JOURNAL OF ALGEBRA **194,** 496–520 (1997)
ARTICLE NO. JA966929

Semisimplicity and Tensor Products of Group Representations: Converse Theorems

Jean-Pierre Serre

Collège de France, 3 rue d'Ulm, F-75005 Paris

With an appendix by Walter Feit

Department of Mathematics, Yale University, New Haven, Connecticut 06520-8283

Communicated by Efin Zelmanov

Received October 8, 1996

INTRODUCTION

Let k be a field of characteristic $p \geq 0$, and let G be a group. If V and W are finite-dimensional G-modules, it is known that:

(1) *V and W semisimple* $\Rightarrow$ *$V \otimes W$ semisimple if $p = 0$* ([2], p. 88), *or if $p > 0$ and* $\dim V + \dim W < p + 2$ ([6], Corollary 1 to Theorem 1.)

(2) *V semisimple* $\Rightarrow$ *$\wedge^2 V$ semisimple if $p = 0$ or if $p > 0$ and* $\dim V \leq (p + 3)/2$ (cf. [6], Theorem 2).

We are interested here in "converse theorems": proving the semisimplicity of V from that of $V \otimes W$ or of $\wedge^2 V$. The results are the following (cf. Sects. 2, 3, 4, 5):

(3) *$V \otimes W$ semisimple* $\Rightarrow$ *V semisimple if* $\dim W \not\equiv 0 \pmod{p}$.

(4) *$\otimes^m V$ semisimple* $\Rightarrow$ *V semisimple if $m \geq 1$.*

(5) *$\wedge^2 V$ semisimple* $\Rightarrow$ *V semisimple if* $\dim V \not\equiv 2 \pmod{p}$.

(6) *$\mathrm{Sym}^2 V$ semisimple* $\Rightarrow$ *V semisimple if* $\dim V \not\equiv -2 \pmod{p}$.

(7) *$\wedge^m V$ semisimple* $\Rightarrow$ *V semisimple if* $\dim V \not\equiv 2, 3, \ldots, m \pmod{p}$.

0021-8693/97 $25.00

Examples show that the congruence conditions occurring in (3), (5), (6), and (7) cannot be suppressed: see Sect. 7 for (3), (5), and (7) and the Appendix for (5) and (6). These examples are due to (or inspired by) W. Feit.

1. NOTATION

1.1. *The Category C_G*

As in the Introduction, G is a group and k is a field; we put $\mathrm{char}(k) = p$. The category of $k[G]$-modules of finite dimension over k is denoted by C_G. If V and W are objects of C_G, the k-vector space of C_G-morphisms of V into W is denoted by $\mathrm{Hom}^G(V, W)$.

1.2. *Split Injections*

A C_G-morphism $f: V \to W$ is called a *split injection* if there exists a left inverse $r: W \to V$ which is a C_G-morphism. This means that f is injective, and that its image is a direct factor of W, viewed as a $k[G]$-module. We also say that f is *split*.

If $f: V_1 \to V_2$ and $g: V_2 \to V_3$ are split injections, so is $g \circ f$. Conversely, if $g \circ f$ is a split injection, so is f.

An object W of C_G is *semisimple* if and only if every injection $V \to W$ is split.

1.3. *Tensor Products*

The tensor product (over k) of two objects V and V' of C_G is denoted by $V \otimes V'$.

If $V \to W$ and $V' \to W'$ are split injections, so is $V \otimes V' \to W \otimes W'$.

The vector space k, with trivial action of G, is denoted by $\underline{1}$. We have $\underline{1} \otimes V = V$ for every V.

1.4. *Duality*

The dual of an object V of C_G is denoted by V^*. If W is an object of C_G, one has $W \otimes V^* = \mathrm{Hom}_k(V, W)$, the action of G on $\mathrm{Hom}_k(V, W)$ being $f \mapsto sfs^{-1}$ for $s \in G$. An element f of $\mathrm{Hom}_k(V, W)$ is G-linear (i.e., belongs to $\mathrm{Hom}^G(V, W)$) if and only if it is fixed under the action of G.

In particular, one has $V \otimes V^* = \mathrm{End}_k(V)$. The unit element 1_V of $\mathrm{End}_k(V)$ defines a G-linear map $i_V: \underline{1} \to V \otimes V^*$, which is injective if $V \neq 0$.

1.5. *Trace*

The trace $t_V\colon V \otimes V^* \to \underline{1}$ is a G-linear map. The composite map

$$t_V \circ i_V\colon \underline{1} \to V \otimes V^* \to \underline{1}$$

is equal to $\dim V$, viewed as an element of $k = \mathrm{End}^G(\underline{1})$; it is 0 if and only if $\dim V \equiv 0 \pmod p$. (When $p = 0$ this just means $\dim V = 0$.)

2. FROM $V \otimes W$ TO V

Let V and W be two objects of C_G.

PROPOSITION 2.1. *Let V' be a subobject of V. Assume*:

$$i_W\colon \underline{1} \to W \otimes W^* \qquad \textit{is a split injection}, \tag{2.1.1}$$

and

$$V' \otimes W \to V \otimes W \qquad \textit{is a split injection}. \tag{2.1.2}$$

Then $V' \to V$ is a split injection.

Proof. Consider the commutative diagram:

$$\begin{tikzcd} V' \arrow[r, "\beta'"] \arrow[d, "\alpha"'] & V' \otimes W \otimes W^* \arrow[d, "\gamma"] \\ V \arrow[r, "\beta"] & V \otimes W \otimes W^*, \end{tikzcd}$$

where the vertical maps come from the injection $V' \to V$ and the horizontal maps are $\beta = 1_V \otimes i_W$ and $\beta' = 1_{V'} \otimes i_W$ (cf. Sect. 1.5). By (2.1.1), β' is split; by (2.1.2), $V' \otimes W \to V \otimes W$ is split, and the same is true for γ. Hence $\beta \circ \alpha = \gamma \circ \beta'$ is split, and this implies that α is split.

Remark 2.2. Assumption (2.1.1) is true in each of the following two cases:

(2.2.1) *When* $\dim W \not\equiv 0 \pmod p$, i.e., when $\dim W$ is invertible in k. Indeed, if c denotes the inverse of $\dim W$ in k, the map

$$c \cdot t_W\colon W \otimes W^* \to \underline{1}$$

is a left inverse of i_W (cf. Sect. 1.5).

(2.2.2) *When $W \neq 0$ and $W \otimes W^*$ is semisimple*, since in that case every injection in $W \otimes W^*$ is split.

PROPOSITION 2.3. *Assume* (2.1.1) *and that $V \otimes W$ is semisimple. Then V is semisimple.*

Proof. Let V' be a subobject of V. Since $V \otimes W$ is semisimple, the injection $V' \otimes W \to V \otimes W$ is split, hence (2.1.2) is true, and Proposition 2.1 shows that $V' \to V$ splits. Since this is true for every V', it follows that V is semisimple.

Alternate proof (sketch). One uses (2.1.1) to show that the natural map

$$H^n(G, \mathrm{Hom}_k(V_1, V_2)) \to H^n(G, \mathrm{Hom}_k(V_1 \otimes W, V_2 \otimes W))$$

is injective for every n, V_1, V_2. If V is an extension of V_1 by V_2 and (V) denotes the corresponding element of the group $\mathrm{Ext}(V_1, V_2) = H^1(G, \mathrm{Hom}_k(V_1, V_2))$, the assumption that $V \otimes W$ is semisimple implies that (V) gives 0 in $\mathrm{Ext}(V_1 \otimes W, V_2 \otimes W)$ and hence $(V) = 0$. This shows that V is semisimple.

THEOREM 2.4. *If $V \otimes W$ is semisimple and* $\dim W \not\equiv 0 \pmod p$, *then V is semisimple.*

Proof. This follows from Proposition 2.3 and Remark (2.2.1).

Remark. The condition $\dim W \not\equiv 0 \pmod p$ of Theorem 2.4 cannot be suppressed. This is clear for $p = 0$, since it just means $W \neq 0$; for $p > 0$, see Feit's examples in Sect. 7.2.

3. FROM $\mathbf{T}^n V \otimes \mathbf{T}^m V^*$ TO V

Let V be an object of C_G.

LEMMA 3.1. *The injection $j_V = 1_V \otimes i_V \colon V \to V \otimes V \otimes V^*$ is split.*

Proof. If we identify $V \otimes V^*$ with $\mathrm{End}_k(V)$, the map

$$j_V \colon V \to V \otimes \mathrm{End}_k(V)$$

is the map $x \mapsto x \otimes 1_V$. Let $f_V \colon V \otimes \mathrm{End}_k(V) \to V$ be the "evaluation map" $x \mapsto \varphi(x)$ $(x \in V,\ \varphi \in \mathrm{End}_k(V))$. It is clear that $f_V \circ j_V = 1_V$. Hence j_V is a split injection.

If $n \geq 0$, let us write $\mathbf{T}^n V$ for the tensor product $V \otimes V \otimes \cdots \otimes V$ of n copies of V, with the convention that $\mathbf{T}^0 V = \underline{1}$.

PROPOSITION 3.2. *Let V' be a subobject of V. Assume that the natural injection of $\mathbf{T}^n V' = V' \otimes \mathbf{T}^{n-1} V'$ in $V \otimes \mathbf{T}^{n-1} V'$ splits for some $n \geq 1$. Then $V' \to V$ splits.*

Proof. This is clear if $n = 1$. Assume $n \geq 2$, and use induction on n. We have a commutative diagram:

$$\begin{array}{ccc}
\mathbf{T}^{n-1}V' & \xrightarrow{\lambda} & V \otimes \mathbf{T}^{n-2}V' \\
\downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\beta} \\
\mathbf{T}^{n-1}V' \otimes V' \otimes V'^* & \xrightarrow{\mu} & V \otimes \mathbf{T}^{n-2}V' \otimes V' \otimes V'^*,
\end{array}$$

where the horizontal maps are the obvious injections, and the vertical ones are of the form $x \mapsto x \otimes 1_{V'}$, with $1_{V'} \in V' \otimes V'^*$ (cf. Sect 1.4).

If we put $W = \mathbf{T}^{n-2}V'$, we may write γ as $1_W \otimes j_{V'}$, where $j_{V'}$ is the map of V' into $V' \otimes V' \otimes V'^*$ defined in Lemma 3.1 (with V replaced by V'). From this lemma, and from Sect. 1.3, it follows that γ is a split injection. On the other hand, μ is the tensor product of the natural injection $\mathbf{T}^nV' \to V \otimes \mathbf{T}^{n-1}V'$, which is split by assumption, with the identity map of V'^*; hence μ is split and the same is true for $\beta \circ \lambda = \mu \circ \gamma$, hence also for λ. By the induction assumption this shows that $V' \to V$ is a split injection.

THEOREM 3.3. *Assume that $\mathbf{T}^nV \otimes \mathbf{T}^mV^*$ is semisimple for some integers $n, m \geq 0$, not both 0. Then V is semisimple.*

COROLLARY 3.4. *If $\mathbf{T}^nV$ is semisimple for some $n \geq 1$, then V is semisimple.*

Proof of Theorem 3.3. Consider first the case of Corollary 3.4, i.e., $m = 0$, $n \geq 1$. Let V' be a subobject of V. Then $V \otimes \mathbf{T}^{n-1}V'$ is a subobject of $\mathbf{T}^nV$. Since $\mathbf{T}^nV$ is assumed to be semisimple, so is $V \otimes \mathbf{T}^{n-1}V'$. Hence the injection $\mathbf{T}^nV' \to V \otimes \mathbf{T}^{n-1}V'$ splits. By Proposition 3.2, this implies that $V' \to V$ splits. Since this is true for every V', it follows that V is semisimple.

Since duality preserves semisimplicity, the same result holds when $n = 0$ and $m \geq 1$. Hence, we may assume that $n \geq 1$ and $m \geq 1$, and also that $V \neq 0$. If n and m are both equal to 1, then $V \otimes V^*$ is semisimple by assumption. Put $W = V^*$; using (2.2.2) we see that W has property (2.1.1) and by Proposition 2.3 this implies that V is semisimple (I owe this argument to W. Feit). The remaining case $n + m \geq 3$ is handled by induction on $n + m$, using the fact that $\mathbf{T}^{n-1}V \otimes \mathbf{T}^{m-1}V^*$ embeds into $\mathbf{T}^nV \otimes \mathbf{T}^mV^*$, hence is semisimple.

4. FROM $\bigwedge^2 V$ AND $\mathrm{Sym}^2 V$ TO V

4.1. *Notation*

Let V be an object of C_G, and let λ_V be the canonical map

$$V \otimes V \to \bigwedge^2 V.$$

Define $\varphi_V\colon V \to \bigwedge^2 V \otimes V^*$ as the composite of the maps $j_V\colon V \to V \otimes V \otimes V^*$ (cf. Lemma 3.1) and $\lambda_V \otimes 1_{V^*}\colon V \otimes V \otimes V^* \to \bigwedge^2 V \otimes V^*$. Define $\psi_V\colon \bigwedge^2 V \otimes V^* \to V$ as the composite

$$\bigwedge^2 V \otimes V^* \to V \otimes V \otimes V^* \to V,$$

where the map on the left is $(x \wedge y) \otimes z \mapsto x \otimes y \otimes z - y \otimes x \otimes z$ (for $x, y \in V$, $z \in V^*$) and the map on the right is the map f_V defined in the proof of Lemma 3.1, i.e., $x \otimes y \otimes z \mapsto \langle x, z\rangle y$. We have

$$\psi_V((x \wedge y) \otimes z) = \langle x, z\rangle y - \langle y, z\rangle x \qquad (x, y \in V,\ z \in V^*).$$

Both φ_V and ψ_V are C_G-morphisms.

PROPOSITION 4.2. *The composite map*

$$V \xrightarrow{\varphi_V} \bigwedge^2 V \otimes V^* \xrightarrow{\psi_V} V$$

is equal to $(1-n)1_V$, *where* $n = \dim V$.

Proof. Choose a k-basis (e_α) of V, and let (e_α^*) be the dual basis of V^*. We have $1_V = \sum e_\alpha \otimes e_\alpha^*$ in $V \otimes V^*$, hence:

$$j_V(x) = \sum x \otimes e_\alpha \otimes e_\alpha^* \qquad (x \in V),$$
$$\varphi_V(x) = \sum (x \wedge e_\alpha) \otimes e_\alpha^*,$$

and

$$\psi_V(\varphi_V(x)) = \sum \langle x, e_\alpha^*\rangle e_\alpha - \sum \langle e_\alpha, e_\alpha^*\rangle x$$
$$= x - nx.$$

COROLLARY 4.3. *If* $\dim V \not\equiv 1 \pmod p$, φ_V *is a split injection.*

PROPOSITION 4.4. *Let* $\rho\colon W \to V$ *be an injection in* C_G. *Assume that* $\dim W \not\equiv 1 \pmod p$ *and that* $\bigwedge^2\rho\colon \bigwedge^2 W \to \bigwedge^2 V$ *splits. Then* ρ *splits.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
W \arrow[rr, "\rho"] \arrow[dd, "\varphi_W"'] & & V \arrow[d, "\varphi_V"] \\
& & \wedge^2 V \otimes V^* \arrow[d, "\sigma"'] \\
\wedge^2 W \otimes W^* \arrow[rr, "\rho'"] & & \wedge^2 V \otimes W^*
\end{tikzcd}$$

where φ_V and φ_W are as above, ρ' is equal to $\wedge^2\rho \otimes 1_{W^*}$ and σ is the tensor product of the identity endomorphism of $\wedge^2 V$ with the natural projection $\rho^*\colon V^* \to W^*$. By Corollary 4.3, applied to W, φ_W is split; by assumption, ρ' is split. Hence $\sigma \circ \varphi_V \circ \rho = \rho' \circ \varphi_W$ is split, and this implies that ρ is split.

THEOREM 4.5. *If* $\wedge^2 V$ *is semisimple and* $\dim V \not\equiv 2 \pmod p$, *then* V *is semisimple*.

Proof. We have to show that every injection $W \to V$ splits. Since $\wedge^2 V$ is semisimple, the injection $\wedge^2 W \to \wedge^2 V$ splits. If $\dim W \not\equiv 1 \pmod p$, Proposition 4.4 shows that $W \to V$ splits. Assume now that $\dim W \equiv 1 \pmod p$. Let W^0 be the orthogonal complement of W in V^*, i.e., the kernel of the projection $V^* \to W^*$. We have $\dim W^0 \equiv \dim V - 1 \pmod p$, hence $\dim W^0 \not\equiv 1 \pmod p$, since $\dim V \not\equiv 2 \pmod p$. By duality, $\wedge^2 V^*$ is semisimple. The first part of the argument, applied to $W^0 \to V^*$, shows that $W^0 \to V^*$ splits, and hence $W \to V$ splits.

The next theorem describes the structure of V in the exceptional case left open by Theorem 4.5 (for explicit examples, see Sect. 7.3):

THEOREM 4.6. *Assume* $\wedge^2 V$ *is semisimple and* V *is not. Then* V *can be decomposed in* C_G *as a direct sum*:

$$V = E \oplus W_1 \oplus \cdots \oplus W_h \qquad (h \geq 0), \tag{$*$}$$

where:

—*the* W_i *are simple, and* $\dim W_i \equiv 0 \pmod p$;

—E *is a nonsplit extension of two simple modules* W, W' *such that* $\dim W \equiv \dim W' \equiv 1 \pmod p$.

(Note that $(*)$ implies $\dim V \equiv \dim E \equiv 2 \pmod p$, as in Theorem 4.5.)

Proof. Using induction on the length of a Jordan−Hölder sequence of V, we may assume that V has no simple direct factor whose dimension is 0 (mod p).

Let W be a simple subobject of V. Let us show that $\dim W \equiv 1 \pmod{p}$. If not, Proposition 4.4 would imply that $W \to V$ splits, hence $V = W \oplus V'$ for some $V' \in C_G$. Clearly V' is not semisimple but $\wedge^2 V'$ is (because it is a subobject of $\wedge^2 V$). By Theorem 4.5, applied to V and V', we have

$$\dim V \equiv \dim V' \equiv 2 \pmod{p},$$

hence $\dim W \equiv 0 \pmod{p}$, which contradicts the hypothesis that V has no simple direct factor of dimension divisible by p.

Hence, we have $\dim W \equiv 1 \pmod{p}$. Moreover, *the injection $W \to V$ does not split*. Indeed, if V would decompose in $W \oplus V'$, we would have $\dim V' \equiv 1 \pmod{p}$, and Theorem 4.5, applied to V', would show that V' is semisimple, hence also V, which is not true. The module W is *the only simple submodule of V*. Indeed, if W_1 were another one, the argument above would show that $\dim W_1 \equiv 1 \pmod{p}$, hence $\dim(W + W_1) \equiv 2 \pmod{p}$ since $W \cap W_1 = 0$. By Proposition 4.4, the injection $W \oplus W_1 \to V$ would split, and so would $W \to V$, contrary to what we have just seen.

Now put $W' = V/W$. We have $\dim W' \equiv 1 \pmod{p}$, and $\wedge^2 W'$ is semisimple (because it is a quotient of $\wedge^2 V$). By Theorem 4.5, W' is semisimple. At least one of the simple factors of W' has dimension $\not\equiv 0 \pmod{p}$. Let S be such a factor, and let V_S be its inverse image in V, so that we have $W \subset V_S \subset V$. One has $\dim V_S \not\equiv 1 \pmod{p}$; by Proposition 4.4, this shows that we may write V as a direct sum $V_S \oplus V''$. If $V'' \neq 0$, it contains a simple subobject, which is distinct from W, contrary to what was proved above. Hence we have $V'' = 0$, i.e., $S = W'$, which shows that W' is simple and that V is a nonsplit extension of two simple objects W, W' with $\dim W \equiv \dim W' \equiv 1 \pmod{p}$.

There are similar results for $\mathrm{Sym}^2 V$. First:

THEOREM 4.7. *If* $\mathrm{Sym}^2 V$ *is semisimple and* $\dim V \not\equiv -2 \pmod{p}$, *then* V *is semisimple*.

Proof (*sketch*). The argument is the same as for $\wedge^2 V$, using symmetric analogues φ_V^σ and ψ_V^σ of φ_V and ψ_V:

$$\varphi_V^\sigma \colon V \to \mathrm{Sym}^2 V \otimes V^*,$$

$$\psi_V^\sigma \colon \mathrm{Sym}^2 V \otimes V^* \to V.$$

Proposition 4.2 is replaced by

$$\psi_V^\sigma \circ \varphi_V^\sigma = (1+n) 1_V \qquad \text{where } n = \dim V.$$

Hence φ_V^σ is a split injection if $\dim V \not\equiv -1 \pmod{p}$. Proposition 4.4 remains valid when $\wedge^2 V$ is replaced by $\mathrm{Sym}^2 V$ and 1 is replaced by -1.

The same is true for the proof of Theorem 4.5 (with 2 replaced by -2), with one difference:

In the case of $\wedge^2$ we have used the fact that $\wedge^2 V$ and $\wedge^2 V^*$ are dual to each other. The analogous statement for $\mathrm{Sym}^2 V$ and $\mathrm{Sym}^2 V^*$ is true when $p \neq 2$, but *is not true* in general for $p = 2$; the dual of $\mathrm{Sym}^2 V$ is the space $\mathbf{TS}^2 V^*$ of symmetric 2-tensors on V^*, which is not $\mathrm{Sym}^2 V^*$. Fortunately, the case $p = 2$ does not give any trouble. Indeed:

PROPOSITION 4.8. *If* $\mathrm{Sym}^2 V$ *is semisimple and* $p = 2$, *then* V *is semisimple*.

Proof. Let $F\colon k \to k$ be the Frobenius map $\lambda \mapsto \lambda^2$, and let V^F be the representation of G deduced from V by the base change F. The F-semilinear map $V \to \mathrm{Sym}^2 V$ defined by $x \mapsto x \cdot x$ gives a *k-linear embedding* of V^F into $\mathrm{Sym}^2 V$, which fits into an exact sequence:

$$0 \to V^F \to \mathrm{Sym}^2 V \to \wedge^2 V \to 0.$$

Since $\mathrm{Sym}^2 V$ is assumed to be semisimple, so is V^F. This means that V becomes semisimple after the base change $F\colon k \to k$. By an elementary result ([1, §13, no. 4, Proposition 4]) this implies that V is semisimple.

Remark. More generally, the same argument shows:

$$\mathrm{Sym}^p V \text{ semisimple} \quad \Rightarrow \quad V \text{ semisimple}$$

if the characteristic p is > 0.

The analogue of Theorem 4.6 is:

THEOREM 4.9. *If* $\mathrm{Sym}^2 V$ *is semisimple and* V *is not*, *then* V *can be decomposed as* $V = E \oplus W_1 \oplus \cdots \oplus W_h$ $(h \geq 0)$, *where*:

—*the* W_i *are simple*, *and* $\dim W_i \equiv 0 \pmod p$;

—*E is a nonsplit extension of two simple modules whose dimensions are congruent to* $-1 \pmod p$.

The proof is the same.

COROLLARY 4.10. *One has* $\dim V \geq 2p - 2$.

Indeed, it is clear that $\dim E \geq (p-1) + (p-1)$.

5. HIGHER EXTERIOR POWERS

The results of Sect. 4 can be extended to $\wedge^m V$ for any $m \geq 1$ (cf. Theorem 5.2.1 below). We start with several lemmas.

5.1. *Extension Classes Associated with an Exact Sequence*

Let

$$0 \to A \to V \to B \to 0 \tag{5.1.1}$$

be an exact sequence in C_G. We denote by (V) its class in the group

$$\mathrm{Ext}(B, A) = H^1(G, \mathrm{Hom}_k(B, A)) = H^1(G, A \otimes B^*).$$

A cocycle representing this class may be constructed as follows: select a k-linear splitting $f\colon B \to V$, and, for every $s \in G$, define $c_f(s)$ in $\mathrm{Hom}_k(B, A)$ as the map $x \mapsto s \cdot f(s^{-1}x) - f(x)$, for $x \in B$. Then c_f is a 1-cocycle on G with values in $\mathrm{Hom}_k(B, A)$, which represents the class (V).

One has $(V) = 0$ if and only if f can be chosen to be G-linear, i.e., if and only if the injection $A \to V$ splits.

5.1.2. *The Filtration of* $\bigwedge^m V$ *Defined by* A

We view A as a subobject of V. For every integer α with $0 \le \alpha \le m$, let F_α be the subspace of $\bigwedge^m V$ generated by the $x_1 \wedge \cdots \wedge x_m$ such that x_i belongs to A for $i \le \alpha$; put $F_{m+1} = 0$. The F_α are G-stable, and they define a decreasing filtration of $\bigwedge^m V$:

$$\bigwedge{}^m V = F_0 \supset F_1 \ \cdots \ \supset F_m \supset F_{m+1} = 0.$$

One has $F_m = \bigwedge^m A$. More generally, the quotient $V_\alpha = F_\alpha / F_{\alpha+1}$ can be identified with $\bigwedge^\alpha A \otimes \bigwedge^\beta B$, where $\beta = m - \alpha$; in this identification, an element $x_1 \wedge \cdots \wedge x_m$ of F_α (with $x_i \in A$ for $i \le \alpha$, as above) corresponds to

$$(x_1 \wedge \cdots \wedge x_\alpha) \otimes (\bar{x}_{\alpha+1} \wedge \cdots \wedge \bar{x}_m),$$

where $\bar{x}_i$ is the image of x_i in B.

Assume now $\alpha \ge 1$, and put $V_\alpha^2 = F_{\alpha-1}/F_{\alpha+1}$. We have an exact sequence

$$0 \to V_\alpha \to V_\alpha^2 \to V_{\alpha-1} \to 0, \tag{5.1.3}$$

hence an extension class (V_α^2) in $H^1(G, V_\alpha \otimes V_{\alpha-1}^*)$.

Since $V_\alpha = \bigwedge^\alpha A \otimes \bigwedge^\beta B$, we may view (V_α^2) as an element of the cohomology group

$$H^1(G, \bigwedge{}^\alpha A \otimes \bigwedge{}^\beta B \otimes \bigwedge{}^{\alpha-1} A^* \otimes \bigwedge{}^{\beta+1} B^*). \tag{5.1.4}$$

5.1.5. *Comparison of the Classes* (V) *and* (V_α^2)

The exterior product $(u, x) \mapsto u \wedge x$ defines a map from $\bigwedge^{\alpha-1}A \otimes A$ to $\bigwedge^\alpha A$, hence a C_G-morphism:

$$\theta_{A,\alpha}\colon A \to \mathrm{Hom}_k\left(\bigwedge^{\alpha-1}A, \bigwedge^\alpha A\right) = \bigwedge^\alpha A \otimes \bigwedge^{\alpha-1}A^*. \quad (5.1.6)$$

The same construction, applied to B^* and to $\beta+1$, gives

$$\theta_{B^*,\beta+1}\colon B^* \to \bigwedge^{\beta+1}B^* \otimes \bigwedge^\beta B. \quad (5.1.7)$$

By tensoring these two maps, and multiplying by $(-1)^\beta$, we get

$$\Theta_\alpha\colon A \otimes B^* \to \bigwedge^\alpha A \otimes \bigwedge^\beta B \otimes \bigwedge^{\alpha-1}A^* \otimes \bigwedge^{\beta+1}B^*. \quad (5.1.8)$$

Since Θ_α is a C_G-morphism, it defines a map

$$\Theta_\alpha^1\colon H^1(G, A \otimes B^*) \to H^1\left(G, \bigwedge^\alpha A \otimes \bigwedge^\beta B \otimes \bigwedge^{\alpha-1}A^* \otimes \bigwedge^{\beta+1}B^*\right).$$

LEMMA 5.1.9. *The image by* Θ_α^1 *of the class* (V) *of* (5.1.1) *is the class* (V_α^2) *of* (5.1.3).

Proof (*sketch*). Select a k-splitting f of (5.1.1). Using f, one may identify the exterior algebra $\bigwedge V$ with $\bigwedge A \otimes \bigwedge B$. This defines a k-splitting f_α of V_α^2. An explicit computation (which we do not reproduce) shows that the cocycle c_{f_α} corresponding to f_α is the image by Θ_α of the cocycle c_f. Hence the lemma.

The next step is to give criteria for Θ_α^1 to be injective. Put

$$a = \dim A \quad \text{and} \quad b = \dim B, \quad (5.1.10)$$

so that we have

$$\dim V = a + b. \quad (5.1.11)$$

LEMMA 5.1.12. *Assume* $\binom{a-1}{\alpha-1} \not\equiv 0 \pmod p$. *Then the morphism* $\theta_{A,\alpha}$ *defined above is a split injection.*

(Recall that $\binom{x}{y}$ is the binomial coefficient $x(x-1)\cdots(x-y+1)/y!$)

Proof (*sketch*). Consider the C_G-morphism

$$\theta_{A^*,\alpha}\colon A^* \to \bigwedge^\alpha A^* \otimes \bigwedge^{\alpha-1}A,$$

and let

$$\theta'_{A^*,\alpha}\colon \bigwedge^\alpha A \otimes \bigwedge^{\alpha-1}A^* \to A$$

be its transpose. One has

$$\theta'_{A^*,\alpha} \circ \theta_{A,\alpha} = \binom{a-1}{\alpha-1} \cdot 1_A \qquad \text{in } \mathrm{End}(A). \quad (5.1.13)$$

This identity is proved by a straightforward computation: one chooses a k-basis of the vector space A; this gives bases of $\bigwedge^\alpha A, \bigwedge^\alpha A^*, \ldots$; one determines the corresponding matrices, etc. The details are left to the reader.

Once (5.1.13) is checked, Lemma 5.1.12 is obvious.

LEMMA 5.1.14. *Assume* $\binom{b-1}{\beta} \not\equiv 0 \pmod p$. *Then the morphism* $\theta_{B^*, \beta+1}$ *defined above is a split injection.*

Proof. This follows from the preceding lemma, with A replaced by B^* and α by $\beta + 1$.

LEMMA 5.1.15. *Assume*

$$\binom{a-1}{\alpha-1} \cdot \binom{b-1}{\beta} \not\equiv 0 \qquad \pmod p.$$

Then:

(i) *The* C_G*-morphism* Θ_α *defined in* (5.1.8) *is a split injection.*

(ii) *The map*

$$\Theta_\alpha^1 : H^1(G, A \otimes B^*) \to H^1(G, \wedge^\alpha A \otimes \wedge^\beta B \otimes \wedge^{\alpha-1} A^* \otimes \wedge^{\beta+1} B^*)$$

is injective.

Proof. Assertion (i) follows from Lemmas 5.1.12 and 5.1.14 since the tensor product of two split injections is a split injection. Assertion (ii) follows from assertion (i).

LEMMA 5.1.16. *Assume*

$$\binom{a-1}{\alpha-1} \cdot \binom{b-1}{\beta} \not\equiv 0 \qquad \pmod p.$$

If the exact sequence (5.1.3) *splits, then* $A \to V$ *is a split injection.*

Proof. We have $(V_\alpha^2) = 0$ by hypothesis. Since (V_α^2) is the image of (V) by Θ_α^1 (cf. Lemma 5.1.9) and Θ_α^1 is injective (cf. Lemma 5.1.15), we have $(V) = 0$.

5.2. *Semisimplicity Statements*

Let V be as above an object of C_G, and m an integer ≥ 1.

THEOREM 5.2.1. *Assume that* $\wedge^m V$ *is semisimple, and that the integer* $\dim V$ *has the following property*:

($*$) *For every pair of integers* $a, b \geq 1$ *with* $a + b = \dim V$, *there exists an integer* α, *with* $1 \leq \alpha \leq m$, *such that*

$$\binom{a-1}{\alpha-1} \cdot \binom{b-1}{m-\alpha} \not\equiv 0 \qquad \pmod p. \tag{5.2.2}$$

Then V *is semisimple.*

Proof. Let A be a subobject of V, and let $B = V/A$. We want to show that $A \to V$ splits. We may assume that $A \neq 0$, $B \neq 0$. Put as above

$$a = \dim A \quad \text{and} \quad b = \dim B.$$

We have $a, b \geq 1$ and $a + b = \dim V$. Choose α as in (5.2.2). Since $\wedge^m V$ is semisimple, the same is true for its subquotients, and in particular for V_α^2 (cf. Sect. 5.1.2). Hence the exact sequence (5.1.3) splits. By Lemma 5.1.16, this implies that $A \to V$ splits.

EXAMPLE 5.2.3. If $m = 2$, α may take the values 1 and 2 and (5.2.2) means:

$$b - 1 \not\equiv 0 \pmod{p} \qquad \text{if } \alpha = 1,$$
$$a - 1 \not\equiv 0 \pmod{p} \qquad \text{if } \alpha = 2.$$

If $\dim V = a + b$ is not congruent to 2 (mod p), one of these two is true. Hence $\wedge^2 V$ semisimple $\Rightarrow V$ semisimple, and we recover Theorem 4.5.

Here are two other examples:

THEOREM 5.2.4. *Assume $\wedge^3 V$ is semisimple and*

$$\dim V \not\equiv 2, 3 \pmod{p} \qquad \textit{if } p \neq 2,$$
$$\dim V \not\equiv 2, 3 \pmod{4} \qquad \textit{if } p = 2.$$

Then V is semisimple.

Proof. Here α may take the values $1, 2, 3$ and (5.2.2) means

$$(b-1)(b-2)/2 \not\equiv 0 \pmod{p} \qquad \text{if } \alpha = 1,$$
$$(a-1)(b-1) \not\equiv 0 \pmod{p} \qquad \text{if } \alpha = 2,$$
$$(a-1)(a-2)/2 \not\equiv 0 \pmod{p} \qquad \text{if } \alpha = 3.$$

If $p \neq 2$, these conditions mean, respectively,

$$b \not\equiv 1, 2 \pmod{p},$$
$$a \not\equiv 1 \pmod{p} \quad \text{and} \quad b \not\equiv 1 \pmod{p},$$
$$a \not\equiv 1, 2 \pmod{p}.$$

If $a + b \not\equiv 2, 3 \pmod{p}$, it is clear that one of them is fulfilled.

The case $p = 2$ is similar; the only difference is that the congruence

$$(x-1)(x-2)/2 \not\equiv 0 \pmod{2}$$

means that $x \not\equiv 1, 2 \pmod{4}$.

THEOREM 5.2.5. *Assume that* $\wedge^m V$ *is semisimple and*

$$\dim V \not\equiv 2, 3, \ldots, m \pmod{p}.$$

Then V *is semisimple*.

Proof. Consider first the case $p = 0$ (see also Sect. 6.1 below). By assumption we have $\dim V \neq 2, 3, \ldots, m$. (Note that it is *a priori* obvious that these dimensions have to be excluded.) We may assume $\dim V \neq 0, 1$, hence $\dim V > m$. If $a + b = \dim V$, with $a, b \geq 1$, we put $\alpha = 1 + \sup(0, m - b)$. We have $a - 1 \geq \alpha - 1$ and $b - 1 \geq m - \alpha$ hence both $\binom{a-1}{\alpha-1}$ and $\binom{b-1}{m-\alpha}$ are $\neq 0$. Hence (5.2.2) is satisfied.

Suppose now $p > 0$. The hypothesis $\dim V \not\equiv 2, 3, \ldots, m \pmod{p}$ implies $p \geq m$. Hence condition (5.2.2) may be rewritten as

$$a \not\equiv 1, 2, \ldots, \alpha - 1 \pmod{p} \quad \text{and} \quad b \not\equiv 1, 2, \ldots, m - \alpha \pmod{p}. \quad (5.2.26)$$

If $b \not\equiv 1, 2, \ldots, m - 1 \pmod{p}$, we put $\alpha = 1$ and (5.2.6) holds. If $b \equiv i \pmod{p}$ with $1 \leq i \leq m - 1$, we put $\alpha = m - i + 1$. One has

$$a \not\equiv 1, 2, \ldots, \alpha - 1 \pmod{p},$$

because otherwise $\dim V$ would be congruent $\pmod{p}$ to $i + 1, \ldots, m$, which would contradict our assumption. Hence (5.2.6) holds

5.3. *Higher Symmetric Powers*

We assume here that $p > m$ (or $p = 0$), so that the dual of $\mathrm{Sym}^\alpha V$ for $\alpha \leq m$ is $\mathrm{Sym}^\alpha V^*$.

THEOREM 5.3.1. *If* $\mathrm{Sym}^m V$ *is semisimple and* $\dim V \not\equiv -2, -3, \ldots, -m \pmod{p}$, *then* V *is semisimple*.

Proof (*sketch*). One rewrites the previous sections with exterior powers replaced by symmetric powers. The sign problems disappear. Moreover, the integer $\binom{a-1}{\alpha-1}$ of (5.1.13) becomes $\binom{a+\alpha-1}{\alpha-1}$. The rest of the proof is the same.

6. FURTHER REMARKS

6.1. *Characteristic Zero*

When $p = 0$, the theorems of Sects. 2–5 can be obtained more simply by the following method (essentially due to Chevalley [2]):

We want to prove that a linear representation V of G is semisimple, knowing (say) that $\wedge^m V$ is semisimple and $\dim V \neq 2, 3, \ldots, m$. By enlarging k, we may assume it is algebraically closed; we may also assume that $G \to \mathbf{GL}(V)$ is injective and that its image is Zariski-closed; hence G may be viewed as a linear algebraic group over k (more correctly: as the group of k-points of an algebraic linear group). See [6] for these easy reduction steps. Let U be the unipotent radical of G (maximal normal unipotent subgroup). Because the characteristic is 0, an algebraic linear representation of G is semisimple if and only if its kernel contains U. Since $\wedge^m V$ is assumed to be semisimple, this shows that U is contained in the kernel of $\mathbf{GL}(V) \to \mathbf{GL}(\wedge^m V)$. If $\dim V \neq 2, 3, \dots, m$, this kernel is of order m (if $\dim V > m$) or is a torus (if $\dim V < 2$); such a group has no nontrivial unipotent subgroup. Hence $U = 1$, and the given representation $G \to \mathbf{GL}(V)$ is semisimple.

6.2. *Generalizations*

All the results of Sects. 2–5 extend to linear representations of *Lie algebras*, and also of *restricted Lie algebras* (if $p > 0$). This is easy to check.

A less obvious generalization consists of replacing C_G by a *tensor category C over k*, in the sense of Deligne [3]. Such a category is an abelian category, with the following extra structures:

(a) for every $V_1, V_2 \in \mathrm{ob}(C)$, a k-vector space structure on $\mathrm{Hom}^C(V_1, V_2)$;

(b) an exact bifunctor $C \times C \to C$, denoted by $(V_1, V_2) \mapsto V_1 \otimes V_2$;

(c) a commutativity isomorphism $V_1 \otimes V_2 \to V_2 \otimes V_1$;

(d) an associativity isomorphism $(V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes (V_2 \otimes V_3)$.

These data have to fulfill several axioms mimicking what happens in C_G (cf. [3]). For instance, there should exist an object "$\underline{1}$" with $\underline{1} \otimes V = V$ for every V, and $\mathrm{End}^C(\underline{1}) = k$; there should be a "dual" V^* with $V^{**} = V$ and $\mathrm{Hom}^C(W, V^*) = \mathrm{Hom}^C(V \otimes W, \underline{1})$ for every $W \in \mathrm{ob}(C)$; etc.

If $V \in \mathrm{ob}(C)$, there are natural morphisms

$$\underline{1} \to V \otimes V^* \quad \text{and} \quad V \otimes V^* \to \underline{1}.$$

The *dimension* of V is the element of $k = \mathrm{End}^C(\underline{1})$ defined by the composition

$$\underline{1} \to V \otimes V^* \to \underline{1}.$$

It is not always an integer.

All the results of Sects. 2 *and* 3 *are true for C provided the conditions on* $\dim V$ *or* $\dim W$ *are interpreted as taking place in k*. For instance, if $V \otimes W$ is semisimple and $\dim W \neq 0$ (in k), then V is semisimple. The proofs require some minor changes: e.g., in Lemma 3.1, one needs to define directly the morphisms

$$f_V: V \otimes V \otimes V^* \to V \quad \text{and} \quad j_V: V \to V \otimes V \otimes V^*.$$

Moreover, the basic equality $f_V \circ j_V = 1_V$ is one of the axioms of a tensor category, (cf. [3], (2.1.2)).

As for the results of Sect. 4 on $\wedge^2 V$ and $\mathrm{Sym}^2 V$, they remain true at least when $p \neq 2$, but some of the proofs (e.g., that of Proposition 4.2) have to be written differently. I am not sure of what happens with Sect. 5: I have not managed to rewrite the proofs in tensor category style. Still, I feel that Theorem 5.2.5 (on $\wedge^m V$) and Theorem 5.3.1 (on $\mathrm{Sym}^m V$) should remain true whenever $m! \neq 0$ in k (i.e., $p = 0$ or $p > m$).

Remark. An interesting feature of the tensor category point of view is the following principle, which was pointed out to me by Deligne:

Any result on $\wedge^m$ *implies a result for* Sym^m, *and conversely* (here again we assume $m! \neq 0$ in k). This is done by associating to each tensor category C the category $C' = \mathrm{super}(C)$, whose objects are the pairs $V' = (V_0, V_1)$ of objects of C; such a V' is viewed as a graded object $V' = V_0 \oplus V_1$, with grading group $\mathbf{Z}/2\mathbf{Z}$. The tensor structure of C' is defined in an obvious way, except that the commutativity isomorphism is modified according to the Koszul sign rule: the chosen isomorphism between $(0, V_1) \otimes (0, W_1)$ and $(0, W_1) \otimes (0, V_1)$ is the *opposite* of the obvious one. With this convention, one finds that

$$\dim V' = \dim V_0 - \dim V_1.$$

In particular, if $V \in \mathrm{ob}(C)$, one has $\dim(0, V) = -\dim V$. Moreover, one checks that

$$\wedge^m(0, V) = \begin{cases} (\mathrm{Sym}^m V, 0) & \text{if } m \text{ is even}, \\ (0, \mathrm{Sym}^m V) & \text{if } m \text{ is odd}. \end{cases}$$

Hence any general theorem on the functor $\wedge^m$, when applied to C', gives a corresponding theorem for the functor Sym^m, with a sign change in dimensions (compare for instance Theorem 4.5 and Theorem 4.7).

7. EXAMPLES

The aim of this section is to construct examples showing that the congruence conditions on $\dim W$ and $\dim V$ in Theorems 2.4, 4.5, and 5.2.5 are *best possible*.

We assume that p is > 0 and that k is algebraically closed

7.1. *The Group G*

Let C be a cyclic group of order p, with generator s. Choose a finite abelian group A on which C acts. Assume

(7.1.1) *the order $|A|$ of A is prime to p, and* > 1.

(7.1.2) *the action of C on $A - \{1\}$ is free.*

Let G be the semidirect product $A \cdot C$ of C by A. It is a Frobenius group, with Frobenius kernel A.

Let $X = \mathrm{Hom}(A, k^{\times})$ be the character group of A; we write X additively and, if $a \in A$ and $x \in X$, the image of a by x is denoted by a^x. The group C acts on X by duality, and condition (7.1.2) is equivalent to:

(7.1.3) *The action of C on $X - \{0\}$ is free* (i.e., $sx = x \Rightarrow x = 0$).

If $x \in X$, denote by $\underline{1}^x \in C_A$ the k-vector space k on which A acts *via* the character x. The induced module $W(x) = \mathrm{Ind}_A^G \underline{1}^x$ is an object of C_G, of dimension p. One checks easily:

(7.1.4) *If $x \neq 0$, $W(x)$ is simple and projective* (in C_G).

Moreover

(7.1.5) *Every $V \in \mathrm{ob}(C_G)$ splits uniquely as $V = E \oplus P$, where E is the subspace of V fixed under A, and P is a direct sum of modules $W(x)$, with $x \in X - \{0\}$.*

If we decompose V in $V = \oplus V_x$, where V_x is the A-eigenspace relative to x (i.e., the set of $v \in V$ such that $a \cdot v = a^x v$ for every $a \in A$), one has $E = V_0$ and $P = \oplus_{y \neq 0} V_y$.

From (7.1.5) follow:

(7.1.6) *V is semisimple if and only if the action of C on E is trivial* (i.e., if and only if $E \cong \underline{1} \oplus \cdots \oplus \underline{1}$).

(7.1.7) *V is projective if and only if E is C-projective* (i.e., if and only if E is a multiple of the regular representation of C).

Note that both (7.1.6) and (7.1.7) apply when $E = 0$, i.e., when no element of V, except 0, is fixed by A.

(7.1.8) *Let x be an element of $X - \{0\}$. If $V = V_0$* (i.e., if A acts trivially on V), *then $V \otimes W(x)$ is isomorphic to the direct sum of m copies of $W(x)$, where $m =$* $\dim V$.

Indeed, V is a successive extension of m copies of $\underline{1}$, hence $V \otimes W(x)$ is a successive extension of m copies of $W(x)$; these extensions split since $W(x)$ is projective (7.1.4); hence the result.

7.2. *Examples Relative to Theorem* 2.4

We reproduce here an example due to W. Feit, showing that the congruence condition "$\dim W \not\equiv 0 \pmod p$" of Theorem 2.4 is the best possible:

PROPOSITION 7.2.1. *Let G be a finite group of the type in Sect.* 7.1, *and let n, m be two positive integers, with $m > 1$ and n divisible by p. There exist $V, W \in \mathrm{ob}(C_G)$ such that*:

(i) $\dim V = m$ *and* $\dim W = n$;

(ii) *V is not semisimple*;

(iii) *$V \otimes W$ is semisimple*.

Proof. Choose:

$V =$ a non-semisimple C-module of dimension m (such a module exists since $m > 1$);

$W = W(x_1) \oplus \cdots \oplus W(x_{n/p})$, with $x_i \in X - \{0\}$.

The projection $G \to C$ makes V into a G-module with trivial A-action. It is clear that (i) and (ii) are true. By (7.1.8), $V \otimes W$ is isomorphic to the direct sum of m copies of W, hence it is semisimple.

7.3. *Examples relative to Theorems* 4.5 *and* 5.2.5

The following proposition shows that the congruence conditions of Theorem 5.2.5 are the best possible:

PROPOSITION 7.3.1. *Let i and n be two integers with $2 \leq i \leq p$, $n > 0$ and $n \equiv i \pmod p$. There exists a finite group G of the type described in Sect.* 7.1 *and an object V of C_G such that*:

(a) $\dim V = n$;

(b) *V is not semisimple*;

(c) *$\wedge^m V$ is semisimple for every m such that $i \leq m \leq p$.*

The case $i = 2$ gives the following result, which shows that the condition $\dim V \not\equiv 2 \pmod p$ of Theorem 4.5 is the best possible:

COROLLARY 7.3.2. *If $n > 0$ and $n \equiv 2 \pmod p$, there exist a finite group G and a non-semisimple G-module V such that $\dim V = n$ and $\wedge^2 V$ is semisimple.*

(Even better: $\wedge^m V$ is semisimple for $2 \leq m \leq p$.)

Proof of Proposition 7.3.1. We need to choose a suitable $G = A \cdot C$ of the type described in Sect. 7.1. To do so, write n as $n = i + hp$, with $h \geq 0$.

LEMMA 7.3.3. *There exist a finite abelian group X, on which C acts, and h elements $x_1, \ldots, x_h$ of X, with the following properties*:

(7.3.4) *The action of C on $X - \{0\}$ is free.*

(7.3.5) *For every family $(I_1, \ldots, I_h)$ of nonempty subsets of $[0, p-1]$ the relation*

$$\sum_{\alpha=1}^{h} \sum_{j \in I_\alpha} s^j x_\alpha = 0 \qquad (*)$$

implies $I_\alpha = [0, p-1]$ for $\alpha = 1, \ldots, h$.

Proof. Assume first that $h = 1$. In that case, (7.3.5) just means that, if I is a subset of $[0, p-1]$, with $0 < |I| < p$, one has $\sum_{j \in I} s^j x_1 \neq 0$. This is easy to achieve: choose some integer $e > 1$, prime to p, and define X_1 to be the augmentation module of the group ring $\mathbf{Z}/e\mathbf{Z}[C]$, i.e., the kernel of $\mathbf{Z}/e\mathbf{Z}[C] \to \mathbf{Z}/e\mathbf{Z}$; put $x_1 = 1 - s$. It is easy to check that (X_1, x_1) has the required property.

If $h > 1$, one takes for X the direct sum of h copies of the C-module X_1 defined above, and one defines $x_1, \ldots, x_h$ to be

$$(x_1, 0, \ldots, 0), \ldots, (0, \ldots, 0, x_1).$$

Proof of Proposition 7.3.1 (*continued*). Let $(X, x_1, \ldots, x_h)$ be as in Lemma 7.3.3. Property (7.3.4) implies

$$|X| \equiv 1 \pmod{p},$$

hence $|X|$ is prime to p. Let $A = \mathrm{Hom}(X, k^\times)$ be the dual of X; then X is the dual of A. The semidirect product $G = A \cdot C$ is a group of the type described in Sect. 7.1. Define $V \in \mathrm{ob}(C_G)$ by

$$V = E \oplus W(x_1) \oplus \cdots \oplus W(x_h), \qquad (7.3.6)$$

where E is a non-semisimple C-module of dimension i (viewed as a G-module with trivial action of A), and $W(x_\alpha) = \mathrm{Ind}_C^G \underline{1}^{x_\alpha}$ (cf. Sect. 7.1). We have $\dim V = i + hp = n$, and it is clear that V is not semisimple. It remains to check that $\wedge^m V$ is semisimple if $i \leq m \leq p$. By (7.3.6), $\wedge^m V$ is a direct sum of modules of type:

$$\wedge^a E \otimes \wedge^{b_1} W(x_1) \otimes \cdots \otimes \wedge^{b_h} W(x_h), \qquad (7.3.7)$$

with $a + b_1 + \cdots + b_h = m$. Let us show that every such module is semisimple. If all b_α are 0, we have $a = m \geq i$, and $\wedge^a E$ is 0 if $m > i$ and $\wedge^a E = \underline{1}$ if $m = i$. Hence (7.3.7) is either 0 or $\underline{1}$ and is semisimple. We may thus assume that one of the b_α is > 0. By using induction on h, we may even assume that all the b_α are > 0. Since

$$b_1 + \cdots + b_h = m - a \leq p,$$

the b_α are $\leq p$. Suppose one of them, say b_1, is equal to p. We have then

$$b_2 = \cdots = b_h = 0, \qquad m = p, \qquad a = 0,$$

and the G-module (7.3.7) is equal to $\wedge^p W(x_1) = \underline{1}$, hence is semisimple. We may thus assume that $0 < b_\alpha < p$ for every α. Observe now that, if $x \in X - \{0\}$, the characters of A occurring in the A-module $W(x)$ are $x, sx, \ldots, s^{p-1}x$, and their multiplicity is equal to 1. Hence the characters occurring in $\wedge^b W(x)$ are of the form $\sum_{j \in I} s^j x$, for a subset I of $[0, p-1]$ with $|I| = b$. By applying this remark to the $W(x_\alpha)$, one sees that the characters of A occurring in (7.3.7) are of the form

$$\sum_{\alpha=1}^{h} \sum_{j \in I_\alpha} s^j x,$$

with $|I_\alpha| = b_\alpha$. Since $0 < b_\alpha < p$ for every α, it follows from (7.3.5) that such a character is $\neq 0$. Hence no element of (7.3.7), except 0, is fixed under A. By (7.1.6), this implies that (7.3.7) is semisimple. This concludes the proof.

APPENDIX

by Walter Feit

A.1

Let G be a finite group, let p be a prime and let k be a field of characteristic $p > 0$. If V is a $k[G]$-module of dimension n such that $\wedge^2 V$ is semisimple, then V is semisimple unless $n \equiv 2 \pmod{p}$ by Theorem 4.5. Similarly, Theorem 4.6 asserts that if $\mathrm{Sym}^2(V)$ is semisimple then so is V unless $n \equiv -2 \pmod{p}$.

Corollary 7.3.2 implies that, for odd p, Theorem 4.5 is the best possible result. In Theorem A2 below, it is shown that for $p = 2$, for infinitely many but not all even n, there exists a non-semisimple module V of dimension n with $\wedge^2 V$ semisimple.

Furthermore, Theorem A1(ii) shows that if p is a prime such that $p|(2^m + 1)$ for some natural number m, then there exist infinitely many integers n and non-semisimple modules V of dimension n with $\mathrm{Sym}^2 V$ semisimple.

If p is odd there always exist infinitely many natural numbers m such that $p|(2^m - 1)$. The situation is more complicated in case (ii) of Theorem A1. By quadratic reciprocity $p|(2^m + 1)$ for some m if $p \equiv 3$ or $5 \pmod 8$, and $p \nmid (2^m + 1)$ for any m if $p \equiv 7 \pmod 8$. In case $p \equiv 1 \pmod 8$, such an m may or may not exist, the smallest value in this case where no such m exists is $p = 73$. It is not known whether a non-semisimple V exists with $\mathrm{Sym}^2 V$ semisimple in case p is a prime such as $7, 23, \dots$ which does not divide $2^m + 1$ for any natural number m.

If $p = 2^m + 1$ is a Fermat prime, Corollary 4.10 implies that the module V constructed in Theorem A1(ii) has the smallest possible dimension $2^{m+1} = 2p - 2$. For no other primes is it known to us whether there exists a non-semisimple module V with $\mathrm{Sym}^2 V$ semisimple of the smallest possible dimension $2p - 2$.

The method of proof of Theorem A1 also yields some additional examples for all odd primes, of non-semisimple modules V with $\wedge^2 V$ semisimple.

Basic results from modular representation theory are used freely below. See, e.g., [4]. The following notation is used, where p is a prime and G is a finite group:

F is a finite extension of $\mathbb{Q}_p$, the p-adic numbers;

R is the ring of integers in F;

π is a prime element in R.

From now on it will be assumed that $k = R/\pi R$ is the residue class field. Moreover both F and k are splitting fields of G in all cases that arise.

PROPOSITION A.1.1. *Let $\alpha = \alpha_1 + \alpha_2$ be a Brauer character of G, where α_1 is the sum of irreducible Brauer characters which are afforded by projective modules, and α_2 is the sum of irreducible Brauer characters φ_i, no two of which are in the same p-block. Then any $k[G]$-module W which affords α is semisimple.*

Proof. Since a projective submodule of any module is a direct summand, $W = W_1 \oplus W_2$, where W_i affords α_i. Furthermore, W_1 is the direct sum of irreducible projective modules, and so is semisimple. W_2 is semisimple as all the constituents of an indecomposable module lie in the same block.

An immediate consequence of Proposition A.1.1 is

COROLLARY A.1.1. *Let $\theta = \Sigma \chi_i + \Sigma \zeta_j$ be a character of G, where each χ_i and ζ_j is irreducible. Let U be an R-free $R[G]$-module which affords θ. Suppose that the following hold*:

(i) *χ_i has defect 0 for each i.*

(ii) *ζ_j is irreducible as a Brauer character for each j.*

(iii) *If $j \neq j'$ then $\zeta_{j'}$ and ζ_j are in distinct blocks.*

Then $\overline{U} = U/\pi U$ is semisimple.

Corollary A.1.1 yields a criterion to determine when a module is semisimple, which depends only on the computation of ordinary characters. To construct a non-semisimple $k[G]$-module the following result is helpful.

PROPOSITION A.1.2 (Thompson, see [4, I.17.12]). *Let U be a projective indecomposable $R[G]$-module. Let V be an $F[G]$-module which is a summand of $F \otimes U$. Then there exists an R-free $R[G]$-module W with $F \otimes W \approx V$ and $\overline{W} = W/\pi W$ indecomposable.*

COROLLARY A.1.2. *Let $\theta = \eta + \psi$ be the character afforded by a projective indecomposable $R[G]$-module, where η and ψ are characters. Then there exists an indecomposable $\overline{R}[G]$-module which affords η as a Brauer character.*

A.2

See [5, pp. 355–357] for the results below.

Let D denote a dihedral group of order 8 and let Q be a quaternion group of order 8.

Let m be a natural number. Up to isomorphism there are two extra-special groups of order 2^{2m+1}, $T(m, \varepsilon)$ for $\varepsilon = \pm 1$. The first, $T(m, 1)$, is the central product of m copies of D, while $T(m, -1)$ is the central product of Q with $m-1$ copies of D. Let $T = T(m, \varepsilon)$, let Z be the center of T and let $\overline{T} = T/Z$. The map $q = q(m, \varepsilon)$: $T \to Z$ with $q(y) = y^2$ defines a nondegenerate quadratic form on $\overline{T}$, where Z is identified with the field of two elements. $\overline{T}(m, 1)$ has a maximal isotropic subspace of dimension m, while $\overline{T}(m, -1)$ has a maximal isotropic subspace of dimension $m-1$. Furthermore the orthogonal group $O_{2m}(q, \varepsilon)$ acts as a group of automorphisms of $T(m, \varepsilon)$.

$O_{2m}(q, \varepsilon)$ has a cyclic subgroup of order $2^m - \varepsilon$ which acts regularly on $\overline{T}(m, \varepsilon)$. Thus if p is a prime with $p | (2^m - \varepsilon)$, then T has an automorphism σ of order p whose fixed point set is Z.

Let $P = \langle \sigma \rangle$ and let G be the semidirect product PT. Then $\overline{G} = P\overline{T}$ is a Frobenius group with Frobenius kernel $\overline{T}$.

Every irreducible character of $\overline{G}$ which does not have $\overline{T}$ in its kernel is induced from a nonprincipal linear character of $\overline{T}$ and so has degree p.

T has one faithful irreducible character χ. Thus χ extends to an irreducible character of G in p distinct ways. The values of χ are easily computed. Hence all characters of G can be described as follows:

PROPOSITION A.2.1. (i) *G has p linear characters $1 = \lambda_1, \dots, \lambda_p$, whose kernels contain T.*

(ii) *The irreducible characters of $\overline{G}$ which do not have $\overline{T}$ in their kernel all have degree p, and so are of p-defect* 0.

(iii) *There is a faithful irreducible character $\tilde{\chi}$ of G such that $\tilde{\chi}\lambda_1, \dots, \tilde{\chi}\lambda_p$ are all the faithful irreducible characters of G. Furthermore, $\tilde{\chi}(1) = 2^m$ and $\tilde{\chi}$ vanishes on all elements of $T - Z$.*

(iv) *There are two p-blocks of G of positive defect. The sets of irreducible characters in them are $\{\lambda_i | 1 \le i \le p\}$ and $\{\tilde{\chi}\lambda_i | 1 \le i \le p\}$, respectively.*

(v) *Every irreducible character of G is irreducible as a Brauer character.*

The notation of this subsection, especially of Proposition A.2.1, will be used freely below.

A.3

THEOREM A1. *Assume that $p \neq 2$.*

(i) *Let m be a natural number such that $p | (2^m - 1)$. Then there exists a finite group G and a non-semisimple $k[G]$-module V of dimension $2^{m+1} \equiv 2 \pmod p$ such that $\wedge^2 V$ is semisimple.*

(ii) *If $p | (2^m + 1)$ for a natural number m, then there exists a finite group G and a non-semisimple $k[G]$-module V of dimension $2^{m+1} \equiv -2 \pmod p$ such that $\mathrm{Sym}^2 V$ is semisimple.*

Proof. Let G be as in the previous subsection. As a Brauer character, $\tilde{\chi}\lambda_i$ is $\mathbb{Q}$-valued for all i. As the induced character $\chi^G = \sum \tilde{\chi}\lambda_i$, it is the character afforded by a projective indecomposable $k[G]$-module. Hence by Corollary A.1.2 there exists an indecomposable $k[G]$-module V which affords the Brauer character $\theta = 2\tilde{\chi}$, since $\tilde{\chi} + \tilde{\chi}\lambda_i$ agrees with $2\tilde{\chi}$ as a Brauer character. Since χ is irreducible, θ^2 restricted to T contains the principal character of T with multiplicity 4. Thus θ^2 is the sum of four linear Brauer characters and irreducible Brauer characters of p-defect 0.

V is a $k[G]$-module, and hence also a $k[T]$-module. As T is a p'-group, Brauer characters of T are ordinary characters. Let skew be the character of T afforded by $\wedge^2 V$ and let sym denote the character of T afforded by $\mathrm{Sym}^2 V$. Then for y in T

$$\mathrm{skew}(y) = \left(\theta(y)^2 - \theta(y^2)\right)/2,$$

$$\mathrm{sym}(y) = \left(\theta(y)^2 + \theta(y^2)\right)/2.$$

Let $\nu = \pm 1$ denote the Frobenius–Schur index of χ.
Then $\sum_{y \in T} \chi(y^2) = \nu|T|$. Hence $\sum_{y \in T} \theta(y^2) = 2\nu|T|$. Therefore

$$\frac{1}{|T|} \sum_{y \in T} \mathrm{skew}(y) = 2 - \nu,$$

$$\frac{1}{|T|} \sum_{y \in T} \mathrm{sym}(y) = 2 + \nu.$$

In particular, both skew and sym contain the principal character as a constituent.

Therefore the Brauer characters sy, sk of G afforded by $\mathrm{Sym}^2 V$ and by $\wedge^2 V$, respectively, both contain at least one linear constituent. Hence each contains at most three linear constituents as $V \otimes V$ has exactly four linear constituents.

(i) $\mathrm{sk}(1) = (2^{m+1}(2^{m+1} - 1))/2$, hence $\mathrm{sk}(1) \equiv 1 \pmod p$.
As $p \geq 3$ this implies that $\mathrm{sk} = 1 + \beta$, where β is the sum of irreducible projective Brauer characters. Thus $\wedge^2 V$ is semisimple.

(ii) $\mathrm{sy}(1) = (2^{m+1}(2^{m+1} + 1))/2$, hence $\mathrm{sy}(1) \equiv 1 \pmod p$.
As $p \geq 3$ this implies that $\mathrm{sy} = 1 + \beta$, where β is the sum of irreducible projective Brauer characters. Thus $\mathrm{Sym}^2 V$ is semisimple.

Remark. The argument in the proof of Theorem A1 involving the Frobenius–Schur index is only needed for $p = 3$. If $p > 3$, then the last two statements in the proof are clear.

Serre has pointed out that V can be defined directly as $E \otimes X$, where E is an indecomposable two-dimensional module of $P = G/T$ and X is the irreducible G-module afforded by $\tilde{\chi}$ as a Brauer character.

A.4

THEOREM A2. *Suppose that $p = 2$. Let $q \equiv 3 \pmod 8$ be a prime power and let $G = \mathrm{SL}(2, q)$. Then there exists a non-semisimple $k[G]$-module V of dimension $(q+1)/2$ such that $\wedge^2 V$ is semisimple.*

Proof. The irreducible characters in the principal 2-block of $\mathrm{PSL}(2, q)$ are 1, St, ψ_1, and ψ_2, where $\psi_i(1) = (q-1)/2$ for $i = 1, 2$. The restriction of ψ_i to a Borel subgroup is irreducible and so ψ_i is irreducible as a Brauer character. The remaining 2-blocks of PSL$(2, q)$ are either of defect 0 or 1.

There are $(q - 3)/8$ 2-blocks B_i of PSL$(2, q)$ of defect 1. The Brauer tree of each B_i has two vertices and one edge, and so every irreducible character in B_i is irreducible as a Brauer character.

Let χ_{i1} and χ_{i2} be the irreducible characters in B_i. The notation can be chosen so that $\chi_{i1}(u) = 2$ and $\chi_{i2}(u) = -2$ for an involution u.

SL$(2, q)$ has a faithful irreducible character η of degree $(q + 1)/2$ whose values lie in $\mathbb{Q}(\sqrt{-q})$ with $\eta = 1 + \psi_1$ as a Brauer character. By Corollary A.1.2 there exists an R-free $R[G]$-module W which affords η such that $V = W/\pi W$ is indecomposable. The center of G acts trivially on $\wedge^2 W$ and so $\wedge^2 W$ is an R[PSL$(2, q)$]-module. Direct computation shows that $\wedge^2 W$ affords $\psi_1 + \Sigma \chi_{i1}$. By Corollary A.1.1, $\wedge^2 V$ is semisimple.

REFERENCES

1. N. Bourbaki, Modules et anneaux semi-simples, *in* ‘‘Algèbre,’’ Chap. VIII, Hermann, Paris, 1958.
2. C. Chevalley, ‘‘Théorie des Groupes de Lie,’’ Vol. III, Hermann, Paris, 1954.
3. P. Deligne, Catégories tannakiennes, *in* ‘‘The Grothendieck Festschrift,’’ Vol. II, pp. 111–195, Birkhäuser, Boston, 1990.
4. W Feit, ‘‘The Representation Theory of Finite Groups,’’ North-Holland, Amsterdam, 1982.
5. B. Huppert, ‘‘Endliche Gruppen’’ I, Springer-Verlag, Berlin/New York, 1967.
6. J.-P. Serre, Sur la semi-simplicité des produits tensoriels de représentations de groupes, *Invent. Math.* **116** (1994), 513–530.