

Bismash Products and Group Algebras



Barbara Ilse Mahler

Hertford College

University of Oxford

A dissertation submitted for the degree of

Master of Science in Mathematics

and the Foundations of Computer Science

September 2, 2013

Abstract

We give a fully detailed and expanded version of the proof given in [5] that the bismash product arising from the standard factorization of the symmetric group on $p + 1$ letters, where p is a prime greater than 3, does not have the structure of a group algebra. We also obtain the same conclusion for several other bismash products constructed from small groups, namely A_5 , S_5 and $GL(3, 2)$. The methods used involve results from group theory, the representation theory of algebras, and the theory of blocks of finite groups.

Contents

1	Introduction	1
2	Preliminaries	3
2.1	Algebras and modules	3
2.2	Characters	8
3	Group factorizations and the bismash product	13
3.1	Group factorizations	13
3.2	The bismash product	14
3.2.1	The action of K on L	14
3.2.2	The bismash product constructed from KL	15
3.3	The modules of the bismash product and its semisimplicity	16
3.3.1	The modules of the bismash product	16
3.3.2	The semisimplicity of the bismash product	18
4	Blocks of characters of groups of order pm where $(p, m) = 1$	25
5	The case A_5	28
6	Symmetric groups and the corresponding bismash products	31
7	The case S_{p+1}	33
7.1	Preparatory results	33
7.2	Proof of Theorem 7.1	36
7.3	The case S_4	40
8	The case S_5	42
9	The case $GL(3, 2)$	47

10 Conclusion and further results	49
Bibliography	51

Chapter 1

Introduction

In [12] A. Masuoka considers a family of finite-dimensional complex algebras which are constructed as so-called bismash products from factorizations of groups. The case where the underlying group is a symmetric group has been studied by S. Montgomery et al in [14] and [13] and M. Collins in [5] and [6]. In particular, they investigate whether these algebras have the structure of group algebras. In [5] M. Collins proves that the bismash product H_n arising from the factorization of the symmetric group S_n as the product of S_{n-1} and an n -cycle is not isomorphic to a group algebra in the case where $n = p + 1$ ($p \geq 5$ a prime). In this work we give a fully detailed and expanded version of this proof. Additionally, we study the same question for several other bismash products constructed from small groups, namely A_5 , S_5 and $GL(3, 2)$.

It turns out that a bismash product over $\mathbb{C}$ is always semisimple and that the dimensions of its simple modules can be determined from its construction. By Wedderburn's Theorem, the question whether, for a given bismash product H , there exists a group G for which H is isomorphic to $\mathbb{C}G$ is thus equivalent to the question whether there exists a group whose character degrees are the same as the dimensions of the simple modules of H .

In Chapter 2 we collect various necessary results from representation theory which will be needed in the following chapters.

Chapter 3 introduces the bismash product and its basic properties such as semisimplicity. The simple modules of a bismash product are explicitly constructed; their dimensions are computed for symmetric groups in Chapter 6.

Chapter 4 presents basic results of Brauer from the theory of p -blocks of groups of order divisible by a prime p to the first power only.

The remaining chapters are devoted to investigating whether the bismash products arising from various groups have the structure of group algebras. This is resolved in the negative for A_5 in Chapter 5, for the symmetric groups S_{p+1} ($p \geq 5$ a prime) in Chapter 7, for S_5 in Chapter 8 and for $GL(3, 2)$ in Chapter 9.

Chapter 2

Preliminaries

In this chapter we present some basic definitions and results from representation theory, which will be needed as a background in the following chapters. No proofs will be given, but all the material except the results 2.22 to 2.25 is covered in either [8] or [16].

2.1 Algebras and modules

An algebra is both a vector space and a ring. It can be seen as a vector space with the additional structure of a bilinear, associative and unital multiplication or as a ring together with a scalar multiplication which commutes with the ring multiplication. Formally, we have the following definition.

Definition 1. For a field k , a k -algebra A is a k -vector space equipped with a multiplication map

$$\begin{aligned} A \times A &\rightarrow A \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

that is bilinear, associative and unital with multiplicative identity 1_A .

In the following we will assume that all our vector spaces, in particular algebras, are finite-dimensional.

It follows from bilinearity that the multiplication of any two elements in the algebra is determined by the multiplication of the basis elements for any given basis. That is, if the algebra A has a basis $\{v_1, \dots, v_n\}$, then for two arbitrary elements $a, b \in A$

with $a = \sum_i a_i v_i$ and $b = \sum_j b_j v_j$, we have

$$ab = \left(\sum_{i=1}^n a_i v_i \right) \left(\sum_{j=1}^n b_j v_j \right) = \sum_{i,j=1}^n a_i b_j (v_i v_j).$$

The coefficients of the products $v_i v_j$ are called the *structure constants* of A .

For a given field k , there is only one k -vector space for each finite dimension up to isomorphism and hence a finite-dimensional k -algebra is determined by its dimension and its structure constants.

There is a family of algebras arising from groups, which occurs frequently, the so-called group algebras.

Definition 2. Let G be a finite group and k be a field. The *group algebra* kG is the algebra which has as underlying vector space the $|G|$ -dimensional k -vector space with a basis $\{v_{g_1}, \dots, v_{g_n}\}$ labeled by the elements of G and whose multiplication is determined by the binary operation of the group, that is

$$v_{g_1} v_{g_2} = v_{g_1 g_2}.$$

It is clear that this does indeed define an algebra since the binary operation of a group is associative, and that the multiplicative identity of kG is v_e , where e is the identity element in G . We normally denote a basis vector v_g by its corresponding group element g and view G as being embedded in kG .

As with most algebraic objects, we have the notion of homomorphism.

Definition 3. A map between two k -algebras is a *k -algebra homomorphism* if it is k -linear, respects multiplication and sends the multiplicative identity of one algebra to the multiplicative identity of the other algebra. A *k -algebra isomorphism* is an invertible k -algebra homomorphism.

Let k be a field and V be a k -vector space. Consider the set $\text{Hom}(V, V)$ of linear transformations of V . It is clear that this is an algebra with the addition coming from the addition in V and the multiplication being the composition of functions.

For an algebra A , an A -module is a vector space V together with an action of A on V by linear transformations. Formally, we have the following definition.

Definition 4. Let A be an algebra over a field k . An *A -module* is a k -vector space V together with a k -algebra homomorphism from A to the algebra $\text{Hom}(V, V)$.

Again, we have the notion of homomorphism.

Definition 5. Let A be an algebra. A map f between two A -modules V and W is an *A -module homomorphism* if it is a linear map and commutes with the action of A , that is, for any $a \in A$ and $v \in V$, we have

$$f(a \cdot v) = a \cdot f(v).$$

The set of A -module homomorphisms between V and W is denoted by $\text{Hom}_A(V, W)$. An *A -module isomorphism* is a bijective A -module homomorphism.

The definition of a direct sum of vector spaces generalizes to algebras.

Definition 6. If A and B are algebras, then the *direct sum* $A \oplus B$ is the algebra with underlying vector space consisting of pairs (a, b) ($a \in A, b \in B$) and componentwise addition $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and multiplication $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$.

We can also form the direct sum of two A -modules by taking the direct sum of vector spaces and letting A act componentwise.

Definition 7. If A is an algebra and V and W are A -modules, then the *direct sum* of V and W is the vector space $V \oplus W$ with A acting componentwise, that is, for $a \in A$ and $(v, w) \in V \oplus W$, we have $a \cdot (v, w) = (a \cdot v, a \cdot w)$.

There is a relationship between the direct sum of algebras and the direct sum of modules. Let $A \oplus B$ be the direct sum of two algebras A and B . If M is an A -module, then we can view M as an $A \oplus B$ -module by letting the B -component of $A \oplus B$ act trivially, that is, for $(a, b) \in A \oplus B$ and $m \in M$,

$$(a, b) \cdot m = a \cdot m.$$

Similarly, every B -module N can be viewed as an $A \oplus B$ -module and we can form the direct sum $M \oplus N$ of $A \oplus B$ -modules. Then for any $(m, n) \in M \oplus N$ and $(a, b) \in A \oplus B$, we have

$$(a, b) \cdot (m, n) = (a \cdot m, b \cdot n).$$

It turns out that all $A \oplus B$ -modules are of this form.

Lemma 2.1. *Every $A \oplus B$ -module is isomorphic to $M \oplus N$ for some A -module M and some B -module N .*

Definition 8. A *submodule* of an A -module V is a subspace $W \subseteq V$ which is invariant under the action of A , that is, for any $a \in A$ and $w \in W$, we have $a \cdot w \in W$. A

module is *simple* if it is non-zero and has no non-trivial submodules.

Lemma 2.2. *If V is an A -module and $v \in V$, then $Av = \{a \cdot v : a \in A\}$ is a submodule of V .*

Lemma 2.3. *Let V be an A -module. Then V is simple if and only if for each $0 \neq v \in V$ we have that $Av = V$.*

The following lemma is called Schur's Lemma and concerns the homomorphisms between simple modules.

Lemma 2.4. (i) *Let A be an algebra over a field k and let V and W be simple A -modules. Any A -module homomorphism from V to W is either an isomorphism or the zero map.*

(ii) *Suppose that k is an algebraically closed field, A an algebra over k and V a simple A -module. Any endomorphism of V (homomorphism from V to V) is a scalar multiple of the identity map.*

Definition 9. A module is *semisimple* if it is isomorphic to a direct sum of simple modules.

In particular, this means that a simple module is semisimple, which explains the terminology.

Lemma 2.5. *If A is an algebra and M is a semisimple A -module, then the decomposition of M into simple A -modules is unique up to isomorphism.*

Definition 10. An algebra A is said to be *semisimple* if all A -modules are semisimple.

Definition 11. If A is an algebra, then A is itself an A -module with the action of A on itself being by left multiplication. This A -module is called the *regular module* of A .

It turns out that the regular module of an algebra determines whether or not the algebra is semisimple.

Lemma 2.6. *An algebra is semisimple if and only if its regular module is semisimple.*

Lemma 2.7. *If A is a semisimple algebra and S is a simple A -module, then S occurs in the decomposition of the regular A -module $\dim S$ times.*

The next two corollaries follow immediately from this lemma.

Corollary 2.8. *If A is a semisimple algebra, then there are only finitely many simple A -modules.*

Corollary 2.9. *If A is a semisimple algebra, then the squares of the dimensions of the simple A -modules add up to the dimension of A .*

Remark. Corollary 2.8 has a more general version. It is true for any finite-dimensional algebra A that there are only finitely many simple A -modules and they are all quotients of the regular A -module. This is a corollary of the so-called 'Jordan-Hölder Theorem'.

Corollary 2.9 on the other hand is special to semisimple algebras. In fact, we shall see in Section 3.3.2 that an algebra is semisimple if the squares of the dimensions of its simple modules add up to its own dimension.

Let k be a field and V be a k -vector space of dimension n . Consider the algebra $\text{Hom}(V, V)$. This has a natural module, namely V together with the action of $\text{Hom}(V, V)$ described by the identity homomorphism from $\text{Hom}(V, V)$ to itself. It turns out that there are no other $\text{Hom}(V, V)$ -modules than V and direct sums of copies of V .

Theorem 2.10. *Let M be any $\text{Hom}(V, V)$ -module. Then M is isomorphic to $V^{\oplus r}$, where $r = \dim(\text{Hom}_{\text{Hom}(V, V)}(V, M))$.*

Corollary 2.11. *The algebra $\text{Hom}(V, V)$ is semisimple.*

If we choose a basis of V , then we get a natural isomorphism from the algebra $\text{Hom}(V, V)$ of linear transformations of V to the algebra $M_n(k)$ of $n \times n$ -matrices over k .

The following special case of a theorem by Wedderburn classifies semisimple algebras over $\mathbb{C}$ as direct sums of matrix algebras.

Theorem 2.12. (Wedderburn) *Let A be a finite-dimensional algebra over $\mathbb{C}$. Then A is semisimple if and only if A is isomorphic to the direct sum of matrix algebras*

$$A \cong M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C}).$$

Hence, we know precisely the structure of a semisimple algebra. Moreover, since we know that a module of a direct sum of algebras is a direct sum of modules of the components and that the only modules of a matrix algebra are the natural modules and direct sums thereof, we also know what the simple modules of a semisimple algebra look like. In particular, we know that their dimensions are $n_1, n_2, \dots, n_k$. Furthermore, Wedderburn's Theorem implies that two semisimple $\mathbb{C}$ -algebras are isomorphic if and only if their sets of dimensions of simple modules are the same.

If $A = kG$ is a group algebra for some group G and some field k and V is an A -module, then we can restrict the action of A on V to group elements of G to obtain

something called a 'representation' of G . Formally, we have the following definition.

Definition 12. Let G be a group and k a field. A G -representation over k is a k -vector space V together with a group homomorphism from G to the group $GL(V)$. So a kG -module restricts to a G -representation and, conversely, a G -representation extends to a kG -module linearly. This means that representations of G and modules of kG are really the same thing. We remark that a representation of G corresponding to a simple kG -module is normally called *irreducible*.

The following theorem by Maschke specifies when a group algebra is semisimple.

Theorem 2.13. (Maschke) *Let G be a finite group and k be some field. The group algebra $A = kG$ is semisimple if and only if the characteristic of k does not divide the order of G .*

2.2 Characters

From now on we will assume that we are working over the algebraically closed field of complex numbers $\mathbb{C}$. This field has characteristic zero and hence, by Maschke's Theorem 2.13, every group algebra over $\mathbb{C}$ is semisimple.

We also assume that all groups considered are finite.

Definition 13. Let G be a group and let $\rho : G \rightarrow GL(V)$ be a representation of G . The *character* afforded by ρ is the map χ taking an element $g \in G$ to the trace of $\rho(g)$:

$$\chi(g) := \text{tr}(\rho(g)).$$

A character is called *irreducible* if the corresponding representation is irreducible. The *degree* of a character is the dimension of the corresponding representation. A character of degree one is called *linear*.

Remark. We note that the trace of a linear transformation is defined to be the trace of the matrix describing it in some given basis. Since for matrices M and N , we have that $\text{tr}(NMN^{-1}) = \text{tr}M$, this does not depend on the choice of basis. Also note that for the same reason isomorphic representations have identical characters.

So the set of characters of a group G forms a subset of the space $\mathbb{C}^G$ of functions from G to $\mathbb{C}$ and it is easy to see from the definition that the sum of two characters is the character corresponding to the direct sum of the representations affording these characters.

Furthermore, characters have the following properties.

Lemma 2.14. *Let G be a group and let ρ be a representation of G affording the character χ .*

(i) If g and h are conjugate elements in G , then

$$\chi(g) = \chi(h).$$

(ii) For any $g \in G$,

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

(iii) If e is the identity element in G and d is the degree of χ , then

$$\chi(e) = d.$$

(iv) For all $g \in G$,

$$|\chi(g)| \leq d$$

and $|\chi(g)| = d$ if and only if $\rho(g) = \lambda \mathbf{1}$ for some constant $\lambda \in \mathbb{C}$.

Property (i) means that the set of characters of a group G is a subset of the space of class functions from G to $\mathbb{C}$.

The following lemma is a corollary of Schur's Lemma 2.4.

Lemma 2.15. *A group is abelian if and only if all its irreducible characters are linear.*

The space of functions from G to $\mathbb{C}$ is equipped with a Hermitian inner product.

Definition 14. Let G be a group and $\xi, \zeta \in \mathbb{C}^G$. Then the *inner product* of ξ and ζ is defined to be

$$\langle \xi, \zeta \rangle_G = \frac{1}{|G|} \sum_{g \in G} \xi(g) \overline{\zeta(g)}.$$

Theorem 2.16. *Let V and W be representations of a group G and χ_V and χ_W be the corresponding characters. Then*

$$\langle \chi_W, \chi_V \rangle_G = \dim \operatorname{Hom}_{\mathbb{C}G}(V, W).$$

In particular, this theorem implies that the inner product of two characters is always a non-negative integer. Moreover, by Schur's Lemma 2.4 applied to the group algebra $\mathbb{C}G$, we have the following corollary.

Corollary 2.17. *Let $\chi_1 \cdots \chi_r$ be the irreducible characters of a group G . Then*

$$\langle \chi_i, \chi_j \rangle_G = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

That is, the irreducible characters of a group G form a set of orthonormal vectors in $\mathbb{C}^G$.

Lemma 2.18. *The number of irreducible characters of a finite group G equals the number of conjugacy classes of G .*

If G is a group with a normal subgroup N and $\tilde{\chi}$ is a character of the quotient group G/N , then we can form a character of G by composing $\tilde{\chi}$ with the natural projection of G onto G/N . This process is called 'lifting'.

Definition 15. Assume that $N \triangleleft G$ and let $\tilde{\chi}$ be a character of G/N . The *lift* of $\tilde{\chi}$ to G is the character χ of G defined by

$$\chi(g) = \tilde{\chi}(Ng).$$

We note that $\tilde{\chi}$ and χ have the same degree and χ is irreducible if and only if $\tilde{\chi}$ is irreducible.

Theorem 2.19. *Assume that $N \triangleleft G$. Associating each character of G/N with its lift to G gives a bijective correspondence between the set of characters of G/N and the set of characters of G whose kernel contains N . Irreducible characters of G/N correspond to irreducible characters of G .*

Lemma 2.20. *If χ is a linear character of a group G , then the commutator subgroup G' is contained in its kernel.*

Corollary 2.21. *The linear characters of a group G are exactly the lifts of the linear characters of its abelianization G/G' . In particular, the number of linear characters of a group G is $|G : G'|$.*

Let G be a group with a subgroup H . If χ is a character of G , then it is clear that we can obtain a character of H by restricting χ to H .

Definition 16. If χ is a character of a group G with a subgroup H , then the *restriction* of χ to H is the character $\chi|_H$ of H defined by

$$\chi|_H(h) = \chi(h).$$

We use a similar notation for the restriction of a module.

Definition 17. Let G be a group and $N \triangleleft G$. Let χ be a character of N and $g \in G$. Define $\chi^g : N \rightarrow \mathbb{C}$ by

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

Then this is a character of N called a G -conjugate of χ .

If N is a normal subgroup of G of index two, then the following special case of Clifford's Theorem gives information about the structure of the restriction of an irreducible character of G to N .

Proposition 2.22. (Proposition 20.9 of [11]) *Let G be a finite group and N be a normal subgroup of G of index 2. If χ is an irreducible character of G , then $\chi|_N$ is either irreducible or the sum of two distinct irreducible characters of the same degree.*

So if $H \leq G$, then restricting is a way of converting a $\mathbb{C}G$ -module into a $\mathbb{C}H$ -module. Conversely, if we have a $\mathbb{C}H$ -module V , then we can obtain a $\mathbb{C}G$ -module from V through a process called 'induction'.

The $\mathbb{C}G$ -module 'induced' from V can be defined as the tensor product of modules $\text{Ind}_H^G V = \mathbb{C}G \otimes_{\mathbb{C}H} V$.

In the case that V is a submodule of the regular $\mathbb{C}H$ -module (for example when V is simple) there is a more concrete way of constructing the induced module $\text{Ind}_H^G V$. (See Chapter 21 of [11] for details on this.)

Definition 18. Assume that G is a group with a subgroup H and that $V \subseteq \mathbb{C}H$ is a submodule of the regular $\mathbb{C}H$ -module. The $\mathbb{C}G$ -module *induced* from V is the space

$$\text{Ind}_H^G V := \text{span}\{gv : g \in G, v \in V\}$$

viewed as a submodule of the regular $\mathbb{C}G$ -module.

The corresponding *induced character* is denoted by $\text{Ind}_H^G \chi$.

Lemma 2.23. *Let G be a group with a subgroup H and let V be a $\mathbb{C}H$ -module. Let $\{v_1, \dots, v_r\}$ be a basis of V and let $\{g_1, \dots, g_t\}$ be a set of representatives of the left cosets of H in G . Then the set*

$$\{g_i v_j : 1 \leq i \leq t, 1 \leq j \leq r\}$$

forms a basis of $\text{Ind}_H^G V$.

In particular, the dimension of the module induced from V is

$$\dim \operatorname{Ind}_H^G V = |G : H| \cdot \dim V.$$

Corollary 2.24. *Let G be a group with a subgroup H and let V be a $\mathbb{C}H$ -module. Let $\{v_1, \dots, v_r\}$ be a basis of V and let $\{g_1, \dots, g_t\}$ be a set of representatives of the left cosets of H in G . Then, as vector spaces,*

$$\operatorname{Ind}_H^G V \cong \bigoplus_{i=1}^t g_i V,$$

that is, $\operatorname{Ind}_H^G V$ is the direct sum of $|G : H| = t$ copies of V .

Remark. This decomposition of $\operatorname{Ind}_H^G V$ into copies of V does not depend on the choice of coset representatives since, if $g_i h$ is any other representative of the coset $g_i H$, then $g_i h V = g_i V$.

Furthermore, we notice that if $g \in G$, then for each $1 \leq i \leq t$ we have $g g_i = g_j h_i$ for some $1 \leq j \leq t$ and $h_i \in H$. So if $g_i v \in g_i V$, then $g \cdot g_i v = g_j h_i v \in g_j V$ and we see that g permutes the copies of V while acting on each copy $g_i V$ by h_i .

The following theorem relates the inner product of two characters of G to the inner product of the corresponding characters of H .

Theorem 2.25. (Frobenius Reciprocity) (Theorem 21.16 of [11]) *Assume that $H \leq G$. Let χ be a character of G and ϕ be a character of H . Then*

$$\langle \operatorname{Ind}_H^G \phi, \chi \rangle_G = \langle \phi, \chi|_H \rangle_H.$$

Chapter 3

Group factorizations and the bismash product

3.1 Group factorizations

Let G be a finite group and $K, L \leq G$ be subgroups. The set

$$KL = \{kl : k \in K, l \in L\}$$

is a subgroup of G if and only if $KL = LK$. If, moreover, $K \cap L = \{e\}$ and $KL = G$, then we call KL a *factorization* of G . Since $|KL| = |K||L|/|K \cap L|$, this is equivalent to the condition that $K \cap L = \{e\}$ and $|K||L| = |G|$.

The following are examples of group factorizations.

(1) Let $G = S_n$ be the symmetric group on n letters, and take the subgroups $K = \text{Stab}_G(n) \cong S_{n-1}$, where we consider the natural action of G on $\{1, \dots, n\}$, and $L = \langle \pi \rangle \cong C_n$, where $\pi = (1 \ 2 \ 3 \ \dots \ n)$ is an n -cycle. Every non-identity element in L acts non-trivially on n . Thus we have $K \cap L = \{e\}$ and, since $|K||L| = (n-1)!n = n! = |G|$, we have that KL is a factorization of G .

This factorization can be considered to be the standard factorization of a symmetric group.

(2) Let $G = A_n$ be the alternating group on n letters for $n \geq 5$ odd. Take the subgroups $K = \text{Stab}_G(n) \cong A_{n-1}$ and $L = \langle \pi \rangle \cong C_n$, where $\pi = (1 \ 2 \ 3 \ \dots \ n)$ is an n -cycle. Notice that $\pi \in A_n$ since n is odd. As in the previous example we have $K \cap L = \{e\}$ and $|K||L| = \frac{1}{2}(n-1)!n = \frac{1}{2}n! = |G|$, and so KL is a factorization of G .

(3) Let $G := KL \leq S_5$ where $K = \langle \tau \rangle \cong C_4$ and $L = \langle \pi \rangle \cong C_5$ with $\tau := (2\ 3\ 5\ 4)$ and $\pi := (1\ 2\ 3\ 4\ 5)$. Note that $\tau^{-1}\pi\tau = \pi^2$, that is $\pi\tau = \tau\pi^2$ and we can move powers of τ from one side of powers of π to the other, which implies that $KL = LK$. Now, since the non-identity elements in K have orders 4 or 2 and the non-identity elements in L have order 5, we also have $K \cap L = \{e\}$ and thus KL is a factorization of the group $G \leq S_5$ of order $|K||L| = 4 \cdot 5 = 20$.

(4) Let $G = A_4$ and take the subgroups $K = V_4 \cong C_2 \times C_2$, the group consisting of the identity element and all three double transpositions, and $L = \langle (1\ 2\ 3) \rangle \cong C_3$. It is clear that $K \cap L = \{e\}$ and $|K||L| = 4 \cdot 3 = 12 = |G|$ so that KL is indeed a factorization of G . Since conjugate permutations have the same cycle shape, K contains full conjugacy classes, i. e. is normal in G , and it follows that in this case G is actually isomorphic to the semidirect product $K \rtimes_\alpha L$ where α is the action of L on K by conjugation.

3.2 The bismash product

Let G be a group with a factorization $G = KL$. Based on this factorization we are going to construct an algebra called the 'bismash product'. We remark that, even though $KL = LK = G$, the bismash product corresponding to KL may be different from the bismash product corresponding to LK .

3.2.1 The action of K on L

Consider the right cosets of K in G . Since $G = KL$, it is clear that every coset of K has a representative in L . Moreover, if $Kl_1 = Kl_2$ for some $l_1, l_2 \in L$, then $l_1l_2^{-1} \in K \cap L = \{e\}$, that is, $l_1 = l_2$. It follows that $G = \bigcup_{l \in L} Kl$ is a disjoint union and we can take L as a set of coset representatives. We can translate the right action of K on its right cosets by right multiplication into a right action of K on L thus. For $k \in K$ and $l \in L$, let

$$l^k := \bar{l} \text{ where } lk \in K\bar{l}.$$

The bismash product is an algebra with a tensor product as underlying vector space and a multiplication involving this action of K on L .

3.2.2 The bismash product constructed from KL

Let $\mathbb{C}^L$ be the $|L|$ -dimensional $\mathbb{C}$ -vector space of functions from L to $\mathbb{C}$ which has a natural basis indexed and denoted by the elements of L and $\mathbb{C}K$ be the group algebra on K . The bismash product arising from KL is an algebra H which has as underlying vector space the tensor product $\mathbb{C}^L \otimes \mathbb{C}K$. Notice that this space has dimension $|K||L| = |G|$ since the natural basis is $\{l \otimes k : l \in L, k \in K\}$. It is common practice to write

$$H := \mathbb{C}^L \# \mathbb{C}K$$

instead of $\mathbb{C}^L \otimes \mathbb{C}K$ and $l \# k := l \otimes k$ for an element of the natural basis to emphasize that we are defining an algebra that is different from the usual tensor product of algebras. The multiplication can then be defined on the natural basis and extended bilinearly as observed in the introduction. We define the product of two basis elements to be either a basis element or zero:

$$(l \# k)(\bar{l} \# \bar{k}) := \begin{cases} l \# k \bar{k} & \text{if } lk \in K\bar{l} \\ 0 & \text{otherwise.} \end{cases} \quad (3.1)$$

We note that the vectors of the form $l \# e$ are orthogonal idempotents:

$$(l_1 \# e)(l_2 \# e) = \begin{cases} l_1 \# e & \text{if } l_1 = l_2 \\ 0 & \text{if } l_1 \neq l_2. \end{cases}$$

The vector $\sum_{l \in L} (l \# e)$ functions as a multiplicative identity. Indeed, we have $le \in K\bar{l}$ if and only if $l = \bar{l}$ so that

$$\left(\sum_{l \in L} (l \# e) \right) (\bar{l} \# \bar{k}) = \sum_{l \in L} ((l \# e)(\bar{l} \# \bar{k})) = (\bar{l} \# e)(\bar{l} \# \bar{k}) = \bar{l} \# \bar{k},$$

and $\bar{l}k \in Kl'$ for exactly one $l' \in L$ so that

$$(\bar{l} \# \bar{k}) \left(\sum_{l \in L} (l \# e) \right) = \sum_{l \in L} ((\bar{l} \# \bar{k})(l \# e)) = (\bar{l} \# \bar{k})(l' \# e) = \bar{l} \# \bar{k}.$$

To ensure that (3.1) really does define a valid associative multiplication on H , we

have to check that it is associative on the basis elements. Indeed,

$$(l\#k)[(l_1\#k_1)(l_2\#k_2)] = \begin{cases} l\#kk_1k_2 & \text{if } l_1k_1 \in Kl_2 \text{ and } lk \in Kl_1 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$[(l\#k)(l_1\#k_1)](l_2\#k_2) = \begin{cases} l\#kk_1k_2 & \text{if } lkk_1 \in Kl_2 \text{ and } lk \in Kl_1 \\ 0 & \text{otherwise,} \end{cases}$$

and the two conditions for the products to be non-zero above are equivalent:

First assume that $l_1k_1 \in Kl_2$ (i.e. $l_1k_1 = \tilde{k}l_2$ for some $\tilde{k} \in K$) and $lk \in Kl_1$ (i.e. $lk = \bar{k}l_1$ for some $\bar{k} \in K$). Then $lkk_1 = \bar{k}l_1k_1 = \bar{k}\tilde{k}l_2 \in Kl_2$, so $lkk_1 \in Kl_2$ (and $lk \in Kl_1$).

Conversely, assume that $lkk_1 \in Kl_2$ (i.e. $lkk_1 = \tilde{k}l_2$ for some $\tilde{k} \in K$) and $lk \in Kl_1$ (i. e. $lk = \bar{k}l_1$ and $\bar{k}^{-1}lk = l_1$ for some $\bar{k} \in K$). Then $l_1k_1 = \bar{k}^{-1}lkk_1 = \bar{k}^{-1}\tilde{k}l_2 \in Kl_2$ (and $lk \in Kl_1$).

3.3 The modules of the bismash product and its semisimplicity

It turns out that the bismash product H is a semisimple algebra. We proceed as follows to prove this and simultaneously find the dimensions of the irreducible modules of H . First, we explicitly construct some H -modules from the irreducible representations of the stabilizers of the action of K on L . Then we show that these modules are simple and pairwise non-isomorphic. Finally, by adding up the squares of their dimensions, we deduce that H is semisimple and that these modules form in fact the complete set of irreducible H -modules.

3.3.1 The modules of the bismash product

The H -modules that we are about to construct are based on the $\mathbb{C}K$ -modules that are induced from the irreducible modules of the stabilizers of the action of K on L .

Let K be one of the factors of our group factorization $G = KL$ and K_l be the stabilizer of some element $l \in L$ for the action of K on L as defined in Section 3.2.1. That is

$$K_l = \{k \in K : Klk = Kl\} = \{k \in K : lkl^{-1} \in K\} = K \cap (l^{-1}Kl).$$

We take some irreducible module V of $\mathbb{C}K_l$ and define an H -module $\tilde{V}$ thus. The underlying vector space of $\tilde{V}$ is the underlying vector space of the induced module $\text{Ind}_{K_l}^K V$ and the action of H on $\tilde{V}$ is based on the action of $\mathbb{C}K$ on $\text{Ind}_{K_l}^K V$ as follows. Let $\{g_1, \dots, g_t\}$ be a set of representatives of the left cosets of K_l in K . We have seen that $\text{Ind}_{K_l}^K V$ splits as the direct sum of vector spaces $\bigoplus_{i=1}^t g_i V$. For a basis element $l_1 \# k$ of H and $g_i v \in g_i V$ we define the action of $l_1 \# k$ on $g_i v$ to be

$$(l_1 \# k) \cdot (g_i v) := \begin{cases} kg_i v & \text{if } l_1 k g_i \in Kl \\ 0 & \text{otherwise} \end{cases} \quad (3.2)$$

and extend bilinearly.

We notice that the condition for this action to be non-zero does not depend on the choice of coset representatives $\{g_1, \dots, g_t\}$ because $l_1 k g_i \in Kl$ is equivalent to $l_1^{kg_i} = l$ and for another representative $g_i s \in g_i K_l$ we have

$$l_1^{kg_i s} = \left(l_1^{kg_i}\right)^s = l \text{ if and only if } l_1^{kg_i} = l$$

since s is in the stabilizer K_l of l .

To ensure that (3.2) does indeed define an action of H on $\tilde{V}$ we have to check that the identity $\sum_{l \in L} (l \# e)$ of H acts trivially on $\tilde{V}$ and that, for two elements $x, y \in H$ and a vector $w \in \tilde{V}$, we have $(xy) \cdot w = x \cdot (y \cdot w)$.

The former is easy to check since, for $g_i v \in g_i V$, we have

$$\left(\sum_{\bar{l} \in L} (\bar{l} \# e)\right) \cdot (g_i v) = \sum_{\bar{l} \in L} ((\bar{l} \# e) \cdot (g_i v)) = (l' \# e) \cdot (g_i v) = g_i v,$$

where l' is the unique element in L that g_i sends to l under the action defined in Section 3.2.1.

To check the latter we have to show that for two basis elements $l_1 \# k_1$ and $l_2 \# k_2$ of H and a vector $g_i v \in g_i V$ we have

$$((l_1 \# k_1)(l_2 \# k_2)) \cdot (g_i v) = (l_1 \# k_1) \cdot ((l_2 \# k_2) \cdot (g_i v)).$$

By the definition of the multiplication in H (3.1) and the definition of the action of H on $\tilde{V}$ (3.2), both sides are either $k_1 k_2 g_i v$ or zero and checking that they are equal amounts to checking that the conditions for them being non-zero are equivalent, which is straightforward.

Now, for each orbit of the action of K on L we pick a representative $l \in L$ and carry out the above construction for each irreducible module of the stabilizer K_l . We thus obtain a number of H -modules which we shall see are all irreducible and, in fact, form a complete set of irreducible H -modules.

We notice that the definition of these H -modules does not depend on the choice of representative for each orbit, since the stabilizers of elements in the same orbit are conjugate and therefore are isomorphic and embedded in K in the same way.

Finally, the actual form of the irreducible H -modules will not be of interest in our investigation of whether or not H is isomorphic to a group algebra. The important information that we take away from the above construction of irreducible H -modules is that they have dimensions

$$\dim \tilde{V} = |K : K_l| \cdot n$$

for the stabilizers K_l of the action of K on L and their irreducible character degrees n .

The action of K on L always has the trivial orbit $\{e\}$ with corresponding stabilizer $K_e = K$. So the most convenient case occurs when there is exactly one non-trivial orbit of size $|L| - 1$.

In this case the dimensions of the irreducible H -modules are the character degrees of K together with $|L| - 1$ times the character degrees of the stabilizer of a non-identity element in L .

3.3.2 The semisimplicity of the bismash product

Theorem 3.1. *Let $l \in L$ and K_l be the stabilizer of l under the action of K on L defined in Section 3.2.1. If V is an irreducible module for $\mathbb{C}K_l$, then $\tilde{V}$ as defined in Section 3.3.1 is an irreducible module for H .*

Proof. We use Lemma 2.3 to prove this theorem.

Let $0 \neq x \in \tilde{V}$. We have to show that the H -submodule Hx of $\tilde{V}$ generated by x is the whole of $\tilde{V}$.

We know that $\tilde{V}$ is the direct sum of vector spaces $\bigoplus_{i=1}^t g_i V$, where $\{g_1, \dots, g_t\}$ is a set of representatives of the left cosets of K_l in K . Hence, we can write x as a sum

$$x = \sum_{i=1}^t g_i w_i,$$

where $w_i \in V$ for $1 \leq i \leq t$ and $w_j \neq 0$ for some $1 \leq j \leq t$ since x is non-zero.

Claim 1. We have $g_j w_j \in Hx$.

Indeed, as g_j permutes L under the action of K on L defined in Section 3.2.1, there exists a unique $l_1 \in L$ such that $l_1 g_j \in Kl$. Moreover, for any $r \neq j$ we have $l_1 g_r \notin Kl$ because otherwise $g_r^{-1} g_j \in K_l$ and this is a contradiction to the definition of the set $\{g_1, \dots, g_t\}$. It now follows from the definition of the action of H on $\tilde{V}$ given in (3.2) that

$$(l_1 \# e)x = g_j w_j$$

proving the claim.

Claim 2. For any $1 \leq i \leq t$ we have $g_i w_j \in Hx$.

Indeed, let $k_2 = g_i g_j^{-1}$. Then $k_2 g_j = g_i$ and, since $k_2 g_j$ permutes L under the action of K on L , there exists a unique l_2 such that $l_2 k_2 g_j \in Kl$. (Moreover, for any $r \neq j$ we have $l_2 k_2 g_r \notin Kl$ because otherwise $g_r^{-1} g_j \in K_l$ and this is a contradiction to the definition of the set $\{g_1, \dots, g_t\}$.) It now follows from the definition of the action of H on $\tilde{V}$ given in (3.2) that

$$(l_2 \# k_2)(g_j w_j) = k_2 g_j w_j = g_i w_j$$

and this lies in Hx as $g_j w_j$ does by the previous claim.

Claim 3. For any $1 \leq i \leq t$ we have $g_i V \subset Hx$.

Indeed, we first notice that since $w_j \in V$ is non-zero and V is an irreducible K_l -module, Lemma 2.3 implies that $\mathbb{C}K_l w_j = \text{span}\{k w_j : k \in K_l\} = V$. To prove the claim it is thus sufficient to show that for any $k \in K_l$ we have $g_i k w_j \in Hx$.

So let $k \in K_l$ and set $k_1 := g_i k g_i^{-1} \in K$. Then $k_1 g_i = g_i k$ and since $k_1 g_i$ permutes L under the action of K on L , there exists a unique $l_3 \in L$ such that $l_3 k_1 g_i \in Kl$. (Moreover, for any $r \neq i$ we have $l_3 k_1 g_r \notin Kl$ because otherwise $g_r^{-1} g_i \in K_l$ and this is a contradiction to the definition of the set $\{g_1, \dots, g_t\}$.) It now follows from the

definition of the action of H on $\tilde{V}$ given in (3.2) that

$$(l_3 \# k_1)(g_i w_j) = k_1 g_i w_j = g_i k w_j$$

and this lies in Hx as $g_i w_j$ does by the previous claim.

So we know that, for each $1 \leq i \leq t$, we have $g_i V \subset Hx$ and since $\tilde{V} = \bigoplus_{i=1}^t g_i V$ this means that $\tilde{V} \subseteq Hx$, completing the proof. □

Proposition 3.2. (a) *If V_1 and V_2 are non-isomorphic irreducible K_l -modules for some $l \in L$, then the corresponding H -modules $\tilde{V}_1$ and $\tilde{V}_2$ are not isomorphic.*

(b) *If V_1 is an irreducible K_e -module and V_2 is an irreducible K_l -module for some $l \neq e$, then the corresponding H -modules $\tilde{V}_1$ and $\tilde{V}_2$ are not isomorphic.*

Proof. (a) Let $l \in L$ and let V_1 and V_2 be two irreducible K_l -modules. Let $\{e = g_1, \dots, g_t\}$ be a set of representatives of the left cosets of K_l in K . Then both the action of H on $\tilde{V}_1$ and the action of H on $\tilde{V}_2$ can be described in terms of $e = g_1 \dots, g_t$: If $l_1 \in L$ and $k \in K$, then for $v \in V_1$ we have

$$(l_1 \# k)(g_i v) = \begin{cases} kg_i v & \text{if } l_1 k g_i \in Kl \\ 0 & \text{otherwise,} \end{cases}$$

and for $w \in V_2$ we have

$$(l_1 \# k)(g_i w) = \begin{cases} kg_i w & \text{if } l_1 k g_i \in Kl \\ 0 & \text{otherwise.} \end{cases}$$

We are going to show that if $\tilde{V}_1$ and $\tilde{V}_2$ are isomorphic, then so are V_1 and V_2 .

So suppose that $\tilde{V}_1$ and $\tilde{V}_2$ are isomorphic and let $\psi : \tilde{V}_1 \rightarrow \tilde{V}_2$ be an isomorphism. Note that as $\dim \tilde{V}_1 = |K : K_l| \cdot \dim V_1$ and $\dim \tilde{V}_2 = |K : K_l| \cdot \dim V_2$, this implies that $\dim V_1 = \dim V_2$.

We restrict ψ to the subspace $g_1 V_1 = e V_1 = V_1$ of $\tilde{V}_1$.

For $k \in K$ and $v \in V_1$ we have

$$(l \# k)(ev) = \begin{cases} kv & \text{if } lk \in Kl \\ 0 & \text{otherwise.} \end{cases}$$

Notice that the condition that $lk \in Kl$ is exactly that k is in the stabilizer K_l and then $kv = ekv \in V_1$. It follows that the subspace V_1 is invariant under the action of elements of the form $l\#k$ and we can apply the restricted map ψ to get

$$\psi[(l\#k)(ev)] = \begin{cases} \psi(kv) & \text{if } k \in K_l \\ 0 & \text{otherwise.} \end{cases}$$

Now consider $(l\#k)\psi(ev)$. We have

$$(l\#k)\psi(ev) = (l\#k)\psi(v) = (l\#k) \sum_{i=1}^t g_i w_i = \sum_{i=1}^t (l\#k)g_i w_i \in \tilde{V}_2$$

for some $w_i \in V_2$. Each term in this sum is

$$(l\#k)g_i w_i = \begin{cases} kg_i w_i & \text{if } lk g_i \in Kl \\ 0 & \text{otherwise.} \end{cases}$$

The condition $lk g_i \in Kl$ is equivalent to $kg_i \in K_l$ and, if we choose k to be in the stabilizer K_l , it is equivalent to $g_i \in K_l$, i. e. $g_i = e$.

So if $k \in K_l$, then

$$(l\#k)\psi(ev) = (l\#k)\psi(v) = (l\#k)(ew_1) = kw_1 \in eV_2.$$

In particular, $\psi(v) = \psi(ev) = \psi[(l\#e)(ev)] = ew_1 \in eV_2$ so that the image of the restriction of ψ to V_1 is contained in V_2 . So, since for any $k \in K_l$ and $v \in V_1$ we have $\psi(kv) = \psi[(l\#k)(ev)] = (l\#k)\psi(ev) = k\psi(v)$, we see that the restriction of ψ to V_1 is an injective K_l -module homomorphism from V_1 to V_2 and, since $\dim V_1 = \dim V_2$, it is actually an isomorphism and so $V_1 \cong V_2$.

We deduce that for two non-isomorphic irreducible K_l -modules V_1 and V_2 the corresponding H -modules $\tilde{V}_1$ and $\tilde{V}_2$ are not isomorphic.

(b) Let $l \neq e$ and let V_1 be an irreducible K_e -module and V_2 an irreducible K_l -module. Since $K_e = K$, there is only one coset of K_e in K and as vector spaces $\tilde{V}_1 = V_1$. Let $l_1 \in L$, $k \in K$ and $v \in \tilde{V}_1$. Notice that if $l_1 k \in K$ then $l_1 = e$ as $K \cap L = \{e\}$ and hence

$$(l_1\#k)v = \begin{cases} kv & \text{if } l_1 = e \\ 0 & \text{otherwise.} \end{cases}$$

Now let $g_1, \dots, g_t$ be representatives of the left cosets of K_l in K , $k \in K$ and $w \in V_2$.

Then

$$(e\#k)(g_iw) = 0$$

since $l \neq e$ and thus $kg_i \notin Kl$.

So, for any $k \in K$, we have that $(e\#k)\tilde{V}_1 = \tilde{V}_1$ whereas $(e\#k)\tilde{V}_2 = 0$ and hence $\tilde{V}_1$ and $\tilde{V}_2$ cannot be isomorphic.

□

Remark. Part (b) of Proposition 3.2 has a more general version, which we are not going to prove here. Assume that l_1 and l_2 are in distinct orbits under the action of K on L . If V_1 is an irreducible K_{l_1} -module and V_2 is an irreducible K_{l_2} -module, then the corresponding H -modules $\tilde{V}_1$ and $\tilde{V}_2$ are non-isomorphic. Proposition 3.2, part (b), is this statement for the special case when either l_1 or l_2 is the identity element. So the modules constructed in Section 3.3.1 form a set of pairwise non-isomorphic irreducible H -modules.

The following discussion will show that H is semisimple and that these modules are actually all of the irreducible modules of H . For details see e. g. Section 5.3.1 of [4].

Assume that A is a finite-dimensional algebra over some field k . We have the following theorem.

Theorem 3.3. *The algebra A has a unique ideal N such that*

- (1) *The quotient A/N is semisimple.*
- (2) *If I is an ideal of A such that A/I is semisimple, then $N \subseteq I$.*

This ideal N is the intersection of all maximal left ideals of A . It is called the radical of A and denoted by $\text{rad}A$.

So the radical $\text{rad}A$ of A is the smallest possible ideal of A such that the quotient $A/\text{rad}A$ is semisimple. Moreover, A is semisimple if and only if $\text{rad}A = 0$.

Now assume that $k = \mathbb{C}$. Then we can apply Wedderburn's Theorem 2.12 to $A/\text{rad}A$ to find that

$$A/\text{rad}A \cong M_{n_1}(\mathbb{C}) \oplus \cdots \oplus M_{n_k}(\mathbb{C}),$$

where the n_i are the dimensions of the simple $A/\text{rad}A$ -modules.

Lemma 3.4. (a) *If S is a simple A -module, then $\text{rad}A$ annihilates S , that is $(\text{rad}A)S = 0$, and S can be viewed as a simple $A/\text{rad}A$ -module.*

(b) *Any simple $A/\text{rad}A$ -module inflates to a simple A -module.*

Proof. (a) Since S is simple, we know from Lemma 2.3 that for $0 \neq x \in S$ we have $A = Ax$. It is easy to check that the map $\phi : A \rightarrow S$ sending $a \in A$ to $\phi(a) = ax$ is a surjective A -module homomorphism from the regular A -module to S . Its kernel is the annihilator $I := \ker \phi = \{a \in A : ax = 0\}$ of x and hence, by the First Isomorphism Theorem for modules, we have that $S \cong A/I$. Now, I is a left ideal of A and, since $A/I \cong S$ is simple, we know that $\text{rad}A \subseteq I$ and hence $(\text{rad}A)S = (\text{rad}A)Ax \subseteq (\text{rad}A)x \subseteq Ix = 0$. It follows that if two elements in A lie in the same coset of $\text{rad}A$, then they have the same action on S . So we can regard S as an $A/\text{rad}A$ -module by letting a coset of $\text{rad}A$ act as any of its representatives and it is clear that this is simple.

(b) Conversely, any $A/\text{rad}A$ -module can be viewed as an A -module by letting an element in A act as its corresponding coset of N . It is clear that a simple $A/\text{rad}A$ -module is still simple when viewed as an A -module.

□

So the simple modules of A and $A/\text{rad}A$ are really the same and, in particular, A and $A/\text{rad}A$ have the same sets of dimensions of simple modules.

Corollary 3.5. *If $n_1, \dots, n_k$ are the dimensions of the simple modules of A and $\sum_{i=1}^k n_i^2 = \dim A$, then A is semisimple.*

Proof. By Lemma 3.4, $n_1, \dots, n_k$ are the dimensions of the simple modules of $A/\text{rad}A$ and, since $A/\text{rad}A$ is semisimple, Wedderburn's Theorem implies that $\sum_{i=1}^k n_i^2 = \dim(A/\text{rad}A) = \dim A - \dim(\text{rad}A)$. If this equals $\dim A$, then $\text{rad}A = 0$ so that $A = A/\text{rad}A$ is semisimple.

□

We now return to the bismash product H .

Corollary 3.6. *The bismash product H is semisimple and the modules $\tilde{V}$ constructed in Section 3.3.1 form the complete set of irreducible H -modules.*

Proof. Let $e = l_1, l_2, \dots, l_r$ be representatives of the orbits of the action of K on L and denote the s_i simple modules of a stabilizer K_{l_i} by $V_{l_i,1}, \dots, V_{l_i,s_i}$ and the corresponding H -modules by $\tilde{V}_{l_i,1}, \dots, \tilde{V}_{l_i,s_i}$. If we sum the squares of the dimensions

of these irreducible H -modules, we get

$$\begin{aligned}
\sum_{i=1}^r \sum_{j=1}^{s_i} (\dim \tilde{V}_{l_i,j})^2 &= \sum_{i=1}^r \sum_{j=1}^{s_i} \left(\frac{|K|}{|K_{l_i}|} V_{l_i,j} \right)^2 \\
&= \sum_{i=1}^r \frac{|K|^2}{|K_{l_i}|^2} \sum_{j=1}^{s_i} (V_{l_i,j})^2 \\
&= \sum_{i=1}^r \frac{|K|^2}{|K_{l_i}|^2} |K_{l_i}| = |K| \sum_{i=1}^r \frac{|K|}{|K_{l_i}|} \\
&= |K| \sum_{i=1}^r [l_i] = |K| |L| = \dim H,
\end{aligned}$$

where $[l_i]$ denotes the size of the orbit of l_i .

So Corollary 3.5 implies that H is semisimple and the $\tilde{V}$ form the complete set of irreducible H -modules.

□

Chapter 4

Blocks of characters of groups of order pm where $(p, m) = 1$

The proofs of our main results on the bismash products of symmetric groups will rely on the theory of blocks of characters developed by Richard Brauer. The case where a prime p divides the order of a group to the first power only has been treated in [1]. In this chapter we give a brief introduction to this and collect the main results.

First we state a well-known theorem by Burnside which will be needed in the discussion.

A finite group is *p-nilpotent* if it has a normal subgroup of order not divisible by p and index a power of p , that is, if it has a normal subgroup such that it is the semi-direct product of this subgroup and any Sylow p -subgroup. Such a subgroup is then called *normal p-complement*. The following theorem by Burnside gives a condition when a group is *p-nilpotent*. For a proof see [2], Chapter 2.4.3.

Theorem 4.1. *Let G be a finite group and P be a Sylow p -subgroup of G . If $P \leq Z(N_G(P))$, that is if P is contained in the centre of its normalizer, then G has a normal p -complement.*

Corollary 4.2. *Let C be a finite group and P be a Sylow p -subgroup of C . If $P \leq Z(C)$, then $C = P \times V$, where $|V|$ is not divisible by p .*

Let G be a group of order pm where p is a prime and m is not divisible by p .

The irreducible characters of G can be partitioned into equivalence classes called *p-blocks* as described in [1]. Let χ be an irreducible character of G .

(i) If the degree of χ is divisible by p , then $\{\chi\}$ is a p -block 'of defect 0'.

(ii) If the degree of χ is not divisible by p , then χ lies in a p -block 'of defect 1'.

Let χ_1 be the trivial character of G . Then $\chi_1(1) = 1$ is not divisible by p . So χ_1 lies in a p -block of defect 1 and this p -block is called the *principal p -block*.

Let P be a Sylow p -subgroup of G , $C := C_G(P)$, $N := N_G(P)$ and $t := |N : C|$. Note that N acts on P by conjugation. Since $g^{-1}abg = g^{-1}agg^{-1}bg$, this action is by automorphisms and hence determines a homomorphism

$$\alpha : N \longrightarrow \text{Aut}(P).$$

The kernel of α is C and so, by the First Isomorphism Theorem and Lagrange's Theorem, t divides $|\text{Aut}(P)|$. Now, P is a cyclic group of order p , and hence $\text{Aut}(P) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ has order $p-1$ and so t divides $p-1$. Since P is abelian, it lies in the centre of C and hence, by Corollary 4.2, we can write $C = P \times V$ for V of order not divisible by p . Let $1 = \phi_1, \phi_2, \dots, \phi_b$ be representatives of the N -conjugacy classes of the irreducible characters of V (see Definition 17).

Theorem 4.3. (Brauer)

(i) *There is a bijective correspondence between the p -blocks of G of defect 1 and the characters $1 = \phi_1, \phi_2, \dots, \phi_b$. Denote the p -block corresponding to ϕ_m by B_m . The p -block B_1 is chosen to be the principal p -block.*

(ii) *For any index m between 1 and b , there exists a parameter t_m dividing $p-1$ such that the p -block B_m consists of a family of $(p-1)/t_m$ so-called exceptional characters $\{\theta_i\}_{1 \leq i \leq (p-1)/t_m}$ of the same degree, together with t_m further characters $\{\chi_i\}_{1 \leq i \leq t_m}$. For the principal p -block B_1 , the parameter t_1 is $t = |N : C|$.*

(iii) *For each χ_i in the block B_m we have that*

$$\chi_i(1) \equiv \pm \Phi_m(1) \pmod{p},$$

where Φ_m is the sum of the distinct N -conjugates of ϕ_m .

(iv) *If θ_i is an exceptional character in the p -block B_m , then*

$$\theta_i(1) \equiv \pm t \phi_m(1) \pmod{p}.$$

Remark. Our use of the parameter t_m differs from that in Brauer's original paper [1] in that he uses the number of exceptional characters as a parameter, which is

$(p-1)/t_m$ with our notation.

For example, consider the symmetric group on 5 letters $G = S_5$. Then G has order 120 and its irreducible character degrees are 1, 1, 4, 4, 5, 5 and 6. We are going to consider the 3-blocks of G . The only character that occurs in a 3-block of defect 0 is the character of degree 6. Let $P \in Syl_3(G)$, that is $|P| = 3$ and without loss of generality, we can assume that $P = \langle (1\ 2\ 3) \rangle$. Then $C_G(P) = P \times V$, where $V = \langle (4\ 5) \rangle$ and $N_G(P) = S_3 \times V$. It follows that $t = |N_G(P) : C_G(P)| = \frac{12}{6} = 2$ and in the principal 3-block there is $\frac{3-1}{2} = 1$ exceptional and two further characters. Moreover, V has exactly two $N_G(P)$ -conjugacy classes of irreducible characters and so $b = 2$, that is in addition to the principal 3-block there is one other 3-block of defect 1 containing 3 irreducible characters.

Chapter 5

The case A_5

We are now going to carry out the constructions described in Chapter 3 explicitly for the standard factorization of the alternating group on 5 letters $A_5 = KL$, where $K = \text{Stab}_{A_5}(5) \cong A_4$ and $L = \langle \pi \rangle$, $\pi = (1\ 2\ 3\ 4\ 5)$.

We will see that the bismash product H arising from this factorization does not have the structure of a group algebra.

Lemma 5.1. *The action of K on L defined in Section 3.2.1 has exactly two orbits with representatives e and π and respective stabilizers $K_e = K \cong A_4$ and $K_\pi = \text{Stab}_{A_5}(5, 1) \cong A_3$.*

Proof. We already know that $\{e\}$ is an orbit with stabilizer $K_e = K \cong A_4$. Now, if $\sigma \in K$ sends 1 to r , then $\pi\sigma$ sends 5 to r . We know that $\pi\sigma = \sigma'\pi^s$ for some $\sigma' \in K$ and $0 \leq s \leq 4$. Now, $\sigma'\pi^s$ sends 5 to s . So we must have $s = r$ and we see that, for any $1 \leq r \leq 4$, there is a $\sigma \in K$ such that $\pi^\sigma = \pi^r$, that is K is transitive on $L \setminus \{e\} = \{\pi, \pi^2, \pi^3, \pi^4\}$. Moreover, the stabilizer of π consists of all permutations in K that fix the letter 1, that is $K_\pi = \text{Stab}_{A_5}(5, 1) \cong A_3$. □

Lemma 5.2. *The dimensions of the irreducible H -modules are 1, 1, 1, 3, 4, 4 and 4.*

Proof. From the above lemma and the results obtained in Section 3.3, we know that the irreducible modules of the bismash product H arising from this factorization $A_5 = KL$ come from the irreducible modules of A_4 and A_3 .

We first find the irreducible character degrees of A_4 .

Since a 3-cycle is an even permutation and $(123)(124)(132)(142) = (12)(34)$, it follows that every double transposition lies in the commutator subgroup A'_4 of A_4 and $V_4 \leq$

A'_4 . On the other hand, V_4 is normal in A_4 and $A_4/V_4 \cong C_3$ has order 3, so is abelian. It follows that $A'_4 \leq V_4$ and so $A'_4 = V_4$. So $|A_4 : A'_4| = 3$ and, by Corollary 2.21, this means that A_4 has 3 linear characters. We know by Corollary 2.9 that the squares of the irreducible character degrees of A_4 add up to $|A_4| = 12$ and thus A_4 has one non-linear character of degree 3. In summary, the irreducible character degrees of A_4 are 1, 1, 1 and 3 and hence the dimensions of the corresponding H -modules are also 1, 1, 1 and 3.

The irreducible character degrees of $A_3 \cong C_3$ are 1, 1 and 1 and thus the dimensions of the corresponding H -modules are 4 times these degrees, that is 4, 4 and 4.

□

Proposition 5.3. *The bismash product H arising from the factorization $A_5 = KL$, where $K = \text{Stab}_{A_5}(5) \cong A_4$ and $L = \langle \pi \rangle$ ($\pi = (1\ 2\ 3\ 4\ 5)$) is not isomorphic to a group algebra.*

Proof. Assume, for a contradiction, that $H \cong \mathbb{C}G$ for some group G . Then G has order 60 and its irreducible character degrees are 1, 1, 1, 3, 4, 4 and 4. Since the number of linear characters of a group is the order of its abelianization, this means that the commutator subgroup G' must have index 3 in G , i. e. must have order 20. Let P be a Sylow 5-subgroup of G' . By Sylow's Third Theorem, the number of Sylow 5-subgroups $|Syl_5(G')| = |G/N_{G'}(P)|$ is congruent to 1 modulo 5 and, as $P \leq N_{G'}(P)$, it divides $20/5 = 4$. It follows that $|Syl_5(G')| = 1$, that is P is the only Sylow 5-subgroup of G' . Now, if $g \in G$ and $p \in P$, then $gpg^{-1} = (gpg^{-1}p^{-1})p \in G'$. So every G -conjugate of P is contained in G' and thus must be P . It follows that P is normal in G and conjugation defines an action of G on P . Since $g^{-1}abg = g^{-1}agg^{-1}bg$, this action is by automorphisms, that is, it gives a homomorphism

$$\alpha : N_G(P) = G \longrightarrow \text{Aut}(P).$$

The kernel of α consists of all the elements in G that commute with every element in P , that is $\ker \alpha = C_G(P)$. By the First Isomorphism Theorem and Lagrange's Theorem, this means that $|G/C_G(P)|$ divides $|\text{Aut}(P)| = |(\mathbb{Z}/5\mathbb{Z})^\times| = 4$. In particular, it means that $G/C_G(P)$ is abelian and thus $G' \leq C_G(P)$. Now G' has index 3 in G and therefore we must have that $G = C_G(P)$. So every element in G commutes with every element in P . Hence, since P is abelian, it is contained in the centre of G and we can apply Corollary 4.2 to see that this means that $G = P \times V$, where V is a normal subgroup of G of index 5. But then $G/V \cong P$ is abelian and thus $G' \leq V$. So the

index of V in G must divide the index of G' in G , which is 3. This is a contradiction and hence proves the proposition. $\square$

Chapter 6

Symmetric groups and the corresponding bismash products

Our next goal is to prove a more general result than the one obtained in the previous chapter, namely that the bismash products arising from a large family of symmetric groups are not isomorphic to group algebras.

In this chapter we establish a couple of useful results on the bismash product arising from the standard factorization of the symmetric group on n letters $S_n = KL$, where $K = \text{Stab}_{S_n}(n) \cong S_{n-1}$ and $L = \langle \pi \rangle \cong C_n$ with π being the n -cycle $\pi = (1\ 2 \cdots n)$.

Lemma 6.1. *The action of K on L has exactly two orbits with representatives e and π and respective stabilizers $\text{Stab}_K(e) = K$ and $\text{Stab}_K(\pi) = \text{Stab}_{S_n}(n, 1) \cong S_{n-2}$.*

Proof. We already know that e forms an orbit of its own, the trivial orbit, and that the corresponding stabilizer is the whole of $K \cong S_{n-1}$. It remains to show that K is transitive on $L \setminus \{e\}$ and that $\text{Stab}_K(\pi) = \text{Stab}_{S_n}(n, 1)$. Indeed, if $\sigma \in K$ sends the letter 1 to r , then $\pi\sigma$ sends n to r . We know that $\pi\sigma = \sigma'\pi^s$ for some $\sigma' \in K$ and $0 \leq s \leq n-1$. Now, $\sigma'\pi^s$ sends n to s . So we must have $s = r$ and we see that, for any $1 \leq r \leq n-1$, there is a $\sigma \in K$ such that $\pi^\sigma = \pi^r$, that is K is transitive on $L \setminus \{e\}$. Moreover, the stabilizer of π consists of all permutations in K that fix the letter 1, that is $\text{Stab}_K(\pi) = \text{Stab}_{S_n}(n, 1) \cong S_{n-2}$. □

This lemma and the results on the dimensions of the simple modules of a bismash product given in Section 3.3 yield the following.

Proposition 6.2. *Let $S_n = KL$ be the standard factorization as above and denote*

the resulting bismash product by $H_n = \mathbb{C}^L \# \mathbb{C}K$. Then the dimensions of the simple H_n -modules are

- (i) $(n - 1)$ times the degrees of the irreducible characters of S_{n-2} , and
- (ii) the degrees of the irreducible characters of S_{n-1} ,
counting multiplicities.

Chapter 7

The case S_{p+1}

We are now almost ready to prove the following theorem.

Theorem 7.1. *If p is a prime greater than 3, then there is no group G such that $H_{p+1} \cong \mathbb{C}G$.*

7.1 Preparatory results

Apart from the machinery developed in the previous chapters, the proof of this theorem will use several more results, which we shall now establish.

Theorem 7.2. *Let T be a non-abelian simple group and assume that T has an irreducible character of degree $n > 1$ and that $|T| \geq (n+1)!$. Then the possibilities for n and T are as follows.*

n	T
3	A_5
5	$PSp_4(3)$
6	$U_3(3), PSp_4(3)$
7	$Sp_6(2)$

Proof. Since T is simple, the representation affording the given character is faithful and hence embeds T in $GL(n, \mathbb{C})$. We now apply Theorem 8 of [7], which says that T is either A_{n+1} or one of the groups given in the table in this theorem. Clearly, A_{n+1} is not a possibility since $|A_{n+1}| < (n+1)!$. Of the groups in the table the ones which are simple and of order greater than or equal to $(n+1)!$ are those listed above.

□

Lemma 7.3. *If $G'' \leq G' \triangleleft G$ and $|G : G'| = 2$, then G has an irreducible character of degree 2.*

Proof. The quotient group G'/G'' is abelian and non-trivial and therefore, by Lemma 2.15 and Corollary 2.9, it has at least two linear characters, which lift to two distinct linear characters of G' . Let χ be a non-trivial linear character of G' . Then the induced character $\text{Ind}_{G'}^G \chi$ has dimension $|G : G'| = 2$.

We claim that $\text{Ind}_{G'}^G \chi$ is an irreducible character of G . Indeed, assume for a contradiction that $\text{Ind}_{G'}^G \chi$ is reducible. Then it must be the sum of two linear characters, say $\text{Ind}_{G'}^G \chi = \chi_1 + \chi_2$. We can apply The Frobenius Reciprocity Theorem 2.25 to find that

$$\langle \text{Ind}_{G'}^G \chi, \chi_1 \rangle_G = \langle \chi_1, \chi_1 \rangle_G + \langle \chi_2, \chi_1 \rangle_G = \langle \chi, \chi_1|_{G'} \rangle_{G'}.$$

Now, by Corollary 2.17, we have that $\langle \chi_1, \chi_1 \rangle_G = 1$ and $\langle \chi_2, \chi_1 \rangle_G$ is either 0 or 1 and so $\langle \chi_1, \chi_1 \rangle_G + \langle \chi_2, \chi_1 \rangle_G$ is either 1 or 2. On the other hand, since χ_1 is linear, we know by Corollary 2.21 that G' is contained in the kernel of the representation affording χ_1 and so $\chi|_{G'}$ is the trivial linear character of G' . But as we chose χ to be non-trivial, we know that $\langle \chi, \chi_1|_{G'} \rangle_{G'} = 0$, which is a contradiction to the above Frobenius Reciprocity equality.

□

Lemma 7.4. *If G is a finite group with a normal subgroup $M \triangleleft G$ and P is a Sylow p -subgroup of M , then $G = MN_G(P)$.*

Proof. Let $g \in G$. Then $g^{-1}Pg \leq M$ is a Sylow p -subgroup of M as M is normal in G . So, since all Sylow p -subgroups of M are conjugate in M by Sylow's Second Theorem, there exist an $m \in M$ such that $g^{-1}Pg = m^{-1}Pm$ and hence $gm^{-1} \in N_G(P)$. It follows that $g \in MN_G(P)$.

□

Lemma 7.5. *If $n \geq 5$ then $S'_n = A_n$.*

Proof. It is clear that $S'_n \triangleleft A_n$ since S'_n is normal in S_n and $S_n/A_n \cong C_2$ is abelian. Now, A_n is simple if $n \geq 5$ (see for example Chapter 3 of [15] for a proof of this) and hence $\{e\} \neq S'_n = A_n$.

□

Lemma 7.6. *Let p be a prime. A Sylow p -subgroup of S_p has index $p - 1$ in its normalizer.*

Proof. Let P be a Sylow p -subgroup of S_p . We know from Sylow's Third Theorem that the number of Sylow p -subgroups is $|S_p : N_{S_p}(P)|$. Now, each Sylow p -subgroup consists of the identity and $p - 1$ p -cycles, and if $P_1 \neq P_2$ are two distinct Sylow p -subgroups, then $P_1 \cap P_2 = \{e\}$. The number of p -cycles is $(p - 1)!$ and hence the number of Sylow p -subgroups is $(p - 2)! = |S_p : N_{S_p}(P)|$. As $|S_p| = p!$, this means that $N_{S_p}(P) = (p - 1)p$ and the lemma follows. □

Lemma 7.7. *Let $\sigma \in S_n$ be a k -cycle. Then the centralizer of σ is*

$$C_{S_n}(\sigma) = \{\sigma^i \tau : 0 \leq i \leq k - 1, \tau \in S_{n-k}\},$$

where S_{n-k} is the subgroup of S_n consisting of all permutations that are disjoint from σ .

Proof. It is clear that σ commutes with powers of itself and disjoint permutations and hence the set $\{\sigma^i \tau : 0 \leq i \leq k - 1, \tau \in S_{n-k}\}$ must be contained in its centralizer. We claim that there are no other elements in $C_{S_n}(\sigma)$. Indeed, $C_{S_n}(\sigma)$ is the stabilizer of σ in the action of S_n on itself by conjugation and the orbit of σ in this action consists of all permutations of the same cycle shape. So we know from the Orbit-Stabilizer Theorem that the index of $C_{S_n}(\sigma)$ in S_n is the number of k -cycles in S_n , and this is $\frac{n(n-1)\cdots(n-k+1)}{k}$. So

$$|C_{S_n}(\sigma)| = \frac{|S_n|}{\frac{n(n-1)\cdots(n-k+1)}{k}} = \frac{n!}{\frac{n(n-1)\cdots(n-k+1)}{k}} = k(n - k)!,$$

which is exactly the size of the set $\{\sigma^i \tau : 0 \leq i \leq k - 1, \tau \in S_{n-k}\}$. □

Lemma 7.8. *Let p be a prime. The symmetric group S_p has exactly one p -block of defect 1, the principal p -block $B_1(S_p)$. This block contains precisely p characters, which have degrees $\pm 1 \pmod p$ and at least one of which has degree $p - 1$.*

Proof. We first notice that $|S_p| = p!$ is divisible by p to the first power only and so we can use the theory presented in Chapter 4.

Let P be a Sylow p -subgroup of S_p . Then P is a cyclic subgroup generated by a p -cycle and so, by Lemmas 7.7 and 7.6, P is self-centralizing and has index $p - 1$ in its normalizer. It follows from Theorem 4.3, part (i), that S_p has exactly one p -block of defect 1, namely the principal p -block B_1 , and from part (ii) that $B_1(S_p)$ contains precisely one exceptional and $(p - 1)$ further characters. Now, from part (iii) and (iv) of Theorem 4.3 we know that these characters have degrees $\equiv \pm 1 \pmod{p}$.

Consider the p -dimensional permutation module $V = \mathbb{C}^p$ of S_p , on which S_p acts by permuting the basis vectors in a natural way. This has a $(p - 1)$ -dimensional submodule consisting of the vectors with coordinates adding up to zero and this submodule must be irreducible since the irreducible characters of degree less than p have degree 1 or $p - 1$ by the previous paragraph.

□

Finally, we need the following number-theoretic lemma, a proof of which can be found in [5].

Lemma 7.9. *Let n be an integer and q be a prime with $q < n$ and q^e dividing $n!$. Then $e < n - 3$ if q is odd and $e < n$ if $q = 2$.*

7.2 Proof of Theorem 7.1

The proof is by contradiction. Assume that there is such a group G with $\mathbb{C}G \cong H_{p+1}$. Then G has order $\dim \mathbb{C}G = \dim H_{p+1} = (p+1)!$ and the irreducible character degrees of G are the dimensions of the simple modules of H_{p+1} , which by Proposition 6.2 are

- (i) p times the degrees of the irreducible characters of S_{p-1} , and
- (ii) the degrees of the irreducible characters of S_p ,

counting multiplicities.

We first notice that both $|G| = (p+1)!$ and $|S_p| = p!$ are divisible by p to the first power only and so we can apply the theory of p -blocks presented in Chapter 4.

Lemma 7.10. *The group G has an irreducible character of degree $p - 1$.*

Proof. This follows immediately from (ii) above since S_p has a character of degree $p - 1$ by Lemma 7.8.

□

Lemma 7.11. (a) *We have $|G : G'| = 2$.*

(b) The group G has only one p -block of defect one, the principal p -block $B_1(G)$.

(c) If P is a Sylow p -subgroup of G , then $P = C_G(P)$ and $N_G(P)/P$ is cyclic of order $p - 1$.

(d) Any non-trivial normal subgroup of $N_G(P)$ contains P .

Proof. (a) From (i) and (ii) above, we know that the linear characters of G correspond to the linear characters of S_p . But, by Lemma 7.5, $S'_p = A_p$ and, by Corollary 2.21, the number of linear characters of S_p is $|S_p : S'_p| = 2$. Hence G also has two linear characters and $|G : G'| = 2$.

(b) By Lemma 7.8, G has precisely p irreducible characters of degree not divisible by p and all of them have degree $\pm 1 \pmod p$. Let P be a Sylow p -subgroup of G and let $t = |N_G(P) : C_G(P)|$. As observed before Theorem 4.3, t divides $p - 1$. Let θ be an exceptional character in the principal block $B_1(G)$. By Theorem 4.3, part (iv), we have that $\theta(1) \equiv \pm t \pmod p$. Hence, $t \equiv \pm 1 \pmod p$, and so $t = 1$ or $p - 1$.

If $t = 1$, that is $C_G(P) = N_G(P)$, then $P \leq Z(N_G(P))$, and hence, by Lemma 4.1, G is p -nilpotent, that is $G = PN$, where $N \triangleleft G$ and $P \cap N = \{e\}$. So $G/N \cong P \cong C_p$ is abelian and $G' \leq N$, which is a contradiction to (a).

Therefore, $t = p - 1$. Now, Theorem 4.3, part (ii), says that the principal block $B_1(G)$ has p characters and since there are only p characters of degree not divisible by p , $B_1(G)$ must be the only p -block of G of defect 1.

(c) If $C_G(P) \neq P$, then $C_G(P) = P \times V$ with V being non-trivial and not divisible by p (see the preamble to Theorem 4.3). Since V has at least one non-trivial character, Theorem 4.3, part (i), then implies that G has more than one p -block of defect one, contradicting (b). Therefore, we have that $C_G(P) = P$ and since we established in the proof of (b) that $t = p - 1$, we have that $|N_G(P) : P| = p - 1$. Finally, $N_G(P)/P$ is isomorphic to a subgroup of $\text{Aut}(P)$, which is cyclic of order $p - 1$.

(d) Let R be a non-trivial normal subgroup of $N_G(P)$. If p divides $|R|$ then R contains the unique Sylow p -subgroup P of $N_G(P)$. Otherwise, $R \cap P = \{e\}$ and hence R centralizes P contradicting the fact that $C_G(P) = P$ established in (c).

□

Lemma 7.12. *The commutator subgroup G' is simple.*

Proof. Since all irreducible characters of G have degrees either divisible by p or $\pm 1 \pmod p$, G has no irreducible character of degree 2. Therefore, G' is perfect by

Lemma 7.3.

Let M be a proper subgroup of G' maximal subject to being normal in G . Let P be a Sylow p -subgroup.

If $P \leq M$, then Lemma 7.4 implies that $G = MN_G(P)$ and, by the Third Isomorphism Theorem,

$$G/M = MN_G(P)/M \cong N_G(P)/(M \cap N_G(P)).$$

Since P is contained in $M \cap N_G(P)$, $N_G(P)/(M \cap N_G(P))$ is a quotient of $N_G(P)/P$, which is abelian by Lemma 7.11, part (c). Hence, G/M is also abelian contradicting the fact that M was chosen to be a proper subgroup of G' .

Therefore we must have that P is not contained in M . Since P was an arbitrary Sylow p -subgroup and $|P| = p$, this means that M is not divisible by p .

Claim 4. The quotient G'/M is simple.

Indeed, suppose not and choose a maximal proper normal subgroup N of G' properly containing M . By the choice of M , this means that N is not normal in G and so there exists an element $x \in G$ such that $N^x := x^{-1}Nx \neq N$. Note that, since N is normal in G' , we have that $x \notin G'$. Also, $N^x \leq (G')^x = G'$ and $M \triangleleft G$ and so $M = M^x \leq N^x$ and it follows that $M \leq N \cap N^x$.

Let $y \in G$. Since G' has index 2 in G , we can write $y = hx$ for some $h \in G'$. So

$$(N \cap N^x)^y = (N \cap N^x)^{hx} = N^{hx} \cap N^{xhx} = N^x \cap N^{x^2} = N^x \cap N,$$

where the last equality follows from the fact that $x^2 \in G'$ as G' has index 2 in G . Hence, $N \cap N^x$ is normal in G and, by the maximal choice of M , this means that $M = N \cap N^x$.

We assert that p does not divide N . Otherwise, choose a Sylow p -subgroup P contained in N and observe that $G' = NN_{G'}(P)$ by Lemma 7.4. This implies that G'/N is cyclic violating the fact that G' is perfect.

We conclude that p divides both the orders of G'/N and G'/N^x . By the maximal choice of N , we know that $G' = NN^x$ and thus

$$G'/N^x = NN^x/N^x \cong N/(N \cap N^x) = N/M.$$

Therefore, p divides $|N : M|$ and p^2 divides $|G : M|$, which is a contradiction, and this proves the claim.

Claim 5. The group M is trivial.

Indeed, suppose $M \neq \{e\}$ and let P be a Sylow p -subgroup of G . Observe that $M \cap N_G(P)$ is a normal subgroup of $N_G(P)$ and has order coprime to p . Since such a subgroup must centralize $P = C_G(P)$, it follows that $M \cap N_G(P) = \{e\}$.

Now define $X = MN_G(P)$ and let q be a prime dividing the order of M . Let Q be a Sylow q -subgroup of M and apply Lemma 7.4 to see that $X = MN_X(Q)$.

We assert that Q can be chosen such that $N_G(P) \leq N_X(Q)$.

Indeed, by the Third Isomorphism Theorem, $X/M \cong N_G(P)$ and hence

$$N_G(P) \cong X/M = MN_X(Q)/M \cong N_X(Q)/M \cap N_X(Q) = N_X(Q)/N_M(Q).$$

Write $M_0 := N_M(Q)$. Then from the structure of $N_G(P)$ established in Lemma 7.11, part (c), we know that $N_X(Q)/M_0 = \langle uM_0, xM_0 \rangle$, where the order of uM_0 and xM_0 are p and $p-1$ respectively and $(uM_0)^{xM_0} = u^iM_0$ for some $i \in \mathbb{N}$. Now, since M_0 is normal in $N_X(Q)$, $\langle u \rangle M_0$ is a subgroup of $N_X(Q)$ of order divisible by p and thus contains a Sylow p -subgroup. Hence we may take u to be an element of order p in the coset uM_0 . If we define $S = \langle u \rangle$, then $S^x \leq SM_0$ and, by Sylow's Second Theorem, there exists $y \in M_0$ such that $S^x = S^y$. Observe that $x \neq y$ since $x \notin M_0$ and therefore $1 \neq z := xy^{-1} \in N_G(S) \cap N^X(Q)$. Since the order of xM_0 is $p-1$, it follows that $\langle S, z \rangle$ has order $p(p-1)$ and hence is equal to $N_G(S)$ and consequently $N_G(S) \leq N_X(Q)$. By Sylow's Second Theorem, we have that $P = S^n$ for some $n \in N_X(Q)$ and then $N_G(P)$ normalizes Q^n , proving the assertion.

Thus, $N := N_G(P)$ normalizes Q and also normalizes $Z(Q)$ and the subgroup $V := \langle z \in Z(Q) : z^q = e \rangle$. We have that $V \cong (C_q)^d$ for some $d \in \mathbb{N}$ and so V is a d -dimensional vector-space over the field $\mathbb{F}_q$ of q elements. Conjugation of V by elements in $N_G(P)$ defines a representation

$$N_G(P) \longrightarrow \text{Aut}(V) = GL(V) \cong GL(d, q).$$

So we may regard V as an $\mathbb{F}_q N_G(P)$ -module. Observe that $N_G(P)$ acts non-trivially on V since V is not contained in $C_G(P) = P$ (as V is a q -group and $q \neq p$). Let u be a generator for P and let $p(x)$ be the characteristic polynomial of u in its action on V . If $\lambda \neq 1$ is a root of $p(x)$ in some extension field of $\mathbb{F}_q$, then λ is a p^{th} root of unity. Since u is conjugate to all its non-trivial powers, $\lambda, \lambda^2, \dots, \lambda^{p-1}$ must all be roots of $p(x)$. Hence, $\dim V = \deg(p(x)) \geq p-1$. It follows that $|V| \geq q^{p-1}$.

Recall that $|G| = (p+1)!$ and thus q^{p-1} divides $(p+1)!$. If q is odd, this contradicts Lemma 7.9. It follows that $q = 2$. Now, $|M|$ is divisible by 2^{p-1} and $|G : G'| = 2$. Moreover, we claim that G'/M has even order. Indeed, otherwise G'/M is soluble by the celebrated Feit-Thompson Theorem (see [9]), which contradicts the perfection of G' . We deduce that $|G| = (p+1)!$ is divisible by 2^{p+1} , which is a contradiction by Lemma 7.9. Hence M is trivial.

The lemma now follows directly from Claim 4 and Claim 5. □

We are now ready to finish the proof of Theorem 7.1.

Recall that G is a group of order $(p+1)!$ and has an irreducible character χ of degree $p-1$ by Lemma 7.10. Also, $|G : G'| = 2$ and G' is simple by Lemmas 7.11 and 7.12. By Proposition 2.22, $\chi|_{G'}$ is either irreducible or the direct sum of two irreducible characters of degree $(p-1)/2$. So we know that there is an irreducible $\mathbb{C}G'$ -module V of dimension $n := p-1$ or $(p-1)/2$ and V must be faithful as G' is simple. We can now apply Theorem 7.2 to G' to find that $n = 3, 5, 6$ or 7 and $G' \cong A_5, PSp_4(3), U_3(3)$ or $Sp_6(2)$. The possibilities for the pair (n, p) are $(3, 7), (5, 11), (6, 7)$ and $(6, 13)$. In each case we check that G' does not have order $(p+1)!/2$. This final contradiction completes the proof of Theorem 7.1.

7.3 The case S_4

The proof in the previous section does not work if the prime p is less than 5. In fact, looking at the case when $p = 3$, we see that the bismash product H_4 does have the structure of a group algebra.

Proposition 7.13. *The bismash product H_4 is isomorphic to $\mathbb{C}S_4$.*

Proof. By Proposition 6.2, the dimensions of the simple H_4 -modules are 3 times the irreducible character degrees of S_2 together with the irreducible character degrees of S_3 . The group S_2 is abelian of order 2 and thus its irreducible character degrees are 1 and 1 by Lemma 2.15. The quotient group $S_3/A_3 \cong C_2$ is abelian and hence $S'_3 \leq A_3$. Conversely, since A_3 consists of the identity permutation and the two 3-cycles in S_3 and e.g. the 3-cycle $(123) = (12)(23)(12)(23)$ is a commutator, we have that $A_3 \leq S'_3$. So $S'_3 = A_3$ has index 2 in S_3 and hence S_3 has exactly two linear characters by Corollary 2.21. The squares of the degrees of the non-linear irreducible characters must sum up to 4 and the only way for this to be possible is that there is

only one remaining irreducible character, which has degree 2. So S_3 has irreducible character degrees 1, 1 and 2.

Therefore, the dimensions of the simple modules of H_4 are 1, 1, 2, 3 and 3.

We claim that these are exactly the irreducible character degrees of S_4 so that Wedderburn's Theorem 2.12 implies that $H_4 \cong \mathbb{C}S_4$.

Indeed, the quotient group $S_4/A_4 \cong C_2$ is abelian and hence $S'_4 \leq A_4$. Conversely, since A_4 consists of the identity permutation, the 3-cycles and the double transpositions in S_4 , and e. g. $(123) = (12)(23)(12)(23)$ and $(12)(34) = (134)(342)(143)(324)$ are commutators, we have that $A_4 \leq S'_4$. So $S'_4 = A_4$ has index 2 in S_4 and hence S_4 has exactly two linear characters by Corollary 2.21. The total number of irreducible characters of S_4 is the number of conjugacy classes, i. e. cycle shapes, of S_4 . This number is 5 and hence S_4 has 3 non-linear irreducible character degrees, which divide $|S_4| = 24$ and whose squares sum up to 22. The only possibility is that they are 2, 3 and 3. In summary, the irreducible character degrees of S_4 are 1, 1, 2, 3 and 3 as required.

□

Remark. The first place where the proof in the previous chapter fails for $p = 3$ is the application of Lemma 7.3, since, unlike larger symmetric groups, S_4 does have an irreducible character of degree 2.

Chapter 8

The case S_5

In the previous chapter we looked at the bismash products arising from the standard factorization of symmetric groups on $p + 1$ letters for p being a prime. We saw that if p is greater than 3, then these are not isomorphic to group algebras. In this chapter we are going to consider the symmetric group on 5 letters. Again, we will see in Proposition 8.5 that the bismash product arising from the standard factorization is not isomorphic to a group algebra.

Before proving this, we establish some results which will be needed in the proof.

Lemma 8.1. *A group of order 60 is either soluble or isomorphic to A_5 .*

Proof. We use the well-known fact that A_5 is the smallest non-abelian simple group. (This can be proved with a routine but lengthy argument using Sylow's Theorems.)

Let G be an insoluble group of order 60. Then G has an insoluble composition factor, which by the remark above must be G itself and isomorphic to A_5 .

□

We also have the following lemma about soluble groups of order 60.

Lemma 8.2. *A soluble group of order 60 has a unique Sylow 5-subgroup.*

Proof. We are going to prove the following (stronger) statement. If a soluble group G has order dividing 60 and divisible by 5, then G has a unique Sylow 5-subgroup.

We are going to proceed by induction on $|G|$. The statement is clearly true when $|G| \leq 5$ or 5 does not divide $|G|$. Now assume that G is a soluble group of order dividing 60 and divisible by 5 and that the statement is true for all groups H with $|H|$ smaller than $|G|$. Let M be a minimal normal subgroup of G . Since G is soluble, M is elementary abelian, so must have order 2, 3, 4 or 5. If $|M| = 5$, then this is a

normal and hence unique Sylow 5-subgroup of G . If $|M| \neq 5$, then 5 divides the order of the quotient G/M . So G/M is a soluble group of order dividing 60, divisible by 5 and smaller than $|G|$ and therefore, by induction assumption, G/M has a unique and hence normal Sylow 5-subgroup $\bar{K}$. By the Second Isomorphism Theorem, $\bar{K} = K/M$ for some normal subgroup K of G containing M with $|K| = 5|M|$. The group K is soluble of order dividing 60, divisible by 5 and smaller than $|G|$ and therefore, by induction assumption, has a unique and hence normal Sylow 5-subgroup P . Notice that $P \setminus \{1\}$ is exactly the set of elements of order 5 in K . Now, P is also a Sylow 5-subgroup of G and as Sylow 5-subgroups of G are conjugate, every Sylow 5-subgroup of G is a conjugate of P . Since P is contained in K and K is normal in G , every conjugate of P is contained in K , so must be equal to P . It follows that P is normal in G , i. e. is the unique Sylow 5-subgroup of G and this completes the proof. $\square$

We will also need the following lemma, characterizing groups that are isomorphic to S_4 .

Lemma 8.3. *A group of order 24 that has irreducible character degrees 1, 1, 2, 3 and 3 is isomorphic to S_4 .*

Proof. Let G be a group of order 24 that has irreducible character degrees 1, 1, 2, 3 and 3.

We claim that G cannot have a normal subgroup of order 2 or 3. Indeed, assume, for a contradiction, that N is a normal subgroup of order 2. Then the quotient group G/N has order 12 and its irreducible characters lift to irreducible characters of G . So the irreducible character degrees of G/N must be a subset of 1, 1, 2, 3 and 3 with their squares adding up to 12. But this is impossible and so G cannot have a normal subgroup of order 2. Similarly, it is impossible for a subset of squares of 1, 1, 2, 3 and 3 to add up to 8 and therefore G cannot have a normal subgroup of order 3.

Now let P be a Sylow 3-subgroup of G , i. e. $|P| = 3$. By the above discussion, we know that P is not normal in G , that is, $|Syl_3(G)| > 1$. By Sylow's Third Theorem, we know that the number of Sylow 3-subgroups of $|Syl_3(G)| = |G/N_g(P)|$ is congruent to 1 modulo 3 and divides $24/3 = 8$. It follows that $|Syl_3(G)| = 4$ and $N_G(P)$ has order 6 and is thus isomorphic to C_6 or D_3 .

If we let G act on $Syl_3(G)$ by conjugation, we get a group homomorphism

$$\rho : G \longrightarrow \text{Sym}(Syl_3(G)) \cong S_4.$$

Let $K := \ker(\rho)$ be the kernel of this homomorphism. Then K is the intersection of all stabilizers of the action. In particular, it is contained in $\text{Stab}_G(P) = N_G(P)$.

We claim that $K = \{e\}$. Indeed, first assume that $K = N_G(P)$. If $N_G(P) \cong D_3$, then, since K is normal in G , we have that, for any $g \in G$, conjugation by g defines an automorphism of D_3 and, since D_3 has only one subgroup of order 3 (the subgroup generated by a rotation), we have that $gPg^{-1} = P$. But this means that P is normal in G , which we know is not true. Similarly, since C_3 has only one subgroup of order 3, we get a contradiction if $N_G(P) \cong C_3$.

Now assume that K is strictly contained in $N_G(P)$. Then K is either $\{e\}$ or has order 2 or 3. But we have seen above that G has no normal subgroups of order 2 or 3 and so it follows that K must be $\{e\}$.

We conclude that $K = \{e\}$ and, by the First Isomorphism Theorem, it follows that G is isomorphic to a subgroup of S_4 . Now, both S_4 and G have order 24 and hence we have $G \cong S_4$.

□

Lemma 8.4. *The dimensions of the simple H_5 -modules are 1, 1, 2, 3, 3, 4, 4 and 8.*

Proof. By Proposition 6.2, the dimensions of the simple H_5 -modules are 4 times the irreducible character degrees of S_3 and the irreducible character degrees of S_4 .

The quotient group $S_3/A_3 \cong C_2$ is abelian and hence $S'_3 \leq A_3$. Conversely, since A_3 consists of the identity permutation and the two 3-cycles in S_3 and e.g. the 3-cycle $(123) = (12)(23)(12)(23)$ is a commutator, we have that $A_3 \leq S'_3$. So $S'_3 = A_3$ has index 2 in S_3 and hence S_3 has exactly two linear characters. The squares of the degrees of the non-linear irreducible characters must sum up to 4 and the only way for this to be possible is that there is only one remaining irreducible character, which has degree 2. So S_3 has irreducible character degrees 1, 1 and 2 and the corresponding dimensions of simple modules of H_5 are 4, 4 and 8.

As observed in the proof of Proposition 7.13, the irreducible character degrees of S_4 are 1, 1, 2, 3 and 3 and these are also the remaining dimensions of simple modules of H_5 .

□

Proposition 8.5. *The bismash product H_5 is not isomorphic to a group algebra.*

Proof. Assume, for a contradiction, that there is a group G such that $H_5 \cong \mathbb{C}G$. Then G has order 120 and irreducible character degrees 1, 1, 2, 3, 3, 4, 4 and 8. So the

number of linear character and hence the index of the commutator subgroup G' of G is 2, that is $G' = 60$. It is clear that every Sylow 5-subgroup of G' is also a Sylow 5-subgroup of G . Conversely, every Sylow 5-subgroup of G is also a Sylow 5-subgroup of G' . Indeed, let $P \leq G$ be a Sylow 5-subgroup of G . By Sylow's First Theorem, G' has a Sylow 5-subgroup $Q \leq G'$. Then Q is also a Sylow 5-subgroup of G and Sylow's Second Theorem says that P must be conjugate to Q , that is, there exists an element $g \in G$ such that $P = gQg^{-1}$. But for any $q \in Q$, $gqg^{-1} = (gqg^{-1}q^{-1})q \in G'$ and so $P \leq G'$.

We claim that G has a unique, i. e. normal, Sylow 5-subgroup P . To prove this, we first show that G' is not isomorphic to A_5 . Lemma 8.1 then implies that G' must be soluble and hence has a normal Sylow 5-subgroup by Lemma 8.2.

So, assume, for a contradiction, that $G' \cong A_5$. We know that A_5 has five conjugacy classes and hence, by Lemma 2.18, five irreducible characters, only one of which is linear as A_5 is simple. The squares of the remaining character degrees add up to 59 and hence must be 3, 3, 4 and 5.

We know that G has an irreducible character χ of degree 2. If we restrict χ to G' , it must be the sum of two copies of the trivial character of degree 1, that is, G' acts trivially on the representation affording χ . But this means that χ is the lift of an irreducible character $\bar{\chi}$ of degree 2 of the quotient group $G/G' \cong C_2$, which is a contradiction since the irreducible characters of an abelian group have degree 1 by Lemma 2.15.

So we know that G' has a normal Sylow 5-subgroup P and, since the Sylow 5-subgroups of G are exactly the Sylow 5-subgroups of G' , P is also normal in G and we have a sequence of groups

$$P \triangleleft G' \triangleleft G$$

with G/P being a group of order 24 with commutator subgroup $(G/P)' = G'/P$ of index 2. We now find the irreducible character degrees of G/P . Every irreducible character of G/P lifts to an irreducible character of G and thus the irreducible character degrees of G/P must be a subset of the irreducible character degrees 1, 1, 2, 3, 3, 4, 4 and 8 of G . Since the commutator subgroup of G/P has index 2, the number of linear characters of G/P is 2 and the squares of the remaining irreducible character degrees must add up to 22. Since 8^2 is greater than 22, G/P cannot have an irreducible character of degree 8 and if it has an irreducible character of degree 4, then the remaining irreducible character degrees must be 2 or 3 and add up to $22 - 16 = 6$, which is

impossible. It follows that the non-linear irreducible characters of G/P have degrees 2, 3, and 3 and therefore, by Lemma 8.3, G/P must be isomorphic to S_4 .

Since P is normal in G , conjugation induces a homomorphism from G to $\text{Aut}(P)$ with kernel $C_G(P)$. As $\text{Aut}(P) \cong C_4$, it follows that $G/C_G(P)$ is cyclic of order dividing 4. Hence, G' is contained in $C_G(P)$ and, as $|G : G'| = 2$, this means that $C_G(P)$ is equal to either G or G' . Also, by Corollary 4.2, $C_G(P) = P \times V$ for some V .

If $G = C_G(P)$, then $G = P \times V$ and so $G' \leq V$ and 5 divides $|G/G'|$, which is a contradiction. Therefore, $G' = C_G(P) = P \times V$ and $|V| = 12$. Moreover, an element of order 2 that does not lie in $C_G(P)$ induces an automorphism of P of order 2, that is inverts every element in P .

The quotient G/V is a group of order 10 which has a subgroup isomorphic to P and an element outside this subgroup inverts all elements in it. It follows that G/V is isomorphic to D_{10} .

However, D_{10} has two irreducible characters of degree 2, each of which can be lifted to an irreducible character of G . But G has only one irreducible character of degree 2 and so this is a contradiction completing the proof.

□

Chapter 9

The case $GL(3, 2)$

We now consider a bismash product arising from a factorization of a group that is not symmetric, namely the general linear group $GL(3, 2)$. Again, we find that the bismash product does not have the structure of a group algebra.

The group $GL(3, 2)$ has a natural transitive action on the set Ω consisting of the seven non-zero vectors in the associated three-dimensional vector space over the field of two elements. The stabilizer of the vector $v := (1\ 0\ 0)^T \in \Omega$ is

$$K := \left\{ \begin{pmatrix} 1 & x \\ 0 & A \end{pmatrix} : x = (a\ b), A \in GL(2, 2) \right\}.$$

This group is isomorphic to S_4 . Indeed, $K = VS$, where

$$V := \left\{ \begin{pmatrix} 1 & x \\ 0 & I \end{pmatrix} : x = (a\ b) \right\}$$

and

$$S := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} : A \in GL(2, 2) \right\}.$$

Observe that V is a normal Klein 4-subgroup of K , S is isomorphic to S_3 and $V \cap S = \{e\}$. Thus, K is the semidirect product of V and S and hence isomorphic to S_4 .

Let

$$l := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in GL(3, 2).$$

We check that l has order 7 and hence acts as a 7-cycle on Ω . Let $L = \langle l \rangle$. Since L is transitive on Ω , it is transitive on the set of cosets of K in $GL(3, 2)$ and thus we get a factorization

$$G = KL.$$

Proposition 9.1. *The bismash product H arising from the factorization $GL(3, 2) = KL$ as described above is not isomorphic to a group algebra.*

Proof. Since L acts regularly on Ω , the action of K on L defined in Section 3.2.1 and the action of K on Ω are equivalent (by the identification of $l' \in L$ with $l'(v) \in \Omega$). Thus, since K is transitive on $\Omega \setminus v$, the action of K on L has two orbits, namely the trivial orbit and another orbit of size 6.

So we know from Section 3.3 that the dimensions of the simple H -modules are the irreducible character degrees of $K \cong S_4$ and 6 times the irreducible character degrees of the stabilizer K_l of l . The latter group has order 4, and hence is abelian and has 4 irreducible characters, all linear. We conclude that the dimensions of the simple H -modules are

$$1, 1, 2, 3, 3, 6, 6, 6 \text{ and } 6.$$

Suppose, for a contradiction, that G is a group with $H \cong \mathbb{C}G$. The order of G is $168 = |GL(3, 2)|$, which is divisible by 7 to the first power only. Thus, we can use the Brauer theory of 7-blocks presented in Chapter 4. The irreducible character degrees of G are $1, 1, 2, 3, 3, 6, 6, 6$ and 6 . None of them are divisible by 7 and hence, G has no 7-blocks of defect 0. Now, by Theorem 4.3, part (ii), the total number of characters in a 7-block B_m of defect 1 is $t_m + 6/t_m$ for some t_m dividing 6. This number is either 5 or 7. However, G has exactly 9 irreducible characters lying in blocks of defect 1, yielding a palpable contradiction.

□

Chapter 10

Conclusion and further results

We have shown that many bismash products constructed from symmetric groups and certain small simple groups do not have the structure of group algebras. Since paper [5], there have been further intriguing developments. Bismash products arising from the standard factorization of S_n are not isomorphic to group algebras for arbitrary $n \geq 5$, as has been proved by M. Collins in [6]. Getting away from symmetric groups, M. Clarke obtains the same conclusion for the standard factorization of $PGL_2(q)$ as the product of the stabilizer of a one-dimension space and a $(q + 1)$ -cycle in [3]. In contrast to this, he shows that the bismash products corresponding to Frobenius groups do have the structure of group algebras. Characterizing which finite groups yield bismash products that are group algebras remains a problem on which there is much further work to be done.

Acknowledgements

I am grateful to my supervisor, Dr Karin Erdmann, for the time and effort she has put into helping me with this work.

Bibliography

- [1] R. Brauer, On groups whose order contains a prime number to the first power I, Amer. J. Math. 64 (1942).
- [2] W. Burnside, *Theory of groups of finite order* (2nd ed.), Cambridge University Press, reprinted by Dover (1955).
- [3] M. C. Clarke, On the algebra structure of some bismash products, J. Algebra 322 (2009), 2590–2600.
- [4] P. M. Cohn, *Basic Algebra*, Springer-Verlag, London, (2003).
- [5] M. J. Collins, Some bismash products that are not group algebras, J. Algebra 316 (2007), 297–302.
- [6] M. J. Collins, Some bismash products that are not group algebras II, J. Algebra 375 (2013), 59–72.
- [7] M. J. Collins, Bounds for finite primitive complex linear groups, J. Algebra 319 (2007), 759–776.
- [8] K. Erdmann, Algebras, lecture notes (2007), Mathematical Institute, University of Oxford.
- [9] W. Feit and J. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963), 1–255.
- [10] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin (1967).
- [11] G. James, M. Liebeck, *Representations and Characters of Finite Groups*, Cambridge University Press (1993).
- [12] A. Masuoka, Calculations of some groups of Hopf algebra extensions, J. Algebra 191 (1997), 568–588.
- [13] A. Jedwab, S. Montgomery, Representations of some Hopf algebras associated to the symmetric group S_n , preprint.
- [14] R. Landers, S. Montgomery, P. Schauenburg, Hopf powers and orders for some

- bismash products, J. Pure Appl. Algebra 191 (2006), 156-188.
- [15] J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, (1995).
- [16] E. Segal, Group Representation Theory, lecture notes (2013), Imperial College London, available at www2.imperial.ac.uk/~epsegal/repthy/.