Block fusion systems and the center of the group ring

Martin Wedel Jacobsen

This document is Martin Wedel Jacobsen's Ph.D. thesis, written at the Department of Mathematical Sciences at the University of Copenhagen under the supervision of Jesper Michael Møller. It was submitted on April 30, 2014. The author's Ph.D. studies at the department were supported by the Danish National Research Foundation through the Center for Symmetry and Deformation.

Abstract

This thesis develops some aspects of the theory of block fusion systems. Chapter 1 contains a brief introduction to the group algebra and some simple results about algebras over a field of positive characteristic. In chapter 2 we define the concept of a fusion system and the fundamental property of saturation. We also define block fusion systems and prove that they are saturated. Chapter 3 develops some tools for relating block fusion systems to the structure of the center of the group algebra. In particular, it is proven that a block has trivial defect group if and only if the center of the block algebra is one-dimensional. Chapter 4 consists of a proof that block fusion systems of symmetric groups are always group fusion systems of symmetric groups, and an analogous result holds for the alternating groups.

Resume

Denne afhandling udvilker nogle aspekter af teorien for blokfusionssystemer. Kapitel 1 indeholder en kort introduktion til gruppealgebraen og nogle simple resultater om algebraer over et legeme med positiv karakteristik. I kapitel 2 definerer vi konceptet et fusionssystem og den grundlæggende egenskab mættethed. Vi definerer også blokfusionssystemer og beviser at de er mættede. Kapitel 3 udvikler nogle værktøjer til at relatere blokfusionssystemer til strukturen af gruppealgebraens center. Specielt bevises det at en blok har triviel defektgruppe hvis og kun hvis blokalgebraens center er en-dimensionalt. Kapitel 4 består af et bevis for at blokfusionssystemer for symmetriske grupper altid er gruppefusionssystemer for symmetriske grupper, og et analogt resultat gælder for de alternerende grupper.

Contents

CHAPTER 1

Introduction and preliminaries

The main object of study of this thesis is the group ring of a finite group G.

DEFINITION 1.1. For any field $\mathbb{F}$ and any finite group G, the group ring $\mathbb{F}G$ is an algebra over $\mathbb{F}$. As a $\mathbb{F}$-vector space, it has basis G, and its multiplication is the unique $\mathbb{F}$-bilinear map satisfying $g \cdot h = gh$ for all $g, h \in G$.

An element of $\mathbb{F}G$ is typically written in the form $\sum_{g\in G} c_g g$ with each c_g being an element of $\mathbb{F}$. An alternative description of $\mathbb{F}G$ is to regard it as the set of functions from G to $\mathbb{F}$, with the multiplication being given by the convolution formula $(\alpha * \beta)(a) = \sum_{g\in G} \alpha(g)\beta(g^{-1}a)$. The function α in this formulation corresponds to the element $\sum_{g\in G} \alpha(g)g$ in the other formulation.

The main reason for studying the group ring is that it determines the possible actions of G on an $\mathbb{F}$-vector space. Given an $\mathbb{F}$-vector space V on which G acts, V becomes an $\mathbb{F}G$-module by setting $v.(\sum_{g\in G} c_g g) = \sum_{g\in G} c_g v^g$ for any $v \in V$. Understanding the module theory of $\mathbb{F}G$ then makes it possible to determine the ways in which G can act on a vector space.

We record a few basic properties of group rings.

PROPOSITION 1.2. *For any group homomorphism $\varphi : G \to H$, the map $\varphi^* : \mathbb{F}G \to \mathbb{F}H$ given by $\varphi^*(\sum_{g\in G} c_g g) = \sum_{g\in G} c_g \varphi(g)$ is an $\mathbb{F}$-algebra homomorphism.*

PROPOSITION 1.3. *For any finite groups G and H, $\mathbb{F}G \otimes \mathbb{F}H$ is isomorphic to $\mathbb{F}(G \times H)$. The isomorphism is given by mapping $g \otimes h$ to (g, h).*

A compact way of stating the above two properties is to say that the group ring over $\mathbb{F}$ is a monoidal functor from the category of finite groups with the direct product to the category of $\mathbb{F}$-algebras with the tensor product.

DEFINITION 1.4. The map $\eta : \mathbb{F}G \to \mathbb{F}$ induced by the group homomorphism $G \to 1$ is called the augmentation map of $\mathbb{F}G$.

The group ring can actually be given significantly more structure. It is possible to define a comultiplication on $\mathbb{F}G$ which together with the augmentation map makes $\mathbb{F}G$ into a coalgebra. Furthermore, the algebra and coalgebra structure on $\mathbb{F}G$ interact in such a way as to make $\mathbb{F}G$ a Hopf algebra. We will not need this additional structure, however.

We now fix the following notation. Choose a prime p, and let k be the algebraic closure of the field with p elements; unless otherwise specified, we

will generally be working in a group ring kG where G is a finite group. When X is a finite set of elements in an algebra A, we write ΣX for the sum of the elements of X. When H is a group acting on an algebra A and x is an element of A, we write x^H for the orbit containing x. When H is a group acting on a set (or algebra) X, we write X^H for the subset (or -algebra) consisting of the fixed points of the action. When x is an element of an algebra A, we write $\mathrm{Ann}_A(x)$ for the (left) annihilator of x in A. (The left/right distinction will not matter as we will only use the notation in cases where x is central in A.)

When H is a group acting on another group G, we write $\mathrm{Cl}_H(G)$ for the set of orbits in G of the action of H. The main use of this notion is that there is an action of H on kG induced by the action on G, and the subalgebra $(kG)^H$ has a basis of the form $\{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}_H(G)\}$. We also write $\mathrm{Cl}(G)$ for $\mathrm{Cl}_G(G)$, the set of conjugacy classes in G. Since $Z(kG) = (kG)^G$, $Z(kG)$ then has a basis of the form $\{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}(G)\}$. When H and K are subgroups of a group G, we write $\mathrm{Aut}_H(K)$ for the group of automorphisms of K having the form $x \mapsto x^h$ for some $h \in H$. This group is isomorphic to $N_H(K)/C_H(K)$ and to $N_H(K)C_G(K)/C_G(K)$. We also write $\mathrm{Aut}(K)$ for the group of all automorphisms of K. We write S_n and A_n for the symmetric and alternating groups on $\{1, \ldots, n\}$. When N is any finite set, we also write S_N and A_N for the symmetric and alternating groups on N. We write C_n for the cyclic group of order n.

When g is an element of G, we say that g is a p-element if its order is a power of p, and we say that g is p-regular if its order is not divisible by p. When P is a p-group and Q is a subgroup of P, we say that Q is centric in P if $C_P(Q)$ is contained in Q.

We record two useful facts from group theory:

PROPOSITION 1.5. *Let g be an element of the finite group G and let p be a prime. Then there are unique elements g_p and $g_{p'}$ of G such that $g = g_p g_{p'} = g_{p'} g_p$, g_p is a p-element, and $g_{p'}$ is p-regular.*

PROPOSITION 1.6. *Let P be a p-group and let Q be a proper subgroup of P. Then $N_P(Q) \neq Q$, and there is a chain of normal inclusions $Q = Q_0 \trianglelefteq Q_1 \trianglelefteq \ldots \trianglelefteq Q_n = P$.*

We will routinely make use of the following fact: when P is a p-group acting on a finite set X, $|X|$ and $|X^P|$ are congruent modulo p. Often X will be a set whose size expresses the coefficient on an element of G in some $x \in kG$, and we will then replace X by X^P for a suitable P.

1. Algebra decomposition

In this section we will establish a few basic facts about k-algebras. We will show that a finite-dimensional k-algebra has a unique maximal decomposition as a direct product of subalgebras, and that the center of the algebra can de decomposed as the sum of two subspaces, of which one is a nilpotent ideal and the other is isomorphic to k^n for some n. The proofs in this section are mostly standard. For the results on lifting idempotents, we follow the approach of [**10**].

Unless otherwise specified, we always assume that our k-algebras have a multiplicative identity.

DEFINITION 1.7. Let A be a k-algebra. A decomposition of unity in A is a finite set X of elements of A such that $0 \notin X$, $x^2 = x$ and $xy = 0$ for all $x, y \in X$ with $x \neq y$, and $\Sigma X = 1$.

PROPOSITION 1.8. *For any decomposition of unity X in $Z(A)$, A is isomorphic to the direct product of the subalgebras Ax as x runs over X. The isomorphism is given by mapping an element in $\prod_{x\in X} Ax$ to the sum of its components, while the inverse is given by mapping $a \in A$ to ax in each component Ax. In each factor Ax, the unit element is x.*

There is a similar result for decompositions of unity in A: they provide a decomposition of A into a direct sum of A-submodules. We will not need this, however. Since we are only interested in central decompositions of unity, we will only consider decompositions of unity in commutative rings, which are somewhat easier to handle. Nevertheless, most of the results below have analogues for noncommutative k-algebras.

LEMMA 1.9. *Any decomposition of unity is linearly independent.*

PROOF. Suppose that $\sum_{x\in X} d_x x = 0$. For any $y \in X$, multiplying by y gives $d_y y = 0$, and then $d_y = 0$ as $y \neq 0$. □

DEFINITION 1.10. A decomposition of unity X is said to be a refinement of another decomposition Y if there exists a partition $\coprod_i X_i$ of X such that for each i, ΣX_i is an element of Y.

LEMMA 1.11. *The relation "X is a refinement of Y" is a partial order on the set of decompositions of unity, with $\{1\}$ as its minimal element.*

PROOF. Write $X \geq Y$ if X is a refinement of Y; it is obvious that $X \geq X$. Suppose that $X \geq Y$, and let X_i and X_j be two different blocks in the partition of X. Then $\Sigma X_i \cdot \Sigma X_j = 0$ since $xy = 0$ for all $x \in X_i$ and $y \in X_j$, so ΣX_i and ΣX_j are different elements of Y. Then $\sum_i \Sigma X_i = \Sigma X = 1$ is a sum over some subset of Y; if it is a proper subset, the sum of the remaining elements of Y is zero. But this is impossible since Y is linearly independent, so every element of Y corresponds to a block of X. In particular, we must have $|X| \geq |Y|$.

Now if $X \geq Y$ and $Y \geq X$, then $|X| = |Y|$. Then the partition of X used in $X \geq Y$ has as many blocks as there are elements of X, so each block consists of a single element. This implies $X = Y$.

Now suppose that $X \geq Y$ and $Y \geq Z$. Given an element z of Z, there is a block Y_i of Y that sums to z. Each element of Y_i now corresponds to a block of X; gathering these blocks together, we create a coarser partition of X that has a block that sums to z. By doing this for each element of Z, we create a partition of X in which every block sums to an element of Z, which shows that $X \geq Z$. We have now shown that refinement is indeed a partial order.

It is clear that $\{1\}$ is a decomposition of unity. For any other decomposition X, we have $X \geq \{1\}$, since we can take the partition of X with a single block. □

LEMMA 1.12. *Suppose that A is commutative. Any two decompositions of unity have a common refinement.*

PROOF. Let X and Y be decompositions of unity and let $Z = \{xy \mid x \in X, y \in Y, xy \neq 0\}$. For any $xy \in Z$, we have $(xy)^2 = x^2y^2 = xy$, and given $x, x' \in X$ and $y, y' \in Y$ with either $x \neq x'$ or $y \neq y'$, we have $(xy)(x'y') = (xx')(yy') = 0$. Then we also have $xy \neq x'y'$ when $x \neq x'$ or $y \neq y'$, unless xy and $x'y'$ are both 0, so $\Sigma Z = \Sigma X \cdot \Sigma Y = 1$. Thus Z is a decomposition of unity. We also have $Z \geq X$, since we can partition Z as $\coprod_{x \in X} \{xy \mid y \in Y, xy \neq 0\}$, and similarly we have $Z \geq Y$. □

THEOREM 1.13. *Suppose that A is finite-dimensional and commutative. Then there is a unique maximal decomposition of unity.*

PROOF. Since a decomposition of unity is linearly independent, its size is no larger than the dimension of A. Let X be a decomposition of unity with $|X|$ maximal, let Y be any other decomposition, and let Z be a common refinement of X and Y. Since $Z \geq X$, we have $|Z| \geq |X|$, and since $|X|$ is maximal, this implies $|Z| = |X|$. As seen above, $|Z| = |X|$ and $Z \geq X$ together imply $Z = X$, and then we have $X \geq Y$. Since Y was arbitrary, X is maximal. □

The generalisation of Theorem 1.13 to noncommutative k-algebras says that any two maximal decompositions of unity are conjugate under $A^\times$.

EXAMPLE 1.14. The requirement that A is finite-dimensional is essential for Theorem 1.13. Consider an infinite-dimensional k-algebra A with basis $\{e, e_1, e_2, e_3, \ldots\}$ and multiplication given by $e^2 = e$, $ee_i = e_ie = e_i^2 = e_i$ for all i, and $e_ie_j = 0$ for all i and j with $i \neq j$. Here e is the multiplicative identity of A, and for any n, the set $\{e_i \mid 1 \leq i \leq n\} \cup \{e - \sum_{i=1}^n e_i\}$ is a decomposition of unity. These decompositions do not all have a common refinement, so there is no maximal decomposition of unity.

DEFINITION 1.15. The elements of the maximal decomposition of unity in $Z(A)$ are called the primitive central idempotents of A. They may also be called block idempotents or just blocks.

COROLLARY 1.16. *Any central idempotent of A can be written as a sum of block idempotents.*

PROOF. Let e be a central idempotent; $\{e, 1 - e\}$ is a decomposition of unity in $Z(A)$, so we have $X \geq \{e, 1 - e\}$ where X is the maximal decomposition. □

COROLLARY 1.17. *Given any decomposition of unity X in $Z(A)$ and any block idempotent e, there is a unique $x \in X$ such that $xe = e$. For any other element y of X, $ye = 0$.*

PROOF. Let Z be the maximal decomposition of unity. Then $Z \geq X$, and as seen above, each element of X is a sum of elements of Z, each element of Z appearing in exactly one sum. This applies in particular to e; taking $x \in X$ to be the element whose sum decomposition contains e we get $xe = e$. For any other $y \in X$, we get $ye = 0$, since y can be written as a sum of elements of Z that differ from e. □

Next we define a particular ideal of k-algebras, the Jacobson radical. We will see that the Jacobson radical of $Z(A)$ is nilpotent, and the k-span of the blocks of A is a complementary subspace to the Jacobson radical in $Z(A)$.

DEFINITION 1.18. Let A be a k-algebra. The Jacobson radical $J(A)$ of A is the set of elements of A that annihilate all simple A-modules.

LEMMA 1.19. *Let A be a finite-dimensional k-algebra. $J(A)$ is nilpotent, and all nilpotent ideals of A are contained in $J(A)$. When A is commutative, $J(A)$ is exactly the set of all nilpotent elements of A.*

PROOF. In the sequence of inclusions $J(A) \supseteq J(A)^2 \supseteq J(A)^3 \supseteq \dots$ the dimension is weakly decreasing and hence must stabilise. Let n be such that $J(A)^n$ and $J(A)^{n+1}$ have the same dimension; since $J(A)^{n+1} \subseteq J(A)^n$, we then have $J(A)^{n+1} = J(A)^n$. Letting $J = J(A)^n$, J is then an A-module such that $J \cdot J(A) = J$. If $J \neq 0$, J contains a maximal submodule K, and J/K is then simple. This implies $J/K \cdot J(A) = 0$, and so $J \cdot J(A) \subseteq K$, which contradicts $J \cdot J(A) = J$. Hence $J = 0$, and $J(A)$ is nilpotent.

Now let I be a nilpotent ideal in A and let M be a simple A-module. Then MI is a submodule of M, so it is either M or 0. If $MI = M$, we get $MI^n = M$ for all n; but there is an n such that $I^n = 0$ since I is nilpotent. Hence we have $MI = 0$, so I annihilates all simple A-modules. It is then contained in $J(A)$.

For the last part, note that when A is commutative, Ax is an ideal of A for any $x \in A$. If x is nilpotent, then so is Ax, so we get $x \in Ax \subseteq J(A)$. Thus every nilpotent element of A lies in $J(A)$; conversely, all elements of $J(A)$ are nilpotent since $J(A)$ itself is nilpotent. □

LEMMA 1.20. *For any k-algebra A, $J(A/J(A)) = 0$.*

PROOF. Let K be the preimage of $J(A/J(A))$ in A; this is an ideal in A. Since $J(A/J(A))$ is nilpotent, there is some n such that $J(A/J(A))^n = 0$; then $K^n \subseteq J(A)$. But $J(A)$ is also nilpotent, so there is some m such that $J(A)^m = 0$. Then $K^{nm} \subseteq J(A)^m = 0$, so K is nilpotent and hence contained in $J(A)$. Then $J(A/J(A)) = K/J(A) = 0$. □

THEOREM 1.21. *Let A be a finite-dimensional k-algebra. Then $J(Z(A))$ equals $J(A) \cap Z(A)$.*

PROOF. Since $J(A)$ is nilpotent, $J(A) \cap Z(A)$ is a nilpotent ideal of $Z(A)$; it is then contained in $J(Z(A))$. Conversely, any element x of $J(Z(A))$ is nilpotent, so Ax is a nilpotent ideal of A. It is then contained in $J(A)$ by Lemma 1.19, so $x \in J(A)$. Then we also have $J(Z(A)) \subseteq J(A) \cap Z(A)$, and so $J(Z(A)) = J(A) \cap Z(A)$. □

THEOREM 1.22. *Let A be a finite-dimensional commutative k-algebra with $J(A) = 0$. Then A is isomorphic to k^n where n is the dimension of A.*

PROOF. By induction on n. We assume that A is a k-algebra with no nilpotent elements other than 0, but we do not assume that A has a multiplicative identity. This will be useful for the induction step.

If $n = 1$, A has a generator x such that $x^2 = cx$ for some $c \in k$. Since x is not nilpotent, c is not zero, so $c^{-1}x$ is an idempotent element of A. Then A is isomorphic to k by the map $dx \mapsto dc$ for $d \in k$.

Now let $n \geq 2$; we first prove that there is a nonzero $x \in A$ such that $xA \neq A$. Suppose that x satisfies $xA = A$. Picking some k-basis B of A, we can express the map $a \mapsto xa$ as a matrix M. Since M has finitely many entries, its entries are all contained in some finite subfield $\mathbb{F}_q$ of k. Then multiplication by x preserves the $\mathbb{F}_q$-subspace generated by B; since this space has finitely many points, any automorphism of it has finite order. There is then some l such that M^l is the identity matrix, so $x^l b = b$ for any $b \in B$. Thus A has the multiplicative identity x^l, and x is invertible. This implies that if $xA = A$ for all nonzero $x \in A$, then A is a field. This is impossible, since there are no nontrivial finite-dimensional field extensions of k.

Thus we have a nonzero $x \in A$ with $xA \neq A$. Now the map $a \mapsto xa$ has image xA and kernel $\mathrm{Ann}_A(x)$, so $\dim(xA) + \dim(\mathrm{Ann}_A(x)) = n$. For any $xa \in xA$ and any $y \in \mathrm{Ann}_A(x)$, we now have $xa \cdot y = y \cdot xa = 0$. Given a $z \in xA \cap \mathrm{Ann}_A(x)$, we then have $z^2 = 0$, so that z is nilpotent. Since $J(A) = 0$, this implies $z = 0$. Then xA and $\mathrm{Ann}_A(x)$ have trivial intersection; combined with the dimension formula above, this gives $A = xA \oplus \mathrm{Ann}_A(x)$ as a k-vector space. Because of the multiplication formula, we actually have $A = xA \times \mathrm{Ann}_A(x)$ as a k-algebra. We have already seen $\mathrm{Ann}_A(x) \neq 0$, and we also have $xA \neq 0$ since it contains A. Thus both factors have dimension less than n, so we may apply the induction hypothesis to them. □

The noncommutative analogue of Theorem 1.22 states that a finite-dimensional k-algebra A with $J(A) = 0$ is isomorphic to a product of matrix rings over k.

COROLLARY 1.23. *Let A be a finite-dimensional commutative k-algebra. Then $A/J(A)$ is isomorphic to k^n for some n.*

PROOF. By Lemma 1.20, $J(A/J(A)) = 0$, so the result follows from Theorem 1.22. □

THEOREM 1.24. *Let A be a finite-dimensional commutative k-algebra. Any idempotent of $A/J(A)$ lifts to an idempotent of A, and this lift is unique. Conversely, any primitive idempotent of A maps to a primitive idempotent of $A/J(A)$ under the quotient map.*

PROOF. Let e be an idempotent element of $A/J(A)$, and let a_1 be any lift of e. Define a sequence (a_n) by setting $a_n = 3a_{n-1}^2 - 2a_{n-1}^3$ for $n \geq 2$. Then by induction each a_n is a lift of e: a_n maps to $3e^2 - 2e^3 = 3e - 2e = e$. Now since $a_1^2 - a_1$ maps to $e^2 - e = 0$, we have $a_1^2 - a_1 \in J(A)$. We prove by induction that $a_n^2 - a_n \in J(A)^n$:

$$\begin{aligned} a_n^2 - a_n &= (3a_{n-1}^2 - 2a_{n-1}^3)^2 - (3a_{n-1}^2 - 2a_{n-1}^3) \\ &= 4a_{n-1}^6 - 12a_{n-1}^5 + 9a_{n-1}^4 + 2a_{n-1}^3 - 3a_{n-1}^2 \\ &= (a_{n-1}^2 - a_{n-1})(4a_{n-1}^4 - 8a_{n-1}^3 + a_{n-1}^2 + 3a_{n-1}) \\ &= (a_{n-1}^2 - a_{n-1})^2(4a_{n-1}^2 - 4a_{n-1} - 3) \end{aligned}$$

Since $a_{n-1}^2 - a_{n-1} \in J(A)^{n-1}$, we have $(a_{n-1}^2 - a_{n-1})^2 \in J(A)^{2n-2} \subseteq J(A)^n$, and so $a_n^2 - a_n \in J(A)^n$. Now since every element of $J(A)$ is nilpotent and

A is finite-dimensional, there is some n such that $J(A)^n = 0$. For this n, a_n is then idempotent.

For the uniqueness, suppose that e has two different idempotent lifts a and b. Then $a - b$ is nilpotent, so there is some n such that $(a-b)^m = 0$ for $m \geq n$. But we also have $(a-b)^{p^l} = a^{p^l} - b^{p^l} = a - b$ for all positive l, which is a contradiction.

For the converse, let X be the set of primitive idempotents of A that occur as lifts of primitive idempotents of $A/J(A)$. Then ΣX maps to the sum of all primitive idempotents of $A/J(A)$, which is 1, so $\Sigma X - 1 \in J(A)$. Since ΣX and 1 are both idempotents, we can use the same uniqueness argument to conclude that $\Sigma X = 1$. Then the set of primitive idempotents of A that do not lie in X sums to 0, so it is empty since the primitive idempotents are linearly independent. □

THEOREM 1.25. *Let A and B be finite-dimensional commutative k-algebras, and let $\varphi : A \to B$ be a surjective map. Every primitive idempotent of B lifts to a primitive idempotent of A.*

PROOF. Write $\pi_A : A \to A/J(A)$ and $\pi_B : B \to B/J(B)$ for the quotient maps. The kernel of the map $\pi_B \circ \varphi : A \to B/J(B)$ contains $J(A)$, since $J(A)$ is nilpotent and the only nilpotent element of $B/J(B)$ is 0. Then the map factors through $A/J(A)$, so there is a map $\bar{\varphi} : A/J(A) \to B/J(B)$ such that $\bar{\varphi} \circ \pi_A = \pi_B \circ \varphi$. Now if e is a primitive idempotent of B, $\pi_B(e)$ is a primitive idempotent of $B/J(B)$. Suppose that we can lift $\pi_B(e)$ to a primitive idempotent of $A/J(A)$; we can then lift it further to A, obtaining a primitive idempotent f of A such that $\varphi(f) - e \in J(B)$. Picking a large enough n, we then have $(\varphi(f) - e)^{p^n} = 0$; this implies $\varphi(f) - e = \varphi(f)^{p^n} - e^{p^n} = (\varphi(f) - e)^{p^n} = 0$, so that $\varphi(f) = e$. It is therefore enough to prove that any primitive idempotent of $B/J(B)$ can be lifted to $A/J(A)$.

$A/J(A)$ and $B/J(B)$ both have trivial Jacobson radical, so they are isomorphic to some power of k. Let X be the maximal decomposition of unity in $A/J(A)$; this is a basis for $A/J(A)$ since $A/J(A) \cong k^n$. Let $X' = \{x \in X \mid \bar{\varphi}(x) \neq 0\}$; then $\bar{\varphi}(X')$ spans $B/J(B)$ since $\bar{\varphi}$ is surjective. Additionally, $\bar{\varphi}(X')$ is a decomposition of unity, so it is linearly independent and so a basis of $B/J(B)$. No decomposition of unity in $B/J(B)$ can have more elements than $\bar{\varphi}(X')$, since it would then not be linearly independent, so $\bar{\varphi}(X')$ is the maximal decomposition of unity in $B/J(B)$. It then contains all primitive idempotents of $B/J(B)$. □

THEOREM 1.26. *Let A be a finite-dimensional commutative k-algebra, and let $X = \{e_1, \ldots, e_n\}$ be the maximal decomposition of unity in A. The k-span of X is a subalgebra E isomorphic to k^n such that $A = E \oplus J(A)$ as a k-vector space. Additionally, $J(A)$ is isomorphic to $\prod_{i=1}^n J(Ae_i)$.*

PROOF. The multiplication rules for elements of X ensure that E is a subalgebra. Given an element $x = \sum_{i=1}^n d_i e_i \in E$, we have $x^m = \sum_{i=1}^n d_i^m e_i$, which can be zero only when $x = 0$. Then $E \cap J(A) = 0$. Conversely, $A/J(A)$ is isomorphic to k^l for some l, and the primitive idempotents of $A/J(A)$ lift to primitive idempotents in A. It follows that E maps surjectively onto $A/J(A)$, so we must have $A = E \oplus J(A)$ as a k-vector space.

Now for any $x \in J(A)$ and any e_i, xe_i is nilpotent. Then $J(A)e_i \subseteq J(A)$, so we get $\prod_{i=1}^{n} J(A)e_i \subseteq J(A)$. The other inclusion is obvious, so we have $\prod_{i=1}^{n} J(A)e_i = J(A)$. Finally, we have $J(Ae_i) \subseteq Ae_i \cap J(A) \subseteq J(A)e_i$ since every element of $J(Ae_i)$ is nilpotent, and we also have $J(A)e_i \subset J(Ae_i)$ since every element of $J(A)e_i$ is nilpotent. Hence $J(Ae_i) = J(A)e_i$. □

We also note a small lemma that will be useful later.

LEMMA 1.27. *Let A be a finite-dimensional commutative k-algebra, and suppose that 1 is a primitive idempotent of A. Then $J(A)$ is the unique maximal ideal of A.*

PROOF. It is enough to show that every element of A that is not in $J(A)$ is invertible. We have $A = E \oplus J(A)$ as a k-vector space where E is the subspace generated by 1. An element of A that is not in $J(A)$ can then be written as $c+x$ with $c \in E$, $x \in J(A)$, and $c \neq 0$. Since c is a nonzero element of E, it is invertible, and x is nilpotent since it is an element of $J(A)$. Then $\sum_{n=0}^{\infty}(-1)^n c^{-n-1}x^n$ is a well-defined element of A, and a straightforward calculation shows that it is the multiplicative inverse of $c + x$. □

LEMMA 1.28 (Rosenberg's lemma). *Let A be a finite-dimensional commutative k-algebra, let $I_1, \ldots, I_n$ be ideals in A, and let e be a primitive idempotent of A. If e is an element of the ideal $\sum_{i=1}^{n} I_i$, then there is some i such that $e \in I_i$.*

PROOF. For each i, eI_i is an ideal of eA. Since $e^2 = e$, e is an element of $\sum_{i=1}^{n} eI_i$, so this ideal is all of eA. Since every proper ideal of eA is contained in $J(eA)$, there must be an i such that $eI_i = eA$. Since $eI_i \subseteq I_i$, it follows that $e \in I_i$. □

To round out this section, we use the augmentation map of kG to distinguish one particular block.

THEOREM 1.29. *Let $\eta : kG \to k$ be the augmentation map. There exists a unique block b of kG with $\eta(b) = 1$; for any other block e, $\eta(e) = 0$.*

PROOF. Let $e_1, \ldots, e_n$ be the blocks of kG. Since each e_i is idempotent, $\eta(e_i)$ is an idempotent element of k, so it is either 0 or 1. Now given two different idempotents e_i and e_j, we have $\eta(e_i)\eta(e_j) = \eta(e_ie_j) = \eta(0) = 0$, so $\eta(e_i)$ can be 1 for at most one i. On the other hand, we have $\sum_{i=1}^{n} \eta(e_i) = \eta\left(\sum_{i=1}^{n} e_i\right) = \eta(1) = 1$, so there must be some i for which $\eta(e_i) = 1$. □

DEFINITION 1.30. The unique block b of kG with $\eta(b) = 1$ is called the principal block of kG.

CHAPTER 2

Fusion systems

For any finite group G and any prime p, one can define a fusion system at p on G. The main idea behind this concept is to isolate the part of the structure of G that can be described in terms of the p-subgroups of G.

DEFINITION 2.1. Given a group G with Sylow p-subgroup P, the fusion system $\mathcal{F}_P(G)$ is a category defined as follows. The objects of $\mathcal{F}_P(G)$ are the subgroups of P, and given any two objects Q and R, the maps from Q to R are all group homomorphisms of the form $x \mapsto x^g$ for some $g \in G$ such that $Q^g \leq R$. The composition of maps is the usual composition of homomorphisms.

The particular choice of P is irrelevant since a conjugation map from one Sylow p-subgroup to another provides an isomorphism between the corresponding fusion systems.

EXAMPLE 2.2. Let G be the symmetric group on 4 elements, let $d = (1234)$ and let $s = (13)$. Then $P = \langle s, d \rangle$ is a Sylow 2-subgroup of G, isomorphic to the dihedral group of order 8. The fusion system $\mathcal{F}_P(G)$ contains the four inner automorphisms of P (given respectively by mapping (s, d) to (s, d), (sd^2, d), (s, d^3), and (sd^2, d^3)) and all their restrictions. It additionally contains all six automorphisms of the subgroup $\langle sd, d^2 \rangle$ (given by permutations of the three nontrivial elements sd, d^2, and sd^3) and all their restrictions. It does not contain any other morphisms.

1. Abstract fusion systems

In order to better study fusion systems of groups, it is useful to have an abstract description of what these fusion systems look like. The definitions and much of the theory were originally developed by Lluis Puig (see [**9**]). Puig did not initially publish his work, but his approach was taken up by others in the interim. As a result, there are now two competing sets of terminology. This thesis uses the second set, which was also used in [**3**] and [**2**], both of which are broad surveys of the then-current literature.

This chapter broadly follows [**2**] in its approach, although many of the proofs are simplified because we do not consider the more general case of arbitrary k-algebras with G-action.

DEFINITION 2.3. Let P be a p-group. A *fusion system* $\mathcal{F}$ on P is a category whose objects are the subgroups of P. The set of morphisms from Q to R must be a subset of the set of injective homomorphisms from Q to R, with composition given by the usual composition of homomorphisms. The morphisms from Q to R must include all morphisms given by $x \mapsto x^g$ for some $g \in P$ such that $Q^g \leq R$. For any morphism $\varphi : Q \to R$, the restriction

$\varphi : Q \to \varphi(Q)$ and its inverse $\varphi^{-1} : \varphi(Q) \to Q$ must also be morphisms in $\mathcal{F}$.

It should be noted that whenever φ is a homomorphism in a fusion system $\mathcal{F}$ with domain Q, the restriction of φ to any subgroup of Q is also a morphism in $\mathcal{F}$. This is because given any $R \leq Q$, the inclusion map from R to Q lies in $\mathcal{F}$ since it is given as conjugation by the identity element. Then we can compose this inclusion map with φ to obtain the restriction of φ to R.

The definition obviously encompasses fusion systems of finite groups, but it is much too general to be of any real use by itself. Because of this, one defines a property called *saturation* that provides strong restrictions on the structure of a fusion system.

DEFINITION 2.4. Two subgroups Q and R of P are called *$\mathcal{F}$-conjugate* if there exists an isomorphism from Q to R in $\mathcal{F}$. A subgroup Q is called *fully automised* if $\mathrm{Aut}_P(Q)$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(Q)$. A subgroup Q is called *receptive* if the following holds: for any $\mathcal{F}$-isomorphism $\varphi : R \to Q$ there exists an $\mathcal{F}$-morphism $\bar{\varphi} : N_\varphi \to P$ whose restriction to Q equals φ, where $N_\varphi = \{g \in N_P(R) \mid (x \mapsto \varphi(\varphi^{-1}(x)^g)) \in \mathrm{Aut}_P(Q)\}$.

A fusion system $\mathcal{F}$ is called *saturated* if every subgroup of P is $\mathcal{F}$-conjugate to a subgroup that is fully automised and receptive.

PROPOSITION 2.5. *Let G be a finite group and P a Sylow p-subgroup of G. The fusion system $\mathcal{F}_P(G)$ is saturated.*

PROOF. Let Q be a subgroup of P and let S be a Sylow p-subgroup of $N_G(Q)$ containing Q. Pick a $g \in G$ such that $S^g \leq P$; then $Q^g \leq P$ and Q is $\mathcal{F}_P(G)$-isomorphic to Q^g. We will show that Q^g is fully automised and receptive. Since S^g is contained in P and is a Sylow p-subgroup of $N_G(Q^g)$, we must have $N_P(Q^g) = S^g$. Then $\mathrm{Aut}_P(Q^g) = N_P(Q^g)C_G(Q^g)/C_G(Q^g)$ is a Sylow p-subgroup of $\mathrm{Aut}_G(Q^g) = N_G(Q^g)/C_G(Q^g)$. Since $\mathrm{Aut}_{\mathcal{F}_P(G)}(Q^g) = \mathrm{Aut}_G(Q^g)$, this shows that Q^g is fully automised.

Next we will prove that Q^g is also receptive. To ease the notation a bit, we drop the g and just write Q and S instead of Q^g and S^g. We then have $Q \leq S \leq P$ with $S = N_P(Q)$ and S being a Sylow p-subgroup of $N_G(S)$.

Now let $R \leq P$ and $h \in G$ such that $R^h = Q$. Let $\varphi : R \to Q$ be the map $x \mapsto x^h$ and set $N_\varphi = \{k \in N_P(R) \mid (x \mapsto \varphi(\varphi^{-1}(x)^k)) \in \mathrm{Aut}_P(Q)\}$. Note that $\varphi(\varphi^{-1}(x)^k)$ equals $x^{h^{-1}kh}$. Then for any $k \in N_\varphi$, we have $Q^{k^h} = Q$, so that $N_\varphi^h \leq N_G(Q)$. In fact we have $N_\varphi^h \leq SC_G(Q)$ since for any $k \in N_\varphi$, the automorphism $x \mapsto x^{k^h}$ of Q is represented by an element of $N_P(Q) = S$.

Note that $SC_G(Q)$ is in fact a group, since S normalizes Q and hence also $C_G(Q)$. Furthermore, S is a Sylow p-subgroup of $SC_G(Q)$, since it is a Sylow p-subgroup of the larger group $N_G(Q)$. Since N_φ^h is a p-subgroup of $SC_G(Q)$, there exists then an $a \in SC_G(Q)$ such that $N_\varphi^{ha} \leq S$. Then $\bar{\varphi} = (x \mapsto x^{ha})$ is an $\mathcal{F}_P(G)$-morphism from N_φ to P. If we can prove that we can choose a to be an element of $C_G(Q)$, we also find that the restriction of $\bar{\varphi}$ to R equals φ. Then Q is receptive.

To prove this last part, let T be an arbitrary Sylow p-subgroup of $SC_G(Q)$. Then there is an $a \in SC_G(Q)$ such that $S^a = T$. Write $a = st$

with $s \in S$ and $t \in C_G(Q)$; then $T = S^{st} = S^t$. Thus T is conjugate to S under $C_G(Q)$, so all the Sylow p-subgroups of $SC_G(Q)$ are conjugate under $C_G(Q)$. □

It is not true, however, that every saturated fusion system occurs as the fusion system of a group. The first example of this phenomenon is essentially due to Ron Solomon, who discovered a family of fusion systems on certain 2-groups that could not occur as fusion systems of a finite group. Solomon's work predates the development of the concept of fusion systems, but was reformulated in these terms by Ran Levi and Bob Oliver (see [**7**] and [**8**]).

When a fusion system is saturated, its structure can be fully recovered from a comparatively small amount of information. It is sufficient to know the $\mathcal{F}$-automorphism groups of the centric subgroups of P. This was first proved by Jonathan Alperin for group fusion systems (see [**1**]), and his result extends nicely to all saturated fusion systems.

LEMMA 2.6. *Let $\mathcal{F}$ be a fusion system on P, let Q be a fully automised and receptive subgroup of P, and let R be a subgroup of P that is $\mathcal{F}$-isomorphic to Q. Then there is a map $\varphi : N_P(R) \to N_P(Q)$ such that $\varphi(R) = Q$.*

PROOF. Let $\psi : R \to Q$ be an $\mathcal{F}$-isomorphism. The set $H = \{\psi\kappa\psi^{-1} \mid \kappa \in \mathrm{Aut}_P(R)\}$ is a p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(Q)$. Since Q is fully automised, $\mathrm{Aut}_P(Q)$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(Q)$, so there is a $\rho \in \mathrm{Aut}_{\mathcal{F}}(Q)$ such that $H^\rho \leq \mathrm{Aut}_P(Q)$. Now $\rho^{-1}\psi$ is an $\mathcal{F}$-isomorphism from R to Q, and H^ρ equals $\{\rho^{-1}\psi\kappa\psi^{-1}\rho \mid \kappa \in \mathrm{Aut}_P(R)\}$. Then $N_{\rho^{-1}\psi} = N_P(R)$, so $\rho^{-1}\psi$ extends to a map $\varphi : N_P(R) \to P$ with $\varphi(R) = Q$. Obviously $\varphi(N_P(R))$ normalizes $\varphi(R) = Q$, so φ restricts to a map from $N_P(R)$ to $N_P(Q)$. □

THEOREM 2.7 (Alperin's Fusion Theorem). *Let $\mathcal{F}$ be a saturated fusion system on P, and let $\mathcal{E}$ be the smallest fusion system on P satisfying $\mathrm{Aut}_{\mathcal{E}}(Q) = \mathrm{Aut}_{\mathcal{F}}(Q)$ whenever Q is a centric subgroup of P. Then $\mathcal{E} = \mathcal{F}$.*

PROOF. Obviously, $\mathcal{E}$ is a subsystem of $\mathcal{F}$. Suppose that $\mathcal{E} \neq \mathcal{F}$, and let $\varphi : Q \to R$ be an $\mathcal{F}$-morphism that is not in $\mathcal{E}$. We can choose φ such that $|Q|$ is maximal; then $Q \neq P$ since $\mathrm{Aut}_{\mathcal{E}}(P) = \mathrm{Aut}_{\mathcal{F}}(P)$. Since $\mathcal{F}$ is a fusion system, we can also assume that φ is an isomorphism. Since $\mathcal{F}$ is saturated, we can pick a fully automised and receptive subgroup S of P such that S is $\mathcal{F}$-isomorphic to both Q and R. Then $\mathcal{F}$ contains isomorphisms $\psi : Q \to S$ and $\rho : R \to S$ that extend to $N_P(Q)$ and $N_P(R)$, respectively. Since $Q \neq P$, $N_P(Q)$ and $N_P(R)$ are larger than Q, so ψ and ρ are maps in $\mathcal{F}$ by the maximality of $|Q|$. Then $\kappa = \rho\varphi\psi^{-1}$ is an $\mathcal{F}$-automorphism of S that is not an $\mathcal{E}$-morphism; it follows that S is not centric. Since S is receptive, κ extends to an automorphism of N_κ, and it is clear from the definition that N_κ contains $C_P(S)$. Then N_κ is larger than S, and the extension of κ is an $\mathcal{F}$-morphism by the maximality of $|Q|$. Then κ is an $\mathcal{F}$-morphism, a contradiction. □

COROLLARY 2.8. *Let $\mathcal{E}$ and $\mathcal{F}$ be saturated fusion systems on P, and suppose that $\mathrm{Aut}_{\mathcal{E}}(Q) = \mathrm{Aut}_{\mathcal{F}}(Q)$ whenever Q is a centric subgroup of P. Then $\mathcal{E} = \mathcal{F}$.*

Theorem 2.7 is is a rather weak form of Alperin's Fusion Theorem. It is possible to require $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{\mathcal{E}}(Q)$ for a somewhat smaller collection of subgroups of P (see for example [**2**, Theorem I.3.5]). Defining this collection requires one to know the fusion system $\mathcal{F}$, however, so the stronger forms of the theorem do not lead to a strengthening of Corollary 2.8.

EXAMPLE 2.9. Let P be the dihedral group of order 8, with generators s and d such that $s^2 = d^4 = 1$ and $ds = sd^3$. Using Alperin's Fusion Theorem, we can determine all saturated fusion systems on P. P has four centric subgroups: P itself, $C = \langle d \rangle$, $V_1 = \langle s, d^2 \rangle$ and $V_2 = \langle sd, d^2 \rangle$. Now let $\mathcal{F}$ be a saturated fusion system on P. $\mathrm{Aut}_{\mathcal{F}}(P)$ is a subgroup of $\mathrm{Aut}(P)$ that has $\mathrm{Aut}_P(P)$ as a Sylow 2-subgroup; since $\mathrm{Aut}_P(P)$ has index 2 in $\mathrm{Aut}(P)$, we must have $\mathrm{Aut}_{\mathcal{F}}(P) = \mathrm{Aut}_P(P)$. Similarly we have $\mathrm{Aut}_P(C) = \mathrm{Aut}(C)$, so $\mathrm{Aut}_{\mathcal{F}}(C) = \mathrm{Aut}_P(C)$. This leaves V_1 and V_2. Here $\mathrm{Aut}(V_i)$ is isomorphic to S_3, and $\mathrm{Aut}_P(V_i)$ is a subgroup of order 2. Then $\mathrm{Aut}_{\mathcal{F}}(V_i)$ must be either $\mathrm{Aut}_P(V_i)$ or all of $\mathrm{Aut}(V_i)$. There are then at most four saturated fusion systems on P, depending on the choice for $\mathrm{Aut}_{\mathcal{F}}(V_1)$ and $\mathrm{Aut}_{\mathcal{F}}(V_2)$, and all four possibilities can actually be realised. Two of these are isomorphic through an outer automorphism of P that interchanges V_1 and V_2, so this leaves three essentially different saturated fusion systems on P. All three occur as fusion systems of groups: the fusion system of P itself has $\mathrm{Aut}_{\mathcal{F}}(V_i) = \mathrm{Aut}_P(V_i)$, the fusion system of S_4 has $\mathrm{Aut}_{\mathcal{F}}(V_1) = \mathrm{Aut}(V_1)$ and $\mathrm{Aut}_{\mathcal{F}}(V_2) = \mathrm{Aut}_P(V_2)$, and the fusion system of A_6 has $\mathrm{Aut}_{\mathcal{F}}(V_i) = \mathrm{Aut}(V_i)$.

2. Block fusion systems

It is possible to associate a fusion system to each block of a group ring. The first step to constructing these fusion systems is to define the Brauer pairs, which function as an analogue of the p-subgroups of G.

DEFINITION 2.10. A *Brauer pair* is a pair (P, e) where P is a p-subgroup of G and e is a primitive central idempotent of $kC_G(P)$.

The group G acts on the set of Brauer pairs the action $(P, e)^g = (P^g, e^g)$. This definition makes sense because the map $x \mapsto x^g$ provides an isomorphism from $kC_G(P)$ to $kC_G(P^g)$. We can then define the group $N_G(P, e)$ to consist of those elements g of G for which $(P, e)^g = (P, e)$. This is always a subgroup of $N_G(P)$ that contains $PC_G(P)$. When P is the trivial subgroup of G, this implies $N_G(P, e) = G$, so that every element of g fixes (P, e).

We next define a partial order on the set of Brauer pairs, analogous to inclusion of p-subgroups.

DEFINITION 2.11. Let P and Q be p-subgroups of G with $Q \trianglelefteq P$. The *Brauer homomorphism* $\mathrm{Br}_{P/Q}$ is the map from $(kC_G(Q))^P$ to $kC_G(P)$ given by $\sum_{g \in C_G(Q)} d_g g \mapsto \sum_{g \in C_G(P)} d_g g$ (note the change in summation range). When Q is the trivial subgroup, $\mathrm{Br}_{P/Q}$ may also be denoted Br_P.

A Brauer pair (Q, f) is said to be normal in another pair (P, e) if $Q \trianglelefteq P$, $f \in (kC_G(Q))^P$, and $\mathrm{Br}_{P/Q}(f)e = e$; this is written $(Q, f) \trianglelefteq (P, e)$. (Q, f) is said to be contained in (P, e) if there is a chain of normal inclusions $(Q, f) \trianglelefteq (Q_1, f_1) \trianglelefteq \ldots \trianglelefteq (Q_n, f_n) \trianglelefteq (P, e)$; this is written $(Q, f) \leq (P, e)$.

The requirement $\mathrm{Br}_{P/Q}(f)e = e$ deserves some explanation. It will turn out that when (Q, f) is a Brauer pair, $\mathrm{Br}_{P/Q}(f)$ is a central idempotent of $kC_G(P)$. Thus $\mathrm{Br}_{P/Q}(f)e$ is equal to either e or 0.

It is easy to see that the Brauer homomorphism commutes with the action of G, in the sense that $((kC_G(Q))^P)^g = (kC_G(Q^g))^P$ and $\mathrm{Br}_{P/Q}(x)^g = \mathrm{Br}_{P^g/Q^g}(x^g)$ for any $x \in (kC_G(Q))^P$. This implies that the action of G preserves inclusion of Brauer pairs.

Example 2.12. Consider the group $G = A_4$ at $p = 3$, and let $P = \langle(123)\rangle$. $kC_G(1) = kG$ has two primitive central idempotents, namely $e = 1+(12)(34)+(13)(24)+(14)(23)$ and $f = 2\cdot(12)(34)+2\cdot(13)(24)+2\cdot(14)(23)$. $C_G(P)$ is just P and $kC_G(P)$ has one primitive central idempotent, namely 1. Both e and f are P-invariant, and we have $\mathrm{Br}_{P/Q}(e) = 1$ and $\mathrm{Br}_{P/Q}(f) = 0$. Thus $(1, e) \trianglelefteq (P, 1)$, while $(1, f)$ is not contained in a Brauer pair at P.

Example 2.13. Consider the group $G = \langle g, h \mid g^3 = h^4 = 1, h^g = h^2\rangle$ at $p = 2$. Define subgroups $P = \langle h\rangle$ and $Q = \langle h^2\rangle$, and let $\alpha \in k$ be a primitive third root of unity. $kC_G(1) = kG$ has two primitive central idempotents, $e = 1 + h + h^2$ and $f = h + h^2$. Now $C_G(Q) = \langle g, h^2\rangle$, and there are three primitive central idempotents of $kC_G(Q)$: $e' = 1 + h + h^2$, $f_1' = 1 + \alpha h + \alpha^2 h^2$, and $f_2' = 1 + \alpha^2 h + \alpha h^2$. Both e and f are Q-invariant, and we have $\mathrm{Br}_Q(e) = e'$ and $\mathrm{Br}_Q(f) = h+h^2 = f_1' + f_2'$. Then $(1, e) \trianglelefteq (Q, e)$, $(1, f) \trianglelefteq (Q, f_1')$, and $(1, f) \trianglelefteq (Q, f_2')$.

Now $C_G(P)$ is $\langle h\rangle$, and $kC_G(P)$ has just one primitive central idempotent, namely 1. Now e' is P-invariant and $\mathrm{Br}_{P/Q}(e') = 1$, so $(Q, e') \trianglelefteq (P, 1)$. Then we also have $(1, e) \leq (P, 1)$. f_1' and f_2' are not P-invariant, since $(f_1')^h = f_2'$, so (Q, f_1) and (Q, f_2) are not contained in any Brauer pair at P. Finally, both e and f are P-invariant, and we have $\mathrm{Br}_P(e) = 1$ and $\mathrm{Br}_P(f) = 0$. Then $(1, e) \trianglelefteq (P, 1)$, while $(1, f)$ is not contained in a Brauer pair at P.

The next step will be to show that whenever (P, e) is a Brauer pair and $Q \leq P$, there exists a unique primitive central idempotent f of $kC_G(Q)$ such that $(Q, f) \leq (P, e)$. First we record some useful facts about the Brauer homomorphism.

Theorem 2.14. *The Brauer homomorphism is a surjective k-algebra homomorphism.*

Proof. It is obvious that $\mathrm{Br}_{P/Q}$ is k-linear, and it is surjective since $kC_G(P)$ is a subalgebra of $(kC_G(Q))^P$ and $\mathrm{Br}_{P/Q}(x) = x$ for $x \in kC_G(P)$. It only remains to check that $\mathrm{Br}_{P/Q}$ preserves multiplication. Let $\mathcal{C}, \mathcal{D} \in \mathrm{Cl}_P(C_G(Q))$; we will show that $\mathrm{Br}_{P/Q}(\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}) = \mathrm{Br}_{P/Q}(\Sigma\mathcal{C}) \cdot \mathrm{Br}_{P/Q}(\Sigma\mathcal{D})$. If both $\mathcal{C}$ and $\mathcal{D}$ are contained in $C_G(P)$, this is obvious.

If $\mathcal{C}$ is not contained in $C_G(P)$, then every element in $\mathcal{C}$ lies outside of $C_G(P)$ since P fixes $C_G(P)$. This implies $\mathrm{Br}_{P/Q}(\Sigma\mathcal{C}) = 0$. In this case we should then have $\mathrm{Br}_{P/Q}(\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}) = 0$. Now if $\mathcal{D}$ is contained in $C_G(P)$, an element of the form cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ cannot lie in $C_G(P)$, since we would then have $c = (cd)d^{-1} \in C_G(P)$. This implies $\mathrm{Br}_{P/Q}(\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}) = 0$, as desired. Suppose instead that $\mathcal{D}$ lies outside $C_G(P)$, and let $g \in C_G(P)$ be arbitrary. The coefficient of g in $\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}$ is the size of the set $\{(c, d) \mid$

$c \in \mathcal{C}, d \in \mathcal{D}, cd = g\}$. P acts on this set by conjugation, and since $\mathcal{C}$ and $\mathcal{D}$ lie outside of $C_G(P)$, this action has no fixed points. It follows that g has coefficient zero, and so we get $\mathrm{Br}_{P/Q}(\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}) = 0$. □

LEMMA 2.15. *Let $Q \trianglelefteq R \trianglelefteq P$ be p-subgroups of G, and suppose that $Q \trianglelefteq P$. Then $\mathrm{Br}_{P/R} \circ \mathrm{Br}_{R/Q}$ is a well-defined map from $(kC_G(Q))^P$ to $kC_G(P)$, and it equals $\mathrm{Br}_{P/Q}$.*

PROOF. Since P normalizes both Q and R, its action on $kC_G(Q)$ maps $(kC_G(Q))^R$ to itself, and we have $\mathrm{Br}_{R/Q}(x)^h = \mathrm{Br}_{R/Q}(x^h)$ for any $x \in (kC_G(Q))^R$ and $h \in P$. Then $\mathrm{Br}_{R/Q}((kC_G(Q))^P) \subseteq (kC_G(R))^P$, so $\mathrm{Br}_{P/R} \circ \mathrm{Br}_{R/Q}$ is a well-defined map on $(kC_G(Q))^P$. It is clear from the definition of the Brauer homomorphisms that it equals $\mathrm{Br}_{P/Q}$. □

LEMMA 2.16. *Let $Q \trianglelefteq P$ be p-subgroups of G, let $x \in kC_G(Q)$, and suppose that $x \notin (kC_G(Q))^P$. Then $\mathrm{Br}_{P/Q}(\Sigma x^P) = 0$.*

PROOF. Since $x \notin (kC_G(Q))^P$, x^P has size divisible by p. Now let $g \in C_G(P)$; then x and x^h has the same coefficient on g for all $h \in P$. It follows that Σx^P has coefficient zero on g, so $\mathrm{Br}_{P/Q}(\Sigma x^P) = 0$. □

LEMMA 2.17. *Let $Q \trianglelefteq P$ be p-subgroups of G, and let X be a set of elements of $kC_G(Q)$ such that $X^g = X$ for all $g \in P$. Then $\mathrm{Br}_{P/Q}(\Sigma X^P) = \mathrm{Br}_{P/Q}(\Sigma X)$.*

PROOF. Let $Y = X \setminus X^P$ and write $Y = \bigcup_{i=1}^n Y_i$ where each Y_i is a single P-orbit. By the Lemma 2.16, $\mathrm{Br}_{P/Q}(\Sigma Y_i) = 0$ for all i, so $\mathrm{Br}_{P/Q}(\Sigma Y) = \sum_{i=1}^n \mathrm{Br}_{P/Q}(Y_i) = 0$. Then $\mathrm{Br}_{P/Q}(\Sigma X) = \mathrm{Br}_{P/Q}(\Sigma X^P) + \mathrm{Br}_{P/Q}(\Sigma Y) = \mathrm{Br}_{P/Q}(\Sigma X^P)$. □

LEMMA 2.18. *Let (P, e) be a Brauer pair and let $Q \trianglelefteq P$. There exists a unique primitive central idempotent f of $kC_G(Q)$ such that $(Q, f) \trianglelefteq (P, e)$.*

PROOF. Let X be the set of primitive central idempotents of $kC_G(Q)$; then $\mathrm{Br}_{P/Q}(\Sigma X^P) = \mathrm{Br}_{P/Q}(\Sigma X) = 1$ by Lemma 2.17. $Z(kC_G(Q))^P$ is obviously central in $(kC_G(Q))^P$, so we have $\mathrm{Br}_{P/Q}(Z(kC_G(Q))^P) \subseteq Z(kC_G(P))$ since $\mathrm{Br}_{P/Q}$ is surjective. Then the set $\{\mathrm{Br}_{P/Q}(x) \mid x \in X^P, \mathrm{Br}_{P/Q}(x) \neq 0\}$ is a decomposition of unity in $kC_G(P)$. By Corollary 1.17, there is then a unique $f \in X^P$ such that $\mathrm{Br}_{P/Q}(f)e = e$, and then (Q, f) is the unique Brauer pair at Q such that $(Q, f) \trianglelefteq (P, e)$. □

LEMMA 2.19. *Let (P, e) be a Brauer pair and let $Q \leq P$. There exists a Brauer pair (Q, f) at Q such that $(Q, f) \leq (P, e)$.*

PROOF. Since P is a p-group, there is a chain of normal inclusions $Q = Q_n \trianglelefteq Q_{n-1} \trianglelefteq \ldots \trianglelefteq Q_1 \trianglelefteq Q_0 = P$. Set $(Q_0, f_0) = (P, e)$; then by induction and Lemma 2.18, there exists a Brauer pair (Q_i, f_i) such that $(Q_i, f_i) \trianglelefteq (Q_{i-1}, f_{i-1})$. Then $(Q_n, f_n) \leq (P, e)$. □

LEMMA 2.20. *Let $(Q, f) \leq (P, e)$ be two Brauer pairs, and suppose that $Q \trianglelefteq P$. Then $(Q, f) \trianglelefteq (P, e)$.*

PROOF. Consider first the case that there is a pair (R, g) such that $(Q, f) \trianglelefteq (R, g) \trianglelefteq (P, e)$. Then $\mathrm{Br}_{R/Q}(f)g = g$ and $\mathrm{Br}_{P/R}(g)e = e$. Let (Q, f')

be the unique Brauer pair at Q with $(Q, f') \trianglelefteq (P, e)$; then $f' \in (kC_G(Q))^P \subseteq (kC_G(Q))^R$, so we may apply $\mathrm{Br}_{R/Q}$ to f'. Assume that $f \neq f'$; then $f'f = 0$. This implies $\mathrm{Br}_{R/Q}(f')g = \mathrm{Br}_{R/Q}(f')\mathrm{Br}_{R/Q}(f)g = \mathrm{Br}_{R/Q}(f'f)g = 0$. Applying $\mathrm{Br}_{P/R}$, we get $0 = \mathrm{Br}_{P/R}(\mathrm{Br}_{R/Q}(f'))\mathrm{Br}_{P/R}(g) = \mathrm{Br}_{P/Q}(f')\mathrm{Br}_{P/R}(g)$ by Lemma 2.15. But then $\mathrm{Br}_{P/Q}(f')e = \mathrm{Br}_{P/Q}(f')\mathrm{Br}_{P/R}(g)e = 0$, contradicting $(Q, f') \trianglelefteq (P, e)$. Thus $f' = f$ and $(Q, f) \trianglelefteq (P, e)$.

Now consider the general case: we have a sequence of normal inclusions of Brauer pairs $(Q, f) \trianglelefteq (R_1, g_1) \trianglelefteq \ldots \trianglelefteq (R_{m-1}, g_{m-1}) \trianglelefteq (R_m, g_m) = (P, e)$. Since Q is normal in P, it is also normal in each of the groups R_i. Then by the previous case, the normal inclusions $(Q, f) \trianglelefteq (R_i, g_i) \trianglelefteq (R_{i+1}, g_{i+1})$ imply $(Q, f) \trianglelefteq (R_{i+1}, g_{i+1})$, so by induction we find that $(Q, f) \trianglelefteq (P, e)$. □

THEOREM 2.21. *Let (P, e) be a Brauer pair and let $Q \leq P$. There exists a unique Brauer pair (Q, f) at Q such that $(Q, f) \leq (P, e)$.*

PROOF. By Lemma 2.19, there exists a Brauer pair at Q such that $(Q, f) \leq (P, e)$, so we only need to prove uniqueness.

Suppose that that there are Brauer pairs (P, e), (Q, f), and (Q, f') such that $(Q, f) \leq (P, e)$, $(Q, f') \leq (P, e)$, and $f \neq f'$; we can pick P and Q such that $|P : Q|$ is minimal with this property. Then we have sequences of normal inclusions $(Q, f) = (R_m, g_m) \trianglelefteq (R_{m-1}, g_{m-1}) \trianglelefteq \ldots \trianglelefteq (R_1, g_1) \trianglelefteq (P, e)$ and $(Q, f') = (R'_n, g'_n) \trianglelefteq (R'_{m-1}, g'_{m-1}) \trianglelefteq \ldots \trianglelefteq (R'_1, g'_1) \trianglelefteq (P, e)$ where we can assume that R_1 and R'_1 are proper normal subgroups of P. Now we have a sequence of normal inclusions $Q = (R_m \cap R'_1) \trianglelefteq (R_{m-1} \cap R'_1) \trianglelefteq \ldots \trianglelefteq (R_1 \cap R'_1) \trianglelefteq (P \cap R'_1) = R'_1$ running from R'_1 down to Q. We can refine this sequence to a sequence of Brauer pairs ending in (R'_1, g'_1) by working downwards: a Brauer pair at $R_i \cap R'_1$ contains a unique normal subpair at $R_{i+1} \cap R'_1$. In this way, we find a Brauer pair at Q that is a subpair of (R'_1, g'_1); this must be (Q, f') by the minimality of $|P : Q|$. We make note of the Brauer pair at $R_1 \cap R'_1$ in this sequence and denote it $(R_1 \cap R'_1, h')$. We then have $(Q, f') \leq (R_1 \cap R'_1, h') \trianglelefteq (R'_1, g'_1) \trianglelefteq (P, e)$.

Interchanging the roles of (Q, f) and (Q, f'), we similarly construct another Brauer pair $(R_1 \cap R'_1, h)$ such that $(Q, f) \leq (R_1 \cap R'_1, h) \trianglelefteq (R_1, g_1) \trianglelefteq (P, e)$. Since $f \neq f'$, we must have $h \neq h'$ by the minimality of $|P : Q|$. Now $R_1 \cap R'_1$ is the intersection of two normal subgroups of P, so it is normal in P. Then we must have $(R_1 \cap R'_1, h) \trianglelefteq (P, e)$ and $(R_1 \cap R'_1, h') \trianglelefteq (P, e)$, so by Lemma 2.18, we have $h = h'$. This is a contradiction. □

Before continuing, we note a few useful corollaries of this result.

COROLLARY 2.22. *Let (P, e) and $(Q_1, f_1), \ldots, (Q_n, f_n)$ be Brauer pairs with $(Q_i, f_i) \leq (P, e)$ for all i, and let R be a subgroup of P that contains all the Q_i. Then there is a unique Brauer pair (R, f) at R such that $(R, f) \leq (P, e)$ and $(Q_i, f_i) \leq (R, f)$ for all i.*

PROOF. Let (R, f) be the unique Brauer pair at R that is contained in (P, e). Then for each Q_i, there is a unique Brauer pair (Q_i, f'_i) at Q_i with $(Q_i, f'_i) \leq (R, f)$. Then $(Q_i, f'_i) \leq (R, f) \leq (P, e)$, so (Q_i, f'_i) is the unique Brauer pair at Q_i contained in (P, e). It is then equal to (Q_i, f_i). □

COROLLARY 2.23. *Let (P, e) be a Brauer pair containing (Q, f) and (R, g), and let $h \in P$ be an element with the property that $Q^h \leq R$. Then $(Q, f)^h \leq (R, g)$.*

PROOF. Let (Q^h, f') be the unique Brauer pair at Q^h contained in (R, g); then $(Q^h, f') \leq (R, g) \leq (P, e)$. $(Q, f)^h$ is also a Brauer pair at Q^h contained in (P, e), so $(Q, f)^h = (Q^h, f')$ by uniqueness of subpairs. □

COROLLARY 2.24. *Let $(Q, f) \leq (P, e)$ be an inclusion of Brauer pairs. Then $N_P(Q, f) = N_P(Q)$ and $\mathrm{Aut}_P(Q, f) = \mathrm{Aut}_P(Q)$.*

PROOF. For any $h \in N_P(Q)$, we have $Q^h = Q$. Then $(Q, f)^h = (Q, f)$ by the Corollary 2.23, so $N_P(Q) = N_P(Q, f)$. Dividing out by $C_G(Q)$, we also get $\mathrm{Aut}_P(Q) = \mathrm{Aut}_P(Q, f)$. □

The uniqueness of subpairs makes it possible to partition the set of Brauer pairs into disjoint subsets, one for each block.

DEFINITION 2.25. The Brauer pair (P, e) is said to be *associated* to the block b if $(1, b) \leq (P, e)$. A Brauer pair associated to b is also called a *b-Brauer pair*.

THEOREM 2.26. *Each Brauer pair is associated to a unique block. For any inclusion of Brauer pairs $(Q, f) \leq (P, e)$, (Q, f) and (P, e) are associated to the same block. For any Brauer pair (P, e) and any $g \in G$, (P, e) and $(P, e)^g$ are associated to the same block.*

PROOF. Given a Brauer pair (P, e), there is a unique block b with $(1, b) \leq (P, e)$ by Theorem 2.21. Then (P, e) is associated to b but not to any other block. If we have $(Q, f) \leq (P, e)$ with (Q, f) associated to b, then $(1, b) \leq (Q, f) \leq (P, e)$, so (P, e) is associated to b. If $(1, b) \leq (P, e)$ and $g \in G$, then $(1, b) = (1, b)^g \leq (P, e)^g$ since b is central in kG, so $(P, e)^g$ is associated to b. □

Since G acts trivially on the set of blocks of kG, the action on the set of Brauer pairs restricts to an action on the set of b-Brauer pairs, where b is any block of G. This makes it possible to define a fusion system associated to the block b.

DEFINITION 2.27. Given a block b and a maximal b-Brauer pair (P, e), the fusion system $\mathcal{F}_{(P,e)}(b)$ is defined as follows. For any $Q \leq P$, let (Q, e_Q) be the unique Brauer pair at Q with $(Q, e_Q) \leq (P, e)$. The maps in $\mathcal{F}_{(P,e)}(b)$ from Q to R are all maps of the form $x \mapsto x^g$ where g is an element of G such that $(Q, e_Q)^g \leq (R, e_R)$.

Note that Corollary 2.23 guarantees that $\mathcal{F}_{(P,e)}(b)$ is in fact a fusion system.

EXAMPLE 2.28. Consider the group $G = \langle g, h, k \mid g^5 = h^3 = s^2 = 1, gh = hg, g^s = g^4, h^s = h^2 \rangle$ at $p = 5$. Set $P = \langle g \rangle$ and let $\alpha \in k$ be a primitive third root of unity. G has two blocks, $e = 2 + 2 \cdot h + 2 \cdot h^2$ and $f = 4 + 3 \cdot h + 3 \cdot h^2$. We have $C_G(P) = \langle g, h \rangle$ and there are three Brauer pairs at P, given by the primitive idempotents $e' = 2 + 2 \cdot h + 2 \cdot h^2$, $f_1' = 2 + 2\alpha \cdot h + 2\alpha^2 \cdot h^2$ and $f_2' = 2 + 2\alpha^2 \cdot h + 2\alpha \cdot h^2$. (P, e') is associated to e,

while (P, f_1') and (P, f_2') are associated to f. Now s maps (P, e') to itself, so $\mathcal{F}_{(P,e')}(e)$ is the fusion system on P that contains the automorphism $g \mapsto g^4$ of P in addition to the identity map. It is also the group fusion system of the subgroup $\langle g, s\rangle$. (P, f_1') and (P, f_2') are interchanged by s, so $\mathcal{F}_{(P,f_1')}(f)$ is the fusion system on P that has only the identity map on P. It is also the group fusion system of P itself.

As written, the definition of $\mathcal{F}_{(P,e)}(b)$ depends on the choice of (P, e). The next step will therefore be to prove that all maximal b-Brauer pairs are conjugate, so that the choice of (P, e) becomes irrelevant. Afterwards we will prove that $\mathcal{F}_{(P,e)}(b)$ is in fact saturated.

Definition 2.29. We write $\mathrm{SCl}_p(G)$ for the set of conjugacy classes of p-subgroups of G. This is a partially ordered set, with ordering given by $\mathcal{C} \leq \mathcal{D}$ if there exist $P \in \mathcal{C}$ and $Q \in \mathcal{D}$ such that $P \leq Q$. We define a map $\mathcal{S} : \mathrm{Cl}(G) \to \mathrm{SCl}_p(G)$ by letting $\mathcal{S}(\mathcal{C})$ be the conjugacy class of the Sylow p-subgroups of $C_G(c)$ where c is any element of $\mathcal{C}$. When $\mathcal{C} \in \mathrm{Cl}(G)$ and $c \in \mathcal{C}$, we also write $\mathcal{S}(c)$ for $S(\mathcal{C})$. Whenever $b = \sum_{g\in G} c_g g$ is a block of kG, we write $\mathcal{S}(b)$ for the set $\{\mathcal{S}(g) \mid c_g \neq 0\}$.

Let b be a block of kG and let $\mathcal{C}$ be a maximal element of $\mathcal{S}(b)$. The groups in $\mathcal{C}$ are called *defect groups* of b.

The reason for this definition is that it will turn out that when (P, e) is a maximal b-Brauer pair, P is a defect group of b.

Theorem 2.30. *Let M be a downward closed subset of $\mathrm{SCl}_p(G)$, and let I_M be the k-span of $\{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}(G), \mathcal{S}(\mathcal{C}) \in M\}$. Then I_M is an ideal of $Z(kG)$.*

Proof. It is enough to prove that if $\mathcal{C}$ and $\mathcal{D}$ are elements of $\mathrm{Cl}(G)$ with $\mathcal{S}(\mathcal{C}) \in M$, then $\Sigma\mathcal{C} \cdot \Sigma\mathcal{D} \in I_M$. For any $g \in G$, the coefficient on g in $\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}$ is the size of the set $X = \{(c, d) \mid c \in \mathcal{C}, d \in \mathcal{D}, cd = g\}$. Let P be a Sylow p-subgroup of $C_G(g)$; P acts on X by conjugation. Suppose now that $\mathcal{S}(g) \notin M$. Since M is downward closed, we have $\mathcal{S}(g) \not\leq \mathcal{S}(\mathcal{C})$, implying that P is not contained in a Sylow p-subgroup of $C_G(c)$ for any $c \in \mathcal{C}$. Then $P \not\leq C_G(c)$ for all $c \in \mathcal{C}$, so the action of P on X has no fixed points. Then g has coefficient zero in $\Sigma\mathcal{C} \cdot \Sigma\mathcal{D}$. □

Theorem 2.31. *For any block b of kG, $\mathcal{S}(b)$ has a unique maximal element.*

Proof. Let Y be the set of maximal elements of X, and define $\mathcal{C}^{\leq} = \{\mathcal{D} \in \mathrm{SCl}_p(G) \mid \mathcal{D} \leq \mathcal{C}\}$ for any $\mathcal{C} \in \mathrm{SCl}_p(G)$. Set $M = \bigcup_{\mathcal{C}\in Y} \mathcal{C}^{\leq}$; then $X \subseteq M$ so that $e \in I_M$. We clearly have $I_M = \sum_{\mathcal{C}\in Y} I_{\mathcal{C}^{\leq}}$, so by Lemma 1.28, b lies in $I_{\mathcal{C}^{\leq}}$ for some $\mathcal{C} \in Y$. This is only possible if Y consists of a single element. □

Thus defect groups of a block are unique up to conjugation.

In [**2**], one characterisation of defect groups is given in terms of the trace map. For any subgroup H of G, the trace map from $(kG)^H$ to $(kG)^G$ is given by $x \mapsto \sum_{g\in H\backslash G} x^g$, and the defect groups of b are characterised as the minimal subgroups with the property that b lies in the image of the

subgroup's trace map. The connection with this characterisation is that the ideal $I_{\mathcal{C}^{\leq}}$ is in fact the image of the trace map of any group in $\mathcal{C}$.

Next we establish the connection between defect groups and maximal Brauer pairs.

LEMMA 2.32. *Let (P, e) be a maximal Brauer pair. (P, e) is associated to a block b with defect group P, and all Brauer pairs at P associated to b are conjugate.*

PROOF. Let $X = e^{N_G(P)}$, and let R be a p-subgroup of G such that $P \trianglelefteq R$; we then have $\mathrm{Br}_{R/P}(\Sigma X) = \mathrm{Br}_{R/P}(\Sigma X^R)$ by Lemma 2.17. For any $f \in X^R$ we have $\mathrm{Br}_{R/P}(f) = 0$ since (P, f) is conjugate to (P, e) and therefore maximal. Then $\mathrm{Br}_{R/P}(\Sigma X) = 0$. Now let $g \in C_G(P)$ be an element with nonzero coefficient in ΣX, and let T be a Sylow p-subgroup of $C_G(g)$ containing P. If $P \neq T$, we can set $U = N_T(P)$, and we then have $U \neq P$ and $\mathrm{Br}_{U/P}(\Sigma X) \neq 0$, a contradiction. Then $T = P$, and we have $\mathcal{S}(g) = [P]$ for all $g \in C_G(P)$ with nonzero coefficient in ΣX.

Now suppose that x and y are elements of $C_G(P)$ such that $\mathcal{S}(x) = \mathcal{S}(y) = [P]$, and x and y are conjugate in G. Pick a $g \in G$ with $x^g = y$; then $P \leq C_G(y)$ and $P^g \leq C_G(x^g) = C_G(y)$. Since $\mathcal{S}(y) = [P]$, P and P^g are then conjugate in $C_G(y)$, so there is some $h \in C_G(y)$ such that $P^{gh} = P$. Then $gh \in N_G(P)$ and $x^{gh} = y^h = y$, so x and y are conjugate under $N_G(P)$. It follows that for any $x \in C_G(P)$ with $\mathcal{S}(x) = [P]$, we have $\mathrm{Br}_P(\Sigma x^G) = \Sigma x^{N_G(P)}$. In particular, $\Sigma x^{N_G(P)}$ lies in $\mathrm{Br}_P(Z(kG))$ provided that $x \in C_G(P)$ and $\mathcal{S}(x) = [P]$. Now ΣX is a linear combination of elements of this form in $kC_G(P)$, because only elements g with $\mathcal{S}(g) = [P]$ can have nonzero coefficient in ΣX and ΣX is invariant under $N_G(P)$. Then ΣX is an idempotent in $\mathrm{Br}_P(Z(kG))$, so by Theorem 1.25 and Corollary 1.16 there is some idempotent b of $Z(kG)$ with $\mathrm{Br}_P(b) = \Sigma X$.

In fact, b can be chosen to be primitive. Let b' be the primitive idempotent such that $(1, b') \leq (P, e)$; then $\mathrm{Br}_P(b')e = e$. Conjugating by any element g of $N_G(P)$, we get $\mathrm{Br}_P(b')e^g = e^g$, and adding these equations, we obtain $\mathrm{Br}_P(b') \cdot \Sigma X = \Sigma X$. Then $\mathrm{Br}_P(b'b) = \mathrm{Br}_P(b') \cdot \Sigma X = \Sigma X \neq 0$, so $b'b \neq 0$. By Corollary 1.17 we must then have $b'b = b'$, and so $\mathrm{Br}_P(b') = \mathrm{Br}_P(b'b) = \Sigma X$.

Now suppose that $\mathcal{S}(b')$ contains a $\mathcal{C}$ with $[P] < \mathcal{C}$. Then we can pick an R with $P \lhd R$ such that $\mathrm{Br}_R(b') \neq 0$; but this is impossible since $\mathrm{Br}_R(b') = \mathrm{Br}_{R/P}(\mathrm{Br}_P(b')) = \mathrm{Br}_{R/P}(\Sigma X) = 0$. Then $[P]$ is a maximal element of $\mathcal{S}(b')$, so b' has defect P. Finally, since $\mathrm{Br}_P(b') = \Sigma X$, the Brauer pairs at P associated to b' are precisely the pairs (P, f) with $f \in X$, and these are all conjugate. □

THEOREM 2.33. *All maximal Brauer pairs associated to a particular block of G are conjugate.*

PROOF. Let b be a block of G with defect P and let (Q, e) be a maximal Brauer pair associated to b. By the previous lemma, Q is also a defect group of b and so conjugate to P. Then (Q, e) is conjugate to a maximal Brauer pair at P associated to b. As all Brauer pairs at P associated to b are conjugate, the result follows. □

Before we proceed with the proof of saturation, we show that the fusion system associated to the principal block is particularly simple.

LEMMA 2.34. *Let b be the principal block of G. A Brauer pair (P, e) is associated to b if and only if e is the principal block of $kC_G(P)$.*

PROOF. We prove first that if $(Q, f) \leq (P, e)$ and e is principal, then f is principal. It is enough to consider the case $(Q, f) \trianglelefteq (P, e)$, since the general case follows by a straightforward induction.

Write η_Q and η_P for the augmentation maps of $kC_G(Q)$ and $kC_G(P)$; we will first prove that $\eta_P(\mathrm{Br}_{P/Q}(x)) = \eta_Q(x)$ for any $x \in (kC_G(Q))^P$. $(kC_G(Q))^P$ has the basis $\{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}_P(C_G(Q))\}$, and it is enough to prove the formula for each element of this basis. Take a $\mathcal{C} \in \mathrm{Cl}_P(C_G(Q))$, and suppose first that $\mathcal{C}$ consists of a single element. Then this single element lies in $C_G(P)$, so $\eta_P(\mathrm{Br}_{P/Q}(\Sigma\mathcal{C})) = 1 = \eta_Q(\Sigma\mathcal{C})$. If $\mathcal{C}$ does not consist of a single element, none of its elements are fixed points of P, so $\eta_P(\mathrm{Br}_{P/Q}(\Sigma\mathcal{C})) = \eta_P(0) = 0$. Since P is a p-group, the size of $\mathcal{C}$ is divisible by p in this case, so we also have $\eta_Q(\Sigma\mathcal{C}) = 0$.

Now $\mathrm{Br}_{P/Q}(f)$ is a sum of primitive idempotents of $kC_G(Q)$; since e is one of these idempotents, we must have $\eta_P(\mathrm{Br}_{P/Q}(f)) = 1$. Then $\eta_Q(f) = 1$ and f is principal. Considering the case $Q = 1$, we see that if (P, e) is a Brauer pair with e principal, then (P, e) is associated to the principal block b of G.

Let S be a Sylow p-subgroup of G and let g be the principal block of $kC_G(S)$. Then (S, g) is associated to the principal block b, and (S, g) is maximal since S is a Sylow p-subgroup. Then the maximal Brauer pairs associated to b are all principal. Any Brauer pair associated to b is then contained in one of these pairs, so it is also principal. □

THEOREM 2.35. *The fusion system associated to the principal block of G is isomorphic to the group fusion system of G.*

PROOF. Let b be the principal block of G. By the previous lemma, there is exactly one Brauer pair associated to b at each p-subgroup of G; write (Q, e_Q) for the Brauer pair at Q associated to b. Then a Sylow p-subgroup S of G is a defect group of b. For any subgroups P and Q of S and any $g \in G$, we see that $P^g \leq Q$ implies $(P, e_P)^g \leq (Q, e_Q)$ since $(P, e_P)^g$ is the unique Brauer pair at P^g associated to b. Then $\mathcal{F}_{(S,e_S)}(b) = \mathcal{F}_S(G)$. □

Finally we prove that the fusion system associated to a block is saturated. The proof is rather similar to the proof for fusion systems of a group, but it requires a few lemmas first.

LEMMA 2.36. *Let P be a p-subgroup of G, and let H be a subgroup of G that contains $PC_G(P)$. Then for any p-subgroup Q of H that contains P, there is a one-to-one correspondence between Brauer pairs in H at Q and Brauer pairs in G at Q given by the identity map on $kC_G(Q)$, and these correspondences preserve inclusion.*

PROOF. Let Q be a p-subgroup of H containing P. Then $C_G(Q) \leq C_G(P) \leq H$, so $C_H(Q) = C_G(Q)$. Then a Brauer pair at Q in H is given by a primitive central idempotent in $kC_G(Q)$, so the identity map on $kC_G(Q)$

provides a one-to-one correspondence with Brauer pairs at Q in G. Given two p-subgroups Q and R of H with $P \leq R \trianglelefteq Q$, the Brauer map $\mathrm{Br}_{Q/R}$ is defined identically in G and in H. The correspondences then preserve normal inclusions of Brauer pairs and hence all inclusions. □

LEMMA 2.37. *Let (P, e) be a Brauer pair with $N_G(P, e) = G$, and let T be a defect group of the block to which (P, e) is associated. Then $TC_G(P)$ contains a Sylow p-subgroup of G.*

PROOF. Since $N_G(P, e) = G$, we have $P \trianglelefteq G$. Then also $C_G(P) \trianglelefteq G$, so $TC_G(P)$ is a subgroup of G. Let R be a Sylow p-subgroup of $TC_G(P)$ containing T, and let S be a Sylow p-subgroup of G containing R. We now have $\mathrm{Aut}_T(P) \leq \mathrm{Aut}_S(P)$. If $\mathrm{Aut}_T(P) = \mathrm{Aut}_S(P)$, then $TC_G(P)/C_G(P) = SC_G(P)/C_G(P)$; lifting through $C_G(P)$, we get $S \leq TC_G(P)$. Then $S = R$ and we are done. We can therefore assume that $\mathrm{Aut}_S(P) \neq \mathrm{Aut}_T(P)$.

To ease the notation a bit, we let $C = C_G(P)$. We define a map $\varphi : Z(kC) \to k$ as follows. $Z(kC)e$ is a direct factor in $Z(kC)$, and since e is primitive in $Z(kC)$, $Z(kC)e/J(Z(kC)e)$ is isomorphic to k. We then let φ be the projection $Z(kC) \to Z(kC)e$ followed by the quotient map $Z(kC)e \to Z(kC)e/J(Z(kC)e)$. It is clear that $\varphi(e) = 1$. Note that since $e^g = e$ for all $g \in G$, $\varphi(x^g) = \varphi(x)$ for any $x \in Z(kC)$ and $g \in G$. In particular, if $x \in Z(kC)$ is not fixed by S, then $\varphi(\Sigma x^S) = 0$, since the number of elements in x^S is divisible by p and they all have the same image under φ.

We can consider e as an element of kG. Since $N_G(P, e) = G$, e is then an element of $Z(kG)$, and clearly $\mathrm{Br}_P(e) = e$. Thus e lies in $\mathrm{Br}_P(Z(kG))$, so we must have $\mathrm{Br}_P(b) = e$ where b is the block to which e is associated. Now let $g \in C_G(P)$ be an element with nonzero coefficient in e. Then g has nonzero coefficient in b, which implies $\mathcal{S}(g) \leq [T]$ since b has defect T. Since $SC \leq N_G(P, e)$, e lies in the span of the set $\{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}_{SC}(C), \mathcal{S}(\mathcal{C}) \leq [T]\}$. We will show that we have $\varphi(\Sigma\mathcal{C}) = 0$ for all elements of this set, which contradicts $\varphi(e) = 1$.

Let $\mathcal{C} \in \mathrm{Cl}_{SC}(C)$; then $\mathcal{C}$ can be written as a union $\bigcup_{i=1}^n \mathcal{C}_i$ with each $\mathcal{C}_i$ being an element of $\mathrm{Cl}(C)$. Since S normalizes C, it permutes the $\mathcal{C}_i$. In fact, it acts transitively, since for any $\mathcal{D} \in \mathrm{Cl}(C)$, $\bigcup_{s \in S} \mathcal{D}^s$ is obviously an element of $\mathrm{Cl}_{SC}(C)$. Setting $x = \Sigma\mathcal{C}_i$ for some i, we then have $x \in Z(kC)$ and $\Sigma\mathcal{C} = \Sigma x^S$. If we can show that $\mathcal{C}_i$ is a proper subset of $\mathcal{C}$, we will have $\varphi(\Sigma\mathcal{C}) = \varphi(\Sigma x^S) = 0$ since x is not fixed by S.

To finish the proof, we show that when $\mathcal{S}(\mathcal{C}) \leq [T]$, $\mathcal{C}$ does not consist of a single element of $\mathrm{Cl}(C)$. Let $g \in \mathcal{C}$; we first note that since $\mathcal{S}(g) \leq [T]$, any p-subgroup of $\mathrm{Aut}_{C_G(g)}(P)$ is conjugate in $\mathrm{Aut}_G(P)$ to a subgroup of $\mathrm{Aut}_T(P)$. This follows from the fact that $\mathrm{Aut}_G(P)$ is a quotient of $G = N_G(P)$, and in this quotient, the image of T is $\mathrm{Aut}_T(P)$ while the images of p-subgroups of $C_G(g)$ are p-subgroups of $\mathrm{Aut}_{C_G(g)}(P)$.

Suppose now that $\mathcal{C} \in \mathrm{Cl}(C)$. Then for any $s \in S$, there is some $c \in C$ such that $g^{sc} = g$. Then the automorphism $x \mapsto x^{sc}$ of P lies in $\mathrm{Aut}_{C_G(g)}(P)$; since $c \in C = C_G(P)$, this is the same automorphism as $x \mapsto x^s$. Then $\mathrm{Aut}_S(P) \leq \mathrm{Aut}_{C_G(g)}(P)$; but we already know that $\mathrm{Aut}_T(P)$ is a proper subgroup of $\mathrm{Aut}_S(P)$. Then $\mathrm{Aut}_S(P)$ is not conjugate to a subgroup of $\mathrm{Aut}_T(P)$, a contradiction. □

THEOREM 2.38. *The fusion system associated to a block is saturated.*

PROOF. Let b be a block with defect group P, let (P, e) be a maximal b-Brauer pair, let $\mathcal{F} = \mathcal{F}_{(P,e)}(b)$, and let $(Q, f) \leq (P, e)$. Set $N = N_G(Q, f)$; note that Q and $C_G(Q)$ are normal subgroups of N. Consider (Q, f) as a Brauer pair in N, and let (T, f_T) be a maximal Brauer pair in N containing (Q, f). Considered as a Brauer pair in G, (T, f_T) is then contained in a maximal Brauer pair that is conjugate to (P, e), so after applying this conjugation, we have $(Q, f) \trianglelefteq (T, f_T) \leq (P, e)$. We will prove that in this situation, (Q, f) is fully automised and receptive.

We first prove that $N_P(Q, f) = T$. If (R, f_R) is a Brauer pair in G such that $(Q, f) \trianglelefteq (R, f_R)$, then $R \leq N_G(Q, f) = N$, so (R, f_R) is also a Brauer pair in N. Then (R, f_R) is contained in some conjugate of (T, f_T) in N, so in particular, $|R| \leq |T|$. Applying this to the unique Brauer pair in G at $N_P(Q, f)$ that contains (Q, f) and is contained in (P, e), we get $|N_P(Q, f)| \leq |T|$. We also have $T \leq P \cap N_G(Q, f) = N_P(Q, f)$, so $T = N_P(Q, f)$. It follows that $\mathrm{Aut}_P(Q, f) = \mathrm{Aut}_T(Q, f) = TC_G(Q)/C_G(Q)$.

We now prove that (Q, f) is fully automised. For this, we need $\mathrm{Aut}_P(Q)$ to be a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(Q)$. Now $\mathrm{Aut}_{\mathcal{F}}(Q) = N_G(Q, f)/C_G(Q)$, and we have $\mathrm{Aut}_P(Q) = \mathrm{Aut}_P(Q, f) = TC_G(Q)/C_G(Q)$ by Corollary 2.24. It is then enough to show that $TC_G(Q)$ contains a Sylow p-subgroup of $N_G(Q, f) = N$. This was shown in Lemma 2.37.

Finally, we prove that (Q, f) is receptive. For this, we consider (T, f_T) as a Brauer pair in $TC_G(Q)$. It is in fact a maximal Brauer pair in $TC_G(Q)$: any larger Brauer pair would also be a Brauer pair in N, which is impossible since (T, f_T) is maximal in N.

We note that all Brauer pairs in $TC_G(Q)$ that are conjugate to (T, f_T) are in fact conjugate under $C_G(Q)$. For this, let $(T', f_{T'})$ be one such pair, and let $ts \in TC_G(Q)$ with $(T, f_T)^{ts} = (T', f_{T'})$. Then $(T, f_T)^t = (T, f_T)$ since $t \in T$, so we have $(T, f_T)^s = (T', f_{T'})$.

Now let (Q', f') be a Brauer pair that is contained in (P, e), and let $\varphi : (Q', f') \to (Q, f)$ be an isomorphism in $\mathcal{F}$. Then there is some $g \in G$ such that $\varphi(x) = x^g$ for all $x \in Q'$. We extend φ to $N_G(Q', f')$ by setting $\bar{\varphi}(x) = x^g$ for all $x \in N_G(Q', f')$; $\bar{\varphi}$ is then an isomorphism from $N_G(Q', f')$ to $N_G(Q, f)$. Define as usual $N_\varphi = \{h \in N_P(Q', f') \mid (x \mapsto \varphi(\varphi^{-1}(x)^h)) \in \mathrm{Aut}_P(Q)\}$, and let (N_φ, n) be the Brauer pair at N_φ that is contained in (P, e) and contains (Q', f'). As before, (N_φ, n) is then a Brauer pair in $N_G(Q', f')$ containing (Q', f'), so $\bar{\varphi}(N_\varphi, n)$ is a Brauer pair in $N_G(Q, f) = N$ containing (Q, f).

Consider now the group $\bar{\varphi}(N_\varphi)$. It is a subgroup of $\bar{\varphi}(N_P(Q', f'))$ consisting of those elements h for which $(x \mapsto \varphi(\varphi^{-1}(x)^{\bar{\varphi}^{-1}(h)})) \in \mathrm{Aut}_P(Q)$. But we now have $\varphi(\varphi^{-1}(x)^{\bar{\varphi}^{-1}(h)}) = \bar{\varphi}(\bar{\varphi}^{-1}(x)^{\bar{\varphi}^{-1}(h)}) = \bar{\varphi}(\bar{\varphi}^{-1}(x^h)) = x^h$, so we just get $\bar{\varphi}(N_\varphi) = \{h \in \bar{\varphi}(N_P(Q', f')) \mid (x \mapsto x^h) \in \mathrm{Aut}_P(Q)\}$. It follows that $\mathrm{Aut}_{\bar{\varphi}(N_\varphi)}(Q) \leq \mathrm{Aut}_P(Q)$; since $\mathrm{Aut}_P(Q) = TC_G(Q)/C_G(Q)$, we get $\bar{\varphi}(N_\varphi) \leq TC_G(Q)$. Then $\bar{\varphi}(N_\varphi, n)$ is a Brauer pair in $TC_G(Q)$ with $(Q, f) \leq \bar{\varphi}(N_\varphi, n)$. It is then contained in a maximal Brauer pair in $TC_G(Q)$, and this maximal Brauer pair must be conjugate to (T, f_T) since (T, f_T) and $\bar{\varphi}(N_\varphi, n)$ are associated to the same block. Then there is an

$s \in C_G(Q)$ that conjugates this maximal Brauer pair into (T, f_T), so we get $(\bar{\varphi}(N_\varphi, n))^s \leq (T, f_T)$.

In total, we now have $(N_\varphi, n)^{gs} = (\bar{\varphi}(N_\varphi, n))^s \leq (T, f_T)$, and for any $x \in Q'$, $x^{gs} = x^g$ since $(Q')^g = Q$ and $s \in C_G(Q)$. Then the map $x \mapsto x^{gs}$ is the desired extension of φ. □

From Theorem 2.35, it is clear that any saturated fusion system that occurs as a group fusion system also occurs as a block fusion system. The converse is not known, and it is difficult to predict whether it should be true. It is however known that there exist saturated fusion systems that do not occur as block fusion systems (see [**2**, Theorem IV.6.9]).

CHAPTER 3

The center of the group ring

Fix a finite group G. In this chapter, we will develop some tools for describing $Z(kG)$, and we will use these tools to relate the structure of $Z(kG)e$ to the fusion system associated to e, where e is any block of kG.

We fix the following notation. Let q be the smallest power of p such that $|G|_{p'}$ divides $q-1$, and let r be any power of q such that $r \geq |G|_p$. Let $\mathcal{P}$ be the set of p-elements in G.

PROPOSITION 3.1. *For any element g of G, g^r equals $g_{p'}$.*

PROOF. If g is a p-element, we have $g^r = 1$ since r is a power of p and $r \geq |G|_p$. If g is p-regular, its order divides $|G|_{p'}$ which divides $q-1$. Then $g^q = g$, and so $g^r = g$ since r is a power of q. For any g, we then have $g^r = g_p^r \cdot g_{p'}^r = g_{p'}$. □

THEOREM 3.2. *Let $\mathcal{C}$ be any conjugacy class of G. If $g \in G$ is not p-regular, the coefficient of g in $(\Sigma\mathcal{C})^r$ is zero. If g is p-regular, the coefficient equals the coefficient of g in $\Sigma\mathcal{C} \cdot \Sigma\mathcal{P}$.*

PROOF. Let $\mathcal{C}^r$ be the set of r-tuples of elements of $\mathcal{C}$. Define a map $\pi : \mathcal{C}^r \to G$ by $\pi(x_1, x_2, \ldots, x_r) = x_1 x_2 \cdots x_r$. Then $(\Sigma\mathcal{C})^r$ equals $\sum_{\alpha \in \mathcal{C}^r} \pi(\alpha)$.

For an $\alpha \in \mathcal{C}^r$ we denote the entries in the tuple by $\alpha_1, \ldots, \alpha_r$, and we extend the notation α_i to all $i \in \mathbb{Z}$ by setting $\alpha_{lr+j} = \alpha_j$ for $1 \leq j \leq r$ and all $l \in \mathbb{Z}$. For $a, b \in \mathbb{Z}$ with $a < b$, we set $\pi_a^b(\alpha) = \alpha_{a+1}\alpha_{a+2}\cdots\alpha_b$. We extend this to all integers a and b by setting $\pi_a^a(\alpha) = 1$ and $\pi_a^b(\alpha) = (\pi_b^a(\alpha))^{-1}$ for $a > b$. Then for all a, b, c and l, we have $\pi_a^b(\alpha) = \pi_b^a(\alpha)^{-1}$, $\pi_a^c(\alpha) = \pi_a^b(\alpha)\pi_b^c(\alpha)$, and $\pi_{a+lr}^{b+lr}(\alpha) = \pi_a^b(\alpha)$. We also have $\pi(\alpha) = \pi_0^r(\alpha)$.

Now let $\langle\sigma\rangle$ be an infinite cyclic group with generator σ. We define an action of this group on $\mathcal{C}^r$ by setting $(\alpha^{\sigma^n})_i = (\alpha_{i-n})^{\pi_{-n}^0(\alpha)}$ for all $i \in \mathbb{Z}$. This satisfies $\pi_a^b(\alpha^{\sigma^n}) = \pi_{a-n}^{b-n}(\alpha)^{\pi_{-n}^0(\alpha)}$ for all a and b. To see that it is actually an action, we calculate:

$$\begin{aligned}((\alpha^{\sigma^n})^{\sigma^m})_i &= \big((\alpha^{\sigma^n})_{i-m}\big)^{\pi_{-m}^0(\alpha^{\sigma^n})} = \Big((\alpha_{i-m-n})^{\pi_{-n}^0(\alpha)}\Big)^{(\pi_{-m-n}^{-n}(\alpha))^{\pi_{-n}^0(\alpha)}} \\ &= (\alpha_{i-m-n})^{\pi_{-n}^0(\alpha)(\pi_{-n}^0(\alpha))^{-1}\pi_{-m-n}^{-n}(\alpha)\pi_{-n}^0(\alpha)} \\ &= (\alpha_{i-m-n})^{\pi_{-m-n}^0(\alpha)} = (\alpha^{\sigma^{m+n}})_i\end{aligned}$$

Now for any n, we have

$$\begin{aligned}\pi(\alpha^{\sigma^n}) &= \pi_0^r(\alpha^{\sigma^n}) = \pi_{-n}^{r-n}(\alpha)^{\pi_{-n}^0(\alpha)} = \pi_0^{-n}(\alpha)\pi_{-n}^{r-n}(\alpha)\pi_{-n}^0(\alpha) \\ &= \pi_0^{r-n}(\alpha)\pi_{r-n}^r(\alpha) = \pi_0^r(\alpha) = \pi(\alpha)\end{aligned}$$

We can therefore pick a $g \in G$ and restrict the action to those elements $\alpha \in \mathcal{C}^r$ that satisfy $\pi(\alpha) = g$. Denote this set by $\mathcal{C}_g^r$; its size equals the

coefficient of g in $(\Sigma\mathcal{C})^r$. From now on, we assume that α is an element of $\mathcal{C}_g^r$.

We now have $(\alpha^{\sigma^r})_i = (\alpha_{i-r})^{\pi_{-r}^0(\alpha)} = (\alpha_i)^{\pi(\alpha)} = \alpha_i^g$, so that the action of σ^r is just to conjugate by g. Then $\sigma^{r|g|}$ acts by conjugation by $g^{|g|} = 1$, so it acts trivially. We then have an action of a cyclic group of order $r|g|$ on $\mathcal{C}_g^r$, where we still denote the generator by σ. Now the p'-part of $r|g|$ is $|g|_{p'}$; this divides $|G|_{p'}$ which in turn divides $r-1$. It follows that the order of σ^{r-1} is a power of p, so any nontrivial orbit of $\langle\sigma^{r-1}\rangle$ has length divisible by p. Then modulo p, the size of $\mathcal{C}_g^r$ equals the size of its set of fixed points under σ^{r-1}. Denote this set by X_g.

Now let $\alpha \in X_g$; we then have $\alpha_i = (\alpha^{\sigma^{r-1}})_i = (\alpha_{i-r+1})^{\pi_{-r+1}^0(\alpha)} = (\alpha_{i+1})^{\pi_1^r(\alpha)}$. Set $h = \pi_1^r(\alpha)$; then $\alpha_1 h = \pi_0^r(\alpha) = g$ so that $h = \alpha_1^{-1}g$. Since we have $\alpha_i = \alpha_{i+1}^h$ for all i, we can write α as $(\alpha_1, \alpha_1^{h^{-1}}, \alpha_1^{h^{-2}}, \ldots, \alpha_1^{h^{-r+1}})$; in particular, α is defined by its first element alone.

It is now a straightforward induction to check that $\pi_0^n(\alpha) = (\alpha_1 h)^n h^{-n}$ for $0 \le n \le r$, so that $\pi(\alpha) = (\alpha_1 h)^r h^{-r} = g^r h^{-r} = g_{p'} h_{p'}$. For this to equal g, we must have $h_{p'} = g_p$, which can happen only if both elements are trivial. Thus g must be p-regular for X_g to be nonempty, so if g is not p-regular, it has coefficient zero.

In the case where g is p-regular, we have obtained that any $\alpha \in X_g$ is determined by α_1 alone, and that $h = \alpha_1^{-1}g$ is a p-element, since $h_{p'}$ is trivial. We can therefore represent these elements by pairs (α_1, h) satisfying $\alpha_1 \in \mathcal{C}$, $h_{p'} = 1$, and $\alpha_1 h = g$. On the other hand, given a pair (α_1, h) satisfying these three conditions, we do obtain an element α of X_g by setting $\alpha_i = \alpha_1^{h^{1-i}}$ for all $i \in \mathbb{Z}$, this being well-defined since $h^r = h_{p'} = 1$. To determine the size of X_g, we may therefore count these pairs instead. In the obvious way, the number of such pairs equals the coefficient of g in $\Sigma\mathcal{C} \cdot \Sigma\mathcal{P}$. □

THEOREM 3.3. *Every block idempotent of kG has coefficients in $\mathbb{F}_q$, the field with q elements, and the coefficient of any element that is not p-regular is zero.*

PROOF. Let e be a central idempotent of kG and write $e = \sum_{\mathcal{C}\in \mathrm{Cl}(G)} d_{\mathcal{C}} \cdot \Sigma\mathcal{C}$. Then $e = e^r = \sum_{\mathcal{C}\in \mathrm{Cl}(G)} d_{\mathcal{C}}^r \cdot (\Sigma\mathcal{C})^r$. Since non-$p$-regular elements have coefficient zero in $(\Sigma\mathcal{C})^r$ for all $\mathcal{C} \in \mathrm{Cl}(G)$, they also have coefficent zero in e.

Now set $X = \{(\Sigma\mathcal{C})^r \mid \mathcal{C} \in \mathrm{Cl}(G)\}$, and let Y be a subset of X that is a basis for the k-span of X. For any $(\Sigma\mathcal{C})^r \in X$, we have $(\Sigma\mathcal{C})^{rq} = (\Sigma\mathcal{C})^r$ since rq would also have been a valid choice for r. Then we also have $x^q = x$ for all $x \in Y$. Now write $e = \sum_{x\in Y} d_x \cdot x$; then also $e = e^q = \sum_{x\in Y} d_x^q \cdot x$. Comparing coefficients, we get $d_x = d_x^q$ so that $d_x \in \mathbb{F}_q$ for all x. Then e has $\mathbb{F}_q$-coefficients in this basis. Since each element of X has $\mathbb{F}_p$-coefficients in the usual basis, e also has $\mathbb{F}_q$-coefficients in the usual basis. □

We consider now the map $\rho : Z(kG) \to Z(kG)$ given by $\rho(\Sigma\mathcal{C}) = \Sigma\mathcal{C}$ if $g \in \mathcal{C}$ is p-regular and $\rho(\Sigma\mathcal{C}) = 0$ otherwise. This is a k-linear map, but generally not a k-algebra homomorphism.

THEOREM 3.4. *Let $Z(kG) = E \oplus J(Z(kG))$ as in Theorem 1.26. Then the projection map $\pi : Z(kG) \to E$ is given by $\pi(x) = \rho(\Sigma\mathcal{P} \cdot x)$.*

PROOF. By Theorem 3.2, we have $x^r = \rho(\Sigma\mathcal{P} \cdot x)$ whenever $x \in \{\Sigma\mathcal{C} \mid \mathcal{C} \in \mathrm{Cl}(G)\}$. Both sides of this formula are $\mathbb{F}_q$-linear, since r is a power of q, so the formula holds for all elements of $\mathbb{F}_q G$. By Theorem 3.3, this includes the primitive idempotents of $Z(kG)$, so for any such idempotent, we have $\pi(e) = e = e^r = \rho(\Sigma\mathcal{P} \cdot e)$.

For any $x \in J(Z(kG))$, we have $\pi(x) = 0$, so we would like to prove that $\rho(\Sigma\mathcal{P} \cdot x) = 0$ for all $x \in J(Z(kG))$. Having done this, we will then have $\pi(x) = \rho(\Sigma\mathcal{P} \cdot x)$ whenever x is a primitive idempotent or an element of $J(Z(kG))$. Together, these elements span $Z(kG)$ by Theorem 1.26, so we will then be done since both $\pi(x)$ and $\rho(\Sigma\mathcal{P} \cdot x)$ are k-linear.

Now $J(Z(kG))$ is nilpotent, so there is some n such that $J(Z(kG))^{rq^n} = 0$. Writing $x = \sum_{\mathcal{C} \in \mathrm{Cl}(G)} d_{\mathcal{C}} \cdot \Sigma\mathcal{C}$ for some $x \in J(Z(kG))$, we have $0 = x^{rq^n} = \sum_{\mathcal{C} \in \mathrm{Cl}(G)} d_{\mathcal{C}}^{rq^n} \cdot \rho(\Sigma\mathcal{P} \cdot \Sigma\mathcal{C})$ by Theorem 3.2, since rq^n would also have been a valid choice for r. Since ρ is k-linear, this implies $0 = \rho(\Sigma\mathcal{P} \cdot x')$ where $x' = \sum_{\mathcal{C} \in \mathrm{Cl}(G)} d_{\mathcal{C}}^{rq^n} \Sigma\mathcal{C}$. Consider $Z(kG)$ as an $\mathbb{F}_q$-algebra; it has an automorphism σ given by $\sigma(\sum_{\mathcal{C} \in \mathrm{Cl}(G)} d_{\mathcal{C}} \cdot \Sigma\mathcal{C}) = \sum_{\mathcal{C} \in \mathrm{Cl}(G)} d_{\mathcal{C}}^q \cdot \Sigma\mathcal{C}$. Now $x' = \sigma^m(x)$ for some m, not depending on x, so we see that for any $x \in J(Z(kG))$, we have $\rho(\Sigma\mathcal{P} \cdot \sigma^m(x)) = 0$. As x runs over $J(Z(kG))$, $\sigma^m(x)$ runs over $\sigma^m(J(Z(kG))$, which must equal $J(Z(kG))$ since σ^m is an automorphism. Then we have $\rho(\Sigma\mathcal{P} \cdot x) = 0$ for all $x \in J(Z(kG))$. □

Theorem 3.4 appears as (65) in [**6**], with a very different proof.

From now on, we will consider ρ as a map from $\Sigma\mathcal{P} \cdot Z(kG)$ to E.

LEMMA 3.5. *Let $x = \sum_{g \in G} d_g g$ be an element of $\Sigma\mathcal{P} \cdot Z(kG)$. Then $d_g = d_{g_{p'}}$ for all $g \in G$.*

PROOF. It is clearly enough to prove that the statement holds for $\Sigma\mathcal{P} \cdot \Sigma\mathcal{C}$ for all $\mathcal{C} \in \mathrm{Cl}(G)$. Fix a $\mathcal{C}$; the coefficient of g in $\Sigma\mathcal{P} \cdot \Sigma\mathcal{C}$ is the size of the set $X = \{(h, c) \mid h \in \mathcal{P}, c \in \mathcal{C}, hc = g\}$. Set $P = \langle g_p \rangle$; this p-group acts on X by conjugation, and we have $X^P = \{(h, c) \mid h \in \mathcal{P} \cap C_G(P), c \in \mathcal{C} \cap C_G(P), hc = g\}$. We analogously define $Y = \{(h, c) \mid h \in \mathcal{P}, c \in \mathcal{C}, hc = g_{p'}\}$, and note that P also acts on Y. Now g_p is a central p-element of $C_G(P)$, so whenever $h \in \mathcal{P} \cap C_G(P)$, we also have $g_p h \in \mathcal{P} \cap C_G(P)$ and $g_p^{-1} h \in \mathcal{P} \cap C_G(P)$. We can then define an bijection from X^P to Y^P by the map $(h, c) \mapsto (g_p^{-1} h, c)$. □

THEOREM 3.6. *The map $\rho : \Sigma\mathcal{P} \cdot Z(kG) \to E$ is bijective, and its inverse is given by $x \mapsto \Sigma\mathcal{P} \cdot x$*

PROOF. By Lemma 3.5, ρ is injective. Now let e be any block idempotent of kG; then we have $e = \rho(\Sigma\mathcal{P} \cdot e)$ by Theorem 3.4. This implies that e is in the image of ρ and that $\rho^{-1}(e) = \Sigma\mathcal{P} \cdot e$. Since the block idempotents of kG form a basis of E, we see that ρ is also surjective, with inverse given by $x \mapsto \Sigma\mathcal{P} \cdot x$. □

THEOREM 3.7. *$J(Z(kG))$ equals $\mathrm{Ann}_{Z(kG)}(\Sigma\mathcal{P})$.*

PROOF. The projection $Z(kG) \to E$ is given by $x \mapsto \rho(\Sigma\mathcal{P} \cdot x)$ and has kernel $J(Z(kG))$. Then $\rho(\Sigma\mathcal{P} \cdot x) = 0$ for all $x \in J(Z(kG))$, and then $\Sigma\mathcal{P} \cdot x = 0$ since ρ is bijective. Then $J(Z(kG))$ is contained in $\mathrm{Ann}_{Z(kG)}(\Sigma\mathcal{P})$. Conversely, suppose that $x \in Z(kG)$ is an element with $\Sigma\mathcal{P} \cdot x = 0$. Then

obviously $\rho(\Sigma\mathcal{P} \cdot x) = 0$, so $x \in J(Z(kG))$. Thus $J(Z(kG))$ must equal $\mathrm{Ann}_{Z(kG)}(\Sigma\mathcal{P})$. □

LEMMA 3.8. *Let e be a block idempotent of kG. $\Sigma\mathcal{P} \cdot e$ equals e if and only if e has trivial defect group.*

PROOF. We have $\rho(\Sigma\mathcal{P} \cdot e) = e$ by Theorem 3.4. Write $e = \sum_{g \in G} d_g g$ and $\Sigma\mathcal{P} \cdot e = \sum_{g \in G} d'_g g$. By Lemma 3.5, we have $d_g = d'_g$ when g is p-regular, and when g is not p-regular, we have $d_g = 0$ and $d'_g = d'_{g_{p'}} = d_{g_{p'}}$. Suppose now that e does not have trivial defect group. Then there is a nontrivial p-subgroup P such that $\mathrm{Br}_P(e) \neq 0$. This implies that there is a p-regular element $g \in C_G(P)$ with $d_g \neq 0$; taking an arbitrary $h \in P$ with $h \neq 1$, we then get $d'_{gh} = d'_g = d_g \neq 0$. Then $\Sigma\mathcal{P} \cdot e$ and e are not equal.

Conversely, suppose there is some $g \in G$ with $d_g \neq d'_g$. Then g is not p-regular, so $P = \langle g_p \rangle$ is a non-trivial p-subgroup. We now have $g_{p'} \in C_G(P)$ and $d_{g_{p'}} = d'_{g_{p'}} = d'_g \neq 0$, so that $\mathrm{Br}_P(e) \neq 0$. Then e does not have trivial defect group. □

LEMMA 3.9. *For any nontrivial p-subgroup P, $\mathrm{Br}_P((\Sigma\mathcal{P})^2)$ equals 0. In particular, $(\Sigma\mathcal{P})^2$ has coefficient zero on all elements of G that are not p-regular.*

PROOF. We have $\mathrm{Br}_P((\Sigma\mathcal{P})^2) = (\mathrm{Br}_P(\Sigma\mathcal{P}))^2$ and $\mathrm{Br}_P(\Sigma\mathcal{P}) = \Sigma(\mathcal{P} \cap C_G(P))$. Let $g \in C_G(P)$; the coefficient of g in $\mathrm{Br}_P((\Sigma\mathcal{P})^2)$ is then the size of $\{(h, h') \mid h, h' \in \mathcal{P} \cap C_G(P), hh' = g\}$. $Z(P)$ acts on this set by $(h, h')^x = (hx, x^{-1}h')$, and this is clearly a free action. Thus the coefficient of g in $\mathrm{Br}_P((\Sigma\mathcal{P})^2)$ is zero.

Now let $g \in G$ be an element that is not p-regular. Then g centralizes the nontrivial p-subgroup $P = \langle g_p \rangle$, so g has coefficient zero in $(\Sigma\mathcal{P})^2$ since $\mathrm{Br}_P((\Sigma\mathcal{P})^2) = 0$. □

THEOREM 3.10. *$(\Sigma\mathcal{P})^2$ equals the sum of those block idempotents that have trivial defect group.*

PROOF. We have $\rho((\Sigma\mathcal{P})^2) = (\Sigma\mathcal{P})^2$ since $(\Sigma\mathcal{P})^2$ has coefficient zero on elements that are not p-regular. Then $(\Sigma\mathcal{P})^2 \in E$, so we can write $(\Sigma\mathcal{P})^2 = \sum_{i=1}^{n} d_i e_i$ where $d_i \in k$ and the e_i are the block idempotents of kG. Applying Br_P for some nontrivial P, we get $\sum_{i=1}^{n} d_i \mathrm{Br}_P(e_i) = 0$. Since the set $\{\mathrm{Br}_P(e_i) \mid 1 \leq i \leq n, \mathrm{Br}_P(e_i) \neq 0\}$ is a decomposition of unity in $kC_G(P)$, it is linearly independent, so we get $d_i = 0$ whenever $\mathrm{Br}_P(e_i) \neq 0$. This applies to every nontrivial p-subgroup, so $(\Sigma\mathcal{P})^2$ must be a linear combination of those block idempotents that have trivial defect group. For such an idempotent e we have $(\Sigma\mathcal{P})^2 e = (\Sigma\mathcal{P})e = e$ by Lemma 3.8, so the coefficient on e must be 1. □

THEOREM 3.11. *Let e be a block idempotent of kG. $J(Z(kG)e) = 0$ if and only if e has trivial defect group.*

PROOF. By Theorem 3.7, we have seen that $J(Z(kG)) = \mathrm{Ann}_{Z(kG)}(\Sigma\mathcal{P})$, so $J(Z(kG)e)$ must be $\mathrm{Ann}_{Z(kG)e}(\Sigma\mathcal{P} \cdot e)$. Now if e has trivial defect group, we have $\Sigma\mathcal{P} \cdot e = e$; as e is the multiplicative identity of $Z(kG)e$, it follows that $J(Z(kG)e) = 0$. Suppose now that e does not have trivial defect group.

Then $(\Sigma\mathcal{P} \cdot e)^2 = (\Sigma\mathcal{P})^2 e = 0$, so $\Sigma\mathcal{P} \cdot e$ is an element of $J(Z(kG)e)$. It is also not zero, since $\rho(\Sigma\mathcal{P} \cdot e) = e$. □

Having established precisely when $J(Z(kG)e)$ is trivial, the natural next step is to ask for the structure of $J(Z(kG)e)$ when it is non-trivial. As part of this, one can consider under what circumstances the ideal $\ker(\mathrm{Br}_P) \cap J(Z(kG)e)$ of $Z(kG)e$ is trivial, when P is contained in some defect group of e. Calculations of some small examples seem to suggest that this is related to the presence of nontrivial fusion maps inside P in the fusion system associated to e.

EXAMPLE 3.12. Consider again the group $G = \langle g, h, k \mid g^5 = h^3 = s^2 = 1, gh = hg, g^s = g^4, h^s = h^2 \rangle$ of Example 2.28, and set $P = \langle g \rangle$. kG has two blocks at $p = 5$, $e = 2 + 2 \cdot h + 2 \cdot h^2$ and $f = 4 + 3 \cdot h + 3 \cdot h^2$. Both have defect group P, and the fusion system associated to e is the group fusion system of $\langle g, s \rangle$, while the fusion system associated to f is the group fusion system of P. There are three Brauer pairs at P, (P, e') associated to e and (P, f_1') and (P, f_2') associated to f. Now $Z(kC_G(P))$ splits as $Z(kC_G(P))e' \times Z(kC_G(P))f_1' \times Z(kC_G(P))f_2'$ with each factor being isomorphic to $Z(kP)$. $Z(kG)e$ maps onto $Z(kC_G(P))e'$ under Br_P, but not surjectively; the image is in fact the subalgebra of $Z(kC_G(P))e'$ that is fixed by s. $J(Z(kG)e)$ has dimension 3, and it has a basis consisting of two elements that map into a basis of $J(Z(kC_G(P))e')$ and one element (Σk^G, in fact) that is contained in the kernel of Br_P. In this way, $Z(kG)e$ is isomorphic to $Z(k\langle g, s \rangle)$, and there is also an isomorphism between $Z(kC_{\langle g,s \rangle}(P))$ and $Z(kC_G(P))e'$ such that these isomorphisms commute with the Brauer homomorphisms Br_P.

For f, we find that $Z(kG)f$ is isomorphic to $Z(kP)$. The Brauer map sends $Z(kG)f$ injectively into $Z(kC_G(P))f_1' \times Z(kC_G(P))f_2'$. Both of these factors are isomorphic to $Z(kP)$, and they are interchanged by s. Br_P embeds $Z(kG)f$ diagonally into this product; combining with the projection map π onto the first factor, we get a map $\pi \circ \mathrm{Br}_P : Z(kG)f \to Z(kC_G(P))f_1'$. Now $Z(kG)f$ was isomorphic to $Z(kP)$ and $Z(kC_G(P))f_1'$ is isomorphic to $Z(kC_P(P))$, and these isomorphisms map $\pi \circ \mathrm{Br}_P$ in kG into Br_P in kP. In this way they preserve the Brauer homomorphism structure of $Z(kG)f$.

EXAMPLE 3.13. Let G be a group with Sylow p-subgroup P, and suppose that $\mathcal{F}_P(G) = \mathcal{F}_P(P)$. One version of Frobenius' normal p-complement theorem (see [**4**, 7.4.5]) states that in this situation, G has a normal subgroup N of order prime to p such that G is isomorphic to semidirect product of P with N. In this situation, any block b with maximal Brauer pair (Q, f) has $\mathcal{F}_{(Q,f)}(b) = \mathcal{F}_Q(Q)$. An element of G is p-regular if and only if it is contained in N; then for any $g \in N$, the only p-regular element appearing in $\Sigma\mathcal{P} \cdot g$ is g itself. It follows that $\rho(\Sigma\mathcal{P} \cdot x) = x$ for any $x \in Z(kG) \cap kN$. Writing $Z(kG) = J(Z(kG)) \oplus E$ as usual, we actually have $E = Z(kG) \cap kN$.

Suppose further that P is abelian. Further study of $Z(kG)$ shows that for any block e with defect group Q, $Z(kG)e$ is isomorphic to $Z(kQ)$ (which is just kQ, of course), and that $\ker(\mathrm{Br}_R) \cap Z(kG)e = 0$ for any proper subgroup R of Q, as expected.

EXAMPLE 3.14. Consider the group $G = A_5$ at $p = 3$, and set $P = \langle (123) \rangle$. G has five conjugacy classes, which we denote by their cycle type:

$[1]$, $[2^2]$, $[3]$, $[5A]$ and $[5B]$. Here $[5A]$ is the class containing (12345) while $[5B]$ is the class containing (12354). $Z(kG)$ then has dimension 5, and it contains two blocks with trivial defect group and one block e with defect group P. e equals $[1]+[2^2]+[5A]+[5B]$, and $Z(kG)e$ has dimension 3. Set $x=[1]+[3]+[2^2]+[5A]+[5B]$ and $y=2\cdot[2^2]+[5A]+[5B]$; then the set $\{e,x,y\}$ is a basis for $Z(kG)e$ and both x and y are elements of $J(Z(kG)e)$. We have $x^2=xy=y^2=0$ so that $J(Z(kG)e)^2=0$, and y is contained in the kernel of Br_P while x is not. In this way, $Z(kG)e$ is isomorphic to $Z(kN_G(P))$, and the isomorphism includes the Brauer homomorphism structure.

Example 3.15. Consider the group $G=S_5$ at $p=5$, and set $P=\langle(12345)\rangle$. We denote the seven conjugacy classes of G by their cycle type: $[1]$, $[2]$, $[3]$, $[4]$, $[5]$, $[2^2]$, and $[23]$. G has two blocks with trivial defect group and one block e with defect group P. e equals $[1]+3\cdot[3]+2\cdot[2^2]$, and $Z(kG)e$ has dimension 5. We write $t=[1]+3\cdot[3]+[5]+2\cdot[2^2]$, $x=[3]+3\cdot[2^2]$, $y=[4]+4\cdot[23]$, and $z=[2]+[4]+[23]$. Then $\{e,t,x,y,z\}$ is a basis for $Z(kG)e$ with t, x, y, and z being elements of $J(Z(kG)e)$, and $J(Z(kG))^2=0$. The kernel of Br_P contains x, y, and z, but not t. In this way, $Z(kG)e$ is isomorphic to $Z(kN_G(P))$, and this isomorphism includes the Brauer homomorphism structure.

It is however far from obvious where the elements x, y, and z come from. The most immediate idea, if we want to relate the existence of these elements to the existence of nontrivial automorphisms of P, is to pick a $g\in G$ representing a nontrivial automorphism of P and perform some operation with the sum over the conjugacy class of G that contains g. This works out in $kN_G(P)$, but it does not work in G. The three nontrivial automorphisms of P can be represented by (1243), (14)(23), and (1342), and other representatives of a given automorphism belong to the same conjugacy class in G. Here (1243) and (1342) are conjugate in G, so the obvious approach only gives us two different conjugacy classes to work with, instead of three.

Having discarded the obvious ideas as unworkable, one possible approach is then to look for nilpotent ideal inside the entire domain of Br_P, $(kG)^P$, and try to relate them to nilpotent ideals in $Z(kG)$. We will show that in fact $\mathrm{Ann}_{(kG)^P}(\Sigma P)$ is nilpotent. This requires some lemmas.

Lemma 3.16. *Let P be a p-group and let I be the kernel of the augmentation map of kP. Then $I^{|P|}=0$ and $I=J(kP)$.*

Proof. By induction on $|P|$. If P has order p, it is cyclic, so kP is a commutative algebra. Let g be a generator of P; the elements of I then have the form $\sum_{i=0}^{p-1}c_ig^i$ with $\sum_{i=0}^{p-1}c_i=0$. Since kP is commutative, we then have $(\sum_{i=0}^{p-1}c_ig^i)^p=\sum_{i=0}^{p-1}c_i^pe=(\sum_{i=0}^{p-1}c_i)^pe=0$ where e is the identity element of P. Thus every element of I is nilpotent, and since kP is commutative, I itself is then nilpotent. Then the sequence $I\supseteq I^2\supseteq I^3\supseteq\dots$ is strictly decreasing until it reaches 0; since I has dimension $p-1$, this happens no later than I^p. This covers the base case.

For the general case, let Q be a normal subgroup of P of index p, and let $T\subset P$ be a set of representatives for the cosets of Q in P. Let $\varphi:kP\to k(P/Q)$ be the map induced by the surjection $P\to P/Q$; then $\varphi(I)$ lies in the kernel of the augmentation map of $k(P/Q)$. Since P/Q has order p, it

follows that $\varphi(I^p) = \varphi(I)^p = 0$, so I^p lies in the kernel of φ. Now $\ker\varphi$ consists of those elements $\sum_{g\in P} c_g g$ for which $\sum_{g\in Q} c_{gt} = 0$ for all $t \in T$. Let I_Q be the kernel of the augmentation map of kQ; we can then write $\ker\varphi$ as $\bigoplus_{t\in T} tI_Q$ as a k-vector space. Since Q is normal in P, we have $tI_Q = I_Q t$ for all t; this implies that given a sequence $t_1, \dots, t_n$ of elements in T, we have $\prod_{i=1}^n (t_i I_Q) = (\prod_{i=1}^n t_i) I_Q^n$. This is 0 when $n \geq |Q|$. We can then write $(\ker\varphi)^{|Q|} = (\bigoplus_{t\in T} tI_Q)^{|Q|}$ and use the distributive law to see that this equals 0. Then we have $I^{|P|} = (I^p)^{|Q|} \subseteq (\ker\varphi)^{|Q|} = 0$.

I is contained in $J(kP)$ since it is a two-sided nilpotent ideal, and it is a maximal ideal since it has codimension 1. Since $J(kP)$ is a proper ideal of kP, we must then have $I = J(kP)$. □

LEMMA 3.17. *Let R be a ring with characteristic p, let P be a p-group, and let $n \in \mathbb{N}$ be large enough that $J(kP)^n = 0$. Let there be given $n|P|$ elements $a_{i,g}$ of R, indexed by $\{1, \dots, n\} \times P$, such that $\sum_{g\in P} a_{i,g} = 0$ for all i. Let $\pi : P^n \to P$ be the map $\pi(g_1, g_2, \dots, g_n) = g_1 g_2 \cdots g_n$ and let $X = \{\alpha \in P^n \mid \pi(\alpha) = 1\}$. Then $\sum_{\alpha\in X} \prod_{i=1}^n a_{i,\alpha_i} = 0$.*

PROOF. For any subset N of $\{1, \dots, n\}$ and any $\alpha \in P^n$, we write $\pi(\alpha_N)$ for the product $\prod_{i\in N} \alpha_i$, with the factors taken in increasing order by i; we also write N^c for the complement of N in $\{1, \dots, n\}$. We can then write

$$\begin{aligned}\sum_{\alpha\in X} \prod_{i=1}^n a_{i,\alpha_i} &= \sum_{\substack{\alpha\in P^n \\ \pi(\alpha)=1}} \prod_{i=1}^n a_{i,\alpha_i} \\ &= \sum_{N\subseteq\{1,\dots,n\}} (-1)^{n-|N|} \sum_{\substack{\alpha\in P^N \\ \pi(\alpha_N)=1}} \prod_{i\in N} a_{i,\alpha_i} \prod_{i\in N^c} \left(\sum_{g\in P} a_{i,g}\right)\end{aligned}$$

In the last expression, only the term $N = \{1, \dots, n\}$ is nonzero; for any other N, all terms in the inner sum contain a factor of the form $\sum_{g\in P} a_{i,g}$, which is zero. We apply the distributive law:

$$\begin{aligned}\sum_{\substack{\alpha\in P^N \\ \pi(\alpha_N)=1}} \prod_{i\in N} a_{i,\alpha_i} \prod_{i\in N^c} \left(\sum_{g\in P} a_{i,g}\right) &= \sum_{\substack{\alpha\in P^N \\ \pi(\alpha_N)=1}} \prod_{i\in N} a_{i,\alpha_i} \left(\sum_{\beta\in P^{N^c}} \prod_{i\in N^c} a_{i,\beta_i}\right) \\ &= \sum_{\substack{\alpha\in P^N \\ \pi(\alpha_N)=1}} \sum_{\beta\in P^{N^c}} \prod_{i\in N} a_{i,\alpha_i} \prod_{i\in N^c} a_{i,\beta_i} \\ &= \sum_{\substack{\alpha\in P^n \\ \pi(\alpha_N)=1}} \prod_{i=1}^N a_{i,\alpha_i}\end{aligned}$$

We insert this and interchange the two sums:

$$\sum_{N\subseteq\{1,\dots,n\}}(-1)^{n-|N|}\sum_{\substack{\alpha\in P^n\\ \pi(\alpha_N)=1}}\prod_{i=1}^n a_{i,\alpha_i}=\sum_{\alpha\in P^n}\sum_{\substack{N\subseteq\{1,\dots,n\}\\ \pi(\alpha_N)=1}}(-1)^{n-|N|}\prod_{i=1}^n a_{i,\alpha_i}$$

$$=\sum_{\alpha\in P^n}\prod_{i=1}^n a_{i,\alpha_i}\left(\sum_{\substack{N\subseteq\{1,\dots,n\}\\ \pi(\alpha_N)=1}}(-1)^{n-|N|}\right)$$

Now for a given α, the expression $\sum_{N\subseteq\{1,\dots,n\},\pi(\alpha_N)=1}(-1)^{n-|N|}$ is precisely the coefficient on the identity element in $\prod_{i=1}^n(\alpha_i-1)$, an element of kP. Since $g-1$ is in the kernel of the augmentation map of kP for all $g\in P$, $\prod_{i=1}^n(\alpha_i-1)$ is an element of $J(kP)^n$, and therefore zero by Lemma 3.16. Thus the entire sum reduces to 0.

It may appear that this argument requires R to be commutative, but this is actually not the case. The product $\prod_{i\in N}a_{i,\alpha_i}\prod_{i\in N^c}(\sum_{g\in P}a_{i,g})$ contains one factor for each $i\in\{1,\dots,n\}$, and all of these factors should be taken in increasing order by i. After applying the distributive law, this product then becomes $\sum_\beta\prod_{i=1}^n a_{i,\beta_i}$ where β runs over those elements of P^n whose restriction to N equals α. This can then be merged with the outer sum, and the argument proceeds as before. □

THEOREM 3.18. *Let P be a p-subgroup of G. $\mathrm{Ann}_{(kG)^P}(\Sigma P)$ is nilpotent.*

PROOF. Let $I=\mathrm{Ann}_{(kG)^P}(\Sigma P)$; we will show that $I^n=0$ if n is large enough that $J(kP)^n=0$. Let $x_1,\dots,x_n$ be elements of $(kG)^P$ and consider the element $\prod_{i=1}^n x_i$. I^n is spanned by elements of this form, so it is enough to show that these elements are 0. Write $x_i=\sum_{g\in G}c_{i,g}g$; we then have $\prod_{i=1}^n x_i=\sum_{\alpha\in G^n}\pi(\alpha)\prod_{i=1}^n c_{i,\alpha_i}$. We define an action of P^{n-1} on G^n by setting $\alpha^\beta=(\alpha_1\beta_1,\beta_1^{-1}\alpha_2\beta_2,\beta_2^{-1}\alpha_3\beta_3,\dots,\beta_{n-2}^{-1}\alpha_{n-1}\beta_{n-1},\beta_{n-1}^{-1}\alpha_{n-1})$. It is clear from the definition that $\pi(\alpha^\beta)=\pi(\alpha)$ for all α and β, and a simple induction argument shows that if $\alpha^\beta=\alpha$ then $\beta=1$. Then the action is free. Picking a set X of representatives of the orbits of P^{n-1} in G^n, we then get:

$$\sum_{\alpha\in G^n}\pi(\alpha)\prod_{i=1}^n c_{i,\alpha_i}=\sum_{\alpha\in X}\sum_{\beta\in P^{n-1}}\pi(\alpha^\beta)\prod_{i=1}^n c_{i,(\alpha^\beta)_i}$$

$$=\sum_{\alpha\in X}\pi(\alpha)\sum_{\beta\in P^{n-1}}\prod_{i=1}^n c_{i,(\alpha^\beta)_i}$$

It is then enough to show that $\sum_{\beta\in P^{n-1}}\prod_{i=1}^n c_{i,(\alpha^\beta)_i}=0$ for any $\alpha\in G^n$.

Define now $d_{i,g}=c_{i,\alpha_i g^{-1}}$ for all i and all $g\in P$. Then $\sum_{g\in P}d_{i,g}$ is the coefficient on α_i in $x_i\cdot\Sigma P$; this equals 0, so $\sum_{g\in P}d_{i,g}=0$ for all i. Since the x_i are elements of $(kG)^P$, we further have $c_{i,g\alpha_i h}=c_{i,\alpha_i hg}=d_{i,(hg)^{-1}}=d_{i,g^{-1}h^{-1}}$ for any $g,h\in P$. In particular, we get $c_{i,(\alpha^\beta)_i}=c_{i,\beta_{i-1}^{-1}\alpha_i\beta_i}=d_{i,\beta_{i-1}\beta_i^{-1}}$ (where we let $\beta_0=\beta_n=1$). Denoting the identity element of G^n as 1, we further get $d_{i,\beta_{i-1}\beta_i^{-1}}=d_{i,(1^{\beta^{-1}})_i}$. Then $\sum_{\beta\in P^{n-1}}\prod_{i=1}^n c_{i,(\alpha^\beta)_i}=$

$\sum_{\beta \in P^{n-1}} \prod_{i=1}^{n} d_{i,(1^{\beta^{-1}})_i}$. From the definition of the action, it is clear that the orbit containing 1 is a subset of P^n in which every element α satisfies $\pi(\alpha) = 1$. It has $|P|^{n-1}$ elements since the action is free; as there are only $|P|^{n-1}$ elements of P^n with $\pi(\alpha) = 1$, they must all lie in the orbit containing 1. Then the sum becomes $\sum_{\alpha \in P^n, \pi(\alpha)=1} \prod_{i=1}^{n} d_{i,\alpha_i}$, which is 0 by Lemma 3.17 □

One possible connection between block fusion systems and the result of Theorem 3.18 is given below.

THEOREM 3.19. *Let $\mathcal{C} \in \mathrm{Cl}_P(G)$. Then $\Sigma\mathcal{C} \cdot \Sigma P = 0$ if and only if there are elements $g \in \mathcal{C}$ and $x \in P$ such that $x^g \in P$ and $x \neq x^g$.*

PROOF. Note that since ΣP is central in $(kG)^P$, we have $\Sigma\mathcal{C} \cdot \Sigma P = \Sigma P \cdot \Sigma\mathcal{C}$.

Suppose that we have $g \in \mathcal{C}$ and $x \in P$ with $x \neq x^g$ and $x \in P$. Set $Q = \langle C_P(g), x \rangle$ and $R = Q^g$; then R is contained in P and P^g and $C_P(g)$ is a proper subgroup of R. Let T be a set of representatives for the right cosets of $C_P(g)$ in R. Since $C_P(g)$ is a proper subgroup of R, $|T|$ is then divisible by p. Let U be a set of representatives for the right cosets of R in P; then TU is a set of representatives of the right cosets of $C_P(g)$ in P, so we have $\Sigma\mathcal{C} = \sum_{z \in TU} g^z$. Now whenever h is an element of P, we have $\Sigma P \cdot h = \Sigma P$, so in particular we get $\Sigma P \cdot g^z = \Sigma P \cdot z^{-1}gz = \Sigma P \cdot gz$. Then we have

$$\begin{aligned} \Sigma P \cdot \Sigma\mathcal{C} &= \sum_{z \in TU} \Sigma P \cdot g^z = \sum_{z \in TU} \Sigma P \cdot gz \\ &= \Sigma P \cdot g \cdot \Sigma(TU) = g \cdot \Sigma P^g \cdot \Sigma T \cdot \Sigma U \end{aligned}$$

Now let V be a set of representatives for the left cosets of R in P^g, so that $\Sigma P^g = \Sigma V \cdot \Sigma R$. We then have $\Sigma P \cdot \Sigma\mathcal{C} = g \cdot \Sigma V \cdot \Sigma R \cdot \Sigma T \cdot \Sigma U$. Now every element of T is contained in R, so $\Sigma R \cdot \Sigma T$ equals $|T|\Sigma R$, which is 0 since $|T|$ is divisible by p. Then $\Sigma P \cdot \Sigma\mathcal{C} = 0$.

For the converse, suppose that $\Sigma\mathcal{C} \cdot \Sigma P = 0$, and pick a $g \in \mathcal{C}$. Let $X = \{(c, h) \mid c \in \mathcal{C}, h \in P, ch = g\}$, so that the coefficient on g in $\Sigma\mathcal{C} \cdot \Sigma P$ equals $|X|$. Since this coefficient is zero, $|X|$ is divisible by p; it is also nonempty since it contains $(g, 1)$. Then there are some $x, y \in P$ with $(g^x, y) \in X$ and $(g^x, y) \neq (g, 1)$. Now since $g^x y = g$, $g^x = g$ implies $y = 1$ and vice versa. Then we must have $y \neq 1$. Now $x^g = g^{-1}xg = g^{-1}x(g^x y) = g^{-1}xx^{-1}gxy = xy$, so $x^g \in P$ and $x^g = xy \neq x$. □

CHAPTER 4

The symmetric and alternating groups

In this chapter, we will prove that fusion system associated to a block of a symmetric group is always the group fusion system of a symmetric group, and an analogous result holds for alternating groups. This is known for the symmetric groups (see [**5**, Theorem 7.2]), and the methods used there transfer easily to the alternating groups when $p > 2$. The case of the alternating groups at $p = 2$ does not seem to have appeared in print, however.

LEMMA 4.1. *Suppose that P is a defect group of a block e of G. Then there exists a p-regular element g such that P is a Sylow p-subgroup of $C_G(P)$ and g has nonzero coefficient in e.*

PROOF. This follows directly from the definition of defect groups. □

LEMMA 4.2. *Every block idempotent of kG is contained in the k-span of the set $\{(\Sigma\mathcal{C})^r \mid \mathcal{C} \in \mathrm{Cl}(G)\}$.*

PROOF. Let e be a block idempotent; since e is central, we can write $e = \sum_{\mathcal{C}\in\mathrm{Cl}(G)} d_{\mathcal{C}} \cdot \Sigma\mathcal{C}$. Then $e = e^r = \sum_{\mathcal{C}\in\mathrm{Cl}(G)} d_{\mathcal{C}}^r \cdot (\Sigma\mathcal{C})^r$. □

THEOREM 4.3. *Let g be a p-regular element of G. Suppose that there are p-subgroups P and T of G such that g centralizes P, g does not centralize T, and T is a normal subgroup of $C_G(P)$. Then g has coefficient zero in all block idempotents of G.*

PROOF. We will prove that g has coefficient zero in $(\Sigma\mathcal{C})^r$ for any $\mathcal{C} \in \mathrm{Cl}(G)$; this is sufficient by Lemma 4.2. Pick a $\mathcal{C} \in \mathrm{Cl}(G)$ and set $M = \{(c, h) \mid c \in \mathcal{C}, h \in \mathcal{P}, ch = g\}$; the coefficient of g in $(\Sigma\mathcal{C})^r$ is then equal to $|M|$ by Theorem 3.2. P acts on M by conjugation, and the coefficient is then also equal to $|M^P|$.

We now define an action of T on M^P by setting $(c, h)^x = (c^x, x^{-1}x^c h)$. Here we have $c^x \in \mathcal{C}$ and $c^x \cdot x^{-1}x^c h = x^{-1}cxx^{-1}c^{-1}xch = ch = g$. Further, $x^{-1}x^c$ lies in T since $c \in C_G(P)$ and T is normal in $C_G(P)$. Then $x^{-1}x^c h$ lies in $\langle T, h\rangle$, which is a p-group since T is a p-group, h is a p-element, and h lies in $C_G(P)$ and so normalizes T. Thus $x^{-1}x^c h$ is a p-element, and so $(c, h)^x$ is an element of M. Since x, c, and h are all contained in $C_G(P)$, so are c^x and $x^{-1}x^c h$, so $(c, h)^x$ is in fact an element of M^P. Finally we check

the associativity of the action:

$$\begin{aligned}((c,h)^x)^y &= (c^x, x^{-1}x^c h)^y = (c^{xy}, y^{-1}y^{c^x}x^{-1}x^c h)\\ &= (c^{xy}, y^{-1}y^{x^{-1}cx}x^{-1}(c^{-1}xc)h)\\ &= (c^{xy}, y^{-1}(x^{-1}c^{-1}xyx^{-1}cx)x^{-1}c^{-1}xch)\\ &= (c^{xy}, (xy)^{-1}c^{-1}(xy)ch)\\ &= (c^{xy}, (xy)^{-1}c^{xy}h) = (c,h)^{xy}\end{aligned}$$

Thus we have a genuine action of T on M^P, and it is enough to prove that this action has no fixed points. Suppose that (c,h) is a fixed point; then $c^x = c$ for all $x \in T$, so c centralizes T. Now we have $c = gh^{-1}$ with both g and h^{-1} contained in $C_G(P)$, so they both normalize T. Then the maps $x \mapsto x^g$ and $x \mapsto x^{h^{-1}}$ are mutually inverse automorphisms of T. But g is p-regular and h^{-1} is a p-element, so this can only happen if both maps are trivial. Then g centralizes T, contrary to our assumptions. □

We record a we basic facts about conjugacy in the symmetric and alternating groups.

PROPOSITION 4.4. *Let g be an element of S_n of cycle type $1^m c_1^{m_1} \cdots c_s^{m_s}$. The centralizer of g in S_n is isomorphic to $S_m \times \prod_{i=1}^s (C_{c_i} \wr S_{m_i})$, with the S_m factor embedded as the group of permutations of the m fixed points of g.*

Here $C_c \wr S_m$ is the wreath product, given as the semidirect product of C_c^m with S_m where S_m acts on C_c^m by permuting its factors.

PROPOSITION 4.5. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

LEMMA 4.6. *Let $S_m \subseteq S_n$ and let $\mathcal{C} \in \mathrm{Cl}(S_n)$. Then $\mathcal{C} \cap S_m$ is an element of $\mathrm{Cl}(S_m)$.*

PROOF. Any two elements of S_m that have the same cycle type in S_n also have the same cycle type in S_m. Thus elements of S_m that are conjugate in S_n are already conjugate in S_m. □

LEMMA 4.7. *Let $A_m \subseteq A_n$ with $n - m \geq 2$ and let $\mathcal{C} \in \mathrm{Cl}(A_n)$. Then $\mathcal{C} \cap A_m$ is an element of $\mathrm{Cl}(S_m)$.*

PROOF. Suppose that $x, y \in A_m$ are conjugate in A_n. Then they have the same cycle type in A_n, so they also have the same cycle type in A_m. They are then conjugate under S_m. □

LEMMA 4.8. *For any $\mathcal{C} \in \mathrm{Cl}(A_n)$ and any odd permutation $x \in S_n$, either $\mathcal{C}^x = \mathcal{C}$ and $\mathcal{C} \in \mathrm{Cl}(S_n)$ or $\mathcal{C}^x$ and $\mathcal{C}$ are disjoint and $\mathcal{C} \cap \mathcal{C}^x \in \mathrm{Cl}(S_n)$.*

PROOF. Because A_n is normal in S_n, we have $\mathcal{C}^x \in \mathrm{Cl}(A_n)$ whenever $\mathcal{C} \in \mathrm{Cl}(A_n)$ and $x \in S_n$. Then $\mathcal{C}$ and $\mathcal{C}^x$ are either identical or disjoint. As every element of S_n lies in either A_n or xA_n, it is clear that in either case, $\mathcal{C} \cup \mathcal{C}^x$ contains all S_n-conjugates of the elements of $\mathcal{C}$, so it is an element of $\mathrm{Cl}(S_n)$. □

LEMMA 4.9. *Let $H \leq S_m \leq S_n$. Then $\mathrm{Aut}_{S_m}(H) = \mathrm{Aut}_{S_n}(H)$.*

PROOF. Let N be the set of fixed points of H in $\{1,\dots,n\}$, and let M be its complement. Then $N_{S_n}(H)$ is contained in $S_N \times S_M$, and all of S_N is contained in $C_{S_n}(H)$ and hence also in $N_{S_n}(H)$. Then $N_{S_n}(H)$ splits as $N_{S_M}(H) \times S_N$, and similarly $C_{S_n}(H)$ splits as $C_{S_M}(H) \times S_N$. Then $\mathrm{Aut}_{S_n}(H)$ equals $(N_{S_M}(H) \times S_N)/(C_{S_M}(H) \times S_N) = N_{S_M}(H)/C_{S_M}(H)$, so $\mathrm{Aut}_{S_n}(H) = \mathrm{Aut}_{S_M}(H)$. By a similar argument, $\mathrm{Aut}_{S_m}(H)$ also equals $\mathrm{Aut}_{S_M}(H)$. □

THEOREM 4.10. *Let $G = S_n$, or let $G = A_n$ and $p > 2$, and let g be a p-regular element of G. Suppose that g contains p cycles of the same length greater than 1. Then g has coefficient zero in all block idempotents of S_n.*

PROOF. We will find p-subgroups P and T of G such that the conditions of Theorem 4.3 are satisfied. We consider the case $G = S_n$. When $p > 2$, P and T are contained in A_n, so the case $G = A_n$ follows immediately.

Suppose that g contains p cycles of length $l > 1$. We label the pl elements of $\{1,\dots,n\}$ involved in these cycles by the elements of $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ in such a way that we have $g(i,j) = (i+1,j)$ for all $(i,j) \in \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. The remaining elements of $\{1,\dots,n\}$ we collect in the set N, so that we have a bijection between $\{1,\dots,n\}$ and $(\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \amalg N$.

For each $i \in \mathbb{Z}/l\mathbb{Z}$, we now define h_i to be the p-cycle mapping $(i,j) \in \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ to $(i,j+1)$ for all $j \in \mathbb{Z}/p\mathbb{Z}$ and fixing all other elements. We define T to be the group generated by all the h_i, and P to be the group generated by $h = \prod_{i \in \mathbb{Z}/l\mathbb{Z}} h_i$. This is unambiguous since the h_i all commute with each other. Now h commutes with g since on N, we have $gh = g = hg$, and on $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, both hg and gh map (i,j) to $(i+1,j+1)$ for all i and j. Then g centralizes P.

A straightforward computation shows that $h_i^g = h_{i-1}$ for all i, so that g does not centralize T when $l > 1$. It now remains to show that T is normal in $C_G(P)$. Take an arbitrary $x \in C_G(P)$ and an $(i,j) \in \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then $x(i,j) \notin N$ since N consists of the fixed points of P and (i,j) is not a fixed point of P. We then have $x(i,j) = (i',j')$ for some i' and j'. Now for any $n \in \mathbb{Z}/p\mathbb{Z}$, we then have $x^{h^n}(i,j-n) = (i',j'-n)$, and $x^{h^n} = x$ since $x \in C_G(P)$. Thus $x(i,j-n) = (i',j'-n)$ for all n. It follows that $h_{i'}^x = h_i$; applying this to all i, we see that x permutes the h_i. Then x normalizes T, so T is normal in $C_G(P)$. □

THEOREM 4.11. *Let $G = A_n$ and $p = 2$, and let g be a p-regular element of G. Suppose that g contains two pairs of cycles of the same length, at least one of these lengths being greater than 1. Then g has coefficient zero in all block idempotents of G.*

PROOF. We again find p-subgroups P and T of G such that the conditions of Theorem 4.3 are satisfied.

Note that since g is 2-regular, its cycles all have odd length. Take two cycles of length l and two of length m (possibly with $l = m$), and decompose $\{1,\dots,n\}$ as $(\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \amalg (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \amalg N$ such that on the first two sets g acts by $g(i,j) = (i+1,j)$. For each $i \in \mathbb{Z}/l\mathbb{Z}$, define h_i to be the transposition interchanging the $(i,0)$ and $(i,1)$ elements of $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and for each $i \in \mathbb{Z}/m\mathbb{Z}$, define analogously h'_i to be the transposition interchanging the $(i,0)$ and $(i,1)$ elements of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $h = \prod_{i \in \mathbb{Z}/l\mathbb{Z}} h_i \cdot \prod_{i \in \mathbb{Z}/m\mathbb{Z}} h'_i$;

as before, this is well-defined since the h_i and h'_i all commute. It is also an even permutation, since l and m are both odd.

Let P be the group generated by h and let T be the group generated by the elements h_ih_j, $h_ih'_j$, and $h'_ih'_j$ for all i and j. Then P and T are both contained in A_n, and the same arguments as before show that T is normal in $C_G(P)$ and that g acts on T by $h_i^g = h_{i-1}$ and $(h'_i)^g = h'_{i-1}$. Now l and m are not both 1; suppose without loss of generality that $l > 1$. Then $l \geq 3$, and we have $(h_1h_2)^g = h_0h_1 \neq h_1h_2$, so that g does not centralize T. □

THEOREM 4.12. *Let $G = S_n$ or $G = A_n$ and let e be a block of G. The defect groups of e are Sylow p-subgroups of some S_m or A_m respectively for $m \leq n$.*

PROOF. Consider first $G = S_n$. Pick a g with nonzero coefficient in e such that the Sylow p-subgroups of $C_G(g)$ are defect groups of e. Writing the cycle type of g as $1^m c_1^{m_1} c_2^{m_2} \cdots c_s^{m_s}$, we have $m_i < p$ and $p \nmid c_i$ for all i. Now $C_G(g)$ is isomorphic to $S_m \times \prod_{i=1}^s (C_{c_i} \wr S_{m_i})$, and each factor $C_{c_i} \wr S_{m_i}$ now has order prime to p. It follows that the Sylow p-subgroups of $C_G(g)$ are the Sylow p-subgroups of S_m.

In the case $G = A_n$, $C_G(g)$ has index 1 or 2 in $C_{S_n}(g)$. It follows that if $p > 2$, $C_G(g)$ and $C_{S_n}(g)$ have the same Sylow p-subgroups, so the defect groups of e are the Sylow p-subgroups of some S_m, $m \leq n$. These are the same as the Sylow p-subgroups of A_m, again since $p > 2$.

In the case $G = A_n$ and $p = 2$, consider first the possibility that $m_i < 2$ for all i. Since g is p-regular, c_i is odd for all i, so the factor $\prod_{i=1}^s (C_{c_i} \wr S_{m_i})$ has odd order. Then all of its elements are even permutations, so they are contained in A_n. It follows that the part of $C_{S_n}(g)$ that lies in A_n is $A_m \times \prod_{i=1}^s (C_{c_i} \wr S_{m_i})$, and its Sylow p-subgroups are those of A_m. Now consider the possibility that there is some i with $m_i \geq 2$. Then we still have $m_i < 4$, and we must have $m_j < 2$ for all $j \neq i$, and also $m < 2$. Then the only factor of the centralizer with even order is $C_{c_i} \wr S_{m_i}$. Since c_i is odd and m_i is 2 or 3, the Sylow p-subgroups of this group are each generated by a transposition in S_{m_i}. This transposition is embedded into S_n as a product of c_i transpositions; since c_i is odd, this element does not lie in A_n. It follows that $C_G(g)$ has odd order, so e has trivial defect group. □

This establishes the defect groups. To determine the fusion systems, we will make use of Corollary 2.8.

LEMMA 4.13. *Let P be a Sylow p-subgroup of S_{pm} or A_{pm}. For any centric subgroup Q of P, Q has no fixed points and $C_{S_{pm}}(Q)$ is a p-group. One exception to this occurs for A_{pm} when $p = 2$ and m is odd; in this case there are two points that may be fixed points of some Q.*

PROOF. Let $G = S_{pm}$ and let z be an element of G of cycle type p^m. $C_G(z)$ is then isomorphic to $C_p \wr S_m$, which has order $p^m \cdot m!$. This equals $\prod_{i=1}^m pi$, the product of those factors of $(pm)!$ that are divisible by p. It follows that the index of $C_G(z)$ in G is prime to p, so the two groups have isomorphic Sylow p-subgroups. We can therefore assume $P \leq C_G(z)$. Since z is a central p-element of $C_G(z)$ and P is a Sylow p-subgroup of $C_G(z)$, we have $z \in P$. Then z is a central element of P; since Q contains $Z(P)$ we have $z \in Q$, and so Q has no fixed points.

Suppose now that $C_G(Q)$ is not a p-group, and let x be a nontrivial p-regular element of $C_G(Q)$; then x is also an element of $C_G(z)$. Since $C_G(z)$ is isomorphic to $C_p \wr S_m$, there is a surjective homomorphism $\varphi : C_G(z) \to S_m$ with kernel C_p^m, and this kernel has a set of generators $g_1, \dots, g_m$ such that the conjugation action of $C_G(z)$ permutes these generators with the permutation given by the map φ. Now $\varphi(x)$ is a nontrivial p-regular element of S_m that commutes with $\varphi(Q)$, a p-subgroup. Let $k \in \{1, \dots, m\}$ be a point that is not a fixed point of $\varphi(x)$ and let K be the orbit of k under $\varphi(Q)$. Assume that $\varphi(x)(k) \in K$; then there is an $s \in \varphi(Q)$ such that $s(k) = \varphi(x)(k)$. By induction we then find $s^n(k) = \varphi(x)^n(k)$ for all n, since s and $\varphi(x)$ commute. Since s is a p-element and $\varphi(x)$ is p-regular, this would imply that k is a fixed point of both elements, contrary to our assumption. Thus $\varphi(x)(k) \notin K$.

Now let $g = \prod_{i \in K} g_i$. This is a p-element contained in the normal subgroup C_p^m of $C_G(z)$, so it is contained in every Sylow p-subgroup of $C_G(z)$. In particular, g is an element of P; since it clearly centralizes Q, it is an element of Q. Then g commutes with x, but since $\varphi(x)(k) \notin K$, g^x cannot equal g. This is a contradiction.

The case $G = A_{pm}$ and $p > 2$ is immediate, since S_{pm} and A_{pm} have the same Sylow p-subgroups when $p > 2$. This leaves the case $G = A_{pm}$ and $p = 2$; here $C_G(Q)$ is a subgroup of $C_{S_{pm}}(Q)$ of index at most 2, so it is enough to show that $C_G(Q)$ is a p-group. We consider the cases m even and m odd separately. Suppose that m is even and let z be an element of cycle type 2^m; this is now an element of G. As before, we can assume $z \in Q$, so Q has no fixed points. $C_G(z)$ is now a subgroup of index 2 in $C_{S_{pm}}(z) \cong C_2 \wr S_m$, so again we have a map $\varphi : C_G(z) \to S_m$. As before, we assume that there is a nontrivial p-regular element x in $C_G(Q)$, we let $k \in \{1, \dots, m\}$ be a point that is not a fixed point of $\varphi(x)$, we let K be the orbit of k under $\varphi(Q)$, and by the same argument as before, we find $\varphi(x)(k) \notin K$.

We let $g_1, \dots, g_m$ be the set of transpositions generating $C_p^m \lhd C_{S_{pm}}(z)$, like before. Now if k is not a fixed point of Q, then $|K|$ is a power of 2, so $\prod_{i \in K} g_i$ is an even permutation. It is then an element of P that centralizes Q but not x, which is impossible since Q is centric in P. We can then assume that every point that is not a fixed point of $\varphi(x)$ is a fixed point of $\varphi(Q)$. Then Q centralizes g_i whenever i is not a fixed point of $\varphi(x)$, so $g_k g_{\varphi(x)(k)}$ is an even permutation centralizing Q. It lies in P by the same arguments as before, so it lies in Q; but it does not centralize x since the cycle in x involving k has length at least 3. Again we have a contradiction.

There remains the case that m is odd. In this case we let z be an element of cycle type $1^2 2^{m-1}$, and we let z' be the transposition interchanging the two fixed points of z. As in the previous cases, comparing orders shows that a Sylow p-subgroup of $C_G(z)$ is also a Sylow p-subgroup of G. By the same arguments as before, Q must contain z, so it has at most two fixed points, namely the points interchanged by z'. Now $C_{S_{pm}}(z)$ is isomorphic to $\langle z' \rangle \times (C_2 \wr S_{m-1})$, and $C_G(z)$ has index 2 in $C_{S_{pm}}(z)$, so it is normal in this group. Since $C_G(z)$ does not contain z', $C_{S_{pm}}(z)$ is also isomorphic to $\langle z \rangle \times C_G(z)$; dividing out $\langle z \rangle$, we see that $C_G(z)$ is isomorphic to $C_2 \wr S_{m-1}$. We can then follow the argument for the case $G = S_{p(m-1)}$ to get the result. $\square$

THEOREM 4.14. *Let $G = S_n$ or $G = A_n$ and let b be a block of G. There exists some $m \leq n$ such that the fusion system associated to b is isomorphic to the fusion system of S_m or A_m, respectively.*

PROOF. Consider first the case $G = S_n$. Let P be a defect group of b and let N be its set of fixed points, let M be the complement of N in $\{1, \dots, \}$, let $\mathcal{F}$ be the fusion system on P associated to b, and let Q be a centric subgroup of P. Then by Lemma 4.13, $C_G(Q)$ has the form $R \times S_N$ where R is a p-group. By Theorem 3.3, every block idempotent of $C_G(Q)$ is then contained in S_N, so the map $\varphi : kC_G(Q) \to kS_N$ induced by the projection onto S_N is bijective on blocks. Then we may identify the Brauer pairs at Q with the blocks of S_N. Additionally, the map $\varphi \circ \mathrm{Br}_Q : Z(kG) \to Z(kS_N)$ is surjective by Lemma 4.6. It follows that there is a unique Brauer pair associated to b at each Q, so $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_G(Q)$. By Lemma 4.9 we have $\mathrm{Aut}_G(Q) = \mathrm{Aut}_{S_M}(Q)$, so Corollary 2.8 implies that $\mathcal{F} = \mathcal{F}_P(S_M)$.

Now consider the case $G = A_n$ and $p > 2$. Keeping the same notation, we have $C_{S_n}(Q) = R \times S_N$, where R is a p-group. Since $p > 2$, R is contained in A_n, so we find $C_G(Q) = R \times A_N$. We again have a projection map $\varphi : kC_G(Q) \to kA_N$, but the map $\varphi \circ \mathrm{Br}_Q : Z(kG) \to Z(A_N)$ is no longer surjective (except in the case where P is the trivial group). By Lemma 4 and Lemma 4.8, the image of the map instead consists of those elements x of $Z(A_N)$ that satisfy $x^\sigma = x$ where σ is any odd element of S_N. Then for any primitive idempotent e of $Z(A_N)$, either e lies in the image of $\varphi \circ \mathrm{Br}_Q$ or $e \neq e^\sigma$ and $e + e^\sigma$ lies in the image. It follows that there are either one or two Brauer pairs at Q associated to b, and this number is independent of Q since the map $\varphi \circ \mathrm{Br}_Q$ is the same for all Q. In the case of two Brauer pairs, we also see that they are interchanged by σ.

Now let $g \in N_G(Q)$. Since N is the set of fixed points of Q, we can write $g = g_1 g_2$ with $g_1 \in S_M$ and $g_2 \in S_N$. Then g_1 and g_2 are either both even or both odd. Now in the case of two Brauer pairs at each Q, the g that fix each Brauer pair are those for which g_2 is even. Then g_1 must also be even, so we find $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{A_M}(Q)$ and so $\mathcal{F} = \mathcal{F}_P(A_M)$. When there is one Brauer pair at each Q and $|N| < 2$, we also find $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{A_M}(Q)$ and $\mathcal{F} = \mathcal{F}_P(A_M)$, since g_2 is always trivial in this case. This leaves the case of one Brauer pair at each Q and $|N| \geq 2$; here we get $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_M}(Q)$ and so $\mathcal{F} = \mathcal{F}_P(S_M)$. But we can now choose a set M' containing M and two additional points; since $p > 2$, P is also a Sylow p-subgroup of $A_{M'}$. We have $\mathrm{Aut}_{S_M}(Q) = \mathrm{Aut}_{A_{M'}}(Q)$ for all Q since for any $g \in S_M$, either g or gt lies in $A_{M'}$ where t is the transposition interchanging the two elements of $M' \setminus M$. We then get $\mathcal{F} = \mathcal{F}_P(A_{M'})$.

This leaves the case $G = A_n$ and $p = 2$. Fix a Q, and let N be its set of fixed points and M the complement of N in $\{1, \dots, n\}$. We then have $C_{S_n}(Q) = R \times S_N$ where R is a p-subgroup of S_M. Now if R is contained in A_M, then $C_G(Q)$ is just $R \times A_N$. Then we again find that there are one or two Brauer pairs at Q associated to b, and if there are two, they are interchanged by any odd permutation in S_N. As before, this implies that $\mathrm{Aut}_{\mathcal{F}}(Q)$ is $\mathrm{Aut}_{S_M}(Q)$ if there is a single Brauer pair and $\mathrm{Aut}_{A_M}(Q)$ if there are two.

If R is not contained in A_M, $C_G(Q)$ consists of $(R \cap A_M) \times A_N$ together with the products of any odd permutation in R and any odd permutation in S_N. Now the block idempotents of $kC_G(Q)$ are still found inside kA_N, since A_N contains all p-regular elements of $C_G(Q)$. Let σ be any odd permutation in S_N; then we actually have $e^\sigma = e$ for any block e of $kC_G(Q)$, since there exists an element $g \in C_G(Q)$ such that $x^g = x^\sigma$ for all $x \in A_M$. Then there is a unique Brauer pair at Q associated to b, so we have $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_M}(Q)$. But since $R = C_{S_M}(Q)$ contains an odd permutation, any element in $\mathrm{Aut}_{S_M}(Q)$ can be given as conjugation by an even permutation, so we actually have $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_M}(Q) = \mathrm{Aut}_{A_M}(Q)$.

Now let N be the set of fixed points of P, M its complement, and write $|M| = 2m$. In the case where m is even, all centric subgroups of P have N as their set of fixed points by Lemma 4.13, so we get $\mathcal{F} = \mathcal{F}_P(S_M)$ or $\mathcal{F} = \mathcal{F}_P(A_M)$ as in the case $p > 2$. If $\mathcal{F} = \mathcal{F}_P(A_M)$ we are done, so suppose that $\mathcal{F} = \mathcal{F}_P(S_M)$. Since $\mathcal{F}$ is saturated, $\mathrm{Aut}_{\mathcal{F}}(P) = \mathrm{Aut}_{S_M}(P)$ has $\mathrm{Aut}_P(P)$ as a Sylow p-subgroup. Let T be a Sylow p-subgroup of S_M containing P; then $\mathrm{Aut}_T(P)$ is obviously also a Sylow p-subgroup of $\mathrm{Aut}_{S_M}(P)$. Then $\mathrm{Aut}_T(P) = \mathrm{Aut}_P(P)$, so there exists an odd permutation in T that centralizes P. This implies that every morphism in $\mathcal{F}_P(S_M)$ can be given as conjugation by an even permutation, so $\mathcal{F} = \mathcal{F}_P(S_M) = \mathcal{F}_P(A_M)$.

Consider now the case where m is odd. For those centric subgroups Q of P that have N as their set of fixed points, we follow the same arguments as in the case $p > 2$ to conclude that $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{A_M}(Q)$ or $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_M}(Q)$, the same case for all Q. As with the case m even, we exclude the possibility $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_M}(Q)$ by considering the Sylow p-subgroups of $\mathrm{Aut}_{\mathcal{F}}(P)$. We then have $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{A_M}(Q)$ for all these groups.

Now define $K \subset M$ to consist of the two points that are fixed points of some centric subgroup Q of P. Then for any $x \in P$, Q^x is a centric subgroup of P with K^x as fixed points, so we must have $K^x = K$. Then K is an orbit under P, and there is a normal subgroup P_K of index 2 in P consisting of those elements in P that do not interchange the two points in K. Writing $M' = M \setminus K$, it is clear that P_K is a subgroup of $A_{M'}$.

Now if Q fixes the two points in K, $C_{S_n}(Q)$ has the form $R \times S_{K \cup N}$ with R a p-group. By the same considerations as before, there is either one or two Brauer pairs at Q associated to b, the same number for all Q. Suppose there are two Brauer pairs. Picking an $x \in P \setminus P_K$, we see that $P_K^x = P_K$ since $P_K \trianglelefteq P$, and x interchanges the two Brauer pairs at Q, since it acts as a transposition on $S_{K \cap N}$. However, x fixes all Brauer pairs at P, since it is an element of P, so there would then be two Brauer pairs at P_K that are contained in the same Brauer pair at P. This is impossible, so there must be one Brauer pair at each Q. Then $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{S_{M'}}(Q) = \mathrm{Aut}_{S_M}(Q) = \mathrm{Aut}_{A_M}(Q)$, where the last equality follows from the fact that S_M contains an odd permutation centralizing Q, namely the transposition interchanging the two elements of K. We then have $\mathrm{Aut}_{\mathcal{F}}(Q) = \mathrm{Aut}_{A_M}(Q)$ for any centric subgroup Q of P, and so $\mathcal{F} = \mathcal{F}_P(A_M)$. □

Bibliography

1. J. L. Alperin, *Sylow intersections and fusion*, J. Algebra **6** (1967), 222–241. MR 0215913 (35 #6748)
2. Michael Aschbacher, Radha Kessar, and Bob Oliver, *Fusion systems in algebra and topology*, London Mathematical Society Lecture Note Series, vol. 391, Cambridge University Press, Cambridge, 2011. MR 2848834 (2012m:20015)
3. Carles Broto, Ran Levi, and Bob Oliver, *The theory of p-local groups: a survey*, Homotopy theory: relations with algebraic geometry, group cohomology, and algebraic K-theory, Contemp. Math., vol. 346, Amer. Math. Soc., Providence, RI, 2004, pp. 51–84. MR 2066496 (2005h:20040)
4. Daniel Gorenstein, *Finite groups*, second ed., Chelsea Publishing Co., New York, 1980. MR 569209 (81b:20002)
5. Radha Kessar, *Introducton to block theory*, Group representation theory, EPFL Press, Lausanne, 2007, pp. 47–77. MR 2336637 (2008f:20020)
6. Burkhard Külshammer, *Group-theoretical descriptions of ring-theoretical invariants of group algebras*, Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991), Progr. Math., vol. 95, Birkhäuser, Basel, 1991, pp. 425–442. MR 1112173 (92d:16037)
7. Ran Levi and Bob Oliver, *Construction of 2-local finite groups of a type studied by Solomon and Benson*, Geom. Topol. **6** (2002), 917–990. MR 1943386 (2003k:55016)
8. ———, *Correction to: "Construction of 2-local finite groups of a type studied by Solomon and Benson" [Geom. Topol.* **6** *(2002), 917–990 (electronic); mr1943386]*, Geom. Topol. **9** (2005), 2395–2415. MR 2209376 (2006j:55018)
9. Lluís Puig, *Frobenius categories versus Brauer blocks*, Progress in Mathematics, vol. 274, Birkhäuser Verlag, Basel, 2009, The Grothendieck group of the Frobenius category of a Brauer block. MR 2502803 (2010j:20015)
10. Jacques Thévenaz, *G-algebras and modular representation theory*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995, Oxford Science Publications. MR 1365077 (96j:20017)