing the elements of G.)

(b) Find *two* (linearly independent) vectors that are eigenvectors for *both* $\rho_{reg}\big((12)\big)$ and $\rho_{reg}\big((13)\big)$. Ⓗ

(c) Use your work from part (b) to find a *nontrivial* representation of degree 1 of G (that is, a nontrivial homomorphism $G \to \mathbb{C}^*$). What is the kernel of this homomorphism? Does this homomorphism look familiar?

10.3. Maschke's Theorem

Sums of representations. Irreducible representations are the building blocks for all representations, much as the prime numbers are the building blocks for all integers ≥ 2. In the case of the integers, we build by multiplying. In this section we define what we mean by adding representations. For integers, we know every integer ≥ 2 can be factored into primes, and this factorization is unique up to the order of factors. For representations, Maschke's Theorem guarantees that an arbitrary representation can be decomposed into a sum of irreducible representations. In Chapter 11 we see that the irreducible components are uniquely determined up to equivalence and order of the summands.

To begin, we define direct sums of vector spaces. Just as with groups, we have the concept of external direct sum (adding two vector spaces that exist independently) and internal direct sum (breaking an existing vector space into a sum of vector subspaces). We then use the direct sums of vector spaces to define direct sums of representations.

Definition. Let V_1 and V_2 be two vector spaces over the field $\mathbb{K}$. The external direct sum of V_1 and V_2, denoted by $V_1 \oplus V_2$, is the Cartesian product of V_1 and V_2. Let $\mathbf{v}_j, \mathbf{w}_j \in V_j$ for $j = 1, 2$ and $c \in \mathbb{K}$. We then define addition and scalar multiplication on $V_1 \oplus V_2$:

$$\begin{aligned}(\mathbf{v}_1, \mathbf{v}_2) + (\mathbf{w}_1, \mathbf{w}_2) &= (\mathbf{v}_1 + \mathbf{w}_1,\ \mathbf{v}_2 + \mathbf{w}_2)\\ c\,(\mathbf{v}_1, \mathbf{v}_2) &= (c\,\mathbf{v}_1, c\,\mathbf{v}_2).\end{aligned}$$

These definitions make $V_1 \oplus V_2$ a vector space over $\mathbb{K}$. We write $\mathbf{0}_1$ and $\mathbf{0}_2$ for the zero vectors of V_1 and V_2, so $\mathbf{0} = (\mathbf{0}_1, \mathbf{0}_2)$ is the zero vector of vector space $V_1 \oplus V_2$. We can use bases of V_1 and V_2 to construct a basis for $V_1 \oplus V_2$, as in the following theorem.

Theorem 10.1. *Let $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m\}$ be a basis for V_1 and let $\{\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_\ell\}$ be a basis for V_2. Then*

$$\Big\{ (\mathbf{e}_1, \mathbf{0}_2), (\mathbf{e}_2, \mathbf{0}_2), \ldots, (\mathbf{e}_m, \mathbf{0}_2), (\mathbf{0}_1, \mathbf{f}_1), (\mathbf{0}_1, \mathbf{f}_2), \ldots, (\mathbf{0}_1, \mathbf{f}_\ell) \Big\}$$

is a basis for $V_1 \oplus V_2$, where $\mathbf{0}_1$ and $\mathbf{0}_2$ are the zero vectors of V_1 and V_2 respectively.

Note that the subspace $V_1' = \{(\mathbf{v}_1, \mathbf{0}_2) \mid \mathbf{v}_1 \in V_1\}$ of the external direct sum is isomorphic to V_1. Similarly, the subspace $V_2' = \{(\mathbf{0}_1, \mathbf{v}_2) \mid \mathbf{v}_2 \in V_2\}$ is isomorphic to V_2. We often identify V_1' with V_1 and V_2' with V_2. Although $V_1' \cap V_2' = \{\mathbf{0}\}$, this is not in general true for subspaces V_1 and V_2 of a vector space V. This accounts for the second hypothesis in the following theorem.

Theorem 10.2. *If a vector space V has two subspaces V_1 and V_2 such that*

(i) Any vector in V can be written as the sum of a vector in V_1 and a vector in V_2 (in shorthand, $V = V_1 + V_2$), and

(ii) $V_1 \cap V_2 = \{\mathbf{0}\}$,

then the transformation $V_1 \oplus V_2 \to V$ defined by $(\mathbf{v}_1, \mathbf{v}_2) \mapsto \mathbf{v}_1 + \mathbf{v}_2$ is an isomorphism of vector spaces. In other words, the transformation is one-to-one and onto as well as linear.

In this situation V is called the internal direct sum of V_1 and V_2, and we write $V \cong V_1 \oplus V_2$. The second condition guarantees that each vector in V is represented *uniquely* as a sum $\mathbf{v}_1 + \mathbf{v}_2$ with $\mathbf{v}_j \in V_j$ for $j = 1, 2$.

Example 14. Let $V = \mathbb{R}^m$ with the usual dot product, and assume W is a subspace of V. We know from linear algebra that

$$W^\perp = \{\mathbf{v} \in V \mid \mathbf{v} \cdot \mathbf{w} = 0 \text{ for all } \mathbf{w} \in W\}$$

is a subspace of V, and V is the internal direct sum of W and $W^\perp$. ◇

Now we link sums of vector spaces with sums of representations. We know how to start with two vector spaces and form a new vector space, their direct sum. Similarly, we start with two representations of a group G and form a new representation, their direct sum. Under certain conditions we can decompose a single vector space into a direct sum of two subspaces. Similarly, we start with a single representation and, under suitable conditions, decompose it into a direct sum of representations.

Definition. Let ρ_1 and ρ_2 be representations of G in vector spaces V_1 and V_2 respectively over $\mathbb{K}$. The direct sum of representations ρ_1 and ρ_2, denoted $\rho_1 \oplus \rho_2$, is the function from G to $GL(V_1 \oplus V_2)$ such that for any $(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \oplus V_2$,

$$\big(\rho_1 \oplus \rho_2\big)(g) : (\mathbf{v}_1, \mathbf{v}_2) \;\mapsto\; \Big(\rho_1(g)(\mathbf{v}_1),\, \rho_2(g)(\mathbf{v}_2)\Big).$$

Theorem 10.3. *Let ρ_1 and ρ_2 be representations of the finite group G in vector spaces V_1 and V_2 respectively over the field $\mathbb{K}$.*

(i) The direct sum $\rho_1 \oplus \rho_2$ is a representation of G in $V_1 \oplus V_2$.

(ii) The representations $\rho_1 \oplus \rho_2$ and $\rho_2 \oplus \rho_1$ are equivalent.

(iii) Assume $\mathbf{e}_i$ and $\mathbf{f}_j$ are bases for V_1 and V_2 respectively, as in Theorem 10.1. For $g \in G$, assume $A(g)$ and $B(g)$ are the matrices of $\rho_1(g)$ and $\rho_2(g)$ respectively with respect to these

bases. Then the matrix of $(\rho_1 \oplus \rho_2)(g)$ *with respect to the basis* $(\mathbf{e}_i, \mathbf{0}_2), (\mathbf{0}_1, \mathbf{f}_j)$ *of* $V_1 \oplus V_2$ *is*

$$\begin{bmatrix} A(g) & 0 \\ 0 & B(g) \end{bmatrix},$$

where the 0s denote zero matrices of the appropriate size.

We are now ready to state the fundamental theorem of group representations. We state it for representations over the complex numbers, since that is the version we will prove. It is actually true over any field of characteristic 0 or of prime characteristic not dividing the order of G.

Theorem 10.4. *(Maschke, 1898) Every representation of a finite group* G *in a finite-dimensional vector space* V *over* $\mathbb{C}$ *can be written as a direct sum of irreducible representations.*

We conclude this subsection with a definition and a theorem that we use in the proof of Maschke's Theorem. At one step of our argument, we need to break a representation into parts. We begin that decomposition by restricting the domain of the representation. We can restrict a representation of G in V to a G-invariant subspace W of V and obtain a representation of G in W. More formally, we have the following definition.

Definition. Let ρ be a representation of G in the vector space V, and let W be a G-invariant subspace of V. The restriction $\rho|_W$ of ρ is the mapping from G to transformations of W defined by $\rho|_W(g)(\mathbf{w}) = \rho(g)(\mathbf{w})$ for $\mathbf{w} \in W$.

Theorem 10.5. *For a* G*-invariant subspace* W*, the restriction* $\rho|_W$ *of* ρ *is a representation of* G *in* W*.*

In Figure 10.2 the degree 3 representation ρ maps the generator of the group to a 90-degree rotation of $\mathbb{R}^3$ around the z-axis (i.e., around the line spanned by $\mathbf{e}_3$). In this case the plane $W = \text{span}\{\mathbf{e}_1, \mathbf{e}_2\}$ is G-invariant, and the restriction $\rho|_W$ is the degree 2 representation of Example 3.

Complex inner products. Our discussion of Examples 1 and 5 provides hints that choosing an orthogonal complement is useful for decomposing a representation. Indeed, this is a crucial ingredient in our proof of Maschke's Theorem. Our representations are in complex vector spaces, so we need to define orthogonality for such spaces. The first step is to define inner products on complex vector spaces.

We begin by noting that simply adopting the familiar dot product on $\mathbb{R}^m$ for $\mathbb{C}^m$ is problematic, since we would then find that it is possible for a nonzero vector $\mathbf{v} \in \mathbb{C}^m$ to satisfy $\mathbf{v} \cdot \mathbf{v} = 0$. (You should find such an example, say in $\mathbb{C}^2$.) This would be a major impediment to defining "length" of a vector in a meaningful way. So we need a different approach.

In the special case of the 1-dimensional complex space $\mathbb{C}$, we already have a useful geometric interpretation based on identifying the complex number $z = a + bi$ with the vector (a, b) in $\mathbb{R}^2$. In that identification, the length of z is the positive square root of $z\overline{z}$, where $\overline{z} = a - bi$ is the complex conjugate of z. Combining this observation with the connection between length and dot product in $\mathbb{R}^m$ suggests the following definition. To avoid confusion[2] with the dot product on $\mathbb{R}^m$, we write $\langle \mathbf{v}, \mathbf{w} \rangle$ for the inner product of $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{C}^m$.

Definition. Consider vectors $\mathbf{v}, \mathbf{w} \in \mathbb{C}^m$, written here as row vectors $\mathbf{v} = (x_1, \ldots, x_m), \mathbf{w} = (y_1, \ldots, y_m)$. Then the standard inner product of $\mathbf{v}$ and $\mathbf{w}$ is given by

$$\langle \mathbf{v}, \mathbf{w} \rangle = \sum_{j=1}^{m} x_j \overline{y_j}.$$

Notice that this definition is equivalent to calculating the dot product of $\mathbf{v}$ and the complex conjugate of $\mathbf{w}$:

$$\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v} \cdot \overline{\mathbf{w}}.$$

[2] Context should make clear when we are using this notation for the inner product of two vectors and when we are using it for the subgroup or subspace generated by elements.

We enumerate the essential properties of this complex inner product by making a formal definition as follows.[3]

Definition. An inner product $\langle\ ,\ \rangle$ on a complex vector space V is a function from $V \times V$ to $\mathbb{C}$, such that for all vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and all scalars $c \in \mathbb{C}$:

(1) $\langle \mathbf{v}, \mathbf{w} \rangle = \overline{\langle \mathbf{w}, \mathbf{v} \rangle}$,

(2) $\langle \mathbf{u} + \mathbf{v}, \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{w} \rangle + \langle \mathbf{v}, \mathbf{w} \rangle$,

(3) $\langle c\,\mathbf{v}, \mathbf{w} \rangle = c\langle \mathbf{v}, \mathbf{w} \rangle$,

(4) $\langle \mathbf{v}, \mathbf{v} \rangle > 0$ for all $\mathbf{v} \neq \mathbf{0}$.

The standard inner product on $\mathbb{C}^m$ in fact has all of these properties. Note that we have lost part of the bilinearity of the dot product over $\mathbb{R}$. Instead this inner product is called "sesquilinear." (Sesqui means one and one half.[4])

From property 1 we know that $\langle \mathbf{v}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{v} \rangle}$, so $\langle \mathbf{v}, \mathbf{v} \rangle \in \mathbb{R}$. It is this that allows us to compare $\langle \mathbf{v}, \mathbf{v} \rangle$ with 0 in property 4. As a consequence of these properties we have the following result.

Theorem 10.6. *If $\langle\ ,\ \rangle$ is an inner product on the complex vector space V, and if $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ and $c \in \mathbb{C}$, then*

(5) $\langle \mathbf{u}, \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u}, \mathbf{v} \rangle + \langle \mathbf{u}, \mathbf{w} \rangle$,

(6) $\langle \mathbf{v}, c\,\mathbf{w} \rangle = \overline{c}\,\langle \mathbf{v}, \mathbf{w} \rangle$,

(7) $\langle \mathbf{v}, \mathbf{v} \rangle = 0$ *if and only if* $\mathbf{v} = \mathbf{0}$.

For a complex vector space, we can use the inner product to define the following geometric concepts.

Definition. Assume V is a complex vector space with inner product $\langle\ ,\ \rangle$, and $\mathbf{v}, \mathbf{w} \in V$. The length of $\mathbf{v}$ is the positive square root of $\langle \mathbf{v}, \mathbf{v} \rangle$. We say $\mathbf{v}$ and $\mathbf{w}$ are orthogonal if $\langle \mathbf{v}, \mathbf{w} \rangle = 0$.

[3] This is the usual definition in mathematics, with linearity in the first component. The convention in physics is linearity in the second component, so (3) becomes $\langle \mathbf{v}, c\mathbf{w} \rangle = c\langle \mathbf{v}, \mathbf{w} \rangle$.

[4] For example, Grinnell College celebrated its sesquicentennial (i.e., its 150-year anniversary) in 1996, and Mount Holyoke College celebrated its in 1987.

Since $\langle \mathbf{v}, \mathbf{v} \rangle \geq 0$ for all $\mathbf{v} \in V$ and $\langle \mathbf{v}, \mathbf{w} \rangle = 0$ if and only if $\langle \mathbf{w}, \mathbf{v} \rangle = 0$, these are reasonable definitions of length and of orthogonality. Exactly as in the real case, if V is a finite-dimensional complex vector space with an inner product, we can find an orthonormal basis for V using the Gram-Schmidt process. (See A.5.)

We can now define the orthogonal complement of a subspace.

Definition. Let V be a complex vector space, W a subspace of V, and $\langle\ ,\ \rangle$ an inner product on V. Then the orthogonal complement of W in V with respect to $\langle\ ,\ \rangle$ is

$$W^{\perp} = \{\mathbf{v} \in V \mid \langle \mathbf{v}, \mathbf{w} \rangle = 0 \text{ for all } \mathbf{w} \in W\}.$$

This language is justified by the following theorem.

Theorem 10.7. *If V is a complex vector space with an inner product and W is a subspace, then $W^{\perp}$ is a subspace and $V = W \oplus W^{\perp}$.*

Given this geometry on complex vector spaces, we wish to consider linear transformations that "preserve" the geometry, in the following sense.

Definition. Let V be a complex vector space with inner product $\langle\ ,\ \rangle$. A linear transformation $S : V \to V$ is called a unitary transformation with respect to $\langle\ ,\ \rangle$ if it preserves the inner product:

$$\langle S(\mathbf{v}), S(\mathbf{w}) \rangle = \langle \mathbf{v}, \mathbf{w} \rangle$$

for all $\mathbf{v}, \mathbf{w} \in V$.

How do we recognize a matrix that describes a unitary transformation?

Theorem 10.8. *Let V be a complex vector space with an inner product, and suppose $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m$ is an orthonormal basis for V. Let $S : V \to V$ be a linear transformation, and let A be the matrix of S with respect to this basis. Then S is a unitary transformation if and only if $A\overline{A}^T = \overline{A}^T A = I_m$ (where $\overline{A}^T$ denotes the conjugate transpose of A). Such a matrix is called a unitary matrix.*

Continuing the notation of the preceding theorem, we can always regard V as a real vector space by restricting scalars to $\mathbb{R}$. If the entries of A are all real, then we can regard S as a linear transformation of this real space. In that case S preserves the real inner product on the real space V if and only if A is an orthogonal matrix: $AA^T = A^TA = I_m$. Thus our definitions of an inner product on a complex space and of transformations preserving the inner product are natural generalizations of those for real vector spaces.

The reward for our introduction of this complex geometry is the following theorem.

Theorem 10.9. *Let ρ be a representation of the group G in a complex space V with an inner product. Assume that $\rho(g)$ is a unitary transformation for each $g \in G$. Let W be a G-invariant subspace of V. Then $W^\perp$ is also G-invariant.*

The proof of Maschke's Theorem. We introduced the complex inner product to help us prove Maschke's Theorem. However, as Theorem 10.9 suggests, the inner product will only be helpful if the transformations $\rho(g)$ for a representation ρ of G in V are actually unitary. Remarkably enough, given a finite group G and a representation ρ of G in a complex vector space V with an inner product, it is possible to define a *new* inner product on V for which each transformation $\rho(g)$ is indeed a unitary transformation.

Theorem 10.10. *Let $\langle\ ,\ \rangle$ be an inner product on the finite dimensional complex vector space V and let $\rho : G \to GL(V)$ be a representation of the finite group G. Then the new function $\ll , \gg$ defined by*

$$\ll \mathbf{v}, \mathbf{w} \gg \ = \ \frac{1}{|G|} \sum_{g \in G} \Big\langle\, \rho(g)(\mathbf{v}),\, \rho(g)(\mathbf{w}) \,\Big\rangle$$

is an inner product on V. Further, for every g in G, $\rho(g)$ is a unitary transformation with respect to this new inner product.

Proof. The properties required for $\ll , \gg$ to be an inner product follow directly from $\langle\ ,\ \rangle$ being an inner product and from $\rho(g)$ being

a linear transformation. As a sample, here we prove property 3:

$$\begin{aligned}
\ll c\,\mathbf{v}, \mathbf{w} \gg &= \frac{1}{|G|} \sum_{g \in G} \Big\langle \rho(g)(c\,\mathbf{v}),\, \rho(g)(\mathbf{w}) \Big\rangle \\
&= \frac{1}{|G|} \sum_{g \in G} \Big\langle c\rho(g)(\mathbf{v}),\, \rho(g)(\mathbf{w}) \Big\rangle \\
&= \frac{1}{|G|} \sum_{g \in G} c \Big\langle \rho(g)(\mathbf{v}),\, \rho(g)(\mathbf{w}) \Big\rangle \\
&= \frac{c}{|G|} \sum_{g \in G} \Big\langle \rho(g)(\mathbf{v}),\, \rho(g)(\mathbf{w}) \Big\rangle \\
&= c \ll \mathbf{v}, \mathbf{w} \gg .
\end{aligned}$$

We must also show that each linear transformation $\rho(g)$ is a unitary transformation. Thus we must show that for any $g \in G$, $\ll \mathbf{v}, \mathbf{w} \gg = \ll \rho(g)(\mathbf{v}), \rho(g)(\mathbf{w}) \gg$:

$$\begin{aligned}
\ll \mathbf{v}, \mathbf{w} \gg &= \frac{1}{|G|} \sum_{h \in G} \Big\langle \rho(h)(\mathbf{v}),\, \rho(h)(\mathbf{w}) \Big\rangle, \text{and} \\
\ll \rho(g)(\mathbf{v}), \rho(g)(\mathbf{w}) \gg &= \frac{1}{|G|} \sum_{h \in G} \Big\langle \rho(h)(\rho(g)(\mathbf{v})),\, \rho(h)(\rho(g)(\mathbf{w})) \Big\rangle \\
&= \frac{1}{|G|} \sum_{h \in G} \Big\langle \rho(hg)(\mathbf{v}),\, \rho(hg)(\mathbf{w}) \Big\rangle \\
&= \frac{1}{|G|} \sum_{h' \in G} \Big\langle \rho(h')(\mathbf{v}),\, \rho(h')(\mathbf{w}) \Big\rangle.
\end{aligned}$$

In the last line we substitute $h' = hg$. Since h' runs over all the elements in G as h does, this last sum is equal to $\ll \mathbf{v}, \mathbf{w} \gg$. □

Remark: We can think of this new inner product as an average over G of the old one. In this approach to representation theory, we will use this trick of taking averages (or sums) over G in many situations. (The proof of Theorem 10.12 is another example.) It thus becomes a valuable strategy, not just a trick.

In Example 1 we used the standard basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3\}$. In the complex version, this is an orthonormal basis with respect to the standard inner product on $\mathbb{C}^3$. Each M_π is a unitary matrix, so each transformation $\rho(\pi)$ is unitary. The plane orthogonal to the vector $\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3$ is thus an invariant subspace for all six linear transformations. (Compare Exercise 3.)

We are now ready to prove Theorem 10.4, which we restate for reference.

Theorem *(Maschke): Every representation of a finite group G in a finite-dimensional vector space V over $\mathbb{C}$ can be written as a direct sum of irreducible representations.*

Proof. Let ρ be a representation of G in V over $\mathbb{C}$. We proceed by induction on the dimension m of V. If $m = 1$, then ρ is irreducible. Now let $m > 1$ and assume that the theorem is true for representations of degree less than m.

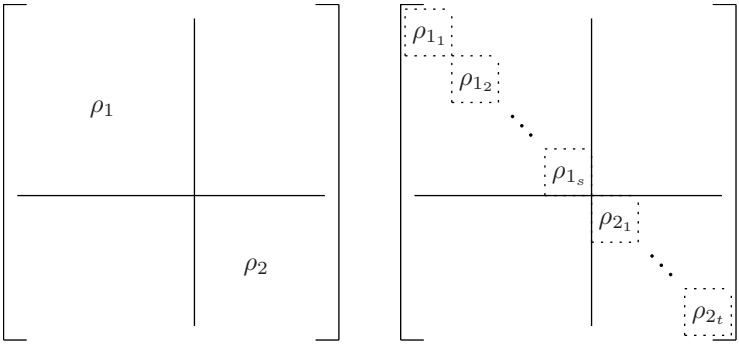
If ρ is irreducible, we are done. If not, there is a nontrivial subspace W of V that is invariant for $\rho(g)$ for all $g \in G$. We use Theorem 10.10 to define an inner product on V so that each transformation $\rho(g)$ is unitary. Define $W^\perp$ to be the orthogonal complement of W with respect to this new inner product. By Theorems 10.9 and 10.7, we know that $W^\perp$ is also a G-invariant subspace and that $V = W \oplus W^\perp$.

Next we define ρ_1 to be ρ restricted to W and ρ_2 to be ρ restricted to $W^\perp$. Then ρ is equal to the direct sum $\rho_1 \oplus \rho_2$. Both W and $W^\perp$ have dimension smaller than m, so by our induction hypothesis,

$$\rho_1 = \rho_{1_1} \oplus \cdots \oplus \rho_{1_s} \quad \text{and} \quad \rho_2 = \rho_{2_1} \oplus \cdots \oplus \rho_{2_t}$$

for irreducible representations ρ_{i_j} of G. Therefore ρ is the direct sum of the ρ_{i_j}. Figure 10.4 illustrates the decomposition of the matrix $\rho(g)$ (where we omit the argument g). □

Maschke's Theorem guarantees the decomposition of an arbitrary complex representation into its irreducible constituents. However, finding those irreducibles is not always easy. In the next chapter we introduce the theory of group characters to aid this work.



(a) Partial decomposition

(b) Complete decomposition

Figure 10.4. Decomposition into irreducible representations

Exercises

9. Let ρ be a representation of G in V, and let W be a G-invariant subspace of V. Show that the restriction $\rho|_W$ is a representation of G in W.

10. Prove Theorem 10.1.

11. Prove Theorem 10.2.

12. Prove Theorem 10.3.

(a) Prove part (i). Ⓢ

(b) Prove part (ii).

(c) Prove part (iii).

13. Prove Theorem 10.6.

14. Prove Theorem 10.8. Ⓗ

15. Prove Theorem 10.9.

16. Complete the proof of Theorem 10.10.

17. Let G be the group $\langle a \mid a^2 = 1 \rangle$ and let $V = \mathbb{C}^2$.

(a) Show that there exists a representation ρ of G in $V = \mathbb{C}^2$ for which the matrix of $\rho(a)$ with respect to the standard basis is $\begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix}$.

(b) Using the standard inner product on $\mathbb{C}^2$ as the "original" inner product $\langle\ ,\ \rangle$ on V, let $\ll , \gg$ be the "new" inner product on V defined in Theorem 10.10. Find explicit formulas for $\ll (x_1, x_2), (y_1, y_2) \gg$ and $\ll (x_1, x_2), (x_1, x_2) \gg$. (Note that the vectors here are really column vectors.)

(c) Find an orthonormal basis of V with respect to $\ll , \gg$.

(d) Find the matrix of $\rho(a)$ with respect to your basis from part (c). (It should be a unitary matrix!)

(e) Find two 1-dimensional invariant subspaces of $V = \mathbb{C}^2$ (under ρ), and show that they are orthogonal complements of each other with respect to $\ll , \gg$.

18. Prove Theorem 10.7 by proceeding as follows:

(a) Show that $W \cap W^\perp = \{\mathbf{0}\}$.

(b) Show that every vector in V can be written as the sum of a vector in W and a vector in $W^\perp$.

19. Let G be any finite group, and let $\rho_{reg} : G \to GL(V)$ be the regular representation over $\mathbb{C}$. This means that vector space V has basis $\{\mathbf{e}_h \mid h \in G\}$.

(a) Show that the vector $\mathbf{v} = \sum_{h \in G} \mathbf{e}_h$ is an eigenvector for $\rho_{reg}(g)$ for *each* $g \in G$. (Hence $\mathbf{v}$ spans an invariant subspace of V under ρ_{reg}.)

(b) Suppose that G_1 is a subgroup of G of index 2. Show that the vector

$$\mathbf{w} = \sum_{h \in G_1} \mathbf{e}_h \ - \sum_{h \in G \setminus G_1} \mathbf{e}_h$$

is an eigenvector for *each* of the $\rho_{reg}(g)$, for $g \in G$. Ⓗ

(c) Explain why the results of Exercise 8 are really examples of parts (a) and (b) of this exercise.

20. Let G be the symmetric group S_m and let ρ be the natural representation of G in $V = \mathbb{C}^m$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_m$ be the standard basis of V and let U be the 1-space spanned by $\mathbf{e}_1 + \cdots + \mathbf{e}_m$.

(a) Show that the subspace $W = \left\{ \sum_j a_j \mathbf{e}_j \;\middle|\; \sum_j a_j = 0 \right\}$ is equal to $U^\perp$ with respect to the standard inner product.

(b) Compare this to your answers to Exercises 2 and 3.

21. Let $G = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle$ be the "Klein four-group" (as in Exercise 7), and let ρ_{reg} be the regular representation of G in $V = \mathbb{C}^4$. Write ρ_{reg} as a direct sum of irreducible representations. Ⓗ

10.4. Representations and difference sets

We apply representation theory to the study of difference sets by extending a group representation $\rho : G \to GL(m, \mathbb{C})$ to a ring homomorphism $\widetilde{\rho}$ from the integral group ring $\mathbb{Z}G$ to the ring $\mathcal{M}(m, \mathbb{C})$ of $m \times m$ matrices with entries in $\mathbb{C}$. The following example illustrates the idea. In the example, the degree of the representation is 1, and we identify $\mathcal{M}(1, \mathbb{C})$ with $\mathbb{C}$.

Example 15. Let $G = \langle a, b \,|\, a^4 = b^4 = 1, ab = ba \rangle$. The set $D = \{a^2, b, ab, a^2b, b^2, ab^3\}$ is a $(16, 6, 2)$-difference set in G. Define a representation ρ of G by $\rho(a) = 1$ and $\rho(b) = i$, so the kernel of ρ is $N = \langle a \rangle$. Let $n_j = |D \cap b^j N|$ for $j = 0, \ldots, 3$. Notice that the intersection numbers for D modulo N are $(n_0, \ldots, n_3) = (1, 3, 1, 1)$. Consider the following sums:

$$\sum_{g \in D} \rho(g) = 1(1) + 3(i) + 1(i^2) + 1(i^3) = 2i = z,$$

$$\sum_{g \in D} \rho(g^{-1}) = 1(1) + 3(i^3) + 1(i^2) + 1(i) = -2i = u.$$

We find that $u = \bar{z}$ and $z\bar{z} = 4 = n$. ◇

Factoring 4 in this way is an instance of a general pattern. The key to the generalization is the following definition.

Definition. Let G be a group and $\rho : G \to GL(m, \mathbb{C})$ a representation of G. Define $\widetilde{\rho} : \mathbb{Z}G \to \mathcal{M}(m, \mathbb{C})$ by

$$\widetilde{\rho}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g\, \rho(g).$$

Theorem 10.11. *If $\rho : G \to GL(m, \mathbb{C})$ is a representation of the group G, then the mapping $\widetilde{\rho} : \mathbb{Z}G \to \mathcal{M}(m, \mathbb{C})$ is a ring homomorphism.*

When we apply $\widetilde{\rho}$ to the integral group ring equation $DD^{(-1)} = n1_G + \lambda G$ we get

$$\widetilde{\rho}(D)\widetilde{\rho}(D^{(-1)}) = nI_m + \lambda\widetilde{\rho}(G). \tag{8}$$

Returning to our example,

$$\begin{aligned}
\widetilde{\rho}(D) &= 1(1) + 3(i) + 1(i^2) + 1(i^3) = 2i = z,\\
\widetilde{\rho}(D^{(-1)}) &= 1(1) + 3(i^3) + 1(i^2) + 1(i) = -2i = \bar{z}, \text{ and}\\
\widetilde{\rho}(G) &= 4(1) + 4(i) + 4(-1) + 4(-i) = 0.
\end{aligned}$$

Equation 8 therefore implies $z\bar{z} = 4$, as we had previously observed.

Three aspects of this example generalize. First, the intersection numbers for D modulo the kernel of ρ can be seen as coefficients in $\widetilde{\rho}(D)$, so knowing the possible values of $\widetilde{\rho}(D)$ constrains the possible values of these intersection numbers. Second, we have the following theorem.

Theorem 10.12. *Let $\rho : G \to GL(m, \mathbb{C})$ be a nontrivial irreducible representation of the finite group G. Then*

$$\widetilde{\rho}(G) = \sum_{g\in G} \rho(g) = 0_m.$$

By Theorem 10.12, whenever a group G contains a (v, k, λ)-difference set D, and ρ is any nontrivial irreducible representation of G of degree m, we have

$$\widetilde{\rho}(D)\widetilde{\rho}(D^{(-1)}) = nI_m. \tag{9}$$

Equation 9 restricts the possible values of $\widetilde{\rho}(D)$, and we use it often.

We also know that we can define an inner product on $\mathbb{C}^m$ for which $\rho(g)$ is a unitary matrix for every $g \in G$. In particular, this tells us that $\rho(d^{-1}) = \overline{\rho(d)}^T$ for each $d \in D$. Therefore if $M = \widetilde{\rho}(D)$ then $\overline{M}^T = \widetilde{\rho}(D^{(-1)})$, and we have

$$M\overline{M}^T = nI_m.$$

We have proved the following theorem—our third generalization.

Theorem 10.13. *Let G be a group and D a (v, k, λ)-difference set in G. Let $\rho : G \to GL(m, \mathbb{C})$ be a nontrivial irreducible representation of G and $\widetilde{\rho}$ the corresponding ring homomorphism from $\mathbb{Z}G$ to the ring $\mathcal{M}(m, \mathbb{C})$. Write $M = \widetilde{\rho}(D)$. Then $\widetilde{\rho}(D^{(-1)}) = \overline{M}^T$ and $M\overline{M}^T = nI_m$.*

In the special case $m = 1$, the image of D under $\widetilde{\rho}$ is a complex number z, and we have $z\overline{z} = n$. In Chapter 12, we use both this special case and also the matrix equation, along with some algebraic number theory, either to search for difference sets or to rule out their existence. In Section 11.4, we obtain useful preliminary results.

Another useful fact for the study of difference sets is that every element $g \in G$ is determined by its image under the regular representation ρ_{reg}. This is because

$$\rho_{reg}(g) : \mathbf{e}_{1_G} \mapsto \mathbf{e}_g.$$

More generally, we have the following theorem, which we apply in Section 11.4.

Theorem 10.14. *Let G be a finite group and ρ_{reg} the regular representation of G. Suppose $A, B \in \mathbb{Z}G$ with $\widetilde{\rho}_{reg}(A) = \widetilde{\rho}_{reg}(B)$. Then $A = B$.*

Exercises

22. This exercise produces a proof of Theorem 10.11 that takes advantage of our work on the integral group ring in Section 7.1. Assume $\rho : G \to GL(m, \mathbb{C})$ is a representation of the group G, and let $H = \rho(G) \subset GL(m, \mathbb{C})$.

(a) Define a function $\Phi : \mathbb{Z}H \to \mathcal{M}(m, \mathbb{C})$ taking the formal sum $\sum_h a_h h$ to the corresponding actual sum of scalar multiples of matrices. Show that Φ is a ring homomorphism.

(b) Recall from Section 7.1 that we used the homomorphism $\rho : G \to H$ to define a ring homomorphism $\widehat{\rho} : \mathbb{Z}G \to \mathbb{Z}H$ by $\widehat{\rho}(\sum_g a_g g) = \sum_g a_g \rho(g)$. Show that $\Phi \circ \widehat{\rho} = \widetilde{\rho}$.

23. Prove Theorem 10.12.

24. Prove Theorem 10.14.

25. Let $G = \langle a, b \mid a^4 = b^4 = 1, ab = ba \rangle$, and suppose G contains a $(16, 6, 2)$-difference set D (not assumed to be the difference set in Example 15). Define the homomorphism $\rho : G \to \mathbb{C}^*$ by $\rho(a) = 1$ and $\rho(b) = i$. Let $z = \widetilde{\rho}(D)$ and $u = \widetilde{\rho}(D^{(-1)})$. Both z and u are in $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, the ring of Gaussian integers.

(a) Explain why $u = \bar{z}$ and $z\bar{z} = 4$. Use what you know about arithmetic in $\mathbb{Z}[i]$ to explain why $z\bar{z} = 4$ implies $z = \pm 2$ or $\pm 2i$.

(b) Let $N = \langle a \rangle$, and suppose $n_j = |D \cap b^j N|$. Explain why the fact that z must equal either ± 2 or $\pm 2i$ implies that either $n_0 = n_2$ or $n_1 = n_3$.

(c) Show that, in some order, the four intersection numbers mod N must be either $1, 1, 1, 3$ or $2, 2, 2, 0$. Also, explain why, without loss of generality, we may assume n_0 is the different value among the four.

(d) Look at the difference sets in this group on Kibler's list:

$$\begin{aligned} D_3 &= \{1,\ a,\ a^2,\ b,\ ab^2,\ a^2b^3\}, \\ D_4 &= \{1,\ a,\ a^2,\ b,\ b^3,\ a^3b^2\}, \\ D_5 &= \{1,\ a,\ b,\ a^2b,\ ab^2,\ a^2b^2\}. \end{aligned}$$

What are the intersection numbers mod N for each of these difference sets?

Coda

Just as the primes are the (multiplicative) building blocks for the integers, irreducible representations are the (additive) building blocks for representations of finite groups. Maschke's Theorem is our key result. It says that every representation is expressible as a sum of irreducible representations. The proof of Maschke's Theorem is complicated. Running through many of the arguments is the potent idea of averaging (more generally, summing) over a group.

We work over the complex numbers. The powerful facts that the field $\mathbb{C}$ is algebraically closed and has characteristic 0 give us an efficient route to the proof of Maschke's Theorem—one exploiting the nice properties of inner products in complex vector spaces and of unitary transformations of those spaces.

This chapter concludes by linking representation theory to the existence question for difference sets. Extending a representation $\rho : G \to GL(m, \mathbb{C})$ to a ring homomorphism $\widetilde{\varphi} : \mathbb{Z}G \to \mathcal{M}(m, \mathbb{C})$ translates the existence question to one in algebraic number theory.

A more general version of Maschke's Theorem applies over arbitrary fields with characteristic 0 or p relatively prime to the order of the group. The proof of this version of the theorem uses projections onto subspaces. A source for the proof of this stronger theorem is Curtis and Reiner's classic monograph [**15**], Section 10.8.

It takes us well beyond the scope of our work, but a theory of representations of infinite groups does exist—part of what is called "harmonic analysis." Representations of infinite "Lie groups" are important in physics. Under suitable hypotheses, satisfied by Lie groups, finite sums over the group can be replaced by integrals. There is also a "modular theory" of representations of finite groups over fields of characteristic p dividing the group order. Modular representation theory played an important role in early work on the classification of the finite simple groups.

Chapter 11

Group Characters

In this chapter we shift our attention from a complex representation ρ of G and the transformations $\rho(g)$ to a new function $\chi_\rho : G \to \mathbb{C}$, called the character of ρ, given by the trace: $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ for $g \in G$. It might seem that starting with a group representation and computing its character throws away much of the information about that representation. On the contrary, we find that the character "determines the representation;" that is, two representations having the same character must be equivalent. Moreover, properties of characters enable us to determine whether a representation is irreducible and to find its irreducible components when it is not.

After definitions, examples and some preliminary results in Section 1, we state in Section 2 what we call the Fundamental Theorem of Character Theory and look at some important consequences. The proof of the Fundamental Theorem is in Section 3. We return to difference sets and group rings in Section 4, where we consider examples drawn from Smith's paper [**65**] and also theorems culminating in characterizations of difference sets using representations. In Section 5 we take a brief look at character tables. Throughout, our vector spaces are over $\mathbb{C}$ and our groups are finite.

11.1. Definitions and examples

Let T be a linear transformation of a vector space V, and let M be the matrix for T with respect to a fixed basis for V. Recall from linear algebra that the trace of T is $\mathrm{Tr}(M)$. (See A.1.)

Definition. Let G be a finite group and let $\rho : G \to GL(V)$ be a representation of G in a finite-dimensional complex vector space. The character χ_ρ of ρ is the function $\chi_\rho : G \to \mathbb{C}$ defined by $\chi_\rho(g) = \mathrm{Tr}\big(\rho(g)\big)$ for all $g \in G$. The degree of χ_ρ is the degree of ρ, namely the dimension of the vector space V. If ρ is irreducible, then χ_ρ is called an irreducible character. If ρ is the trivial representation (mapping each group element to 1), then χ_ρ is the trivial character.

When the degree of χ_ρ is 1, then $\chi_\rho = \rho$ (identifying a 1×1 matrix $[a]$ and its trace a), and χ_ρ is a homomorphism from G to the multiplicative group $\mathbb{C}^*$. However, for degrees greater than 1, characters are not homomorphisms. Since for any representation ρ of degree m, $\rho(1_G) = I_m$, we have that $\chi_\rho(1_G)$ gives the degree of χ_ρ.

Example 1. Let ρ be the natural representation of $G = S_3$ given in Example 10.1 (but work over the complex numbers). Since $\rho(g)$ is a permutation matrix for each $g \in G$, its trace $\chi_\rho(g)$ counts the elements that are fixed by the permutation. So we have

$$\begin{aligned} \chi_\rho\big(1_G\big) &= 3, \\ \chi_\rho\big((12)\big) &= 1, \\ \chi_\rho\big((13)\big) &= 1, \\ \chi_\rho\big((23)\big) &= 1, \\ \chi_\rho\big((123)\big) &= 0, \\ \chi_\rho\big((132)\big) &= 0. \end{aligned}$$

In this case, the values of the character are integers. ◇

Example 2. Recall the representation of the group $G = \langle a \mid a^5 = 1 \rangle$ with $\rho(a) = e^{2\pi i/5}$. Since the representation is degree 1 the character coincides with the representation. In this case the character is a homomorphism, and the values it takes are fifth roots of unity. ◇

Example 3. Recall the representation ρ of the dihedral group $G = \langle a, b \mid a^5 = b^2 = 1,\ bab^{-1} = a^{-1} \rangle$ in Example 10.9:

$$\rho(a) = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix} \quad \text{and} \quad \rho(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where $\eta = e^{2\pi i/5}$. Call its character χ. Convince yourself that $\chi(a^j b) = 0$ for $j = 0, 1, \ldots, 4$. What about the values of χ on the rotations a^j? We have $\chi(a^j) = \eta^j + \eta^{-j}$, a sum of roots of unity. Since the inverse of a root of unity is its complex conjugate, we see that $\chi(a^j)$ is a real number. Of course $\chi(1_G) = 2$, but the other values $\chi(a^j)$ are not integers. Still,

$$\begin{aligned} \sum_{g \in G} \chi(g) &= (1+1) + (\eta + \eta^4) + (\eta^2 + \eta^3) + (\eta^3 + \eta^2) + (\eta^4 + \eta) \\ &= 0, \end{aligned}$$

since $1 + \eta + \cdots + \eta^4 = (\eta^5 - 1)/(\eta - 1) = 0$. We encounter other nice character sums later. ◇

Example 4. Let G be any group, and let ρ_{reg} be the regular representation of G in the complex vector space V. If G has m elements, then V has dimension m, and with respect to the basis $\{\mathbf{e}_h \mid h \in G\}$, each $\rho_{reg}(g)$ is an $m \times m$ permutation matrix. The trace of a permutation matrix is the number of fixed points, so $\chi_{reg}(1_G) = m$, and $\chi_{reg}(g) = 0$ for all $g \neq 1_G$. ◇

Recall that Maschke's Theorem tells us that every representation is a sum of irreducible representations. The next theorem describes the character of a sum of representations.

Theorem 11.1. *Let χ_1 and χ_2 be characters of G associated with representations ρ_1 and ρ_2 respectively. Define the function $\chi_1 + \chi_2 : G \to \mathbb{C}$ by $(\chi_1 + \chi_2)(g) = \chi_1(g) + \chi_2(g)$ for $g \in G$. Then $\chi_1 + \chi_2$ is the character of G associated with the representation $\rho_1 \oplus \rho_2$.*

Along with Maschke's Theorem, Theorem 11.1 tells us that every character is a sum of irreducible characters. We combine this decomposition with the Fundamental Theorem of Character Theory (in the next section) to obtain powerful results.

In the examples that we have seen thus far, $\chi(g)$ is equal to a sum of roots of unity for $g \in G$. The following lemma helps us show that this is true in general. This fact enables us to prove that for any representation ρ of a finite group G over $\mathbb{C}$, the value of $\chi_\rho(g^{-1})$ is the complex conjugate of $\chi_\rho(g)$.

Lemma 11.2. *If G is a finite group of order m, and if $\rho : G \to GL(V)$ is a representation, then for any transformation $\rho(g)$, if λ is an eigenvalue, then λ is an mth root of unity. In particular, $|\lambda| = 1$ so $1/\lambda = \overline{\lambda}$.*

Proof. Let λ be an eigenvalue for $\rho(g)$ with eigenvector $\mathbf{v}$. So $\rho(g)(\mathbf{v}) = \lambda\mathbf{v}$. Since $g^m = 1_G$, we know that $\rho(g^m) = \rho(1_G) = I$, the identity map. Therefore, $\rho(g^m)(\mathbf{v}) = \rho(g)^m(\mathbf{v}) = \lambda^m\mathbf{v} = \mathbf{v}$. We conclude that $\lambda^m = 1$, and $|\lambda| = 1$. □

Theorem 11.3. *If G is a finite group, $g \in G$, and ρ is a representation of G over $\mathbb{C}$, then*

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

Proof. Fix a basis for V, and let $\rho(g) = A$ with respect to this basis. Since ρ is a group homomorphism, $\rho(g^{-1}) = A^{-1}$. Let λ_j be the eigenvalues for matrix A, counting algebraic multiplicities. From linear algebra we know that $\chi_\rho(g) = \mathrm{Tr}(A) = \sum \lambda_j$. (See A.2.) The eigenvalues of A^{-1} are the inverses of the λ_js. So $\chi_\rho(g^{-1}) = \mathrm{Tr}(A^{-1}) = \sum 1/\lambda_j$. By Lemma 11.2, $1/\lambda_j = \overline{\lambda_j}$ for each j, so

$$\begin{aligned}\chi_\rho(g^{-1}) &= \mathrm{Tr}(A^{-1}) = \sum \frac{1}{\lambda_j} = \sum \overline{\lambda_j} = \overline{\sum \lambda_j} \\ &= \overline{\mathrm{Tr}(A)} = \overline{\chi_\rho(g)}.\end{aligned}$$

□

Note that the previous theorem makes no assumption that the matrix for $\rho(g)$ is unitary.

Exercises

1. Let $G = \langle a \mid a^2 = 1 \rangle$ and let ρ be the representation of G given by

$$\rho(a) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let χ_ρ be the character of ρ. What is the value of $\chi_\rho(a)$? Write this value as a sum of eigenvalues of $\rho(a)$.

2. Let $G = S_4$ and let ρ be the natural representation of G of degree 4, and let χ_ρ be its character. List the elements $g \in G$ for which:

(a) $\chi_\rho(g) = 0$.
(b) $\chi_\rho(g) = 1$.
(c) $\chi_\rho(g) = 2$. Ⓢ
(d) $\chi_\rho(g) = 3$.
(e) $\chi_\rho(g) = 4$.

3. Let $G = D_4 = \{R_0, R_{90}, R_{180}, R_{270}, F_H, F_V, F_1, F_2\}$, the dihedral group of order 8 described as the group of symmetries of a square, and let ρ be the corresponding representation of degree 2. (See Exercise 10.1, page 175.) Find $\chi_\rho(g)$ for each $g \in G$.

4. Prove Theorem 11.1.

11.2. The Fundamental Theorem

We study group characters to investigate the irreducible representations of a group. As often happens in mathematics, we will learn more about characters if we step back and study a more general set of functions that includes the characters. The Fundamental Theorem of Character Theory describes the relationship of the characters to this larger set. We state it after introducing the necessary ideas.

Since homomorphisms map conjugate group elements to conjugates, and representations are homomorphisms, representations take conjugate group elements to similar matrices. Since similar matrices

have equal traces, group characters are functions that are constant on conjugacy classes.

Definition. A function α from the group G to the complex numbers is called a class function if it is constant on each conjugacy class of G; that is, if $g, h \in G$ are conjugate, then $\alpha(g) = \alpha(h)$.

Characters of representations are thus class functions. The set $\mathcal{V}$ of all class functions on a group G has algebraic structure. If α and β are class functions on G, define their sum by $(\alpha+\beta)(g) = \alpha(g)+\beta(g)$ for $g \in G$. For a complex scalar c, define $(c\alpha)(g) = c\,\alpha(g)$. With these definitions, we have the following theorem.

Theorem 11.4. *The set $\mathcal{V}$ of class functions on a finite group G is a complex vector space with dimension equal to the number of conjugacy classes in G.*

Proof. We claim that $\mathcal{V}$ is indeed a vector space. To show that its dimension equals the number of conjugacy classes, we provide a basis for $\mathcal{V}$. Let $\alpha_j : G \to \mathbb{C}$ be the function that takes the value 1 on elements of the jth conjugacy class, and 0 elsewhere. The functions α_j are independent, since if $\sum c_j\alpha_j = 0$, then, in particular, for each j the sum has value zero on g in the jth conjugacy class. This forces $c_j = 0$. Further, these functions span the vector space of class functions: if $\beta \in \mathcal{V}$ has value c_j on the jth conjugacy class, then $\beta = \sum_j c_j\alpha_j$. □

Next we define an inner product on $\mathcal{V}$. We refer to the inner product space $\mathcal{V}$ as the space of class functions on G.

Definition. Let α, β be class functions from G to $\mathbb{C}$. We define the inner product of two class functions

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\ \overline{\beta(g)}.$$

This really is an inner product on the complex space $\mathcal{V}$. Notice that if $|G| = m$ and if you think of a class function α as an m-tuple of complex numbers whose components are the values $\alpha(g)$ as g ranges

over the elements of G, then this inner product resembles the standard inner product on $\mathbb{C}^m$.

The main result in this chapter, which we call the Fundamental Theorem of Character Theory[1], is that the set of irreducible characters of G is an orthonormal basis for the space $\mathcal{V}$ of class functions on G.

Theorem 11.5. *(Fundamental Theorem of Character Theory) Let G be a finite group and let $\mathcal{V}$ be the space of class functions on G.*

(i) Let χ_1 and χ_2 be the characters of two inequivalent irreducible representations of G. Then $\langle \chi_1, \chi_2 \rangle = 0$.

(ii) If χ is an irreducible character of G, then $\langle \chi, \chi \rangle = 1$.

(iii) The irreducible characters span $\mathcal{V}$.

In this section we examine some important consequences of this theorem. We postpone the proof to Section 3.

Our first result leads to the addition of a uniqueness statement to the decomposition into irreducibles guaranteed by Maschke's Theorem in Chapter 10.

Theorem 11.6. *Let G be a finite group, and let ρ be a representation of G with character χ_ρ. Let φ be an irreducible representation of G with character χ_φ. Then the number of irreducible components of ρ equivalent to φ is equal to $\langle \chi_\rho, \chi_\varphi \rangle$.*

Proof. We decompose ρ into its irreducible summands. By Theorem 10.3, we may rearrange the summands, grouping them by equivalence, and write the following:

$$\rho \sim \bigoplus_{s=1}^{t} \left(\bigoplus_{j=1}^{m_s} \rho_{s_j} \right).$$

We choose notation so that for fixed s, the ρ_{s_j} are all equivalent, but for $r \neq s$, ρ_{s_j} is not equivalent to ρ_{r_i}. It follows that

$$\chi_\rho = \sum_{s=1}^{t} m_s \chi_s,$$

[1] In this language, we follow Isaacs ([**33**], p, 217).

where χ_s is the character of each ρ_{s_j}. We now calculate the inner product

$$\begin{aligned}\langle \chi_\rho, \chi_\varphi \rangle &= \left\langle \sum_s m_s \chi_s, \chi_\varphi \right\rangle \\ &= \sum_s m_s \langle \chi_s, \chi_\varphi \rangle.\end{aligned}$$

By the Fundamental Theorem, we know that $\langle \chi_s, \chi_\varphi \rangle = 1$ if and only if the ρ_{s_j} are equivalent to φ. Therefore, $\langle \chi_\rho, \chi_\varphi \rangle = m_s$, the number of irreducible components of ρ equivalent to φ. □

Now we can state and prove the augmented version of Maschke's Theorem.

Theorem 11.7. *Every representation of a finite group in a finite-dimensional complex vector space can be written as a direct sum of irreducible representations, and the decomposition is unique up to order and equivalence.*

Proof. We need only establish the uniqueness claim. To do so, we use the notation introduced in the proof of Theorem 11.6. Suppose the representation ρ can be written in two ways as a sum of irreducible representations,

$$\rho \sim \bigoplus_{s=1}^{t} \left(\bigoplus_{j=1}^{m_s} \rho_{s_j} \right) \sim \bigoplus_{r=1}^{z} \left(\bigoplus_{j=1}^{n_r} \varphi_{r_j} \right),$$

where we have grouped the irreducible representations according to equivalence. We then have the corresponding sums for the character χ_ρ of ρ:

$$\chi_\rho = \sum_{s=1}^{t} m_s \chi_s = \sum_{r=1}^{z} n_r \psi_r,$$

where χ_s is the character of the ρ_{s_j}, ψ_r is the character of the φ_{r_j}, and the multiplicities m_s and n_r are positive.

By Theorem 11.6, we have $\langle \psi_r, \chi_\rho \rangle = n_r > 0$, so there is an s with $\rho_{s_j} \sim \psi_{r_j}$, and $m_s = n_r$. Proceeding in this way, we verify that all of the φ_{r_i} occur, up to equivalence, among the ρ_{s_j}, and all of the ρ_{s_j} occur, up to equivalence, among the ϕ_{r_i}. Thus the two decompositions of ρ are the same up to order and equivalence. □

The preceding theorem gives us a key result: characters really do tell us all we need to know about representations, in the following sense.

Theorem 11.8. *Let φ and ψ be representations of the finite group G, and let χ_φ and χ_ψ be the corresponding characters. Then φ and ψ are equivalent if and only if $\chi_\varphi = \chi_\psi$.*

Now that we know that every character can be written uniquely as a sum of irreducible characters, we have a useful test for irreducibility.

Theorem 11.9. *Let χ be a character of a finite group. Then χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$.*

Since the regular representation comes from the complete multiplication table for a group, we might expect it to hold all the information for the representations of the group. Indeed it does, as the following theorem shows.

Theorem 11.10. *Every irreducible representation of a finite group G is a component of the left regular representation.*

Proof. Using the notation of Theorem 11.7, the regular representation ρ_{reg} is equivalent to a sum of irreducible representations that are themselves grouped by equivalence. Since traces are additive, we have a corresponding sum for the character χ_{reg},

$$\chi_{reg} = \sum_{j=0}^{t} m_j \chi_j.$$

We prove the theorem by contradiction. Suppose the irreducible representation ρ_s does not occur in ρ_{reg}, so χ_s does not occur in χ_{reg} and $m_s = 0$. Then we have

$$\begin{aligned} \langle \chi_s, \chi_{reg} \rangle &= \sum_{j=0}^{t} \langle \chi_s, m_j \chi_j \rangle \\ &= \sum_{j=0}^{t} m_j \langle \chi_s, \chi_j \rangle \\ &= m_s = 0. \end{aligned}$$

Recall that $\chi_{reg}(g) = 0$ for $g \neq 1_G$, and $\chi_{reg}(1_G) = |G|$. Using the definition of the inner product to calculate $\langle \chi_s, \chi_{reg} \rangle = 0$ thus gives

$$\frac{1}{|G|}(\chi_s(1_G)|G|) = \chi_s(1_G) = 0.$$

This implies that the degree of the irreducible representation ρ_s is 0, which is impossible. □

The next theorem relates the degrees of the irreducible representations to the size of the group and identifies them as the multiplicities of the irreducible components of the regular representation.

Theorem 11.11. *Let $\{\rho_j \mid j = 0, \ldots, t\}$ be the irreducible representations of the finite group G, and let d_j be the degree of ρ_j. Then*

$$\sum_{j=0}^{t} d_j^2 = |G|,$$

and d_j is the multiplicity of ρ_j in the decomposition of the regular representation.

Proof. From Theorem 11.10 we know that each irreducible representation ρ_j appears in the decomposition of ρ_{reg}. Therefore $\rho_{reg} = m_0\,\rho_0 \oplus \cdots \oplus m_t\,\rho_t$ for some positive integers $m_0, \ldots, m_t$, and $\chi_{reg} = m_0\,\chi_0 + m_1\,\chi_1 + \cdots + m_t\,\chi_t$. Since the irreducible characters form an orthonormal set, we can find the coefficient m_j by calculating the inner product. As in the proof of the preceding theorem, we find that $\langle \chi_j, \chi_{reg} \rangle = m_j$. On the other hand, again as in the proof of Theorem 11.10, since $\chi_{reg}(1_G) = |G|$ and $\chi_{reg}(g) = 0$ for $g \neq 1_G$, $\langle \chi_j, \chi_{reg} \rangle = \chi_j(1_G) = d_j$. So $d_j = m_j$.

Finally we calculate $\langle \chi_{reg}, \chi_{reg} \rangle$ two different ways. On the one hand, $\langle \chi_{reg}, \chi_{reg} \rangle = (1/|G|)|G|^2 = |G|$. On the other hand, if we write χ_{reg} as the weighted sum of the irreducible characters, then

$$\langle \chi_{reg}, \chi_{reg} \rangle = \sum_j \sum_\ell m_j m_\ell \langle \chi_j, \chi_\ell \rangle = \sum_j m_j^2 = \sum_j d_j^2.$$

So $\sum_j d_j^2 = |G|$. □

A useful consequence of Theorem 11.11 is the following characterization of an abelian group.

Theorem 11.12. *Let G be a finite group. Then G is abelian if and only if all of its irreducible characters have degree 1.*

Exercises

5. Prove Theorem 11.8.

6. Prove Theorem 11.9.

7. Prove Theorem 11.12.

8. Recall the representation ρ of degree 2 of the dihedral group $D_m = \langle a, b \mid a^m = b^2 = 1, bab^{-1} = a^{-1} \rangle$ in Example 10.11, page 174. Select j so that $\eta^2 \neq 1$, and use the inner product of characters to verify that ρ is irreducible.

9. Let ρ be a representation of the group G and let χ_ρ be the corresponding character.

(a) Show that if $\chi_\rho : G \to \mathbb{C}^*$ is a homomorphism, then the degree of ρ must be 1.

(b) Can χ_ρ be a homomorphism from G to the additive group of $\mathbb{C}$?

10. Characters of $G = S_3$.

(a) How many conjugacy classes does G have?

(b) Let ρ be the natural representation of $G = S_3$ in $\mathbb{C}^3$. Calculate $\langle \chi_\rho, \chi_\rho \rangle$. Ⓢ

(c) Let χ_0 be the trivial character on G. Calculate $\langle \chi_\rho, \chi_0 \rangle$.

(d) Let χ_1 be the character of the representation of G that maps even permutations to 1 and odd permutations to -1. Calculate $\langle \chi_\rho, \chi_1 \rangle$.

(e) Look back at Exercise 10.2. Let $\mathbf{v}_2 = \mathbf{e}_1 - \mathbf{e}_2$ and $\mathbf{v}_3 = \mathbf{e}_1 - \mathbf{e}_3$. Verify that $\text{span}\{\mathbf{v}_2, \mathbf{v}_3\} = \text{span}\{\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3\}^\perp$, and let ρ_2 be the representation of G in this 2-dimensional space. Write out the matrices $\rho_2(\pi)$ for $\pi \in G$ and use them

to calculate the values of the corresponding character χ_2. Calculate $\langle \chi_2, \chi_2 \rangle$. Also calculate $\langle \chi_\rho, \chi_2 \rangle$.

(f) What do you conclude about the decomposition of ρ as a sum of irreducible representations?

11. Repeat Exercise 10 for $G = S_4$, modifying part (e) as appropriate.

12. The conjugacy classes of D_4 were determined in Exercise 3.2. In this exercise you will find the conjugacy classes of the other dihedral groups D_m, where $D_m = \langle a, b \mid a^m = b^2 = 1, bab^{-1} = a^{-1} \rangle$. Recall that the size of the conjugacy class containing an element $x \in G$ is the index of its centralizer, $[G : C_G(x)]$. (See Exercise 3.6.)

(a) Find the conjugacy classes of D_5.

(b) Find the conjugacy classes of D_m for $m = 2j + 1$.

(c) Find the conjugacy classes of D_m for $m = 2j$.

13. Let G be a finite group.

(a) Let $V = \mathbb{C}$ and suppose that $\rho : G \to GL(V)$ and $\sigma : G \to GL(V)$ are degree 1 representations of G. Show that we can create another degree 1 representation $\tau : G \to GL(V)$ by defining $\tau(g) = \rho(g)\sigma(g)$ for all $g \in G$ (where we multiply complex numbers as usual).

(b) How is the character of τ related to the characters of ρ and σ?

(c) Suppose that $\rho : G \to GL(\mathbb{C}^d)$ is any representation of G, with character χ_ρ, and that χ' is a character of degree 1 of G. Show that the product $\chi_\rho \chi'$ is a character of G.

(d) Explain why, in general, the construction from part (a) does *not* work if ρ and σ are both representations of G of degree $d > 1$.

Remark: It turns out that the product of *any* two characters of G is again a character. To prove this requires a construction called the "tensor product."

14. Let G be a finite abelian group, and let G^* be the set of irreducible characters of G. Recall that by Theorem 11.12, all irreducible characters of G have degree 1. As this exercise will show, G^* is a group called the character group of G.

(a) Explain why G and G^* have the same cardinality.

(b) As in Exercise 13a, define a binary operation on G^* by $(\chi\psi)(g) = \chi(g)\psi(g)$. Show that G^* is a group under this operation. Ⓗ

(c) Assume $G = \langle a \rangle$ is cyclic of order r, and let ω be a primitive rth root of unity. Show that $G^* = \langle \alpha \rangle$, where $\alpha(a) = \omega$, and $G \simeq G^*$ via $g = a^j \mapsto \chi_g = \alpha^j$.

(d) Assume $G = \langle a, b \,|\, a^r = b^s = 1, ab = ba \rangle$. Let ω, η be primitive rth and sth roots of unity respectively and define homomorphisms α and β mapping $G \to \mathbb{C}^*$ by $\alpha(a) = \omega, \alpha(b) = 1, \beta(a) = 1$, and $\beta(b) = \eta$. Show that $G^* = \langle \alpha, \beta \,|\, \alpha^r = \beta^s = 1, \alpha\beta = \beta\alpha \rangle$ and $G \simeq G^*$ via $g = a^j b^\ell \mapsto \chi_g = \alpha^j \beta^\ell$.

Note that in this correspondence $gh \mapsto \chi_{gh} = \chi_g \chi_h$ and $g^{-1} \mapsto \chi_{g^{-1}} = (\chi_g)^{-1}$. This observation will be used in Chapter 13.

(e) Explain, informally, why $G \simeq G^*$ for any abelian group G, and why there is a natural way to identify elements of G with elements of G^*. (This isomorphism is not canonical, since it depends on a choice of generators for G and of corresponding primitive roots of unity.)

11.3. Proof of the Fundamental Theorem

In this section we prove the Fundamental Theorem of Character Theory.

Theorem 11.5 *Let G be a finite group and let $\mathcal{V}$ be the space of class functions on G.*

(i) Let χ_1 and χ_2 be characters of two inequivalent irreducible representations of G. Then $\langle \chi_1, \chi_2 \rangle = 0$.

(ii) If χ is an irreducible character of G then $\langle \chi, \chi \rangle = 1$.

(iii) The irreducible characters span $\mathcal{V}$.

Our argument makes heavy use of the following concept.

Definition. Given representations $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ of G in vector spaces over the same field, a linear transformation $\tau : V_1 \to V_2$ is called an intertwining transformation (or intertwining operator) from ρ_1 to ρ_2 (in that order) if $\rho_2(g)\tau = \tau\rho_1(g)$ for all $g \in G$. In other words, for all $g \in G$, the following diagram commutes:

$$\begin{array}{ccc} V_1 & \xrightarrow{\rho_1(g)} & V_1 \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ V_2 & \xrightarrow{\rho_2(g)} & V_2 \end{array}$$

Note that if τ is an *invertible* intertwining transformation, then ρ_1 and ρ_2 are equivalent.

Proof of orthogonality. Our first goal is to prove part (i) of Theorem 11.5, showing that if ρ_1 and ρ_2 are inequivalent irreducible representations with characters χ_1 and χ_2 respectively, then

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\chi_2(g^{-1}) = 0.$$

This part of Theorem 11.5 has a complicated proof, so we outline the steps that bring us to our goal.

(1) We prove Schur's Lemma, which tells us that the intertwining transformations between two irreducible representations are very restricted: (i) if the irreducible representations are not equivalent, the intertwining transformation is zero; (ii) if they are equivalent, it is a scalar times the identity transformation. [Theorem 11.13]

(2) Given representations in spaces V_1 and V_2 respectively and a linear transformation $\sigma : V_1 \to V_2$, we show how to build a transformation that intertwines the representations. [Theorem 11.14]

(3) This is the key tool. For any linear transformation $\sigma : V_1 \to V_2$, by using the first part of Schur's Lemma and the construction in step 2 of an intertwining operator based on σ, we show that if ρ_1 and ρ_2 are inequivalent irreducible representations, then

$$\sum_{g \in G} \rho_2(g^{-1}) \sigma \rho_1(g) = 0.$$

[Theorem 11.15]

(4) We convert to matrix notation, writing $\rho_1(g) = A(g) = (a_{st}(g))$ and $\rho_2(g^{-1}) = B(g^{-1}) = (b_{st}(g^{-1}))$. By making simple choices for the matrix corresponding to σ we show that for any s, t, j, k,

$$\sum_{g \in G} b_{sj}(g^{-1}) a_{kt}(g) = 0.$$

Specifically, when $j = s$ and $k = t$, we have

$$\sum_{g \in G} b_{ss}(g^{-1}) a_{tt}(g) = 0.$$

[Lemma 11.16]

(5) From this last equation, it is a short step to $\langle \chi_1, \chi_2 \rangle = 0$.
[Theorem 11.5(i)]

Now, off we go!

Step 1:

Theorem 11.13. *(Schur's Lemma) Let ρ_1, ρ_2 be irreducible representations of a finite group G in vector spaces V_1, V_2 over $\mathbb{C}$.*

(i) If ρ_1 and ρ_2 are not equivalent, then the only intertwining transformation from ρ_1 to ρ_2 is $\tau = 0$. (This much is true over any field.)

(ii) If $\rho_1 = \rho_2$, then the only intertwining transformations (that is, the only linear transformations $\tau : V_1 \to V_1$ that commute with all the $\rho_1(g)$) are scalar multiples of the identity.

Proof. Part (i): Assume ρ_1 and ρ_2 are inequivalent, irreducible representations of G and $\rho_2(g)\tau = \tau\rho_1(g)$ for all $g \in G$. We note that

$\mathrm{Ker}(\tau) \subseteq V_1$ must be an invariant subspace for ρ_1. Since ρ_1 is irreducible, $\mathrm{Ker}(\tau)$ must be either $\{\mathbf{0}\}$ or all of V_1. A similar argument shows that $\mathrm{Im}(\tau)$ must be either $\{\mathbf{0}\}$ or all of V_2. Putting these results together, if $\mathrm{Ker}(\tau)$ is $\{\mathbf{0}\}$, then τ is an invertible transformation from V_1 to V_2, and ρ_1 and ρ_2 are equivalent. This contradicts our hypothesis, so $\mathrm{Ker}(\tau) = V_1$, and $\tau = 0$.

Part (ii): Suppose that $\tau\rho_1(g) = \rho_1(g)\tau$ for all $g \in G$. Since we are working over $\mathbb{C}$, τ must have at least one eigenvalue λ. We will show that $\tau = \lambda I$. There is a nonzero eigenvector $\mathbf{v} \in V$ such that $\tau\mathbf{v} = \lambda\mathbf{v}$. So $(\tau - \lambda I)\mathbf{v} = \mathbf{0}$. Consider the transformation $\tau - \lambda I$. Since ρ_1 is irreducible and $\mathrm{Ker}(\tau - \lambda I)$ is a nonzero invariant subspace for ρ_1, $\mathrm{Ker}(\tau - \lambda I) = V$. Thus $\tau - \lambda I = 0$, and $\tau = \lambda I$. □

Step 2: We show how to construct intertwining transformations so that we can use Schur's Lemma. The property we want for an intertwining transformation τ from ρ_1 to ρ_2 is that $\rho_2(g)\tau = \tau\rho_1(g)$ for all $g \in G$. This would mean that $\tau = \rho_2(g^{-1})\tau\rho_1(g)$. Certainly $\rho_2(g^{-1})\tau\rho_1(g)$ is a linear transformation from V_1 to V_2. We also note that the sum of linear transformations is again a linear transformation. So we are again prompted to sum over all elements in G, our trick elevated to strategy.

Theorem 11.14. *If G is a finite group and if $\rho_1 : G \to GL(V_1)$ and $\rho_2 : G \to GL(V_2)$ are representations of G over $\mathbb{K}$, then for any linear transformation $\sigma : V_1 \to V_2$,*

$$\tau = \sum_{g \in G} \rho_2(g^{-1})\, \sigma\, \rho_1(g)$$

is an intertwining transformation from ρ_1 to ρ_2.

Proof. We show that for all $h \in G$, $\rho_2(h)\tau = \tau\rho_1(h)$:

$$\begin{aligned} \rho_2(h)\tau &= \rho_2(h)\Big(\sum_{g \in G} \rho_2(g^{-1})\sigma\rho_1(g)\Big) \\ &= \sum_{g \in G} \rho_2(h)\rho_2(g^{-1})\sigma\rho_1(g) \\ &= \sum_{g \in G} \rho_2(hg^{-1})\sigma\rho_1(g), \text{ and} \end{aligned}$$

$$\begin{aligned}\tau\rho_1(h) &= \Big(\sum_{g\in G}\rho_2(g^{-1})\sigma\rho_1(g)\Big)\rho_1(h)\\ &= \sum_{g\in G}\rho_2(g^{-1})\sigma\rho_1(g)\rho_1(h)\\ &= \sum_{g\in G}\rho_2(g^{-1})\sigma\rho_1(gh).\end{aligned}$$

If we now substitute $g_1 = gh$ into this second expression, so that $g^{-1} = hg_1^{-1}$, we see that the two expressions are equal. □

Step 3: We note that in Step 2 we constructed τ from *any* linear transformation σ from V_1 to V_2. Also, recall from Schur's Lemma that if ρ_1 and ρ_2 are inequivalent irreducible representations of G on V_1 and V_2, then any intertwining transformation from ρ_1 to ρ_2 must be the zero transformation. Putting these two facts together, we have the following theorem.

Theorem 11.15. *Let ρ_1 and ρ_2 be inequivalent irreducible representations of G in complex vector spaces V_1 and V_2, respectively. Then for any linear transformation $\sigma : V_1 \to V_2$*

$$\sum_{g\in G}\rho_2(g^{-1})\sigma\rho_1(g) = 0.$$

Step 4: The preceding theorem is our key to proving that the inner product of any two inequivalent irreducible characters is zero. We translate it into matrix notation in the next technical lemma. (We call it a technical lemma because its proof is an intricate calculation but uses no new ideas.)

Lemma 11.16. *Let ρ_1 and ρ_2 be inequivalent irreducible representations of G in complex vector spaces V_1 and V_2, respectively. We fix a basis for V_1 and for V_2. With respect to these bases, $\rho_1(g)$ is the $m \times m$ matrix $A(g)$ and $\rho_2(g^{-1})$ is the $n \times n$ matrix $B(g^{-1})$. Then for any $0 \le s, j \le n$ and $0 \le k, t \le m$,*

$$\sum_{s,t} b_{sj}(g^{-1})a_{kt}(g) = 0.$$

Proof. Theorem 11.15 tells us that for any linear transformation $\sigma : V_1 \to V_2$,

$$\sum_{g\in G} \rho_2(g^{-1})\,\sigma\,\rho_1(g) \;=\; 0.$$

In terms of the fixed bases, this equation of transformations becomes an equation of matrices:

$$\sum_{g\in G} B(g^{-1})\,S\,A(g) \;=\; 0,$$

where S is any $n \times m$ matrix. We write

$$A(g) \;=\; \begin{bmatrix} a_{11}(g) & a_{12}(g) & \cdots & a_{1m}(g) \\ \vdots & \vdots & & \vdots \\ a_{m1}(g) & a_{m2}(g) & \cdots & a_{mm}(g) \end{bmatrix}$$

$$B(g^{-1}) \;=\; \begin{bmatrix} b_{11}(g^{-1}) & b_{12}(g^{-1}) & \cdots & b_{1n}(g^{-1}) \\ \vdots & \vdots & & \vdots \\ b_{n1}(g^{-1}) & b_{n2}(g^{-1}) & \cdots & b_{nn}(g^{-1}) \end{bmatrix}.$$

To pick off the entries that we wish to relate, we choose the matrix $S = S_{jk}$ to be the matrix of all 0s except for a single 1 in the jkth entry. We let

$$C(g) \;=\; B(g^{-1})\,S_{jk}\,A(g).$$

Then

$$\begin{aligned} c_{st}(g) \;&=\; \Big(\text{ row } s \text{ of } B(g^{-1})\Big) \cdot \Big(\text{ column } t \text{ of } S_{jk}A(g)\Big) \\ &=\; \Big[b_{s1}(g^{-1}), \ldots, b_{sn}(g^{-1})\Big] \cdot \begin{bmatrix} 0 \\ \vdots \\ a_{kt}(g) \\ \vdots \\ 0 \end{bmatrix} \quad \leftarrow j\text{th entry} \\ &=\; b_{sj}(g^{-1})a_{kt}(g). \end{aligned}$$

Finally, summing over all $g \in G$ we get our result:

$$\sum_{g\in G} c_{st}(g) \;=\; \sum_{g\in G} b_{sj}(g^{-1})a_{kt}(g) \;=\; 0. \qquad \square$$

We actually use this result in the restricted case that $s = j$, and $t = k$:

$$\sum_{g \in G} b_{ss}(g^{-1}) a_{tt}(g) \;=\; 0.$$

Note that this sum involves only the diagonal elements of the matrices $A(g)$ and $B(g^{-1})$. These are the elements that appear in the traces of these matrices.

Step 5: We are now ready to show that inequivalent irreducible characters are orthogonal.

Fundamental Theorem, *part (i). Let G be a finite group, and $\mathcal{V}$ be the space of class functions on G. Let χ_1 and χ_2 be characters of inequivalent irreducible representations for G. Then $\langle \chi_1, \chi_2 \rangle = 0$.*

Proof. Using the notation in the proof of Lemma 11.16, with $A(g)$ and $B(g^{-1})$ the matrices for transformations $\rho_1(g)$ and $\rho_2(g^{-1})$, then

$$\begin{aligned} \chi_1(g) &= \mathrm{Tr}\big(A(g)\big) &&= \sum_{t=1}^{m} a_{tt}(g), \\ \chi_2(g^{-1}) &= \mathrm{Tr}\big(B(g^{-1})\big) &&= \sum_{s=1}^{n} b_{ss}(g^{-1}). \end{aligned}$$

Using these expressions for $\chi_1(g)$ and $\chi_2(g^{-1})$, we calculate the inner product of χ_1 and χ_2:

$$\begin{aligned}
\langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\, \overline{\chi_2(g)} \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_1(g)\, \chi_2(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g \in G} \Big(\sum_t a_{tt}(g) \Big) \Big(\sum_s b_{ss}(g^{-1}) \Big) \\
&= \frac{1}{|G|} \sum_{g \in G} \Big(\sum_{s,t} a_{tt}(g)\, b_{ss}(g^{-1}) \Big) \\
&= \frac{1}{|G|} \sum_{s,t} \Big(\sum_{g \in G} a_{tt}(g)\, b_{ss}(g^{-1}) \Big) \\
&= \frac{1}{|G|} \sum_{s,t} 0 \\
&= 0.
\end{aligned}$$

We conclude that characters of inequivalent irreducible representations are orthogonal. □

Proof of normality. Our next goal is to prove Theorem 11.5(ii) by showing that if χ is an irreducible character, then $\langle \chi, \chi \rangle = 1$. We do this by traversing the same steps as in the proof of part (i), but using the second part of Schur's Lemma.

Fundamental Theorem, *part (ii). If χ is an irreducible character of a finite group G, then $\langle \chi, \chi \rangle = 1$.*

Proof. As in the proof of Lemma 11.16, we assume χ is the character of a representation ρ of G and consider the transformation

$$\tau = \sum_{g \in G} \rho(g^{-1})\, \sigma_{jk}\, \rho(g),$$

where σ_{jk} is represented by the matrix with all zeroes except for a one in the jkth entry. By Theorem 11.14, this is an intertwining transformation from ρ to itself. So by part (ii) of Schur's Lemma, $\tau = \lambda I_m$, where m is the degree of ρ.

To get a value for λ we take the trace of τ. On the one hand, $\mathrm{Tr}(\tau) = \mathrm{Tr}(\lambda I_m) = m\lambda$; on the other hand, the trace is the sum over $g \in G$ of the traces of $\rho(g^{-1})\,\sigma_{jk}\,\rho(g)$. Since each of these is a conjugate of σ_{jk}, the trace of the sum is simply $|G|$ times the trace of σ_{jk}. If $j \neq k$, then the trace is zero, and $\mathrm{Tr}(\tau) = 0$ (so $\lambda = 0$). If $j = k$ then $\mathrm{Tr}(\sigma_{jj}) = 1$. Therefore $\mathrm{Tr}(\tau) = m\lambda = |G|$, and $\lambda = |G|/m$.

In the calculation of τ we again use matrices $A(g)$ to represent $\rho(g)$ and S_{jk} to represent σ_{jk}. The matrix calculation from the proof of Lemma 11.16 shows us that the stth entry of $A(g^{-1})S_{jk}A(g)$ is $a_{sj}(g^{-1})a_{kt}(g)$. Summing over $g \in G$ we get the matrix for τ, whose diagonal entries are λ and whose other entries are 0. Therefore:

$$\sum_{g\in G} a_{sj}(g^{-1})\,a_{kt}(g) \quad = \quad \begin{cases} |G|/m & \text{if } s = t \text{ and } j = k \\ 0 & \text{otherwise.} \end{cases}$$

We use these facts to calculate $\langle \chi, \chi \rangle$:

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{|G|} \sum_{g\in G} \chi(g)\,\overline{\chi(g)} \\ &= \frac{1}{|G|} \sum_{g\in G} \chi(g)\,\chi(g^{-1}) \\ &= \frac{1}{|G|} \sum_{g\in G} \Big(\sum_{t=1}^{m} a_{tt}(g)\Big)\Big(\sum_{s=1}^{m} a_{ss}(g^{-1})\Big) \\ &= \frac{1}{|G|} \sum_{s,t} \sum_{g\in G} a_{tt}(g)\,a_{ss}(g^{-1}). \end{aligned}$$

The sum over $g \in G$ equals $|G|/m$ only when $s = t$, and is 0 otherwise. Over all the combinations of the outer sum, $s = t$ exactly m times. So the inner product is:

$$\langle \chi, \chi \rangle = \frac{1}{|G|}\, m\, \frac{|G|}{m} = 1. \qquad \square$$

Proof of spanning. Finally, we prove Theorem 11.5(iii) by showing that the irreducible characters span $\mathcal{V}$, so their number is exactly the number of conjugacy classes. For our proof, we need the following result.

Theorem 11.17. *Let ρ be a representation of G over $\mathbb{C}$, and let α be a class function for G. Then*

$$\tau = \sum_{g \in G} \alpha(g)\rho(g)$$

is an intertwining transformation from ρ to itself.

Proof. As in the proof of Theorem 11.14, we can show that $\rho(h)\tau = \tau\rho(h)$ for all $h \in G$. □

Fundamental Theorem, *part (iii). Let G be a finite group and $\mathcal{V}$ the space of class functions on G. Then the irreducible characters of G span $\mathcal{V}$.*

Proof. Let $\mathcal{W}$ be the subspace of $\mathcal{V}$ spanned by the irreducible characters. Recall from Theorem 10.7 that $\mathcal{V} = \mathcal{W} \oplus \mathcal{W}^\perp$. Our plan is to show that $\mathcal{W} = \mathcal{V}$ by showing $\mathcal{W}^\perp = \{\mathbf{0}\}$. We do this by proving that any class function α that is orthogonal to all the irreducible characters must be the zero function.

Let α be a class function that is orthogonal to all the irreducible characters of G, and let ρ_j be an irreducible representation of G. Since α is a class function, $\overline{\alpha} : g \mapsto \overline{\alpha(g)}$ is also a class function. By Theorem 11.17 we know that $\sum \overline{\alpha(g)}\rho_j(g)$ is an intertwining transformation from ρ_j to itself. So by part (ii) of Schur's Lemma,

$$\sum_{g \in G} \overline{\alpha(g)}\rho_j(g) = \lambda I \quad \text{for some } \lambda.$$

Next take the trace of both sides. On the one hand, $\mathrm{Tr}(\lambda I)$ is λ times the degree of ρ_j; on the other hand,

$$\begin{aligned} \mathrm{Tr}\left(\sum_{g \in G} \overline{\alpha(g)}\rho_j(g)\right) &= \sum_{g \in G} \overline{\alpha(g)}\mathrm{Tr}(\rho_j(g)) \\ &= \sum_{g \in G} \overline{\alpha(g)}\chi_{\rho_j}(g) \\ &= |G| \left\langle \chi_{\rho_j}, \alpha \right\rangle \\ &= 0. \end{aligned}$$

We conclude that $\lambda = 0$. Consequently, for any irreducible representation ρ_j, $\sum \overline{\alpha(g)}\rho_j(g)$ is the zero transformation. Since we can write any representation as the sum of irreducible representations, we have for every representation ρ that

$$\sum_{g\in G} \overline{\alpha(g)}\rho(g) = 0.$$

In particular, this is true for the left regular representation ρ_{reg}. We then apply this, the zero transformation, to the basis vector $\mathbf{e}_{1_G}$ to get:

$$\begin{aligned}\left(\sum_{g\in G} \overline{\alpha(g)}\rho_{reg}(g)\right)(\mathbf{e}_{1_G}) &= \sum_{g\in G} \overline{\alpha(g)}\,\rho_{reg}(g)(\mathbf{e}_{1_G}) \\ &= \sum_{g\in G} \overline{\alpha(g)}\,\mathbf{e}_g = \mathbf{0}.\end{aligned}$$

This linear combination of the basis vectors $\mathbf{e}_g$ can be $\mathbf{0}$ only if all scalars $\overline{\alpha(g)}$ are 0. So $\alpha(g) = 0$ for all $g \in G$. We conclude that $\mathcal{W}^\perp = \{\mathbf{0}\}$, so the irreducible characters span all of $\mathcal{V}$. □

Exercises

15. Details in the proof of Schur's Lemma

(a) Assume ρ_1 and ρ_2 are inequivalent irreducible representations of G and $\rho_2(g)\tau = \tau\rho_1(g)$ for all $g \in G$. Show that $\mathrm{Ker}(\tau)$ is an invariant subspace for ρ_1 and $\mathrm{Im}(\tau)$ is an invariant subspace for ρ_2. Ⓢ

(b) Assume ρ_1 is irreducible and $\rho_1(g)\tau = \tau\rho_1(g)$ for all $g \in G$. Show $\mathrm{Ker}(\tau - \lambda I)$ is an invariant subspace for ρ_1.

16. Use Schur's Lemma (not Theorems 11.11 or 11.12) to prove that if G is a finite abelian group then all of its irreducible characters have degree 1.

11.4. Characters and difference sets

We begin this section on the use of characters to study difference sets with a discussion of some of the initial steps in Smith's construction [**65**] of his surprising non-abelian $(100, 45, 20)$-difference set. We then turn to a sequence of theorems about characters of finite abelian groups yielding a characterization of an abelian difference set, Theorem 11.21. We already know from Theorem 10.13 that if χ is a nontrivial character of an abelian (v, k, λ)-difference set D, then $z = \widetilde{\chi}(D)$ satisfies $z\overline{z} = n$ for $n = k-\lambda$. This necessary condition can be used to narrow the search for a difference set. Theorem 11.21 guarantees that a subset of G of size k surviving this search process for all nontrivial characters of G really is a difference set. Davis and Jedwab turned this result into a general strategy for constructing difference sets, leading to a uniform construction for difference sets with $\gcd(v, n) > 1$ and the discovery of new families of difference sets along the way ([**16**]). Theorem 11.22 extends this characterization to non-abelian groups.

Smith's construction

Smith [**65**] constructed his $(100, 45, 20)$-difference set in the group

$$G = \langle a, b, c \mid a^5 = b^5 = c^4 = 1,\ ab = ba,\ cac^{-1} = a^2,\ cbc^{-1} = b^2 \rangle.$$

The subgroups $\langle a \rangle$, $\langle b \rangle$ and $\langle a, b \rangle$ are normal subgroups of G. (In fact, $G' = \langle a, b \rangle$ is the *commutator subgroup* of G. It is also the Sylow 5-subgroup of G.) In the following two examples, we describe some of Smith's use of group representations in his successful search for a $(100, 45, 20)$-difference set in G.

Example 5. We begin with four irreducible representations of G of degree 1. For $j = 0, 1, 2, 3$, define

$$\chi_j(a) = 1, \quad \chi_j(b) = 1, \quad \chi_j(c) = i^j.$$

We can use inner products to verify that these four irreducible characters are inequivalent. It is easiest to calculate the inner products we need by working with the right cosets of $G' = \langle a, b \rangle$ in G. Notice that

$$\begin{aligned} g \in G'c &\quad \Leftrightarrow \quad g^{-1} \in G'c^3 \quad \text{and} \\ g \in G'c^2 &\quad \Leftrightarrow \quad g^{-1} \in G'c^2. \end{aligned}$$

For example, we calculate

$$\langle \chi_2, \chi_1 \rangle = \frac{1}{100}\Big[25(1)(1)+25(-1)(\overline{i})+25(1)(-1)+25(-1)(\overline{-i})\Big] = 0.$$

We suppose D is a $(100, 45, 20)$-difference set in G. For D in the integral group ring, $z_j = \widetilde{\chi}_j(D)$ is in the ring of Gaussian integers $\mathbb{Z}[i]$, and $\widetilde{\chi}_j(D^{(-1)}) = \overline{z_j}$. In fact, z_2 is actually an integer. Now by Theorem 10.13 (page 193) we have $z_j\overline{z_j} = 25$ for $j = 1, 2, 3$. We know that a Gaussian integer $z = x + iy$ satisfies $z\overline{z} = 25$ if and only if $x^2 + y^2 = 25$. Therefore $z_2 = \pm 5$ and $z_3 = \overline{z_1} \in \{\pm 5, \pm 5i, \pm 3 \pm 4i, \pm 4 \pm 3i\}$. If we write $u_j = |D \cap G' c^j|$, then our work thus far tells us that these intersection numbers must satisfy the following equations:

$$\begin{aligned} u_0 + u_1 + u_2 + u_3 &= 45, \\ u_0 + u_1 i - u_2 - u_3 i &= z_1, \\ u_0 - u_1 + u_2 - u_3 &= z_2. \end{aligned}$$ ◇

From the equations in Example 5, Smith finds that there are two possibilities for the unordered set $\{u_0, u_1, u_2, u_3\}$:

$$\{15, 10, 10, 10\} \quad \text{or} \quad \{14, 12, 11, 8\}.$$

In fact, up to translation of D or applying a group automorphism of G/G', Smith concludes that there are three possibilities for the ordered quadruple (u_0, u_1, u_2, u_3):

$$(15, 10, 10, 10),\ (14, 12, 11, 8) \ \text{ or } \ (14, 8, 11, 12).$$

(This is Lemma 1 of his paper [**65**].)

Example 6. We continue with Smith's paper [**65**], using the notation of the previous example. The subgroup $G' = \langle a, b \rangle$ has exactly six subgroups of order 5; Smith labels them $H_j = \langle a^j b \rangle$ for $j = 0, 1, 2, 3, 4$ and $H_\infty = \langle a \rangle$. Much of Smith's analysis is based on the structure and representations of the factor groups $G/H_j \cong F$, where

$$F = \langle \alpha, \gamma \mid \alpha^5 = \gamma^4 = 1_F, \gamma\alpha\gamma^{-1} = \alpha^2 \rangle.$$

To begin, Smith defines the representation $\psi' : F \to GL(4, \mathbb{C})$ by

$$\psi'(\alpha) = \begin{bmatrix} \eta & 0 & 0 & 0 \\ 0 & \eta^2 & 0 & 0 \\ 0 & 0 & \eta^4 & 0 \\ 0 & 0 & 0 & \eta^3 \end{bmatrix} \quad \psi'(\gamma) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

where $\eta = e^{2\pi i/5}$. Let χ' be the character of ψ'. Then for $j = 1, 2, 3, 4$, $\chi'(\alpha^j) = -1$, and $\chi'(\alpha^j\gamma^\ell) = 0$ for all j and for $\ell = 1, 2, 3$. It follows that $\langle \chi', \chi' \rangle = (1/20)[1(4)(4) + 4(-1)(-1)] = 1$, so χ' (and ψ') are irreducible.

Next Smith defines a representation ψ of F by

$$\psi(\alpha) = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad \psi(\gamma) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

This is actually the permutation representation of F on the 5 left cosets of $H = \langle \gamma \rangle$. Let χ be the character of ψ. To find values of χ we need to count fixed points (i.e., fixed cosets) under the various elements of F. Since $\gamma H = H$ and $\gamma\alpha^j H = \alpha^{2j} H \neq \alpha^j H$ for $j = 1, 2, 3, 4$, we have $\chi(\gamma) = 1$. Likewise $\chi(\gamma^2) = \chi(\gamma^3) = 1$. Similarly $(\alpha^i\gamma)(\alpha^j H) = \alpha^{2j+i} H = \alpha^j H$ if and only if $j + i \equiv 0 \bmod 5$, which implies $\chi(\alpha^i\gamma) = 1$. We also find $\chi(\alpha^i\gamma^j) = 1$ for $j = 2, 3$. Finally, for $j \neq 0$, α^j acts as a 5-cycle on the cosets and so has no fixed points. Therefore $\chi(\alpha^j) = 0$ for $j = 1, 2, 3, 4$. Putting all this information together, we have

$$\begin{aligned} \langle \chi, \chi_0 \rangle &= \frac{1}{20}\Big[1(5)(1) + 4(0)(1) + 15(1)(1)\Big] = 1, \\ \langle \chi, \chi' \rangle &= \frac{1}{20}\Big[1(5)(4) + 4(0)(-1) + 15(1)(0)\Big] = 1. \end{aligned}$$

This tells us that the irreducible components of ψ are ψ' and the trivial representation. ◇

We leave Smith's analysis here for now, but very briefly summarize the rest. Each representation ϕ of the factor group $G/H_j \cong F$ defines a representation ρ of G by $\rho(g) = \phi(H_j g)$. Proceeding as in

Example 6, Smith finds all six of the irreducible representations of G of degree 4 (like ψ') and constructs an integer-valued representation (like ψ) for each. Specifically, for each j he determines a representation $\omega_j : G \to GL(5, \mathbb{C})$ producing matrices with integer entries. He then defines the matrix $M = \widetilde{\omega}_j(D) - 9J$, where J is the 5×5 all 1s matrix. Determining M will determine $\widetilde{\omega}_j(D)$ and bring him closer to finding D. He finds that up to permutations of rows and columns, there are just four possibilities for M. (This is Lemma 2 in [**65**].) There is still a long way to go to determine D, and to traverse the rest of the distance, Smith employs some very interesting geometric arguments along with more representation theory. Finally, when the possibilities for D are restricted enough to make it tractable, a computer search (with the help of mathematicians at the National Security Agency) produces several $(100, 45, 20)$-difference sets in G.

Characterizing difference sets. We now return to difference sets in arbitrary finite groups. Suppose D is a (v, k, λ)-difference set in G. We already know that a representation φ of G gives a ring homomorphism $\widetilde{\varphi}$ of $\mathbb{Z}G$. Let $M = \widetilde{\varphi}(D)$. Theorem 10.13 tells us that a necessary condition for the existence of a difference set D is that $M\overline{M}^T = nI$. We now work toward a companion sufficient condition. Theorems 11.21 and 11.22 (one for an abelian group and one for an arbitrary group) require that this necessary condition holds for *every* irreducible representation φ of G. In other words, these theorems assure that any possible difference set D that survives the necessary condition for every irreducible φ really is a difference set. However, we cannot apply these theorems without knowing the full set of irreducible representations of a group. The following example illustrates some of what is involved in finding all the irreducible representations of a given group. For a bit more, see Section 5.

Example 7. To illustrate, we find the full set of irreducible representations of $G = D_4 = \langle a, b \,|\, a^4 = b^2 = 1, bab = a^3 \rangle$. By Exercise 3.2, we know G has 5 conjugacy classes and therefore 5 irreducible representations. By Theorem 11.11, we know that the sum of the squares of the degrees of these representations must equal $|G| = 8$. From this we conclude that there must be four irreducible representations of degree 1 and one of degree 2. Indeed, we saw in Example 10.11

(page 174) the degree-2 representation:

$$a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We also know the trivial representation is one of the degree 1 representations. We must find three more. To do this, notice that the non-identity elements of $G/\langle a^2 \rangle$ all have order 2, so we may define the following three representations, each of which has $\langle a^2 \rangle$ in its kernel:

$$\chi_1 : \begin{cases} a \mapsto +1 \\ b \mapsto -1 \end{cases} \qquad \chi_2 : \begin{cases} a \mapsto -1 \\ b \mapsto +1 \end{cases} \qquad \chi_3 : \begin{cases} a \mapsto -1 \\ b \mapsto -1. \end{cases}$$

$\diamond$

To reach Theorem 11.21, we begin with a result that translates Theorem 10.12 into the language of characters.

Theorem 11.18. *Let G be a finite group and ρ an irreducible representation of G of degree m with corresponding character χ. We write χ_0 for the trivial character. Then*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

In the abelian case, a useful companion result to the preceding theorem is Theorem 11.19. These two theorems are often referred to as orthogonality relations, although we do not actually need the Fundamental Theorem to prove them.

Theorem 11.19. *Let G be a finite abelian group and let G^* be the set of all irreducible characters of G. Then the following equations hold:*

$$\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ \\ 0 & \text{if } g \neq 1. \end{cases}$$

Using these orthogonality relations for abelian groups, we can show that the coefficients of $A = \sum a_g g \in \mathbb{C}G$ are determined by the images of A under the irreducible characters in G^*.

Theorem 11.20. *(Inversion formula) Let G be a finite abelian group and $A = \sum a_g g$ an element of the group ring $\mathbb{C}G$. Then*

$$a_h = \frac{1}{|G|} \sum_{\chi \in G^*} \widetilde{\chi}(A)\chi(h^{-1}) \quad \text{for } h \in G.$$

The inversion formula now gives us the promised characterization of an abelian difference set. The implication in one direction is familiar; it is the converse that is new and perhaps surprising.

Theorem 11.21. *Let G be an abelian group of order v, and let G^* be the set of irreducible characters of G. Write χ_0 for the trivial character in G^*. Let D be a subset of G of cardinality k, and assume $\lambda = k(k-1)/(v-1)$ is an integer. Then D is a (v, k, λ)-difference set in G if and only if for all irreducible characters χ*

$$\widetilde{\chi}(D)\overline{\widetilde{\chi}(D)} = \begin{cases} n & \text{if } \chi \neq \chi_0 \\ \\ k^2 & \text{if } \chi = \chi_0. \end{cases}$$

What about non-abelian difference sets? Liebler [**45**] generalized the inversion formula for non-abelian groups. His generalization depends on aspects of the structure of $\mathbb{C}G$ beyond those we have discussed. Nonetheless, his largely expository and somewhat philosophical article "Constructive Representation Theoretic Methods and nonAbelian Difference Sets" [**46**] is well worth a look. However, the following theorem, also due to Liebler and appearing in [**17**], *is* accessible to us.

Theorem 11.22. *(Liebler) Let D be a subset of size k in a group G of order v, with $k(k-1) = \lambda(v-1)$ for some integer λ. Assume $\varphi_1, \ldots, \varphi_t$ are the nontrivial irreducible representations of G, with $m_j = \deg \varphi_j$. If*

$$\widetilde{\varphi}_j(D)\widetilde{\varphi}_j(D^{(-1)}) = nI_{m_j}$$

for $j = 1, \ldots, t$, then D is a (v, k, λ)-difference set in G.

Proof. Write ρ_{reg} for the regular representation of G. Recall Theorem 10.14, which tells us that if A and B are in $\mathbb{Z}G$ and satisfy $\widetilde{\rho}_{reg}(A) = \widetilde{\rho}_{reg}(B)$, then $A = B$. Let $A = DD^{(-1)}$ and $B = n1_G + \lambda G$. We will show that $\widetilde{\rho}_{reg}(A) = \widetilde{\rho}_{reg}(B)$.

We know that ρ_{reg} decomposes as a sum of irreducible representations. In fact, we know (Theorem 11.11) that every irreducible representation of G appears in ρ_{reg} with multiplicity equal to its degree. Together with the hypotheses of the theorem, this tell us that $\widetilde{\rho}_{reg}(A)$ is block diagonal, with the block nI_{m_j} appearing m_j times, after a $(1,1)$ entry equal to k^2 corresponding to the trivial representation. Thus,

$$\widetilde{\rho}_{reg}(A) = \begin{bmatrix} k^2 & 0 \\ 0 & nI_{v-1} \end{bmatrix}.$$

On the other hand, $\widetilde{\rho}_{reg}(B) = nI_v + M$, where M consists entirely of zeroes except for λv in the $(1,1)$ entry. Since Theorem 4.1 tells us $n + \lambda v = k^2$, we have $\widetilde{\rho}_{reg}(A) = \widetilde{\rho}_{reg}(B)$, so $A = B$. Therefore D satisfies the difference set equation in $\mathbb{Z}G$ and is thus a difference set. □

Exercises

17. Refer to Example 5:

(a) Explain the calculation of $\langle \chi_2, \chi_1 \rangle$.

(b) Calculate $\langle \chi_1, \chi_1 \rangle$.

(c) Why is $\langle a, b \rangle$ the commutator subgroup for G?

18. Refer to Example 6:

(a) Explain how to define a representation of a group G given a representation of a factor group G/N.

(b) Explain why $\chi(\gamma^2) = \chi(\gamma^3) = 1$.

(c) Explain why $\chi(\alpha^i \gamma^j) = 1$ for $j = 2, 3$ and $i = 1, \ldots, 4$.

19. In this exercise you will find all the irreducible representations of a group G in two special cases. In each case, explain how you know that you have them all.

(a) Find all the irreducible representations of $G = \langle a \,|\, a^{12} = 1 \rangle$.

(b) Find all the irreducible representations of the dihedral group $G = \langle a, b \mid a^6 = b^2 = 1, bab = a^{-1} \rangle$.

20. Choose $G = \langle b \mid b^4 = 1 \rangle$, so $G^* = \{\chi_0, \chi_1, \chi_2, \chi_3\}$, where $\chi_j(b) = i^j$.

(a) Calculate the sums in Theorem 11.18.

(b) Calculate the sums in Theorem 11.19.

(c) Let $A = 3 + 7ib - \pi b^2 + (2 - 5i)b^3$ and use the inversion formula (Theorem 11.20) to recover the coefficient of b.

21. Let $G = \langle b \mid b^7 = 1 \rangle$, and let $\omega = e^{2\pi i/7}$ be a primitive seventh root of unity. Define χ_j by $\chi_j(b) = \omega^j$ so $G^* = \{\chi_0, \chi_1, \ldots, \chi_6\}$.

(a) Let $D = \{b, b^2, b^4\}$ and verify that D satisfies the criterion in Theorem 11.21.

(b) Let $D' = \{b, b^2, b^3\}$. What goes wrong in checking the criterion in Theorem 11.21?

22. Prove Theorem 11.19. Ⓗ

23. Prove Theorem 11.20.

24. Prove Theorem 11.21

25. Let G be a finite group and let $\rho : G \to GL(V)$ be an arbitrary representation of G in V over $\mathbb{C}$ with character χ_ρ. Assume that $\sum_{g \in G} \chi_\rho(g) \neq 0$.

(a) Let χ_0 be the trivial character and calculate the inner product $\langle \chi_\rho, \chi_0 \rangle$.

(b) Show there exists a nonzero vector $\mathbf{v}$ such that $\rho(g)(\mathbf{v}) = \mathbf{v}$ for all $g \in G$. Ⓗ

26. In [**8**] on pages 320–321 is a proof of Theorem 6.9 that uses, in part, the theorems in this section. (It also uses quite a bit of group theory.) Try to read it!

11.5. Character tables

In this brief section, we introduce the idea of a character table, a useful way to tabulate information about the irreducible characters of a finite group G. A character table is a square array with rows indexed by the irreducible characters and columns indexed by the conjugacy classes of G. The orders of the rows and the columns are somewhat arbitrary, although the trivial character and the class of the group identity are listed first.

Example 8. We write out the character table for $G = S_3$.

We know from abstract algebra that the conjugacy classes of S_m consist of permutations with the same disjoint cycle structure, so there are 3 conjugacy classes in G. We write $[\pi]$ for the class containing π. Thus the classes are $[(1)] = \{(1)\}$, $[(123)] = \{(123), (132)\}$, and $[(12)] = \{(12), (13), (23)\}$. The three irreducible representations of S_3 were determined in Exercise 10. From these we get the character table:

	$[(1)]$	$[(123)]$	$[(12)]$
χ_0	1	1	1
χ_1	1	1	-1
χ_2	2	-1	0

$\diamond$

There are important facts about the structure of a finite group that are revealed in its character table. The exercises explore some of them. For example, we can determine from its character table whether a group is simple or not, and we can find its center. However, the character table of a finite group G does not determine G up to isomorphism. For example, the two non-abelian groups of order 8 (the dihedral group D_4 and the quaternion group) have the same character table.

Exercises

27. Let $G = \langle a \mid a^4 = 1 \rangle$.

(a) Find the character table of G.

(b) Let ρ_{reg} be the (left) regular representation of G, and let $\mathbf{e}_1, \mathbf{e}_a, \mathbf{e}_{a^2}, \mathbf{e}_{a^3}$ be the corresponding basis vectors of $\mathbb{C}^4$. Write ρ_{reg} as a sum of irreducible representations of G.

28. Find the character table of the dihedral group D_4. (The conjugacy classes of D_4 were determined in Exercise 12, page 208. A representation of degree 2 for the dihedral group is described in Example 10.11.) Ⓢ

29. Orthogonality relations for character tables.

Assume G is a finite group with irreducible characters $\chi_0, \ldots, \chi_t$, conjugacy classes $\mathcal{C}_0, \ldots, \mathcal{C}_t$ and class representatives $g_s \in \mathcal{C}_s$. Recall that $|\mathcal{C}_s| = [G : C_G(g_s)]$. (See Exercise 3.6.) We use the "Kronecker delta" δ_{rs}, where $\delta_{rs} = 0$ if $r \neq s$ and $\delta_{rr} = 1$.

(a) Row orthogonality: Show that

$$\sum_{j=0}^{t} \frac{\chi_r(g_j)\,\overline{\chi_s(g_j)}}{|C_G(g_j)|} = \delta_{rs}.$$

(b) Column orthogonality: Show that

$$\sum_{j=0}^{t} \chi_j(g_r)\,\overline{\chi_j(g_s)} = \delta_{rs}|C_G(g_r)|. \qquad \text{Ⓗ}$$

30. This is a companion to Exercise 28. In it you will find the character table for the quaternion group $Q = \langle a, b \,|\, a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle$, the other non-abelian group of order 8. (If you know the quaternion group as $\{\pm 1, \pm i, \pm j, \pm k\}$, choose $a = i$ and $b = j$.) You will see that the character tables for Q and D_4 are the same.

(a) Find the conjugacy classes of Q.

(b) Explain why you know Q has four linear irreducible characters $\chi_0, \chi_1, \chi_2, \chi_3$ and also an irreducible character ψ of degree 2, and find the linear characters of Q.

(c) From (b) write four rows of the character table of Q for the linear irreducible characters. The fifth row corresponds to

the irreducible character ψ of degree 2. As described below, there are two ways to determine the values of ψ. Do it both ways.

(i) Using x, y, z, w for the unknown values of ψ, write out the character table for Q. Now use the column orthogonality relations to find the values of x, y, z, w.

(ii) Find an irreducible representation of Q of degree 2 and determine the values of its character ψ directly.

31. Finding the center of a group from its character table.

Use the notation from Exercise 29. Show

$$Z(G) = \left\{ g \in G \;\middle|\; \sum_{j=0}^{t} \chi_j(g)\,\overline{\chi_j(g)} = |G| \right\}.$$

32. Finding normal subgroups from a character table.

(a) Suppose N is a normal subgroup of a finite group G. Define a representation of G of degree $[G:N]$ that has kernel N. Ⓗ

(b) Suppose ρ_1 is an irreducible components of a representation ρ of G. Show that the kernel of ρ is a subset of the kernel of ρ_1.

(c) Assume $\rho : G \to GL(m, \mathbb{C})$ is a representation of G and χ is the character of ρ. Show that $|\chi(g)| = \chi(1_G)$ if and only if $\rho(g) = \mu I_m$ for some root of unity μ. Ⓗ

(d) Let ρ be a representation of G. Show that $\mathrm{Ker}(\rho) = \{g \in G \,|\, \chi(g) = \chi(1)\}$.

(e) Explain how you can tell by looking at a character table for a finite group whether it has any nontrivial proper normal subgroups.

Coda

Although we only scratch the surface of the theory of characters of a finite group G, we see that the irreducible characters encode detailed information about the structure of G and about its representations. The class functions on G form a complex inner product space of dimension equal to the number of conjugacy classes in G. The Fundamental Theorem of Character Theory states that the irreducible characters form an orthonormal basis for this space. Consequently the character of a representation identifies it up to equivalence and tells us whether it is irreducible. Another consequence is that G is abelian if and only if all of its irreducible characters have degree 1.

Detailed examples drawn from [**65**] illustrate the use of these ideas in the search for a difference set. The key result in this chapter for tackling the existence question for abelian difference sets is Theorem 11.21. From Chapter 10 we know that if χ is a nontrivial irreducible character of an abelian (v, k, λ)-difference set D, then $z = \widetilde{\chi}(D)$ satisfies $z\overline{z} = n$ for $n = k - \lambda$. Theorem 11.21 guarantees that a subset of G of size k that survives a search using this necessary condition for every nontrivial irreducible character of G really is a difference set. Theorem 11.22 extends this characterization to non-abelian groups.

The origin of the theory of characters of a finite group goes back to the German mathematician G. Frobenius, in particular to his 1896 paper *Über die Gruppencharactere*, of which he wrote[2], "I shall develop the concept [of character for arbitrary finite groups] here in the belief that through its introduction, group theory will be substantially enriched." Frobenius' belief was correct, and tools from character theory belong in every group theorist's kit. Character tables for certain groups also play important roles in chemistry. (Physicists are more likely to be interested in infinite groups, especially the Lie groups mentioned in the Coda to Chapter 10.)

[2]From `www.history.mcs.st-andrews.ac.uk/Biographies/Frobenius.html`.

Chapter 12

Using Algebraic Number Theory

In this chapter we will combine tools from representation theory and algebraic number theory to investigate the existence of a difference set with particular parameters in a specific group.

Section 1 addresses the question you may be asking: why do we need all this machinery? In Section 2 we provide definitions and state without proof the facts we need from algebraic number theory to do our work. In Section 3 we examine instances of the use of these tools either to find a (v, k, λ)-difference set in a particular group or to disprove its existence. In Section 4 we use these methods to prove the second version of Turyn's exponent bound, our Theorem 7.7.

12.1. Why algebraic number theory?

The theory of multipliers is a major tool for the study of abelian difference sets. However, the hypotheses of the first and second multiplier theorems fail when $n = k - \lambda$ is a factor of v, as happens for the Hadamard family. For this family, Turyn's exponent bound is valuable, and its proof illustrates the power of the use of algebraic number theory and characters.

Representations and algebraic number theory serve us in more general ways too. A common strategy is to suppose that a (v, k, λ)-difference set D exists in the group G, and apply representations of G to the integral group ring equation $DD^{(-1)} = n1_G + \lambda G$. Let $\rho : G \to GL(d, \mathbb{C})$ be a representation. If ρ is nontrivial and irreducible, we know by Theorem 10.13 that $M = \widetilde{\rho}(D)$ implies $M\overline{M}^T = nI_d$.

An important special case is when the degree of ρ is 1, and we know the complex number $z = \widetilde{\rho}(D)$ satisfies $z\overline{z} = n$. Further, z is a special kind of complex number: it is a sum of mth roots of unity, where m is the exponent of G. The coefficients of the $|G|/|N|$ summands of z are the intersection numbers for D modulo $N = \text{Ker}\rho$. Our use of algebraic number theory will constrain these coefficients. We use the resulting information to determine possible intersection numbers for D, either to narrow the search for D or to prove such a difference set cannot exist.

We will return later to the general case, but for now we study representations of degree 1. We illustrate with the following example.

Example 1. Recall Example 10.5 (page 220), which was drawn from Smith's construction of a $(100, 45, 20)$-difference set in a non-abelian group G. With $v = 100$ and $n = 25$, this is a member of the Hadamard family. We used the normal subgroup G' for which $G/G' \cong \mathbb{Z}_4$ to define a representation ρ of degree 1 with

$$z = \widetilde{\rho}(D) = u_0 + u_1(i) + u_2(i^2) + u_3(i^3)$$

in $\mathbb{Z}[i]$, the ring of Gaussian integers, where the u_j are the intersection numbers $|D \cap G'c^j|$. We understand the Gaussian integers well. In particular, we know how to go from $z\overline{z} = 25$ to possible values for z, because we know how to factor 25 into a product of irreducible elements of the ring $\mathbb{Z}[i]$,

$$25 = (1 + 2i)^2(1 - 2i)^2,$$

and we know this factorization is unique up to unit factors. These facts enabled Smith to show that there were only three possibilities for the ordered list (u_0, u_1, u_2, u_3). $\diamond$

In general, we find ourselves dealing with the equation $z\overline{z} = n$ in a ring $\mathbb{Z}[\eta]$, where η is a primitive mth root of unity for values of

m other than 4. These more general rings (sometimes called rings of *cyclotomic integers*) are not always unique factorization domains.

Remark: Mathematicians trying to prove Fermat's Last Theorem in the first half of the nineteenth century fell into the trap of assuming unique factorization was guaranteed in these rings. In 1844, Kummer proved that when $m = 23$, $\mathbb{Z}[\eta]$ is *not* a unique factorization domain. It is now known that there are only finitely many values of m for which unique factorization holds.[1] However, Kummer did more than identify a problem. He began the solution: replacing products of ring elements by products of ideals. In fact, this is the origin of the notion of an ideal of a ring. Fortunately, using ideals in this way restores unique factorization.

12.2. Definitions and basic facts

Here we collect the information we need, omitting proofs but giving references at the end of the section. Some of the results in this section are major theorems and some are not, but for our purposes, we label all of them theorems.

Throughout this chapter we work in the complex numbers. Fix a positive integer m and assume η is a primitive mth root of unity, for example $\eta = e^{2\pi i/m}$. (Refer to A.15.)

Definition. Let η be a primitive mth root of unity. The smallest subfield of the complex numbers containing $\mathbb{Q}$ and η is denoted $\mathbb{Q}(\eta)$. It is called the mth cyclotomic field. It contains as a subring

$$\mathbb{Z}[\eta] = \left\{ \sum_{j=0}^{m-1} a_j \eta^j \;\middle|\; a_j \in \mathbb{Z} \right\},$$

which is the set of cyclotomic integers in $\mathbb{Q}(\eta)$.[2]

[1] The values of m, excluding $m \equiv 2 \pmod 4$, for which η an mth root of unity makes $\mathbb{Z}[\eta]$ a unique factorization domain are 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84. There is no loss in excluding $m \equiv 2 \pmod 4$ because in that case adjoining an $(m/2)$th root of unity to $\mathbb{Q}$ gives the same field as adjoining an mth root of unity. A reference is [**49**].

[2] It is an important theorem that $\mathbb{Z}[\eta]$ is exactly the set of elements of $\mathbb{Q}(\eta)$ that are zeroes of monic polynomials with integer coefficients.

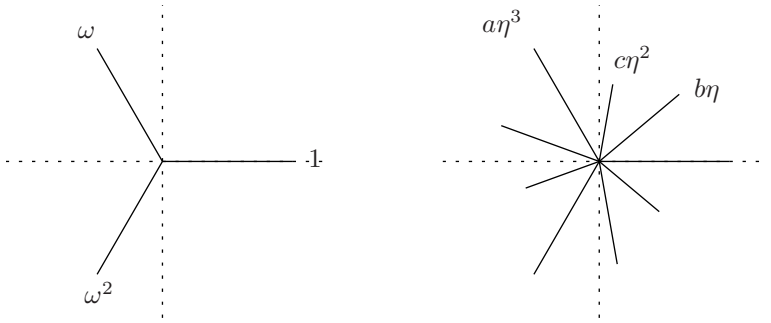
We often deal with equations of the form $\sum a_j \eta^j = 0$ where the a_j are ordinary integers, $0 \le j \le m-1$. A special case is $1 + \eta + \eta^2 + \cdots + \eta^{m-1} = (\eta^m - 1)/(\eta - 1) = 0$. Here all the coefficients of powers of η are equal. The following result is a partial converse. It shows that when m is a power of a prime, then for a sum of powers of η to equal 0, certain powers of η must have equal coefficients. We use this result often.

Theorem 12.1. *Let η be a primitive p^sth root of unity for a prime p. Suppose $\sum a_j \eta^j = 0$ for some $a_j \in \mathbb{Q}$. Then $a_j = a_\ell$ whenever $j \equiv \ell$ modulo p^{s-1}.*

Example 2. Let η be a primitive 9th root of unity. Notice that makes $\omega = \eta^3$ a primitive cube root of unity, and we know $1 + \omega + \omega^2 = 0$. For any $a, b, c \in \mathbb{Q}$, it follows that $a(1 + \omega + \omega^2) + b\eta(1 + \omega + \omega^2) + c\eta^2(1 + \omega + \omega^2) = 0$, so

$$a + b\eta + c\eta^2 + a\eta^3 + b\eta^4 + c\eta^5 + a\eta^6 + b\eta^7 + c\eta^8 = 0.$$

The force of the preceding theorem is that this is the only way a sum of powers of η can equal zero. Thus the coefficients of 1, η^3, and η^6 must be equal. Similarly the coefficients of η, η^4, and η^7 must be equal, and the coefficients of η^2, η^5, and η^8 must be equal. We illustrate this in Figure 12.1 using the lengths of rays to indicate the coefficients of the terms. ◇



(a) 3rd roots of unity **(b)** 9th roots of unity

Figure 12.1. Roots sum to 0, as in Example 2.

Next we recall some facts about rings and ideals from abstract algebra. A proper ideal A of a commutative ring R is called *prime* if it has the property that $a, b \in R$ with $ab \in A$ implies either $a \in A$ or $b \in A$. If A and B are ideals of R, then

$$AB = \left\{ \sum_{j=1}^{t} a_j b_j \;\middle|\; a_j \in A,\ b_j \in B,\ t \text{ a positive integer} \right\}$$

is also an ideal of R. If R is a commutative ring with 1, and if $a \in R$, then the set $aR = \{ar \mid r \in R\}$ is an ideal of R containing a. Such an ideal is called the *principal ideal* generated by a. The product of principal ideals is again principal: $(aR)(bR) = abR$.

If σ is a ring automorphism of R, then the image of any ideal under σ is again an ideal. Further, a ring automorphism takes products of ideals to products of ideals, and it takes prime ideals to prime ideals and principal ideals to principal ideals. We are particularly interested in the ring automorphism $\sigma(z) = \overline{z}$ of $\mathbb{C}$. Specifically, if R is a subring of the complex numbers fixed under complex conjugation and if aR is a principal ideal of R, then $\overline{(aR)} = \overline{a}R$. Note that since $\overline{\eta} = \eta^{-1} = \eta^{m-1}$, the ring $R = \mathbb{Z}[\eta]$ is fixed under complex conjugation.

Since $\mathbb{C}$ has no zero divisors and R is a subset of $\mathbb{C}$, it follows that R has no zero divisors. We are interested in cases when $aR = bR$ for $a, b \in R$. Since R has no zero divisors, $a = br$ and $b = as$ imply $rs = 1$, so $a = br$ where r is a unit in R. Further, if $|a| = |b|$, then $|r| = 1$. The next theorem tells us that complex numbers of length 1 in $R = \mathbb{Z}[\eta]$ have a special form.

Theorem 12.2. *Let η be a primitive mth root of unity. If $r \in \mathbb{Z}[\eta]$ and $r\overline{r} = 1$, then $r = \pm\eta^{\ell}$ for some integer ℓ.*

The major result we exploit in this chapter is the following.

Theorem 12.3. *Let η is a primitive mth root of unity and $R = \mathbb{Z}[\eta]$. Then every ideal in R can be written uniquely as a product of prime ideals.*

The next theorem tells us about the factorization of the ideal pR into prime ideals, when $p \in \mathbb{Z}$ is a prime. Recall that for a positive

integer m, the *Euler phi function* $\phi(m)$ is the number of positive integers less than m and relatively prime to m.

Theorem 12.4. *Let η be a primitive mth root of unity and let $R = \mathbb{Z}[\eta]$. Let p be a prime integer.*

(i) Assume p does not divide m. Let f be the order of p modulo m; that is, f is the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then in R, $pR = P_1 \cdots P_g$ where the P_j are distinct prime ideals and $g = \phi(m)/f$.

(ii) Let $m = p$. Then $(1-\eta)R$ is a prime ideal in R, and $pR = ((1-\eta)R)^{p-1}$.

(iii) Assume P is a prime ideal occurring in the factorization of pR. If p is odd, then P occurs with exponent greater than 1 if and only if $p|m$. If $p = 2$, then P occurs with exponent greater than 1 if and only if $4|m$.

Recall that when we apply a linear character to the equation $DD^{(-1)} = n1_G + \lambda G$ we get the equation $z\overline{z} = n$. In our first example we illustrate the use of our theorems from number theory to determine possible values for the complex number z.

Example 3. Let $\eta = e^{2\pi i/5}$ and $R = \mathbb{Z}[\eta]$. Suppose $z \in R$ and $z\overline{z} = 36$. We show $z = \pm 6\eta^\ell$ for some ℓ. Let $u = z/6$. Since $|z| = 6$, it follows that $|u| = 1$. The tricky part is to show that $u \in R$.

First, note that 2 and 3 each have order 4 modulo 5, and $\phi(5) = 4$. So by Theorem 12.4(i) we know $2R$ and $3R$ are prime ideals. By the multiplication of principal ideals we have

$$(zR)(\overline{z}R) = 36R = (2R)^2(3R)^2.$$

Since $\overline{2}R = 2R$ and $\overline{3}R = 3R$, Theorem 12.3 implies $zR = \overline{z}R = (2R)(3R) = 6R$. Now we know $z = 6r$ for $r \in R$. Since $|z| = 6$, we have $|r| = 1$. By Theorem 12.2, $r = \epsilon\eta^\ell$ for some $\epsilon = \pm 1$ and some integer ℓ. So $z = \pm 6\eta^\ell$. ◇

This next example illustrates how we use these number theory facts to find intersection numbers for difference sets.

Example 4. Let $\eta = e^{2\pi i/5}$ and assume $v_0, \ldots, v_4$ are non-negative integers that satisfy $\sum v_j = 24$ and $\sum v_j\eta^j = 6\epsilon\eta^\ell$ for some $\epsilon = \pm 1$

and some ℓ. Applying Theorem 12.1, we have that $v_\ell - 6\epsilon = v_j$ for $j \neq \ell$, and the set $\{v_j\} = \{c + 6\epsilon, c, \ldots, c\}$ for some c. Thus $\sum v_j = 5c + 6\epsilon = 24$. This can only be true if $\epsilon = -1$ and $c = 6$, so the numbers v_j are determined up to order: $\{0, 6, 6, 6, 6\}$. $\diamond$

Theorem 12.4(ii) shows us the prime factorization of the ideal pR in the case that prime $p = m$. Here we look at a specific example.

Example 5. Let η be a primitive cube root of unity and $R = \mathbb{Z}[\eta]$. By Theorem 12.4(ii), $3R = ((1-\eta)R)^2$. This says $3R = (1-\eta)^2 R$. This is confirmed when we calculate $(1-\eta)^2 = 1-2\eta+\eta^2 = 1+\eta+\eta^2-3\eta = 3(-\eta)$. $\diamond$

We need one more result for our proof of Turyn's exponent bound in Section 4. Notice in particular that it explains the reason for the terminology when we say one integer is *self-conjugate* modulo another in the definition in Section 7.2, page 114.

Theorem 12.5. *Let η be a primitive mth root of unity and let $R = \mathbb{Z}[\eta]$. Let $p \in \mathbb{Z}$ be a prime that is self-conjugate modulo m. Let P be a prime ideal occurring in the prime factorization of pR. Then P is fixed under complex conjugation; that is, $\overline{P} = P$.*

References. A good general reference for this material is [**32**]. There are also useful summaries (with references) in Chapter VI, Section 15 of [**8**] and in Section 1.2 of [**59**]. For more specific references, see the following list.

- The proof of Theorem 12.1 can be found in [**31**], where it appears as Lemma 3.2. The case of Theorem 12.1 when $m = p$ is prime is due to McFarland in [**51**].
- For the proof of Theorem 12.2, see Corollary 15.9 in [**8**].
- For the proof of Theorem 12.3, see, for example, Theorem 2 on page 180 of [**32**].
- For the proof of the first part of Theorem 12.4, see [**32**], Theorem 2 on page 196. For proofs of the second and third parts see Propositions 13.27 and 13.28 on page 197.
- For the proof of Theorem 12.5 see [**8**], p. 438.

Exercises

1. Let $\eta = e^{2\pi i/7}$ and let $R = \mathbb{Z}[\eta]$. Suppose $z \in R$ with $z\overline{z} = 9$, and show that $z = \pm 3\eta^\ell$ for some integer ℓ.

2. Let $\eta = e^{2\pi i/5}$ and assume that $\{v_j\}$ is a set of five non-negative integers satisfying $\sum v_j = 24$ and $\sum v_j \eta^j = 4\epsilon\eta^\ell$ for some integer ℓ and $\epsilon = \pm 1$. Find the set of values $\{v_j\}$, using the theorems of this section to justify your work. Ⓢ

3. Let $\eta = e^{2\pi i/7}$ and assume that $\{v_j\}$ is a set of seven non-negative integers satisfying $\sum v_j = 11$ and $\sum v_j \eta^j = 3\epsilon\eta^\ell$ for some integer ℓ and $\epsilon = \pm 1$. Show that this leads to a contradiction.

4. Let $\eta = e^{2\pi i/7}$, and let $R = \mathbb{Z}[\eta]$. Theorem 12.4(ii) says that the ideal $7R$ can be factored into prime ideals as $7R = ((1-\eta)R)^6$. Confirm this by calculating $(1-\eta)^6$.

12.3. Seeking difference sets

Now we use the techniques of the previous section to address the existence question for difference sets. Some of these examples could be analyzed by other means (e.g., multipliers), but we concentrate here on illustrating the use of tools from representation theory and algebraic number theory.

Example 6. Let G be an abelian group of order 25. We show that G cannot contain a $(25, 9, 3)$-difference set. We know that either G is cyclic or is isomorphic to $\mathbb{Z}_5 \oplus \mathbb{Z}_5$, so G contains a normal subgroup N of order 5. Then G/N must be cyclic of order 5, say $G/N = \langle aN \rangle$. Let $\eta = e^{2\pi i/5}$, and consider the character χ of G with kernel N that maps a to η.

Suppose D is a $(25, 9, 3)$-difference set in G, and let $v_j = |D \cap a^j N|$ be the intersection numbers for D in the cosets of N. Then $z = \widetilde{\chi}(D) = \sum_j v_j \eta^j \in R = \mathbb{Z}[\eta]$. In Example 3 we found that both $2R$ and $3R$ are prime ideals in R. We know $z\overline{z} = n = 6$, so $(zR)(\overline{z}R) = (2R)(3R)$. However, since $\overline{2}R = 2R \neq \overline{3}R = 3R$,

$(zR)(\overline{z}R) = (2R)(3R)$ is impossible. Therefore no such difference set can exist. ◇

Example 7. Let G be a group of size 78 that contains a normal subgroup N of size 6. We show that G does not contain a nontrivial difference set.

Suppose D is a nontrivial difference set in G. We may assume that $k < v/2$, so its parameters must be $(78, 22, 6)$. The factor group G/N is cyclic of order 13, say $G/N = \langle aN \rangle$. Let $v_j = |D \cap a^j N|$ be the intersection numbers. Let $\eta = e^{2\pi i/13}$ and $R = \mathbb{Z}[\eta]$, and consider the linear character χ with kernel N that maps a to η. Let $z = \widetilde{\chi}(D) = \sum v_j \eta^j$. Applying $\widetilde{\chi}$ to $DD^{(-1)} = n1_G + \lambda G$ yields $z\overline{z} = n = 16$.

Since 2 has order 12 mod 13 and $\phi(13) = 12$, Theorem 12.4(i) tells us that $2R$ is a prime ideal in R. We have $(zR)(\overline{z}R) = (2R)^4$, so it must be that $zR = 4R$ and $z = 4\epsilon\eta^\ell$ for some integer ℓ and some choice of $\epsilon = \pm 1$. Now Theorem 12.1 tells us that $\{v_j\} = \{c+4\epsilon, c, \ldots, c\}$ for some integer c. So $\sum v_j = 22 = 13c+4\epsilon$. Solving, we get $\epsilon = -1$ and $c = 2$. This would give an intersection number equal to $c + 4\epsilon = 2 - 4 < 0$, which is impossible. ◇

Example 8. This example may seem too elementary (and familiar), but it sets us up for a more interesting one. Let $G = \langle a \,|\, a^7 = 1 \rangle$, and suppose D is a $(7, 3, 1)$-difference set in G. Let $\eta = e^{2\pi i/7}$ and $R = \mathbb{Z}[\eta]$. Since the order of 2 modulo 7 is 3 while $\phi(7) = 6$, the ideal $2R$ factors as a product of *two* prime ideals in R. We observed in Chapter 1 that if $\alpha = \eta+\eta^2+\eta^4$, then $\alpha\overline{\alpha} = 2$. Since $\overline{\alpha} \neq \pm\eta^j\alpha$ for any j, αR and $\overline{\alpha}R$ are distinct ideals. This tells us that $2R = (\alpha R)(\overline{\alpha}R)$ is the desired factorization as a product of two (prime) ideals.

Define a character of G by $\chi(a) = \eta$ and let $z = \widetilde{\chi}(D)$. Then $z\overline{z} = 2$, so $(zR)(\overline{z}R) = (\alpha R)(\overline{\alpha}R)$ and we have two cases: either $zR = \alpha R$ or $zR = \overline{\alpha}R$. In the first case, $z = \epsilon\eta^\ell(\eta + \eta^2 + \eta^4)$ for some ℓ and some $\epsilon = \pm 1$. Translating D by a suitable power of a we can assume $\ell = 0$ and $z = \epsilon(\eta + \eta^2 + \eta^4)$. Since the coefficients of z are non-negative, $\epsilon = 1$ and we must have $D = \{a, a^2, a^4\}$, our old friend from Chapter 1. Similarly, if $zR = \overline{\alpha}R$, up to translation we get $D = \{a^3, a^5, a^6\}$, also a difference set (and equivalent to the previous one via the automorphism $a \mapsto a^{-1}$). ◇

Example 9. In Exercise 6.16 we used multipliers to find a difference set in $\mathbb{Z}_{21}$. We revisit this case to illustrate the use of other methods. In particular, we use the number theory from Example 8 to look for a $(21, 5, 1)$-difference set D in $G = \langle a, b \mid a^7 = b^3 = 1, ab = ba\rangle$. First choose $N_1 = \langle a\rangle$ and let $u_s = |D \cap b^s N_1|$. By Theorem 7.1, $u_0 + u_1 + u_2 = 5$ and $u_0^2 + u_1^2 + u_2^2 = 4 + 1 \cdot 7 = 11$. We find that the only possibility is $\{u_s\} = \{3, 1, 1\}$. By translating D by a suitable power of b if necessary, we can assume $|D \cap N_1| = 3$.

Next choose $N_2 = \langle b\rangle$ and let $v_j = |D \cap a^j N_2|$. Let $\eta = e^{2\pi i/7}$ and let $R = \mathbb{Z}[\eta]$. From Example 8 we know $2R = (\alpha R)(\overline{\alpha}R)$ as a product of prime ideals in R for $\alpha = \eta + \eta^2 + \eta^4$. Now let χ be the character of G with kernel N_2 taking a to η. Then $z = \widetilde{\chi}(D)$ satisfies $(zR)(\overline{z}R) = (\alpha R)^2(\overline{\alpha}R)^2$. We see there are three cases:

(a) $zR = (\alpha R)(\overline{\alpha}R) = 2R$ and $z = 2\epsilon\eta^\ell$ for some ℓ and some $\epsilon = \pm 1$.

(b) $zR = \alpha^2 R = (\eta + \eta^2 + 2\eta^3 + \eta^4 + 2\eta^5 + 2\eta^6)R$.

(c) $zR = \overline{\alpha}^2 R$.

Case a. We have $\sum v_j\eta^j = 2\epsilon\eta^\ell$. Translating by a power of a if necessary, we may assume $\ell = 0$ (without changing the N_1 intersection numbers). We find that $\{v_j\} = \{c+2\epsilon, c, \ldots, c\}$ for some c, so $\sum v_j = 7c+2\epsilon = 5$. The only solution is $\epsilon = -1$ and $c = 1$, but then $v_0 = 1-2$, which is impossible. Therefore this case cannot occur.

Case b. This time we have $\sum v_j\eta^j = \epsilon\eta^\ell(\eta+\eta^2+2\eta^3+\eta^4+2\eta^5+2\eta^6)$. As before, we may assume $\ell = 0$. Now we have

$$(v_0, v_1, \ldots, v_6) = (c, c+\epsilon, c+\epsilon, c+2\epsilon, c+\epsilon, c+2\epsilon, c+2\epsilon),$$

so $\sum v_j = 7c + 9\epsilon = 5$. This has a solution: $\epsilon = -1$ and $c = 2$, giving $(v_0, \ldots, v_6) = (2, 1, 1, 0, 1, 0, 0)$. This is consistent with $\sum v_j^2 = 4+1\cdot 3$.

We consider the grid in Figure 12.2, where the column totals are the N_2 intersection numbers and the row totals are the N_1 intersection numbers. Since $b^s N_1 \cap a^j N_2 = \{a^j b^s\}$, each empty cell can be filled only with 0 or 1. Looking at the first row, we see there are four possibilities for where the fourth 0 can go. If the first row of the table is $(1, 1, 1, 0, 0, 0, 0)$ then D contains $\{1, a, a^2\}$, and a equals a

	N_2	aN_2	a^2N_2	a^3N_2	a^4N_2	a^5N_2	a^6N_2	
N_1				0		0	0	3
bN_1				0		0	0	1
b^2N_1				0		0	0	1
	2	1	1	0	1	0	0	5

Figure 12.2. Intersection numbers for possible cyclic (21,5,1)-difference set.

"difference" of elements of D in at least two ways. So this cannot lead to a difference set.

Next we try the first row $(0, 1, 1, 0, 1, 0, 0)$. This time the only way to complete the table consistent with the intersection numbers gives $D = \{a, a^2, a^4, b, b^2\}$. Making a "difference" table, we see this *is* a difference set.

We leave the rest of Case (b) and also Case (c) as an exercise. $\diamond$

In the next example we consider a group representation of degree 2. We see this basic idea again in Example 11 and in Exercises 8–10.

Example 10. Let G be the group of order 78 defined by

$$\begin{aligned} G &= \langle a, b, c \mid a^{13} = b^2 = c^3 = 1,\, bab^{-1} = a^{-1},\, ac = ca,\, bc = cb \rangle \\ &\cong D_{13} \times \mathbb{Z}_3, \end{aligned}$$

and suppose G contains a non-trivial difference set. Then it would contain a difference set D with parameters $(78, 22, 6)$. We show that this leads to a contradiction.

First note that $N_1 = \langle a, c \rangle$ is a normal subgroup of G of order 39. Suppose u_0 and u_1 are the intersection numbers for N_1, so $u_0 + u_1 = 22$ and $u_0^2 + u_1^2 = 16 + 6 \cdot 39 = 250$. Just by trying possibilities, we see that we must have $\{u_0, u_1\} = \{9, 13\}$.

Now choose $\eta = e^{2\pi i/13}$ and let $R = \mathbb{Z}[\eta]$. As in Example 10.11 (page 174), we can define an irreducible representation ρ with kernel $N_2 = \langle c \rangle$ by

$$\rho(a) = \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix} \quad \text{and} \quad \rho(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let $v_{js} = |D \cap a^j b^s N_2|$. Then

$$M = \widetilde{\rho}(D) = \begin{bmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{bmatrix},$$

for $\alpha = \sum_j v_{j0}\eta^j$ and $\beta = \sum_j v_{j1}\eta^j$. By Theorem 10.13, we know $M\overline{M}^T = 16I_2$, so $\alpha\overline{\alpha} + \beta\overline{\beta} = 16$ and $\alpha\beta = 0$. There are thus two cases: $\beta = 0$ and $\alpha\overline{\alpha} = 16$, or $\alpha = 0$ and $\beta\overline{\beta} = 16$. In the first case, because $2R$ is a prime ideal in R, we have $\alpha = 4\epsilon\eta^\ell$ for some ℓ and $\epsilon = \pm 1$. By Theorem 12.1 it follows that $\{v_{j0}\} = \{d + 4\epsilon, d, \ldots, d\}$ for some constant d. Thus $\sum_j v_{j0} = 13d + 4\epsilon$.

Note that $a^j N_2 \subseteq N_1$ for each j, so $\sum_j v_{j0} = u_0$, which is 9 or 13. There is no solution to $13d + 4\epsilon = 13$. If $13d + 4\epsilon = 9$, the only solution is $\epsilon = -1$ and $d = 1$. However, that would give an intersection number of $d + 4\epsilon = -3 < 0$, which is impossible. A similar argument leads to a contradiction in the case $\alpha = 0$. $\diamond$

Example 11. In 1993 a new symmetric $(160, 54, 18)$ design was found. Prompted by this discovery, in the summer of 1994 a group of undergraduates searched for difference sets with these parameters [**1**]. One of the students' results was that no $(160, 54, 18)$-difference set exists in a group G with a normal subgroup N' of size 4 for which $G/N' \cong D_{10} \times \mathbb{Z}_2$. The argument is intricate, but we sketch part of it here. If we choose $\eta = e^{2\pi i/5}$ (and let $R = \mathbb{Z}[\eta]$), then $-\eta$ has order 10 and G has an irreducible representation ρ with kernel $N = N' \times \mathbb{Z}_2$ and with

$$a \mapsto \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix} \quad \text{and} \quad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

where $\zeta = (-\eta)^m$ for some m. As usual, we suppose D is such a difference set and let $v_{js} = |D \cap a^j b^s N|$. Then we find

$$\widetilde{\rho}(D) = \begin{bmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{bmatrix},$$

where $\alpha = \sum v_{j0}\zeta^j$ and $\beta = \sum v_{j1}\zeta^j$. As in Example 10, we have $\overline{\alpha}\alpha + \overline{\beta}\beta = 36$ and $\alpha\beta = 0$. In this case $2R$ and $3R$ are prime ideals in R, so $36R = (2R)^2(3R)^2$ as a product of prime ideals. Suppose first that $\beta = 0$, so $(\alpha R)(\overline{\alpha R}) = (2R)^2(3R)^2$. The only possibility is that $\alpha R = 6R$ and $\alpha = 6\epsilon\eta^\ell$ for some $\epsilon = \pm 1$ and some ℓ. If $\zeta = \eta^2$, then

$\alpha = \alpha_1$ where

$$\begin{aligned}\alpha_1 &= (v_{00} + v_{50}) + (v_{10} + v_{60})\eta + (v_{20} + v_{70})\eta^2 \\ &\quad + (v_{30} + v_{80})\eta^3 + (v_{40} + v_{90})\eta^4.\end{aligned}$$

On the other hand, if we choose $\zeta = -\eta$, then $\alpha = \alpha_2$ where

$$\begin{aligned}\alpha_2 &= (v_{00} - v_{50}) + (v_{60} - v_{10})\eta + (v_{20} - v_{70})\eta^2 \\ &\quad + (v_{80} - v_{30})\eta^3 + (v_{40} - v_{90})\eta^4.\end{aligned}$$

Similar equations in $\mathbb{Z}[\eta]$ hold for β in the two cases, giving $\beta = \beta_1$ and $\beta = \beta_2$. Without loss of generality, we can assume $\sum v_{j0} = 24$ and $\sum v_{j1} = 30$. By a careful examination of cases, and up to equivalence, the students showed there were just two possibilities for the ordered list of 20 intersection numbers. The rest of the analysis involved calculating intersection numbers for normal subgroups containing N and their relationship to unions of cosets mod N and also intersection numbers for cosets mod N' to show that no difference set can exist. (There is also a slicker proof using Dillon's dihedral trick along with a theorem of Lander.) ◇

Exercises

5. Fill in the details in Example 9 as follows:

(a) Explain why in case (a) we may assume $\ell = 0$.

(b) Complete case (b).

(c) Analyze case (c).

6. Let G be a group of order 154 that contains a normal subgroup N of order 14. Show that G cannot contain a $(154, 18, 2)$-difference set. Ⓢ

7. Fill in the details in Example 10 as follows:

(a) Verify that $\{u_0, u_1\} = \{9, 13\}$.

(b) Explain why $\alpha = \sum v_{j0}\eta^j$ and $\beta = \sum v_{j1}\eta^j$.

(c) Carry out the calculations for the case when $\alpha = 0$.

The next two exercises are based on [**56**]. Note that Walker was an undergraduate when she did the work in this paper.

8. Let $G \cong D_{11} \times \mathbb{Z}_3$. Show that G cannot contain a $(66, 26, 10)$-difference set by assuming D is such a difference set and obtaining a contradiction as follows:

(a) Explain why G has a normal subgroup of index 2 and find the intersection numbers for D modulo this subgroup.

(b) Use an irreducible representation of G of degree 2 (as in Example 10) to analyze the intersection numbers for D modulo the normal subgroup of order 3. Show that this leads to a contradiction.

9. The goal of this exercise is to prove the following theorem from [**56**].

Theorem *Let p and q be odd primes with $q < p$, and let $G \cong D_p \times \mathbb{Z}_q$. Then the existence of a nontrivial (v, k, λ)-difference set in G implies the existence of positive integers t and r such that $r < p$ and $t < q$ and satisfying $k = pt + qr$, $\lambda = 2rt$, and $n = (pt - qr)^2$. Furthermore, if the order modulo p of each prime divisor of n is equal to $p - 1$, then $qr > pt$, $t + \sqrt{n} \leq q$, and $t = (k - \sqrt{n})/(2p)$.*

Let $G = \langle a, b, c \mid a^p = b^2 = c^q = 1,\ bab^{-1} = a^{-1},\ ac = ca,\ bc = cb \rangle$ where p and q are odd primes with $q < p$, and assume G contains a (v, k, λ)-difference set with $k < v/2 = pq$.

(a) Let $N_1 = \langle a, c \rangle$, a normal subgroup of G of index 2, and let w_0, w_1 be the intersection numbers modulo N_1. Show $2w_0w_1 = \lambda pq$ and explain why this implies each of p and q must divide exactly one of w_0 or w_1. Further, without loss of generality, we may assume $p|w_1$ and $q|w_0$.

(b) Write $w_0 = qr$ and $w_1 = pt$. Show that $r < p$ and $t < q$, and that $k = pt + qr$, $\lambda = 2rt$, and $n = (pt - qr)^2$.

Now assume the order mod p of each prime divisor of n is $p - 1$. Let $\eta = e^{2\pi i/p}$ and $R = \mathbb{Z}[\eta]$. Use the irreducible representation of G of

degree 2 with kernel $N_2 = \langle c \rangle$:

$$a \mapsto \begin{bmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{bmatrix} \quad \text{and} \quad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad c \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and write the intersection numbers $v_{js} = |D \cap a^j b^s N_2|$. As in Example 10,

$$\widetilde{\rho}(D) = \begin{bmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{bmatrix},$$

for $\alpha = \sum_j v_{j0}\eta^j$ and $\beta = \sum_j v_{j1}\eta^j$, elements in R.

(c) Show that $\alpha = 0$ leads to a contradiction.

(d) Assume that $\beta = 0$ and show that $v_{j1} = t$ for all j. Also in this case explain why $\alpha = \epsilon\eta^\ell\sqrt{n}$ for some ℓ and some $\epsilon = \pm 1$, and therefore $p-1$ of the v_{j0} equal some constant d, and the other is $d+\epsilon\sqrt{n}$. Conclude that $qr = pd + \epsilon|pt - qr|$.

(e) Show that $pt > qr$ leads to a contradiction. Ⓗ

(f) Show that $pt < qr$ implies $t = (k - \sqrt{n})/2p$ (which must be an integer) and $t + \sqrt{n} \le q$.

10. Use the Moore-Walker theorem given in Exercise 9 to rule out a $(370, 82, 18)$-difference set in $G \cong D_{37} \times \mathbb{Z}_5$. (By the way, if η is a primitive 37th root of unity, then $R = \mathbb{Z}[\eta]$ is not a unique factorization domain, so it really matters that our methods depend on the unique factorization of ideals, not of ring elements.)

12.4. Proving Turyn's exponent bound

In this section we prove the second version of Turyn's exponent bound, a nice illustration of the use of some of the methods of this chapter. Indeed, the innovative arguments in Turyn's paper [**69**] pointed the way to the increased use of these tools for the study of difference sets.

We begin with two lemmas. The first—usually called "Ma's lemma"—was proved by Ma in his 1985 thesis in Hong Kong. In [**8**] (p. 412) the authors call it "one of the most useful tools in the non-existence theory of difference sets," and a proof is given of a

more general result.[3] The use of the second lemma explains why self-conjugacy appears in the hypothesis of Turyn's theorem.

Recall that we write $X \equiv 0 \pmod{q}$ for $X \in \mathbb{Z}G$ if every coefficient of X is divisible by $q \in \mathbb{Z}$. Similarly, for $x = \sum a_j \eta^j \in \mathbb{Z}[\eta]$, we write $x \equiv 0 \pmod{q}$ if $a_j \equiv 0 \pmod{q}$ for each j.

Lemma 12.6. *(Ma) Let G be a finite abelian group with a cyclic Sylow p-subgroup P, and let Q be the unique subgroup of P of order p. Suppose $Y \in \mathbb{Z}G$ satisfies $\widetilde{\chi}(Y) \equiv 0 \pmod{p^a}$ for every nontrivial character χ of G. Then there exist $X_1, X_2 \in \mathbb{Z}G$ with $Y = p^a X_1 + QX_2$. Further, if the coefficients of Y are non-negative, X_1 and X_2 can be chosen with non-negative coefficients.*

Lemma 12.7. *Let η be a primitive mth root of unity and let $R = \mathbb{Z}[\eta]$. Let $p \in \mathbb{Z}$ be a prime with p self-conjugate modulo m. Suppose further that $z \in R$ satisfies $z\overline{z} = n \in \mathbb{Z}$ and $p^{2a} | n$ for some $a \geq 1$. Then $z \equiv 0 \pmod{p^a}$.*

Proof. The proof depends on the prime factorizations of the ideals zR and pR. Suppose $zR = Q_1 \cdots Q_s$ and $pR = P_1 \cdots P_t$ where the Q_i and P_j are prime ideals. Since p is self-conjugate modulo m, we know $P_j = \overline{P_j}$ for each j. By hypothesis, we may write $n = p^{2a}q$ for some integer q. Then we have $(zR)(\overline{z}R) = nR = (pR)^{2a}(qR)$ and

$$\begin{aligned}(Q_1 \cdots Q_s)(\overline{Q}_1 \cdots \overline{Q}_s) &= (P_1)^a \cdots (P_t)^a (\overline{P}_1)^a \cdots (\overline{P}_t)^a (qR) \\ &= (P_1)^{2a} \cdots (P_t)^{2a} (qR).\end{aligned}$$

From this we see that for each prime ideal P_j, all $2a$ factors must appear among $Q_1, \ldots, Q_s, \overline{Q}_1, \ldots, \overline{Q}_s$. Further, because P_j is self-conjugate, it must appear the same number of times among the Q_i and among the $\overline{Q}_i$. It follows that $P_1^a, \ldots, P_t^a$ all occur among $Q_1, \ldots, Q_s$. This means $zR = (p^a R)A$ for some ideal A, and $z = p^a r$ for some $r \in R$. From this it follows that $z \equiv 0 \pmod{p^a}$. □

Now we are ready to prove Turyn's Theorem 7.7, which we restate here for convenience.

[3] The authors note that a similar result was previously obtained by Lander (using different language). It appears as Proposition 4.29 in [**43**].

Theorem *(Turyn's exponent bound, second version) Assume the existence of a (v, k, λ)-difference set D in an abelian group G. Let p be a prime divisor of v and denote the Sylow p-subgroup of G by P. Assume that p^{2a} divides n for some $a \geq 1$. Let U be any subgroup of G with $U \cap P = \{1_G\}$. If p is self-conjugate modulo $e = exp(G/U)$, then*

$$exp(P) \leq |U| \frac{|P|}{p^a}.$$

Proof. By the structure theorem for finite abelian groups, the p-group P is isomorphic to a direct sum of cyclic p-groups, $P \simeq C_1 \oplus \cdots \oplus C_t$, with $|C_i| = p^{a_i}$. Without loss of generality, we can assume $a_1 \geq \cdots \geq a_t$. Then the exponent of P is p^{a_1}. Further, P contains a subgroup W with $W \simeq C_2 \oplus \cdots C_t$, and $P/W \simeq C_1$ is cyclic of order p^{a_1}. It follows that $|W| = |P|/\exp(P)$.

Choose a subgroup U of G with $U \cap P = \{1_G\}$, and let K be the subgroup of G generated by U and W, so $|K| = |U||W|$. Let $H = G/K$, so H has a cyclic Sylow p-subgroup of order p^{a_1}. (It is isomorphic to C_1.)

Let $\varphi : G \to H$ be the natural map and let $E = \widehat{\varphi}(D) \in \mathbb{Z}H$. By Theorem 7.3, we know that in $\mathbb{Z}H$

$$EE^{(-1)} = n1_H + \lambda|K|H.$$

Let χ be a nontrivial irreducible character of H and let $z = \widetilde{\chi}(E)$. We know $z \in \mathbb{Z}[\eta]$ for η a primitive mth root of unity, where m is the exponent of H. By Theorem 10.13 we also know $z\overline{z} = n \equiv 0 \pmod{p^{2a}}$.

In order to apply Lemma 12.7, we need to know that p is self-conjugate modulo the exponent of $H = G/K$. By hypothesis we know p is self-conjugate modulo the exponent of G/U. Recall that this means there is some non-negative integer j with $p^j \equiv -1 \pmod{w'}$, where $\exp(G/U) = w'p^b$ for w' relatively prime to p.

How do the exponents of G/U and G/W compare? To aid in our explanation, we refer to group elements whose orders are relatively prime to p as p'-elements. Since $K = \langle U, W\rangle$ with $U \cap P = \{1_G\}$ and $W \subset P$, the p'-elements of G/K have the same orders as the p'-elements of G/U. It follows that $\exp(G/K) = w'p^c$ for the same

choice of w' relatively prime to p. Thus p is also self-conjugate modulo the exponent of G/K, and we can conclude that $z \equiv 0 \pmod{p^a}$.

Now we are ready to apply Ma's lemma to the abelian group H and to $E \in \mathbb{Z}H$. Since $\widetilde{\chi}(E) \equiv 0 \pmod{p^a}$ for every nontrivial character χ of H, we can find $X_1, X_2 \in \mathbb{Z}H$ with $E = p^a X_1 + QX_2$, where Q is the unique subgroup of order p in the Sylow p-subgroup of H. Since the coefficients of E are non-negative, we may assume those of X_1 and X_2 are as well.

Next we show that X_1 cannot be zero. If $X_1 = 0$, we would have $E = QX_2$. Let ψ be a character of H and let τ be the restriction of ψ to Q. We can choose ψ so that τ is nontrivial on Q. Then $\widetilde{\psi}(Q) = \widetilde{\tau}(Q) = 0$. This implies $z = \widetilde{\psi}(E) = 0$, contradicting $z\overline{z} = n \neq 0$. Therefore $X_1 \neq 0$.

Since X_1 is nonzero and X_1 and X_2 have non-negative coefficients, $E = p^a X_1 + QX_2$ has at least one coefficient greater than or equal to p^a. However, the coefficients of E are the intersection numbers for the difference set D with respect to the subgroup K. Therefore no coefficient of E can exceed $|K| = |U||W|$ so

$$p^a \leq |U||W| = |U| \frac{|P|}{\exp(P)}.$$

Rearranging the inequality gives us

$$\exp(P) \leq |U| \frac{|P|}{p^a}.$$ □

Coda

If D is a (v, k, λ)-difference set in G and χ is a nontrivial linear character of G, then the complex number $z = \widetilde{\chi}(D)$ satisfies $z\overline{z} = n$. We want to use the factorization of n to recover z. Since z is in $\mathbb{Z}[\eta]$ for a suitable primitive root of unity η, we face the problem of factoring n into primes in $\mathbb{Z}[\eta]$. However, in general $R = \mathbb{Z}[\eta]$ is not a unique factorization domain, so the full list of possibilities for z is difficult to determine. To overcome this obstacle, we translate our problem into factoring the ideal nR into prime ideals in R, where the factorization is unique.

Our treatment of algebraic number theory is quite cursory, and we make heavy use of [**32**] as a reference for the theorems we quote without proof. Although this is a graduate text, it is very clearly written, and much of it is accessible after a course in abstract algebra that includes rings and fields. It is a good resource for the reader who wants more depth. We also recommend the undergraduate text [**67**]. It has nice historical motivation and helpful examples.

We have only tasted the application of tools from algebraic number theory to the study of difference sets. For the reader who would like to see more, we recommend McFarland's paper [**51**]. The first two sections (introduction and abelian characters) lay out the tools from character theory and algebraic number theory that he uses to get his main result. The third section (character sums) contains a sequence of lemmas whose proofs clearly illustrate the use of the tools and deepen one's understanding.

Chapter 13

Applications

While difference sets are mathematically rich, they also have many applications to real-world problems. Indeed, the North Atlantic Treaty Organization sponsored an Advanced Study Institute on difference sets and sequences that brought together students and experts from electrical engineering, computer science and mathematics from many of the NATO countries to pursue some of them (see [**60**]). In this chapter we briefly describe a few of these applications and offer some suggestions for further reading. We are not experts in these engineering and science contexts, but we try to give the flavor of how difference sets are used for optical alignment, interpreting signals in the presence of noise, imaging astronomical events, constructing error-correcting codes, and facilitating processes in quantum informatics. The first three of these applications exploit the relationship between cyclic difference sets and binary sequences with good autocorrelation properties. The mathematical roles of the difference sets in the last two are quite different.

13.1. Binary sequences

A binary sequence of period v is a v-tuple $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ with the a_j either all chosen from $\{-1, +1\}$ or all chosen from $\{0, 1\}$.[1]

[1]The use of the word *period* is because $\mathbf{a}$ may be extended to an infinite periodic sequence by repeating the finite sequence.

For our first new application, imagine a source of signals, where each signal is binary sequence of period v with entries ± 1. Assume that these signals are transmitted over a channel corrupted by noise. The sender can transmit any one of N signals. When one is received, the receiver has to decide which of the N was sent. The receiver can do this by calculating the correlation between the received signal and ideal models of each of the possible transmitted signals and then choosing the one with the highest value of this correlation.[2]

Definition. Let $\mathbf{a} = (a_0, a_1, \ldots, a_{v-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{v-1})$ be two binary sequences of period v with either all of the a_j, b_j in $\{-1, +1\}$ or all in $\{0, 1\}$. Then the correlation $C(\mathbf{a}, \mathbf{b})$ is defined by

$$C(\mathbf{a}, \mathbf{b}) = \frac{1}{v} \sum_{j=0}^{v-1} a_j b_j.$$

For a_j, b_j in $\{-1, +1\}$, we have $C(\mathbf{a}, \mathbf{b}) = (A-D)/(A+D)$, where A is the number of positions in which $\mathbf{a}$ and $\mathbf{b}$ agree and D is the number of positions in which they disagree. In this case we observe the following nice analogies to the statistician's correlation defined for vectors in $\mathbb{R}^v$:

- For all $\mathbf{a}, \mathbf{b}$, we have $-1 \le C(\mathbf{a}, \mathbf{b}) \le 1$.
- If $\mathbf{a} = \mathbf{b}$, then $C(\mathbf{a}, \mathbf{b}) = 1$.
- If $\mathbf{a}$ and $\mathbf{b}$ disagree in every position, then $C(\mathbf{a}, \mathbf{b}) = -1$.
- If v is even and $\mathbf{a}$ and $\mathbf{b}$ agree in exactly half their positions, then $C(\mathbf{a}, \mathbf{b}) = 0$.

One way to define a binary sequence $\mathbf{a}$ is by specifying a difference set $D \subset \mathbb{Z}_v = \{0, 1, \ldots, v-1\}$ and choosing $a_j = +1$ if and only if j is in D. Then we can choose for the source signals $\mathbf{a} = (a_0, \ldots, a_{v-1})$ and the $v-1$ cyclic shifts of $\mathbf{a}$: $(a_t, a_{t+1}, \ldots, a_{t+v-1})$ for $t = 1, \ldots, v-1$, where the subscripts are interpreted modulo v. Since the v translates of D (the blocks of the associated design dev$D$) are all distinct, the cyclic shifts of $\mathbf{a}$ indeed give v distinct sequences. Difference sets give useful binary sequences for another reason too. To

[2] There is a theorem that states that if the noise is normally distributed, then this decision rule is optimal in some sense. It is a 1961 result of Fano—not the Fano of the Fano plane.

explain why, we introduce language and notation for the correlation between a sequence and its translate.

Definition. Let **a** be a binary sequence of period v. The periodic autocorrelation function of **a**, $C_{\mathbf{a}}(t)$ is given by

$$C_{\mathbf{a}}(t) = \frac{1}{v} \sum_{j=0}^{v-1} a_j a_{j+t} \,,$$

for $t = 0, \ldots, v-1$. The values of $C_{\mathbf{a}}(t)$ for $t \neq 0$ are called the *off-peak correlations.*

Example 1. Choose $\mathbf{a} = (-1, 1, 1, -1, 1, -1, -1)$. Then $C_{\mathbf{a}}(0) = (1/7)(\mathbf{a} \cdot \mathbf{a}) = (1/7)(7) = 1$ and $C_{\mathbf{a}}(1) = (1/7)(-1) = -1/7$. ◇

Example 2. Recall the alignment problem in Example 1.2. It implicitly involves the 0,1 version of the sequence in the preceding example, $\mathbf{a} = (0, 1, 1, 0, 1, 0, 0)$. When the light-emitting pattern surrounding the opening to the fuel tank and the light-transmitting pattern on the nozzle are perfectly aligned, the amount of light detected is essentially the value of the peak autocorrelation $C_{\mathbf{a}}(0)$. When the patterns are shifted out of alignment by 6 or fewer cells (in either direction), the amount of light detected is the off-peak autocorrelation $C_{\mathbf{a}}(t)$ for $t \neq 0$. (Look again at Figure 1.1 on page 3.) See Figure 13.1. ◇

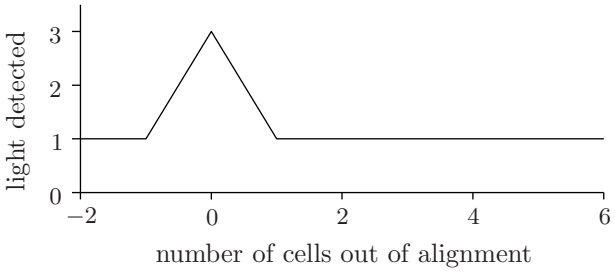


Figure 13.1. Light detected, Example 2

Return now to the communication example with which this section began. Shifted binary sequences are particularly useful as signal sources when the off-peak correlations are all equal and are as small

as possible in absolute value. The special usefulness of cyclic difference sets in this setting is a consequence of the following theorem (see Jungnickel and Pott, [**36**], p. 264). The proof is a nice review of some ideas in Section 4.2.

Theorem 13.1. *Choose integers $v \geq 2$ and k with $0 < k < v$. Let $\mathbf{a}$ be a binary sequence with period v, entries a_j in $\{-1, +1\}$, and having exactly k entries equal to $+1$. Suppose further that there are two numbers b and c with $C_{\mathbf{a}}(0) = b$ and $C_{\mathbf{a}}(t) = c$ for $0 < t < v$. Let $D = \{j \in \mathbb{Z}_v \,|\, a_j = +1\}$. Then D is a (v, k, λ)-difference set in $\mathbb{Z}_v$, $b = 1$ and $c = (v - 4n)/v$ for $n = k - \lambda$. Moreover, every cyclic difference set arises in this way.*

Theorem 13.1 also holds for $0, 1$ sequences, but in that case the values of b and c are different.

For ± 1 binary sequences, the off-peak correlations are all equal to 0 when we use a Hadamard difference set with $v = 4n$. However, no cyclic Hadamard difference sets are known for $v > 4$, and it is conjectured that none exist. The next smallest off-peak value in absolute value occurs for the Paley-Hadamard family with $v = 4n - 1$, and then the off-peak correlation is equal to $-1/v$. Cyclic difference sets in this family are abundant.

Binary sequences obtained from cyclic difference sets have some other nice properties too. Sequences coming from nonzero squares in $\mathbb{Z}_p$ for $p \equiv 3 \pmod 4$ have $(v-1)/2$ entries equal to $+1$ and $(v+1)/2$ entries equal to -1. This nearly equal balance of $+1$s and -1s makes them similar to *random sequences* (like a sequence of v coin tosses, with $+1$ for heads and -1 for tails). Another desirable property for a "pseudo-random" sequence is that knowing a subsequence gives little information about the entire sequence. In particular, if $v = 2^m - 1$, it is desirable if the $2^m - 1$ consecutive subsequences of length m are all distinct.

Example 3. Consider the difference set $\{1, 2, 4\} \subset \mathbb{Z}_7$. It yields the sequence $(- + + - + - -)$ of Example 1, where we write $+$ and $-$ instead of $+1$ and -1. The 7 subsequences of length 3 are:

$$- + +,\ + + -,\ + - +,\ - + -,\ + - -,\ - - -,\ - - + .$$

These triples are all distinct. ◇

Further reading

This section relies heavily on Golomb's "Signals with good correlation properties," in [**25**].[3] This paper has an extensive bibliography. You may also want to look at the paper [**48**] by MacWilliams and Sloane. They define *pseudo-random* sequences (also called *pseudo-noise* sequences) as binary sequences $\mathbf{a} = (a_0, \ldots, a_{v-1})$ of length $v = 2^m - 1$ with special properties, including the one they say is "most important": periodic autocorrelation function values equal to 1 at $t = 0$ and with off-peak value $-1/v$. (Although they use $1, 0$ sequences, they define the autocorrelation function for the corresponding sequence with jth entry $(-1)^{a_j}$; in other words, they convert to a ± 1 sequence for autocorrelation computations.) Some of the other properties on their defining list also seem to hold for more general cyclic Paley-Hadamard difference sets. The applications they mention are "range-finding, scrambling, fault detection, modulation, synchronizing, etc.", and they give many references.

13.2. Imaging with coded masks

Astronomers study high-energy radiation such as X-rays and gamma rays with instruments mounted on satellites, to avoid blocking of the radiation by the earth's atmosphere. According to NASA's Goddard Space Flight Center, gamma ray bursts are the most powerful explosions our Universe has experienced since the Big Bang. They occur very briefly but almost daily. So far, scientists don't know what causes them and what they mean. Are they evidence of the birth of a black hole? The product of the collision of two neutron stars? The space observatory SWIFT, developed by NASA along with an international consortium, was launched in 2004 to study gamma ray bursts with a precision never available before. Among the instruments on the orbiting SWIFT spacecraft was one using a "coded mask". (See [**64**].)

Astronomers cannot rely on ordinary lenses to focus high energy radiation and produce images of distant objects. Instead, they use

[3] Golomb was awarded the 2012 National Medal of Honor in recognition of his contributions to mathematics and engineering, particularly in interplanetary communication.

a process similar to the way medical images are obtained from X-rays, where the patient is positioned between a source of radiation and a detector sensitive to the radiation. Parts of the body that absorb X-rays cast shadows on the detector, and radiologists interpret this shadow image to draw inferences about the patient's body. For astronomical investigations, the idea is to put a "mask" that absorbs the radiation between the source and the detector. Then a computer uses the information on the detector to reconstruct an image of the source.

The simplest mask has a single hole, like a pin-hole camera. The result is an inverted image of the source. The smaller the hole is, the sharper the resulting image will be. However, if the hole is very small, only a few high energy rays would pass through. Even worse, the number of rays from the distant source that pass through the hole would be small compared to the background "noise" produced by cosmic rays. In the language of science and engineering, the *signal to noise ratio* (SNR) is too low. Therefore a mask with a single hole is not workable.

The obvious solution is to use a mask with multiple holes, but now we have another problem. Each hole produces its own image, so we have multiple overlapping images projected onto the detector. The task is to position the holes in the mask—to code them—so that it is possible to recover a single clear image of the source from these multiple images on the detector. Since noise is a factor, the computer algorithm to reconstruct the location and intensity of each source in the field of view is in part statistical. Figure 13.2 schematically illustrates what is involved in the use of a coded mask instrument for a single source of high energy radiation.

So, what is a *good* coded mask? One important consideration is that we want the shadow cast by the mask to be a poor match to any shifted version of itself. This sounds familiar. We want the coded mask to have a pattern of holes that has low correlation with shifted versions of itself. As in Section 1, we can use a cyclic difference set.

But how do we change from a sequence of holes in a line to a rectangular array of holes and still retain the desired autocorrelation

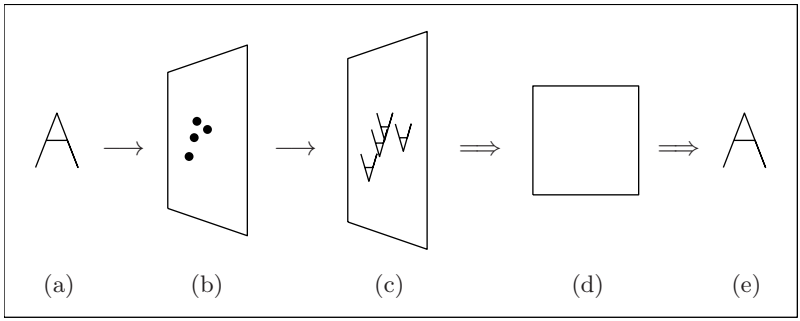


Figure 13.2. Schematic for imaging using a coded mask: (a) source image, (b) mask (dots represent holes), (c) detector, (d) computer to reconstruct source image, (e) reconstructed source image

property? One method is to use a twin primes difference set in $\mathbb{Z}_p \oplus \mathbb{Z}_{p+2}$. We illustrate with the next example for $p = 3$.

Example 4. Arrange the elements of $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ in a rectangular array, with the rows indexed by elements of $\mathbb{Z}_3$ and the columns indexed by elements of $\mathbb{Z}_5$. (See Figure 13.3, where the elements not in the difference set are shaded.) Notice that cyclically shifting the array horizontally by one cell is the same as adding $(1, 0)$ to each element, and shifting vertically by one is the same as adding $(0, 1)$. Thus we retain the desirable autocorrelation property. ◇

0, 0	0, 1	0, 2	0, 3	0, 4
1, 0	1, 1	1, 2	1, 3	1, 4
2, 0	2, 1	2, 2	2, 3	2, 4

Figure 13.3. The rectangular array for the $(15, 7, 3)$-difference set

Of course, the coded mask for $p = 3$ is much too small to be useful. Figure 13.4 shows a somewhat more realistic coded mask based

on the twin primes difference set with $p = 41$. In the mid 1990s, an Italian institute for space research in collaboration with the Russian Academy of Sciences developed a high-energy coded aperture telescope based on a twin primes difference set with $p = 71$ for an international high-energy astrophysics observatory—still in the planning stages—to be launched into space with a Soyuz rocket.

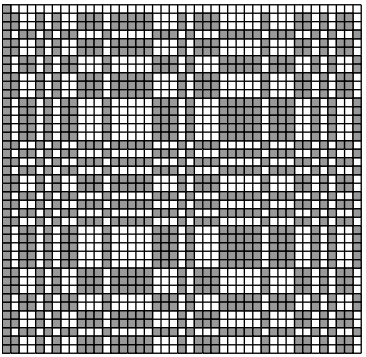


Figure 13.4. Mask for X-rays, based on twin primes (41,43)

The satellite INTEGRAL was launched in 2003 by a consortium of many nations. One of its missions was to carry out a 9-year survey of our galaxy, which it completed in December 2012. INTEGRAL was equipped with multiple imaging instruments that use coded masks, notably a gamma-ray imaging telescope called IBIS with a rectangular mask.

Further reading

The Skinner article [**63**] is useful and has some nice illustrations. Another, more up to date, general resource is the Goddard Space Center website "Coded Aperture Imaging in High Energy Astronomy" at website (1) listed on the following page. See especially the link "Coded aperture imaging: a short review." The link "A selection of coded aperture instruments" gives a list of actual coded aperture instruments.

A reference for the SWIFT project is website (2). You can read about the Italian/Russian project using the twin prime difference set

with $p = 71$ on the website of the SRON Netherlands Institute for Space Research on website (3). Some spectacular images obtained by the INTEGRAL's 9-year galactic survey can be found at website (4). An extensive bibliography for papers on coded aperature imaging is available at website (5).

Websites:

(1) `astrophysics.gsfc.nasa.gov/cai/`

(2) `heasarc.gsfc.nasa.gov/docs/swift/swiftsc.html`

(3) `www.sron.nl/~jeanz/cai/coded_mart.html`

(4) `hea.iki.rssi.ru/integral/nine-years-galactic-survey/index.php`

(5) `www.sron.nl/~jeanz/cai/coded_bibl_short.html`

13.3. Error correcting codes

You may have encountered error correcting codes in your study of linear algebra or abstract algebra. A linear error correcting code is a subspace C of a v-dimensional vector space V over a finite field $\mathbb{F}$. Typically, the field is $\mathbb{F} = GF(2)$, so the vectors in V are strings of length v consisting of the "bits" 0 and 1. The vectors in C are the code words. If the dimension of C is k, we regard each codeword as having k bits of information. We can think of the embedding of $C \simeq \mathbb{F}^k$ in $V \simeq \mathbb{F}^v$ as "smearing out" the information bits to protect them. More specifically, the $v - k$ additional bits when we regard a codeword as an element of V are the redundancy added to the original information. If the redundancy is added cleverly, the receiver of the information can detect and correct some number of errors.

For a vector $\mathbf{v}$ in V, the weight of $\mathbf{v}$ is the number of nonzero entries in $\mathbf{v}$. If the minimum weight of a nonzero vector in C is d, then the code can correct $\lfloor (d-1)/2 \rfloor$ errors. The amount of information that can be encoded depends on the dimension k of C. The code parameters v, k and d are thus key.

There are many deep connections between coding theory and design theory, with theoretical and practical links in both directions,

but here we focus on the connection between linear codes and designs arising from abelian difference sets.

The easiest way to associate a linear code with a design $\mathcal{D}$ is via the incidence matrix of $\mathcal{D}$. Since the entries of the incidence matrix A make sense in any field, we may choose any field $\mathbb{F}$ and then define the code as the $\mathbb{F}$-space spanned by the rows of A. In general, it is difficult to determine the minimum weight of such codes, but it is possible to determine their dimension.

An important family of codes is associated in this way with the Paley difference sets in $GF(q)$ for q a prime, $q \equiv 3 \pmod 4$. If we choose a field $\mathbb{F} = GF(p)$ for which p is a quadratic residue in $GF(q)$, then the difference set determines a design whose corresponding code is called a *quadratic-residue code*. These codes have dimension $(q \pm 1)/2$ and are related to an important family of codes called *Reed-Muller codes*. (See Assmus and Key [**4**], Sections 2.10 and 7.8.) For example, we have the following theorem.

Theorem 13.2. *(MacWilliams and Mann, 1968). The code generated by the Paley difference set in $GF(q)$ for $q \equiv 3$ (mod 4) has dimension $(q+1)/2$ if the characteristic of $\mathbb{F}$ is a prime divisor of $(q+1)/4$.*

Example 5. Choose the $(7, 3, 1)$-difference set in $GF(7)$ and choose $\mathbb{F} = GF(2)$. Then the characteristic of $\mathbb{F}$ is 2, which is a divisor of $(7+1)/4$, so the corresponding code has dimension 4. It turns out that it is the smallest Hamming code, which is known to have minimum distance 3 and so corrects a single error. ◇

In [**43**] Lander discusses codes defined by an abelian (v, k, λ)-difference set $D \subset G$ somewhat differently. He identifies the elements of the group ring $\mathbb{F}G$ with the vectors in $V = (\mathbb{F})^v$. He defines the code C as the ideal of the ring $\mathbb{F}G$ generated by the element $D = \sum_{d \in D} d \in \mathbb{F}G$. His definition is actually equivalent to the definition of the code as the row space of the incidence matrix of dev$D$, but his approach leads to the use of somewhat different algebraic tools.

Further reading

For more on difference sets and codes, see the books by Pott ([**59**]) and Lander ([**43**]). For more on designs and codes, see the volumes by Beth, Jungnickel and Lenz ([**8**]) or E.F. Assmus and J.D. Key ([**4**]). Another useful reference on designs and codes that is aimed more at undergraduates is P.J. Cameron and J.H. vanLint ([**12**]).

13.4. Quantum information and MUBs

In this section we use a generalization of a difference set to construct mutually unbiased bases (MUBs for short). What are MUBs?

Definition. Let $\mathbb{C}^N$ be an inner product space with the standard inner product, and let $\{\mathbf{u}_j \,|\, j = 1, \ldots, N\}$ and $\{\mathbf{v}_j \,|\, j = 1, \ldots, N\}$ be two orthonormal bases of this space. These bases are said to be mutually unbiased if there is a constant c such that for all $j, k = 1, \ldots, N$,

$$|\langle \mathbf{u}_j, \mathbf{v}_k \rangle|^2 = c.$$

Example 6. Here are three MUBs for $N = 2$, where $\mathbf{e}_1$ and $\mathbf{e}_2$ denote the standard basis for $\mathbb{C}^2$.

$$\begin{aligned} M_1 &= \{\mathbf{e}_1, \mathbf{e}_2\} \\ M_2 &= \{(\mathbf{e}_1 - \mathbf{e}_2)/\sqrt{2}, (\mathbf{e}_1 + \mathbf{e}_2)/\sqrt{2}\} \\ M_3 &= \{(\mathbf{e}_1 - i\,\mathbf{e}_2)/\sqrt{2},\ (\mathbf{e}_1 + i\,\mathbf{e}_2)/\sqrt{2}\}. \end{aligned}$$ ◇

It is a theorem that at most $N+1$ MUBs can exist for $\mathbb{C}^N$. When N is a power of a prime, $N + 1$ MUBs do exist. Thus $N + 1 = 3$ is the maximum number of MUBs possible for $\mathbb{C}^2$. It is known that 3 MUBs exist for $\mathbb{C}^6$, but it is unknown whether more than 3 exist.

MUBs are rich in mathematical connections, but here we very briefly describe their link to quantum mechanics. Mathematically, states of a quantum system are identified with unit vectors in a complex inner product space. For example, in quantum computation, the analog of a classical "bit" is a "qubit", a 2-state quantum system with states given by unit vectors in $\mathbb{C}^2$. A larger system might consist of m qubits. The states of this bigger system are represented by unit vectors in $\mathbb{C}^{2^m}$.

More generally, we might have a system with states corresponding to unit vectors in $\mathbb{C}^N$ for some N. A measurement of the system is represented by an operator A with the property that an orthonormal basis for $\mathbb{C}^N$ can be chosen from among its eigenvectors. Then $A = \sum a_{\mathbf{v}} P_{\mathbf{v}}$, where $\mathbf{v}$ ranges over this basis of eigenvectors and $P_{\mathbf{v}}$ is the projection onto the subspace spanned by $\mathbf{v}$. We call this basis of eigenvectors the *measurement basis*. If we carry out this measurement for a system in a state represented by an arbitrary unit vector $\mathbf{w}$, then the result of our measurement is equal to the eigenvalue $a_{\mathbf{v}}$ with probability $|\langle \mathbf{w}, \mathbf{v} \rangle|^2$.

Example 7. Suppose we want to measure a polarized photon; its state corresponds to a unit vector $\mathbf{w}$ in $\mathbb{C}^2$. We make a measurement with a vertically polarized filter. The measurement is represented by $A = 0P_{\mathbf{e}_1} + 1P_{\mathbf{e}_2}$, so the measurement basis is the standard basis of $\mathbb{C}^2$. If the photon is itself polarized vertically, its state is $\mathbf{w} = \mathbf{e}_2$, and the measurement gives the result 1 with probability equal to 1. On the other hand, if the photon is polarized horizontally, its state is $\mathbf{w} = \mathbf{e}_1$, and the measurement gives the result 0 with probability equal to 1. Results are more interesting if the photon is polarized neither vertically nor horizontally. For example, suppose its state is $\mathbf{w} = (1/\sqrt{2})\mathbf{e}_1 + (1/\sqrt{2})\mathbf{e}_2$. In this case, the result of the measurement can vary; with probability 1/2 it gives the result 0, and with probability 1/2 it gives the result 1. ◇

We say two measurements are *mutually unbiased* if their measurement bases are MUBs. In this case, the result of doing one measurement gives no information about the result of the other measurement. Under certain circumstances, a set of $N + 1$ mutually unbiased measurements provides the optimal determination of an unknown state.[4]

MUBs are used in quantum-informatics applications, including "dense coding, teleportation, entanglement swapping, covariant cloning, and state tomography," quoting from [**21**]. Applications are numerous whenever maximal sets of MUBs are available, in particular when the physical system is composed of many qubits ($N = 2^m$), the building blocks of devices for quantum information processing.

[4]Most of this description is drawn from [**71**].

Now we define the generalization of a difference set that we need for the construction of MUBs.

Definition. Let G be a group and U a normal subgroup of G. Then the nonempty proper subset $D \subset G$ is a relative difference set (with respect to U) if the multiset of differences of distinct elements of D represents every element of $G \setminus U$ exactly λ times and represents elements of U zero times. Equivalently,

$$DD^{(-1)} = |D|1_G + \lambda(G - U)$$

in the integral group ring $\mathbb{Z}G$. Let $k = |D|$, $u = |U|$, and $s = |G/U|$, so $|G| = su$. Then D is an (s, u, k, λ)-relative difference set. It is a semi-regular relative difference set if $s = k$.

Counting differences of distinct elements of an (s, u, k, λ)-relative difference set D gives us $k(k-1) = \lambda(su - u)$. In the case of a semi-regular relative difference set, this says $k = \lambda u$.

Example 8. Let $G = \langle x, y \,|\, x^4 = y^4 = 1, xy = yx \rangle$, and let $U = \langle x^2, y^2 \rangle$. Then $D = \{1, y, x, x^3y^3\}$ is a semi-regular $(4, 4, 4, 1)$-relative difference set with respect to U. $\diamond$

The main result of this section is the following theorem of Godsil and Roy.

Theorem 13.3. *The existence of a semi-regular (k, u, k, λ)-relative difference set in an abelian group G implies the existence of a set of $u + 1$ mutually unbiased bases of $\mathbb{C}^k$.*

Notice that in the special case when $\lambda = 1$, this theorem guarantees the existence of a maximal number of MUBs: $k + 1$ MUBs for $\mathbb{C}^k$.

The proof of this theorem is accessible to a reader of this book. Here is a sketch. Let $D = \{d_1, \ldots, d_k\}$ be the semi-regular relative difference set of the theorem. Let G^* be the group of complex-valued characters of G, and for each $\chi \in G^*$, define a vector

$$(\chi(d_1), \ldots, \chi(d_k)) \in \mathbb{C}^k.$$

It can be shown that we can arrange these $|G| = ku$ vectors in u sets of k vectors each, and these sets give u MUBs for $\mathbb{C}^k$. These u

bases turn out to be unbiased with respect to the standard basis also, producing a total of $u + 1$ MUBs.

The proof requires the following observations about the group G^* from Exercise 11.14. The groups G and G^* are isomorphic, and we can use this isomorphism to label the elements of G^* by elements of G. Using this labeling, in the group G^* we have $(\chi_a)^{-1} = \chi_{a^{-1}}$ and $\chi_a\chi_b = \chi_{ab}$ for $a, b \in G$.

Now we can link the relative difference set to the inner product in $\mathbb{C}^k$. Let $\mathbf{x}_a, \mathbf{x}_b \in \mathbb{C}^k$ be determined by $\chi_a, \chi_b \in G^*$. Then we calculate:

$$\begin{aligned}\langle \mathbf{x}_a, \mathbf{x}_b \rangle &= \sum_{d\in D} \chi_a(d)\overline{\chi_b(d)} \\ &= \sum_{d\in D} \chi_a(d)(\chi_b(d))^{-1} \\ &= \sum_{d\in D} \chi_a(d)\chi_{b^{-1}}(d) \\ &= \sum_{d\in D} \chi_{ab^{-1}}(d) = \chi_{ab^{-1}}(D).\end{aligned}$$

Thus $|\langle \mathbf{x}_a, \mathbf{x}_b \rangle|^2$ is constant for all $a \neq b$.

Further reading

The main source for the mathematics in this section is Godsil and Roy's paper [**24**].[5] It also contains a theorem linking the existence of "equiangular lines" to the existence of a difference set, and the proof of this theorem is a nice application of the methods included in this book.

For further reading on the mathematics of MUBs, see [**39**]. For more on relative difference sets see [**8**], pages 369 and following. For a mathematical introduction to error correction in quantum computing, see [**58**].

[5] It is also available at `arXiv.org`. (In the seach box enter: godsil roy.)

Appendix A

Background

Linear Algebra

A.1. Let $M \in \mathcal{M}(m, \mathbb{C})$. The trace of M, denoted $\mathrm{Tr}(M)$, is the sum of the diagonal elements of M. Also, $\mathrm{Tr}(PMP^{-1}) = \mathrm{Tr}(M)$ for any $P \in GL(m, \mathbb{C})$. If $V = \mathbb{C}^m$ and T is a linear transformation of V with matrix M with respect to some basis of V, then by definition $\mathrm{Tr}(T)$ is equal to $\mathrm{Tr}(M)$, and this is well-defined.

A.2. If M is a square matrix over $\mathbb{C}$, then $\mathrm{Tr}(M)$ is the sum of the eigenvalues of M.

Proof. Look at the coefficient of the λ^{n-1} term of the characteristic polynomial. On the one hand, the characteristic polynomial factors completely into linear terms with λ_i the (not necessarily distinct) eigenvalues for A

$$p(\lambda) \;=\; (\lambda_1 - \lambda)(\lambda_2 - \lambda)\cdots(\lambda_n - \lambda)$$

and the coefficient of λ^{n-1} is $(-1)^{n-1}(\lambda_1 + \lambda_2 + \cdots + \lambda_n)$.

On the other hand, when we calculate the characteristic polynomial from the determinant of $M - \lambda I$, the only terms with degree $n-1$ come from the product of the diagonal elements:

$$p(\lambda) \;=\; (m_{11} - \lambda)(m_{22} - \lambda)\cdots(m_{nn} - \lambda) \;+\; \text{lower degree terms}$$

and the coefficient of λ^{n-1} is $(-1)^{n-1}(m_{11}+m_{22}+\cdots+m_{nn})$. Equating these coefficients gives us our result. □

A.3. Let V be a vector space of dimension d over the field $\mathbb{F}$. A hyperplane is a subspace of dimension $d-1$. The span of any two hyperplanes is all of V. The intersection of any two hyperplanes is a subspace of dimension $d-2$. ([**3**], p. 103)

A.4. Let V be an d-dimensional vector space over a field $\mathbb{F}$. There is a 1-1 correspondence between the subspaces of V of dimension $d-1$ and the subspaces of V of dimension 1. When $\mathbb{F}$ is a finite field, this can be proved by counting, as in the proof given of Theorem 2.16. If there is a non-degenerate inner product on V, this can be proved by considering the correspondence between a subspace W and the subspace $W^{\perp}$ of vectors orthogonal to W. The most general argument avoids either of these special cases, using instead the dual space V^* of linear functionals on V and the notion of the annihilator of either a subspace of V or of V^*. ([**30**], Section 17)

A.5. Let V be a finite dimensional vector space over $\mathbb{R}$ with the standard dot product. Then V has an orthonormal basis, and this basis can be obtained from an arbitrary basis by the Gram Schmidt process. ([**22**], p. 342)

Groups

Note: All groups referred to here are finite.

A.6. Let G be a cyclic group. For every divisor of the order of G, there is a unique subgroup of that order. ([**23**], p. 78)

A.7. Structure Theorem: Every abelian group is the direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group. ([**23**], p. 217)

A.8. The exponent of a finite group G, denoted $\exp(G)$, is the least common multiple of the orders of the elements of G.

A.9. The centralizer of element a in a group G is the set of elements of G that commute with a,

$$C_G(a) \quad = \quad \{g \in G \mid ag = ga\}.$$

A.10. Let G be a group and write $Cl(a)$ for the conjugacy class of $a \in G$,

$$Cl(a) = \{gag^{-1} \mid g \in G\}.$$

Then

$$|G| = \sum |Cl(a)| = \sum [G : C_G(a)],$$

where the sum contains one term for each conjugacy class of G. ([**23**], p. 402)

A.11. If G is a group of order p^2 for p a prime, then G is abelian. ([**23**], p. 403)

A.12. Let G be a group. The commutator subgroup of G is the group generated by all elements of the form $xyx^{-1}y^{-1}$ for $x, y \in G$. Such elements are called commutators.

A.13. Let G be a finite group of order m and let p be a prime that divides m. If $p^j | m$ and p^{j+1} does not divide m, then any subgroup of G of order p^j is a Sylow p-subgroup of G.

A.14. The Sylow theorems. ([**23**], pp. 405–407)

(1) Let G be a finite group and let p be a prime. If p^j divides $|G|$, then G has at least one subgroup of order p^j.

(2) If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.

(3) The number of Sylow p-subgroups of G is congruent to 1 mod p and divides $|G|$. Further, any two Sylow p-subgroups of G are conjugate.

Fields

A.15. Let $z \in \mathbb{C}$. If $z^m = 1$ for some integer m, then z is an mth root of unity. If z has multiplicative order m, we say z is a primitive mth root of unity . If z is an mth root of unity then $|z| = 1$, and $z = e^{(i\theta)k}$ for some $k = 0, \ldots, m-1$, where $\theta = 2\pi/m$ and $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. ([**23**], p. 46)

Note that $\overline{z} = z^{-1}$ in this case. If z is an mth root of unity for $m > 1$, then $1 + z + z^2 + \cdots + z^{m-1} = (z^m - 1)/(z - 1) = 0$.

A.16. The group of nonzero elements of a finite field $\mathbb{F}$ is a group under multiplication. This group is known as the group of units of $\mathbb{F}$ and is denoted $\mathbb{F}^*$. If $\mathbb{F}$ is finite, the group $\mathbb{F}^*$ is cyclic. ([**23**], p. 383)

A.17. Let q be an odd prime power and let $GF(q)$ be the finite field of order q. Then -1 is a square in $GF(q)$ if and only if $q \equiv 1 \pmod 4$. (There is a group-theoretic proof using the fact that -1 is a square if and only if the multiplicative group $GF(q)^*$ contains an element of order 4.) ([**20**], p. 54)

A.18. Let q be a power of a prime, and let $\mathbb{F}_q = GF(q)$. To construct a field of order q^m, we begin with the ring of polynomials in x over $\mathbb{F}_q$, find a polynomial $p(x)$ of degree m that is irreducible in this ring, and form the quotient field of the ring modulo the ideal generated by $p(x)$:

$$GF(q^m) \quad = \quad \mathbb{F}_q[x]/\langle p(x)\rangle.$$

Further it is possible to select $p(x)$ so that the element $x + < p(x) >$ generates the group of units of $GF(q^m)$. For a specific example see Exercise 4.12. ([**23**], p. 383, Corollary 2)

A.19. Let $\mathbb{F}$ be a finite field of order q and let r be a divisor of q. Then $\{a \in \mathbb{F} \,|\, a^r = a\}$ is the unique subfield of $\mathbb{F}$ of order r. ([**33**], p. 327)

Miscellaneous

A.20. The principle of inclusion/exclusion: Let $\mathcal{U}$ be a finite set and let A and B be subsets of $\mathcal{U}$. Then

$$|\mathcal{U} \setminus (A \cup B)| \quad = \quad |\mathcal{U}| - |A| - |B| + |A \cap B|.$$

More generally, let $\mathcal{U}$ be a finite set and let $\{A_j\}$ be a collection of m subsets of $\mathcal{U}$. Let S_t be the sum of sizes of the intersections of t of the A_j, taken over all t-sets of the A_j. Then

$$\Big|\mathcal{U} \setminus \bigcup_j A_j\Big| \quad = \quad |\mathcal{U}| - S_1 + S_2 - \cdots (-1)^m S_m.$$

Further, if for each t the size of the intersection of any t of the subsets A_j is the same, say s_t, then

$$S_t = s_t \binom{m}{t}.$$

So

$$\Big|\mathcal{U} \setminus \bigcup_j A_j\Big| = |\mathcal{U}| - s_1 \binom{m}{1} + s_2 \binom{m}{2} - \cdots (-1)^m s_m \binom{m}{m}.$$

([**68**], p. 323)

A.21. Let $x, y \in \mathbb{Z}$ and p a prime integer. Then $(x+y)^p \equiv x^p + y^p \bmod p$. The proof depends on the binomial theorem and the fact that for $1 \le k \le p-1$, the numerator of

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

is divisible by p, while the denominator is not.

Appendix B

Notation

Misc.

$\mathbb{Z}$	integers
$\mathbb{R}$	real numbers
$\mathbb{Q}$	rational numbers
$\mathbb{C}$	complex numbers
$G \setminus D$	set subtraction, p. 15
$\emptyset$	empty set, p. 20
$\overline{S}$	complement of set S
$\lvert S \rvert$	cardinality of set S

Matrices and Linear Transformations

I	identity matrix
I_m	$m \times m$ identity matrix
J	square matrix of all 1s, p. 19
A^T	transpose of matrix A, p. 13
$A \otimes B$	Kronecker product, p. 137
$GL(m, \mathbb{K})$	invertible $m \times m$ matrices over field $\mathbb{K}$, p. 155
$GL(V)$	invertible linear transformations on V, p. 168
$\text{span}\{v_1, \ldots, v_t\}$	vector space spanned by vectors, p. 170
$\mathcal{M}(m, \mathbb{C})$	$m \times m$ matrices with entries in $\mathbb{C}$, p. 192
$\text{Ker}(\tau)$	Kernel of τ
$\text{Im}(\tau)$	Image of τ

Groups, Rings, Fields

$\mathbb{Z}_m$	group of integers mod m (sometimes ring)
$\mathbb{F}_p$, $\mathbb{Z}_p$	field of p elements, p a prime
$\mathbb{K}$	field
$\mathbb{F}$	field, usually finite
$GF(q)$	field of order q (Galois field), p. 24
$\mathbb{K}^*$	multiplicative group of nonzero elements of $\mathbb{K}$
$\pi_g(x)$	group action of g on x, p. 38
$\mathrm{orb}_G(x)$	orbit of x under G, p. 38
$\mathrm{stab}_G(x)$	stabilizer in G of x, p. 38
$\mathrm{Fix}(g)$	set of elements of X fixed by g, p. 40
$C_G(a)$	centralizer in G of a; $\{g \in G \mid ga = ag\}$, p. 40
D_m	dihedral group of order $2m$, p. 48
$G \oplus H$	direct sum of groups, $\{(a, b) \mid a \in G,\ b \in H\}$, p. 48
$G \times H$	direct product of groups, p. 48
$\langle g \rangle$	group generated by g
$\langle S \mid R \rangle$	group presentation; S is set of generators, R is set of relations, p. 48
$\mathbb{Z}G$	integral group ring, p. 59 Elements are of the form $\sum_{g\in G} a_g g,\ a_g \in \mathbb{Z}$
$S^{(t)}$	$\sum_{s\in S} s^t$ in integral group ring, p. 60
$\widehat{\varphi}$	ring homomorphism $\mathbb{Z}G \to \mathbb{Z}H$ induced by $\varphi : G \to H$, p. 107
$\exp(G)$	exponent of group G, p. 113
S_m	symmetric group on set $X = \{1, 2, \ldots, m\}$, p. 168

Designs

$\mathcal{D}$	design, (often symmetric design), p. 26
$\mathcal{P}$	set of points in a design, p. 26
$\mathcal{B}$	set of blocks in a design, p. 26
$\mathcal{I}$	incidence relation, p. 9
v	number of points in a symmetric design, p. 16
b	number of blocks, p. 16
k	number of points per block, p. 16
r	number of blocks per point, p. 16
λ	number of elements two blocks have in common, p. 16
n	$k - \lambda$, order of a symmetric design, p. 26
t-(v, k, λ)	parameters for a t-design, p. 14
(v, k, λ)	parameters for a symmetric design, p. 26
$\overline{\mathcal{D}}$	complement design, p. 17
s-set	set containing s points, p. 14
λ_s	number of blocks containing an s-set, p. 16
λ^s	number of blocks disjoint from an s-set, p. 17

Difference sets

D	difference set, p. 46
$\overline{D}$	complement difference set, p. 60
v	order of group, p. 47
k	number of elements in a difference set, p. 47
λ	number of ways a non-identity element is represented as a difference, p. 47
n	$k - \lambda$, order of a difference set, p. 47
(v, k, λ)	parameters for difference set, p. 47
Δ	multiset of non-identity differences, p. 46
dev$D$	development of a difference set, p. 54
$D^{(-1)}$	$\sum_{d \in D} d^{-1}$ in integral group ring, p. 60
ϕ_t	numerical multiplier, p. 89

Geometry

$\mathcal{P}$	set of points
$\mathcal{L}$	set of lines
ℓ	line
$\ell(A, B)$	line through points A and B
$AG(m, \mathbb{F})$	coordinatized affine m-space over $\mathbb{F}$, p. 23
$AG(m, q)$	coordinatized affine m-space over $GF(q)$, p. 23
$PG(m, \mathbb{F})$	coordinatized projective m-space over $\mathbb{F}$, p. 31
$PG(m, q)$	coordinatized projective m-space over $GF(q)$, p. 31

Number Theory

p	usually a prime integer
q	usually a prime power
$\binom{k}{t}$	binomial coefficient, p. 16
$\mathrm{ord}_p n$	highest power of p that divides n
$\gcd(a, b)$	the greatest common divisor of a and b, p. 54
$\gcd(a, b) = 1$	a and b are relatively prime, p. 54
$a \, R \, b$	a is a square mod $\lvert b \rvert$ (Legendre), p. 73
$\chi(a)$	quadratic character, p. 146
$\mathbb{Z}[i]$	Gaussian integers, p. 194
$\mathbb{Z}[\omega]$	cyclotomic integers, p. 236

Representations and Characters

$V_1 \oplus V_2$	direct sum of vector spaces, p. 180
$\rho_1 \oplus \rho_2$	direct sum of representations, p. 181
ρ	group representation, p. 168
$\widetilde{\rho}$	ring homomorphism $\mathbb{Z} \to \mathcal{M}(m, \mathbb{C})$ induced by $\rho : G \to GL(m, \mathbb{C})$, p. 192
ρ_{reg}	(left) regular representation, p. 175
$\langle \ , \ \rangle$	complex inner product, p. 183
$\ll , \gg$	constructed inner product, p. 186
χ	group character, p. 198
χ_{reg}	regular character, p. 199
$\mathcal{V}$	vector space of complex-valued class functions, p. 202

Appendix C

Hints and Solutions to Selected Exercises

Chapter 2. Designs

2.1(a). The permutation matrix is: $P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. Ⓢ

2.5. Blocks with the three edges of a triangle can be counted by choosing 3 of the 6 vertices, for a total of $\binom{6}{3} = 20$. Blocks with the three edges of a perfect matching can be found by choosing pairs of points for the first, second, and third edges, and then dividing by 3! since the order of the edges does not count. The number of these blocks is $\binom{6}{2}\binom{4}{2}\binom{2}{2}/3! = 15$. This is a 2-design with parameters: 2-$(15, 3, 1)$; $b = 20 + 15 = 35$; $r = 7$. Using Theorem 2.1: $b = \lambda\binom{v}{t}/\binom{k}{t} = 1 \cdot \binom{15}{2}/\binom{3}{2} = 35$. Ⓢ

2.13. Find two ways to count the number of ordered pairs (B, T) with B a block and T a t-set with $T \subseteq B$. Ⓗ

2.17(c) There are 12 lines and 3 points per line. The order $n = 3$. The parameters as a 2-design are 2-$(9, 3, 1)$, with $r = 4$ and $b = 12$. Ⓢ

2.24. We explain the value of λ. Consider any two blocks T_i and T_j. If squares i and j are in the same row but different columns, the blocks intersect in the two squares in this row that are not squares i and j. A similar argument holds for two blocks whose defining squares are in the same column. Otherwise squares i and j are in different rows and different columns. Thus they are at diagonally opposite points of a rectangle, and blocks T_i and T_j intersect at the other two corners of this rectangle. So $\lambda = 2$. Ⓢ

2.32(b). Show that A commutes with A^T. Ⓗ

2.36(a). The line through points [0,1,3] and [2,1,1] is [1,2,1]. Ⓢ

Chapter 3. Automorphisms

3.2. Write $G = \langle a, b \mid a^4 = b^2 = 1, ba = a^3b\rangle$. Then the G-orbits are: $\{1\},\ \{a, a^3\},\ \{a^2\},\ \{b, a^2b\},\ \{ab, a^3b\}$. Ⓢ

3.4. Set up a correspondence between left cosets of G_x in G and elements of $\mathrm{orb}_G(x)$. Ⓗ

3.7. The permutation of points is $(0)(2)(6)(35)(14)$. The permutation of lines is $(\ell_1)(\ell_2)(\ell_6)(\ell_3\ell_5)(\ell_0\ell_4)$. Notice that their cycle structures are the same. Ⓢ

3.8. An automorphism does not have to preserve our drawing of the Fano plane. It must simply be a permutation of points that preserves the set of blocks. Consider the group of 3×3 invertible matrices with entries in $\mathbb{Z}_2$ acting on $(\mathbb{Z}_2)^3$. Ⓗ

Chapter 4. Difference Sets

4.3(a). The proof that $\lambda(v-1) = k(k-1)$ is in Chapter 1. Solving $\lambda(v-1) = k(k-1)$ for λv gives $\lambda v = k^2 - (k-\lambda) = k^2 - n$. Ⓢ

4.3(d). For the case $k < v/2$, show $n < (v/2)(k - 2\lambda)$ and use $n > 0$. Ⓗ

4.8. $ba = a^jb \Leftrightarrow bab^{-1} = a^j$; that is, conjugation by b takes a to a^j. Ⓗ

4.19(e). $D = \{g \in G \mid g(1) \in B_0\} = \{\alpha, \alpha^2, \alpha^3, \beta, \beta^2, \beta^3\}$. Ⓢ

4.23(a). Since $g \mapsto sg$ and $g \mapsto gs$ are permutations of G, we have $sG = G = Gs$, and therefore $SG = \sum_s sG = |S|G = \sum_s Gs = GS$. Ⓢ

4.28. $\mathbb{Q}G$ is a vector space over $\mathbb{Q}$. Ⓗ

4.32. Use the ring homomorphism of $\mathbb{Z}[x]$ taking $\sum_g a_g x^g$ to $\sum a_g$. Ⓗ

4.33. Use induction on the number of nonzero coefficients of S. See A.21 for $(x+y)^p \pmod p$. Ⓗ

4.34. Choose $q = p^e > m$ and consider A^q. Ⓗ

4.35. Suppose v is odd and get a contradiction. Ⓗ

4.38(c). The automorphisms φ_a for $a = 1, 2, 4$ fix D, and for $a = 3, 5, 6$, $\varphi_a(D) = \{3, 5, 6\}$. The seven translates of $\{3, 5, 6\}$ are distinct from the seven translates of D, so there are a total of 14 difference sets equivalent to D. Ⓢ

4.40. Imitate the strategy in Example 8. Ⓗ

4.43. Without loss of generality, assume the difference set contains 0. Show that it must contain a set of generators of G. Ⓗ

Chapter 5. BRC

5.1(b). $x^2 = 10y^2 - 2z^2$ has no solution since $-2 \equiv 8 \pmod{10}$ is not a square. Ⓢ

5.4. Look at the determinant of the incidence matrix. See Exercise 2.31. Ⓗ

5.10. Since $A \equiv a$, there is an integer t_1 so that $A = a + t_1 m$. Similarly we write $B = b + t_2 m$, $C = c + t_3 m$, $D = d + t_4 m$. Then $aA+bB+cC+dD = a(a+t_1 m)+b(b+t_2 m)+c(c+t_3 m)+d(d+t_4 m)$. If we let $t = at_1 + bt_2 + ct_3 + dt_4$ then the expression above equals $a^2 + b^2 + c^2 + d^2 + tm = m(p + t)$. The other cases are similar. Ⓢ

5.15. Use Lemmas 5.6 and 5.7. Ⓗ

5.18. Use Lemma 5.8 and Witt's theorem. Ⓗ

Chapter 6. Multipliers

6.2(a). ϕ_2 is a multiplier since it is an automorphism and $2D = 19 + D$. Ⓢ

6.2(b). ϕ_3 is not an automorphism, so it is not a multiplier. Ⓢ

6.7(a). D has parameters $(31, 6, 1)$ with $n = 5$, so $t = 5$ is a multiplier. Ⓢ

6.8(c) Use Exercise 4.3(d). Ⓗ

6.13. The parameters must be $(11, 5, 2)$, with multiplier $t = 3$. The orbits for ϕ_3 are: (0) $(1, 3, 9, 5, 4)$ $(2, 6, 7, 10, 8)$. The elements in the first 5-cycle form the difference set of Theorem 4.3. The second is the image of the first under ϕ_2, so it is equivalent. Ⓢ

Chapter 7. Necessary Conditions

7.2(b). Using $N = \langle a \rangle$ we find the intersection numbers 6, 4, 3 with respect to $G = N \cup bN \cup b^2N$. They sum to $k = 13$ and their squares sum to $n + \lambda s = 61$. Ⓢ

7.6. Use the Sylow theorems to show that G must contain a normal subgroup of order 13. Ⓗ

7.12. Use the Sylow theorems to show that a group of order 111 has a normal subgroup of order 37. Ⓗ

7.15(a). Since $p = 3$ and $a = 2$, the exponent bound is 9. Ⓢ

Chapter 8. Geometry

8.1(a). $x^0 = 1$, $x^1 = x$, x^2, $x^3 = x + 1$, $x^4 = x^2 + x$, $x^5 = x^2 + x + 1$, $x^6 = x^2 + 1$. Ⓢ

8.1(b). $T_x(x^2) = x + 1 = (0, 1, 1)$, $T_x(x) = x^2 = (1, 0, 0)$, $T_x(x^0) = x = (0, 1, 0)$, so the matrix of T_x is M. Ⓢ

8.5(b).

slope	equation	points
0	$y = 0$	$(0,0),(1,0),(\omega,0),(\omega^2,0)$
1	$y = x+1$	$(0,1),(1,0),(\omega,\omega^2),(\omega^2,\omega)$
ω	$y = \omega x+\omega^2$	$(0,\omega^2),(1,1),(\omega,0),(\omega^2,\omega)$
ω^2	$y = \omega^2 x+\omega$	$(0,\omega),(1,1),(\omega,\omega^2),(\omega^2,0)$
∞	$x = 0$	$(0,0),(0,1),(0,\omega),(0,\omega^2)$ Ⓢ

8.9(a). Since the zero vector belongs to every hyperplane it appears r times in the multiset. We know from Section 2.5 that every 1-space of V appears in $(q^s-1)/(q-1)$ hyperplanes. Each nonzero vector spans a unique 1-space, so each nonzero vector appears $(q^s-1)/(q-1)$ times in the multiset. Ⓢ

8.11. $\displaystyle\sum_{1\le i,j\le r} k_i^{-1}k_j = (K-k_0^{-1})(K-k_0)$. Ⓗ

Chapter 9. Hadamard Difference Sets

9.4(b)

$$\begin{array}{rcl} \text{row } 2\cdot\text{row } 2 = m & \text{implies} & x+y+z+w = m,\\ \text{row } 2\cdot\text{row } 1 = 0 & \text{implies} & x+y-z-w = 0,\\ \text{row } 3\cdot\text{row } 1 = 0 & \text{implies} & x-y+z-w = 0,\\ \text{row } 2\cdot\text{row } 3 = 0 & \text{implies} & x-y-z+w = 0. \end{array}$$ Ⓢ

9.13. We know $\lambda(v-1) = k(k-1)$, so $k \le (v-1)/2$ implies $\lambda(v-1) \le ((v-1)/2)((v-3)/2)$. Since we assume a nontrivial difference set, we may divide both sides by $v-1$ to get $\lambda \le (v-3)/4$. Ⓢ

9.15. As in the proof of Theorem 9.3, a normalized Hadamard matrix H of order 12 defines the incidence matrix A of a symmetric $(11,5,2)$ design. Show that by suitable row and column permutations, A can be transformed to a fixed matrix. A very useful fact is that there are exactly 10 ways to choose two items out of five. Ⓗ

9.29. We have $v = 4n = 4u^2$ and $\lambda = k-n$. The relation $\lambda(v-1) = k(k-1)$ can be written in terms of u and k as $(4u^2-1)(k-u^2) =$

$k(k-1)$. This can be rearranged into the quadratic $k^2 - k(4u^2) + u^2(4u^2-1) = 0$. Using the quadratic formula and simplifying we get

$$k = \frac{4u^2 \pm \sqrt{4u^2}}{2} = 2u^2 \pm u.$$

Solving for λ we get $\lambda = k - u^2 = u^2 \pm u$. If $k = 2u^2 + u$ then $v - k = 4u^2 - (2u^2 + u) = 2u^2 - u$. Also if $\lambda = u^2 + u$, then $v - 2k + \lambda = 4u^2 - 2(2u^2 + u) + u^2 + u = u^2 - u$. Thus the choice of sign in the expressions for k and λ gives the parameters for a difference set or its complement. Ⓢ

Chapter 10. Representations

10.3.

(a) For each $g \in G$, the transformation $\rho(g)$ takes $\sum a_j \mathbf{e}_j$ to $\sum a_j \mathbf{e}_{g(j)}$. The set of coefficients $a_1, \ldots, a_m$ is unchanged, so their sum is unchanged. Ⓢ

(b) Let $\mathbf{w} = \mathbf{e}_1 - \mathbf{e}_2$, and let $g = (12)$. Then $\rho(g)(\mathbf{w}) = -\mathbf{w}$. Ⓢ

10.7. We give the matrix for $\rho_{reg}(a)$:

$$\rho_{reg}(a) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \qquad \text{Ⓢ}$$

10.8(b). You can find one, at least, by inspection. To find the other one, look for eigenvectors of $\rho_{reg}\big((12)\big)$, say, for the eigenvalue -1. Ⓗ

10.12 (a). We show the proof of part (i) of Theorem 10.3. First we show $\rho_1 \oplus \rho_2$ is a linear transformation:

$$\begin{aligned}
&(\rho_1 \oplus \rho_2)(g)(a(\mathbf{v}_1, \mathbf{v}_2) + b(\mathbf{w}_1, \mathbf{w}_2)) \\
&\quad = (\rho_1 \oplus \rho_2)(g)(a\mathbf{v}_1 + b\mathbf{w}_1, a\mathbf{v}_2 + b\mathbf{w}_2) \\
&\quad = (\rho_1(g)(a\mathbf{v}_1 + b\mathbf{w}_1), \rho_2(g)(a\mathbf{v}_2 + b\mathbf{w}_2)) \\
&\quad = (a\rho_1(g)(\mathbf{v}_1) + b\rho_1(g)(\mathbf{w}_1), a\rho_2(g)(\mathbf{v}_2) + b\rho_2(g)(\mathbf{w}_2)) \\
&\quad = a(\rho_1(g)(\mathbf{v}_1), \rho_2(g)(\mathbf{v}_2)) + b(\rho_1(g)(\mathbf{w}_1, \rho_2(g)(\mathbf{w}_2)) \\
&\quad = a(\rho_1 \oplus \rho_2)(\mathbf{v}_1, \mathbf{v}_2) + b(\rho_1 \oplus \rho_2)(\mathbf{w}_1, \mathbf{w}_2).
\end{aligned}$$

To show $\rho_1 \oplus \rho_2$ is a homomorphism, let $(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \oplus V_2$. Then

$$\begin{aligned}
&(\rho_1 \oplus \rho_2)(gh)(\mathbf{v}_1, \mathbf{v}_2) \\
&\quad = (\rho_1(gh)(\mathbf{v}_1), \rho_2(gh)(\mathbf{v}_2)) \\
&\quad = (\rho_1(g)(\rho_1(h)(\mathbf{v}_1)), \rho_2(g)(\rho_2(h)(\mathbf{v}_2)) \\
&\quad = (\rho_1 \oplus \rho_2)(g)(\rho_1(h)(\mathbf{v}_1), \rho_2(h)(\mathbf{v}_2)) \\
&\quad = ((\rho_1 \oplus \rho_2)(g) \circ (\rho_1 \oplus \rho_2)(h))(\mathbf{v}_1, \mathbf{v}_2).
\end{aligned}$$

This shows $(\rho_1 \oplus \rho_2)(gh) = (\rho_1 \oplus \rho_2)(g) \circ (\rho_1 \oplus \rho_2)(h)$. Ⓢ

10.14. If $\mathbf{v}$ and $\mathbf{w}$ are column vectors, then $\mathbf{v} \cdot \mathbf{w} = \mathbf{v}^T \overline{\mathbf{w}}$. Ⓗ

10.19(b). Consider the cases $g \in G_1$ and $g \in G \setminus G_1$ separately. Ⓗ

10.21. Use Exercise 19(b) to find three eigenvectors. Ⓗ

Chapter 11. Characters

11.2(c). $\chi_\rho(g) = 2$ for elements of cycle type (12); there are 6 of these. Ⓢ

11.10(b). For the natural representation, $\chi_\rho((1)) = 3$, $\chi_\rho((12)) = 1$ and $\chi_\rho((123)) = 0$, so $\langle \chi_\rho, \chi_\rho \rangle = \frac{1}{6}(3^2 + 3 \cdot 1^2 + 2 \cdot 0) = 2$. Ⓢ

11.14(b) The inverse of $\chi \in G^*$ is the character $g \mapsto \chi(g^{-1})$. Ⓗ

11.15(a). We use only the assumption that $\rho_2(g)\tau = \tau\rho_2(g)$. Let $v \in \mathrm{Ker}(\tau)$. We want to show that $w = \rho_1(g)(v) \in \mathrm{Ker}(\tau)$. We have $\tau(w) = \tau(\rho_1(g)(v)) = \rho_2(g)(\tau(v)) = \rho_2(g)(0) = 0$, where we write 0 for the zero vector. Now let $v \in \mathrm{Im}(\tau)$, say $v = \tau(w)$ for some w. We want to show $\rho_2(g)(v) \in \mathrm{Im}(\tau)$. We find that $\rho_2(g)(v) = \rho_2(g)(\tau(w)) = \tau(\rho_2(g)(w)) \in \mathrm{Im}(\tau)$. Ⓢ

11.22. If $g \neq 1$, choose $\eta \in G^*$ with $\eta(g) \neq 1$, and consider

$$\eta(g) \sum_{\chi \in G^*} \chi(g). \qquad \text{Ⓗ}$$

11.25(b). Interpret the sum as an inner product of characters. From this, what can you say about ρ as a direct sum of irreducible representations? Ⓗ

11.28. We know $G = D_4 = \langle a, b \,|\, a^4 = b^2 = 1, bab = a^{-1} \rangle$ has five conjugacy classes, and we label the columns with them. Since $G/\langle a^2 \rangle$ is abelian of order 4, we know the 4 linear characters of this factor group become 4 linear characters of G, and we label them χ_0, χ_1, χ_2 and χ_3. By summing squares of degrees, we know the remaining irreducible ρ is of degree 2 and we know from Example 10.11 that it maps

$$a \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad b \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

This gives us the following character table:

	$[1]$	$[a^2]$	$[a]$	$[b]$	$[ab]$
χ_0	1	1	1	1	1
χ_1	1	1	1	-1	-1
χ_2	1	1	-1	1	-1
χ_3	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

Ⓢ

11.29(b). One approach is via the set of class functions α_s, $s = 0, \ldots, t$, where $\alpha_s(g) = 1$ if $g \in \mathcal{C}_s$ and $\alpha_s(g) = 0$ otherwise. Write α_s as a sum of irreducible characters. Ⓗ

11.32(a). Let G act on its left cosets modulo N by left multiplication.

11.32(c). Use the fact that for complex numbers z_j, $|z_1 + \cdots + z_m| \leq |z_1| + \cdots + |z_m|$, and equality holds if and only if there is a fixed real number θ with $z_j = r_j e^{i\theta}$ for $r_j \geq 0$ and $j = 1, \ldots, m$. This fact about complex numbers will seem natural if you think of the standard visual representation of adding complex numbers as adding vectors in the plane. Ⓗ

Chapter 12. Algebraic Number Theory

12.2. Using Theorem 12.1 we know that $\{v_j\} = \{c + 4\epsilon, c, c, c, c\}$. Then $\sum v_j = 5c + 4\epsilon = 24$, so $5c = 24 - 4\epsilon$. This requires $\epsilon = +1$, and $c = 4$. That is, $\{v_j\} = \{8, 4, 4, 4, 4\}$. Ⓢ

12.6. Suppose D is a $(154, 18, 2)$-difference set in a group G that has a normal subgroup N of order 14, so $G/N = \langle aN \rangle$ is cyclic of order 11. Let χ be the character of G with kernel N that maps a to

$\eta = e^{2\pi i/11}$. The order of 2 modulo 11 is 10, so $2R$ is a prime ideal in $R = \mathbb{Z}[\eta]$. Let $v_j = |D \cap a^j N|$. Then $z = \widetilde{\chi}(D) = \sum v_j \eta^j$ and $(zR)(\overline{z}R) = (2R)^4$ implies $z = 4\epsilon\eta^\ell$ for some ℓ and some $\epsilon = \pm 1$. It follows that $\{v_j\} = \{c + 4\epsilon, c, \ldots, c\}$, and $\sum v_j = 11c + 4\epsilon = 18$. The only solution is $\epsilon = -1$ and $c = 2$, which would give a negative intersection number, and thus is a contradiction. Ⓢ

12.9(e) Use Exercise 4.3(d). Ⓗ

Bibliography

1. J. Alexander, R. Balasubramanian, J. Martin, K. Monahan, H. Pollatsek, and R. Sen, *There is no* $(160, 54, 18)$ *difference set in* $G = D_{20} \times H$, J. Combin. Designs **8** (2000), 221–231.
2. K.T. Arasu and D.K. Ray-Chaudhuri, *Multiplier theorem for a difference list*, Ars Combinatoria **22** (1986), 119–137.
3. M. Artin, *Algebra*, Prentice Hall, New Jersey, 1991.
4. E.F. Assmus and J.D. Key, *Designs and their codes*, Cambridge Univ. Press, Cambridge, 1992.
5. L.D. Baumert, *Cyclic difference sets*, Springer–Verlag, New York, 1971, Lecture Notes in Mathematics #182.
6. M.K. Bennett, *Affine and projective geometry*, John Wiley and Sons, Inc., New York, 1995.
7. T. Beth and D. Jungnickel, *Variations on seven points: An introduction to the scope and methods of coding theory and finite geometries*, Aequationes Mathematicae **25** (1982), 153–176.
8. T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, second ed., Cambridge Univ. Press, 1999, 2 vol.
9. E. Brown, *The many names of* $(7, 3, 1)$, Mathematics Magazine **75** (2002), 83–94.
10. R.H. Bruck, *Difference sets in a finite group*, Trans. AMS **78** (1955), 464–481.
11. R.H. Bruck and H.J. Ryser, *The nonexistence of certain finite projective planes*, Can. J. Math. **1** (1949), 88–93.

12. P.J. Cameron and J.H. van Lint, *Designs, graphs, codes and their links*, Cambridge Univ. Press, Cambridge, 1991, London Math. Soc., Student Texts 22.
13. S. Chowla and H.J. Ryser, *Combinatorial problems*, Can. J. Math. **2** (1950), 93–99.
14. G.W. Cobb, *Introduction to design and analysis of experiments*, Springer, New York, 1997.
15. C.W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley and Sons, New York, 1962.
16. J.A. Davis and J. Jedwab, *A unifying construction for difference sets*, J. Combin. Theory A **80** (1997), 13–78, First appeared as Hewlett-Packard Tech Report, 1996.
17. J.A. Davis and K.W. Smith, *A construction of difference sets in high exponent 2-groups using representation theory*, J. Alg. Combin. **3** (1994), 137–151.
18. J.F. Dillon, *Variations on a scheme of McFarland for noncyclic difference sets*, J. Combin. Theory A **40** (1985), 9–21.
19. J.H. Dinitz and D.R. Stinson (eds.), *Contemporary design theory: A collection of surveys*, John Wiley and Sons, Inc., New York, 1992.
20. U. Dudley, *A guide to elementary number theory*, MAA, Washington, D.C., 2009.
21. T. Durt, B-G. Englert, I. Bengtsson, and K. Zyczkowski, *On mutually unbiased bases*, Int. J. Quantum Information **8** (2010), 535–640.
22. J.B. Fraleigh and R.A. Beauregard, *Linear algebra*, third ed., Pearson, Glenview, IL, 1995.
23. J.A Gallian, *Contemporary abstract algebra*, 6 ed., Houghton Mifflin, Boston, 2006.
24. C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European J. Comb. **30** (2009), 246–262.
25. S.W. Golomb, *Signals with good correlation properties*, pp. 331–352, in Pott et al. [**60**], 1999, NATO Science Series, Vol. 542.
26. M. Hall, Jr., *Cyclic projective planes*, Duke Math J. **14** (1947), 1079–1090.
27. ———, *A survey of difference sets*, Proc. AMS **7** (1956), 975–986.
28. ———, *Combinatorial theory*, 2 ed., Wiley, Waltham, MA, 1986.
29. M. Hall, Jr. and H.J. Ryser, *Cyclic incidence matrices*, Can. J. Math. **3** (1951), 495–502.
30. P.R. Halmos, *Finite dimensional vector spaces*, second ed., Van Nostrand, Princeton, NJ, 1958.

31. J.E. Iiams, *On difference sets in groups of order* $4p^2$, J. Combin. Theory A **72** (1995), 256–276.
32. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Springer-Verlag, NY, 1982.
33. I.M. Isaacs, *Algebra: A graduate course*, AMS Graduate Studies in Mathematics, Providence, RI, 2009.
34. B.W. Jones, *The arithmetic theory of quadratic forms*, MAA, Washington, DC, 1950, Carus Monograph no. 10.
35. D. Jungnickel, *Difference sets*, pp. 241–324, in Dinitz and Stinson [**19**], 1992.
36. D. Jungnickel and A. Pott, *Difference sets: An introduction*, pp. 259–295, in Pott et al. [**60**], 1999, NATO Science Series, Vol. 542.
37. D. Jungnickel and S.A. Vanstone (eds.), *Coding theory, design theory, group theory: Proc. of the Marshall Hall conf.*, Wiley, New York, 1993.
38. W.M. Kantor, *Exponential numbers of two-weight codes, difference sets and symmetric designs*, Disc. Math. **46** (1984), 95–98.
39. ———, *MUBs inequivalence and affine planes*, J. Math. Physics **53** (2012), 1–9.
40. R. Kibler, *A summary of noncyclic difference sets,* $k < 20$, J. Combin. Theory A **25** (1978), 62–67.
41. R.G. Kraemer, *Proof of a conjecture on Hadamard 2-groups*, J. Combin. Theory A **63** (1993), 1–10.
42. C.W.H. Lam, *The search for a finite projective plane of order 10*, Am. Math. Monthly **98** (1991), 305–318.
43. E.S. Lander, *Symmetric designs: an algebraic approach*, Cambridge University Press, Cambridge, 1983, London Math. Soc. Lecture Note Series 74.
44. E. Lehmer, *On residue difference sets*, Can. J. Math. **5** (1953), 425–432.
45. R.A. Liebler, *The inversion formula*, J. Combin. Math. Combin. Comput. **13** (1993), 143–160.
46. ———, *Constructive representation theoretic methods and non-abelian difference sets*, pp. 331–352, in Pott et al. [**60**], 1999, NATO Science Series, Vol. 542.
47. R.A. Liebler and K.W. Smith, *On difference sets in certain 2-groups*, pp. 195–212, in Jungnickel and Vanstone [**37**], 1993.
48. J. MacWilliams and N.J.A. Sloane, *Pseudo-random sequences and arrays*, Proc. IEEE **64** (1976), 1715–1729.
49. J.M. Masley, *Solution of the class number two problem for cyclotomic fields*, Inventiones **28** (1975), 243–244.

50. R.L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combin. Theory A **15** (1973), 1–10.
51. ———, *Difference sets in Abelian groups of order* $4p^2$, Mitt. Math. Sem. Giessen **192** (1989), 1–70.
52. R.L. McFarland and S.L. Ma, *Abelian difference sets with multiplier minus one*, Arch. Math. (Archiv der Mathematik) **54** (1990), 610–623.
53. R.L. McFarland and H.B. Mann, *On multipliers of difference sets*, Can. J. Math. **17** (1965), 541–542.
54. R.L. McFarland and B.F. Rice, *Translates and multipliers of abelian difference sets*, Proc. AMS **68** (1978), 375–379.
55. P.K. Menon, *On difference sets whose parameters satisfy a certain relation*, Proc. AMS **13** (1962), 739–745.
56. E. Moore and A. Walker, *Looking for difference sets in* $D_{2p} \times Z_q$, J. Combin. Designs **8** (2000), 34–41.
57. R.E.A.C. Paley, *On orthogonal matrices*, J. Math. Phys. MIT **12** (1933), 311–320.
58. H. Pollatsek, *Quantum error correction: Classic group theory meets a quantum challenge*, Math. Monthly **108** (2001), 932–962.
59. A. Pott, *Finite geometry and character theory*, Springer-Verlag, Berlin, 1995, Lecture Notes in Mathematics, #1601.
60. A. Pott, P.V. Kumar, T. Helleseth, and D. Jungnickel (eds.), *Difference sets, sequences and their correlation properties*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999, NATO Science Series, Vol. 542.
61. H.J. Ryser, *The existence of symmetric block designs*, J. Combin. Theory A **32** (1982), 103–105.
62. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. AMS **43** (1938), 377–385.
63. G.K. Skinner, *X-ray imaging with coded masks*, Scientific American (1988), 84–89.
64. ———, *Sensitivity of coded mask telescopes*, Applied Optics **47** (2008), 2739–2749.
65. K.W. Smith, *Non-abelian Hadamard difference sets*, J. Combin. Theory A **70** (1995), 144–156.
66. R.G. Stanton and Sprott, *A family of difference sets*, Can. J. Math. **10** (1958), 73–77.
67. I.N. Stewart and D.O. Tall, *Algebraic number theory*, second ed., Chapman and Hall, New York, 1987.
68. A. Tucker, *Applied combinatorics*, fifth ed., Wiley, Hoboken, NJ, 2007.

69. R.J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.

70. J.H. van Lint and R.M. Wilson, *A course in combinatorics*, Cambridge Univ. Press, 1992.

71. W.K. Wootters and B.D. Fields, *Optimal state-determination by mutually unbiased measurements*, Annals of Physics **191** (1989), 363–381.

Index

Index of Parameters

Difference sets belong both to group theory and to combinatorics. Studying them requires tools from geometry, number theory, and representation theory. This book lays a foundation for these topics, including a primer on representations and characters of finite groups. It makes the research literature on difference sets accessible to students who have studied linear algebra and abstract algebra, and it prepares them to do their own research.

This text is suitable for an undergraduate capstone course, since it illuminates the many links among topics that the students have already studied. To this end, almost every chapter ends with a coda highlighting the main ideas and emphasizing mathematical connections. This book can also be used for self-study by anyone interested in these connections and concrete examples.

An abundance of exercises, varying from straightforward to challenging, invites the reader to solve puzzles, construct proofs, and investigate problems—by hand or on a computer. Hints and solutions are provided for selected exercises, and there is an extensive bibliography. The last chapter introduces a number of applications to real-world problems and offers suggestions for further reading.

Both authors are experienced teachers who have successfully supervised undergraduate research on difference sets.

Photograph by Mitch Wilson

ISBN: 978-0-8218-9176-6

9 780821 891766

STML/67

For additional information and updates on this book, visit
www.ams.org/bookpages/stml-67