Transposable Character Tables

by

Ivan Andrus

Submitted to

Central European University

Department of Mathematics and its Applications

In partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Supervisor: Pál Hegedűs

Budapest, Hungary

2013

Declaration

I hereby declare that the dissertation contains no materials accepted for any other degrees in any other institution.

Ivan Andrus

(signature)

Declaration

I hereby declare that the dissertation contains no materials previously written and/or published by another person, except where appropriate acknowledgment is made in the form of bibliographic reference, etc.

Ivan Andrus

(signature)

Declaration

I hereby declare that Ivan Andrus is the primary author of the following joint papers which are based on material contained in this dissertation:

1. Determination of conjugacy class sizes from products of characters (Arch. Math. (Basel) 100.1 (2013))

2. Transposable character tables, dual groups (arXiv:1212.6380)

Pál Hegedűs

(signature)

Tetsuro Okuyama

(signature)

Acknowledgments

Although there are many who have helped me during the last few years, there are two people in particular without whose help I would not have finished this dissertation.

The first is my wife who moved across an ocean with two small children to live off a student's stipend. Although we were separated for long periods on several occasions, I have always felt her support. Her love for me has never been more evident than in the past few years.

The second is my adviser Pál Hegedűs. He has been patient, understanding, and positive. I always left his office feeling better than when I went in. Whenever I felt I could not finish, he somehow restored my hope. Not only has he helped me mathematically, he has been a genuine mentor and friend.

Abstract

In the study of finite groups a sort of duality has been observed between conjugacy classes and irreducible characters, but the connection is quite murky. Abelian groups are special in that, as $\mathbb{Z}$-modules, they have true duals. They also have the property that the transpose of their character tables is still a character table. We generalize this by allowing rows to be multiplied by constants before and after transposition. A group whose character table is still a character table after this generalized transposition is called transposable. Transposable groups generalize slightly the notion of self-dual groups of Okuyama and Hanaki [Oku13; HO97; Han97; Han96a; Han96b]. We derive some properties of transposable groups and give some examples. We also study the related property of having square conjugacy class sizes and show that no non-abelian simple group has square class sizes.

Table of Contents

Declaration of Authorship **ii**

Acknowledgments **iii**

Abstract **iv**

1 Duality of Irreducible Characters and Conjugacy Classes **1**
1.1 Introduction 1
1.2 Duality of Character Degrees and Conjugacy Class Sizes 5
1.2.1 Graphs 13
1.3 Some Dual Results 17

2 Transpositions of Character Tables **23**
2.1 Introduction 23
2.2 Basic Results 24
2.3 Self-dual Groups 29

3 Properties of Transposable Groups **31**
3.1 Normal Subgroup Correspondences 31
3.1.1 Central Series 34
3.2 Nilpotency of Transposable Groups 39
3.3 Multiplication Constants of Characters and Classes 41
3.4 Potential Constraints 43

4 Square Conjugacy Class Sizes **45**
4.1 Simple Groups of Square Order 46
4.1.1 Orthogonal and Symplectic Groups: $C_n(q)$ and $B_n(q)$ 51
4.1.2 Linear and Unitary Groups: $A_n(q)$ and ${}^2A_n(q^2)$ 52
4.1.3 Sporadic Groups 53
4.1.4 Orthogonal Groups: $D_n(q)$ and ${}^2D_n(q^2)$ 54
4.1.5 Chevalley Groups: $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, and $G_2(q)$ 55
4.1.6 Twisted Groups: ${}^2E_6(q^2)$, ${}^3D_4(q^3)$ ${}^2B_2(2^{2n+1})$, ${}^2F_4(2^{2n+1})$, ${}^2G_2(3^{2n+1})$ 58

4.2 Class Sizes in Simple Groups 60

5 Examples of Transposable Groups **66**

5.1 Constructions 67

5.2 Examples 69

5.3 Self-duality of a certain family of p-groups 72

5.3.1 Determination of Characters 74

5.3.2 Duality 85

References **88**

Chapter 1

Duality of Irreducible Characters and Conjugacy Classes

1.1 Introduction

Since much of this dissertation has been motivated by the apparent duality between irreducible characters and conjugacy classes, we begin with a brief introduction to the concept of duality and why it is interesting. We summarize some results illustrating the duality (and lack thereof) between irreducible characters and conjugacy classes, and give a few brief results dual to some in the literature. The bulk of the dissertation is then devoted to the exploration of what happens when we require this "quasi-"duality to become closer to a real duality. That is, when the character table of one group is the transpose of the character table of another group.

In this dissertation all groups are finite unless otherwise noted. For the most part, our notation is standard, generally following Isaacs [Isa76]. We shall, at various times, denote the conjugacy class of x in G by x^G or $\mathcal{K}_x$. We usually assume that a character table has been rearranged so that the first row consists of ones and the first column of positive integers in ascending order. In other words, the first row corresponds to the trivial character, and the first column the trivial conjugacy class. We shall often say class to mean conjugacy class, and occasionally simply use character to mean irreducible character if it's clear from context.

Duality is a concept that permeates mathematics, nevertheless, it has no formal definition. In general terms it means that two structures are similar to each other so that statements and theorems about one can be translated into the language of the other and still be true. An example is plane projective geometry, in which the concepts of point and line can be interchanged and theorems (once properly translated) still hold.

The concept of duality often comes with an interchanging of "large" and "small." The dual of a poset is a poset in which the order is reversed. Reversal of the order relation is often known as a Galois correspondence because, in Galois theory, subfields correspond to subgroups of the Galois group in such a way that the intersection (meet) of subfields corresponds to the generated subgroup (join). The dual of a length n linear code with dimension k has dimension $n - k$ (and length n) so that dimension is interchanged in this case.

Another important property which is often true is that the bidual (dual of the dual) of an object is isomorphic to the original object. This isn't true in general, for example an infinite dimensional vector space is *not* isomorphic to its bidual. However, it is true for duality of finite dimensional vector spaces, posets, modules, and the platonic solids to name a few.

It is also useful to see an example of something which is not dual. Every platonic solid is dual to the solid formed by placing a point in the center of every face and taking the convex hull. This leads to an interchange of faces and corners (2-dimensional and 0-dimensional respectively). Given this example, and the example of plane projective geometry, one might presume that interchanging the vertices and edges of an undirected graph would result in a duality. However, the resulting graph, called the line graph, is usually not considered a dual because it fails to have many of the desirable properties of duality. For example, the bidual is only isomorphic to the original in the case of cyclic graphs. Most importantly, theorems about graphs do not translate nicely into theorems about line graphs.

Thus, the ability to dualize statements (and operations) is extremely important. Open and closed sets in topology are dual under the operation of complementation, and union and intersection are dual operations. This means that the complement of an open set is a closed set. Likewise, the definition that the union of open sets is open translates into the equivalent definition that the intersection of closed sets is closed. Clearly duality is a useful concept, since when stating or proving theorems one can choose the more convenient form. Many times this is more than just notational, allowing completely new techniques to be of use. In algebraic geometry the duality between varieties (a geometric concept) and ideals of polynomial rings (an algebraic concept) allows techniques from both fields to be used and has proven very fruitful.

One common method of constructing the dual of some structure X is to use the set $X^* = \mathrm{Hom}(X, Y)$ where Y is some fixed set. If X^* can be given a similar structure to X, this can lead to a duality. Usually the privileged set Y must be chosen carefully. This type of duality is used with vector spaces, for example. If X is a k-vector space, then $\mathrm{Hom}(X, k)$ has the structure of a k-vector space as well. Moreover, there is an injective "evaluation" map sending $x \in X$ to $(f \mapsto f(x)) \in X^{**}$ (where $f \in \mathrm{Hom}(X, k)$). This map is an isomorphism if and only if X is finite dimensional, though the duality is still useful in general.

Compact abelian groups (including all finite abelian groups) are handled in the same way. Define the characters of an abelian group G to be the continuous homomorphisms from G into the circle group (the complex numbers of magnitude 1). The characters then form a group called the dual group $\hat{G}$, and the bidual $\hat{\hat{G}}$ is canonically isomorphic to G. This is known as the Pontryagin duality theorem. If G is finite then $G \cong \hat{G}$, though not in a canonical way.

If we wish to find the dual of an arbitrary finite group G we run into a problem: the construction above only gives information about the abelianization of G. To overcome this problem we can try choosing a different object for Y. Representation theory studies the case when Y is the general linear group $\mathrm{GL}_n(k)$ for some field k. The homomorphisms are called (linear) representations of G. The simplest case is when k is algebraically closed of characteristic 0 (*e.g.*, $k = \mathbb{C}$). In this case every representation decomposes into a direct product of irreducible representations. The traces of these representations, called characters, are maps from G into k and determine the representations when the characteristic of k is 0. Since these characters are maps from $G \to k$ they share many properties with the characters of abelian groups. (They are not homomorphisms, however, and so the analogy is not perfect.) In particular, they are constant on conjugacy classes, and so (except in the abelian case) cannot be used to separate elements. This prohibits the notion of a bidual with an injective evaluation map.

It is well known that the number of irreducible representations (equivalently characters) is equal to the number of conjugacy classes. Thus we might hope for a duality between conjugacy classes and irreducible representations (characters). In some sense, this duality does exist. First, we should note that conjugacy class sums form a basis for the center of the group algebra $\mathbb{C}G$, and that the irreducible characters form a basis for $\mathrm{Char}(G)$, the algebra of complex valued class functions on G. We can associate to every irreducible character χ, a primitive central idempotent e_χ of the group algebra by

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g. \tag{1.1}$$

This gives another basis for the center of the group algebra which is different from the first.

In fact, this is true in the more general setting of table algebras. Table algebras are generalizations of character tables and capture many of their elementary properties. They come in a dizzying number of definitions and names from C-algebra, to hypergroup, to generalized fusion algebra, and back. Some of the names and definitions used are explained in the survey paper [Bla09]. Kawada duality states that every table algebra with basis has a dual basis defined by an equation similar to (1.1).

Given the power of duality in the rest of mathematics, it seems prudent to investigate the quasi-duality between conjugacy classes and irreducible characters. Indeed, it has been extensively studied by many people. We are unaware, however, of attempts to use the techniques employed in this dissertation for this purpose.

1.2 Duality of Character Degrees and Conjugacy Class Sizes

Irreducible characters and conjugacy classes of finite groups are "dual" in many ways. The most well known is that a group G has the same number of conjugacy classes as irreducible characters. The second similarity encountered by students is that they satisfy similar orthogonality relations. Namely, if we let $\operatorname{Rep}(G)$ indicate a set of conjugacy class representatives and $\delta_{i,j}$ the Kronecker delta function, then

$$\delta_{\chi,\varphi} = \frac{1}{|G|} \sum_{g \in \mathrm{Rep}(G)} \left| g^G \right| \chi(g) \overline{\varphi(g)},$$
$$\delta_{g^G,h^G} = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \left| g^G \right| \chi(g) \overline{\chi(h)},$$

for all $\chi, \varphi \in \mathrm{Irr}(G)$ and $g, h \in G$. Thus, at least for these equations, it might be natural to work with the character table multiplied by the square root of the conjugacy class sizes (and perhaps divided by the square root of the order of G). Later on, we shall see more evidence that this is, in fact, a better object for highlighting the duality of irreducible characters and conjugacy classes.

In this section we further explore this apparent duality by summarizing some results from the literature. Many of these results involve the multisets of character degrees $\mathrm{cd}(G) = \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$ and conjugacy class sizes $\mathrm{ccs}(G) = \{|\mathcal{K}_i| \mid \mathcal{K}_i \in \mathrm{Cl}(G)\}$. Here, and throughout the rest of this dissertation, $\mathrm{Cl}(G) = \left\{ g^G \mid g \in G \right\}$ is the set of conjugacy classes.

This section is by no means an exhaustive survey of the interesting results in the area. Rather, we focus on theorems which show the similarities or differences between the irreducible characters and conjugacy classes. For further information see the survey articles [CC11], [CH07] and [Lew08]. We shall avoid introducing notation unnecessarily.

A theorem of Brauer [Isa76, Theorem 6.32] states that if a group Γ acts compatibly on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$, then for each $\alpha \in \Gamma$, the number of fixed irreducible characters equals the number of fixed conjugacy classes. Here compatibly means that $\chi(g) = \chi^\alpha(g^\alpha)$ for all $\alpha \in \Gamma$, $\chi \in \mathrm{Irr}(G)$, $g \in G$, and $g^\alpha \in \mathcal{K}_g^\alpha$. Thus, orbit theorems can often be applied to both conjugacy classes and irreducible characters, which helps explain some of the similarities between the two. By showing that solvable groups have "large" orbits on completely reducible faithful G-modules, Yang improved earlier results of Moretó and Wolf [MW04]. Denote by $F_i(G)$ the ith term of the upper Fitting series, *i.e.*, $F_1(G) = F(G)$ and $F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G))$.

Theorem 1.2.1 ([Yan09]). *If G is solvable, then $|G : F_8(G)|$ divides the size of some conjugacy class. Also, $|G : F_8(G)|$ divides $\chi(1)$ for some $\chi \in \mathrm{Irr}(G)$.*

We now examine what happens when every conjugacy class of a group has distinct sizes, or when every irreducible character has a different degree. The concepts of distinct sizes and distinct nontrivial sizes are equivalent for conjugacy classes, but they are separate for character degrees.

Theorem 1.2.2 ([KLT95; Zha94]). *Suppose that distinct noncentral classes of G have distinct sizes. Then $Z(G) = 1$, and if G is solvable, $G \cong S_3$. It is still open for non-solvable groups and is known as the S_3-conjecture.*

Theorem 1.2.3 ([BCH92]). *There are no nontrivial groups whose character degrees are all distinct.*

Theorem 1.2.4 ([BCH92]). *Suppose that $\chi(1) \neq \varphi(1)$ for all nonlinear characters $\chi \neq \varphi$. Then G is one of*

1. *An extraspecial 2-group of order 2^{2m+1}, with a unique irreducible character of degree 2^m.*
2. *A Frobenius group of order $p^n(p^n - 1)$ for some p, with an elementary abelian kernel G' of order p^n, a cyclic complement and a unique nonlinear character of degree $p^n - 1$.*
3. *The Frobenius group of order 72, with a complement isomorphic to the quaternion group of order 8 and two nonlinear irreducible characters of degrees 2 and 8.*

As shown in [Chi04], this is the same set of groups that satisfy the condition of all nonlinear characters having distinct 0-sets; *i.e.*, they vanish on different conjugacy classes. As a dual to characters having distinct 0-sets, Chillag gave in the same paper a classification of groups whose noncentral conjugacy classes have distinct vanishing sets.

Theorem 1.2.5. *If every two distinct noncentral conjugacy classes have different sets of irreducible characters which vanish on them, then G is abelian or $G \cong S_3$.*

If the S_3-conjecture is true, the conditions of having distinct vanishing sets and distinct sizes are equivalent for both character degrees and conjugacy class sizes.

Since the complex conjugate of characters (conjugacy classes) will have the same degree (size), odd order groups cannot have distinct character degrees (class sizes). In order to extend the notion to odd order groups, it is natural to require that they have exactly two irreducible characters (conjugacy classes) of each degree (size).

Theorem 1.2.6 ([HS06])**.** *Let G be a non-abelian odd order group. Then G has exactly two classes of each size if and only if G is the non-abelian group of order 21.*

Strikingly, the same result is true for irreducible characters.

Theorem 1.2.7 ([CH07])**.** *Let G be a non-abelian odd order group. Then G has exactly two non-principal characters of each degree if and only if G is the non-abelian group of order 21.*

But again, if we relax the condition to nonlinear characters, a larger class of groups arises.

Theorem 1.2.8 ([CH08])**.** *Let G be a non-abelian odd order group. Then G has exactly two nonlinear characters of each degree if and only if G is one of the following groups.*

- *An extraspecial 3-group with exactly 2 nonlinear irreducible characters of degree $\sqrt{|G|/3}$.*
- *A Frobenius group of order $p^n(p^n-1)/2$ for some odd prime p and an abelian kernel G' of order p^n, and exactly 2 nonlinear irreducible characters of degree $(p^n-1)/2$.*

Chillag studied the zeros of characters and found two dual theorems. He even notes that the proofs are "dual."

Theorem 1.2.9 ([Chi99]). *If G is a group with $G \neq G' \neq G''$, then G has a conjugacy class $\mathcal{K}$ with $\frac{|G|}{|\mathcal{K}|} \leq 2m$ where m is the maximal number of zeros in a row of the character table of G.*

Theorem 1.2.10 ([Chi99]). *If G is a group with $1 \neq Z(G) \neq Z_2(G)$, then G has an irreducible character χ with $\frac{|G|}{|\chi(1)^2|} \leq 2m$ where m is the maximal number of zeros in a column of the character table of G.*

Much can be said about a group based on the divisors of its class sizes and character degrees.

Theorem 1.2.11 ([Tho64]). *Suppose that $p \mid \chi(1)$ for all nonlinear irreducible characters χ of G, then G has a normal p-complement.*

A good corresponding theorem for conjugacy classes is unknown. The two obvious candidates, having a normal p-complement or normal Sylow p-subgroup, are not true. For example consider $SL_2(3)$, which has conjugacy class sizes of $\{1, 4, 6\}$ but not a normal 2-complement. The dihedral group of order 24 has conjugacy class sizes of $\{1, 2, 6\}$, but its Sylow 2-subgroup is not normal. The following is one theorem that does apply under these conditions.

Theorem 1.2.12. *If $p \mid |\mathcal{K}|$ for all noncentral conjugacy classes $\mathcal{K}$, then $C_G(P) \leq Z(G)$ for P a Sylow p-subgroup of G.*

Another situation in which more is known about character degrees than class sizes is given below. In fact, nothing is known about class sizes in this case.

Theorem 1.2.13 ([Tho70]). *If the character degrees of G are linearly ordered by divisibility, then G has a Sylow series.*

The opposite situation occurs when p doesn't divide the orders.

Theorem 1.2.14 ([Mic86; Itô51]). *G has a normal abelian Sylow p-subgroup if and only if* $p \nmid \chi(1)$ *for all* $\chi \in \mathrm{Irr}(G)$.

Theorem 1.2.15 ([Cam72]). *The Sylow p-subgroup of G is an abelian direct factor if and only if* $p \nmid |\mathcal{K}|$ *for all conjugacy classes* $\mathcal{K}$ *of G.*

By relaxing the restriction to allow p to divide at most 1 character degree or conjugacy class size, we obtain the following theorems.

Theorem 1.2.16 ([Isa+09]). *Suppose* $p \mid \chi(1)$ *for at most one* $\chi \in \mathrm{Irr}(G)$. *Let P be a Sylow p-subgroup of G, and* $U = O_p(G)$. *If P is not normal in G* (i.e., $U < P$), *then*

1. *U is abelian.*

2. P/U *is abelian and is cyclic if G is p-solvable.*

3. $|P/U| = \chi(1)_p$.

4. P/U *is a trivial intersection set in* G/U.

Theorem 1.2.17 ([DMN09]). *Let G be a group with exactly one conjugacy class whose size is divisible by a prime p. Then one of the following holds*

1. *G is a Frobenius group with Frobenius complement of order* 2 *and Frobenius kernel of order divisible by p.*

2. *G is a doubly transitive Frobenius group whose Frobenius complement has a nontrivial central Sylow p-subgroup.*

3. *p is odd,* $G = KH$ *where* $K = F(G)$ *is a q-group for some prime q. Also* $H = C_G(P)$ *for a Sylow p-subgroup P of G,* $K \cap H = Z(K)$ *and* $G/Z(K)$ *is a doubly transitive Frobenius group.*

Several other similar results are summarized in [CH07]. In fact, we can say something about the sizes of the hypercenter and nilpotent residual if we retain information about the number of times each class size or character degree appears.

Theorem 1.2.18 ([CH93])**.** *If G is a group then*

$$|G/\mathbf{O}^p(G)| = \Big(\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \chi(1)=p^a}} \chi(1)^2\Big)_p.$$

The index of the nilpotent residual is the product, for all primes p, of such indices.

Theorem 1.2.19 ([CHM92])**.** *Let G be a group and* $\mathrm{Cls}(G)$ *the set of conjugacy classes. The order of the hypercenter* $Z_\infty(G)$*, can be computed from the prime power class sizes according to*

$$|Z_\infty(G)|_p = \Big(\sum_{\substack{\mathcal{K}\in\mathrm{Cls}(G)\\ |\mathcal{K}|=p^a}} |\mathcal{K}|\Big)_p.$$

As we have seen previously, restrictions on conjugacy class sizes often leads to stronger restrictions on groups structure. The following is another example of this.

Theorem 1.2.20 ([CH90])**.** *If no conjugacy class size is divisible by* 4*, then G is solvable.*

Theorem 1.2.21 ([Lew07])**.** *If no character degree is divisible by* 4*, then G is solvable or* $G \cong A_7 \times S$ *where S is solvable and* 2 *does not divide any character degree of S.*

Theorem 1.2.22 ([CW99; Li99])**.** *If all conjugacy class sizes are square-free then G is supersolvable, the derived length is bounded by* 3*, both* $G/F(G)$ *and* G' *are cyclic groups with square-free orders, and the nilpotency class of* $F(G)$ *is at most* 2*.*

Theorem 1.2.23 ([HM85])**.** *Let all character degrees of G be square-free. If G is solvable it has derived length at most* 4 *and Fitting height no more than* 3*. If G is not solvable, then* $G \cong A_7 \times S$ *where S is solvable.*

The following illustrate another difference between the theories.

Theorem 1.2.24 ([BF06; BF08a; BF08b; BF11]). *Suppose a group G has conjugacy class sizes $\{1, n, m, mn\}$ with $\gcd(m, n) = 1$. Then G is nilpotent and m, n are prime powers.*

Theorem 1.2.25 ([Lew98, Example 8.1]). *Given any coprime integers m, n, there exists a directly indecomposable group G with character degrees $\{1, n, m, mn\}$.*

Given the previous theorem, the following may be slightly surprising.

Theorem 1.2.26 ([Lew98]). *If G has character degrees of $\{1, p, q, r, pq, pr\}$ for distinct primes p, q, and r, then $G = A \times B$ where $\mathrm{cd}(A) = \{1, p\}$ and $\mathrm{cd}(B) = \{1, q, r\}$.*

Stronger results for conjugacy classes, including the following, are found in [CC00].

Theorem 1.2.27 ([CC00]). *Suppose G has conjugacy class sizes of*

$$\{1, p_1^{a_1}, \ldots, p_s^{a_s}\} \times \{1, q_1^{b_1}, \ldots, q_r^{b_r}\}$$

for distinct primes p_i, q_j. Then $G = A \times B$ where $\mathrm{ccs}(A) = \{1, p_1^{a_1}, \ldots, p_s^{a_s}\}$ and $\mathrm{ccs}(B) = \{1, q_1^{b_1}, \ldots, q_r^{b_r}\}$.

Despite all the similarities, the following theorem illustrates just how different character degrees and conjugate class sizes can be.

Theorem 1.2.28 ([FM01]). *Given any two integers r and s greater than 1, there exists a p-group of nilpotency class 2 such that the number of distinct character degrees is r and the number of distinct class sizes is s.*

One final interesting comparison is in the multiplication of conjugacy classes (characters) with coprime sizes (degrees). It is easy to prove (see Lemma 3.4.1 and Corollary 3.4.2) the following lemma about conjugacy classes.

Lemma 1.2.29. *If $x, y \in G$ are elements such that $(|x^G|, |y^G|) = 1$, then $x^G y^G = (xy)^G$. In other words products of conjugacy classes of coprime size are "irreducible."*

In [Gaj79], Gajendragadkar studies the case of π-separable groups. There he proves that $\chi\varphi$ is irreducible for two characters χ and φ if they are π-special and π'-special respectively (which implies coprime degrees). Being π-special is more restrictive than just having coprime degrees. In general, products of characters with coprime degrees are not irreducible, even for π-separable groups, as the symmetric group S_4 demonstrates.

In the other direction, Adan-Bante was motivated in [Ada06] by a result about multiplication of characters to find the corresponding result for conjugacy classes. The duality here is probably the least straightforward of any we present.

Theorem 1.2.30 ([ALM04]). *Suppose G is a finite nilpotent group and χ, φ are faithful irreducible characters such that $\chi\varphi$ is a multiple of an irreducible. Then χ and φ both vanish outside the center of G.*

Theorem 1.2.31 ([Ada06]). *Let G be a finite group, a^G and b^G be conjugacy classes of G such that $C_G(a) = C_G(b)$. Then $a^G b^G = (ab)^G$ if and only if $[ab, G] = [a, G] = [b, G]$ and $[ab, G]$ is a normal subgroup of G.*

1.2.1 Graphs

To better understand the arithmetical properties of the character degrees and conjugacy class sizes, two graphs have been studied. The notation for these graphs is not standard across the different papers, so care must be taken when reading the literature. Let X denote a set of positive integers, and $\pi(X)$ the set of divisors of elements of X. The **prime vertex graph**, denoted $\Delta(X)$, has as vertices the set $\pi(X)$. Two primes p and q are connected in $\Delta(X)$ if pq divides some integer $x \in X$. The second graph, which we

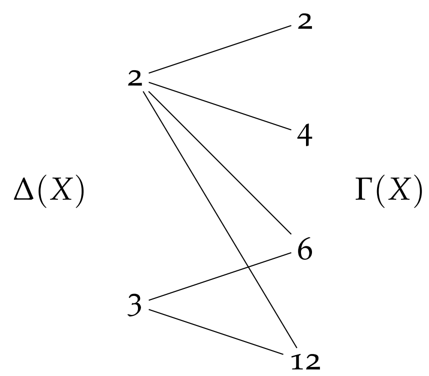

Figure 1.1: $B(X)$ for $X = \{2, 4, 6, 12\}$

denote $\Gamma(X)$, is called the **common divisor graph** and has as vertices all elements of X except 1. Two vertices $a, b \in \Gamma(X)$ are connected if $\gcd(a, b) > 1$.

Given a graph G, it is not difficult to construct a set X so that $\Delta(X)$ or $\Gamma(X)$ is isomorphic to G. Once X is fixed, however, the structure of the two graphs is related. For example, the number of connected components is the same between $\Delta(X)$ and $\Gamma(X)$. Moreover, the diameter of the two graphs differs by at most 1. These facts are easily seen by considering the bipartite graph $B(X)$, introduced in [IP10], whose vertex set is the disjoint union of the vertices of $\Delta(X)$ and $\Gamma(X)$. There is an edge between $p \in \pi(X)$ and $x \in X$ if $p \mid x$. By "collapsing" the vertices of $\Delta(X)$, $\Gamma(X)$ can be recovered and vice versa.

We shall often write $\Delta(\mathrm{ccs})$ and $\Delta(\mathrm{cd})$ instead of $\Delta(\mathrm{ccs}(G))$ and $\Delta(\mathrm{cd}(G))$ when the group G is understood, and we use the notation $n(\Gamma)$ to indicate the number of connected components of a graph Γ. It should also be noted that some authors define the graphs slightly differently, *e.g.,* by creating a vertex for each noncentral conjugacy class instead of one for each distinct size. However, this does not change the essence of any of the theorems we quote.

In general, all of the graphs studied have "many" edges. For example, if G has a non-abelian p-group quotient for some prime p, then p will be adjacent to every other prime in $\Delta(\text{cd})$. We start by considering $\Delta(\text{cd})$ and $\Delta(\text{ccs})$.

Theorem 1.2.32 ([Pál98]). *If G is a solvable group, then given any 3 primes in $\Delta(\text{cd}(G))$ there will be an edge connecting 2 of them.*

Theorem 1.2.33 ([Dol06]). *For any 3 primes in $\Delta(\text{ccs})$, there will be an edge connecting 2 of them.*

Corollary 1.2.34 ([Man85; MWW89]). *The graph $\Delta(\text{cd})$ for solvable groups, or $\Delta(\text{ccs})$ for all groups, has at most 2 connected components. If it is connected, then the diameter is no more than 3, otherwise each connected component is a complete graph.*

There are examples of solvable groups for which $\Delta(\text{cd})$ have diameter 3, and examples for $\Delta(\text{ccs})$ as well. The non-solvable case is predictably more complicated.

Theorem 1.2.35 ([LW07; LW05; LW03; MSW88]). *If G is a non-solvable group, then $\Delta(\text{cd})$ can have up to three connected components. If $\Delta(\text{cd})$ is connected, then its diameter is at most 3. Otherwise one connected component is an isolated vertex. If $n(\Delta(\text{cd})) = 2$, it is possible that the other component has diameter 2, rather than being complete as in the solvable case.*

The cases where $\Delta(\text{cd})$ is disconnected were classified in [Lew01] for solvable groups, and in [LW03; LW05] for non-solvable groups. The only groups with disconnected $\Delta(\text{ccs})$ are quasi-Frobenius with abelian kernel and complement as noted in Theorem 1.2.40.

Theorem 1.2.36 ([Itô53; Dol95]). *If p and q are not connected in $\Delta(\text{ccs}(G))$, then G is either p-nilpotent or q-nilpotent. If G is solvable, then the Sylow p-subgroups and Sylow q-subgroups are abelian.*

Theorem 1.2.37 ([CD09]). *For a given group G, $\Delta(\text{cd}(G))$ is a subgraph of $\Delta(\text{ccs}(G))$.*

We now consider the common divisor graphs.

Theorem 1.2.38 ([Lew08]). *The graph $\Gamma(\text{cd})$ has at most 3 connected components.*

1. *If* $n(\Gamma(\mathrm{cd})) = 3$*, then* G *is non-solvable and each component is an isolated vertex.*

2. *If* $n(\Gamma(\mathrm{cd})) = 2$ *and* G *is non-solvable, then one component is an isolated vertex and the other has diameter at most* 2*.*

3. *If* $n(\Gamma(\mathrm{cd})) = 2$ *and* G *is solvable, then one component is complete and the other has diameter at most* 2*.*

Theorem 1.2.39 ([McV04b; McV04a])**.** *If* $\Gamma(\mathrm{cd})$ *is connected, then the diameter of* $\Gamma(\mathrm{cd})$ *is at most* 3 *with examples showing that this is best possible for both the solvable and non-solvable cases.*

Theorem 1.2.40. *[Kaz81; BHM90; CHM93; FA87] Let* G *be a group, then* $n(\Gamma(\mathrm{ccs})) \leq 2$

1. $n(\Gamma(\mathrm{ccs})) = 2$ *if and only if* G *is quasi-Frobenius with abelian kernel and complement. In this case both connected components are isolated vertices.*

2. $\operatorname{diam}\Gamma(\mathrm{ccs}) \leq 3$ *if* $\Gamma(\mathrm{ccs})$ *is connected.*

3. *If* G *is a non-abelian simple group, then* $\Gamma(\mathrm{ccs}(G))$ *is complete.*

4. *If* G *is a nontrivial perfect group, then* $\Gamma(\mathrm{ccs}(G))$ *is connected of diameter at most* 2*.*

In fact, groups for which $\Gamma(\mathrm{ccs})$ is not complete have been characterized.

Theorem 1.2.41 ([Ada+96])**.** $\Gamma(\mathrm{ccs})$ *is not a complete graph if and only if there exist subgroups* A *and* B *and a set of primes* π *such that*

1. $G = AB$*.*

2. $C_G(A) > Z(G)$*.*

3. $C_G(B) > Z(B)$*.*

4. $|G|_\pi \mid |A|$ *and* $|G|_{\pi'} \mid |B|$*, and* A *and* B *are minimal with respect to this property.*

The following result may be unexpected given that $\Gamma(\text{ccs})$ is complete for simple groups, and $\Delta(\text{cd})$ is complete for most simple groups.

Theorem 1.2.42 ([Bia+07]). *If $\Gamma(\text{cd})$ is complete, then G is solvable.*

There are various generalizations of these graphs defined, for example, by restricting to certain subsets of $\text{cd}(G)$ or $\text{ccs}(G)$. However, the results already included are sufficient to give a flavor of theorems found in the literature.

1.3 Some Dual Results

In this section we prove two results dual to some in the literature. These results were first published in [AH13]. Robinson showed in [Rob09] that the character degrees are determined by knowing, for all n, the number of ways that the identity can be expressed as a product of n commutators. Earlier, in [Str92], Strunkov showed that the existence of characters of p-defect 0 can be determined by counting solutions to equations involving commutators and conjugates.

Robinson is able to determine *all* character degrees by knowing how many ways the identity can be represented as a product of commutators. Strunkov, on the other hand, determines information about p-defects but only requires counting modulo p.

Theorem 1.3.1 ([Rob09]). *Given a finite group G, knowing the number of solutions, for $n = 1, 2, \ldots, |G|$, to equations $1 = [a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$ determines the character degrees (with multiplicity) of G.*

If instead, the equations are of the form $1 = a_1^2 b_1^2 a_2^2 b_2^2 \cdots a_n^2 b_n^2$ then the degrees of real characters are obtained.

Theorem 1.3.2 ([Str91]). *Let G be a finite group and S a Sylow p-subgroup of G. Let $f(x_1, \ldots, x_k, u_1, \ldots, u_l)$ be a function on G that it is the product of elementary functions*

$[x_i, x_{i+1}]$ and $u_j^{x_j}$ where $x_i \in G$ and $u_j \in S$. Moreover, let $k \geq 2$ and let each variable appear in a single elementary function. Then G has a p-block of defect 0 if and only if the number of solutions to $g = f(x_1, \ldots, x_k, u_1, \ldots, u_l)$ is not divisible by $p|S|^l$ for some $g \in G$.

If f contains at least one elementary multiplier of the form x_j^2, then the existence of real characters with p-defect 0 is determined instead.

In particular the existence of a p-block of defect 0 is equivalent to the fact that the number of solutions to $g = [x_1, x_2]$ is coprime to p for some $g \in G$.

We prove analogous theorems to those of Robinson and Strunkov, showing that knowledge of character multiplication is enough to determine information about conjugacy class sizes. This shows that, in this sense at least, multiplication of characters is dual to that of conjugacy classes.

We first give a few definitions. Let $\pi = \sum_{\chi \in \mathrm{Irr}(G)} \chi\overline{\chi}$ be the permutation character of G acting on itself via conjugation, and let $\gamma_n(\varphi)$ denote the multiplicity of φ in π^n. Similarly, let $\psi = \sum_{\chi \in \mathrm{Irr}(G)} \chi^2$ and $\delta_n(\varphi)$ be the multiplicity of φ in ψ^n. Recall that a conjugacy class $\mathcal{K}$ has p-defect 0 if $|\mathcal{K}|_p = |G|_p$.

Theorem 1.3.3. *The conjugacy class sizes of G are determined by knowing $|G|$, and $\gamma_n(1_G)$ for $n = 1, 2, \ldots, |G|$. Knowing $\delta_n(1_G)$ instead gives the sizes of real conjugacy classes.*

Theorem 1.3.4. *Let $n \geq 2$. A group G has a conjugacy class of p-defect 0 if and only if $\gamma_n(\varphi)$ is not divisible by p for some irreducible character φ. Likewise, G has a real class of p-defect 0 if and only if $\delta_n(\varphi)$ is coprime to p for some $\varphi \in \mathrm{Irr}(G)$.*

Where Robinson counted the appearance of the identity in products of the form $[a_1, b_1][a_2, b_2] \cdots [a_n, b_n]$ or $a_1^2 b_1^2 a_2^2 b_2^2 \cdots a_n^2 b_n^2$, we count the appearance of the trivial character in products of the form $\chi_1\overline{\chi_1}\chi_2\overline{\chi_2}\cdots\chi_n\overline{\chi_n}$ or $\chi_1^2\chi_2^2\cdots\chi_n^2$. This is because

$$\pi^n = \Big(\sum_{\chi\in\mathrm{Irr}(G)} \chi\overline{\chi}\Big)^n = \sum_{\chi_i\in\mathrm{Irr}(G)} \chi_1\overline{\chi_1}\chi_2\overline{\chi_2}\cdots\chi_n\overline{\chi_n},$$
$$\psi^n = \Big(\sum_{\chi\in\mathrm{Irr}(G)} \chi^2\Big)^n = \sum_{\chi_i\in\mathrm{Irr}(G)} \chi_1^2\chi_2^2\cdots\chi_n^2.$$

Similarly, Strunkov equates the existence of (real) characters of p-defect 0 to the existence of a group element such that the multiplicity of its appearance in certain products is not divisible by p. In the simplest case his products take the same form as those of Robinson. Our analog states that G has a (real) conjugacy class of p-defect 0 if and only if there exists an irreducible character such that the multiplicity of its appearance in certain products is not divisible by p.

Our proof of Theorem 1.3.3 is very different from that of Robinson, though the proof of Theorem 1.3.4 is similar to Strunkov's. We recall the statements for convenience.

Theorem 1.3.3. The conjugacy class sizes of G are determined by knowing $|G|$, and $\gamma_n(1_G)$ for $n = 1, 2, \ldots, |G|$. Knowing $\delta_n(1_G)$ instead gives the sizes of real conjugacy classes.

Proof. First, note that $\pi(g) = |C_G(g)| = |G|/|g^G|$. Consider the multiplicity of the trivial character in π^n:

$$[1_G, \pi^n] = \frac{1}{|G|}\sum_{\mathcal{K}}|\mathcal{K}|1_G(g_{\mathcal{K}})\overline{\pi^n(g_{\mathcal{K}})}$$
$$= \sum_{\mathcal{K}}\frac{|\mathcal{K}|}{|G|}\Big(\frac{|G|}{|\mathcal{K}|}\Big)^n = \sum_{\mathcal{K}}\Big(\frac{|G|}{|\mathcal{K}|}\Big)^{n-1}$$

where the sum is over all conjugacy classes $\mathcal{K}$, and $g_{\mathcal{K}} \in \mathcal{K}$.

Let a_i be the number of conjugacy classes of size i and $C_i = \frac{|G|}{i}$. By reformulating the equations above, the equations

$$\begin{aligned}
[1_G, \pi] &= \sum a_i \\
[1_G, \pi^2] &= \sum a_i C_i \\
[1_G, \pi^3] &= \sum a_i C_i^2 \\
&\vdots
\end{aligned}$$

are seen to hold. Clearly $a_i = 0$ for all $i > |G|$, so the sums are finite. Suppose that the $[1_G, \pi^n]$ are given, and view each line as having variables a_i with known coefficients C_i^j. Considering the first $|G|$ of them gives a set of linear equations. There is a unique solution since the coefficient matrix is of Vandermonde type, hence non-singular. Thus, the sequence $[1_G, \pi^n]$ for $n = 1, 2, \ldots, |G|$ determines the conjugacy class sizes of G.

Note that

$$\begin{aligned}
\psi(g) &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)^2 \\
&= \sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(g^{-1})} \\
&= \begin{cases} |C_G(g)| & \text{if } g \text{ is a real element} \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

is essentially π above, but restricted to real classes.

The proof follows exactly the same as before, except the sum

$$[1_G, \psi^n] = \sum_{\mathcal{K} = \mathcal{K}^{-1}} \left(\frac{|G|}{|\mathcal{K}|} \right)^{n-1}$$

is over real classes, and therefore only determines their class sizes. ■

Note that the multiplicity of an irreducible character in π or ψ is given by row sums in the character table

$$[\varphi, \pi] = \sum_{\mathcal{K}} \varphi(g_{\mathcal{K}});$$

$$[\varphi, \psi] = \sum_{\mathcal{K}=\mathcal{K}^{-1}} \varphi(g_{\mathcal{K}}).$$

We now prove a partial analog of Strunkov's theorem.

Theorem 1.3.4. Let $n \geq 2$. A group G has a conjugacy class of p-defect 0 if and only if $\gamma_n(\varphi)$ is not divisible by p for some irreducible character φ. In the same way, G has a real class of p-defect 0 if and only if $\delta_n(\varphi)$ is coprime to p for some $\varphi \in \mathrm{Irr}(G)$.

Proof. Fix $n \geq 2$, and consider the following equation for $\varphi \in \mathrm{Irr}(G)$:

$$\gamma_n(\varphi) = [\varphi, \pi^n] = \frac{1}{|G|} \sum_{\mathcal{K}} |\mathcal{K}| \varphi(g_{\mathcal{K}}) \overline{\pi^n(g_{\mathcal{K}})} = \sum_{\mathcal{K}} \left(\frac{|G|}{|\mathcal{K}|} \right)^{n-1} \varphi(g_{\mathcal{K}}).$$

It is a weighted sum of the row of φ in the character table. If G has no class of p-defect 0, then all coefficients $|G|/|\mathcal{K}|$ are divisible by p, and so are $\gamma_n(\varphi)$ for every φ. The weights at p-singular columns are always divisible by p.

Consider now the above equations mod p and suppose that the sums are 0 for all $\varphi \in \mathrm{Irr}(G)$. That is, there is a mod p combination of the p-regular columns of the character table that gives the all zero column. Every Brauer character η is a $\mathbb{Z}$-linear combination of ordinary characters [Nav98, Corollary 2.16], and so the same linear combination of the columns of the Brauer character table is also zero. But the columns of the Brauer character table are linearly independent over k, an algebraically closed field of characteristic p [Nav98, Theorem 1.19], and so a nontrivial combination of them cannot be zero. Consequently all weights are divisible by p, as required.

All the same arguments hold for real classes when π is replaced by ψ. ∎

Since $\pi^n \psi^m = \psi^{n+m}$, information about real classes (for both theorems) is determined by counting over products of the form

$$|\chi_1|^2 |\chi_2|^2 \cdots |\chi_n|^2 \chi_{n+1}^2 \cdots \chi_{n+m}^2$$

as long as $m \geq 1$ and $n + m \geq 2$.

Theorem 1.3.4 is not a complete analog of Strunkov's because we only include an analog for commutators (or squares), not for conjugates of elements of S. One must first determine what the analog of elements of S would be. The conjugates of elements in S comprise the conjugacy classes of p-elements.

Let ε be a primitive $|G|$th root of unity and R the algebraic integers of $\mathbb{Q}[\varepsilon]$. Let M be a maximal ideal of R containing the prime p. The element $g \in G$ is a p-element if and only if for all $\chi \in \mathrm{Irr}(G)$, $\chi(g) \equiv \chi(1) \bmod M$. See [Isa76, Theorem 8.20].

An analog for characters based on similar congruence criteria is that χ is in the principal block B_0 of G if and only if $\frac{\chi(g)|g^G|}{\chi(1)} \equiv |g^G| \bmod M$ for all $g \in G$. The analog of $u_j^{x_j}$ would be $|\chi|^2\varphi$. However, the corresponding result does not hold.

As a counter example, consider S_3 for $p = 3$. It has a unique 3-block B_0, and the class of transpositions is of 3-defect 0. Calculating

$$\gamma(\psi) = \sum_{\substack{\chi_1,\chi_2,\chi_3 \in \mathrm{Irr}(G) \\ \varphi \in \mathrm{Irr}(B_0)}} [\psi, |\chi_1\chi_2|^2 |\chi_3|^2 \varphi]$$

(the analog of $[x_1, x_2]u^{x_3}$) gives results divisible by $9 = 3|G|_3$ for all $\psi \in \mathrm{Irr}(G)$. One might consider using $\sum_{\varphi \in \mathrm{Irr}(B_0)} \varphi(1)^2$ (or its p-part) in place of $|S| = |G|_p$, but under these conditions there are other groups which do not satisfy the theorem (*e.g.*, the dihedral group of order 12). So it seems that, if it exists, the correct analog is not the principal block. See, however, Corollary 3.2.5 where it *is* the correct analog.

Chapter 2

Transpositions of Character Tables

2.1 Introduction

Although the number of conjugacy classes and irreducible characters is always the same, there is usually not a "natural" bijection between the two. If there were a natural bijection, it might help us understand the quasi-duality between them. We seek such a bijection by studying groups G whose character table is the transpose of the character table of some other group H. That is, when the transpose of a character table is itself a character table. This gives us a "natural" bijection between the irreducible characters of G and the conjugacy classes of H, and vice versa.

The trivial conjugacy class is the only column of the character table consisting of all positive integers, and hence must correspond in the transpose to the trivial character which is always a row of ones. This implies that all character degrees are 1, which is only true for abelian groups. In fact, abelian groups are $\mathbb{Z}$-modules, and for $\mathbb{Z}$-modules there is a concept of duality $M \mapsto M^* = \mathrm{Hom}(M, \mathbb{C})$. That $M \cong M^*$ follows from the structure of finite abelian groups.

We now explore one way to extend this notion of duality to non-abelian groups.

Definition 2.1.1. We say that a group G with character table X is **transposable** if there exist non-negative diagonal integer matrices D and N such that $\tilde{X} = (D^{-1}XN)^T$ is the character table of some group G^T. We also say that G^T is a **transpose group** of G.

Remark 2.1.2. In our definition we stipulated that the matrices D and N must be matrices of non-negative integers. It is clear that it is sufficient to consider such matrices. In fact, D is the diagonal matrix consisting of the character degrees of G, and N is of the degrees of G^T.

With this definition we shall find that, although G^T is not unique, its character table is. We also show that G and G^T have dual normal subgroup lattices, and that the lower central series of G is "dual" to the upper central series of G^T. These two results can be used to prove that if G is solvable and transposable, then G is nilpotent. However, a very different proof by Okuyama, which we give as Corollary 3.2.5, shows that all transposable groups are nilpotent without requiring the assumption of solvability.

2.2 Basic Results

Of immediate concern are the possible values for the new character degrees. Perhaps unsurprisingly, they are unique and given by the square roots of the conjugacy class sizes.

Proposition 2.2.1. *Let X be the character table of a finite group G. Let D be the diagonal matrix with the character degrees of G along the diagonal (in the same order as they appear in X). Let N be an arbitrary diagonal matrix such that $\tilde{X} = (D^{-1}XN)^T = NX^TD^{-1}$ is the character table of some group G^T. Then N^2 is the diagonal matrix with entries equal to the conjugacy class sizes of G (in the same order as they appear in X).*

Proof. If $\tilde{X}$ is the character table of a group, then it must satisfy the orthogonality relations, in particular column orthogonality. The columns of $\tilde{X}$ are indexed by irreducible characters of G, and the rows by conjugacy classes. We indicate by d_i the new character degrees, *i.e.,* the diagonal entries of N, and by g_i a representative of the ith conjugacy class of G (as indexed by X). Assume that g_1 is the identity element, hence $d_1 = 1$, and denote by 1_G the trivial character of G. Let n be the number of irreducible characters of G.

The new character table $\tilde{X}$ has $d_i \frac{\chi(g_i)}{\chi(1)}$ in row i, column χ.

$$
\begin{array}{c|cccc|}
 & 1_G & & \chi & \\
\hline
1 & 1 & \dots & \frac{\chi(g_1)}{\chi(1)} & \dots \\
 & \vdots & & \vdots & \\
d_i & d_i & \dots & d_i \frac{\chi(g_i)}{\chi(1)} & \dots \\
 & \vdots & & \vdots & \\
d_n & d_n & \dots & d_n \frac{\chi(g_n)}{\chi(1)} & \dots \\
\hline
\end{array}
$$

Column orthogonality of $\tilde{X}$ implies that for $\chi \neq 1_G$

$$0 = \sum_{i=1}^{n} d_i \frac{\chi(g_i)}{\chi(1)} \overline{d_i} = \frac{1}{\chi(1)} \sum_{i=1}^{n} d_i^2 \chi(g_i) = \sum_{i=1}^{n} d_i^2 \chi(g_i),$$

which constrains the possible values for the d_i. Letting $k_i = d_i^2$, we obtain a system of $n-1$ linear equations in $n-1$ unknowns (since $d_1 = 1$). From the row orthogonality relations for X, we know that $k_i = \left|g_i^G\right|$ is a solution. Since the equations are simply $n-1$ of the rows of X, they are linearly independent and so the solution is unique. ∎

Corollary 2.2.2. *If a finite group G is transposable then the conjugacy classes of G must all have square size.*

Proof. Since the d_i are the character degrees of the dual character table they must be integers which can only be the case when $d_i^2 = k_i$ is a square. ■

In other words, if $\tilde{X}$ is a character table obtained from X by dividing each row by the character degree and multiplying columns by positive integers, then the columns must be multiplied by the square root of the conjugacy class sizes. It is convenient to define the **weighted character table** to be the character table with the columns multiplied by the square root of the conjugacy class sizes. This definition allows us to calculate the weighted character table (which is straightforward given the character table) and compare the transpose of this matrix with the weighted character table of another group to determine if they are transpose groups. Likewise, it would be enough to consider character tables divided by character degrees, which we call **normalized character tables**. In this case it is more difficult to simply "read off" data from the table, but they are also convenient, particularly for proofs. From a normalized character table it is easy to determine the character degrees, thereby returning to an ordinary character table, since by row orthogonality

$$\frac{|G|}{\chi(1)^2} = \sum_g \frac{\chi(g)}{\chi(1)} \frac{\overline{\chi(g)}}{\chi(1)}.$$

Suppose that the character tables for two groups G, H are such that their transposes are character tables for some groups G^T, H^T respectively. It is clear from the construction of character tables of direct products that the character table of $G \times H$ is the transpose of $G^T \times H^T$. Because transposability of character tables is closed under forming direct products, one might hope that the converse is true, that is, that it suffices to check the direct factors of the group. This is, in fact, the case.

Proposition 2.2.3. *Suppose that M is the character table of a group G and factors as the Kronecker product of two matrices X and Y such that the first row of both X and Y consists of ones and the first column of positive integers. Then G is a nontrivial direct product of groups* *having character tables X and Y.*

Proof. By assumption of the structure of M, we have character degrees $a_i = (X)_{i,1}$, $b_i = (Y)_{i,1}$ such that $a_1 = b_1 = 1$,

$$X = \begin{pmatrix} 1 & 1 & \cdots & \\ b_2 & * & & \\ \vdots & & & \end{pmatrix}, \qquad Y = \begin{pmatrix} 1 & 1 & \cdots & \\ a_2 & * & & \\ \vdots & & & \end{pmatrix},$$

and M has the form

	$\mathcal{A}$			
A	$1 \quad 1 \quad \ldots$	$1 \quad 1 \quad \ldots$	$1 \quad 1 \quad \ldots$	
	a_2	a_2	a_2	B
	$\vdots$	$\vdots$	$\vdots$	
A	$b_2 \quad b_2 \quad \ldots$			
A	$b_3 \quad b_3 \quad \ldots$		$\ddots$	
				$\vdots$
	$\mathcal{B}$	$\mathcal{B}$	$\mathcal{B}$	$\ldots$

as hypothesized. Note that the upper left block is the matrix Y, and the upper left entries of each block form the matrix X.

Let $\mathcal{A}$ be the subset of conjugacy classes consisting of the first column of blocks. Also, let A be the subset of rows consisting of the first row of each block as marked. We claim that the intersection of the kernels of these characters

$$N = \bigcap_{\chi \in A} \ker \chi = \ker \bigoplus_{\chi \in A} \chi$$

is the normal subgroup containing exactly the conjugacy classes in $\mathcal{A}$.

It is clear that $N \supset \mathcal{A}$ since, when restricted to $\mathcal{A}$, the characters are all integer multiples of the trivial character. Suppose $N \supsetneq \mathcal{A}$, then some column of M outside of $\mathcal{A}$ is such that the first entry in the ith block is given by b_i for all i. Since these entries are $1 \cdot b_{i,j}$, it must be that $b_{i,j} = b_i$ for $j > 1$ and all i. This is impossible since the columns of M are linearly independent and so the columns of X must be as well. Thus $N = \mathcal{A}$.

Similarly, let B be the first block of rows and $\mathcal{B}$ the first column in each block. The intersection of kernels $H = \bigcap_{\chi \in B} \ker \chi = \ker \bigoplus_{\chi \in B} \chi$ corresponds to the subset $\mathcal{B}$ of conjugacy classes. In particular N and H are normal subgroups with trivial intersection.

We now determine the character tables of the factor groups G/H and G/N. To find the character table of G/N (see for example [Isa76, Lemma 2.22]), take the submatrix of characters with kernel containing N and delete duplicate columns. Since the first row of Y is all ones, this submatrix will be the Kronecker product $[1, 1, \dots] \otimes X$. Once duplicate columns are removed it will be exactly X, and in the same way the character table for G/H is Y.

Calculating the order of N and H can be done by summing the squares of the character degrees:

$$|G : H| = |G/H| = \sum_i a_i^2$$

$$|G : N| = |G/N| = \sum_j b_j^2$$

$$|NH| = |N||H| = \frac{|G|}{|G/N|} \frac{|G|}{|G/H|}$$

$$= \frac{|G|^2}{\sum_j b_j^2 \sum_i a_i^2} = \frac{|G|^2}{\sum_{i,j}(a_i b_j)^2}$$
$$= \frac{|G|^2}{|G|} = |G|.$$

Finally, $G \cong N \times H$ since (1) N and H are normal in G, (2) they have trivial intersection, and (3) $G = NH$. ∎

Proposition 2.2.4. *If $G \times H$ is transposable then so are G and H.*

Proof. Let M be the character table of $G \times H$ written as $M = X \otimes Y$, where X and Y are the character tables of G and H respectively. Then the (matrix) transpose of M is $X^T \otimes Y^T$ and by assumption is a character table of some group Γ after proper multiplication and division of character degrees. This multiplication splits across the product so that X^T is the character table of some group G_0 and Y^T is that of some other group H_0. That is, G and H are transposable. ∎

2.3 Self-dual Groups

The concept of a self-dual group has appeared in a series of papers by Hanaki and Okuyama [Oku13; HO97; Han97; Han96a; Han96b]. They call a group self-dual if (after a suitable rearrangement)

$$\frac{\left|x_j^G\right| \chi_i(x_j)}{\chi_i(1)} = \chi_j(1)\chi_j(x_i)$$

for $\chi_i \in \mathrm{Irr}(G)$ and $x_i \in \mathrm{Rep}(G)$. This condition is equivalent to the condition that the group association scheme is self-dual. It is also equivalent to being transposable with $G^T = G$, which is easily seen after noting that $\chi_j(1)^2 = \left|x_j^G\right|$ must hold. This last condition is called the B-condition in [Han96a] after E. Bannai who studied it in [Ban93]. In that paper, Bannai studies generalizations of fusion algebras from mathematical physics and shows that they are in one-to-one correspondence with "character algebras," which are a generalization of the character algebras obtained from finite groups.

The majority of Hanaki's and Okuyama's papers are spent constructing examples of self-dual groups which we include in Chapter 5. In an unpublished paper [Oku13], Okuyama proved that self-dual groups must be nilpotent. Professor Okuyama was kind enough to send us his proof, and we include it as Section 3.2 slightly generalized to transposable groups.

Chapter 3

Properties of Transposable Groups

Transposable groups must have square conjugacy class sizes as we have shown. In this chapter we investigate other properties which transposable groups satisfy. The most important of these is a correspondence between the normal subgroups of G and G^T. Much of this chapter, as well as the examples from Chapter 5 are included in the forthcoming paper [AHO12].

3.1 Normal Subgroup Correspondences

We start with a simple observation.

Proposition 3.1.1. *Let G be a transposable group and let $A = G^T/(G^T)'$ be the abelianization of G^T. Then $A \cong Z(G)$.*

Proof. First, recall that the linear characters are precisely those whose kernel contains the commutator subgroup. Thus, we can calculate the character table of A by taking the linear characters of G^T and deleting duplicate columns. There are exactly enough duplicate columns to make the table square.

The linear characters of G^T correspond to the central classes of G for these classes have size 1. Note that the number and size of conjugacy classes do not change when we restrict our attention to the character table of $Z = Z(G)$. In order to calculate the character table of Z, take the character table of G and divide by the character degrees. Since all the characters of G are homogeneous on Z, each row in the resulting table is an irreducible character of Z.

Next, remove duplicate rows. These will be the same as those columns removed when calculating the character table of A. The rows now correspond to distinct characters, and there are enough to make the table square. Hence the character table of Z is the transpose of that of A. Since abelian groups are determined by their character tables, we have that $Z \cong A$. ■

In fact we have nearly proven a more general theorem. Recall that a character is called **homogeneous** if it is a multiple of an irreducible character. A character $\chi \in \mathrm{Irr}(G)$ is called **quasi-primitive** if χ_N is homogeneous for all $N \lhd G$.

Proposition 3.1.2. *Let G be a transposable group, and let $N \lhd G$ be such that all irreducible characters of G are homogeneous when restricted to N. Further, assume that there is no fusion in N; that is, if $n_1 = n_2^g$ for $n_1, n_2 \in N$, $g \in G$, then g can be chosen to be in N. Let N^T be the set of characters of G^T corresponding to the conjugacy classes of N. Then the character table of N is the transpose of the character table of $H = G^T / \ker N^T$.*

Proof. The only thing which does not follow immediately from the previous proof is that the character degrees of N match the square roots of the conjugacy class sizes of H. This follows from the orthogonality relations and the lack of fusion. ■

In light of the above proposition, it is tempting to consider groups in which all characters are quasi-primitive. In the case of solvable groups, these turn out to be the abelian groups [Isa76, Corollary 6.6] for which the result was obvious.

While there is no correspondence which preserves (transposes of) character tables for all $N \lhd G$, we can generalize the correspondence to all normal subgroups. For certain special subgroups, namely those of the upper and lower central series, we are able to retain some structural information.

Lemma 3.1.3. *Given two normal subgroups $N_1, N_2 \lhd G$ let N be the join $N = N_1 \vee N_2 = N_1 N_2$ in the normal subgroup lattice. It can be determined from the character table by taking the union of the conjugacy classes of N_1 and N_2 and finding the set $\mathcal{N}$ of characters whose kernels contain these classes. Then the classes in $K = \ker \mathcal{N}$ is the join $N = N_1 N_2$.*

Proof. The join $N_1 N_2$ must contain all of the conjugacy classes of both N_1 and N_2 (which K does), and it is the minimal such, which K is by construction. ■

Proposition 3.1.4. *Let G be a transposable group and G^T one of its transpose groups. Then for every normal subgroup $N \lhd G$, there is a normal subgroup $N^T \lhd G^T$ such that $|G/N| = \left|N^T\right|$ (equivalently $|N| = \left|G^T/N^T\right|$). Furthermore $(N_1 N_2)^T = N_1^T \cap N_2^T$, so that the lattice of normal subgroups of G is the dual of that of G^T including orders of subgroups.*

*We say that N **corresponds** to N^T.*

Proof. Consider some normal subgroup $N \lhd G$ as a collection of conjugacy classes. It also can be thought of in terms of the set $\mathcal{N}$ of irreducible characters whose kernels contain N. In the transposed character table these concepts are switched: the conjugacy classes of N correspond to the characters whose kernel make up N^T, and the characters defining N become the conjugacy classes of N^T.

Consider the normalized character table, and note that an entry is in the kernel of a character if its value is 1. In this way kernel entries are easily seen to remain kernel entries after transposition.

We now determine the orders of N^T and G/N. The character table of G/N is easily determined from the characters in $\mathcal{N}$ by removing duplicate columns. In particular this leaves the character degrees intact, so that $|G/N| = \sum_{\chi\in\mathcal{N}} \chi(1)^2$. The characters in $\mathcal{N}$ become the conjugacy classes of N^T whose order can be computed by summing the sizes of its conjugacy classes. But this is simply $\left|N^T\right| = \sum_{\chi\in\mathcal{N}} \chi(1)^2$ since the squares of the character degrees in G are the conjugacy class sizes in G^T.

To prove that $N_1^T \cap N_2^T = (N_1N_2)^T$, observe that conjugacy classes of $N_1^T \cap N_2^T$ are given by the intersection of the set of characters whose kernels are N_1 and N_2 respectively. The intersection of these sets consists of the irreducible characters whose kernel contains both N_1 and N_2, and it follows from Lemma 3.1.3 that $N_1^T \cap N_2^T = (N_1N_2)^T$. ■

We should not be too surprised by this result since characters give information about quotient groups, and conjugacy classes about normal subgroups. Interchanging the two concepts might be expected to interchange normal subgroups and quotients.

Because they can be determined from the normal subgroup lattice (when augmented with order information), transposing the character table preserves commutativity, nilpotency, π-separability, (super-)solvability, and simplicity of the underlying group.

3.1.1 Central Series

Recall that the lower (descending) and upper (ascending) central series are defined as

$$\begin{aligned} \gamma_1(G) &= G & Z_0(G) &= 1 \\ \gamma_i(G) &= [\gamma_{i-1}(G), G]; & Z_i(G)/Z_{i-1}(G) &= Z(G/Z_{i-1}(G)). \end{aligned}$$

One way to determine $Z_i(G)$ is to locate the conjugacy classes of $Z_{i-1}(G)$ and then find conjugacy classes $\mathcal{K}$ such that $[\mathcal{K}, G] \subset Z_{i-1}(G)$. The following proposition gives us a way to do that using only the character table.

Proposition 3.1.5 ([Isa76, Problem 3.10]). *Let G be a group and fix $g \in G$. Then $h \in G$ is conjugate to $[g, g']$ for some $g' \in G$ if and only if*

$$n(g,h) = \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(g)|^2 \overline{\chi(h)}}{\chi(1)} \neq 0. \tag{3.1}$$

According to this we have

$$g \in Z_i(G) \Leftrightarrow n(g,h) = 0 \, \forall h \notin Z_{i-1}(G). \tag{3.2}$$

We now translate this description into a condition within G^T. Let $\mathcal{K}_g$ denote the G-conjugacy class of g, and φ_g the character of G^T which corresponds to this class. If χ is an irreducible character of G, then $\mathcal{K}_\chi$ will denote the corresponding conjugacy class of G^T, and x_χ a representative of this class. With this notation we have the identity

$$\frac{\chi(g)}{\chi(1)} = \frac{\varphi_g(x_\chi)}{\varphi_g(1)}.$$

Substituting into (3.1) gives

$$\sum_{\mathcal{K}_\chi} \frac{\left|\varphi_g(x_\chi)\right|^2 \frac{\chi(1)^2}{\varphi_g(1)^2} \overline{\varphi_h(x_\chi)} \frac{\chi(1)}{\varphi_h(1)}}{\chi(1)} \neq 0$$

$$\sum_{\mathcal{K}_\chi} \frac{\left|\varphi_g(x_\chi)\right|^2 \overline{\varphi_h(x_\chi)} \chi(1)^2}{\varphi_g(1)^2 \varphi_h(1)} \neq 0$$

and since $\varphi_g(1)^2 \varphi_h(1)$ is constant

$$\sum_{\mathcal{K}_\chi} \left|\varphi_g(x_\chi)\right|^2 \overline{\varphi_h(x_\chi)} |\mathcal{K}_\chi| \neq 0$$

$$\left|G^T\right| [\varphi_g \overline{\varphi_g}, \varphi_h] \neq 0$$

$$[\varphi_g \overline{\varphi_g}, \varphi_h] \neq 0$$

where [,] is the usual inner product on characters of G^T.

Now denote $n^T(\varphi, \psi) = [\varphi\overline{\varphi}, \psi]$. The following proposition claims

$$\ker \varphi \supseteq \gamma_i(G) \Leftrightarrow n^T(\varphi, \psi) = 0 \, \forall \psi, \ker \psi \not\supseteq \gamma_{i-1}(G). \tag{3.3}$$

Proposition 3.1.6. *Let G be a finite group and $\varphi \in \mathrm{Irr}(G)$ an irreducible character. All irreducible components of $\varphi\overline{\varphi}$ contain $\gamma_{i-1}(G)$ in their kernel if and only if the kernel of φ contains $\gamma_i(G)$.*

Proof. Let U be a module affording φ, so that $|\varphi|^2$ is the character of $\mathrm{Hom}(U, U)$. We need to prove that the kernel of U contains $\gamma_i(G)$ if and only if every simple submodule of $\mathrm{Hom}(U, U)$ has kernel containing $\gamma_{i-1}(G)$, that is if and only if $\mathrm{Hom}(U, U)$ has kernel containing $\gamma_{i-1}(G)$.

If $\gamma_i(G) \subset \ker U$, then every $c \in \gamma_{i-1}(G)$ is central with respect to the action on U. Let $\mu \in \mathrm{Hom}(U, U)$ and $c \in \gamma_{i-1}(G)$. We wish to prove that c fixes μ, *i.e.*, $\mu c = \mu$. Consider the action on a vector $u \in U$, by definition

$$(\mu c)(u) = \mu(uc^{-1})c.$$

Now, the action of c is central on U, so it's equivalent to multiplication by a scalar λ

$$= \mu(u\lambda^{-1})\lambda = \mu(u).$$

This is true for every μ and every u, so that $\ker \mathrm{Hom}(U, U) \supseteq \gamma_{i-1}(G)$.

To prove the converse, suppose $\ker \mathrm{Hom}(U, U) \supseteq \gamma_{i-1}(G)$. This means that for

$c \in \gamma_{i-1}(G)$ we have $\mu c = \mu$, that is

$$\mu(u) = (\mu c)(u) = \mu(uc^{-1})c.$$

Then

$$\mu(u)c^{-1} = \mu(uc^{-1})$$

for all μ and all u, so the action of c commutes with every μ. Hence, the action of c is central in U. This is true for every c in $\gamma_{i-1}(G)$, so the kernel of U contains $[\gamma_{i-1}(G), G] = \gamma_i(G)$ as claimed. ■

Theorem 3.1.7. *Given a transposable group G, the (abelian) factors $Z_i(G)/Z_{i-1}(G)$ are isomorphic to $\gamma_i(G^T)/\gamma_{i+1}(G^T)$ for all i.*

Proof. From Propositions 3.1.5 and 3.1.6, there is a correspondence between the conjugacy classes of the upper central series of G and the irreducible characters defining the lower central series of G^T. Due to the special nature of the subgroups involved, we are able to determine the character tables (and hence isomorphism type) of the central series factors, from the character table of G.

To find the character table of $Z_i(G)/Z_{i-1}(G)$, restrict attention to the characters of G which contain $Z_{i-1}(G)$ in their kernel, and the conjugacy classes of $Z_i(G)$. This corresponds to finding the character table of $G/Z_{i-1}(G)$, and then restricting to $Z_i(G)/Z_{i-1}(G)$. As in Proposition 3.1.1, we simply divide by character degrees and then remove duplicate columns and duplicate rows to find the character table of $Z_i(G)/Z_{i-1}(G)$.

The character table of $\gamma_i(G^T)/\gamma_{i+1}(G^T)$ is found in a completely dual manner. This time we restrict attention to the conjugacy classes of $\gamma_i(G^T)$ and characters whose kernel contains $\gamma_{i+1}(G^T)$. These are the same rows as columns before, and vice versa. Again, we divide by character degrees and then remove duplicate rows and columns, leading to the transpose of the character table of $Z_i(G)/Z_{i-1}(G)$. Since they are abelian groups, $Z_i(G)/Z_{i-1}(G)$ and $\gamma_i(G^T)/\gamma_{i+1}(G^T)$ are isomorphic. ■

Corollary 3.1.8. *The Fitting subgroup and hypercenter of G coincide and they correspond to the nilpotent residual of G^T.*

Proof. It follows from the previous theorem that the hypercenter of G and the nilpotent residual of G^T correspond. From Proposition 3.1.4 the nilpotent residual corresponds to the Fitting subgroup of G. ■

Remark 3.1.9. This can also be seen by comparing formulas for the orders of the hypercenter (Theorem 1.2.19) and nilpotent residual (Theorem 1.2.18).

Corollary 3.1.10. *The solvable residual of G corresponds to the hypercenter of G^T.*

Proof. Let G be transposable. Denote by $G^{(i)^T}$ the subgroup of G^T corresponding to $G^{(i)}$ the ith term of the derived series. We prove by induction that $G^{(i)^T}$ is in the hypercenter of G^T. By Proposition 3.1.1 the case $i = 1$ holds.

Suppose that $G^{(i)^T}$ is in the hypercenter of G^T. As $G^{(i)}/G^{(i+1)}$ is abelian, every Sylow subgroup of this factor has a normal preimage in G. Hence the same holds for $G^{(i+1)^T}/G^{(i)^T}$ by Proposition 3.1.4, and thus this factor group is nilpotent. By assumption, $G^{(i)^T}$ is in the hypercenter of G^T and so $G^{(i+1)^T}$ is nilpotent and therefore in the hypercenter by Corollary 3.1.8. ■

Corollary 3.1.11. *All solvable normal subgroups are hypercentral, and all solvable quotients are nilpotent.*

Corollary 3.1.12. *If $N \lhd G$ such that* $\gcd(|N|, |G/N|) = 1$, *then N is a direct factor of G.*

Proof. By interchanging G and G^T if necessary, we can assume that N is solvable and hence in the hypercenter. Then, since $\gcd(|N|, |G/N|) = 1$, N is a direct factor. ■

Corollary 3.1.13. *If G is transposable and solvable, then G is nilpotent.*

In fact, we shall see in Corollary 3.2.5 that all transposable groups are nilpotent. This supports the intuition that transposable groups are "close" to being abelian. Interestingly, one of the transposable examples in Chapter 5 is used by Kiss and Pálfy [KP98] as an example of a nilpotent group whose normal subgroup lattice does *not* embed in the (normal) subgroup lattice of an abelian group. In this way the class of transposable groups is "larger" than merely abelian groups.

We finally remark on two more important subgroups corresponding to each other.

Proposition 3.1.14. *If G is a transposable group, then the Frattini subgroup $\Phi(G)$ corresponds to the socle.*

Proof. The Frattini subgroup is the intersection of all the maximal subgroups (which will all be normal if G is nilpotent). The socle, on the other hand, is the join of all the minimal normal subgroups. The result follows from the duality of the subgroup lattices. ∎

3.2 Nilpotency of Transposable Groups

This section is from an unpublished paper [Oku13] of Tetsuro Okuyama. In this next section we write $a \equiv b$ to mean that a is congruent to b modulo a maximal ideal M, as explained near the end of Section 1.3.

Proposition 3.2.1. *Every p-block B of a transposable group G is of full defect.*

Proof. By the definition of defect of a block B, there exists $\chi \in B$ and a conjugacy class $\mathcal{K}$ such that

$$\chi(x^{-1})\frac{|\mathcal{K}|\chi(x)}{\chi(1)} \not\equiv 0$$

for $x \in \mathcal{K}$. By the definition of transposable groups, we have that

$$\frac{|\mathcal{K}|\chi(x)}{\chi(1)} = \varphi_{\mathcal{K}}(1)\varphi_{\mathcal{K}}(x_\chi) \not\equiv 0$$

and in particular $\varphi_{\mathcal{K}}(1) \not\equiv 0$, so that $|\mathcal{K}| = \varphi_{\mathcal{K}}(1)^2 \not\equiv 0$. Therefore, B has full defect. ■

Proposition 3.2.2. *Let G be a transposable group. If $\chi \in B_0(G)$, then $\frac{|\mathcal{K}_\chi|\varphi(x_\chi)}{\varphi(1)} \equiv |\mathcal{K}_\chi|$ for all $\varphi \in \mathrm{Irr}(G^T)$.*

Proof. Since

$$\frac{|\mathcal{K}_\chi|\varphi_1(x_\chi)}{\varphi_1(1)} \equiv \frac{|\mathcal{K}_\chi|\varphi_2(x_\chi)}{\varphi_2(1)}$$

for all φ_1 and φ_2 in the same p-block, we may assume that $\varphi(1) \not\equiv 0$ by Proposition 3.2.1.

Since $\chi \in B_0(G)$, for any conjugacy class $\mathcal{K}$ of G, we have

$$\frac{|\mathcal{K}|\chi(x)}{\chi(1)} \equiv |\mathcal{K}|$$
$$\varphi_{\mathcal{K}}(1)\varphi_{\mathcal{K}}(x_\chi) \equiv \varphi_{\mathcal{K}}(1)^2$$

so that

$$\varphi_{\mathcal{K}}(x_\chi) \equiv \varphi_{\mathcal{K}}(1).$$

From this it follows that $\frac{|\mathcal{K}_\chi|\varphi(x_\chi)}{\varphi(1)} \equiv |\mathcal{K}_\chi|$. ■

Corollary 3.2.3. *If G is transposable and $\chi \in B_0(G)$ with $\chi(1) \not\equiv 0$, then $\chi(1) = 1$.*

Proof. Since $|\mathcal{K}_\chi| = \chi(1)^2 \not\equiv 0$, it follows from Proposition 3.2.2 that $\chi(1)\chi(x) = \frac{|\mathcal{K}_\chi|\varphi(x_\chi)}{\varphi(1)} \not\equiv 0$ for all $x \in G$. In particular $\chi(1)\chi(x) \neq 0$ for all $x \in G$, and so χ must be linear by a famous theorem of Burnside [Isa76, Theorem 3.15]. ■

Theorem 3.2.4 ([IS76, Corollary 3]). *Suppose that every nonlinear irreducible character of G in the principal p-block has degree divisible by p. Then G has a normal p-complement,* i.e., *is p-nilpotent.*

Corollary 3.2.5. *If G is transposable, then G is nilpotent.*

Proof. Fix a prime p. By Corollary 3.2.3, we have that the nonlinear irreducible characters in the principal block have degree divisible by p, and so it follows from 3.2.4 that G is p-nilpotent. Thus, G is p-nilpotent for all p, and therefore nilpotent. ∎

Note that the correspondence seen here between the principal p-block of G and the p-elements of G^T is *not* reflected in Theorem 1.3.4 as noted at the end of Section 1.3.

3.3 Multiplication Constants of Characters and Classes

It is well known (*e.g.*, [Isa76, Exercise 3.9]) that the character table determines multiplication of both characters and conjugacy classes. To be more precise, if $\mathcal{K}_i$ is a conjugacy class and $\hat{\mathcal{K}}_i$ its class sum, then class multiplication is given by

$$\hat{\mathcal{K}}_i \hat{\mathcal{K}}_j = \sum_\nu a_{ij\nu} \hat{\mathcal{K}}_\nu$$

for non-negative integers $a_{ij\nu}$ which can be calculated as

$$a_{ij\nu} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_\nu)}}{\chi(1)}.$$

Recall that the multiplication constants for the product of two irreducible characters are

$$b_{ij\nu} = [\chi_i \chi_j, \chi_\nu] = \frac{1}{|G|} \sum_l |\mathcal{K}_l| \chi_i(g_l) \chi_j(g_l) \overline{\chi_\nu(g_l)}.$$

Proposition 3.3.1. *The multiplication constants for characters of G are determined by the multiplication constants for conjugacy classes of G^T and the class sizes of G.*

Proof. Consider conjugacy classes $\mathcal{K}_i$ and $\mathcal{K}_j$ as characters of G^T, and compute the coefficients $b^T_{ij\nu}$. Using the correspondence $\mathcal{K}_i \leftrightarrow \varphi_i$, $\chi \leftrightarrow \mathcal{K}_\chi$, and $x_\chi \in \mathcal{K}_\chi$ as before, we have

$$\begin{aligned}
b^T_{ij\nu} &= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} |\mathcal{K}_\chi| \varphi_i(x_\chi)\varphi_j(x_\chi)\overline{\varphi_\nu(x_\chi)} \\
&= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \frac{\chi(x_i)\sqrt{|\mathcal{K}_i|}}{\chi(1)} \frac{\chi(x_j)\sqrt{|\mathcal{K}_j|}}{\chi(1)} \overline{\left(\frac{\chi(x_\nu)\sqrt{|\mathcal{K}_\nu|}}{\chi(1)}\right)} \\
&= \frac{\sqrt{|\mathcal{K}_i||\mathcal{K}_j||\mathcal{K}_\nu|}}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(x_\nu)}}{\chi(1)} \\
&= \frac{\sqrt{|\mathcal{K}_\nu|}}{\sqrt{|\mathcal{K}_i||\mathcal{K}_j|}} \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(x_\nu)}}{\chi(1)} \\
&= \frac{\sqrt{|\mathcal{K}_\nu|}}{\sqrt{|\mathcal{K}_i||\mathcal{K}_j|}} \, a_{ij\nu}. \quad \blacksquare
\end{aligned}$$

We can then apply the fact (see [Isa76, Exercise 4.12]) that for arbitrary characters $[\chi\psi, \vartheta] \leq \vartheta(1)$ to find

$$b^T_{ij\nu} = \frac{\sqrt{|\mathcal{K}_\nu|}}{\sqrt{|\mathcal{K}_i||\mathcal{K}_j|}} \, a_{ij\nu} \leq \sqrt{|\mathcal{K}_\nu|}$$

so that

$$a_{ij\nu} \leq \sqrt{|\mathcal{K}_i||\mathcal{K}_j|}$$

for transposable groups. Of course for all groups the following trivial bound holds

$$a_{ij\nu} \leq \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|\mathcal{K}_\nu|}.$$

3.4 Potential Constraints

Since conjugacy classes and irreducible characters are dual in transposable groups, we may be able to constrain conjugacy classes by using constraints on the characters (and vice versa). Such constraints could then be used to constrain the structure of transposable groups. We examine a few obvious candidates in this section. All but one of the constraints in this section are guaranteed by nilpotency, and therefore they are not useful in restricting the set of possible transposable groups any further. We include them here because they are simple questions and arise naturally.

We discussed in the introduction (see Lemma 1.2.29) the multiplication of characters (conjugacy classes) with coprime degrees (sizes).

Lemma 3.4.1. *Let x and y be elements of G such that $C_G(x)C_G(y) = G$, then $(xy)^G = x^G y^G$.*

Corollary 3.4.2. *Let x and y be elements of G such that $|x^G|$ and $|y^G|$ are coprime, then $(xy)^G = x^G y^G$. Moreover, $|(xy)^G| \geq \max\{|x^G|, |y^G|\}$, and $|(xy)^G| \mid |x^G||y^G|$.*

Based on this, the product of irreducible characters of coprime degree must be irreducible in a transposable group. But this is true for nilpotent groups, so it provides us with no new information.

We can also use some properties of character degrees to constrain the sizes of conjugacy classes. For example, $|(xy)^G| = |x^G||y^G|$ when x and y have coprime conjugacy class sizes. This is not true in general, but is true for nilpotent groups.

A classic theorem of Burnside [Isa76, Theorem 3.15] states that if $\chi \in \mathrm{Irr}(G)$ is nonlinear, then $\chi(g) = 0$ for some $g \in G$. This gives rise to another necessary condition for the character table of a group to be transposable: that it not contain any noncentral non-vanishing classes. A **non-vanishing class** is a conjugacy class $\mathcal{K}$ for which $\chi(g) \neq 0$ for g a representative of $\mathcal{K}$ and all $\chi \in \mathrm{Irr}(G)$.

There are several results about non-vanishing classes in [INW99] indicating that, in some sense, they are close to being central elements. Given that all transposable groups are nilpotent, the theorem given below is the most relevant.

Theorem 3.4.3 ([INW99, B]). *If G is supersolvable, then the non-vanishing elements of G all lie in $Z(F(G))$. In particular, if G is nilpotent, then the non-vanishing elements of G are central.*

It is easy to see that in a transposable group the characters cannot be as large as they can in an arbitrary group. But, again, this condition (in fact something stronger) is implied by nilpotency.

Proposition 3.4.4. *If G is a transposable group then $\chi(1)^2$ divides $|G|$ for every irreducible character χ. Equivalently, $|\chi(1)|_p \leq p^{a/2}$ where $|G|_p = p^a$.*

Proof. The squares of the character degrees of G are conjugacy class sizes of a transpose group G^T and must therefore divide $|G^T| = |G|$. ■

Theorem 3.4.5 ([GL99]). *A group G is nilpotent if and only if $\chi(1)^2$ divides $|G : \ker \chi|$ for all $\chi \in \mathrm{Irr}(G)$.*

One final condition is related to the integrality of character values. It is well known that the values in a character table are algebraic integers, as are the values $\chi(x)\frac{|\mathcal{K}|}{\chi(1)}$. In the case of a transposable group, the values $\chi(x)\frac{\sqrt{|\mathcal{K}|}}{\chi(1)}$ are also algebraic integers since they are character values of G^T.

Clearly the class sizes of G must be square in order for $\chi(x)\frac{\sqrt{|\mathcal{K}|}}{\chi(1)}$ to be integral. We may then ask whether all groups with square class sizes satisfy this criteria. Although some larger non-nilpotent groups do, the smallest non-abelian group with square class sizes (group [36,9] in GAP's small group database [GAP] and isomorphic to $C_3^2 \rtimes C_4$) does not. We do not have an example of a nilpotent group with square class sizes which does not satisfy this integrality criteria.

Chapter 4

Square Conjugacy Class Sizes

One of the first restrictions placed on transposable groups was that they have square conjugacy class sizes. Yet, unlike most of the properties investigated in the last chapter, square class sizes seem unrelated to nilpotence. This chapter investigates the property of having square conjugacy class sizes and, to a lesser extent, square order. It appears difficult to say much about such groups, but we do show they cannot be simple.

Theorem 4.0.6. *Suppose G has square conjugacy class sizes. If $N \lhd G$ with $(|N|, |G/N|) = 1$ then N and G/N have square conjugacy class sizes.*

Proof. Let $\pi = \pi(N)$, and let x be a π-element. By assumption, $\left|x^G\right|$ is a square, which means that $|G|/|C_G(x)|$ is a square. From the Schur–Zassenhaus theorem, G is a semidirect product of N and G/N. Then

$$\frac{|G|_\pi}{|C_G(x)|_\pi} = \frac{|N|}{|C_N(x)|} = \left|x^N\right|$$

is a square and so N has square class sizes. Similarly, let x be a π'-element, and then

$$\frac{|G|_{\pi'}}{|C_G(x)|_{\pi'}} = \frac{|G/N|}{|C_{G/N}(x)|} = \left|x^{G/N}\right|$$

must be a square. ■

A group G is called **quasi-Frobenius** if $G/Z(G)$ is Frobenius. Suppose G is quasi-Frobenius and let K, H be the preimages of the kernel and complement respectively. If K and H are abelian then the nontrivial conjugacy class sizes are $|H/Z(G)|$ and $|K/Z(G)|$ (see the remarks at the end of Section 2 of [CC11]). This means that if K and H are abelian and have square orders, then G has square class sizes. However, quasi-Frobenius groups are not nilpotent, and so cannot be transposable. Thus, we have a family of groups with square class sizes which are not transposable.

4.1 Simple Groups of Square Order

In this section we consider the questions of when a simple group can have square conjugacy classes. We include tables 4.1 and 4.2 of the simple groups with their orders.

Proposition 4.1.1 ([CH90, Proposition 3]). *If $p \mid |C_G(x)|$ for all $x \in G$, then G is not a non-abelian simple group. In other words every non-abelian simple group G has a conjugacy class K such that $|G|_p = |K|_p$.*

Corollary 4.1.2. *If G is a non-abelian simple group with square conjugacy class sizes then $|G|$ must be a square.*

The obvious question is whether there are simple groups with square order. The answer is yes, as shown in [NSW81]. In that paper they show that the groups $B_2(p) \cong$

Table 4.1: Families of Simple Groups

Group	Order	Restrictions
Z_p	p	p prime
A_n	$n!/2$	$n > 4$
$A_n(q)$	$\frac{1}{(n+1,q-1)} q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - 1)$	$(n,q) \neq (1,2),(1,3)$
$B_n(q)$	$\frac{1}{(2,q-1)} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$	$n > 1, (n,q) \neq (2,2)$
$C_n(q)$	$\frac{1}{(2,q-1)} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$	$n > 2$
$D_n(q)$	$\frac{1}{(4,q^n-1)} q^{n(n-1)} (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$	$n > 3$
$E_6(q)$	$\frac{1}{(3,q-1)} q^{36} (q^5 - 1)(q^9 - 1) \prod_{i=1,3,4,6} (q^{2i} - 1)$	
$E_7(q)$	$\frac{1}{(2,q-1)} q^{63} \prod_{i=1,3,4,5,6,7,9} (q^{2i} - 1)$	
$E_8(q)$	$q^{120} \prod_{i=1,4,6,7,9,10,12,15} (q^{2i} - 1)$	
$F_4(q)$	$q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)$	
$G_2(q)$	$q^6(q^6 - 1)(q^2 - 1)$	$q \neq 2$
${}^2A_n(q^2)$	$\frac{1}{(n+1,q+1)} q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - (-1)^{i+1})$	$n > 1, (n,q) \neq (2,2)$
${}^2D_n(q^2)$	$\frac{1}{(4,q^n+1)} q^{n(n-1)} (q^n + 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$	$n > 3$
${}^2E_6(q^2)$	$\frac{1}{(3,q+1)} q^{36} (q^9 + 1)(q^5 + 1) \prod_{i=1,3,4,6} (q^{2i} - 1)$	
${}^3D_4(q^3)$	$q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$	
${}^2B_2(2^{2n+1})$	$q^2(q^2 + 1)(q - 1)$	$n \geq 1, q = 2^{2n+1}$
${}^2F_4(2^{2n+1})$	$q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1)$	$n \geq 1, q = 2^{2n+1}$
${}^2G_2(3^{2n+1})$	$q^3(q^3 + 1)(q - 1)$	$n \geq 1, q = 3^{2n+1}$

Table 4.2: Sporadic Simple Groups

Group	Order
${}^2F_4(2)'$	$2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

$C_2(p)$ for primes p of the form

$$s_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} + (1-\sqrt{2})^{2m+1}}{2} \tag{4.1}$$

have square order. The integers s_{2m+1} have particular importance when they are prime, in which case they are called Newman–Shanks–Williams (or NSW) primes. For such a prime p, $|B_4(p)| = (p^2(p^2-1)t_{2m+1})^2$ where

$$t_{2m+1} = \frac{(1+\sqrt{2})^{2m+1} - (1-\sqrt{2})^{2m+1}}{2\sqrt{2}}.$$

The first NSW primes (OEIS sequence A088165) are 7, 41, 239, 9369319, 63018038201, and 489133282872437279. Newman, Shanks, and Williams also showed that there are no other groups in the families $B_n(q)$ or $C_n(q)$ which have square size. Since the paper was written before the classification of finite simple groups, they did not attempt to prove that there are no other simple groups with square size. We are unaware of such a classification for all finite simple groups. In this section we make some progress towards this end, leaving only the cases of $A_n(q)$ and ${}^2A_n(q^2)$ unsettled. We use many of the techniques employed in [NSW81] to characterize when $C_n(q)$ has square order. We start by stating a few well known results.

Lemma 4.1.3 (Bertrand–Chebyshev Theorem)**.** *If $n > 2$ is an integer, there is an odd prime p such that $n/2 < p \leq n$.*

In fact, a stronger statement is true: for all integers $m > 3$ there is a prime p such that $m < p < 2m-2$. This in turn implies $(n+1)/2 < p \leq n$ for all $n > 4$.

Lemma 4.1.4. *If m and n are positive integers and $x \neq 1$ is an integer, then the gcd*

$$\left(\frac{x^m-1}{x-1}, \frac{x^n-1}{x-1}\right) = \frac{x^{(m,n)}-1}{x-1}.$$

Lemma 4.1.5 ([Lju43; Nag21]). *If $n \geq 3$, then the only solutions to the Diophantine equation*

$$y^2 = \frac{x^n - 1}{x - 1}$$

which have $|x| > 1$ are

$$n = 4, x = 7, y = \pm 20,$$

$$n = 5, x = 3, y = \pm 11.$$

Corollary 4.1.6. *The Diophantine equation $\frac{x^{2p}-1}{x^2-1} = py^2$ with p an odd prime has no solutions with $x > 1$.*

Proof. Let

$$u = \frac{x^p - 1}{x - 1}, \qquad v = \frac{x^p + 1}{x + 1} = \frac{(-x)^p - 1}{(-x) - 1}$$

so that $uv = py^2$. Since p is odd, so are u and v, and therefore the identity

$$(x+1)v - (x-1)u = 2$$

implies that u and v are coprime. By Lemma 4.1.5, v cannot be a square (since $x > 0$), and hence $p \nmid u$. Thus $p \mid v$ and u is a square. Checking $x = 3$ and $p = 5$, as required by 4.1.5, we find that $\frac{3^{10}-1}{3^2-1} = 7381$ is not divisible by 3. ∎

Lemma 4.1.7. *If $(m, n) = 1$ and p is an odd prime then the following hold.*

$$\left(\frac{q^{2n} - 1}{q^2 - 1}, \frac{q^m + 1}{q + 1}\right) = 1 \tag{4.2}$$

$$\left(\frac{q^n - 1}{q - 1}, \frac{q^m - 1}{q - 1}\right) = 1 \tag{4.3}$$

$$\left(\frac{q^n - 1}{q - 1}, \frac{q^m + 1}{q + 1}\right) = 1 \tag{4.4}$$

$$\left(\frac{q^n+1}{q+1}, \frac{q^m+1}{q+1}\right) = 1 \tag{4.5}$$

$$\left(q \pm 1, \frac{q^p \pm 1}{q \pm 1}\right) = 1, p \tag{4.6}$$

Proof. All but the last of these follow from 4.1.4 by judicious multiplication of one or both terms. Suppose

$$g = \left(q-1, \frac{q^p-1}{q-1}\right) > 1.$$

We have $q \equiv 1 \bmod g$, so $(q^p-1)/(q-1) = 1 + q + \cdots + q^{p-1} \equiv p \bmod g$, and therefore $g = p$. The case of $\left(q+1, \frac{q^p+1}{q+1}\right)$ follows from the fact that $\frac{q^p+1}{q+1} = \frac{(-q)^p+1}{(-q)+1}$ and that no assumptions were made on the sign of q. ■

We shall also use the elementary fact that squares cannot be too close together. To be precise $(x \pm 1)^2 = x^2 \pm 2x + 1$, so they must differ by at least $2x - 1$.

We begin by following [NSW81] in studying the case of $C_n(q)$ and $B_n(q)$, and then continue with the other families of simple groups. Often we will use N to denote the order of the group and $N_1, N_2, \ldots$ to denote other integers which must be square if N is. Although they did not assume in [NSW81] that q was a prime power, we shall do so when it makes the arguments easier.

4.1.1 Orthogonal and Symplectic Groups: $C_n(q)$ and $B_n(q)$

The order of $C_n(q)$ (and $B_n(q)$) is

$$\begin{aligned} N &= \frac{1}{(2, q-1)} q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1) \\ &= q^{n^2} (q^2-1)^n \frac{(q^4-1)}{(2, q-1)(q^2-1)} \frac{(q^6-1)}{(q^2-1)} \cdots \frac{(q^{2n}-1)}{(q^2-1)}. \end{aligned}$$

Note that the third factor is an integer since $(2, q-1)$ divides q^2+1.

Newman, Shanks, and Williams prove that, if N is a square, then $n = 2$ and

$$N_1 = \frac{1}{(2, q-1)}(q^2+1)$$

is also a square. The gcd in the denominator must be 2, and hence q must be odd. Moreover, they prove the following theorem, thereby showing that q must be a prime.

Theorem 4.1.8. *If $m \geq 2$, the Diophantine equation*

$$x^{2m} + 1 = 2y^2$$

has no solution with $|x| > 1$.

Thus the case of the Symplectic groups has been reduced to $n = 2$ and q a prime with the additional property that $\frac{q^2+1}{2}$ is a square. They prove that such primes exist and have the form given in (4.1).

4.1.2 Linear and Unitary Groups: $A_n(q)$ and ${}^2A_n(q^2)$

The families $A_n(q)$ (for all n) and ${}^2A_n(q)$ (for $n > 1$ and $(n, q) \neq (2, 2)$) have orders

$$|A_n(q)| = \frac{1}{(n+1, q-1)} q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - 1)$$
$$\left|{}^2A_n(q)\right| = \frac{1}{(n+1, q+1)} q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - (-1)^{i+1})$$

which can be combined into a single formula where $\varepsilon = \pm 1$

$$N = \frac{1}{(n+1, q-\varepsilon)} q^{n(n+1)/2} \prod_{i=1}^{n} (q^{i+1} - \varepsilon^{i+1}).$$

Unfortunately, finding when N is square seems to be a difficult problem. When using the techniques of [NSW81], the following Diophantine equation arises

$$p\frac{q^p-1}{q-1} = z^2 \tag{4.7}$$

for primes p. Number theorists have studied such equations since z^2 is a repdigit in base q (assuming $p < q$). See, for example, [Ink72].

Solutions to (4.7) do exist, for example when $p = 2$. There are an infinite number of solutions [Waa73] when $p = 3$ given by

$$q = \frac{\sqrt{3}}{4}\left((2+\sqrt{3})^{2n+1} - (2-\sqrt{3})^{2n+1}\right) - \frac{1}{2}.$$

This is OEIS sequence A028231 and the first few terms are 1, 22, 313, 4366, 60817. Broughan [Bro12, Lemma 7] finds that for any $p \geq 5$, there are (at most) a finite number of solutions with $|q| > 1$ to (4.7). This was also proven in [ST76].

Every solution to $p\frac{q^p-1}{q-1} = z^2$ is one less than a solution to $p\frac{q^p+1}{q+1} = z^2$, so such equations (arising when $\varepsilon = -1$) need not be considered separately. Several restrictions on q can be derived, but a full solution is elusive, so in Section 4.2 we prove instead that $A_n(q)$ and ${}^2A_n(q)$ (and $C_2(q)$) do not have square class sizes.

Apart from the families already mentioned, there are no other simple groups which can have square sizes.

4.1.3 Sporadic Groups

The sporadic groups (we include the Tits group ${}^2F_4(2)'$ in the list) do not have square order, which can be easily checked from Table 4.2.

4.1.4 Orthogonal Groups: $D_n(q)$ and ${}^2D_n(q^2)$

The family $D_n(q)$ ($n > 3$) has order

$$N = \frac{1}{(4, q^n - 1)} q^{n(n-1)} (q^n - 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$$

so that we only need to consider

$$N_1 = \frac{(q^n - 1)}{(4, q^n - 1)} \prod_{i=1}^{n-1} (q^{2i} - 1).$$

Moreover ${}^2D_n(q^2)$ ($n > 3$) has order

$$N = \frac{1}{(4, q^n + 1)} q^{n(n-1)} (q^n + 1) \prod_{i=1}^{n-1} (q^{2i} - 1)$$
$$N_1 = \frac{(q^n + 1)}{(4, q^n + 1)} \prod_{i=1}^{n-1} (q^{2i} - 1)$$

so for these cases we deal with more general equations.

If n is even, consider

$$N_2 = \frac{1}{(4, q^n \pm 1)} \frac{(q^n \pm 1)}{(q^2 - 1)} \prod_{i=1}^{n-1} \frac{q^{2i} - 1}{q^2 - 1}.$$

By Lemma 4.1.3, there is a prime $p > (n-1)/2$ so that $\frac{q^{2p}-1}{q^2-1}$ is coprime to the other factors. Unless $n = 4$, we can choose $p > n/2$, and if $n = 4$, then $p = n - 1 = 3$ will work. The factor $\frac{q^{2p}-1}{q^2-1}$ is also coprime to $\frac{q^n \pm 1}{q^2-1}$ unless $n = 2p$ which is impossible.

The contribution of $(4, q^n \pm 1)$ is only interesting in terms of determining squareness if it is 2. So we consider $\frac{q^{2p}-1}{q^2-1} = 1 + q^2 + \cdots + q^{2(p-1)} \bmod 4$. Because $q^2 \equiv 0, 1 \bmod 4$, $\frac{q^{2p}-1}{q^2-1}$ is congruent to either 1 or p mod 4. Neither of these is equal to 2 unless $p = 2$, but p is an odd prime. Thus, $\frac{q^{2p}-1}{q^2-1}$ must itself be a square which contradicts Lemma 4.1.5.

If n is odd, let

$$N_2 = \frac{1}{(4, q^n \pm 1)}(q^n \pm 1)\prod_{i=1}^{n-1}\frac{q^{2i}-1}{q^2-1}.$$

As before, there is a prime such that $\frac{q^{2p}-1}{q^2-1}$ is coprime to the other factors, except perhaps $q^n \pm 1$. By considering the gcd (using Lemma 4.1.7)

$$1 = \left(\frac{q^n \pm 1}{q \pm 1}, \frac{q^{2p}-1}{q^2-1}\right)$$

we see that we need only consider

$$g = \left(q \pm 1, \frac{q^{2p}-1}{q^2-1}\right)$$

which divides

$$g' = \left(q^2 - 1, \frac{q^{2p}-1}{q^2-1}\right) = 1, p.$$

Hence we see that $\frac{q^{2p}-1}{q^2-1}$ is a square or p times a square. The latter is impossible by Corollary 4.1.6. Thus in both cases it must be that $\frac{q^{2p}-1}{q^2-1}$ is a square, which means by Lemma 4.1.5 that $p = 5$ and $q^2 = 3$, which cannot be.

4.1.5 Chevalley Groups: $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, and $G_2(q)$

The family $E_6(q)$ has order

$$N = \frac{1}{(3, q-1)}q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$$

which isn't square unless

$$N_1 = \frac{1}{(3,q-1)} \frac{(q^{12}-1)}{(q-1)} \frac{(q^9-1)}{(q-1)} \frac{(q^8-1)}{(q-1)} \frac{(q^6-1)}{(q-1)} \frac{(q^5-1)}{(q-1)} \frac{(q^2-1)}{(q-1)}$$

is. But we know by Lemma 4.1.4 that $\frac{(q^5-1)}{q-1}$ is coprime to the other factors and so it must either be a square, or 3 times a square. By Lemma 4.1.5 it can only be a square if $q = 3$, in which case the order of $E_6(3) = 96708364468594278400$ is not a square. But if $g = (q-1, \frac{q^5-1}{q-1}) > 1$, then $g = 5$ and hence $\frac{(q^5-1)}{q-1}$ is not divisible by $(3, q-1)$.

A similar situations arises for the family $E_7(q)$.

$$\begin{aligned} N &= \frac{1}{(2,q-1)} q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1) \\ N_1 &= \frac{(q^2-1)}{(2,q-1)} \frac{(q^{18}-1)}{(q^2-1)} \frac{(q^{14}-1)}{(q^2-1)} \frac{(q^{12}-1)}{(q^2-1)} \frac{(q^{10}-1)}{(q^2-1)} \frac{(q^8-1)}{(q^2-1)} \frac{(q^6-1)}{(q^2-1)} \end{aligned}$$

In this case the factor $\frac{q^{14}-1}{q^2-1}$ is coprime to the rest (except perhaps the first). Now $(q^2-1, \frac{q^{14}-1}{q^2-1}) = 1, 7$ and the first case is ruled out by 4.1.5 and the second by 4.1.6.

Exactly the same arguments (including the same factor) hold for $E_8(q)$:

$$\begin{aligned} N &= q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1) \\ N_1 &= \frac{(q^{30}-1)}{(q^2-1)} \frac{(q^{24}-1)}{(q^2-1)} \frac{(q^{20}-1)}{(q^2-1)} \frac{(q^{18}-1)}{(q^2-1)} \frac{(q^{14}-1)}{(q^2-1)} \frac{(q^{12}-1)}{(q^2-1)} \frac{(q^8-1)}{(q^2-1)}. \end{aligned}$$

A different argument shows that the family $F_4(q)$ does not have square order.

$$\begin{aligned} N &= q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1) \\ N_1 &= \frac{(q^{12}-1)}{(q^6-1)} \frac{(q^8-1)}{(q^2-1)} \frac{(q^6-1)}{(q^6-1)} \frac{(q^2-1)}{(q^2-1)} \\ &= (q^6+1)(q^4+1)(q^2+1) \end{aligned}$$

$$
\begin{aligned}
N_2 &= \frac{(q^6+1)}{(q^2+1)}(q^4+1)\frac{(q^2+1)}{(q^2+1)} \\
&= (q^4-q^2+1)(q^4+1) = q^8 - q^6 + 2q^4 - q^2 + 1 \\
N_3 &= 64q^8 - 64q^6 + 128q^4 - 64q^2 + 64 \\
&= (8q^4 - 4q^2 + 7)^2 - 8q^2 + 15.
\end{aligned}
$$

Since N_3 cannot be too close to a square, we must have

$$
\left| -8q^2 + 15 \right| \geq 2(8q^4 - 4q^2 + 7) - 1 = 16q^4 - 8q^2 + 13
$$

so that

$$
\begin{aligned}
-8q^2 + 15 &\geq 16q^4 - 8q^2 + 13 \\
2 &\geq 16q^4
\end{aligned}
$$

which has no solutions of interest, or

$$
\begin{aligned}
8q^2 - 15 &\geq 16q^4 - 8q^2 + 13 \\
0 &\geq 16q^4 - 16q^2 + 28
\end{aligned}
$$

which is not satisfied for any real q. Thus, N_3 is not a square.

Next we consider the simple groups $G_2(q)$ with $q \neq 2$. Their order is given by

$$
N = q^6(q^6-1)(q^2-1)
$$

which is square if and only if

$$
N_1 = \frac{(q^6-1)}{(q^2-1)}
$$

is. But N_1 cannot be a square by Lemma 4.1.5.

4.1.6 Twisted Groups: ${}^2E_6(q^2)$, ${}^3D_4(q^3)$ ${}^2B_2(2^{2n+1})$, ${}^2F_4(2^{2n+1})$, ${}^2G_2(3^{2n+1})$

The family ${}^2E_6(q^2)$ requires a slightly different approach.

$$\begin{aligned}
N &= \frac{1}{(3,q+1)}q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1) \\
N_1 &= \frac{1}{(3,q+1)}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1) \\
N_2 &= \frac{1}{(3,q+1)}\frac{(q^{12}-1)}{(q^2-1)}\frac{(q^9+1)}{(q+1)}\frac{(q^8-1)}{(q^2-1)}\frac{(q^6-1)}{(q^2-1)}\frac{(q^5+1)}{(q+1)}
\end{aligned}$$

Since $(q^5+1)/(q+1)$ is coprime to the other factors by Lemma 4.1.7, we only need to consider its gcd with respect to the term $(3,q+1)$. But $q+1$ can only share a factor of 5 in common with $(q^5+1)/(q+1)$ (again by 4.1.7), and so $(q^5+1)/(q+1)$ must be square.

Consider now the Diophantine equation

$$y^2 = q^4 - q^3 + q^2 - q + 1. \tag{4.8}$$

Multiply by 2^2 so that

$$\begin{aligned}
(2y)^2 &= 4q^4 - 4q^3 + 4q^2 - 4q + 4 \\
(2y)^2 &= (2q^2 - q + 1)^2 - q^2 - 2q + 3.
\end{aligned}$$

In order to avoid being too close to another square, we must have that

$$\begin{aligned}
2(2q^2 - q + 1) &\leq q^2 + 2q - 3 \\
4q^2 - 2q + 2 &\leq q^2 + 2q - 3
\end{aligned}$$

$$3q^2 - 4q + 5 \leq 0$$

which is not satisfied by any real numbers. Since there are no solutions to this equation, there are no solutions to (4.8). Hence, $\frac{q^5+1}{q+1}$ is not a square and neither is N.

The case of ${}^3D_4(q^3)$ is simpler.

$$\begin{aligned} N &= q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1) \\ N_1 &= (q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1) \\ N_2 &= \frac{(q^{12} - 1)}{(q^4 - 1)} \frac{(q^6 - 1)}{(q^2 - 1)} \\ N_3 &= \frac{(q^{12} - 1)(q^6 - 1)}{(q^2 + 1)} \\ N_4 &= \frac{(q^6 + 1)}{(q^2 + 1)} = q^4 - q^2 + 1 \end{aligned}$$

But N_4 is too close to the square q^4 to be a square itself.

Calculations for the family ${}^2B_2(2^{2n+1})$ are even easier.

$$\begin{aligned} N &= q^2(q^2 + 1)(q - 1) \\ N_1 &= (q^2 + 1)(q - 1) \end{aligned}$$

Because $N_1 \equiv -1 \bmod 4$, it cannot be a square.

The family ${}^2F_4(q)$ with $q = 2^{2n+1}$ has order

$$N = q^{12}(q^6 + 1)(q^4 - 1)(q^3 + 1)(q - 1)$$

and so the following must also be square

$$N_1 = (q^6 + 1)(q^2 + 1)(q + 1)(q - 1)(q^3 + 1)(q - 1)$$

$$N_2 = \frac{(q^6+1)}{(q^2+1)}\frac{(q^3+1)}{(q+1)} = (q^4-q^2+1)(q^2-q+1).$$

Neither factor of N_2 is a square, so their gcd must be nontrivial. However,

$$\begin{aligned}(q^4-q^2+1, q^2-q+1) &= (q^4-q^2+1-(q^2+q-1)(q^2-q+1), q^2-q+1)\\ &= (-2q+2, q^2-q+1).\end{aligned}$$

Since q^2-q+1 is odd, this is further equal to

$$(q-1, q^2-q+1) = (q-1, q^2-q+1-(q^2-q)) = (q-1, 1) = 1.$$

Finally, the family ${}^2G_2(q)$ for $q = 3^{2n+1}$ has order $q^3(q^3+1)(q-1)$, which is not a square given that q^3 is not a square.

4.2 Class Sizes in Simple Groups

As seen in the previous section no simple group can have square conjugacy class sizes with the possible exceptions of $B_2(p) \cong C_2(p)$, $A_n(q)$, and ${}^2A_n(q)$. First we note that the groups of interest are the classical groups $C_2(p) = PSp_{2\cdot 2}(q)$, $A_n(q) = PSL_{n+1}(q)$ and ${}^2A_n(q) = PSU_{n+1}(q^2)$.

It is possible to calculate class sizes in these groups, though the formulas tend to be quite complicated [Wal63]. We shall not reproduce the theory here, but the basic idea is that in $GL_n(q)$ the Jordan canonical form determines the conjugacy class. Thus, the conjugacy classes are identified by irreducible monic polynomials (whose roots are the eigenvalues) as well as block sizes. From this information centralizer sizes can then be calculated. To simplify our calculations, we will consider only unipotent elements, *i.e.*, elements whose eigenvalues are all 1. Then the only polynomials involved are $x-1$, and the block sizes correspond to partitions of m.

We shall use μ to indicate a partition of m, μ' to be its conjugate (or dual) partition, and $m_i(\mu)$ to be the number of parts of μ of size i. Given these definitions we have the formulas below for centralizer sizes. We shall use q^* to indicate some power of q. The exact power of q is usually unimportant since q will always be coprime to the other terms. We use g_μ to indicate a unipotent element of the appropriate group with a corresponding partition μ.

$$C_{GL_m(q)}(g_\mu) = \prod_i \left| GL_{m_i(\mu)}(q) \right|$$
$$C_{GU_m(q^2)}(g_\mu) = \begin{cases} q^* \prod_i \left| GU_{m_i(\mu)}(q^2) \right| & q \text{ odd} \\ q^* \prod_i \left| GL_{m_i(\mu)}(q^2) \right| & q \text{ even} \end{cases}$$
$$C_{GSp_{2m}(q)}(g_\mu) = \begin{cases} q^* \prod_i \left| GSp_{2m_i(\mu)}(q) \right| & i \text{ odd} \\ q^* \prod_i \left| O^{\pm}_{m_i(\mu)}(q) \right| & i \text{ even} \end{cases}$$

For the symplectic case, all even parts of μ must have even multiplicity. In addition, there is a choice of sign for the even parts which gives rise to the different orthogonal groups in those cases (hence the appearance of $O^{\pm}_{m_i(\mu)}(q)$).

Theorem 4.2.1. *There are no non-abelian simple groups all of whose conjugacy class sizes are square.*

Proof. The only symplectic groups of interest are $C_2(q) = PSp_{2\cdot 2}(q)$ with q an odd prime. Consider the symplectic group with partition $\mu = (2,2)$ of $2 \cdot 2$, and both choices of sign. Let $G = GSp_4(q)$ and $g_{(2,2)}$ a unipotent element of G corresponding to the partition $(2,2)$. Then

$$\left| C_G(g_{(2,2)}) \right| = q^* \left| O^{\pm}_{2\cdot 2}(q) \right| = q^*(q^2 \pm 1)(q^2 - 1)$$

$$\left|g^G_{(2,2)}\right| = q^* \frac{(q^4-1)(q^2-1)}{(q^2\pm 1)(q^2-1)} = q^*(q^2 \mp 1)$$

When factoring by the center (scalar matrices) the class sizes stay the same because the only central unipotent element is the identity. So we have that both q^2+1 and q^2-1 must be square, but clearly neither can be.

We now turn our attention to the linear and unitary groups, which are similar, and rule out a few small cases. Let G be either $PSL_m(q)$ or $PSU_m(q)$ with $\varepsilon = \pm 1$ accordingly. If $m = 2$, then

$$|G| = \frac{q}{(2, q-\varepsilon)}(q^2-1).$$

Clearly q must be a square itself, say r^2. If q is even, then $(2, q-\varepsilon) = 1$, and $|G|$ is not square. Otherwise $(r^4-1)/2$ must be a square, but this is impossible by Theorem 4.1.8, and so $m \neq 2$.

For $m = 3$ we have

$$|G| = \frac{q^{2\cdot 3/2}}{(3, q-\varepsilon)}(q^2-\varepsilon^2)(q^3-\varepsilon^3)$$

so that

$$N = \frac{q^3}{(3, q-\varepsilon)} \frac{(q^2-\varepsilon^2)}{(q-\varepsilon)} \frac{(q^3-\varepsilon^3)}{(q-\varepsilon)}$$

must also be square. The last two factors are coprime, and $\frac{(q^3-\varepsilon^3)}{(q-\varepsilon)}$ is not square by Lemma 4.1.5 Nor is it 3 times a square by Corollary 4.1.6 (since q must be a square).

For $m = 5$

$$|G| = \frac{q^*}{(5, q-\varepsilon)}(q^2-\varepsilon^2)(q^3-\varepsilon^3)(q^4-\varepsilon^4)(q^5-\varepsilon^5).$$

There are an even number of terms, so dividing each by $q-\varepsilon$ does not change the squareness of the number. Because of this, $\frac{(q^3-\varepsilon^3)}{(q-\varepsilon)} = \frac{((\varepsilon q)^3-1)}{((\varepsilon q)-1)}$ is coprime to all other terms and not a square by Lemma 4.1.5.

In fact, similar arguments hold for all larger odd m. This is because we have a large prime $p > m/2$, and $\frac{q^p-\varepsilon}{q-\varepsilon}$ cannot be square. (It is easy to check the few cases when $\frac{q^p-\varepsilon}{q-\varepsilon}$ can be a square, namely $q=3$ and $p=5$, do not lead to a square group order.) Thus, in order for $|G|$ to be square it must be that $(m, q-\varepsilon, \frac{q^p-\varepsilon^p}{q-\varepsilon}) = p$. Since $2p > m$ we have $m = p$, in which case there is another prime p' between $(m-1)/2$ and p for which $\frac{q^p-\varepsilon^p}{q-\varepsilon}$ cannot be square.

This leaves the cases when $m \geq 4$ is even. In these cases there must be at least one solution to the Diophantine equation

$$p\frac{q^p-\varepsilon}{q-\varepsilon} = y^2$$

for p an odd prime. If $p > 3$ ($m \geq 6$), then from [Rot83, Theorems 5″ and 6′] we have that $q \equiv 1 \bmod 4$.

Since q is odd, both linear and unitary groups can be treated simultaneously. Let $G_m(q)$ denote either $GL_m(q)$ or $GU_m(q^2)$. We will consider two partitions of m, $\mu_1 = (2, 1, \ldots)$ and $\mu_2 = (2, 2, 1, \ldots)$, which lead to class sizes of

$$\begin{aligned}
\left|C_{G_m(q)}(g_{\mu_1})\right| &= q^*|G_1(q)||G_{m-2}(q)| = q^*(q-\varepsilon)\prod_{i=1}^{m-2}(q^i-\varepsilon^i); \\
\left|g^G_{\mu_1}\right| &= q^*\frac{\prod_{i=1}^{m}(q^i-\varepsilon^i)}{(q-\varepsilon)\prod_{i=1}^{m-2}(q^i-\varepsilon^i)} = q^*\frac{(q^m-\varepsilon^m)(q^{m-1}-\varepsilon^{m-1})}{(q-\varepsilon)}; \\
\left|C_{G_m(q)}(g_{\mu_2})\right| &= q^*|G_2(q)||G_{m-4}(q)| = q^*(q-\varepsilon)(q^2-1)\prod_{i=1}^{m-4}(q^i-\varepsilon^i); \\
\left|g^G_{\mu_2}\right| &= q^*\frac{\prod_{i=1}^{m}(q^i-\varepsilon^i)}{(q-\varepsilon)(q^2-1)\prod_{i=1}^{m-4}(q^i-\varepsilon^i)}
\end{aligned}$$

$$= q^* \frac{(q^m - \varepsilon^m)(q^{m-1} - \varepsilon^{m-1})}{(q-\varepsilon)} \frac{(q^{m-2} - \varepsilon^{m-2})(q^{m-3} - \varepsilon^{m-3})}{(q^2-1)}.$$

When passing to the $SL_m(q)$ or $SU_m(q)$ the classes split into $(m, q-\varepsilon)$ classes of equal size, and factoring out by the center does not change the class size.

When $m = 4$ (and q odd) the class size of g_{μ_1} in G, the appropriate simple group, is

$$\left| g_{\mu_1}^G \right| = q^* \frac{(q^4 - \varepsilon^4)(q^3 - \varepsilon^3)}{(4, q-\varepsilon)(q-\varepsilon)}.$$

Combining with the group order

$$|G| = \frac{q^*}{(4, q-\varepsilon)} (q^2 - \varepsilon^2)(q^3 - \varepsilon^3)(q^4 - \varepsilon^4)$$

we find that

$$N = \frac{q^2 - \varepsilon^2}{q - \varepsilon} = q + \varepsilon$$

is a square. On the other hand, by combining the two conjugacy class sizes, we know that

$$N_1 = \frac{(q^2 - \varepsilon^2)(q^1 - \varepsilon^1)}{(q^2-1)} = q - \varepsilon$$

must also be square. But of course $q - \varepsilon$ and $q + \varepsilon$ cannot both be square.

If $m = 4$ and q is even then, $(4, q-\varepsilon) = 1$ so

$$|G| = q^*(q^2 - \varepsilon^2)(q^3 - \varepsilon^3)(q^4 - \varepsilon^4)$$

which is square if and only if

$$N_1 = q^*(q^3 - \varepsilon^3)(q^2 + 1)$$

$$= q^*(q-\varepsilon)\frac{(q^3-\varepsilon^3)}{(q-\varepsilon)}(q^2+1)$$

is as well. However, the gcd

$$\begin{aligned}(q-\varepsilon, q^2+1) &= (q-\varepsilon, q^2+1-(q+\varepsilon)(q-\varepsilon)) \\ &= (q-\varepsilon, 1+\varepsilon^2) = (q-\varepsilon, 2) = 1\end{aligned}$$

so that $(q-\varepsilon)$ is coprime to q^2+1, which is also coprime to $\frac{(q^3-\varepsilon^3)}{(q-\varepsilon)}$ (by Lemma 4.1.7). This means that q^2+1 must be square, which is impossible.

If $m > 4$ is even, then by combining the group order with the class size of g_{μ_1}, we find that

$$N = \prod_{i=1}^{m-2}(q^i - \varepsilon^i)$$

and

$$N_1 = \prod_{i=1}^{m-2}\frac{(q^i-\varepsilon^i)}{(q-\varepsilon)}$$

must be square. Since $m \geq 6$, we will have an odd prime $p > (m-2)/2$ and a factor which is coprime to all others. By Lemma 4.1.5 only $q = 3$ and $p = 5$ is possible. This means that $m < 12$ since $5 > (m-2)/2$. All such m are easily checked to not give rise to square group order.

And so there are no simple groups with square class sizes. ■

Remark 4.2.2. As m increases the number of simultaneous Diophantine equations to solve increases and so the likelihood of $|G|$ being square decreases. For this reason it is likely that symplectic groups are the only simple groups with square order.

Chapter 5

Examples of Transposable Groups

Relatively few examples of non-abelian transposable groups are known. Since such groups are nilpotent, only directly indecomposable p-groups need to be considered. In this chapter we discuss the known families and some methods of creating new transposable groups.

We first introduce the method of grafting two transposable groups together. This method yields abelian groups when applied to abelian groups, but it allows us to turn a non-abelian transposable group into an infinite family of examples. It also allows us to concentrate on certain basic families of groups which we call stem groups, mimicking the terminology of isoclinism. Our method is reminiscent of grafting roots or branches onto a group, so the terminology is fitting.

Then, we enumerate all known stem groups. All of these are self-dual, but grafting allows us to create transposable groups which are not self-dual. It is an interesting question whether there are any transposable groups that are *not* self-dual in an essential way. Finally, we prove the transposability of a family of stem groups which has not appeared in the literature.

5.1 Constructions

We now explain the important construction of **grafting**.

Proposition 5.1.1. *Let G be a transposable group, $x \in Z(G)$ and $X = \langle x \rangle$. Furthermore, suppose that $X \cap G' = 1$, then G/X is transposable.*

Proof. Let $g \in G \setminus X$ and $\bar{g}$ its image in G/X. We first show that $|g^G| = |\bar{g}^{G/X}|$. To find $\bar{g}^{G/X}$, take g^G and all X-translates of it, and then factor out by X. Since X intersects G' trivially and is central, the X-translates are all distinct and all the same size. Thus, $|\bar{g}^{G/X}| = |g^G|\frac{|X|}{|X|} = |g^G|$.

The concept dual to factoring by a cyclic group is taking a linear character $\lambda \in \operatorname{Irr}(G^T)$ and restricting all characters to $H = \ker \lambda$. If all the restrictions are irreducible, then these (after removing duplicates) give the character table of H. This is not true in general, but comes from what we know of the character table of G/X. The character degrees remain the same and are the same as the conjugacy class sizes of G/X. The duplicate characters will be the same as the duplicate conjugacy classes which were merged in the character table of G/X. Hence $\sum_{\chi \in \operatorname{Irr}(H)} \chi(1)^2 = \sum_{\mathcal{K} \in \operatorname{Cl}(G/X)} |\mathcal{K}| = |G/X| = |H|$.

Since x is a central element, its dual, λ, is a linear character of the same order. Hence, $\ker \lambda$ has index $|X|$ in G^T. Since $x \notin G'$, the kernel of λ does not contain the center of G^T and $Z(G^T)$ contains a full set of right coset representatives of H. The inertia subgroup of any $\varphi \in \operatorname{Irr}(H)$ is therefore all of G^T because g can be chosen from the center when calculating $\varphi^g = \varphi(ghg^{-1})$. Thus, φ_H is homogeneous for all $\varphi \in \operatorname{Irr}(G)$.

Because $Z(G^T)$ contains a full set of right coset representatives of H, there is no fusion in H; *i.e.*, every conjugacy class of H is also a conjugacy class of G. This means that the operations performed in calculating the character tables of H and G/X are exactly the duals of each other. Therefore, the number of conjugacy classes of H is the same as the number of irreducible characters, and the φ_H must be irreducible and not only homogeneous. And thus we see that the character table of H is the transpose of that of G/X. ■

Corollary 5.1.2. *If G is transposable and $N \lhd G$ such that $G = NZ(G)$, then N is transposable.*

Proof. The dual property to $X \cap G' = 1$ is that $NZ(G) = G$, and the dual property to $X \leq Z(G)$ is that $N \geq G'$. However, $N \geq G'$ is implied because elements of G have the form $g = zn$ for $z \in Z(G)$ and $n \in N$. Since central elements are irrelevant when calculating commutators,

$$[z_1 n_1, z_2 n_2] = [n_1, n_2]$$

and so $N \geq G'$. ■

By starting with two transposable groups G_1, G_2 (in particular one may be abelian) we can create new (directly indecomposable) transposable groups. First, let $G = G_1 \times G_2$, and choose $g_i \in Z(G_i)$ so that $(g_1, g_2) \in Z(G)$. If, say, $\langle g_2 \rangle \cap G_2' = 1$, then $\langle (g_1, g_2) \rangle \cap G' = 1$ and so $G/\langle (g_1, g_2) \rangle$ will be transposable.

We often think of this as adding an abelian group rather than combining two groups, though combining two non-abelian is certainly possible as well. The additional elements either "hang down" from the top of the group, or "grow up" from the bottom. In fact, starting with a transposable group, we can choose $g, h \in G$ with $g^p = h^p = 1$, $g \notin G'$, $h \in Z(G)$ and create a new group with a new power map of $g^p = h$ and $h^p = 1$.

When adding an abelian group we do not change the commutator structure, only the power map of the original group. Therefore, this construction doesn't change the nilpotency class or the derived length of the groups.

Another method, called **inflation**, can be used to turn a transposable group into a family of such groups. Inflation results in transposable groups in many cases, but its efficacy has not been proven in general. Let $G = \langle g_i \rangle$ be a group with a presentation such that every generator g_i has a relation of the form $g_i^p = x_i$, where x_i is some product of the other generators. Fix $q = p^a$, and define the **inflated group** $H_q = \langle g_i \rangle$ to have the same relations as G, except that $g_i^q = x_i$. Obviously, an inflated abelian group is abelian.

5.2 Examples

Apart from abelian groups, there are two families of finite transposable groups found in the literature, to which we add a third.

The first family, discussed in [Han97], exists for $p \geq 3$ and has order p^5. It has a presentation of the form

$$G = \left\langle a_1, a_2, b, c_1, c_2 \;\middle|\; [a_1, a_2] = b, [a_i, b] = c_i, a_i^p = \zeta_i, b^p = c_i^p = 1 \right\rangle$$

where ζ_i is central, and unlisted commutators of generators are trivial. The possible values of ζ_i leading to distinct groups is found in [Jam80] but are irrelevant for our purposes.

It is clear from the presentation that $Z(G) = \langle c_i \rangle \cong \mathbb{Z}_p^2$ and $G' = \langle b, c_i \rangle$. Moreover, $G/Z(G)$ is an extraspecial group of type $+$. The nilpotency class is 3 and the derived length is 2. It is not difficult to see that all normal subgroups of G are either contained in the center, or contain the commutator subgroup. This leads to the normal subgroup lattice in Figure 5.1. Of course, the number of normal subgroups depends on the prime p.

The second family appears to be unknown as being self-dual. It exists for $p \geq 5$ and has order p^7. For the cases with $p \leq 11$, these groups are included in the database of small groups available in GAP [GAP]. Its structure is strikingly similar to the previous

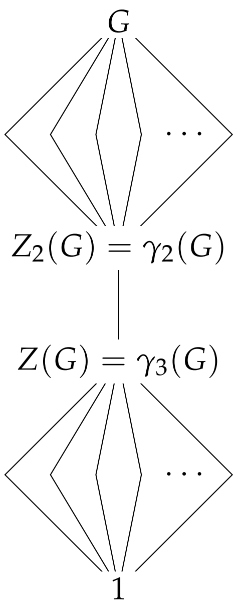

Figure 5.1: Hanaki's Groups

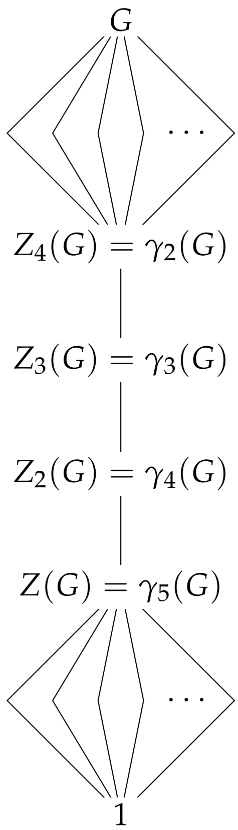

Figure 5.2: Class 5 Groups

family. It has a presentation of

$$\begin{aligned} G = \big\langle a_1, a_2, b_1, b_2, b_3, c_1, c_2 \big| \\ & [a_2, a_1] = b_1, [b_{i=1,2}, a_1] = b_{i+1}, [b_3, a_1] = c_1, \\ & [b_2, a_2] = [b_3, a_2] = [b_1, b_2] = c_2, a_i^p = \zeta_i, b_i^p = c_i^p = 1 \big\rangle \end{aligned}$$

where ζ_i is central and trivial commutators are not listed.

It is clear from the presentation that $Z(G) = \langle c_i \rangle \cong \mathbb{Z}_p^2$ and $G' = \langle b_i, c_i \rangle$. The nilpotency class is 5 and the derived length is 3. Similar to before, G has coclass 2 and $G/Z_3(G)$ is an extraspecial group of type $+$. Its normal subgroup lattice is similar and given in Figure 5.2.

We shall prove that this family of groups is transposable in the next section. Our attempts to construct similar groups of class 7 have failed. More precisely, we assumed a presentation of the form

$$G = \langle a_1, a_2, b_1, b_2, b_3, b_4, b_5, c_1, c_2 \big| [a_2, a_1] = b_1, [b_{i=1,2,3,4}, a_1] = b_{i+1}, [b_5, a_1] = c_1,$$
$$[b_i, a_2] = \zeta_i, [b_i, b_j] = \zeta_{i,j},$$
$$a_i^p = b_i^p = c_i^p = 1 \rangle$$

with ζ_i and $\zeta_{i,j}$ powers of c_2. Groups created this way fail to have square class sizes.

The final family of self-dual groups is a generalization of the Suzuki 2-groups $A(n, \theta)$ and has been studied in several papers [Rie99; Han96b; Sag03]. The nontrivial claims below are proven in one or more of those papers.

Let $q = p^a$ be a prime power, s and l be positive integers, and θ a generator of the Galois group of F_{q^s} over F_q. Furthermore, assume that s is odd and $(s, l!) = (s, q) = (s, q-1) = 1$. Then, we can define a group $G = G(q, s, l)$, whose elements are l-tuples of elements of F_q and multiplication $c = ab$ given by

$$c_i = a_i + \sum_{j=1}^{i-1} a_{i-j}^{\theta^j} b_j + b_i.$$

This can be thought of as multiplication of skew polynomials of the form $1 + \sum_{i=1}^{l} a_i x^i$ modulo the ideal $\left(x^{l+1}\right)$, see [Rie99]. It is also easily seen to be equivalent to

$$a = (a_1, a_2, \ldots, a_l) = \begin{pmatrix} 1 & & & & & \\ a_1 & 1 & & & & \\ a_2 & a_1^{\theta} & 1 & & & \\ a_3 & a_2^{\theta} & a_1^{\theta^2} & 1 & & \\ \vdots & \vdots & & \ddots & \ddots & \\ a_l & a_{l-1}^{\theta} & a_{l-2}^{\theta^2} & \cdots & a_1^{\theta^{l-1}} & 1 \end{pmatrix}$$

with the regular matrix multiplication.

The lower and upper central series of G coincide and each central series factor is isomorphic to the additive group of $\mathbb{F}_{q^s}$, *i.e.*, elementary abelian of order q^s. In fact, the central series is easily defined in terms of "layers" in the matrix or fixed powers of x. Clearly $G(q,s,l)/Z(G(q,s,l)) \cong G(q,s,l-1)$. The nilpotency class of G is l, and its derived length is $\lceil \log_2(l+1) \rceil$.

The group G has $q^{l-i}(q^s-1)$ (or q^s if $l = i$) irreducible characters of degree $q^{(l-i)(s-1)/2}$ and the same number of conjugacy classes of size $q^{(l-i)(s-1)}$.

Not all such groups are self-dual. If $l > p$ then $G(p^a,s,l)$ is not self-dual, but when $l = s-1 < p$ it is self-dual [HO97]. This gives a construction for transposable groups with arbitrarily large nilpotency class. It is unknown whether $G(p^a,s,l)$ is self-dual for all $l \leq p$, but at least $G(p,3,2)$ is self-dual, so it is reasonable to conjecture that they are when $l \leq p$.

5.3 Self-duality of a certain family of p-groups

For a fixed prime $p > 3$, let G be the class 5 p-group defined previously, namely the group with presentation

$$G = \langle a_1, a_2, b_1, b_2, b_3, c_1, c_2 \mid [a_2,a_1] = b_1, [b_{i=1,2}, a_1] = b_{i+1}, [b_3,a_1] = c_1, [b_2,a_2] = [b_3,a_2] = [b_1,b_2] = c_2, a_i^p = b_i^p = c_i^p = 1 \rangle.$$

There is a privileged chain of normal subgroups $G > N > \gamma_2 > \gamma_3 > \gamma_4 > \gamma_5 > C > 1$ where $N = \langle a_2, b_i, c_i \rangle$, $\gamma_i = \gamma_i(G)$, and $C = \langle c_2 \rangle$. Each subgroup has index p in the previous (recall the normal subgroup lattice in Figure 5.2).

We divide the conjugacy classes into different sets as listed below. For each set we give a complete list of class representatives. Unless otherwise noted, all exponents range from 0 to $p-1$. The sizes of all conjugacy classes are p^2 except in the center and in $\mathrm{Cl}_6(G)$ where they are p^4.

$$\begin{aligned}
\mathrm{Cl}_0(G) &= C &&= \left\{ (c_2^f)^G \right\} \\
\mathrm{Cl}_1(G) &= Z(G) \setminus C &&= \left\{ (c_1^e c_2^f)^G \,\middle|\, e \neq 0 \right\} \\
\mathrm{Cl}_2(G) &= Z_2(G) \setminus Z(G) &&= \left\{ (b_3^d)^G \,\middle|\, d \neq 0 \right\} \\
\mathrm{Cl}_3(G) &= Z_3 \setminus Z_2(G) &&= \left\{ (b_2^c c_1^e)^G \,\middle|\, c \neq 0 \right\} \\
\mathrm{Cl}_4(G) &= Z_4 \setminus Z_3(G) &&= \left\{ (b_1^b b_3^d c_1^e)^G \,\middle|\, b \neq 0 \right\} \\
\mathrm{Cl}_5(G) &= N \setminus Z_4(G) &&= \left\{ (a_2^a b_2^c b_3^d c_1^e)^G \,\middle|\, a \neq 0 \right\} \\
\mathrm{Cl}_6(G) &= G \setminus N &&= \left\{ ((a_1 a_2^a)^b c_2^c)^G \,\middle|\, b \neq 0 \right\}
\end{aligned}$$

The case of $\mathrm{Cl}_0(G)$ and $\mathrm{Cl}_1(G)$ is obvious. For $\mathrm{Cl}_6(G)$, note that conjugation by a_2, b_1, b_2, and b_3, can be used to produce any desired power of b_1, b_2, b_3 and c_1. However, the power of c_2 cannot be chosen in this way. Conjugating by a_1 will never produce c_2, so the class representatives are as stated.

For the rest of the classes, conjugation by a_1 can be used to get desired powers of the "missing" element. For example, the leading element of $\mathrm{Cl}_5(G)$ is a_2, so powers of b_1 are "missing" because they can be obtained through conjugation by a_1. Of course, only powers of a single element can be produced in this way. Powers of c_2 can be obtained through conjugation by a_2, and the classes are as stated.

Likewise, we group the irreducible characters into disjoint sets. To determine the irreducible characters in each class takes more work than in the case of conjugacy classes. We do this in the following section.

$$\begin{aligned}
\mathrm{Irr}_0(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi \supseteq N\} \\
\mathrm{Irr}_1(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi \supseteq \gamma_2(G), \ker\chi \not\supseteq N\} \\
\mathrm{Irr}_2(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi = \gamma_3(G)\} \\
\mathrm{Irr}_3(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi = \gamma_4(G)\} \\
\mathrm{Irr}_4(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi = \gamma_5(G)\} \\
\mathrm{Irr}_5(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi = C\} \\
\mathrm{Irr}_6(G) &= \{\chi \in \mathrm{Irr}(G) \mid \ker\chi \subseteq Z(G), \ker\chi \neq C\}
\end{aligned}$$

5.3.1 Determination of Characters

The characters in $\mathrm{Irr}_0(G)$ are obvious. We shall save $\mathrm{Irr}_6(G)$ for later, and deal with $\mathrm{Irr}_1(G)$ through $\mathrm{Irr}_5(G)$ now.

Because $[G, N] = \langle c_2 \rangle$, it is easy to see that N/C is an abelian group with generators a_2, b_1, b_2, b_3, and c_1. Fix ω, a primitive pth root of unity, and define $\varphi_{a_2} \in \mathrm{Irr}(N/C)$ as

$$\varphi_{a_2}(a_2^a b_1^b b_2^c b_3^d c_1^e) = \omega^a.$$

Define φ_{b_1}, φ_{b_2}, φ_{b_3}, and φ_{c_1} similarly, and then any $\chi \in \mathrm{Irr}(N/C)$ is the product of powers of these characters. We then induce these characters from N/C to G/C and lift to G.

The powers of a_1 give a set of coset representatives for N. Using $x = a_2^a b_1^b b_2^c b_3^d c_1^e$ and $\chi = \varphi_{a_2}^j \varphi_{b_1}^k \varphi_{b_2}^l \varphi_{b_3}^m \varphi_{c_1}^n$ it is a long, but simple calculation to show

$$(a_2^a b_1^b b_2^c b_3^d c_1^e)^{a_1^i} = a_2^a b_1^{b+ia} b_2^{c+ib+a\binom{i}{2}} b_3^{d+ic+b\binom{i}{2}+a\binom{i}{3}} c_1^{e+id+c\binom{i}{2}+b\binom{i}{3}+a\binom{i}{4}}$$

and then

$$\chi^G(x) = \sum_{i=0}^{p-1} \chi^\circ\left(a_2^a b_1^{b+ia} b_2^{c+ib+a\binom{i}{2}} b_3^{d+ic+b\binom{i}{2}+a\binom{i}{3}} c_1^{e+id+c\binom{i}{2}+b\binom{i}{3}+a\binom{i}{4}} \right).$$

Since χ is linear on N/C, we have

$$= \sum_{i=0}^{p-1} \varphi_{a_2}^j(a_2^a)\varphi_{b_1}^k(b_1^{b+ia})\varphi_{b_2}^l\left(b_2^{c+ib+a\binom{i}{2}}\right)$$
$$\varphi_{b_3}^m\left(b_3^{d+ic+b\binom{i}{2}+a\binom{i}{3}}\right)\varphi_{c_1}^n\left(c_1^{e+id+c\binom{i}{2}+b\binom{i}{3}+a\binom{i}{4}}\right)$$
$$\chi^G(x) = \omega^{ja+kb+lc+md+ne} \sum_{i=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mic+mb\binom{i}{2}+ma\binom{i}{3}+nid+nc\binom{i}{2}+nb\binom{i}{3}+na\binom{i}{4}}. \qquad (5.1)$$

Proposition 5.3.1. *Inducing nontrivial characters from N/C to G/C preserves irreducibility.*

Proof. With notation as before we have

$$\begin{aligned}
[\chi^{G/C}, \chi^{G/C}]_{G/C} &= [\chi^{G/C}|_{N/C}, \chi]_{N/C} \\
&= \frac{1}{|N/C|} \sum_{x \in N/C} \chi^G(x)\overline{\chi(x)} \\
&= \frac{1}{p^5} \sum_{i,a,b,c,d,e=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mic+mb\binom{i}{2}+ma\binom{i}{3}+nid+nc\binom{i}{2}+nb\binom{i}{3}+na\binom{i}{4}}
\end{aligned}$$

and since e doesn't appear in the sum, it simplifies to

$$= \frac{1}{p^4} \sum_{i,a,b,c,d=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mic+mb\binom{i}{2}+ma\binom{i}{3}+nid+nc\binom{i}{2}+nb\binom{i}{3}+na\binom{i}{4}}.$$

Considering the exponent d we find

$$= \frac{1}{p^4} \sum_{i,a,b,c,d=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mic+mb\binom{i}{2}+ma\binom{i}{3}+nc\binom{i}{2}+nb\binom{i}{3}+na\binom{i}{4}} \begin{cases} p & ni = 0 \\ 0 & ni \neq 0 \end{cases}$$

and if $n \neq 0$, then i must be 0 and the whole sum simplifies to p^4. We now consider the case when $n = 0$ and eliminate the exponent c using the same method.

$$= \frac{1}{p^3} \sum_{i,a,b,c=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mic+mb\binom{i}{2}+ma\binom{i}{3}}$$
$$= \frac{1}{p^3} \sum_{i,a,b=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}+mb\binom{i}{2}+ma\binom{i}{3}} \begin{cases} p & mi = 0 \\ 0 & mi \neq 0 \end{cases}$$

Again if $m \neq 0$, then the sum simplifies to p^3, so we consider $m = 0$, and so on

$$= \frac{1}{p^2} \sum_{i,a,b=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}} = \frac{1}{p^2} \sum_{i,a=0}^{p-1} \omega^{kia+la\binom{i}{2}} \begin{cases} p & ci = 0 \\ 0 & ci \neq 0 \end{cases}$$
$$= \frac{1}{p} \sum_{i,a=0}^{p-1} \omega^{kia} = 1$$

since not all of j, k, l, m, and n can be 0. ■

Define φ_{a_1} in the manner similar to before, namely as the character (this time of G) which takes value ω on a_1 and 1 on the other generators. We shall use φ_{a_2} to indicate either a character of N or of G defined in the same way and distinguish based on context.

Proposition 5.3.2. *The sets* $\mathrm{Irr}_0(G)$ *through* $\mathrm{Irr}_5(G)$ *can be parametrized as*

$$\begin{aligned}
\mathrm{Irr}_0(G) &= \left\{\varphi_{a_1}^i\right\}, \\
\mathrm{Irr}_1(G) &= \left\{\varphi_{a_1}^i \varphi_{a_2}^j \,\middle|\, j \neq 0\right\}, \\
\mathrm{Irr}_2(G) &= \left\{(\varphi_{b_1}^k)^G \,\middle|\, k \neq 0\right\}, \\
\mathrm{Irr}_3(G) &= \left\{(\varphi_{a_2}^j \varphi_{b_2}^l)^G \,\middle|\, l \neq 0\right\}, \\
\mathrm{Irr}_4(G) &= \left\{(\varphi_{a_2}^j \varphi_{b_1}^k \varphi_{b_3}^m)^G \,\middle|\, m \neq 0\right\}, \\
\mathrm{Irr}_5(G) &= \left\{(\varphi_{a_2}^j \varphi_{b_1}^k \varphi_{b_2}^l \varphi_{c_1}^n)^G \,\middle|\, n \neq 0\right\}.
\end{aligned}$$

Corollary 5.3.3. *The characters in* $\mathrm{Irr}_0(G)$ *through* $\mathrm{Irr}_5(G)$ *comprise all characters of* G/C.

Proof. The characters in $\mathrm{Irr}_2(G)$ through $\mathrm{Irr}_5(G)$ have degree p, so simply calculate

$$\begin{aligned}\sum_{i=0}^{5}|\mathrm{Irr}_i(G)|\chi(1)^2 &= p + p(p-1) + p^2(p-1) + p^3(p-1) + p^4(p-1) + p^5(p-1)\\ &= p^6 = |G/C|. \quad \blacksquare\end{aligned}$$

Proof of 5.3.2. The cases of $\mathrm{Irr}_0(G)$ and $\mathrm{Irr}_1(G)$ are obvious. All the other cases are basically identical, so we work through $\mathrm{Irr}_3(G)$ as an example. In this case, $l \neq 0$ and $m = n = 0$, so (5.1) simplifies to

$$\chi^G(x) = \omega^{ja+kb+lc} \sum_{i=0}^{p-1} \omega^{kia+lib+la\binom{i}{2}}.$$

If $a = b = 0$ ($x \in \mathrm{Cl}_{1,2,3}(G)$), then $\chi^G(x) = p\chi(x)$, and if $a = 0$, $b \neq 0$ ($x \in \mathrm{Cl}_4(G)$) then $\chi^G(x) = 0$. It is always the case that $\chi^G(x) = 0$ when $\chi \in \mathrm{Irr}_i(G)$ and $g \in \mathrm{Cl}_{i+1}(G)$

Now suppose $a \neq 0$. Then the choice of k is redundant which can be seen by letting $k = k' + l$ and relabeling the sum by replacing i with $i - 1$. Relabeling the sum doesn't change it since the terms depend only on the value of i mod p. These changes give

$$\begin{aligned}\chi^G(x) &= \omega^{ja+(k'+l)b+lc} \sum_{i=0}^{p-1} \omega^{k'ia+lib+la\binom{i}{2}-k'a-lb}\\ &= \omega^{(j-k')a+(k'+l-l)b+lc} \sum_{i=0}^{p-1} \omega^{k'ia+lib+la\binom{i}{2}}\\ &= \omega^{(j-k')a+k'b+lc} \sum_{i=0}^{p-1} \omega^{k'ia+lib+la\binom{i}{2}}\end{aligned}$$

so that changing the value of k is equivalent to changing the value of j. Thus, there are

$p(p-1)$ distinct characters, namely

$$\mathrm{Irr}_3(G) = \left\{ (\varphi_{a_2}^j \varphi_{b_2}^l)^G \,\middle|\, l \neq 0 \right\}.$$

For the general case, consider the exponent of ω as a polynomial in i. Once the leading coefficient is fixed, the next term can vary arbitrarily. The result is multiplication by a power of ω, but such multiplication can also be achieved by changing the lower terms. What this means is that the second to last exponent in $\chi = \varphi_{a_2}^j \varphi_{b_1}^k \varphi_{b_2}^l \varphi_{b_3}^m \varphi_{c_1}^n$ is irrelevant. Notice that this is the dual of the case for conjugacy classes. ■

Characters in $\mathrm{Irr}_6(G)$

The case of $\mathrm{Irr}_6(G)$ is quite different. Let x be an element of $G \setminus N$, then $\langle x \rangle G'$ is one of p different groups. We may assume for simplicity that $x = a_1 a_2^a$ with $0 \leq a < p$, and define $H_x = \langle x, b_2, b_3, c_1, c_2 \rangle$. Inducing certain linear characters from H_x will give rise to irreducible characters of degree p^2. Let χ be a linear character of H_x. Of course, $[H_x, H_x]$ must be in its kernel. Because $[b_2, b_3] = 1$, $H_x' = \langle [b_2, x], [b_3, x] \rangle$ so that $|H_x'| = p^2$. In particular $[b_3, a_1 a_2^a] = c_1 c_2^a$ is in the kernel. Since $[b_2, x] = b_3 c_2^a$ is not central, c_2 is not forced to be in the kernel of χ. In fact, c_2 cannot be in the kernel or the induced character wouldn't be in $\mathrm{Irr}_6(G)$.

Thus, we have p independent choices for each of $\chi(x)$ and $\chi(b_2)$, and $p-1$ choices for the value of $\chi(c_2)$. It can happen that $x^p \neq 1$, in which case $\chi(x)^p$ is a fixed power of $\chi(c_2)$, but we can choose such a value in p ways. We shall see, however, that the choices for $\chi(b_2)$ are unimportant. In the end we have p choices for H_x, each of which gives $p(p-1)$ distinct characters of degree p^2. Combining these characters with those of $\mathrm{Irr}_{0,\ldots,5}(G)$ we have

$$p^6 + p^4|\mathrm{Irr}_6(G)| = p^6 + p^6(p-1) = p^7 = |G|$$

so that there are enough of these characters once we prove they are irreducible and distinct.

We must first spend some time calculating the value of χ^G. It is easy to see that $\left\{ b_1^i a_2^j \,\middle|\, 0 \leq i,j < p \right\}$ is a set of coset representatives of H_x. Since $\mathrm{Cl}_4(G)$ and $\mathrm{Cl}_5(G)$ intersect H_x trivially, $\chi^G = 0$ on them. We turn our attention to $\mathrm{Cl}_{0,1,2,3}(G)$:

$$\begin{aligned}
\chi^G(b_2^c b_3^d c_1^e c_2^f) &= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi^\circ(a_2^{-j} b_1^{-i} (b_2^c b_3^d c_1^e c_2^f) b_1^i a_2^j) \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi(a_2^{-j} (b_2^c b_3^d c_2^{ic}) a_2^j \cdot c_1^e c_2^f) \\
&= \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi(b_2^c b_3^d c_1^e c_2^{f-ic+j(c+d)})
\end{aligned}$$

and since χ is linear on H_x,

$$\begin{aligned}
&= \chi(b_2^c b_3^d c_1^e c_2^f) \sum_{i=0}^{p-1}\sum_{j=0}^{p-1} \chi(c_2^{-ic+jc+jd}) \\
&= \chi(b_2^c b_3^d c_1^e c_2^f) \sum_{i=0}^{p-1} \chi(c_2)^{-ic} \sum_{j=0}^{p-1} \chi(c_2)^{j(c+d)}.
\end{aligned}$$

Unless $c = 0$ the first sum will be zero. On the other hand, if $c = 0$ the second sum will be zero unless d is also 0. If $c = d = 0$, then we are in the center and

$$\chi^G(c_1^e c_2^f) = p^2\chi(c_1^e c_2^f) = p^2\chi(c_1^e c_2^{ae})\chi(c_2^{f-ae}) = p^2\chi(c_2^{f-ae}). \tag{5.2}$$

Portions of $\mathrm{Cl}_6(G)$ intersect H_x. In fact, $\mathrm{Cl}_6(G)$ can be broken up into p different sets, each corresponding to H_x for a different x. As noted at the beginning of this section, a conjugacy class in $\mathrm{Cl}_6(G)$ has a representative of the form $(a_1 a_2^a)^b c_2^c$ with $b \neq 0$. Since the powers of a_1 and a_2 are invariant under conjugation, $\chi^G = 0$ except on a conjugacy class of the form $(x^b c_2^c)^G$. Thus, we only need to consider the value that it takes on such conjugacy classes:

$$\chi^G((a_1 a_2^a)^b c_2^c) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \chi^\circ(b_1^{-j} a_2^{-i}\ (a_1 a_2^a)^b c_2^c\ a_2^i b_1^j).$$

If we consider conjugation by a_2, we get (ignoring powers of elements other than b_1)

$$= \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \chi^\circ(b_1^{-j}\ (a_1 a_2^a)^b b_1^{ib} \cdots c_2^c\ b_1^j).$$

Of course, conjugation by b_1 will not change the power of b_1. Hence, this element is in H_x only if $ib = 0$, and the sum simplifies to the case $i = 0$:

$$= \sum_{j=0}^{p-1} \chi^\circ(b_1^{-j}\ (a_1 a_2^a)^b c_2^c\ b_1^j).$$

We next multiply out x^b. There are some extra powers of c_2 involved, but they are irrelevant (as we shall see) and messy so we denote them by $*$ to get

$$\begin{aligned}
&= \sum_{j=0}^{p-1} \chi^\circ(b_1^{-j}(a_1^b a_2^{ab} b_1^{a\binom{b}{2}} b_2^{a\binom{b}{3}} b_3^{a\binom{b}{4}} c_1^{a\binom{b}{5}} c_2^{c+*}) b_1^j) \\
&= \sum_{j=0}^{p-1} \chi^\circ((b_1^{-j} a_1^b b_1^j) a_2^{ab} b_1^{a\binom{b}{2}} b_2^{a\binom{b}{3}} b_3^{a\binom{b}{4}} c_1^{a\binom{b}{5}} c_2^{c+*} c_2^{-aj\binom{b}{3}}) \\
&= \sum_{j=0}^{p-1} \chi^\circ(a_1^b a_2^{ab} b_1^{a\binom{b}{2}} b_2^{a\binom{b}{3}} b_3^{a\binom{b}{4}} c_1^{a\binom{b}{5}} c_2^{*} \\
&\qquad b_2^{-jb} b_3^{-j\binom{b}{2}} c_1^{-j\binom{b}{3}} c_2^{c+b\binom{j}{2}-aj\binom{b}{3}-ajb\binom{b}{2}-ajb^2+ajb\binom{b}{2}})
\end{aligned}$$

$$= \sum_{j=0}^{p-1} \chi^\circ((a_1a_2^a)^b b_2^{-jb} b_3^{-j\binom{b}{2}} c_1^{-j\binom{b}{3}} c_2^{c+b\binom{j}{2}-aj\binom{b}{3}-ajb^2}).$$

We are now in H_x where χ is linear, so

$$= \sum_{j=0}^{p-1} \chi(x^b)\chi(b_2^{-jb})\chi(b_3^{-j\binom{b}{2}} c_2^{-aj\binom{b}{2}})\chi(c_1^{-j\binom{b}{3}} c_2^{-aj\binom{b}{3}})$$
$$\chi(c_2^{c+b\binom{j}{2}-aj\binom{b}{3}-ajb^2+aj\binom{b}{2}+aj\binom{b}{3}}).$$

Since the kernel of χ contains both $[b_2, a_1a_2^a] = b_3c_2^a$ and $[b_3, a_1a_2^a] = c_1c_2^a$, we have

$$= \sum_{j=0}^{p-1} \chi(x)^b \chi(b_2)^{-jb} \chi(c_2)^{c+b\binom{j}{2}-ajb^2+aj\binom{b}{2}}$$
$$= \chi(x)^b \chi(c_2)^c \sum_{j=0}^{p-1} \chi(b_2)^{-jb} \chi(c_2)^{-jb(ab+a-j+1)/2}.$$

For simplicity we relabel the sum, changing j to $-j$ for a final form of

$$\chi^G((a_1a_2^a)^b c_2^c) = \chi(a_1a_2^a)^b \chi(c_2)^c \sum_{j=0}^{p-1} \chi(b_2)^{jb} \chi(c_2)^{jb(ab+a+j+1)/2}.$$

Proposition 5.3.4. *When enumerating the characters $\chi^G \in \mathrm{Irr}_6(G)$, the choice of $\chi(b_2)$ is redundant.*

Proof. To show the redundancy of $\chi(b_2)$, we first substitute $\chi(b_2) = \omega^m$ and $\chi(c_2) = \omega^l$. Fix ζ such that $\zeta^p = \omega$. Then, $\chi(x)^p = \chi(c_2)^r$ for some r depending only on x (it is possible that $r = 0$). In other words, $\chi(x) = \zeta^{rl+kp} = \zeta^{rl}\omega^k$. This gives

$$\chi((a_1a_2^a)^b c_2^c) = \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{bk+cl+jbm+\frac{jbl}{2}(a(b+1)+j+1)}. \tag{5.3}$$

CEU eTD Collection

We can now make substitutions of $k = k' - m' - \frac{al}{2}(b+1)$ and $m = m' - l$ to find

$$
\begin{aligned}
&= \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{b(k'-m'-\frac{al}{2}(b+1))+cl+jb(m'-l)+\frac{jbl}{2}(a(b+1)+j+1)} \\
&= \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{bk'+cl+jbm'-bm'-\frac{abl}{2}(b+1)-jbl+\frac{jbl}{2}(a(b+1)+j+1)} \\
&= \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{bk'+cl+(j-1)bm'+\frac{jbl}{2}(a(b+1)+j+1)-\frac{jbl}{2}-\frac{abl}{2}(b+1)-\frac{jbl}{2}} \\
&= \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{bk'+cl+(j-1)bm'+\frac{jbl}{2}(a(b+1)+(j-1)+1)-\frac{bl}{2}(a(b+1)-(j-1)+1)} \\
&= \sum_{j=0}^{p-1} \zeta^{rbl} \omega^{bk'+cl+(j-1)bm'+\frac{(j-1)bl}{2}(a(b+1)+(j-1)+1)}
\end{aligned}
$$

which, of course, is the same by re-indexing the sum. Since $b \neq 0$ we can obtain any value of m that we want without changing the sum simply by choosing a new k. Thus, we may assume that $m = \frac{al^2-l}{2}$, which will be convenient later. It is important to note that only k was changed to account for different m, so this choice of m will not restrict our choice of l. ■

Proposition 5.3.5. *Suppose that $\psi \in \mathrm{Irr}_6(G)$ as described. Then ψ is irreducible.*

Proof. Let $\psi \in \mathrm{Irr}_6(G)$, and suppose $\varphi \in \mathrm{Irr}_6(G)$ is induced from another H_x, then their product is nonzero only on the center where they restrict homogeneously to distinct characters (they have distinct kernels). Thus, $[\psi, \varphi] = 0$. This same argument holds for all $\varphi \in \mathrm{Irr}(G)$ unless φ is linear. Suppose φ is linear,

$$
\begin{aligned}
[\psi = \chi^G, \varphi] &= \sum_{g \in G} \psi(g)\overline{\varphi(g)} \\
&= \sum_{g \in Z(G)} \psi(g)1 + \sum_{b,c} \left|(x^b c_2^c)^G\right| \psi(x^b c_2^c)\overline{\varphi(x^b)}
\end{aligned}
$$

then $\varphi(x) = \overline{\omega}$ is a pth root of unity.

$$= 0 + p^4 \sum_{b,c} \psi(x^b c_2^c) \omega^b$$
$$= p^4 \sum_b \chi(x)^b \omega^b \sum_j \chi(b_2)^{jb} \chi(c_2)^{jb(ab+a+j+1)/2} \sum_c \chi(c_2)^c$$

and since $\chi(c_2) \neq 1$, the sum over c is zero.

The final case is when ψ and φ are both induced from the same H_x.

$$\begin{aligned} |G|[\psi = \chi^G, \varphi = \eta^G] &= \sum_{g \in G} \psi(g) \overline{\varphi(g)} \\ &= \sum_{g \in Z(G)} \psi(g) \overline{\varphi(g)} + \sum_{b=1,c=0}^{p-1} \left| (x^b c_2^c)^G \right| \psi(x^b c_2^c) \overline{\varphi(x^b c_2^c)} \\ &= \sum_{g \in Z(G)} p^4 \chi(g) \overline{\eta(g)} + p^4 \sum_{b,c} \psi(x^b c_2^c) \overline{\varphi(x^b c_2^c)} \\ &= p^6 \delta_{\chi(c_2),\eta(c_2)} + p^4 \sum_{i,j,b,c} \chi(x)^b \chi(c_2)^c \overline{\eta(x)^b \eta(c_2)^c} \chi(c_2)^{\cdots} \overline{\eta(c_2)^{\cdots}} \end{aligned}$$

For the moment we omit the exponents of $\chi(c_2)$ and $\eta(c_2)$, though we shall add them later. As we shall see, c is not involved in these exponents, so we can pull out the sum over c.

$$= p^6 \delta_{\chi(c_2),\eta(c_2)} + p^4 \sum_c \chi(c_2)^c \overline{\eta(c_2)^c} \sum_{i,j,b} \chi(x)^b \overline{\eta(x)^b} \chi(c_2)^{\cdots} \overline{\eta(c_2)^{\cdots}}$$

If $\chi(c_2) \neq \eta(c_2)$, then the sum over c is zero (and the first term is as well), so assume that $\chi(c_2) = \eta(c_2)$. That is, the l's in each exponent are the same. We use the value of $m = (al^2 - l)/2$ and (5.3) to find

$$= p^6 + p^5 \sum_{i,j,b} \chi(x)^b \overline{\eta(x)^b} \omega^{ibl(ab+al+a+i)/2} \omega^{-jbl(ab+al+a+j)/2}$$

$$= p^6 + p^5 \sum_{i,j,b} \chi(x)^b \overline{\eta(x)^b} \omega^{ibl(ab+al+a+i)/2 - jbl(ab+al+a+j)/2}$$

Relabeling $j = j + i$

$$\begin{aligned}
&= p^6 + p^5 \sum_{i,j,b} \chi(x)^b \overline{\eta(x)^b} \omega^{ibl(ab+al+a+i)/2 - (j+i)bl(ab+al+a+(j+i))/2} \\
&= p^6 + p^5 \sum_b (\chi(x)\overline{\eta(x)})^b \sum_j \omega^{-jbl(ab+al+a+j)/2} \sum_i \omega^{-ijbl} \\
&= p^6 + p^5 \sum_b (\chi(x)\overline{\eta(x)})^b \sum_j \omega^{-jbl(ab+al+a+j)/2} p\delta_{j,0} \\
&= p^6 + p^6 \sum_{b=1}^{p-1} (\chi(x)\overline{\eta(x)})^b \\
&= p^6 + p^6 \left(-1 + \sum_{b=0} (\chi(x)\overline{\eta(x)})^b \right) \\
&= p^6 + p^6(-1 + p\delta_{\chi(x),\eta(x)}) = |G|\delta_{\chi,\eta} \quad \blacksquare
\end{aligned}$$

Enumerating the characters in $\mathrm{Irr}_6(G)$ is slightly different than the other cases. We would like $\varphi_{a_1 a_2^a}$ to be the character of $H_{a_1 a_2^a}$ which sends $a_1 a_2^a$ to ω and φ_{c_2} the character sending c_2 to ω. However, for $\chi \in \mathrm{Irr}_6(G)$ the value on x must be of the form $\chi(x) = \zeta^{rl+kp} = \zeta^{rl}\omega^k$ (see equation (5.3)), which depends on $\chi(c_2)$ for l and on x for r. For this reason we must write $\varphi^{k,l}_{a_1 a_2^a c_2}$ to be the character sending $c_2 \mapsto \omega^l$ and $x \mapsto \zeta^{rl+kp} = \zeta^{rl}\omega^k$. This definition allows us to enumerate the characters of $\mathrm{Irr}_6(G)$ in a similar style to the others:

$$\mathrm{Irr}_6(G) = \left\{ (\varphi^{k,l}_{a_1 a_2^a c_2})^G \,\middle|\, l \neq 0 \right\}.$$

Note that the set also ranges over a.

We now have enough information to prove that G is transposable.

5.3.2 Duality

For each set of characters, we have already determined the sets of conjugacy classes that are in the kernel and those where the characters are zero. This information is summarized in Table 5.1 where, in addition, c indicates that the elements are in the center of the characters, and $*$ indicates some other relation. Table 5.2 recalls our labeling of irreducible characters and conjugacy classes.

We define a bijection, called **reversal**, between conjugacy classes and characters by "reversing the presentation." Or, more explicitly, $c_2 \leftrightarrow \varphi_{a_1}$, $c_1 \leftrightarrow \varphi_{a_2}$, $b_i \leftrightarrow \varphi_{b_{4-i}}$, $a_2 \leftrightarrow \varphi_{c_1}$, and $a_1 \leftrightarrow \varphi_{c_2}$. Reversal between $\mathrm{Cl}_6(G)$ and $\mathrm{Irr}_6(G)$ is slightly different with $(a_1 a_2^a)^b c_2^c$ corresponding to $\varphi^{c,b}_{a_1 a_2^{-a} c_2}$. Note the negation of a in this case.

Table 5.1: Known values of $\chi(g)$

	$\mathrm{Cl}_0(G)$	$\mathrm{Cl}_1(G)$	$\mathrm{Cl}_2(G)$	$\mathrm{Cl}_3(G)$	$\mathrm{Cl}_4(G)$	$\mathrm{Cl}_5(G)$	$\mathrm{Cl}_6(G)$
$\mathrm{Irr}_0(G)$	1	1	1	1	1	1	c
$\mathrm{Irr}_1(G)$	1	1	1	1	1	c	c
$\mathrm{Irr}_2(G)$	1	1	1	1	c	0	0
$\mathrm{Irr}_3(G)$	1	1	1	c	0	$*$	0
$\mathrm{Irr}_4(G)$	1	1	c	0	$*$	$*$	0
$\mathrm{Irr}_5(G)$	1	c	0	$*$	$*$	$*$	0
$\mathrm{Irr}_6(G)$	c	c	0	0	0	0	$*$

Proposition 5.3.6. *Reversal defines the transpose of the character table.*

Proof. We shall treat $\mathrm{Irr}_6(G)$ specially and proceed by verifying the self-duality criteria: $\chi(g)\sqrt{|g^G|} = \varphi_g(h_\chi)\sqrt{|(h_\chi)^G|}$ when $\chi \leftrightarrow h$ and $g \leftrightarrow \eta$. Entries in Table 5.1 that are 0 or 1 can be ignored.

Let $\chi \in \mathrm{Irr}_1(G)$ and $\mathcal{K} \in \mathrm{Cl}_5(G)$, and let $\eta \in \mathrm{Irr}_5(G)$ and $\mathcal{K}' \in \mathrm{Cl}_1(G)$ be their duals.

Table 5.2: Representative characters and classes

$$\begin{aligned}
\mathrm{Cl}_0(G) &= \left\{(c_2^f)^G\right\} & \mathrm{Irr}_0(G) &= \left\{\varphi^i_{a_1}\right\}\\
\mathrm{Cl}_1(G) &= \left\{(c_1^e c_2^f)^G \,\middle|\, e \neq 0\right\} & \mathrm{Irr}_1(G) &= \left\{\varphi^i_{a_1}\varphi^j_{a_2} \,\middle|\, j \neq 0\right\}\\
\mathrm{Cl}_2(G) &= \left\{(b_3^d)^G \,\middle|\, d \neq 0\right\} & \mathrm{Irr}_2(G) &= \left\{(\varphi^k_{b_1})^G \,\middle|\, k \neq 0\right\}\\
\mathrm{Cl}_3(G) &= \left\{(b_2^c c_1^e)^G \,\middle|\, c \neq 0\right\} & \mathrm{Irr}_3(G) &= \left\{(\varphi^j_{a_2}\varphi^l_{b_2})^G \,\middle|\, l \neq 0\right\}\\
\mathrm{Cl}_4(G) &= \left\{(b_1^b b_3^d c_1^e)^G \,\middle|\, b \neq 0\right\} & \mathrm{Irr}_4(G) &= \left\{(\varphi^j_{a_2}\varphi^k_{b_1}\varphi^m_{b_3})^G \,\middle|\, m \neq 0\right\}\\
\mathrm{Cl}_5(G) &= \left\{(a_2^a b_2^c b_3^d c_1^e)^G \,\middle|\, a \neq 0\right\} & \mathrm{Irr}_5(G) &= \left\{(\varphi^j_{a_2}\varphi^k_{b_1}\varphi^l_{b_2}\varphi^n_{c_1})^G \,\middle|\, n \neq 0\right\}\\
\mathrm{Cl}_6(G) &= \left\{((a_1 a_2^a)^b c_2^c)^G \,\middle|\, a \neq 0\right\} & \mathrm{Irr}_6(G) &= \left\{(\varphi^{k,l}_{a_1 a_2^a c_2})^G \,\middle|\, l \neq 0\right\}
\end{aligned}$$

Then

$$\begin{aligned}
\chi(a_2^a b_1^c b_3^d c_1^e)\sqrt{|\mathcal{K}|} &= p(\varphi^i_{a_1}\varphi^j_{a_2})(a_2^a b_1^c b_3^d c_1^e) = p\varphi^j_{a_2}(a_2^a)\\
&= p\omega^{aj} = p\varphi^a_{c_1}(c_1^j c_2^i) = p(\varphi^e_{a_2}\varphi^d_{b_1}\varphi^c_{b_2}\varphi^a_{c_1})^G(c_1^j c_2^i)\\
&= \eta(c_1^j c_2^i)\sqrt{|\mathcal{K}'|}.
\end{aligned}$$

We treat the rest of the cases (except $\mathrm{Irr}_6(G)$) simultaneously. For all these cases $\sqrt{\mathcal{K}} = p$, so we can ignore it in our calculations:

$$\begin{aligned}
\chi(g) &= (\varphi^j_{a_2}\varphi^k_{b_1}\varphi^l_{b_2}\varphi^m_{b_3}\varphi^n_{c_1})^G(a_2^a b_1^b b_2^c b_3^d c_1^e)\\
&= \omega^{ja+kb+lc+md+ne}\sum_{i=0}^{p-1}\omega^{kai+lbi+mci+ndi+la\binom{i}{2}+mb\binom{i}{2}+nc\binom{i}{2}+ma\binom{i}{3}+nb\binom{i}{3}+na\binom{i}{4}}\\
&= \omega^{en+dm+cl+bk+aj}\sum_{i=0}^{p-1}\omega^{dni+cmi+bli+aki+cn\binom{i}{2}+bm\binom{i}{2}+al\binom{i}{2}+bn\binom{i}{3}+am\binom{i}{3}+an\binom{i}{4}}\\
&= (\varphi^e_{a_2}\varphi^d_{b_1}\varphi^c_{b_2}\varphi^b_{b_3}\varphi^a_{c_1})^G(a_2^n b_1^m b_2^l b_3^k c_1^j).
\end{aligned}$$

Finally, we must deal with the cases of $\mathrm{Irr}_{0,6}(G)$ and $\mathrm{Cl}_{0,6}(G)$. The characters from $\mathrm{Irr}_6(G)$ are nonzero only on $\mathrm{Cl}_6(G)$ and the center.

Suppose that $\chi \in \mathrm{Irr}_6(G)$, and let $g \in Z(G)$. Then, from (5.2)

$$\begin{aligned}
\chi(g)\sqrt{|g^G|} &= (\varphi^{k,l}_{a_1 a_2^a c_2})^G(c_1^e c_2^f) \\
&= p^2 \varphi^l_{c_2}(c_2^{f-ae}) \\
&= p^2 \omega^{fl-ael} \\
&= p^2 \varphi^f_{a_1}(a_1^l)\varphi^e_{a_2}(a_2^{-al}) \\
&= (\varphi^f_{a_1}\varphi^e_{a_2})(a_1^l a_2^{-al} c_2^k)p^2 \\
&= (\varphi^f_{a_1}\varphi^e_{a_2})((a_1 a_2^{-a})^l c_2^k)\sqrt{|((a_1 a_2^{-a})^l c_2^k)^G|}.
\end{aligned}$$

Finally, we handle the case of $\chi \in \mathrm{Irr}_6(G)$ and $g \in \mathrm{Cl}_6(G)$. Since the size of the conjugacy classes will be the same before and after reversal, they are omitted from the calculation. We also know that χ is zero except on conjugacy classes of the right form: those for which the exponent a is the same. Thus, using equation (5.3)

$$\begin{aligned}
\chi(g) &= (\varphi^{k,l}_{a_1 a_2^a c_2})^G((a_1 a_2^a)^b c_2^c) \\
&= \varphi^k_{a_1 a_2^a}(a_1 a_2^a)^b \varphi^l_{c_2}(c_2)^c \sum_{i=0}^{p-1} \varphi^l_{c_2}(c_2)^{ib(ab+al+a+i)/2} \\
&= \zeta^{brl}\omega^{kb+lc}\sum_{i=0}^{p-1}\omega^{ibl(ab+al+a+i)/2} = \zeta^{lrb}\omega^{cl+bk}\sum_{i=0}^{p-1}\omega^{-ilb(-al-ab-a-i)/2} \\
&= \zeta^{lrb}\omega^{cl+bk}\sum_{i=0}^{p-1}\omega^{ilb(-al-ab-a+i)/2} \\
&= \varphi^c_{a_1 a_2^{-a}}(a_1 a_2^{-a})^l \varphi^b_{c_2}(c_2)^k \sum_{i=0}^{p-1}\varphi^b_{c_2}(c_2)^{il(-al-ab-a+i)/2} \\
&= (\varphi^{c,b}_{a_1 a_2^{-a} c_2})^G((a_1 a_2^{-a})^l c_2^k). \quad \blacksquare
\end{aligned}$$

References

[Ada+96] S. Adami, M. Bianchi, A. Gillio Berta Mauri, and M. Herzog. "On graph-complete groups". In: *Istit. Lombardo Accad. Sci. Lett. Rend. A* 130.1-2 (1996), 295–307 (1997). ISSN: 0021-2504.

[Ada06] Edith Adan-Bante. "Homogeneous products of conjugacy classes". In: *Arch. Math. (Basel)* 86.4 (2006), pp. 289–294. ISSN: 0003-889X.

[AH13] Ivan Andrus and Pál Hegedűs. "Determination of conjugacy class sizes from products of characters". In: *Arch. Math. (Basel)* 100.1 (2013), pp. 1–6. ISSN: 0003-889X.

[AHO12] Ivan Andrus, Pál Hegedűs, and Tetsuro Okuyama. "Transposable character tables, dual groups". In: (Dec. 2012).

[ALM04] Edith Adan-Bante, Maria Loukaki, and Alexander Moretó. "Homogeneous products of characters". In: *Journal of Algebra* 274.2 (2004), pp. 587–593. ISSN: 0021-8693.

[Ban93] Eiichi Bannai. "Association schemes and fusion algebras (an introduction)". In: *J. Algebraic Combin.* 2.4 (1993), pp. 327–344. ISSN: 0925-9899.

[BCH92] Yakov Berkovich, David Chillag, and Marcel Herzog. "Finite groups in which the degrees of the nonlinear irreducible characters are distinct". In: *Proc. Amer. Math. Soc.* 115.4 (1992), pp. 955–959. ISSN: 0002-9939.

[BF06] Antonio Beltrán and María José Felipe. "Variations on a theorem by Alan Camina on conjugacy class sizes". In: *J. Algebra* 296.1 (2006), pp. 253–266. ISSN: 0021-8693.

[BF08a] Antonio Beltrán and María José Felipe. "Corrigendum to: "Variations on a theorem by Alan Camina on conjugacy class sizes" [J. Algebra **296** (2006), no. 1, 253–266;]" in: *J. Algebra* 320.12 (2008), pp. 4317–4319. ISSN: 0021-8693.

[BF08b] Antonio Beltrán and María José Felipe. "Structure of finite groups under certain arithmetical conditions on class sizes". In: *J. Algebra* 319.3 (2008), pp. 897–910. ISSN: 0021-8693.

[BF11] Antonio Beltrán and María José Felipe. "Corrigendum: Some class size conditions implying solvability of finite groups". In: *J. Group Theory* 14.5 (2011), pp. 783–784. ISSN: 1433-5883.

[BHM90] Edward A. Bertram, Marcel Herzog, and Avinoam Mann. "On a graph related to conjugacy classes of groups". In: *Bull. London Math. Soc.* 22.6 (1990), pp. 569–575. ISSN: 0024-6093.

[Bia+07] Mariagrazia Bianchi, David Chillag, Mark L. Lewis, and Emanuele Pacifici. "Character degree graphs that are complete graphs". In: *Proc. Amer. Math. Soc.* 135.3 (2007), 671–676 (electronic). ISSN: 0002-9939.

[Bla09] Harvey I. Blau. "Table algebras". In: *European J. Combin.* 30.6 (2009), pp. 1426–1455. ISSN: 0195-6698.

[Bro12] Kevin A. Broughan. "An explicit bound for aliquot cycles of repdigits." English. In: *Integers* 12.4 (2012), pp. 689–704.

[Cam72] A. R. Camina. "Arithmetical conditions on the conjugacy class numbers of a finite group". In: *J. London Math. Soc. (2)* 5 (1972), pp. 127–132. ISSN: 0024-6107.

[CC00] A. R. Camina and R. D. Camina. "Recognizing direct products from their conjugate type vectors". In: *J. Algebra* 234.2 (2000). Special issue in honor of Helmut Wielandt, pp. 604–608. ISSN: 0021-8693.

[CC11] A. R. Camina and R. D. Camina. "The influence of conjugacy class sizes on the structure of finite groups: a survey". In: *Asian-Eur. J. Math.* 4.4 (2011), pp. 559–588. ISSN: 1793-5571.

[CD09] Carlo Casolo and Silvio Dolfi. "Products of primes in conjugacy class sizes and irreducible character degrees". In: *Israel J. Math.* 174 (2009), pp. 403–418. ISSN: 0021-2172.

[CH07] David Chillag and Marcel Herzog. "Finite groups with extremal conditions on sizes of conjugacy classes and on degrees of irreducible characters". In: *Groups St. Andrews 2005. Vol. 1*. Vol. 339. London Math. Soc. Lecture Note Ser. Cambridge: Cambridge Univ. Press, 2007, pp. 269–273.

[CH08] David Chillag and Marcel Herzog. "Finite groups with almost distinct character degrees". In: *J. Algebra* 319.2 (2008), pp. 716–729. ISSN: 0021-8693.

[CH90] David Chillag and Marcel Herzog. "On the length of the conjugacy classes of finite groups". In: *J. Algebra* 131.1 (1990), pp. 110–125. ISSN: 0021-8693.

[CH93] John Cossey and Trevor Hawkes. "Computing the order of the nilpotent residual of a finite group from knowledge of its group algebra". In: *Arch. Math. (Basel)* 60.2 (1993), pp. 115–120. ISSN: 0003-889X.

[Chi04] David Chillag. "Finite groups with restrictions on the zero sets of their irreducible characters". In: *Algebra Colloq.* 11.3 (2004), pp. 387–398. ISSN: 1005-3867.

[Chi99] David Chillag. "On zeros of characters of finite groups". In: *Proc. Amer. Math. Soc.* 127.4 (1999), pp. 977–983. ISSN: 0002-9939.

[CHM92] John Cossey, Trevor Hawkes, and Avinoam Mann. "A Criterion for a Group to be Nilpotent". In: *Bulletin of the London Mathematical Society* 24.3 (1992), pp. 267–270.

[CHM93] David Chillag, Marcel Herzog, and Avinoam Mann. "On the diameter of a graph related to conjugacy classes of groups". In: *Bull. London Math. Soc.* 25.3 (1993), pp. 255–262. ISSN: 0024-6093.

[CW99] John Cossey and Yanming Wang. "Remarks on the length of conjugacy classes of finite groups". In: *Comm. Algebra* 27.9 (1999), pp. 4347–4353. ISSN: 0092-7872.

[DMN09] Silvio Dolfi, Alexander Moretó, and Gabriel Navarro. "The groups with exactly one class of size a multiple of p". In: *J. Group Theory* 12.2 (2009), pp. 219–234. ISSN: 1433-5883.

[Dol06] Silvio Dolfi. "On independent sets in the class graph of a finite group". In: *J. Algebra* 303.1 (2006), pp. 216–224. ISSN: 0021-8693.

[Dol95] Silvio Dolfi. "Arithmetical conditions on the length of the conjugacy classes of a finite group". In: *J. Algebra* 174.3 (1995), pp. 753–771. ISSN: 0021-8693.

[FA87] Elsa Fisman and Zvi Arad. "A proof of Szep's conjecture on nonsimplicity of certain finite groups". In: *J. Algebra* 108.2 (1987), pp. 340–354. ISSN: 0021-8693.

[FM01] Gustavo A. Fernández-Alcober and Alexander Moretó. "On the number of conjugacy class sizes and character degrees in finite p-groups". In: *Proc. Amer. Math. Soc.* 129.11 (2001), 3201–3204 (electronic). ISSN: 0002-9939.

[Gaj79] Dilip Gajendragadkar. "A characteristic class of characters of finite π-separable groups". In: *J. Algebra* 59.2 (1979), pp. 237–259. ISSN: 0021-8693.

[GAP] *GAP – Groups, Algorithms, and Programming, Version 4.6.4*. The GAP Group. 2013.

[GL99] Stephen M. Gagola and Mark L. Lewis. "A character theoretic condition characterizing nilpotent groups". In: *Communications in Algebra* 27.3 (1999), pp. 1053–1056.

[Han96a] Akihide Hanaki. "A condition on lengths of conjugacy classes and character degrees". In: *Osaka J. Math.* 33.1 (1996), pp. 207–216. ISSN: 0030-6126.

[Han96b] Akihide Hanaki. "Self dual groups and finite symmetric algebras self dual groups and finite symmetric algebras of Loewy length 4". Preprint at `http://math.shinshu-u.ac.jp/~hanaki/notes.html`. 1996.

[Han97] Akihide Hanaki. "Self-dual groups of order p^5 (p an odd prime)". In: *Osaka J. Math.* 34.2 (1997), pp. 357–361. ISSN: 0030-6126.

[HM85] Bertram Huppert and Olaf Manz. “Degree-problems I squarefree character degrees”. In: *Archiv der Mathematik* 45 (2 1985). 10.1007/BF01270483, pp. 125–132. ISSN: 0003-889X.

[HO97] Akihide Hanaki and Tetsuro Okuyama. “Groups with some combinatorial properties”. In: *Osaka J. Math.* 34.2 (1997), pp. 337–356. ISSN: 0030-6126.

[HS06] M. Herzog and J. Schönheim. “On groups of odd order with exactly two non-central conjugacy classes of each size”. In: *Arch. Math. (Basel)* 86.1 (2006), pp. 7–10. ISSN: 0003-889X.

[Ink72] K. Inkeri. “On the diophantine equation $a(x^n - 1)/(x - 1) = y^m$”. In: *Acta Arith.* 21 (1972), pp. 299–311. ISSN: 0065-1036.

[INW99] I. M. Isaacs, Gabriel Navarro, and Thomas R. Wolf. “Finite group elements where no irreducible character vanishes”. In: *J. Algebra* 222.2 (1999), pp. 413–423. ISSN: 0021-8693.

[IP10] Mohammad A. Iranmanesh and Cheryl E. Praeger. “Bipartite divisor graphs for integer subsets”. In: *Graphs Combin.* 26.1 (2010), pp. 95–105. ISSN: 0911-0119.

[IS76] I. M. Isaacs and Stephen D. Smith. “A note on groups of p-length 1”. In: *J. Algebra* 38.2 (1976), pp. 531–535. ISSN: 0021-8693.

[Isa+09] I. M. Isaacs, Alexander Moretó, Gabriel Navarro, and Pham Huu Tiep. “Groups with just one character degree divisible by a given prime”. In: *Trans. Amer. Math. Soc.* 361.12 (2009), pp. 6521–6547. ISSN: 0002-9947.

[Isa76] Irving Martin Isaacs. *Character theory of finite groups*. English. New York: Academic Press, 1976, xii, 303 p. ISBN: 0123745500.

[Itô51] Noboru Itô. “On the degrees of irreducible representations of a finite group”. In: *Nagoya Math. J.* 3 (1951), pp. 5–6. ISSN: 0027-7630.

[Itô53] Noboru Itô. “On finite groups with given conjugate types. I”. In: *Nagoya Math. J.* 6 (1953), pp. 17–28. ISSN: 0027-7630.

[Jam80] Rodney James. “The groups of order p^6 (p an odd prime)”. In: *Math. Comp.* 34.150 (1980), pp. 613–637. ISSN: 0025-5718.

[Kaz81] L. S. Kazarin. “On groups with isolated conjugacy classes”. In: *Izv. Vyssh. Uchebn. Zaved. Mat.* 7 (1981), pp. 40–45. ISSN: 0021-3446.

[KLT95] R. Knörr, W. Lempken, and B. Thielcke. “The S_3-conjecture for solvable groups”. In: *Israel J. Math.* 91.1-3 (1995), pp. 61–76. ISSN: 0021-2172.

[KP98] E.W. Kiss and P. P. Pálfy. “A lattice of subgroups that is not emheddable into the subgroup lattice of an abelian group”. In: *Mathematica scandinavica* 83 (1998), pp. 169–176.

[Lew01] Mark L. Lewis. “Solvable groups whose degree graphs have two connected components”. In: *J. Group Theory* 4.3 (2001), pp. 255–275. ISSN: 1433-5883.

[Lew07] Mark L. Lewis. "Generalizing a theorem of Huppert and Manz". In: *J. Algebra Appl.* 6.4 (2007), pp. 687–695. ISSN: 0219-4988.

[Lew08] Mark L. Lewis. "An overview of graphs associated with character degrees and conjugacy class sizes in finite groups". In: *Rocky Mountain J. Math.* 38.1 (2008), pp. 175–211. ISSN: 0035-7596.

[Lew98] Mark L. Lewis. "Determining group structure from sets of irreducible character degrees". In: *J. Algebra* 206.1 (1998), pp. 235–260. ISSN: 0021-8693.

[Li99] Shirong Li. "On the class length of elements of prime power order in finite groups". In: *Guangxi Sci.* 6.1 (1999), pp. 12–13. ISSN: 1005-9164.

[Lju43] Wilhelm Ljunggren. "Some theorems on indeterminate equations of the form $x^n - 1/x - 1 = y^q$". In: *Norsk Mat. Tidsskr.* 25 (1943), pp. 17–20.

[LW03] Mark L. Lewis and Donald L. White. "Connectedness of degree graphs of nonsolvable groups". In: *J. Algebra* 266.1 (2003), pp. 51–76. ISSN: 0021-8693.

[LW05] Mark L. Lewis and Donald L. White. "Diameters of degree graphs of nonsolvable groups". In: *J. Algebra* 283.1 (2005), pp. 80–92. ISSN: 0021-8693.

[LW07] Mark L. Lewis and Donald L. White. "Diameters of degree graphs of nonsolvable groups. II". In: *J. Algebra* 312.2 (2007), pp. 634–649. ISSN: 0021-8693.

[Man85] Olaf Manz. "Degree problems. II. π-separable character degrees". In: *Comm. Algebra* 13.11 (1985), pp. 2421–2431. ISSN: 0092-7872.

[McV04a] John K. McVey. "Bounding graph diameters of nonsolvable groups". In: *J. Algebra* 282.1 (2004), pp. 260–277. ISSN: 0021-8693.

[McV04b] John K. McVey. "Bounding graph diameters of solvable groups". In: *J. Algebra* 280.2 (2004), pp. 415–425. ISSN: 0021-8693.

[Mic86] Gerhard O. Michler. "A finite simple group of Lie type has p-blocks with different defects, $p \neq 2$". In: *J. Algebra* 104.2 (1986), pp. 220–230. ISSN: 0021-8693.

[MSW88] O. Manz, R. Staszewski, and W. Willems. "On the number of components of a graph related to character degrees". In: *Proc. Amer. Math. Soc.* 103.1 (1988), pp. 31–37. ISSN: 0002-9939.

[MW04] Alexander Moretó and Thomas R. Wolf. "Orbit sizes, character degrees and Sylow subgroups". In: *Adv. Math.* 184.1 (2004), pp. 18–36. ISSN: 0001-8708.

[MWW89] Olaf Manz, Wolfgang Willems, and Thomas R. Wolf. "The diameter of the character degree graph". In: *J. Reine Angew. Math.* 402 (1989), pp. 181–198. ISSN: 0075-4102.

[Nag21] T Nagell. "Sur l'impossibilité de l'equation indéterminée $z^p + 1 = y^2$". In: *Norsk. Mat. Forenings Skrifter I* 3 (1921).

[Nav98] Gabriel Navarro. *Characters and Blocks of Finite Groups*. London Mathematical Society Lecture Notes Series 250. Cambridge University Press, 1998.

[NSW81] Morris Newman, Daniel Shanks, and H. C. Williams. "Simple groups of square order and an interesting sequence of primes". In: *Acta Arith.* 38.2 (1980/81), pp. 129–140. ISSN: 0065-1036.

[Oku13] Tetsuro Okuyama. "Self Dual Groups are Nilpotent". Personal Communication. Jan. 2013.

[Pál98] Péter Pál Pálfy. "On the character degree graph of solvable groups. I. Three primes". In: *Period. Math. Hungar.* 36.1 (1998), pp. 61–65. ISSN: 0031-5303.

[Rie99] Jeffrey M. Riedl. "Character degrees, class sizes, and normal subgroups of a certain class of p-groups". In: *J. Algebra* 218.1 (1999), pp. 190–215. ISSN: 0021-8693.

[Rob09] Geoffrey R. Robinson. "Characters and the commutator map". In: *Journal of Algebra* 321.11 (2009). Special Issue in Honor of Gus Lehrer, pp. 3521–3526. ISSN: 0021-8693.

[Rot83] A. Rotkiewicz. "Applications of Jacobi's symbol to Lehmer's numbers". In: *Acta Arith.* 42.2 (1983), pp. 163–187. ISSN: 0065-1036.

[Sag03] I. A. Sagirov. "A generalization of the Suzuki 2-groups $A(m,\theta)$". In: *Izv. Vyssh. Uchebn. Zaved. Mat.* 10 (2003), pp. 56–61. ISSN: 0021-3446.

[ST76] T. N. Shorey and R. Tijdeman. "New applications of Diophantine approximations to Diophantine equations". In: *Math. Scand.* 39.1 (1976), pp. 5–18. ISSN: 0025-5521.

[Str91] S. P. Strunkov. "Existence and the number of p-blocks of defect 0 in finite groups". In: *Algebra i Logika* 30.3 (1991), pp. 355–368, 381. ISSN: 0373-9252.

[Str92] S. P. Strunkov. "Some arithmetical properties of finite groups and their linear representations". In: *Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989)*. Vol. 131. Contemp. Math. Providence, RI: Amer. Math. Soc., 1992, pp. 375–382.

[Tho64] John G. Thompson. "Normal p-complements for finite groups". In: *J. Algebra* 1 (1964), pp. 43–46. ISSN: 0021-8693.

[Tho70] John G. Thompson. "Normal p-complements and irreducible characters". In: *J. Algebra* 14 (1970), pp. 129–134. ISSN: 0021-8693.

[Waa73] Robert W. van der Waall. "On the Diophantine equations $x^2 + x + 1 = 3v^2$, $x^3 - 1 = 2y^2$, $x^3 + 1 = 2y^2$". In: *Simon Stevin* 46 (1972/73), pp. 39–51. ISSN: 0037-5454.

[Wal63] G. E. Wall. "On the conjugacy classes in the unitary, symplectic and orthogonal groups". In: *J. Austral. Math. Soc.* 3 (1963), pp. 1–62. ISSN: 0263-6115.

[Yan09] Yong Yang. "Orbits of the actions of finite solvable groups". In: *Journal of Algebra* 321.7 (2009), pp. 2012–2021. ISSN: 0021-8693.

[Zha94] Ji Ping Zhang. "Finite groups with many conjugate elements". In: *J. Algebra* 170.2 (1994), pp. 608–624. ISSN: 0021-8693.