TWISTED GROUP ALGEBRAS OVER ARBITRARY FIELDS[1]

BY
William F. Reynolds

1. Introduction

A twisted group algebra A for a finite group G over a field F is an F-algebra which has a basis $\{a_g : g \in G\}$ with

$$(1.1) \qquad a_g a_{g'} = f(g, g')a_{gg'}, \qquad g, g' \in G$$

where $0 \neq f(g, g') \in F$ (see [6], [22]). This paper is devoted to determining the number $k(A)$ of non-equivalent irreducible representations of A. The new feature of this investigation is that F is not required to be algebraically closed or even to be a splitting field for A; rather F is an arbitrary (commutative) field of characteristic $p \geq 0$.

In the algebraically closed case, $k(A)$ was determined by Schur [18] for $p = 0$ and by Asano, Osima, and Takahasi [2] for $p \neq 0$ (see Theorem 1 below), in the language of projective representations. For general F, $k(A)$ has been determined only when A is the group algebra of G, i.e. when $f(g, g') = 1$ for all $g, g' \in G$. (See, however, [3, Theorem VI].) This was done for the rational and real fields by Frobenius and Schur [11, §6], and for general F by Witt [21, Theorem 4] and by Berman (see [4, Theorem 5.1] and earlier papers); a simple presentation based on a permutation lemma of Brauer [5, Lemma 1] appears in [10, (12.3)].

To describe our result, let G^0 be the set of all p'-elements of G, i.e. of all elements whose order is not divisible by p; thus $G^0 = G$ if $p = 0$. Let n^0 be the least common multiple of the orders of the elements of G^0, and let ω be a primitive n^0-th root of unity in an algebraic closure E of F. For each F-automorphism σ of E, $\omega^\sigma = \omega^{m(\sigma)}$ where $m(\sigma)$ is an integer determined modulo n^0. Call two elements g, g' of G^0 *F-conjugate* if $g' = x^{-1}g^{m(\sigma)}x$ for some $x \in G$ and for some σ. In the group-algebra case, $k(A)$ is the number of F-conjugacy classes of elements of G^0. Our main theorem, Theorem 6, states that in general $k(A)$ is the number of such classes which satisfy a certain regularity condition.

The definition of F-conjugacy involves both (i) the inner automorphisms of G, which are permutations, and (ii) the permutations $g \mapsto g^{m(\sigma)}$ of G^0. The regularity condition involves some corresponding monomial transformations of the algebra A^E obtained from A by extending the field of scalars to E: namely (i) "inner automorphisms" $\mathbf{K}_A(x)$ of A^E (see (4.1)), which are monomial, and (ii) some monomial transformations $\mathbf{S}_A(\sigma)$ of A^E (see (6.4)). While the $\mathbf{K}_A(x)$ appeared implicitly in Schur's work, the $\mathbf{S}_A(\sigma)$ are new; in fact

Received September 23, 1968.
[1] This research was supported in part by National Science Foundation grants.

the construction and study of the latter are our main task. If $\mathcal{G}$ is the Galois group of E over F, then setting $\mathbf{D}_A(\sigma, x) = \mathbf{S}_A(\sigma)\mathbf{K}_A(x)$ yields a monomial representation of $\mathcal{G} \times G$ (see (8.1)), and the orbits of $\mathbf{D}_A$ composed of p'-elements are precisely the F-conjugate classes in G^0. Then the regularity condition for an orbit in the main theorem says in effect that $\mathbf{D}_A$ acts like a permutation representation on the orbit. This regularity condition is not what one might guess in the light of the previously known results: see the Corollary to Theorem 6.

Sections 2 and 3 are devoted mainly to establishing a viewpoint; we introduce a categorical approach for twisted group algebras for later use, and to be consistent we do the same for monomial representations. Sections 4 and 5 deal with results that we shall quote. In Sections 6 and 7, the heart of the paper, we study $\mathbf{S}_A(\sigma)$, and in Section 8 we quickly obtain the main theorem. In the final section we consider the special case where all $f(g, g')$ are roots of unity, and a partial reduction to this case due to Asano and Shoda [3]; this special case is the only one in which Schur's method of (finite) covering groups could be used. Throughout the paper the cases $p = 0$ and p prime are treated together by essentially the same arguments.

In a future paper we shall show that the restriction of $\mathbf{S}_A(\sigma)$ to the center of A^E is an algebra-automorphism, and use this fact together with some results from Section 9 to obtain some results on the number of blocks of A when p is prime.

2. Twisted group algebras

Throughout the paper, F will be a field of characteristic $p \geq 0$, and E will be a fixed algebraic closure of F.

Following Yamazaki's approach [22, p. 170], we can recast the definition of twisted group algebras as follows: a *twisted group algebra* over F is a triple $(A, G, (A_g))$ where A is an F-algebra with identity 1_A, G is a finite group, and (A_g) is a family of one-dimensional F-subspaces of A indexed by G such that $A = \oplus_{g \in G} A_g$ and $A_g A_{g'} = A_{gg'}$ for all $g, g' \in G$ (cf. the definitions given in a more general situation by Dade [8, p. 18] and Ward [20]). Of course A has dimension $|G|$, and it is easily seen that $1_A \in A_1$ where the subscript 1 means the identity of G. We often refer loosely to the algebra A as a twisted group algebra and write A in place of $(A, G, (A_g))$.

The class of all twisted group algebras over F becomes a category $\mathfrak{T}(F)$ if we define morphisms as follows (cf. [8, p. 26]): a morphism (M, μ) from $(A, G, (A_g))$ to $(A', G', (A'_g))$ consists of an algebra-homomorphism $M : A \rightarrow A'$ (with $1_A M = 1_{A'}$) and a group-homomorphism $\mu : G \rightarrow G'$ such that

$$A_g M \subseteq A'_{g\mu}, \qquad g \in G. \tag{2.1}$$

For example, if G' is any subgroup of G and if we set $A_{G'} = \oplus_{g' \in G'} A_{g'}$, then

$(A_{G'}, G', (A_{g'}))$ is a twisted group algebra, and the embeddings of $A_{G'}$ into A and of G' into G form a morphism.

The E-algebra $A^E = E \otimes_F A$ has a twisted group algebra structure $(A^E, G, (A_g^E))$ where $A_g^E = E \otimes_F A_g$; we usually regard A as being embedded in A^E. Each morphism (M, μ) of A to A' extends uniquely to a morphism (M^E, μ) of A^E to $(A')^E$, so that extension of the ground field is a functor from $\mathfrak{I}(F)$ to $\mathfrak{I}(E)$.

3. Monomial representations

By a *monomial space* over F we mean a triple $(V, S, (V_s))$ where V is a vector space over F, S is a finite set, and (V_s) is a family of one-dimensional F-subspaces of V indexed by S such that $V = \oplus_{s \in S} V_s$; thus the dimension of V equals the cardinality of S. These triples are the objects of a category $\mathfrak{M}(F)$ where a morphism from $(V, S, (V_s))$ to $(V', S', (V'_{s'}))$ is a pair (L, λ), where L is a linear transformation of V into V' and λ a mapping of S into S' such that $V_s L \subseteq V'_{s\lambda}$ for all $s \in S$. In particular, each subset S' of S determines a monomial space $(V_{S'}, S', (V_{s'}))$ where $V_{S'} = \oplus_{s' \in S'} V_{s'}$. There is a forgetful functor from $\mathfrak{I}(F)$ to $\mathfrak{M}(F)$ which drops the multiplications in A and G: in other words, each twisted group algebra over F can be regarded as a monomial space over F.

By a *monomial representation* of a finite or infinite group H on $(V, S, (V_s))$ we mean a homomorphism $h \mapsto (\mathbf{R}(h), \mathbf{r}(h))$ of H into the group of invertible morphisms from $(V, S, (V_s))$ to itself; we denote it by $(\mathbf{R}, \mathbf{r})$. (Usually $\mathbf{R}$ is called a monomial representation of H on V, and $\mathbf{r}$ is called the associated permutation representation of H on S: cf. [10, p. 44]; some authors allow only the case where $\mathbf{r}$ is transitive.) For each subset S' of S which is invariant under $\mathbf{r}$ there is a *subrepresentation* of $(\mathbf{R}, \mathbf{r})$ on $(V_{S'}, S', (V_{s'}))$ defined by restricting $\mathbf{R}$ and $\mathbf{r}$.

We shall be concerned with the *fixed-point space* of $\mathbf{R}$, i.e. the set of those $v \in V$ such that $v\mathbf{R}(h) = v$ for all $h \in H$. If $(\mathbf{R}_i, \mathbf{r}_i)$ is the subrepresentation of $(\mathbf{R}, \mathbf{r})$ determined by the orbit S_i of $\mathbf{r}$, then the fixed-point space of $\mathbf{R}$ is the direct sum of the fixed-point spaces of all the $\mathbf{R}_i$, while the dimensions of these spaces are all 0 or 1. Call S_i an $\mathbf{R}$-*regular orbit* of $\mathbf{r}$ if this dimension is 1. Thus:

LEMMA 1 (Cf. Berman [4, Lemma 3.1]). *The dimension of the fixed-point space of* $\mathbf{R}$ *is the number of* $\mathbf{R}$-*regular orbits of* $\mathbf{r}$.

This simple lemma will play a role analogous to Brauer's permutation lemma [5, Lemma 1], [10, (12.1)].

S_i is $\mathbf{R}$-regular if and only if there exists a basis $\{v_s : s \in S_i\}$ of V_{S_i} with $v_s \in V_s$ such that $\mathbf{R}_i$ acts as a permutation representation of G on this basis. It is possible to determine whether S_i is $\mathbf{R}$-regular by looking at a single element s_i of S_i, as follows. Let $H_i (\subseteq H)$ be the stability group of s_i under $\mathbf{r}$; then

[12, p. 582, Lemma 18.9] $\mathbf{R}_i$ is induced by a linear representation of H_i on V_{s_i}. Easily, S_i is R-regular if and only if this is the 1-representation of H_i, i.e. if and only if H_i is also the stability group of v_{s_i} under $\mathbf{R}$, where v_{s_i} is any non-zero element of V_{s_i}. In other words:

LEMMA 2. *S_i is $\mathbf{R}$-regular if and only if $v_{s_i}\mathbf{R}(h) \in V_{s_i}$ and $h \in H$ imply that $v_{s_i}\mathbf{R}(h) = v_{s_i}$.*

For any monomial space $(V, S, (V_s))$, the dual space V^* of V has a monomial space structure $(V^*, S, (V_s^*))$ where an element of V^* lies in V_s^* if and only if it annihilates $V_{s'}$ for all $s' \neq s$; thus if $\{v_s\}$ is a basis of V with $v_s \in V_s$ and if $\{v_s^*\}$ is the dual basis of V^*, then $v_s^* \in V_s^*$. If (L, λ) is an *invertible* morphism of $(V, S, (V_s))$ to itself, then (L^*, λ^{-1}) is a morphism of $(V^*, S, (V_s^*))$, where L^* is the linear transformation of V^* to V^* which is dual (i.e. transposed) to L. If $(\mathbf{R}, \mathbf{r})$ is a monomial representation of H on $(V, S, (V_s))$, then the *contragredient* monomial representation of H on $(V^*, S, (V_s^*))$ is defined to be $(\mathbf{R}^*, \mathbf{r})$ where $\mathbf{R}^*(h) = (\mathbf{R}(h^{-1}))^*$.

LEMMA 3. *An orbit of $\mathbf{r}$ is $\mathbf{R}^*$-regular if and only if it is $\mathbf{R}$-regular.*

4. Algebraically closed ground field

For any twisted group algebra $(A, G, (A_g))$ over F, each element x of G acts by "conjugation" on A^E as follows (and similarly on A): choose any non-zero element a_x of A_x, and set

$$a\mathbf{K}_A(x) = a_x^{-1}aa_x, \qquad a \in A^E. \tag{4.1}$$

Then $\mathbf{K}_A(x)$ is an algebra-automorphism of A^E, and is independent of the choice of a_x. If $\mathbf{k}_G(x)$ is the inner automorphism of G determined by x, i.e. if

$$g\mathbf{k}_G(x) = x^{-1}gx, \qquad x \in G, \tag{4.2}$$

then $(\mathbf{K}_A, \mathbf{k}_G)$ is a monomial representation of G on $(A^E, G, (A_g^E))$ regarded as a monomial space over E. Since the set G^0 of all p'-elements g^0 of G is invariant under $\mathbf{k}_G$, we have a subrepresentation $(\mathbf{K}_A^0, \mathbf{k}_G^0)$ on $((A^E)^0, G^0, (A_{g^0}^E))$ where $(A^E)^0 = (A^E)_{G^0}$; this in turn has a contragredient representation $(\mathbf{K}_A^{0*}, \mathbf{k}_G^0)$ on $((A^E)^{0*}, G^0, (A^E)_{g^0}^*)$.

The algebraically-closed case of our main theorem can be stated as follows:

THEOREM 1 (Schur [18, Theorem VI], Asano-Osima-Takahasi [2, Theorem 4]). *The number $k(A^E)$ of non-equivalent (absolutely) irreducible representations of A^E is equal to the number of $\mathbf{K}_A^0$-regular orbits of $\mathbf{k}_G^0$, i.e. the number of $\mathbf{K}_A$-regular conjugate classes of p'-elements of G.*

If p does not divide $|G|$, for example if $p = 0$, A^E is semisimple [6, p. 156], [22, Theorem 4.1], so that $k(A^E)$ is the dimension of the center of A^E; since this center is the fixed-point space of $\mathbf{K}_A = \mathbf{K}_A^0$, the theorem holds in this case by Lemma 1. For the general case we refer to [2] or to [6, p. 156]. (To check that our regularity condition is equivalent to that used by other authors, use Lemma 2.)

Let $\{\mathbf{F}_j : 1 \leq j \leq k(A^E)\}$ be a full set of non-equivalent irreducible repretations of A^E. By the *irreducible characters* of A^E we mean the traces $\phi_j = \operatorname{tr} \mathbf{F}_j$, which are elements of the dual space $(A^E)^*$ of A^E; observe that the values of ϕ_j lie in a field of characteristic p. Let ϕ_j^0 be the restriction of ϕ_j to $(A^E)^0$, so that $\phi_j^0 \in (A^E)^{0*}$. Then Theorem 1 has the following

COROLLARY. *$\{\phi_j^0 : 1 \leq j \leq k(A^E)\}$ is an E-basis of the fixed-point space U of $\mathbf{K}_A^{0*}$.*

Proof. By definition, for any $a \in (A^E)^0$ and $x \in G$,

$$(\phi_j^0 \mathbf{K}_A^{0*}(x))(a) = \phi_j^0(a(\mathbf{K}_A^0(x))^{-1}) = \operatorname{tr} \mathbf{F}_j(a_x a a_x^{-1}) = \operatorname{tr} \mathbf{F}_j(a) = \phi_j^0(a)$$

so that $\phi_j^0 \in U$. Now the ϕ_j^0 form a linearly independent set: this follows from the orthogonality relations for projective Brauer characters as given by Osima [15, (11.2)], applied to A^E and then reduced (if necessary) to characteristic p. Alternatively, it can be proved by combining the linear independence of the ϕ_j (cf. the proof of [7, (30.15)] with an analogue of the fact (cf. [7, (82.3)]) that in the group-algebra case ϕ_j is constant on each p'-section of G. Thus $\{\phi_j^0\}$ is a basis of a subspace of U of dimension $k(A^E)$. On the other hand, since the $\mathbf{K}_A^{0*}$-regular orbits of $\mathbf{k}_G^0$ are the same as the $\mathbf{K}_A^0$-regular orbits by Lemma 3, Theorem 1 shows that $k(A^E)$ is the dimension of U.

5. Extension of ground field

In this section, let A be any finite-dimensional algebra with 1 over F. Let $\mathcal{G}$ be the group of all F-automorphisms of E, i.e. the (infinite) Galois group of E over F. Define $\mathbf{F}_j$ and ϕ_j as in the preceding section. For each $\sigma \in \mathcal{G}$, let ϕ_j^σ be the mapping of A^E into E defined by $\phi_j^\sigma(a) = (\phi_j(a))^\sigma$, $a \in A^E$. In general ϕ_j^σ is not a character since it is only F-linear, not E-linear. However, the restriction $\phi_j^\sigma \mid A = (\phi_j \mid A)^\sigma$ is the trace of an irreducible representation of A over E, and is therefore the restriction of a uniquely determined irreducible character of A^E, which we shall call $\phi_j^{[\sigma]}$. Thus

$$\phi_j^{[\sigma]}(a) = (\phi_j(a))^\sigma, \qquad a \in A. \tag{5.1}$$

Clearly $(\phi_j^{[\sigma]})^{[\sigma']} = \phi_j^{[\sigma\sigma']}$, so that $\mathcal{G}$ acts as a permutation group on the irreducible characters ϕ_j.

Let $\{\mathbf{Z}_i : 1 \leq i \leq k(A)\}$ be a full set of non-equivalent irreducible representations of A (over F). The linear extension $\mathbf{Z}_i^E$ of each $\mathbf{Z}_i$ to a representation of A^E (over E) is reducible but not completely reducible in general; its irreducible constituents may be taken from $\{\mathbf{F}_j\}$. We paraphrase a theorem of Noether [14, p. 541, Zusammenfassung] which generalizes a result of Schur [19, Theorem VI].

THEOREM 2 (Schur, Noether). *The characters of all the irreducible constituents of $\mathbf{Z}_i^E$ are the elements of an orbit of the action of $\mathcal{G}$ on $\{\phi_j\}$, each appearing with the same multiplicity.*

For proof we refer to [14]. Fein [9, Theorem 1.2] has given a proof in the case that F is a perfect field; for the case of a group algebra over a perfect field see [7, (70.15)], [10, (11.4)], or [12, p. 546, Theorem 14.12]; for the case where A is commutative and F is arbitrary, see [17, Lemma 2]. It is not possible to avoid considering inseparable extensions even when A is a twisted group algebra: see the example in the last paragraph of [17]. On the other hand, the multiplicity in Theorem 2 is irrelevant for our purposes; in other words, we do not need to study the Schur index.

Since each $\mathbf{F}_j$ appears as a constituent of $\mathbf{Z}_i^E$ for exactly one i (cf. [12, p. 547, Theorem 14.13]), Theorem 2 establishes a bijection between the $\mathbf{Z}_i$ and the orbits of $\mathcal{G}$:

COROLLARY. *The number $k(A)$ of non-equivalent irreducible representations of the finite-dimensional F-algebra A with 1 is equal to the number of orbits of the action of $\mathcal{G}$ on the irreducible characters of A^E.*

6. Definition of $\mathbf{S}_A(\sigma)$

Again let $(A, G, (A_g))$ be a twisted group algebra over F. For each element σ of the Galois group $\mathcal{G}$ of E over F, we shall now define an E-linear transformation $\mathbf{S}_A(\sigma)$ of A^E onto A^E. The motivation of this definition will appear in the following section.

For each $g \in G$, choose $a_g \in A_g$, $a_g \neq 0$; then $\{a_g\}$ is an F-basis of A and an E-basis of A^E (cf. (1.1)). Choose a positive integer n divisible by the order of every element of G. Write $n = n_p n_{p'}$, where the factors are the p-part and p-regular part of n if p is prime, and where $n_p = 1$, $n_{p'} = n$ if $p = 0$. For each $\sigma \in \mathcal{G}$, choose[2] an integer $m(\sigma)$ such that

$$\omega^\sigma = \omega^{m(\sigma)} \tag{6.1}$$

for every $n_{p'}$-th root of unity $\omega \in E$, while

$$m(\sigma) \equiv 1 \pmod{n_p}; \tag{6.2}$$

$m(\sigma)$ is uniquely determined modulo n. Then

$$a_g^n = u(g)1_A \tag{6.3}$$

for some non-zero $u(g) \in E$ for each $g \in G$. Choose an element $v(g) \in E$ such that $v(g)^n = u(g)$. Having made these choices, define $\mathbf{S}_A(\sigma)$ for each $\sigma \in \mathcal{G}$ to be the unique E-linear transformation of A^E to A^E such that

[2] The requirements on $m(\sigma)$ are more stringent than those stated in the introduction.

$$a_g \mathbf{S}_A(\sigma) = (v(g)^{\sigma^{-1}}/v(g)^{m(\sigma^{-1})})a_g^{m(\sigma^{-1})}, \qquad g \in G. \tag{6.4}$$

(The presence of all the inverses here is explained by Theorem 5.)

We must show that $\mathbf{S}_A(\sigma)$ does not depend on the choices of a_g, n, $m(\sigma^{-1})$, and $v(g)$. If $m(\sigma^{-1})$ is changed without changing a_g, n, or $v(g)$, then a multiple of n is added to $m(\sigma^{-1})$, so that $a_g \mathbf{S}_A(\sigma)$ is multiplied by a power of $v(g)^{-n}a_g^n = 1_A$ and hence is unchanged. Similarly if $v(g)$ alone is changed, $v(g)$ is multiplied by an element ω of E such that $\omega^n = 1$; then $\omega^{n_{p'}} = 1$, and $a_g \mathbf{S}_A(\sigma)$ is multiplied by $\omega^{\sigma^{-1}}\omega^{-m(\sigma^{-1})}$, which is 1 by (6.1).

In changing n, we can suppose that the new choice of n is a multiple of the old, while a_g is unchanged. Then any choice of $m(\sigma^{-1})$ which satisfies (6.1) and (6.2) for the new n also satisfies them for the old n, and any choice of $v(g)$ for the old n also works for the new n (although $u(g)$ is changed). Then since n does not appear explicitly in (6.4), $\mathbf{S}_A(\sigma)$ is unchanged.

Finally if we replace a_g by $w(g)a_g$ where $0 \neq w(g) \in F$ without changing n or $m(\sigma^{-1})$, we must replace $u(g)$ by $w(g)^n u(g)$, and we can replace $v(g)$ by $w(g)v(g)$. Then each side of (6.4) is multiplied by $w(g)$, so that $\mathbf{S}_A(\sigma)$ is unchanged. Therefore $\mathbf{S}_A(\sigma)$ is well-defined.

$(\mathbf{S}_A(\sigma), \mathbf{s}_G(\sigma))$ is an invertible morphism of the monomial space $(A, G, (A_g))$, where we set

$$g\mathbf{s}_G(\sigma) = g^{m(\sigma^{-1})}, \qquad g \in G. \tag{6.5}$$

Remark. Although we have taken E to be an algebraic closure of F, our arguments will use only the following properties of E : E is a normal algebraic (not necessarily separable) extension of F, E contains a primitive $n_{p'}$-th root of 1 as well as $v(g)$ for all $g \in G$, and E is a splitting field for A^E; such fields exist which are also of finite degree over F. If the algebraic closure of F is replaced by such a field, $\mathcal{G}$ is replaced by a finite quotient group of itself while $\mathbf{S}_A(\mathcal{G}) = \{\mathbf{S}_A(\sigma) : \sigma \in \mathcal{G}\}$, which is a group by Theorem 5 below, is replaced by an isomorphic group. Hence $\mathbf{S}_A(\mathcal{G})$ is always finite.

7. Properties of $\mathbf{S}_A(\sigma)$

We continue the notations of Section 6, and assume whenever necessary that the choices required in the definition of $\mathbf{S}_A(\sigma)$ have been made. The following theorem will provide the main connection between the $\mathbf{S}_A(\sigma)$ and the problem of determining $k(A)$.

THEOREM 3. *For each irreducible character ϕ_j of A^E and each $\sigma \in \mathcal{G}$,*

$$\phi_j(a\mathbf{S}_A(\sigma)) = \phi_j^{[\sigma^{-1}]}(a), \qquad a \in A^E. \tag{7.1}$$

Proof. It suffices to take $a = a_g$. For fixed g and ϕ_j, let $\lambda_1, \lambda_2, \cdots$ be the characteristic roots of $\mathbf{F}_j(a_g)$. By (6.3), $\lambda_i^n = u(g)$, so that $\lambda_i = v(g)\omega_i$ where $\omega_i^{n_{p'}} = 1$. Setting $\tau = \sigma^{-1}$, by (6.1)

$$\phi_j^{[\tau]}(a_g) = (\operatorname{tr} \mathbf{F}_j(a_g))^\tau = (\textstyle\sum_i \lambda_i)^\tau = v(g)^\tau \sum_i \omega_i^\tau = v(g)^\tau \sum_i \omega_i^{m(\tau)};$$

on the other hand, by (5.1)

$$\begin{aligned}\phi_j(a_g\, \mathbf{S}_A(\sigma)) &= (v(g)^\tau/v(g)^{m(\tau)}) \operatorname{tr} (\mathbf{F}_j(a_g))^{m(\tau)} \\ &= (v(g)^\tau/v(g)^{m(\tau)}) \textstyle\sum_i \lambda_i^{m(\tau)} \\ &= v(g)^\tau \textstyle\sum_i \omega_i^{m(\tau)}.\end{aligned}$$

The property expressed in Theorem 3 is not enough to characterize $\mathbf{S}_A(\sigma)$ in general, but the following theorem and its corollary provide characterizations.

THEOREM 4. *For any fixed* $\sigma \in \mathcal{G}$, *the mapping*

$$\mathfrak{S}(\sigma) : A \mapsto \mathbf{S}_A(\sigma)$$

of objects $A = (A, G, (A_g))$ *of* $\mathfrak{Z}(F)$ *to E-linear transformations of* A^E *to* A^E *is characterized by the following four conditions*:

(a) *For each morphism* (M, μ) *of* A *to* A' *in* $\mathfrak{Z}(F)$,

$$\mathbf{S}_A(\sigma)M^E = M^E\mathbf{S}_{A'}(\sigma).$$

(b) *For each irreducible character of* ϕ_j *of* A^E,

$$\phi_j(a\mathbf{S}_A(\sigma)) = \phi_j^{[\sigma^{-1}]}(a), \qquad a \in A^E.$$

(c) *If* G *is cyclic, then* $\mathbf{S}_A(\sigma)$ *is an algebra-automorphism of* A^E.

(d) *If the characteristic* p *of* F *is prime and if* G *is a* p*-group, then* $\mathbf{S}_A(\sigma)$ *is the identity mapping.*

Proof. First we show that $\mathfrak{S}(\sigma)$ satisfies the four conditions. Condition (b) is a restatement of Theorem 3. As for (a), in defining $\mathbf{S}_A(\sigma)$ and $\mathbf{S}_{A'}(\sigma)$ we can assume that $n = n'$ and $m(\sigma^{-1}) = m'(\sigma^{-1})$, and that for any fixed $g \in G$ we have $a'_{g\mu} = a_g M = a_g M^E$. (The meaning of the primes should be clear.) Then $u'(g\mu) = u(g)$, so that we can take $v'(g\mu) = v(g)$. Then (a) follows from (6.4).

Observe that (a) implies that if G' is a subgroup of G and if $A' = A_{G'}$ as in Section 2, then $\mathbf{S}_{A'}(\sigma)$ is the restriction of $\mathbf{S}_A(\sigma)$ to $A^E_{G'} = (A^E)_{G'}$.

Suppose that G is cyclic, with a fixed generator g. We can choose $n = |G|$; then the algebra A^E is isomorphic to the polynomial algebra $E[X]$ modulo the ideal $(X^{|G|} - u(g))$. To prove (c) it suffices to show that

$$a_g^i\, \mathbf{S}_A(\sigma) = (a_g\, \mathbf{S}_A(\sigma))^i, \qquad 1 \leq i \leq |G|. \tag{7.2}$$

We can suppose that $a_{g^i} = a_g^i$ for these values of i. Then $u(g^i) = (u(g))^i$, so that we can choose $v(g^i) = (v(g))^i$; now (6.4) implies (7.2).

Finally, suppose that G is a p-group; take $n = n_p = |G|$. By (6.2), we can take $m(\sigma^{-1}) = 1$. Since $v(g)^{|G|} \in F$ for every $g \in G$, $v(g)$ is purely inseparable over F, so that $(v(g))^{\sigma^{-1}} = v(g)$. Then (6.4) shows that $a_g\, \mathbf{S}_A(\sigma) = a_g$, which proves (d).

Conversely, let $\mathfrak{T}(\sigma) : A \mapsto \mathbf{T}_A(\sigma)$ be any mapping which satisfies the analogues of (a) through (d); we want to show that $\mathbf{T}_A(\sigma) = \mathbf{S}_A(\sigma)$ for all A. It suffices to show that $a_g \mathbf{T}_A(\sigma) = a_g \mathbf{S}_A(\sigma)$ for each $g \in G$. Since the analogue of (a) implies that $\mathbf{T}_{A'}(\sigma)$ is the restriction of $\mathbf{T}_A(\sigma)$ if $A' = A_{\langle g \rangle}$ where $\langle g \rangle$ is the cyclic group generated by g, we can suppose without loss of generality that G is cyclic. Then $G = G' \times G''$ where G' is a cyclic p-group and G'' is a cyclic p'-group, and the analogues of (a), (c), and (d) show that $\mathbf{T}_A(\sigma)$ is completely determined by $\mathbf{T}_{A''}(\sigma)$ where $A'' = A_{G''}$; hence we can suppose that G is a cyclic p'-group. (For $p = 0$, we define that a p-group is a group of order 1, and that every finite group is a p'-group.) In this case A^E is a commutative semisimple [6, p. 156] algebra over an algebraically closed field, so that the ϕ_j form a basis of $(A^E)^*$. Then (b) and its analogue imply that $\mathbf{T}_A(\sigma) = \mathbf{S}_A(\sigma)$, which completes the proof.

Remark. We can express condition (a) in categorical terminology as follows. Let Φ be the functor from $\mathfrak{J}(F)$ to the category of all finite-dimensional E-spaces which sends each object $(A, G, (A_g))$ to A^E, and each morphism (M, μ) to M^E. By [13, p. 62, Proposition 10.3], we can suppose that Φ carries distinct objects to distinct objects. (Here we do not regard A as embedded in A^E, and we speak a bit loosely besides.) We can now regard Φ as a morphism of $\mathfrak{J}(F)$ to its image category Im Φ [13, p. 62]. Then (a) says precisely that the mapping $\mathfrak{S}(\sigma)$ is a natural transformation of Φ to Φ; since $\mathbf{S}_A(\sigma)$ is invertible, $\mathfrak{S}(\sigma)$ is actually a natural equivalence. Then (b), (c), and (d) provide a characterization of this natural equivalence. A similar result holds with Φ replaced by a functor from $\mathfrak{J}(\mathrm{F})$ to $\mathfrak{M}(E)$.

I wish to thank my colleagues J. W. Schlesinger and D. C. Newell for help concerning this remark.

The proof of Theorem 4 also yields the following variant.

COROLLARY. *Let $(A, G, (A_g))$ be a fixed twisted group algebra over F, and let $\sigma \in \mathcal{G}$. Then $\mathbf{S}_A(\sigma)$ is the unique E-linear transformation of A^E to A^E such that the following hold.*

(e) *For each cyclic subgroup $\langle g \rangle$ of G, the restriction of $\mathbf{S}_A(\sigma)$ to $A^E_{\langle g \rangle}$ is an algebra-automorphism of $A^E_{\langle g \rangle}$.*

(f) *For each cyclic p'-subgroup $\langle g \rangle$ of G,*

$$\psi_j(a\mathbf{S}_A(\sigma)) = \psi_j^{[\sigma^{-1}]}(a)$$

whenever $a \in A^E_{\langle g \rangle}$ and ψ_j is an irreducible character of $A^E_{\langle g \rangle}$.

(g) *For each p-element g of G, $\mathbf{S}_A(\sigma)$ fixes every element of the subspace A^E_g of A^E.*

The characterization of $\mathbf{S}_A(\sigma)$ leads to the following important property.

THEOREM 5. *For each twisted group algebra $(A, G, (A_g))$ over F, the mapping*

$$(\mathbf{S}_A, \mathbf{s}_G) : \sigma \mapsto (\mathbf{S}_A(\sigma), \mathbf{s}_G(\sigma))$$

is a monomial representation of $\mathcal{G}$ on the monomial E-space $(A^E, G, (A^E_g))$.

Proof. Since $\mathbf{S}_A(1)$ is the identity, we need only show that if $\sigma, \sigma' \in \mathcal{G}$, the mapping $A \mapsto \mathbf{S}_A(\sigma)\mathbf{S}_A(\sigma')$ satisfies the four conditions of Theorem 4 for $\mathbf{S}_A(\sigma\sigma')$. Only (b) requires an explicit calculation: let $\tau = \sigma^{-1}$, $\tau' = (\sigma')^{-1}$; then

$$\phi_j(a\mathbf{S}_A(\sigma)\mathbf{S}_A(\sigma')) = \phi_j^{[\tau']}(a\mathbf{S}_A(\sigma)) = (\phi_j^{[\tau']})^{[\tau]}(a) = \phi_j^{[\tau'\tau]}(a).$$

8. The main theorem

Let $(A, G, (A_g))$ be a twisted group algebra over F. We have found monomial representations $(\mathbf{S}_A, \mathbf{s}_G)$ and $(\mathbf{K}_A, \mathbf{k}_G)$ of $\mathcal{G}$ and G respectively on the same space $(A^E, G, (A_g^E))$, by Theorem 5 and Section 4. By applying (a) of Theorem 4 to the morphism $(\mathbf{K}_A(x) \mid A, \mathbf{k}_G(x))$ of A to A, we can define a monomial representation $(\mathbf{D}_A, \mathbf{d}_G)$ of the abstract direct product $\mathcal{G} \times G$ on the same space by setting

$$\mathbf{D}_A(\sigma, x) = \mathbf{S}_A(\sigma)\mathbf{K}_A(x) = \mathbf{K}_A(x)\mathbf{S}_A(\sigma), \tag{8.1}$$

$$\mathbf{d}_G(\sigma, x) = \mathbf{s}_G(\sigma)\mathbf{k}_G(x) = \mathbf{k}_G(x)\mathbf{s}_G(\sigma) \tag{8.2}$$

for all $\sigma \in \mathcal{G}$, $x \in G$. Thus

$$g\mathbf{d}_G(\sigma, x) = x^{-1}g^{m(\sigma^{-1})}x, \qquad g \in G. \tag{8.3}$$

As in Section 4, we have subrepresentations $(\mathbf{S}_A^0, \mathbf{s}_G^0)$, $(\mathbf{K}_A^0, \mathbf{k}_G^0)$, and $(\mathbf{D}_A^0, \mathbf{d}_G^0)$ on $((A^E)^0, G^0, (A_{g^0}^E))$ and their contragredients $(\mathbf{S}_A^{0*}, \mathbf{s}_G^0)$, etc. Now we can state the main theorem.

THEOREM 6. *The number $k(A)$ of non-equivalent irreducible representations of the twisted group algebra A is equal to the number of $\mathbf{D}_A^0$-regular orbits of $\mathbf{d}_G^0$, i.e. the number of $\mathbf{D}_A$-regular F-conjugacy classes of p'-elements of G.*

Proof. (7.1) implies that $\phi_j^0\, \mathbf{S}_A^{0*}(\tau) = (\phi_j^{[\tau]})^0$ for all $\tau \in \mathcal{G}$; thus $\mathbf{S}_A^{0*}(\tau)$ permutes the set $\{\phi_j^0\}$ in the same way that τ permutes $\{\phi_j\}$ in (5.1). Then the mapping $\tau \mapsto \mathbf{S}_A^{0*}(\tau) \mid U$ is a permutation representation of $\mathcal{G}$ on the space U of the corollary to Theorem 1; in other words the family $(\phi_j^0 E)$ of subspaces of U defines a monomial-space structure on U indexed by $\{\phi_j\}$ on which $\mathbf{S}_A^{0*}$ yields a monomial representation of $\mathcal{G}$ with all orbits regular. By the Corollary to Theorem 2, $k(A)$ is the number of orbits of $\mathcal{G}$ on $\{\phi_j\}$; by Lemma 1, this is the dimension of the fixed-point space W of the restriction of $\mathbf{S}_A^{0*}$ to U. Since U is in turn the fixed-point space of $\mathbf{K}_A^{0*}$, W consists of those elements of $(A^E)^{0*}$ which are fixed by both $\mathbf{K}_A^{0*}$ and $\mathbf{S}_A^{0*}$, i.e. W is the fixed-point space of $\mathbf{D}_A^{0*}$. Then Lemmas 1 and 3 imply that $k(A)$ is the number of $\mathbf{D}_A^0$-regular orbits of $\mathbf{d}_G^0$. To see that these orbits coincide with F-conjugacy classes, use the fact that the integer n^0 of the Introduction can be taken as n in defining $\mathbf{s}_G(\sigma) \mid \langle g \rangle$ for p'-elements G.

If A is a group algebra, then all F-conjugacy classes are $\mathbf{D}_A$-regular, so that Theorem 6 implies the known results in this case. Theorem 6 also implies Theorem 1.

COROLLARY. *$k(A)$ is less than or equal to the number of F-conjugacy classes of p'-elements of G which are unions of $\mathbf{K}_A$-regular conjugacy classes.*

An example of strict inequality here is provided by taking G cyclic of order 4 and $A = \mathbf{Q}[X]/(X^4 + 1)$ as in the discussion preceding (7.2): all three $\mathbf{Q}$-conjugacy classes are $\mathbf{K}_A$-regular, but $k(A) = 1$ since A is a field.

9. Relationships with a special case

The definition (6.4) of $\mathbf{S}_A(\sigma)$ can be simplified in the special case where the a_g in (1.1) can be chosen in such a way that all $f(g, g')$ are l-th roots of 1 for some positive integer l, i.e. such that

$$f^l = 1 \tag{9.1}$$

for the 2-cocycle $f \in Z^2(G, F^\times)$. (Here $F^\times$ is the multiplicative group of F, the action of G on $F^\times$ is trivial, and the notation is multiplicative.) Since $a_g^e \in A_1$ where e is the exponent of G, (9.1) implies that $a_g^{el} = 1_A$ for all $g \in G$. Then in (6.3) we can choose n so that $a_g^n = 1_A$ for all g. For such n we can take $v(g) = 1$, so that (6.4) becomes

$$a_g\, \mathbf{S}_A(\sigma) = a_g^{m(\sigma-1)}, \qquad g \in G. \tag{9.2}$$

Since $m(\sigma\sigma') \equiv m(\sigma)m(\sigma') \equiv m(\sigma'\sigma) \pmod{n}$ by (6.1) and (6.2), (9.2) implies that the group $\mathbf{S}_A(\mathcal{G})$ is abelian whenever (9.1) holds. In general $\mathbf{S}_A(\mathcal{G})$ can be non-abelian, e.g. for $A = \mathbf{Q}[X]/(X^3 - 2) \cong \mathbf{Q}(\sqrt[3]{2})$, $\mathbf{S}_A(\mathcal{G})$ is the symmetric group on 3 letters.

For an arbitrary twisted group algebra $A = (A, G, (A_g))$, a construction due to Asano and Shoda produces a related twisted group algebra $A^\#$ (not unique in general) which satisfies the condition of the previous paragraph, as follows. Choose $\{a_g\}$ as in (1.1). As Schur showed in [18] (cf. [7, p. 360]), the order r of the cohomology class $fB^2(G, E^\times)$ of f in $H^2(G, E^\times)$ divides the p'-part of $|G|$, and this class contains at least one 2-cocycle $f^\# \in Z^2(G, E^\times)$ of the same order r. Asano and Shoda [3, p. 237, lines 15 and 16] proved that in fact

$$f^\# \in Z^2(G, F^\times). \tag{9.3}$$

It seems worthwhile to give a proof of (9.3) that (unlike the original proof) avoids using covering groups. Let

$$f^\# = (\delta c)f,\ c \in C^1(G, E^\times);$$

for $\sigma \in \mathcal{G}$ define f^σ by $f^\sigma(g, g') = f(g, g')^\sigma$, etc. Then $(f^\#)^\sigma = (\delta c)^\sigma f^\sigma = \delta(c^\sigma)f = \delta(c^\sigma c^{-1})f^\#$. Since $(f^\#)^r = 1$, $f^\#(g, g')$ is separable over F, and there is an integer $q(\sigma)$ such that $f^\#(g, g')^\sigma = f^\#(g, g')^{q(\sigma)}$ for all $g, g' \in G$. Hence $f^\#$ is cohomologous to $(f^\#)^\sigma = (f^\#)^{q(\sigma)}$ over E, and by the assumption on orders $f^\# = (f^\#)^{q(\sigma)}$; i.e. $f^\# = (f^\#)^\sigma$ for all σ, so that $f^\#(g, g') \in F$ as stated.

If we set $a_g^\# = c(g)a_g \in A^E (\supseteq A)$, then $a_g^\# a_{g'}^\# = f^\#(g, g')a_{gg'}^\#$, and by (9.3)

$\{a_g^\#\}$ is an F-basis of a twisted group algebra $A^\#$ over F, with $(A^\#)^E = A^E$ as twisted group algebras. Although $k(A^\#) \neq k(A)$ in general, as for $A \cong \mathbf{Q}(\sqrt[3]{2})$, we shall use $A^\#$ to gain information about A in a future paper.

If we choose n divisible by the orders of all $a_g^\#$ in the definition of $\mathbf{S}_A(\sigma)$, then $c(g)^n a_g^n = 1_A$, so that we can take $v(g) = c(g)^{-1}$ in (6.4). In particular this is true if we take $n = |G|$, for by a result of Alperin and Kuo [1, p. 412, lines 5 and 6], *er* divides $|G|$, so that

$$(a_g^\#)^{|G|} = 1_{A^\#} = 1_A \tag{9.4}$$

by the discussion preceding (9.2). Furthermore if for the moment we let E be any normal algebraic extension of F which contains a primitive $|G|_{p'}$-th root of 1 as well as all $c(g)$, then E will fulfill the requirements of the remark in Section 6: for by the proof of [16, Theorem] (see also [1, Theorem 2] or [12, p. 641, Theorem 24.6]), E is a splitting field for $(A^\#)^E = A^E$ (and similarly for $A_{G'}^E$, for all subgroups G' of G). This argument uses the fact that the 2-cocycles used in the proof of [16, Theorem] are defined in the same way as our $f^\#$; note that that theorem does not say that every twisted group algebra for G over the field of $|G|$-th roots of 1 has this field as a splitting field, cf. $\mathbf{Q}(i)$!

Although $\mathbf{S}_A \neq \mathbf{S}_{A^\#}$ in general, we do have agreement on the p'-commutator subgroup $G'(p')$ of G, i.e. the intersection of all normal subgroups of G whose factor group is an abelian p'-group, as follows. In the proof of (9.3), $\delta(c^\sigma c^{-1}) = 1$, so that $c^\sigma c^{-1}$ is a homomorphism of G into $E^\times$. Then $c(g)^\sigma = c(g)$ for all $g \in G'(p')$. Taking $n = |G|$ and $v(g) = c(g)^{-1}$, (6.4) yields

$$a_g\,\mathbf{S}_A(\sigma) = (c(g)^{m(\sigma^{-1})}/c(g))a_g^{m(\sigma^{-1})}, \qquad g \in G'(p').$$

This says that $a_g^\#\mathbf{S}_A(\sigma) = (a_g^\#)^{m(\sigma^{-1})}$, and by (9.2) for $A^\#$,

$$\mathbf{S}_A(\sigma) \mid A_{G'(p')}^E = \mathbf{S}_{A^\#}(\sigma) \mid A_{G'(p')}^E. \tag{9.5}$$

If also F is a perfect field, then $c(g) \in F$ for these g, so that $A_{G'(p')}^\# = A_{G'(p')}$. These results are analogous to a result of Schur [18, Theorem 3], [12, p. 634, Theorem 23.6].

References

1. J. L. Alperin and Tzee-Nan Kuo, *The exponent and the projective representations of a finite group*, Illinois J. Math., vol. 11 (1967), pp. 410–413.
2. K. Asano, M. Osima, and M. Takahasi, *Über die Darstellung von Gruppen durch Kollineationen im Körper der Charakteristik p*, Proc. Phys.-Math. Soc. Japan (3), vol. 19 (1937), pp. 199–209.
3. K. Asano and K. Shoda, *Zur Theorie der Darstellungen einer endlichen Gruppe durch Kollineationen*, Compositio Math., vol. 2 (1935), pp. 230–240.
4. S. D. Berman, *Characters of linear representations of finite groups over an arbitrary field*, Mat. Sb., vol. 44 (1958), pp. 409–456. (Russian)
5. R. Brauer, *On the connection between the ordinary and the modular characters of groups of finite order*, Ann. of Math., vol. 42 (1941), pp. 926–935.
6. S. B. Conlon, *Twisted group algebras and their representations*, J. Austral. Math. Soc., vol. 4 (1964), pp. 152–173.

7. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962.
8. E. C. Dade, *Characters and solvable groups*, mimeographed notes, Univ. of Illinois, Urbana, 1968.
9. B. Fein, *The Schur index for projective representations of finite groups*, Pacific J. Math., vol. 28 (1969), pp. 87–100.
10. W. Feit, *Characters of finite groups*, Benjamin, New York, 1967.
11. G. Frobenius and I. Schur, *Über die reellen Darstellungen der endlichen Gruppen*, S.-B. Preussischen Akad. Wiss. Berlin, 1906, pp. 186–208; reprinted in F. G. Frobenius, *Gesammelte Abhandlungen*, vol. 3, Springer, Berlin, 1968, pp. 355–377.
12. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
13. B. Mitchell, *Theory of categories*, Academic Press, New York, 1965.
14. E. Noether, *Nichtkommutative Algebra*, Math. Zeitschr., vol. 37 (1933), pp. 514–541.
15. M. Osima, *On the representations of groups of finite order*, Math. J. Okayama Univ., vol. 1 (1952), pp. 33–61.
16. W. F. Reynolds, *Projective representations of finite groups in cyclotomic fields*, Illinois J. Math., vol. 9 (1965), pp. 191–198.
17. ———, *Block idempotents and normal p-subgroups*, Nagoya Math. J., vol. 28 (1966), pp. 1–13.
18. I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math., vol. 127 (1904), pp. 20–50.
19. ———, *Beiträge zur Theorie der Gruppen linearer homogener Substitutionen*, Trans. Amer. Math. Soc., vol. 10 (1909), pp. 159–175.
20. H. N. Ward, *The analysis of representations induced from a normal subgroup*, Michigan Math. J., vol. 15 (1968), pp. 417–428.
21. E. Witt, *Die algebraische Struktur des Gruppenringes einer endlichen Gruppe über einem Zahlkörper*, J. Reine Angew. Math., vol. 190 (1952), pp. 231–245.
22. K. Yamazaki, *On projective representations and ring extensions of finite groups*, J. Fac. Sci. Univ. Tokyo Sect. I, vol. 10 (1964), pp. 147–195.

Tufts University
Medford, Massachusetts