A remark on a theorem of Ritter and Segal

Serge Bouc

A well-known theorem proved independently by Ritter ([4]) and Segal ([5]) states that if P is a p-group, then the natural morphism from the Burnside ring $B(P)$ of P to the Grothendieck ring $R_{\mathbb{Q}}(P)$ of rational representations of P, mapping a finite P-set X to the permutation module $\mathbb{Q}X$, is surjective.

The object of this note is to complete this theorem in the following way:

Theorem 1 *Let p be a prime number, and P be a finite p-group. If V is a non-trivial simple $\mathbb{Q}P$-module, then there exist subgroups $R \supset Q$ of P, with $|R:Q| = p$, and an isomorphism of $\mathbb{Q}P$-modules*

$$V \simeq \mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$$

where $\Omega_{R/Q}$ is the augmentation ideal of the group algebra $\mathbb{Q}R/Q$.

In other words there is an exact sequence of $\mathbb{Q}P$-modules

$$0 \to V \to \mathbb{Q}(P/Q) \to \mathbb{Q}(P/R) \to 0$$

where the map $\mathbb{Q}(P/Q) \to \mathbb{Q}(P/R)$ is the natural projection. In particular in $R_{\mathbb{Q}}(P)$

$$V = \mathbb{Q}(P/Q) - \mathbb{Q}(P/R)$$

The following lemma is a special case of this theorem:

Lemma 2 *1. Let P be a cyclic p-group. Then the modules*

$$\mathrm{Ind}_R^P \mathrm{Inf}_{R/\Phi(R)}^R \Omega_{R/\Phi(R)}$$

for non-trivial subgroups R of G, are the non-trivial irreducible $\mathbb{Q}P$-modules.

2. Let P be an elementary abelian p-group. Then the modules

$$\mathrm{Inf}_{P/Q}^P \Omega_{P/Q}$$

for subgroups Q of index p in P are the non-trivial simple $\mathbb{Q}P$-modules.

Proof: The number of simple $\mathbb{Q}P$-modules for a finite group P is equal to the number of conjugacy classes of cyclic subgroups of P (see [6] Chapitre 13 Théorème 29 Corollaire 1). Hence in both cases, it suffices to show that the listed modules are simple and not isomorphic to each other. Indeed the number of non-trivial subgroups of a cyclic group P is equal to the number of (conjugacy classes of) cyclic subgroups of P, minus one, and the number of subgroups of index p in an elementary abelian p-group P is equal to the number of (conjugacy classes of) cyclic subgroups of P, minus one.

If P is cyclic of order p^n, and R is a subgroup of P of order $p^d > 1$, then the module $\mathrm{Ind}_R^P \mathrm{Inf}_{R/\Phi(R)}^R \Omega_{R/\Phi(R)}$ has dimension $p^{n-d}(p-1)$. Thus as d varies from 1 to n, those modules are not isomorphic to each other. Since moreover

$$\mathrm{Ind}_R^P \mathrm{Inf}_{R/\Phi(R)}^R \Omega_{R/\Phi(R)} \simeq \mathrm{Inf}_{P/\Phi(R)}^P \mathrm{Ind}_{R/\Phi(R)}^{P/\Phi(R)} \Omega_{R/\Phi(R)}$$

and since inflation takes simple modules to simple modules, it suffices to prove that for any cyclic p-group P, if R is the subgroup of P of order p, the module $V = \mathrm{Ind}_R^P \Omega_R$ is simple. But looking at scalar products of the character of V with complex characters of P shows that the character of V is the sum of all primitive characters of P. If W is a non-zero rational direct summand of V, with character χ_W, then there is a primitive complex character ζ of P such that the scalar product (χ_W, ζ) is non-zero, hence equal to 1. It follows that $(\chi_W, {}^s\zeta) = 1$ for all automorphism s of the field of p^n-th roots of unity. Since the Galois group of this field is transitive on the primitive roots of unity, it follows that $(\chi_W, \zeta') = 1$ for all primitive complex character ζ' of P. This shows that the character of W is equal to the character of V, hence that $W = V$. Thus V is a simple $\mathbb{Q}P$-module.

Now if P is elementary abelian, the modules $\mathrm{Inf}_{P/Q}^P \Omega_{P/Q}$, for $|P : Q| = p$, are inflated from simple modules for the group of order p, by the previous discussion of the cyclic group case. Hence they are simple. Since the kernel of $\mathrm{Inf}_{P/Q}^P \Omega_{P/Q}$ is Q, it follows that those modules are not isomorphic to each other. □

Corollary 3 *Let E be an elementary abelian subgroup of P. Then any simple $\mathbb{Q}P$-module has dimension at most $(p-1)|P : E|$.*

Proof: Let V be a simple $\mathbb{Q}P$-module, and E be an elementary abelian subgroup of P. By Frobenius reciprocity, there is a non-zero morphism of $\mathbb{Q}P$-modules from V to $\mathrm{Ind}_E^P \mathrm{Res}_E^P V$. Since $\mathbb{Q}P$ is semi-simple, this morphism is split injective, and there is a simple direct summand W of $\mathrm{Res}_E^P V$ such that V is a direct summand of $\mathrm{Ind}_E^P W$. By lemma 2, the dimension of W is at most $p-1$, thus $\dim_{\mathbb{Q}} V \leq |P : E|(p-1)$. □

Proof of theorem 1: The following proof is inspired by methods of M. Enguehard ([2]), and goes by induction on the order of P. I can suppose that P is neither cyclic nor elementary abelian.

Let V be a non-trivial simple $\mathbb{Q}P$-module. If V is not faithful, then there exists a non-trivial normal subgroup N of P such that

$$V \simeq \mathrm{Inf}_{P/N}^P W$$

where W is a $\mathbb{Q}(P/N)$-module. If V is simple and non-trivial, then so is W. By induction hypothesis, there are subgroups $R/N \supset Q/N$ of P/N such that

$$W \simeq \mathrm{Ind}_{R/N}^{P/N} \mathrm{Inf}_{R/Q}^{R/N} \Omega_{R/Q}$$

Taking inflation to P gives

$$V \simeq \mathrm{Ind}_R^P \mathrm{Inf}_{R/N}^R \Omega_{R/Q} \simeq \mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$$

Hence I can suppose that V is faithful. Now there are two cases:

• There exists a normal subgroup E of P which is elementary abelian of order p^2. Let L be a simple summand of $\mathrm{Res}_E^P V$ as a $\mathbb{Q}E$-module, and let I denote the inertial subgroup of L in P, i.e.

$$I = \{x \in P \mid {}^x L \simeq L\}$$

Then by Clifford theory (see [1] Theorem 11.1) there exists a positive integer e such that

$$\mathrm{Res}_E^P V \simeq e(\sum_{g \in P/I} {}^g L)$$

Let $\tilde{L}$ denote the L-isotypic component of $\mathrm{Res}_E^P V$ (i.e. the submodule generated by all simple summands isomorphic to L). Then

$$V \simeq \mathrm{Ind}_I^P \tilde{L}$$

Now I contains the centralizer $C_P(E)$ of E in P, and the quotient $P/C_P(E)$ is a p-subgroup of the automorphism group of E, which has order $p(p-1)(p^2-1)$. Hence I has index 1 or p in P.

If $|P:I| = p$, then $V \simeq \mathrm{Ind}_I^P \tilde{L}$, and $\tilde{L}$ is a simple I-module. It cannot be the trivial module, since in this case $V \simeq \mathrm{Ind}_I^P \mathbb{Q}$ which is not simple. By induction hypothesis, there exist subgroups $R \supset Q$ of P such that

$$\tilde{L} \simeq \mathrm{Ind}_R^I \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$$

Taking induction up to P gives

$$V \simeq \mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$$

Hence I can suppose $I = P$, and in this case $V = \tilde{L}$. If V is faithful, then L has to be a faithful simple $\mathbb{Q}E$-module. By Lemma 2, there are no such simple $\mathbb{Q}E$-modules, and this is a contradiction.

• The other case is when P has no normal subgroup of order p^2. In this case, by Theorem 4.10 of Chapter 5 of [3], the group P is cyclic if p is odd, and if $p = 2$, the group P is cyclic, or quaternion of order at least 8, dihedral of order at least 16, or semi-dihedral of order at least 16.

If P is cyclic, the result holds by Lemma 2. Hence I can suppose that $p = 2$, and P is quaternion, dihedral, or semi-dihedral, and P has order 2^n, with $n \geq 3$.

In this case P has a non-central cyclic subgroup A of index 2. Let C denote the unique subgroup of order 2 of A.

The restriction of V to A is a faithful $\mathbb{Q}A$-module, hence by lemma 2 it must contain $\mathrm{Ind}_C^A \Omega_C$ as a direct summand. In particular $\dim_{\mathbb{Q}} V \geq 2^{n-2}$.

Now if P contains an elementary abelian subgroup E of order 4, then there is a simple $\mathbb{Q}E$-module W such that V is a direct summand of $\mathrm{Ind}_E^P W$. Since W is one dimensional by lemma 2, it follows that $\dim_{\mathbb{Q}} V \leq |P:E| = 2^{n-2}$. Thus $\dim_{\mathbb{Q}} V = 2^{n-2}$, and V is isomorphic to $\mathrm{Ind}_E^P W$. Moreover W must be non-trivial, since otherwise $\mathbb{Q}$ is a direct summand of $\mathrm{Ind}_E^P W \simeq V$. Hence $W = \mathrm{Inf}_{E/F}^E \Omega_{E/F}$, for some subgroup F of E of index 2, and V has the form required for theorem 1.

If P contains no elementary abelian subgroup E of order 4 (and P is not cyclic), then P is generalized quaternion. In this case C is the only subgroup of P of order 2, and the simple $\mathbb{Q}C$-modules are one dimensional, isomorphic to $\mathbb{Q}$ and Ω_C. Since V is faithful, the restriction $\mathrm{Res}_C^P V$ must contain Ω_C as a direct summand. By Frobenius reciprocity, it follows that V is a direct summand of $M = \mathrm{Ind}_C^P \Omega_C$. To complete the proof of theorem 2, it suffices to show that M is simple.

This can be done by the following elementary proof. The quaternion group P of order 2^n has the following presentation

$$P = < x, y \mid x^{2^{n-1}} = 1,\ x^{2^{n-2}} = y^2,\ yxy^{-1} = x^{-1} >$$

The subgroup A is generated by x, and C is generated by $x^{2^{n-2}} = y^2$. The group P is the disjoint union of A and Ay. Thus

$$M = \mathbb{Q}P \otimes_{\mathbb{Q}C} \Omega_C = (\mathbb{Q}A \otimes_{\mathbb{Q}C} \Omega_C) \oplus (\mathbb{Q}Ay \otimes_{\mathbb{Q}C} \Omega_C)$$

Now the generator $x^{2^{n-2}}$ of C acts by -1 on Ω_C. It follows that

$$\mathbb{Q}A \otimes_{\mathbb{Q}C} \Omega_C \simeq \mathbb{F} = \mathbb{Q}[X]/<X^{2^{n-2}} + 1>$$

and this is an isomorphism of $\mathbb{Q}A$-modules if the action of x on $\mathbb{F}$ is given by multiplication by X. Moreover $\mathbb{F}$ is a field, since $X^{2^{n-2}} + 1$ is a cyclotomic polynomial.

Denote by σ the automorphism of $\mathbb{F}$ sending X to $X^{-1} = -X^{2^{n-2}-1}$, and by Y the element $y \otimes 1$ of $\mathbb{Q}Ay \otimes_{\mathbb{Q}C} \Omega_C$. Then $M \simeq \mathbb{F} \oplus \mathbb{F}Y$ as $\mathbb{Q}P$-modules, where the action of x is given by left multiplication by X, and the action of y is given by

$$y(A + BY) = -\sigma(B) + \sigma(A)Y, \quad \forall A, B \in \mathbb{F}$$

since moreover y^2 acts by -1 on Ω_C. In other words if M is endowed with the $\mathbb{Q}$-algebra structure induced by the following multiplication

$$(A' + B'Y)(A + BY) = A'A - B'\sigma(B) + \big(A'B + B'\sigma(A)\big)Y, \quad \forall A, A', B, B' \in \mathbb{F}$$

then the generators x and y of P act on M by multiplication by X and Y respectively. To show that M is simple, it suffices to show that M is a skew field. But for $A, B \in \mathbb{F}$

$$(A + BY)\big(\sigma(A) - BY\big) = A\sigma(A) + B\sigma(B) \in \mathbb{F}$$

If $A = a_0 + a_1X + \ldots + a_{2^{n-2}-1}X^{2^{n-2}-1}$ and $B = b_0 + b_1X + \ldots + b_{2^{n-2}-1}X^{2^{n-2}-1}$, with coefficients a_i and b_i in $\mathbb{Q}$, for $0 \leq i < 2^{n-2}$, then the coefficient of 1 in $A\sigma(A) + B\sigma(B)$ is equal to $a_0^2 + a_1^2 + \ldots + a_{2^{n-2}-1}^2 + b_0^2 + b_1^2 + \ldots + b_{2^{n-2}-1}^2$. This is positive if $A + BY$ is non-zero, hence $A\sigma(A) + B\sigma(B) \neq 0$ is invertible in $\mathbb{F}$, hence in M. Thus M is a skew-field, as was to be shown. □

In view of theorem 1, it is natural to ask when conversely, being given two subgroups $R \supset Q$ with $|R : Q| = p$, the module $\mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$ is an irreducible $\mathbb{Q}P$-module. A possible answer is the following:

Proposition 4 *Let p be a prime number, and P be a p-group. Let $R \supset Q$ be subgroups of P, with $|R : Q| = p$. Then the following conditions are equivalent:*

1. *The module $\mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$ is an irreducible $\mathbb{Q}P$-module.*
2. *If S is any subgroup of P such that $R \cap S \subseteq Q$, then $|S| < |R|$.*
3. *The group $N_P(Q)/Q$ is cyclic or generalized quaternion, the group R/Q is its unique subgroup of order p, and if S is any subgroup of P such that $|S| > |Q|$, then $S \cap N_P(Q) \not\subseteq Q$.*

Proof: Suppose first that the $\mathbb{Q}P$-module $\mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$ is irreducible. Then its character is orthogonal (for the scalar product) to any irreducible module of the form $S_{U,V} = \mathrm{Ind}_U^P \mathrm{Inf}_{U/V}^U \Omega_{U/V}$, where $U \supset V$ are subgroups of P with $|U:V| = p$ and $|U| > |R|$.

Those irreducible modules, together with the trivial one, generate the submodule M of $R_{\mathbb{Q}}(P)$ generated by the permutation modules $\mathbb{Q}(P/S) = \mathrm{Ind}_S^P \mathbb{Q}$, for $|S| \geq |R|$: clearly $S_{U,V} \in M$ if $|U| > |R|$, since $S_{U,V} = \mathrm{Ind}_V^P \mathbb{Q} - \mathrm{Ind}_U^P \mathbb{Q}$ in $R_{\mathbb{Q}}(P)$. Conversely, if S is a subgroup of P with $|S| \geq |R|$, then $\mathrm{Ind}_S^P \mathbb{Q}$ is the sum of the trivial module and of some irreducible modules $S_{U,V}$. And if $S_{U,V}$ is a direct summand of $\mathrm{Ind}_S^P \mathbb{Q}$, then in particular

$$\dim_{\mathbb{Q}} S_{U,V} = |P:U|(p-1) \leq \dim_{\mathbb{Q}} \mathrm{Ind}_S^P \mathbb{Q} - 1 = |P:S| - 1 < |P:S|$$

Thus

$$|S| \leq (p-1)|S| < |U|$$

and it follows that $|U| > |S| \geq |R|$.

Thus if $W_{R,Q} = \mathrm{Ind}_R^P \mathrm{Inf}_{R/Q}^R \Omega_{R/Q}$ is irreducible, then its character is orthogonal to the characters $\mathrm{Ind}_S^P 1$, for $|S| \geq |R|$. Since the character of $W_{R,Q}$ is equal to

$$\mathrm{Ind}_Q^P 1 - \mathrm{Ind}_R^P 1$$

and since the scalar product of $\mathrm{Ind}_Q^P 1$ with $\mathrm{Ind}_S^P 1$ is equal to the number of double cosets QxS, for $x \in P$, it follows that

$$|Q\backslash P/S| = |R\backslash P/S|$$

for any subgroup S of P with $|S| \geq |R|$. This is equivalent to requiring that $QxS = RxS$ for any $x \in P$, or equivalently that $R \subseteq Q.^x S$. Now this is equivalent to $R = Q(R \cap {}^x S)$, or $R \cap {}^x S \not\subseteq Q$ since Q has index p in R. It follows that if S is a subgroup of P with $R \cap S \subseteq Q$, then $|S| < |R|$. In other words, condition 1 implies condition 2.

Conversely, if condition 2 holds, then the previous discussion shows that the character of the module $W_{R,Q}$ is orthogonal to the characters of all the simple modules $S_{U,V}$, for $|U| > |R|$. Now for dimension reasons, the module $W_{R,Q}$ cannot have a simple direct summand $S_{U,V}$, for $|U| < |R|$. It follows that $W_{R,Q}$ has a direct summand $S_{U,V}$, with $|U| = |R|$. Then $S_{U,V}$ and $W_{R,Q}$ have the same dimension, hence they are isomorphic. Hence $W_{R,Q}$ is irreducible, and this completes the proof of the equivalence of conditions 1 and 2.

If condition 2 holds, and if S is a subgroup of P containing Q, and not containing R, the intersection $R \cap S$ is equal to Q, since Q is maximal in R. It follows that $|S| < |R|$, or equivalently that $|S| \leq |Q|$. Hence $S = Q$, and R is the smallest element of $]Q, P]$. Hence it is the smallest element of $]Q, N_P(Q)]$, and the group $N_P(Q)/Q$ has a single subgroup R/Q of order p. It follows that $N_P(Q)/Q$ is cyclic or generalized quaternion. If S is any subgroup of P with $|S| > |Q|$, or equivalently $|S| \geq |R|$, then $R \cap S \not\subseteq Q$. Since $R \subseteq N_P(Q)$, it follows that $S \cap N_P(Q) \not\subseteq Q$ and 2 implies 3.

Conversely if 3 holds, and if S is any subgroup of P with $|S| \geq |R|$, then $S \cap N_P(Q) \not\subseteq Q$ and $Q.\big(S \cap N_P(Q)\big) \neq Q$. Since R/Q is the unique minimal non-trivial subgroup of $N_P(Q)/Q$, it follows that $R \subseteq Q.\big(S \cap N_P(Q)\big)$, or equivalently $R = Q.\big(R \cap S \cap N_P(Q)\big) = Q.(R \cap S)$. Thus $R \cap S \not\subseteq Q$, and 3 implies 2. □

Theorem 1 has the following easy consequence:

Corollary 5 *Let P be a p-group, and V be a finite dimensional $\mathbb{Q}P$-module. Then*

$$\dim_{\mathbb{Q}} V \equiv \dim_{\mathbb{Q}} V^P \mod (p-1)$$

More generally, for $k \in \mathbb{N}$ denote by N_k the intersection of all subgroups S of P with $|P:S| = p^k$. Then

$$\dim_{\mathbb{Q}} V \equiv \dim_{\mathbb{Q}} V^{N_k} \mod p^k(p-1)$$

Proof: The first congruence is a special case of the second one, when $k = 0$. To prove this second congruence, decompose V as a direct sum of simple modules

$$V = n_1\mathbb{Q} \oplus \bigoplus_{S_{R,Q} \in \Sigma} n_{R,Q} S_{R,Q}$$

for integers n_1 and $n_{R,Q}$, where Σ is a set of mutually non-isomorphic non-trivial simple modules $S_{R,Q}$. Now since N_k is a normal subgroup of P, the set of fixed points $S_{R,Q}^{N_k}$ is a $\mathbb{Q}P$-submodule of $S_{R,Q}$. Hence it is zero or the whole of $S_{R,Q}$. This last case occurs exactly when N_k acts trivially on $S_{R,Q}$, i.e. when $N_k \subseteq Q$. It follows that

$$V^{N_k} = n_1\mathbb{Q} \oplus \bigoplus_{S_{R,Q}} n_{R,Q} S_{R,Q}$$

where the sum runs over those simple modules $S_{R,Q} \in \Sigma$ for which $Q \supseteq N_k$.

The previous two equations show that

$$\dim_{\mathbb{Q}} V = \dim_{\mathbb{Q}} V^{N_k} + \sum_{S_{R,Q}} n_{R,Q} \dim_{\mathbb{Q}} S_{R,Q}$$

where the sum runs over those simple modules $S_{R,Q} \in \Sigma$ for which $Q \not\supseteq N_k$. This implies $|P:Q| > p^k$, i.e. $|P:R| \geq p^k$. Now the dimension of $S_{R,Q}$ is equal to $|P:R|(p-1)$, and the congruence follows. □

Acknowledgments: I wish to thank the referee for suggesting substantial simplifications of the proof of theorem 1.

References

[1] C. Curtis and I. Reiner. *Methods of representation theory with applications to finite groups and orders*, volume 1 of *Wiley classics library*. Wiley, 1990.

[2] M. Enguehard. Sur les caractères de permutation d'un groupe fini. Technical report, Université Paris 7, 1974. Thesis.

[3] D. Gorenstein. *Finite groups*. Chelsea.

[4] J. Ritter. Ein Induktionssatz für rational Charaktere von nilpotenten Gruppen. *J. f. reine u. angew. Math.*, 254:133–151, 1972.

[5] G. Segal. Permutation representations of finite p-groups. *Quart. J. Math. Oxford*, 23:375–381, 1972.

[6] J.-P. Serre. *Représentations linéaires des groupes finis*. Méthodes. Hermann, second edition, 1971.