

HALL-HIGMAN TYPE THEOREMS. IV

T. R. BERGER¹

ABSTRACT. Hall and Higman's Theorem B is proved by constructing the representation in the group algebra. This proof is independent of the field characteristic, except in one case.

Let R be an extra special r group. Suppose $C \leq \text{Aut}(R)$ is cyclic, irreducible faithful on $R/Z(R)$, and trivial on $Z(R)$. The group CR and its representation theory have been widely studied and are of some importance. Let k be a field of characteristic $q \neq r$ containing a splitting field for R . Then any faithful irreducible $k[R]$ -module V is absolutely irreducible and extends to CR .

Hall and Higman [3] studied $V|_C$ when C was a q group. Their result is proved using inequalities on the dimension of $\text{Hom}_{k[C]}(V, V)$. This proof also works if we only know $q \mid |C|$. The central ideal of this proof also works when $(q, |C|) = 1$ [5]. However, the count is quite different. There are character proofs of the result when $(q, |C|) = 1$ [1]. Thompson gave a very pretty proof of Hall and Higman's original result using vertices and sources [4].

These proofs suffer from one or more of the following difficulties:

- (1) They are all tied to the characteristic q .
- (2) When $q \mid |C|$ they depend upon knowing all indecomposable $k[C]$ -modules.
- (3) They are indirect in that they do not construct a representation of CR .

The theorem in all cases is that $V|_C$ is a direct sum of copies of the regular C -module and one other module U isomorphic to $k[C]/k[C]F$ where $F = \sum_{x \in C} x$. The number of regular modules and the appearance of U are completely independent of the field characteristic. This makes (1) a strong objection. Objection (2) becomes important if we drop the condition that C be cyclic. Finally, a "useful" construction of a given module is often better than no construction at all.

Received by the editors February 11, 1972.

AMS (MOS) subject classifications (1970). Primary 20C15, 20C20; Secondary 16A64, 20H20.

Key words and phrases. Hall-Higman Theorem B, representation theory, group theory, group algebra, modular representation.

¹ This research was partially supported by NSF grant GP-29224X.

© American Mathematical Society 1973

The object of this paper is to remedy these three objections for *odd primes* r . The representation of CR on V is explicitly constructed independent of field characteristic. Then its restriction to C is studied. If $|R|=r^{2e+1}$ then it is shown that $V|_C$ contains $(r^e+1)/|C|-1$ copies of the regular C -module and one copy of $k[C]/k[C]F$.

I. A remark on central simple algebras.

(1.1) Suppose k is a field and A is a central simple algebra over k of dimension t^2 . Assume B is a commutative quasi-Frobenius subalgebra with 1. Let V be an irreducible A -module. Then $V|_B \simeq {}_B B \oplus U$ where ${}_B B$ is B^+ considered as a left B -module and U is some complementary B -module.

The proof is easy. Since B is quasi-Frobenius, ${}_B B$ is injective. Now $B^+ \subseteq A^+$ so that ${}_A A|_B \simeq {}_B B \oplus W$ for some B -module W . The subalgebra B is commutative. So in a complete decomposition of ${}_B B$ into indecomposables, each indecomposable summand appears with multiplicity one. For some $s|t$, ${}_A A \simeq s \times V$ where V is the irreducible A -module uniquely determined up to isomorphism. Using the Krull-Schmidt theorem to compare complete decompositions of the isomorphic modules ${}_B B \oplus W$ and $s \times V|_B$ we discover that ${}_B B$ is isomorphic to a summand of $V|_B$.

(1.2) If in (1.1) the dimension of B is t then $V|_B \simeq {}_B B$.

(1.3) Suppose k is a field and $g(x) \in k[x]$ has positive degree. Then $k[x]/(g(x))$ is a quasi-Frobenius algebra.

This is well known. See [2, Section 58, Problem 2(c)].

II. A nonsingular matrix.

(2.1) Let r be an odd prime and $K = GF(r)$. Let V be an $e \geq 1$ dimensional vector space over K and $f: V \times V \rightarrow K$ a nonsingular symmetric form.

Since $Z/rZ \simeq GF(r)$ for the integers Z , we may imagine that each $a \in K$ is a least residue in Z .

(2.2) If k is a field of characteristic $q \neq r$ containing a primitive r th root of unity ζ then the matrix $M = [\zeta^{a\beta}]_{(\alpha, \beta) \in K \times K}$ is nonsingular.

Let $N = [\zeta^{-a\beta}]$. Then the (β, γ) entry of MN is

$$\sum_{\alpha} \zeta^{\beta\alpha - \alpha\gamma} = \sum_{\alpha} \zeta^{(\beta - \gamma)\alpha} = 0$$

unless $\beta = \gamma$ in which case it is r . So $MN = rI$ where I is the identity. Since $r \neq 0$ in k , M has inverse $r^{-1}N$.

(2.3) If k is a field of characteristic $q \neq r$ containing a primitive r th root of unity ζ then the matrix $M = [\zeta^{f(u,v)}]_{(u,v) \in V \times V}$ is nonsingular.

We proceed by induction on $\dim V$. If $\dim V=1$ then $f(\alpha u, \beta u)=\alpha\beta\mu$ for some $\mu \neq 0$ in K so M is the matrix of (2.2) with $\zeta\mu$ in place of ζ and (2.3) holds in this case.

Suppose $\dim V=e$ and (2.3) holds for all spaces of smaller dimension. Let $\{v_1, \dots, v_e\}$ be an orthogonal basis for V . Such a basis exists since r is odd. Let $U=\langle v_2, \dots, v_e \rangle$. Now $f(v_1, v_1)=\mu$. Set $B=[\zeta^{\alpha\beta\mu}]$. Then we may arrange M into blocks

$$\begin{aligned} M &= [\zeta^{f(\alpha v_1+u, \beta v_1+v)}] \\ &= [\zeta^{\alpha\beta\mu+f(u,v)}] = [B\zeta^{f(u,v)}] \\ &= B \otimes [\zeta^{f(u,v)}]_{(u,v) \in U \times U}. \end{aligned}$$

So our matrix is formed as a Kronecker product. Now $\dim U=e-1$ so the second matrix in the product is nonsingular. The first matrix is just the matrix of (2.2) for some primitive root; hence is nonsingular. Therefore M is nonsingular.

As a corollary we obtain the following:

(2.4) Let $\tilde{K}=\text{GF}(r^e)$. Let $\Gamma \in \tilde{K}^\times$, $\text{Tr}: \tilde{K} \rightarrow K$ the trace map, $V=\tilde{K}^+$, and $f(u, v)=\text{Tr}(\Gamma uv)$. Let ζ be a primitive r th root in k of characteristic $q \neq r$. If $\phi_u \in k$, $u \in \tilde{K}$ and $\sum_u \phi_u \zeta^{f(u,v)}=0$ for all $v \in \tilde{K}$, then all $\phi_u=0$.

The ϕ_u 's give a linear dependence on the columns of M in (2.3). So this is obvious.

III. The group. Let r be an odd prime and $e \geq 1$ an integer. Let $K=\text{GF}(r)$, $\tilde{K}=\text{GF}(r^e)$, and $\hat{K}=\text{GF}(r^{2e})$. Let \mathcal{G} be the Galois group of \hat{K}/K and $\phi \in \mathcal{G}$ the element of order two in \mathcal{G} . Let $\mu \in \hat{K}^+$ be of order r^e+1 . Set $v=\mu-\mu^{-1}$. For $u, v \in \hat{K}^+$ set

$$h(u, v) = 2^{-1} \text{Tr}(v[uv^\phi - u^\phi v])$$

where $\text{Tr}: \tilde{K} \rightarrow K$ is the trace map.

Note that $v[uv^\phi - u^\phi v] \in \tilde{K}$, the fixed field of ϕ . Thus h is a nonsingular alternating form on \hat{K}^+ . Let $R=\hat{K}^+ \times K^+$. For $(u, \zeta), (v, \xi) \in R$ set

$$(u, \zeta)(v, \xi) = (u + v, h(u, v) + \zeta + \xi).$$

This multiplication makes R into an extra special r group of exponent r and order r^{2e+1} .

Let $C=\langle \mu \rangle$. Now C acts as automorphisms of R by

$$(u, \zeta)^x = (ux, \zeta) \quad \text{for } x \in C, \quad (u, \zeta) \in R.$$

We let $G=CR$ be the semidirect product of R by C .

If $G_0 = C_0 R_0$ where R_0 is a normal extra special r subgroup of G_0 with $Z(R_0) = Z(G_0)$ and C_0 is a cyclic r' group irreducible on $R_0/Z(R_0)$ then G_0 is isomorphic to a subgroup of G . This fact seems to be well known. In any case it is a straightforward computation.

IV. The group algebra of CR . Let k be a field of characteristic $q \neq r$ which contains a primitive r th root of 1.

We now state some facts about the group algebra of R over k . Let λ be a primitive r th root of unity in k . If $z = (0, 1) \in R$ then set

$$(4.1) \quad E = r^{-1}(\lambda^{r-1} + \lambda^{r-2}z + \cdots + \lambda z^{r-2} + z^{r-1})$$

and

$$\begin{aligned} \chi((u, \zeta)) &= 0 & \text{if } u \neq 0, \\ &= r^e \lambda^\zeta & \text{if } u = 0. \end{aligned}$$

Then E is the primitive central idempotent of $k[R]$ belonging to the irreducible character χ . Also $k[R]E$ is a central simple algebra of dimension r^{2e} over k .

Let $c \in C^\#$ and set

$$\mathcal{O}_c = \{(v, -h(vv^\phi(c-1)^{-1}), 1) \mid v \in \hat{K}^+\}$$

and

$$(4.2) \quad K_c = -r^{-e} \sum_{x \in \mathcal{O}_c} xE.$$

$$(4.3) \quad \text{If } x \in R \text{ and } c \in C^\# \text{ then } K_c x^c = x K_c.$$

Before starting we note a few properties of the form h . If $u, v \in \hat{K}$ then

$$h(u, v) = h(v^\phi, u^\phi) = -h(v, u) = h(uv^\phi, 1) = -h(vu^\phi, 1).$$

We let $h(u) = h(u, 1)$. There should be no confusion since the two h 's are related and functions of different numbers of variables. Now $h(u)$ is a nontrivial K -linear functional from \hat{K} to K .

For $x = (u, \delta)$, we compute

$$\begin{aligned} -r^e x^{-1} K_c x^c &= \sum_v (u, \delta)^{-1} (v, -h(vv^\phi[c-1]^{-1}))(u, \delta)^c E \\ &= \sum_v (-u, -\delta)(v, -h(vv^\phi[c-1]^{-1}))(uc, \delta) E \\ &= \sum_t (t, -h([t-u(c-1)][t-u(c-1)]^\phi(c-1)^{-1} \\ &\quad + u[t-u(c-1)]^\phi - [t-u(c-1)]u^\phi c^{-1} + uu^\phi c^{-1})) E. \end{aligned}$$

Here we have substituted $t = v + u(c-1)$. Proceeding further,

$$= \sum (t, -h(tt^\phi(c-1)^{-1}))(0, -h(uu^\phi)) E.$$

But $uu^\phi \in \tilde{K}$ so $h(uu^\phi)=0$. Thus $-r^e x^{-1} K_c x^e = -r^e K_c$. This proves (4.3). We now compute $K_c K_d$ for $c, d \in C^\#$.

$$\begin{aligned} r^{2e} K_c K_d &= \sum_u (u, -h(uu^\phi(c-1)^{-1})) \sum_v (v, -h(vv^\phi(d-1)^{-1})) E \\ &= \sum_{u,v} (u+v, -h(uu^\phi(c-1)^{-1} + vv^\phi(d-1)^{-1} - uv^\phi)) E. \end{aligned}$$

Let $t=u+v$ and compute,

$$\begin{aligned} (*) \quad &= \sum_{t,v} (t, -h(tt^\phi(c-1)^{-1} + tv^\phi(c^{-1}-1)^{-1} - vt^\phi(c-1)^{-1} \\ &\quad + vv^\phi[1 + (c-1)^{-1} + (d-1)^{-1}])) E. \end{aligned}$$

(4.4) For $c \in C^\#$, $K_c K_{c^{-1}} = E$.

From our computation of $K_c K_d$ we obtain,

$$\begin{aligned} r^{2e} K_c K_{c^{-1}} &= \sum_{t,v} (t, -h(tt^\phi(c-1)^{-1} + tv^\phi(c^{-1}-1)^{-1} - vt^\phi(c-1)^{-1} \\ &\quad + vv^\phi[1 + (c-1)^{-1} + (c^{-1}-1)^{-1}])) E \\ &= \sum_t (t, -h(tt^\phi(c-1)^{-1})) \\ &\quad \cdot \sum_v (0, -h(tv^\phi(c^{-1}-1)^{-1} - vt^\phi(c-1)^{-1})) E. \end{aligned}$$

Now

$$tv^\phi(c^{-1}-1)^{-1} - vt^\phi(c-1)^{-1} = [t(c^{-1}-1)^{-1}]v^\phi - v[t(c^{-1}-1)^{-1}]^\phi.$$

Set $A(t) = t(c^{-1}-1)^{-1}$. Then the second term of the above expression is

$$\sum_v (0, -h(A(t)v^\phi - A(t)^\phi v)) E.$$

But $-h(A(t)v^\phi - A(t)^\phi v) = f(v)$ is a nontrivial K -linear map of \hat{K}^+ onto K provided $t \neq 0$. But then the sum is

$$\begin{aligned} \sum_v (0, f(v)) E &= r^{2e-1} \sum_{\alpha \in K} (0, \alpha) E \quad \text{if } t \neq 0, \\ &= r^{2e} (0, 0) E \quad \text{if } t = 0. \end{aligned}$$

Now $\sum_\alpha (0, \alpha) E = \sum_\alpha \lambda^\alpha E = 0$. So our sum is zero unless $t=0$. Then we get

$$r^{2e} K_c K_{c^{-1}} = r^{2e} E.$$

We now have the obvious corollary:

(4.5) If $c \in C^\#$ then K_c is invertible in $k[R]E$ and has inverse equal to $K_{c^{-1}}$.

Let $K_1 = E$.

(4.6) The map $cx \rightarrow K_c x E$ is a representation of CR in $k[R]E$.

The collection $\{(v, 0)E | v \in \hat{K}\}$ is a k -basis for $k[R]E$. Also $k[R]E$ is a central simple algebra over k . Thus $cx \rightarrow K_c x E$ is a projective representation of CR with a factor set n by (4.3) and (4.5). Further, n is trivial on R . That is, $K_c^{-1}(v, 0)K_c = (v, 0)^c$ all $v \in \hat{K}$.

But then $K_c K_d = n(c, d)K_{cd}$. We continue our earlier computation from (*) for the case $d \neq c^{-1}$.

$$\begin{aligned} r^{2e} K_c K_d &= \sum_t (t, -h(tt^\phi(cd - 1)^{-1})) \\ &\quad \cdot \sum_v (0, -h(tt^\phi[(c - 1)^{-1} - (cd - 1)^{-1}] + tv^\phi(c^{-1} - 1)^{-1} \\ &\quad - vt^\phi(c - 1)^{-1} + vv^\phi[1 + (c - 1)^{-1} + (d - 1)^{-1}]))E. \end{aligned}$$

Put the last sum equal to $A'(t)$. Then

$$\begin{aligned} &= \sum_t (t, -h(tt^\phi(cd - 1)^{-1}))A'(t)E \\ &= -r^e n(c, d) \sum_t (t, -h(tt^\phi(cd - 1)^{-1}))E. \end{aligned}$$

Since $A'(t)$ is a sum of elements from $Z(R)$, $A'(t)E = a(t)E$ where $a(t) \in k$. Further, $\{(t, -h(tt^\phi(cd - 1)^{-1}))E | t \in \hat{K}\}$ is a k -basis for $k[R]E$. Therefore $-r^e n(c, d) = a(t)$ for all values of t . In particular,

$$\begin{aligned} -r^e n(c, d)E &= a(0)E \\ &= \sum_v (0, -h(vv^\phi[1 + (c - 1)^{-1} + (d - 1)^{-1}]))E. \end{aligned}$$

The map $v \rightarrow vv^\phi$ is the norm map $N: \hat{K}^\times \rightarrow \tilde{K}^\times$. The kernel has order $r^e + 1$. Therefore

$$\begin{aligned} -r^e n(c, d)E &= E + \sum_{v \in \hat{K}^\times} (0, -h(vv^\phi[1 + (c - 1)^{-1} + (d - 1)^{-1}]))E \\ &= E + (r^e + 1) \sum_{u \in \tilde{K}^\times} (0, -h(u[1 + (c - 1)^{-1} + (d - 1)^{-1}]))E \\ &= -r^e E + (r^e + 1) \sum_{u \in \tilde{K}} (0, -h(u[1 + (c - 1)^{-1} + (d - 1)^{-1}]))E. \end{aligned}$$

Now $-h(u[1 + (c - 1)^{-1} + (d - 1)^{-1}]) = f(u)$ is a nontrivial K -linear map of \tilde{K} to K since $d \neq c^{-1}$. Thus

$$\begin{aligned} -r^e n(c, d)E &= -r^e E + (r^e + 1) \sum_u (0, f(u))E \\ &= -r^e E + r^{e-1}(r^e + 1) \sum_{\alpha \in K} (0, \alpha)E = -r^e E. \end{aligned}$$

Thus $n(c, d) = 1$ if $d \neq c^{-1}$. By (4.4) and the definition of K_1 we know that

$$n(1, c) = n(c, 1) = n(c, c^{-1}) = n(c^{-1}, c) = 1.$$

So n is the trivial factor set and we have an ordinary representation.

$$(4.7) \quad \sum_{c \in C^\#} K_c = -E.$$

As usual, we compute

$$\begin{aligned} -r^e \sum_{c \in C^\#} K_c &= \sum_{c, v} (v, -h(vv^\phi(c-1)^{-1}))E \\ &= \sum_v (v, 0) \sum_c (0, -h(vv^\phi(c-1)^{-1}))E. \end{aligned}$$

Fix $v \neq 0$. Compute

$$\begin{aligned} -h(vv^\phi(c-1)^{-1}) &= -\text{Tr}(2^{-1}vv^\phi[(c-1)^{-1} - (c^{-1}-1)^{-1}]) \\ &= -\text{Tr}(2^{-1}vv^\phi v(c+1)/(c-1)). \end{aligned}$$

Next we show that the map $c \rightarrow v(c+1)/(c-1)$ is a one-one map of $C^\#$ onto \tilde{K} . Note that $(v(c+1)/(c-1))^\phi = v(c+1)/(c-1)$ so the map is into \tilde{K} . Since $|C^\#| = r^e = |\tilde{K}|$, if the map is one-one, it is onto. So suppose

$$v \frac{c+1}{c-1} = v \frac{d+1}{d-1}, \quad c, d \in C^\#.$$

Then $(c+1)(d-1) = (d+1)(c-1)$ or $2(c-d) = 0$. But r is odd so $c = d$. Thus the map is one-one onto \tilde{K} .

Returning again to our computation

$$\begin{aligned} -r^e \sum_{c \in C^\#} K_c &= \sum_v (v, 0) \sum_{u \in \tilde{K}} (0, -\text{Tr}(2^{-1}vv^\phi u))E \\ &= r^e(0, 0)E + \sum_{v \neq 0} (v, 0)r^{e-1} \sum_{\alpha \in K} (0, \alpha)E = r^e E. \end{aligned}$$

This proves (4.7).

(4.8) $\{K_c | c \in C^\#\}$ is a linearly independent set of vectors in $k[R]E$.

Suppose there are constants $\psi_c \in k$ so that $\sum_{c \in C^\#} \psi_c K_c = 0$. Then

$$\begin{aligned} 0 &= -r^e \sum_{c \in C^\#} \psi_c K_c = \sum_{c \in C^\#; v \in \hat{K}} \psi_c (v, -h(vv^\phi(c-1)^{-1}))E \\ &= \sum_{v \in \hat{K}} (v, 0) \sum_c \psi_c (0, -h(vv^\phi(c-1)^{-1}))E. \end{aligned}$$

But $\{(v, 0)E | v \in \hat{K}\}$ is a k -basis for $k[R]E$. Therefore

$$\sum_c \psi_c(0, -h(vv^\phi(c-1)^{-1}))E = 0$$

for all $v \in \hat{K}$. But $v \mapsto vv^\phi$ is the norm map from \hat{K} to \tilde{K} and is onto. So

$$\sum_c \psi_c(0, -h(\alpha(c-1)^{-1}))E = 0$$

for all $\alpha \in \tilde{K}$.

Next look at

$$\begin{aligned} h(\alpha(c-1)^{-1}) &= 2^{-1} \text{Tr}(\nu\alpha[(c-1)^{-1} - (c^{-1} - 1)^{-1}]) \\ &= 2^{-1} \text{Tr}(\alpha\nu(c+1)/(c-1)). \end{aligned}$$

In (4.7) we saw that the map $c \mapsto \nu(c+1)/(c-1)$ was one-one from $C^\#$ onto \tilde{K} . Let $\beta = \beta(c) = \nu(c+1)/(c-1)$. Then we may take $\psi_c = \psi'_{\beta(c)} = \psi'_\beta$ and

$$0 = \sum_{\beta \in \tilde{K}} \psi'_\beta(0, f(\alpha, \beta))E$$

for all $\alpha \in \tilde{K}$ where $f(\alpha, \beta) = -2^{-1} \text{Tr}(\alpha\beta)$ is a nonsingular symmetric form from $\tilde{K} \times \tilde{K}$ to K . That is,

$$0 = \sum_{\beta \in \tilde{K}} \psi'_\beta \lambda^{f(\alpha, \beta)} \quad \text{for all } \alpha \in \tilde{K}.$$

By (2.4) all $\psi'_\beta = 0$. This proves (4.8).

(4.9) Define $\Phi(c) = K_c$ and extend linearly to $k[C]$. Then Φ is an algebra homomorphism with kernel $k[C]F$ where $F = \sum_{x \in C} x$.

This is an easy consequence of (4.6), (4.7), and (4.8).

(4.10) THEOREM. Let V be an irreducible $k[CR]$ -module nontrivial on $Z(R)$. Then there is a $k[C]$ -module W so that

$$V|_C \simeq (k[C]/k[C]F) \otimes_k W.$$

Let E be the primitive central idempotent of $k[R]$ such that $EV \neq (0)$. For appropriate choice of λ in (4.1), E is given there. Let B be the k -subalgebra generated by the K_c 's. Let U be an irreducible $k[R]$ module with $EU \neq (0)$. Then U is a $k[CR]$ module if we let $c \in C$ act as K_c . By (1.2), (1.3) and (4.9), $U|_C \simeq_B B$.

So by [2, (51.7)] there is a $CR/R \simeq C$ -module W such that

$$V \simeq U \otimes_k W \quad \text{or} \quad V|_C \simeq (k[C]/k[C]F) \otimes W|_C.$$

We have the following easy corollary.

(4.11) COROLLARY. *Let D be a subgroup of C and V an irreducible $k[CR]$ -module faithful on $Z(R)$. Then there is a $k[D]$ -module W so that*

$$V|_D \simeq (\dim W)((r^e + 1)/|D| - 1)k[D] \oplus (k[D]/k[D]F_0) \otimes W$$

where $F_0 = \sum_{x \in D} x$.

We have completed the proof of the theorem. This construction need not be confined to k . With modification it gives a representation of CR in \mathcal{O} , the ring of p -adic integers $p \neq r$, in k when k is an algebraic number field.

Is there a characteristic free proof for $r=2$?

REFERENCES

1. T. R. Berger, *Class two p groups as fixed point free automorphism groups*, Illinois J. Math. **14** (1970), 121–149. MR **41** #3336.
2. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York, 1962. MR **26** #2519.
3. P. Hall and G. Higman, *On the p -length of p -soluble groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc. (3) **6**(1956), 1–42. MR **17**, 344.
4. J. G. Thompson, *Vertices and sources*, J. Algebra **6** (1967), 1–6. MR **34** #7677.
5. E. E. Shult, *On groups admitting fixed point free abelian operator groups*, Illinois J. Math. **9** (1965), 701–720. MR **32** #1269.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MINNESOTA 55455