TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 228, 1977

HALL-HIGMAN TYPE THEOREMS. III

BY
T. R. BERGER[1]

ABSTRACT. This paper continues the investigations of this series. Suppose that $G = ANS$ where S and NS are normal subgroups of G. Suppose that $(|A|, |NS|) = 1$, S is extraspecial, and $S/Z(S)$ is a faithful minimal module for the subgroup AN of G. Assume that $\mathbf{k}$ is a field of characteristic prime to $|G|$ and V is a faithful irreducible $\mathbf{k}[G]$-module. The structure of G is discussed in the minimal situation where N is cyclic, A is nilpotent, and $V|_A$ does not have a regular A-direct summand.

We shall assume familiarity with the ideas of [3]. Most results needed here are quoted but familiarity should help.

We study V by observing that $V \simeq V_\lambda \otimes V^*$ where V_λ is a certain canonical AG-module. Actually, we only investigate $\mathfrak{X}_\lambda$ the character of V_λ. This character $\mathfrak{X}_\lambda$ is described in §2. It is a fairly well-known entity. In §3 we give sufficient information to completely determine $\mathfrak{X}_\lambda|_A$ where $S/Z(S)$ is a minimal A-module. Finally in §4 we determine all exceptions to the statement: "$\mathfrak{X}_\lambda|_A$ contains at least three copies of the regular A-character" under the hypothesis that $S/Z(S)$ is a minimal AN-module for a nonnilpotent group AN.

The organization of §4 is similar to that of §2 of [2]. We translate in (4.3) the question of regular A-characters in $\mathfrak{X}_\lambda|_A$ to questions about A-orbits upon N and characters in $\mathfrak{X}_\lambda|_{C_A(N)N}$. The major portion of that section is devoted to studying A-orbits upon N. Combinatorial-number theoretic methods are used to pin down the bad cases of AN.

One corollary of all the analysis of §4 is:

THEOREM. *Assume $S/Z(S)$ is a faithful minimal AN-module for cyclic N, A is nilpotent, AN nonnilpotent, and $NS = G$. Suppose A is $\mathbf{Z}_2 \wr \mathbf{Z}_2$-free. Then $V|_A$ contains a copy of the regular A-module.*

Putting the results of this paper together with those of [3] we may prove (the actual topic of [5]) that the answer to our question is "always" under the hypotheses: $(\operatorname{char} \mathbf{k}, |AG|) = 1$; A is $\mathbf{Z}_p \wr \mathbf{Z}_p$-free for all $p \mid |A|$; and $C_G(S/Z(S)) < G$.

Received by the editors May 29, 1975.

AMS (MOS) subject classifications (1970). Primary 20C15, 20D10.

[1] Research partially supported by NSF Grant GP 38879.

The major theorems of this paper are much too long to restate here. They are (3.8) and (4.28).

1. **Some estimates.** Most proofs of this paper are finished off with combinatorial arguments. This leads to the necessity for certain elementary estimates with integers. We list these now with their proofs.

(1.1) Suppose x, n are integers such that $x \geqslant 2$ and $n \geqslant 3$. Then

$$(x^n + 1)/(x + 1) < (x^n - 1)/(x - 1).$$

Putting this another way, we wish to prove that

$$(x^n + 1)/(x^n - 1) < (x + 1)/(x - 1).$$

The function $(x + 1)/(x - 1)$ is decreasing for $x \geqslant 2$. This proves (1.1).

(1.2) If x, n are integers such that $x \geqslant 2$ and $n \geqslant 3$ then $(x^n + 1)/(x + 1) > n(4n + 1)$ except as tabulated below:

x	2	3	4	5	6
$n \leqslant$	10	5	4	3	3

The function $f(x, n) = (x^n + 1)/(x + 1) - n(4n + 1)$ is increasing in $x \geqslant 2$. It is increasing in n also unless we have the following values:

x	2	3	4
$n \leqslant$	8	4	4

This is easily checked by taking the derivative with respect to n. Using this, plug in values for (x, n) finding where $f(x, n)$ is both increasing and positive. It is positive and increasing for the values tabulated below:

x	2	3	4	5	6	7
n	11	6	5	4	4	3

The lemma follows immediately.

(1.3) Suppose $x \geqslant 2$ and $n \geqslant 3$ are integers. Let $\varepsilon = \pm 1$. Then

$$(x^n + \varepsilon)/(x + \varepsilon) > f(n)$$

where $f(n) = n$, $(2n + 1)$, $(4n + 1)$, $n(2n + 1)$, or $n(4n + 1)$ except as tabulated below:

ε	$f(n)$	x	$n \leqslant$
$+1$	n	2	3
	$2n + 1$	2	5
		3	3
	$4n + 1$	2	6
		3	3
		4	3

	$n(2n+1)$	2	9
		3	4
		4	4
		5	3
	$n(4n+1)$	2	10
		3	5
		4	4
		5	3
		6	3
-1	$2n+1$	2	3
	$4n+1$	2	4
		3	3
	$n(2n+1)$	2	6
		3	3
		4	3
	$n(4n+1)$	2	8
		3	4
		4	3
		5	3

By (1.1) and (1.2) we need only check the values for x, n tabulated in (1.3).

(1.4) Suppose $x \geqslant 2$ and $n \geqslant 3$ are integers. Let $\varepsilon = \pm 1$. Then

$$(x^n + \varepsilon)/(x + \varepsilon) = f(n)$$

where $f(n) = n$, $2n + 1$, $4n + 1$, $n(2n + 1)$, or $n(4n + 1)$ only for x, n as tabulated below:

ε	$f(n)$	x	n
$+1$	n	2	3
	$2n+1$	2	5
		3	3
	$4n+1$	4	3
	$n(2n+1)$	2	9
		5	3
-1	$2n+1$	2	3
	$4n+1$	3	3
	$n(2n+1)$	4	3

By (1.3) we need only check the values there.

(1.5) Suppose ξ, r are primes, $n \geqslant 1$ is an integer and $\varepsilon = \pm 1$.
(a) If $(r^n + \varepsilon, \xi) = 1$, then $(r^{n\xi} + \varepsilon, \xi) = 1$.
(b) If $\xi > 2$ and $\xi^s \| r^n + \varepsilon$ for $s \geqslant 1$ then $\xi^{s+1} \| r^{n\xi} + \varepsilon$.

(c) If $\xi = 2$ and $2^s \| r^n + \varepsilon$ for $s \geqslant 1$ then $2 \| r^{2n} + 1$ and $2^{s+1} \| r^{2n} - 1$ unless $r^n \equiv -1 \pmod 4$, $s = 1$, and $\varepsilon = -1$.

If $r = \xi$ then (a) is obvious. Suppose $r \neq \xi$. By Fermat's Little Theorem $r^{n\xi} \equiv r^n \not\equiv -\varepsilon \pmod \xi$. This proves (a).

Let $r^n + \varepsilon = \xi^s m$ where $(\xi, m) = 1$ and $s > 0$. Consider (b). Here we expand by the binomial theorem.

$$r^{n\xi} + \varepsilon = (\xi^s m - \varepsilon)^\xi + \varepsilon = \left[\sum_{j=2}^{\xi} (-\varepsilon)^{\xi-j} m^j \xi^{s(j-2)-1} \binom{\xi}{j} \right] \xi^{2^{s+1}}$$

$$+ (-\varepsilon)^{\xi-1} m \xi^{s+1} + (-\varepsilon)^\xi + \varepsilon \equiv m\xi^{s+1} \pmod{\xi^{2s+1}}.$$

This proves (b).

In (c) $r^{2n} + \varepsilon = (2^s m - \varepsilon)^2 + \varepsilon = 2^{2s}m^2 - 2^{s+1}m\varepsilon + 1 + \varepsilon$. If $\varepsilon = 1$ then $r^{2n} + 1 \equiv 2 \pmod 4$. If $\varepsilon = -1$ then $r^{2n} - 1 \equiv 2^{s+1}m \pmod{2^{2s}}$. If $s > 1$ then $2^{s+1} \| r^{2n} - 1$. So we may assume that $s = 1$. Now $2 \| r^n - 1$ so that $4 \|^{rn} + 1$ or $r^n \equiv -1 \pmod 4$. The proof of (c) is finished.

(1.6) Suppose ξ, r are primes, $n \geqslant 1$ is an integer, and $\varepsilon = \pm 1$. If

$$(r^{n\xi} + \varepsilon)/(r^n + \varepsilon) = \xi^s \quad \text{for } s \geqslant 1$$

then

(i) $\xi = 2$, $n = 1$, $\varepsilon = -1$, and $2^s = r + 1$; or
(ii) $\xi = 3$, $n = 1$, $\varepsilon = 1$, and $r = 2$.

By (1.5) we have $s = 1$ unless $\xi = 2$, $\varepsilon = -1$, and $r^n \equiv -1 \pmod 4$. In this latter case $(r^{2n} - 1)/(r^n - 1) = r^n + 1$. Since $r^n \equiv -1 \pmod 4$, n is odd. If $2^s \| r^n + 1$ then $2^s \| r + 1$. Therefore $2^s = r^n + 1 \geqslant r + 1 \geqslant 2^s$. So $n = 1$ and $2^s = r + 1$.

We may now assume that $s = 1$. With $x = r^n$ we have $(x^\xi + \varepsilon)/(x + \varepsilon) = \xi$. If $\xi > 2$ then by (1.4) we must have $r^n = 2$, $\xi = 3$, $\varepsilon = 1$. If $\xi = 2$ then $\varepsilon = -1$ and $2 = x + 1 = r^n + 1$. Obviously this has no solution with $r > 1$. The proof is complete.

(1.7) Suppose r, p are primes and $a, b > 1$ are integers. If $r^a = p^b + 1$ then $r = 3, p = 2, a = 2, b = 3$.

This little result is well known.

(1.8) Suppose that r is a prime, $n \geqslant 1$ an integer, and $r^n - 1 = 2^s, 2^s \cdot 3, 2^s \cdot 5, 2^s \cdot 3 \cdot 5$. Then $n = 1$ unless we have one of the tabulated values below:

r	2	2	3	3	5	7	11	31
n	2	4	2	4	2	2	2	2
$r^n - 1$	3	$3 \cdot 5$	2^3	$2^4 \cdot 5$	$2^3 \cdot 3$	$2^4 \cdot 3$	$2^3 \cdot 3 \cdot 5$	$2^6 \cdot 3 \cdot 5$

Assume that $n > 1$. If $r^n - 1 = 2^s$ then by (1.7) $r = 3$, $n = 2$, $s = 3$. We ignore this case now. Let $\varepsilon = \pm 1$. Assume that $n = 2m$. We have the following possibilities:

$r^m + \varepsilon$	$2^a \cdot 3$	$2^a \cdot 5$	$2^a \cdot 3$	$2^a \cdot 3 \cdot 5$
$r^m - \varepsilon$	2^b	2^b	$2^b \cdot 5$	2^b

Suppose $r^m = \delta \pmod 4$ where $\delta = \pm 1$. Then $r^m + \delta = 1, 2, 3, 5, 3 \cdot 5, 2 \cdot 3, 2 \cdot 5, 2 \cdot 3 \cdot 5$. These give the following values:

r^m	0	1	2	2^2	$2 \cdot 7$	5	3^2	29	2	3	2^2	$2 \cdot 3$	2^4	7	11	31
$r^m + \delta$	1	2	3	5	$3 \cdot 5$	$2 \cdot 3$	$2 \cdot 5$	$2 \cdot 3 \cdot 5$	1	2	3	5	$3 \cdot 5$	$2 \cdot 3$	$2 \cdot 5$	$2 \cdot 3 \cdot 5$
$r^m - \delta$	-1	0	1	3	13	2^2	2^3	$2^2 \cdot 7$	3	2^2	5	7	17	2^3	$2^2 \cdot 3$	2^5
δ	1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1

From this table we have the following possibilities:

r	2	2	5	3	7	11	31
m	1	2	1	2	1	1	1
ε	1	-1	1	1	-1	1	-1
$r^m + \varepsilon$	3	3	$2 \cdot 3$	$2 \cdot 5$	$2 \cdot 3$	$2^2 \cdot 3$	$2 \cdot 3 \cdot 5$
$r^m - \varepsilon$	1	5	2^2	2^3	2^3	$2 \cdot 5$	2^5

These values are all tabulated in the result.

Next assume that $n = m\zeta$ is odd and ζ is an odd prime. Then

$$(r^{m\zeta} - 1)/(r^m - 1) = 3, 5, 3 \cdot 5$$

since the power of 2 in $r^n - 1$ is equal to the power of 2 in $r^m - 1$. Since $\zeta > 3$, $\zeta(2\zeta + 1) > (r^{m\zeta} - 1)/(r^m - 1)$. We need only check $x = r^m$, $\zeta = n$ as in (1.3). None of the values listed there satisfies our equality. The proof is complete.

2. **Characters of extensions.**

In this section we study how to determine character values for certain extensions of extraspecial groups. A very general method is given in a recent paper of Isaacs [10]. The method given here was found independently but is very similar. Since the method has been around for some time, we will quote and piece together the necessary results.

Let G be a group and χ a character of G in some field. Let $\hat{\chi}$ be a representation of G affording χ. We set $\varphi(\chi) = \det \hat{\chi}$. Since the determinant is invariant, φ is well defined.

(2.1) THEOREM. *Let G be a group with normal subgroup N. Let* **k** *be a field of characteristic* 0 *containing the* $|G|$*th roots of unity. Assume that λ is an irreducible character of N and*

(1) λ *is G-invariant,*

(2) $\varphi(\lambda)$ *extends to a linear character α of G, and*

(3) $\lambda(1)$ *and* $[G\colon N]$ *are relatively prime.*

Then there exists a unique character χ of G such that

(a) $\chi|_N = \lambda$ *and*

(b) $\varphi(\chi) = \alpha$.

This result is quoted in [1], [7]. Various sources of proof are given there. As a corollary we obtain the following result.

(2.2) Proposition. *Suppose $G = AR$ where R is a normal extraspecial r-subgroup of G, $(|A|, r) = 1$, and $Z(R) \leqslant Z(AG)$. Assume that* $\mathbf{k}$ *is a characteristic 0 field containing the $|G|$th roots of unity. Let λ be a nontrivial linear* $\mathbf{k}$*-character of $Z(R)$. There is a unique* $\mathbf{k}$*-character $\mathfrak{X}_\lambda = \mathfrak{X}_\lambda(AR)$ of G lying over λ such that:*

(1) $\mathfrak{X}_\lambda|_{Z(R)}$ *is a multiple of* λ;

(2) $\mathfrak{X}_\lambda|_R$ *is irreducible*;

(3) $\varphi(\mathfrak{X}_\lambda)$ *is the trivial character on A.*

As is well known [9, Kapitel V, Satz 16.14] there is a unique character χ of G which is irreducible on R such that $\chi|_{Z(R)}$ is a multiple of λ. It is not difficult to show that $\varphi(\chi)$ is the trivial character of R. Let α be the trivial character of G. Since $\chi(1)$ is a power of r and $(|A|, r) = 1$, (2.1) tells us that $\mathfrak{X}_\lambda$ exists satisfying the required conditions and uniqueness.

Observe that:

(2.3) Proposition. *In (2.2) if $A_0 \leqslant A$ then*

$$\mathfrak{X}_\lambda(A_0R) = \mathfrak{X}_\lambda(AR)|_{A_0R}.$$

In other words, if $x \in A$ then $\mathfrak{X}_\lambda(AR)(x)$ can be determined as $\mathfrak{X}_\lambda(\langle x\rangle R)(x)$. It is sufficient to determine $\mathfrak{X}_\lambda$ for cyclic extensions.

Let $\bar{R} = R/Z(R)$. Then for $x \in A$, $\bar{R}$ is an $\langle x\rangle$-module with a nonsingular symplectic form g induced by the commutator map of R and fixed by x. It is easy to see, using elementary properties of symplectic spaces, that:

(2.4) Proposition. *$\bar{R} = \bar{R}_1 \dotplus \cdots \dotplus \bar{R}_t$ where the $\bar{R}_i$ are $\langle x\rangle$-modules such that $C_{\langle x\rangle}(\bar{R}_i) = C_{\langle x\rangle}(T)$ for every $\langle x\rangle$-submodule $T \neq (0)$ of $\bar{R}_i$ and $C_{\langle x\rangle}(\bar{R}_i) \neq C_{\langle x\rangle}(\bar{R}_j)$, $i \neq j$. Further, each $\bar{R}_i$ is a nonsingular space. In particular, $\bar{R}_i = R_i/Z(R)$ where R_i is an $\langle x\rangle$-invariant extraspecial group. And for $i \neq j$, $\bar{R}_i$ is orthogonal to $\bar{R}_j$.*

It is obvious that R is the central product of the extraspecial groups R_i. Using this fact we may further reduce the problem of constructing $\mathfrak{X}_\lambda$.

(2.5) Proposition [1, (IV.5)]. *Assume that AR is a group with normal extraspecial r-subgroup R and complement A with $(|A|, r) = 1$. Suppose $R =$*

R_1R_2 is a central product of two normal extraspecial subgroups, R_1 and R_2, of AR. Let χ_i be an irreducible character of AR_i such that $\chi_i|_{R_i}$ is faithful and irreducible, and $\chi_i|_{Z(R)}$ is a multiple of λ. Form $AR_1 \times AR_2$ and let

$$M = \{(z_1, z_2)|z_i \in Z(R), z_1z_2 = 1\}.$$

There is an isomorphism of AR into $(AR_1 \times AR_2)/M$. Further, $\chi_1\chi_2$ is an irreducible character of $(AR_1 \times AR_2)/M$ and is irreducible on the image of R in this group and is a multiple of λ on $Z(R)$.

Note that $\chi_1(1)$ and $\chi_2(1)$ are powers of r. If $\hat{\chi}_1$ and $\hat{\chi}_2$ are representatives affording χ_1 and χ_2 respectively then $\hat{\chi}_1 \otimes \hat{\chi}_2$ affords $\chi_1\chi_2$. Thus $\varphi(\chi_1\chi_2) = \varphi(\chi_1)^{\chi_2(1)}\varphi(\chi_2)^{\chi_1(1)}$. In particular, if $\chi_1 = \mathfrak{X}_\lambda(AR_1)$ and $\chi_2 = \mathfrak{X}_\lambda(AR_2)$ then $\chi_1\chi_2 = \mathfrak{X}_\lambda(AR)$.

(2.6) Proposition. *If $\bar{R}_i = R_i/Z(R)$ in (2.4) then*

$$\mathfrak{X}_\lambda(AR) = \prod_i \mathfrak{X}_\lambda(AR_i).$$

Now we need only compute $\mathfrak{X}_\lambda(\langle x\rangle R)$ where $C_{\langle x\rangle}(\bar{y})$ is the same for all $\bar{y} \neq 1, \bar{y} \in \bar{R} = R/Z(R)$.

(2.7) Proposition [1, (IV.8), (IV.9)]. *Suppose AR is a group with normal extraspecial r-subgroup R of order r^{2m+1}. Suppose $Z(R) < Z(AR)$ and $R/Z(R)$ is a direct sum of faithful irreducible $\mathbf{k}[A]$-modules. If A is cyclic, $r^m \equiv (-1)^t$ (mod$|A|$), and λ is a nontrivial linear character of $Z(R)$ then*

$$\begin{aligned}\chi(x) &= r^m\lambda(x), && x \in Z(R),\\ &= (-1)^t\lambda(z), && x \sim wz, w \in A^{\#}, z \in Z(R),\\ &= 0, && \textit{elsewhere},\end{aligned}$$

is an irreducible character of AR. Further,

$$\chi|_A = a\rho_A + (-1)^t 1_A$$

where $a = [r^m - (-1)^t]/|A|$, ρ_A is the regular, and 1_A is the trivial character of A.

Remark. Under these hypotheses $t = 0, 1$ exists with $r^m \equiv (-1)^t$ (mod|A|) [1, (IV.7)].

Now $\chi|_R$ and $\mathfrak{X}_\lambda(\langle x\rangle R)|_R$ are both the irreducible characters of R lying over λ. Thus [6, (51.7)] there is a linear character μ of $AR/R \simeq A$ so that $\chi\mu = \mathfrak{X}_\lambda$. Computing restrictions to A we have

$$\begin{aligned}1_A &= \varphi(\mathfrak{X}_\lambda) = \varphi(\chi\mu) = \varphi(\chi)\,\mu^{\chi(1)} = \varphi(a\rho_A \pm 1_A)\,\mu^{\chi(1)}\\ &= \varphi(\rho_A)^a\,\mu^{\chi(1)} = \nu^a\mu^{\chi(1)}, \qquad a = [r^m - (-1)^t]/|A|,\end{aligned}$$

where ν is the alternating character of the regular A-representation. If $r = 2$ then $|A|$ is odd so that $\nu = 1_A$. Thus $\mu = 1_A$. If $r > 2$ then ν^a has values ± 1.

Since $(|A|, \chi(1)) = 1$, μ has values ± 1. So $\mu^{\chi(1)} = \mu$. In particular, $\mu = \nu^{a}$. Therefore, μ will be the alternating character of A if a is odd, otherwise $\mu = 1_{A}$.

(2.8) Proposition. *Suppose χ, A, R are as in* (2.7). *Then there is a linear character μ of $AR/R \simeq A$ so that*

$$\chi\mu = \mathfrak{X}_{\lambda}(AR).$$

Further, $\mu = 1_{A}$ unless $r > 2$, $|A|$ is even, and $a = [r^{m} - (-1)^{t}]/|A|$ is odd. In this latter case μ is the alternating character of the regular representation of A.

Now (2.2), (2.3), (2.4), (2.6), (2.7) and (2.8) are sufficient to calculate the values of $\mathfrak{X}_{\lambda}(AR)$ for any appropriate A and R. By (2.4) and (2.7) it is sufficient to know that action of A upon $\overline{R} = R/Z(R)$ in order to determine $\mathfrak{X}_{\lambda}(AR)|_{A}$. In the next section we shall explicitly compute $\mathfrak{X}_{\lambda}$ in some cases.

3. Ordinary theory of minimal nilpotent modules.

(3.1) Hypotheses. (a) $G = AR$ is a group with normal extraspecial r-subgroup R of order r^{2m+1} and $(r, |A|) = 1$. The group A is nilpotent, faithful and irreducible upon $R/Z(R)$, and centralizes $Z(R)$. The A-module $R/Z(R)$ is a minimal A-module.

(b) $\mathbf{Q}$ is the rational field, δ is a primitive $|G|$th root of unity and $\mathbf{k} = \mathbf{Q}(\delta)$. All characters are $\mathbf{k}$-characters.

A little explanation is in order.

(3.2) Definition. Suppose $\mathbf{K}$ is a field, H is a group and V is an irreducible $\mathbf{K}[H]$-module. Assume that there is a nonsingular symplectic form $g\colon V \times V \to \mathbf{K}$ fixed by H. We call V a *minimal* $\mathbf{K}[H]$-module if for any subgroup N normal in G either $V|_{N}$ is homogeneous or $V|_{N} = V_{1} \dotplus V_{2}$ where the V_{i} are the homogeneous components and are totally isotropic subspaces.

The commutator map on R induces a nonsingular symplectic form upon $\overline{R} = R/Z(R)$ fixed by A. If we let $\mathbf{K}$-GF(r) then $\overline{R}$ is a minimal A-module. The group A is nilpotent. All nilpotent minimal modules have been classified. The group A is a subgroup of a larger nilpotent group B which acts upon $\overline{R}$ [3, (3.20)].

We describe the structure of these groups B now [3, §2].

Recall that $|R| = r^{2m+1}$. Let $\mathbf{K} = \mathrm{GF}(r)$, $\tilde{\mathbf{K}} = \mathrm{GF}(r^{m})$, and $\hat{\mathbf{K}} = \mathrm{GF}(r^{2m})$.

(3.3) Example. B is cyclic of order $r^{m} + 1$.

Let $\overline{R} = \hat{\mathbf{K}}^{+}$ and $\varphi\colon \varepsilon \to \varepsilon^{r^{m}}$, the automorphism of order two of $\hat{\mathbf{K}}$. Let B be the multiplicative subgroup of $\hat{\mathbf{K}}^{\times}$ of order $r^{m} + 1$. Then B acts upon $\overline{R}$ by multiplication.

Let Tr: $\tilde{\mathbf{K}} \to \mathbf{K}$ be the trace map. Choose $\mu \in \hat{\mathbf{K}}^\times$ so that $\mu^\varphi = -\mu$ (if $r = 2$ let $\mu = 1$) and set

$$g(u, v) = \operatorname{Tr}(\mu(uv^\varphi - u^\varphi v)), \qquad u, v \in \bar{R}.$$

(3.4) Example. $|B| = 2^{t+1}$ where $2^t \| r^m + 1$, $r > 2$, and $r^m \equiv -1 \pmod 4$.

Let $\bar{R}$, g be as in (3.3). Let Q be the 2-Sylow subgroup of B in (3.3). Form the semidirect product $\langle\varphi\rangle\hat{\mathbf{K}}^\times$. Choose $\nu \in \hat{\mathbf{K}}^\times$ so that $\nu^{r^m+1} = -1$. In the semidirect product set $B = \langle Q, \varphi\nu\rangle$. Then B is quaternion.

(3.5) Example. $|B| = 2^{t+1}$ where $2^t \| r^m - 1$, $r > 2$, and $r^m \equiv 1 \pmod 4$.

Let $\bar{R}$ be a 2-dimensional $\tilde{\mathbf{K}}$-space with basis e_1, e_2. As a $\tilde{\mathbf{K}}$-space we write matrices in the basis e_1, e_2 to represent linear transformations. Choose $\nu \in \tilde{\mathbf{K}}^\times$ of order 2^t where $2^t \| r^m - 1$. Let

$$B = \left\langle w = \begin{bmatrix} \nu & \\ & \nu^{-1} \end{bmatrix}, b = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \right\rangle.$$

If Tr: $\tilde{\mathbf{K}} \to \mathbf{K}$ is the trace map and $u = \alpha e_1 + \beta e_2$, $v = \alpha' e_1 + \beta' e_2$ where α, α', β, $\beta' \in \tilde{\mathbf{K}}$ then set

$$g(u, v) = \operatorname{Tr}(\alpha\beta' - \alpha'\beta).$$

Here B is quaternion. Let $Q = \langle w\rangle$.

(3.6) Example. $|B| \mid 2(r^m - 1)$, $r > 2$, $m = 2n$, and $r^n \equiv 1 \pmod 4$.

Let $\bar{R}$ be a 2-dimensional $\tilde{\mathbf{K}}$-space with basis e_1, e_2. Let $Q_0 = \langle\nu\rangle$ be the 2-Sylow subgroup of $\tilde{\mathbf{K}}^\times$. Choose θ of order $(r^n + 1)/2$ in $\tilde{\mathbf{K}}^\times$. Let $\psi\colon \varepsilon \to \varepsilon^{r^n}$ be the automorphism of order two on $\tilde{\mathbf{K}}$. Using matrices in the basis e_1, e_2 to denote linear transformations set

$$Q = \left\langle w = \begin{bmatrix} \nu & \\ & \nu^{-1} \end{bmatrix}, b = \begin{bmatrix} & \psi \\ -\psi & \end{bmatrix} \right\rangle$$

and

$$D = \left\langle c = \begin{bmatrix} \theta & \\ & \theta^{-1} \end{bmatrix} \right\rangle.$$

The group Q is semidihedral. Let $B = QD = Q \times D$, and $C = \langle w\rangle$. If $u = \alpha e_1 + \beta e_2$ then $yu = \beta^\psi e_1 - \alpha^\psi e_2$. If Tr: $\tilde{\mathbf{K}} \to \mathbf{K}$ is the trace map and $u = \alpha e_1 + \beta e_2$, $v = \alpha' e_1 + \beta' e_2$ where $\alpha, \alpha', \beta, \beta' \in \tilde{\mathbf{K}}$ then set $g(u, v) = \operatorname{Tr}(\beta\alpha' - \alpha\beta')$.

In [3, (3.20)] we proved the following.

(3.7) Theorem. *Assume* (3.1). *Then there is an identification so that* $A \leqslant B$ *and* $\bar{R} = R/Z(R)$ *is given by one of* (3.3)–(3.6).

To determine $\mathfrak{X}_\lambda = \mathfrak{X}_\lambda(AR)$, then, it will suffice to determine $\mathfrak{X}_\lambda$ for $A = B$ since other values may be obtained by restriction (see (2.3)).

(3.8) THEOREM. *Assume* (3.1). *Then* $\bar{R}$, $A \leqslant B$ *are given by* (3.3)–(3.6). *Further, on B, the values of* $\mathfrak{X}_\lambda$ *are given below.*

(i) B, $\bar{R}$ *as in* (3.3).

$$\text{(a)}\qquad \begin{aligned} \mathfrak{X}_\lambda(x) = {} & r^m, && x = 1, \\ & -1, && x \in (B^2)^{\#}, \\ & 1, && x \in B \setminus B^2; \end{aligned}$$

$$\text{(b)}\qquad \mathfrak{X}_\lambda|_B = \rho_B - \mu \quad \textit{where } \mu = 1_B$$

unless $2|\,|B|$ *in which case* μ *is the alternating character of the regula B-representation.*

(ii) B, $\bar{R}$ *as in* (3.4).

$$\text{(a)}\qquad \begin{aligned} \mathfrak{X}_\lambda(x) = {} & r^m, && x = 1, \\ & -1, && x \in (Q^2)^{\#}, \\ & 1, && x \in Q \setminus Q^2, \\ & -1, && x \in B \setminus Q, |Q| > 4, \\ & 1, && x \in B \setminus Q, |Q| = 4; \end{aligned}$$

$$\text{(b)}\qquad |Q| = 4, \quad \mathfrak{X}_\lambda|_B = \left(\left[r^m + 1\right]/|B| - \tfrac{1}{2}\right)\rho_B + \sum_{\chi(1)>1} \chi + 1_B;$$

$$\text{(c)}\qquad |Q| > 4, \quad \mathfrak{X}_\lambda|_B = \left(\left[r^m + 1\right]/|B| - \tfrac{1}{2}\right)\rho_B + \sum_{\chi(1)>1} \chi + \mu$$

where μ *is the faithful linear character of* B/Q.

(iii) B, $\bar{R}$ *as in* (3.5).

$$\text{(a)}\qquad \begin{aligned} \mathfrak{X}_\lambda(x) = {} & r^m, && x = 1, \\ & 1, && x \in (Q^2)^{\#}, \\ & -1, && x \in Q \setminus Q^2, \\ & 1, && x \in B \setminus Q, |Q| > 4, \\ & -1, && x \in B \setminus Q, |Q| = 4; \end{aligned}$$

$$\text{(b)}\qquad |Q| = 4, \quad \mathfrak{X}_\lambda|_B = \left(\left[r^m - 1\right]/|B| - \tfrac{1}{2}\right)\rho_B + \sum_{\chi(1)>1} \chi + \sum_{\substack{\eta(1)=1 \\ \eta \neq 1_A}} \eta;$$

$$\text{(c)}\qquad |Q| > 4, \quad \mathfrak{X}_\lambda|_B = \left(\left[r^m - 1\right]/|B| - \tfrac{1}{2}\right)\rho_B + \sum_{\chi(1)>1} \chi + \sum_{\substack{\eta(1)=1 \\ \eta \neq \mu}} \eta$$

where μ *is the faithful linear character of* B/Q.

(iv) B, $\bar{R}$ *as in* (3.6).

(a)
$$\begin{array}{rl} \mathfrak{X}_\lambda(x) = r^m, & x = 1, \\ 1, & x \in (C^2D)^\#, \\ -1, & x \in (C \setminus C^2)D, \\ 1, & x \in (Q \setminus C)D, x^2 \not\in D, \\ -1, & x \in (Q \setminus C)D^\#, x^2 \in D, \\ r^{m/2}, & x \in Q \setminus C, x^2 = 1; \end{array}$$

(b)
$$\mathfrak{X}_\lambda|_B = ([r^m - 1]/|B| - \tfrac{1}{2})\rho_B + \sum_{\chi(1)>1} \chi + (1_Q + \mu_1)\delta + \mu_2$$

where μ_1 is the linear character of Q with dihedral kernel, μ_2 is the linear character of Q with quaternion kernel, and δ is the regular character of D.

The calculation of values is carried out by the methods of §2. We illustrate the method for one value, possibly the most difficult. In (iv) let $x \in Q \setminus C$ have order two. Then x is conjugate to bw. So we may take $x = bw$. Let $\mathbf{K}_0$ be the fixed subfield of ψ in $\tilde{\mathbf{K}}$. If $\alpha \in \mathbf{K}_0$ then

$$bw(e_1 + \nu e_2) = e_1 + \nu e_2 \quad \text{and} \quad bw(e_1 - \nu e_2) = -(e_1 - \nu e_2).$$

Let $\overline{R}_1 = \mathbf{K}_0(e_1 + \nu e_2) + \mathbf{K}_0\nu(e_1 - \nu e_2)$ and $\overline{R}_2 = R_1^{\perp}$. These are nonsingular orthogonal components as in (2.4). Let $R_i/Z(R) = \overline{R}_i$.

Since $bw = x$ is trivial upon $\overline{R}_1$ we have

$$\mathfrak{X}_\lambda(\langle x \rangle R_1)(x) = r^{m/2}.$$

Now we use χ of (2.7) for $\langle x \rangle R_2$. Thus $\chi(x) = (-1)^t$ where $r^{m/2} \equiv (-1)^t$ (mod 2) since $|\langle x \rangle| = 2$. Since r is odd we may take $t = 0$. Now

$$a = (r^{m/2} - 1)/2$$

is even, so that

$$\chi(x) = 1 = \mathfrak{X}_\lambda(\langle x \rangle R_2)(x)$$

by (2.8). Finally, by (2.6)

$$\mathfrak{X}_\lambda(AR)(x) = \mathfrak{X}_\lambda(\langle x \rangle R_1)(x)\mathfrak{X}_\lambda(\langle x \rangle R_2)(x) = r^{m/2} \cdot 1 = r^{m/2}.$$

If we had chosen $t = 1$ above then $a = (r^m + 1)/2$, which is odd. So we obtain, by (2.8),

$$-\chi(x) = 1 = \mathfrak{X}_\lambda(\langle x \rangle R_2)(x).$$

Other character values are obtained this same way.

The characters are decomposed upon B by means of inner products. We illustrate this only for (iv)(b). In this case, $B = Q \times D$ and C is cyclic of index two in Q. The group Q is semidihedral. Let D^* be the maximal dihedral and Q^* the maximal quaternion subgroups of Q. Then $T = D^* \setminus C^2$ is the set of noncentral involutions of Q; and $F = Q^* \setminus C^2$ is the set of elements of order four in Q but not in C. Set $E = C \setminus C^2$.

Let χ be an irreducible character of B. How many times does χ appear in $\mathfrak{X}_\lambda|_B$? That is, what is the value of $(\mathfrak{X}_\lambda|_B, \chi)_B$?

First assume that $\chi(1) > 1$. Then $\chi = \eta|^B$ for some linear character η of CD nontrivial upon C^2. Using part (i)(b) which follows directly from (2.7) and (2.8) we have

$$\mathfrak{X}_\lambda|_{CD} = (r^m - 1)/|CD|\rho_{CD} + \mu$$

where μ is the alternating character of the regular representation for CD. So

$$(\mathfrak{X}_\lambda|_B, \chi)_B = (\mathfrak{X}_\lambda|_{CD}, \eta)_{CD} = (r^m - 1)/|CD| = 2\left([r^m - 1]/|B| - \tfrac{1}{2}\right) + 1.$$

This shows, since $\chi(1) = 2$, that the count of χ in $\mathfrak{X}_\lambda|_B$ is correct in (iv)(b).

Next assume that $\eta = \nu\mu$ where ν is linear upon D and μ is linear upon Q. Thus $\ker \mu \geqslant C^2$. In fact, the kernel of μ is one of Q, C, Q^*, D^*. But then

$$\begin{aligned}
|B|(\mathfrak{X}_\lambda|_B, \eta) = r^m &+ \sum_{x \in (C^2D)^{\#}} \nu(x) \\
&- \sum_{x \in ED} \nu(x)\mu(x) + \sum_{x \in FD} \nu(x)\mu(x) \\
&- \sum_{x \in TD^{\#}} \nu(x)\mu(x) + r^{m/2} \sum_{x \in T} \mu(x) \\
= r^m &- 1 + |C^2| \sum_{x \in D} \nu(x) \\
&+ \left(\sum_{x \in D} \nu(x)\right)\left(\sum_{y \in F} \mu(y) - \sum_{y \in E} \mu(y) - \sum_{y \in T} \mu(y)\right) \\
&+ (r^{m/2} + 1) \sum_{y \in T} \mu(y).
\end{aligned}$$

Let $\delta_1 = 0$ if $\nu \neq 1_D$ and 1 if $\nu = 1_D$. Observe that μ is constant with value ± 1 upon the sets F, E, and T. Let $u_J = \pm 1$ be the value of μ on the set $J = F, E, T$. Recall that $2^t \,|\, |r^{m/2} - 1$. Then $|C^2| = |F| = |E| = |T| = 2^t$. Since $|D| = (r^{m/2} + 1)/2$ our equality has the following form.

$$|B|(\mathfrak{X}_\lambda|_B, \eta) = r^m - 1 + |C^2D|(1 + \mu_F - \mu_E - \mu_T)\delta_{\nu_1} + |CD|\,\mu_T.$$

The values of μ are easily determined. If $\mu = 1_Q$ then $\mu_F = \mu_E = \mu_T = 1$. If $\mu \neq 1_Q$ then μ is $+1$ on one and -1 on the other two of F, E, T. We tabulate the value of $1 + \mu_F - \mu_E - \mu_T$ below.

$$\begin{aligned}
1 + \mu_F - \mu_E - \mu_T = 0, &\qquad \ker \mu = Q, \\
4, &\qquad \ker \mu = Q^*, \\
0, &\qquad \ker \mu = D^*, \\
0, &\qquad \ker \mu = C.
\end{aligned}$$

Let $\delta_{\mu Q^*} = 0$ if $\ker \mu \neq Q^*$ and 1 if $\ker \mu = Q^*$. Then our equality can be stated as below.

$$|B|(\mathfrak{X}_\lambda|_B, \eta) = r^m - 1 + |B|\,\mu_T/2 + |B|\delta_{\nu_1}\delta_{\mu Q^*}$$

or

$$(\mathfrak{X}_\lambda|_B, \eta) = \left([r^m - 1]/|B| - \tfrac{1}{2}\right) + (1 + \mu_T)/2 + \delta_{\nu_1}\delta_{\mu Q^*}.$$

The value $\mu_T = -1$ unless $\ker \mu = Q$ or D^*. The $(1 + \mu_T)/2$ accounts for the expression $(1_Q + \mu_1)\delta$ in (iv)(b). The expression $\delta_{\nu_1}\delta_{uQ^*}$ accounts for μ_2. The proof of (iv)(b) is now complete. Other parts of (3.8) are proved in the same manner.

4. **Other minimal cases.** In the previous section we gave sufficient information to answer the following question. If G satisfies (3.1) then when does $\mathfrak{X}_\lambda|_A$ contain copies of the regular A-character ρ_A? In this section we consider this same question in a more general setting. Actually we wish to prove the analogue to [2, (4.2)].

(4.1) Hypothesis. (a) Suppose $H = AN$ is not nilpotent where $N \triangle H$ is cyclic, A is nilpotent, and $A \cap N = 1$. Let r be a prime not dividing $|H|$, and $G = HR$ where R is a normal extraspecial r-group $Z(R) \leqslant Z(G)$, and $R/Z(R)$ is a faithful minimal H-module.

(b) Let $\mathbf{k}$ be a finite extension of the rational field containing all $|G|$th roots of unity. Let λ be a nontrivial linear character of $Z(R)$ in $\mathbf{k}$ and $\mathfrak{X}_\lambda(G) = \mathfrak{X}_\lambda$ the unique character of (2.2).

The group H acts upon the module $V = R/Z(R)$ fixing the form g given by the commutator map of R. So it is meaningful to assume that V is a minimal $\mathbf{K}[H]$-module where $\mathbf{K} = \mathrm{GF}(r)$.

We wish to determine how many times ρ_A, the regular A-character, is contained in $\mathfrak{X}_\lambda|_A$. We shall first prove a theorem which is the basis of our computations.

(4.2) Hypotheses. Condition (A): $\bar{H} = H/C_H(N)$ has at least a regular orbits in its action upon the elements of N.

Condition (B): $\mathfrak{X}_\lambda|_{C_H(N)}$ contains $b\mu(1)$ copies of $\mu\nu$ for every irreducible character μ of $C_A(N)$ and every linear character ν of N with order greater than two.

Since $C_H(N) = C_A(N) \times N$, Condition (B) is meaningful. We may prove the following theorem.

(4.3) Theorem. *Suppose* (4.1) *and* (4.2) *hold. Then* $\mathfrak{X}_\lambda|_A$ *contains at least ab copies of* ρ_A, *the regular* A*-character.*

The proof is a straightforward computation with inner products. Observe that for ν, a linear character of N, $x \in N$, $yC_H(N) \in \bar{H}$ the formula

$$\nu^y(x) = \nu(x^{y^{-1}})$$

gives an action for $\bar{H}$ upon the linear characters of N dual to the action of $\bar{H}$ upon N. Condition (A) tells us that $\bar{H}$ permutes the linear characters of N with at least a regular orbits. Let $\mathfrak{V}$ be a complete set of distinct orbit representations for a regular $\bar{H}$-orbits upon the linear characters of N.

By (4.1) (a) H is not nilpotent so that $|\bar{H}| > 1$. The characters of N form a cyclic group of order $|N|$. Therefore, for $\bar{y} \in \bar{H}$ and $\nu \in \mathfrak{V}$, $\nu^{\bar{y}}$ is a power of ν. In particular, ν must have order greater than two. By Condition (B) we know that $\mathfrak{X}_\lambda|_{C_H(N)}$ contains $b\mu(1)$ copies of $\mu\nu$ for every irreducible character μ of $C_A(N)$.

We are now ready to compute. Let χ be any irreducible character of A. It is sufficient to prove that $(\mathfrak{X}_\lambda|_A, \chi) \geqslant ab\chi(1)$. Restricting to $A_0 = C_A(N)$

$$\chi|_{A_0} = c(\mu_1 + \cdots + \mu_d)$$

where the μ_i are distinct irreducible characters of A_0. Form the characters $\mu_i\nu$ of $C_H(N) = A_0 \times N$ where $\nu \in \mathfrak{V}$ and $1 \leqslant i \leqslant d$. Since ν generates a regular $\bar{H}$-orbit, $C_H(N)$ is the stabilizer in H of ν. Therefore $C_H(N)$ is the stabilizer in H of $\mu_i\nu$. Induction gives $\chi_{i\nu} = \mu_i\nu|^H$, a collection of irreducible characters of H. Since the ν's belong to distinct $\bar{H}$-orbits, the $\chi_{i\nu}$'s are all distinct irreducible characters of H. As remarked earlier, $\mathfrak{X}_\lambda|_{C_H(N)}$ contains $b\mu_i(1)$ copies of $\mu_i\nu$ for each μ_i and ν. We may calculate

$$(\mathfrak{X}_\lambda|_H, \chi_{i\nu})_H = (\mathfrak{X}_\lambda|_{C_H(N)}, \mu_i\nu)_{C_H(N)} \geqslant b\mu_i(1) = b\chi(1)/cd.$$

Therefore $\mathfrak{X}_\lambda|_H$ contains $b(\chi(1)/cd)\Sigma_{i,\nu}\chi_{i\nu}$.

Next we compute

$$\begin{aligned}(\chi_{i\nu}|_A, \chi)_A &= (\mu_i\nu|^H|_A, \chi)_A \\ &= (\mu_i\nu|_{C_H(N)\cap A}|^A, \chi)_A = (\mu_i\nu|_{A_0}, c(\mu_1 + \cdots + \mu_d))_{A_0} \\ &= (\mu_i, c(\mu_1 + \cdots + \mu_d))_{A_0} = c.\end{aligned}$$

We know now that $\chi_{i\nu}|_A$ contains $c\chi$. That is, $\mathfrak{X}_\lambda|_A$ contains $b(\chi(1)/cd)\Sigma\chi_{i\nu}|_A$ which contains $b(\chi(1)/cd)\Sigma_{i,\nu}c\chi = b|\mathfrak{V}|\chi(1)\chi = ab\chi(1)\chi$. We conclude that $\mathfrak{X}_\lambda|_A$ contains $ab\rho_A$. The proof of (4.3) is complete.

1. Condition A. Our attention must turn now to Conditions (A) and (B). Next we carry out an extensive analysis of Condition (A). We wish to determine partially the order of N and of $\bar{H}$. Since $\bar{H}$ acts faithfully upon N we may consider $\bar{H} \leqslant \operatorname{Aut}(N)$. This is a fairly nice situation since N is cyclic. We shall be concerned with the case where $a < 3$ in Condition (A). Since $\operatorname{Aut}(N)$ is regular upon generators of N, this forces $[\operatorname{Aut}(N) \colon \bar{H}] < 3$.

We shall describe $\bar{H}$ more thoroughly later, but for our purposes now we need only know that $\bar{H}$ is either cyclic or $\bar{H} \simeq \mathbf{Z}_2 \times F$ where F is cyclic of even order. This allows us to fix the following hypotheses.

(4.4) Hypothesis. Suppose that L is a cyclic group, $K \leqslant \mathrm{Aut}(L)$ $[\mathrm{Aut}(L) \colon K] \leqslant 2$, and K is cyclic or $K \simeq \mathbf{Z}_2 \times F$ where F is cyclic of even order.

(4.5) Proposition. *Assume* (4.4).

(1) *If K is cyclic then* $\mathrm{Aut}(L)$ *is cyclic or* $\mathrm{Aut}(L) \simeq \mathbf{Z}_2 \times F_0$ *where F_0 is cyclic of even order.*

(2) *If $K \simeq \mathbf{Z}_2 \times F$ then* $\mathrm{Aut}(L)$ *has one of the following types*: (a) $\mathbf{Z}_2 \times F_0$; (b) $\mathbf{Z}_2 \times \mathbf{Z}_2 \times F_0$; *or* (c) $\mathbf{Z}_4 \times F_1$ *where F_0 is cyclic of even order and F_1 is cyclic such that* $4|\,|F_1|$.

The invariants of the 2-Sylow subgroup of K are (2^t) or $(2, 2^t)$ as K is cyclic or not. Since $[\mathrm{Aut}(L) \colon K] \leqslant 2$ the possible invariants for a 2-Sylow subgroup of $\mathrm{Aut}(L)$ are:

(1) if K has (2^t) then $\mathrm{Aut}(L)$ has (2^t), (2^{t+1}), or $(2, 2^t)$;

(2) if K has $(2, 2^t)$ then $\mathrm{Aut}(L)$ has $(2, 2^t)$, $(2, 2^{t+1})$, $(2, 2, 2^t)$, or $(4, 2^t)$.

These invariants cover all cases listed above.

This result implies certain facts about the structure of L.

(4.6) Proposition. *Assume* (4.4). *Suppose* $t \geqslant 1$.

(1) *If* (2^t) *is the* 2*-invariant of* $\mathrm{Aut}(L)$ *then L has order* $1, 2, 4, p^e$, *or* $2p^e$ *for an odd prime p.*

(2) *If* $(2, 2^t)$ *are the* 2*-invariants of* $\mathrm{Aut}(L)$ *then L has order 2^s for $s > 2$, $4p^e$, p^eq^f, or $2p^eq^f$ where p, q are distinct odd primes such that* $2|\,|q-1$ *and* $(p^{e-1}(p-1), q^{f-1}(q-1)) = 2$.

(3) *If* $(2, 2, 2^t)$ *are the* 2*-invariants of* $\mathrm{Aut}(L)$ *then L has order* $8p^e$, $2^{t+2}q^f$, $4p^eq^f$, $p^eq^fr^g$, *or* $2p^eq^fr^g$ *where p, q, r are distinct odd primes such that* $2|\,|q-1, 2|\,|r-1$, *and*

$$\left(p^{e-1}(p-1), q^{f-1}(q-1)\right) = \left(p^{e-1}(p-1), r^{g-1}(r-1)\right)$$
$$= \left(q^{f-1}(q-1), r^{g-1}(r-1)\right) = 2.$$

(4) *If* $(4, 2^{t+1})$ *are the* 2*-invariants of* $\mathrm{Aut}(L)$ *then L has order p^eq^f or $2p^eq^f$ where p and q are distinct odd primes such that* $4|p-1$, $4|\,|q-1$ *and* $(p^{e-1}(p-1), q^{f-1}(q-1)) = 4$.

Write $L \simeq C_0 \times C_1 \times \cdots \times C_n$ where C_0 is cyclic of order 2^m and $|C_i| = p_i^{e_i}$ for $e_i > 0$ and p_i an odd prime. Then

$$\mathrm{Aut}(L) \simeq \mathrm{Aut}(C_0) \times \mathrm{Aut}(C_1) \times \cdots \times \mathrm{Aut}(C_n).$$

Further $\mathrm{Aut}(C_0)$ is of order 2^{m-1}. If $m > 2$ then $\mathrm{Aut}(C_0) \simeq \mathbf{Z}_2 \times \mathbf{Z}_{2^{m-2}}$. Each $\mathrm{Aut}(C_i)$ is cyclic of order $p_i^{e_i-1}(p_i - 1)$. The 2-rank of $\mathrm{Aut}(L)$ is n if $m = 0, 1$; $n + 1$ if $m = 2$; and $n + 2$ if $m > 2$. For an odd prime p^* the p^*-rank of $\mathrm{Aut}(L)$ is t^* where $p^*|p_i^{e_i-1}(p_i - 1)$ for exactly t^* values of i. Since $t^* = 1$ we conclude that $(p_i^{e_i-1}(p_i - 1), p_j^{e_j-1}(p_j - 1))$ is a power of 2 for all $i \neq j$.

The rest of the proof involves checking invariants. We complete the proof only for (3). Assume $m > 2$. Then $n + 2 = 3$ so $n = 1$. That is, $|L| = 2^m p^e$. If $2^x \| p - 1$ then $\mathrm{Aut}(L)$ has 2-invariants $(2, 2^{m-2}, 2^x)$. So $m = 3$ or $x = 1$. Therefore $|L| = 2^{t+2}p^e$, $2 \| p - 1$ or $8p^e$. Assume $m = 2$. Then $n + 1 = 3$ so that $n = 2$. Here $2^x \| p - 1$ and $2^y \| q - 1$ and L has order $4p^e q^f$. The 2-invariants of $\mathrm{Aut}(L)$ are $(2, 2^x, 2^y)$. So $y = 1$. Assume $m = 0, 1$. Then $n = 3$. The order of L is $2p^e q^f r^g$ or $p^e q^f r^g$. If $2^x \| p - 1$, $2^y \| q - 1$, and $2^z \| r - 1$ then the 2-invariants of $\mathrm{Aut}(L)$ are $(2^x, 2^y, 2^z)$. Therefore $y = z = 1$. Part (3) follows from these considerations. Other cases have similar proofs.

This result, (4.6), gives strong conditions upon the number of primes which may divide $|L|$. In our specific application, we may also limit the exponent upon these primes. To carry our such an argument, however, we need information about our particular group.

Recall the group H and the module $V = R/Z(R)$. Checking hypothesis (4.1) shows that [3, (3.1)] is a valid hypothesis. In particular, we may quote the following properties of H from [3].

(4.7) LEMMA [3, (3.2)]. *If $L \triangle H$ is abelian then L is cyclic.*

(4.8) LEMMA [3, (3.3)]. *H contains a cyclic self-centralizing normal subgroup $M \geqslant N$. Further,*

(a) $C_H(N) = C_A(N) \times N$;

(b) $(|C_A(N)|, |N|) = 1$;

(c) *$M = C_H(N)$ or $[C_H(N): M] = 2$ and an S_2-subgroup of $C_H(N)$ is quaternion, dihedral, or semidihedral.*

We may actually give canonical forms for H and V. First we must introduce the canonical groups and modules.

For an extension $\mathbf{K}_0$ of $\mathbf{K} = \mathrm{GF}(r)$ let $\mathcal{G} = \mathcal{G}(\mathbf{K}_0/\mathbf{K})$ be the Galois group of $\mathbf{K}_0$ over $\mathbf{K}$. Form the semidirect product $\mathcal{T}(\mathbf{K}_0/\mathbf{K}) = \mathcal{G} \cdot \mathbf{K}_0^\times$ where $\mathbf{K}_0^\times$ is the multiplicative group of $\mathbf{K}_0$. We shall use this group in our constructions. The additive group $\mathbf{K}_0^+$ is naturally a $\mathcal{T}(\mathbf{K}_0/\mathbf{K})$-module by

$$(\sigma x) \cdot v = \sigma(xv) = (xv)^{\sigma^{-1}}$$

where $\sigma \in \mathcal{G}$, $x \in \mathbf{K}_0^\times$, and $v \in \mathbf{K}_0^+$.

Observe that we have set $\mathcal{G} = \mathcal{G}(\mathbf{K}_0/\mathbf{K})$ when there is no confusion. We shall use other notational conventions in the following.

Let $\hat{\mathbf{K}} = \mathrm{GF}(r^{2m})$, $\tilde{\mathbf{K}} = \mathrm{GF}(r^m)$, and $\varphi: \varepsilon \to \varepsilon^{r^m}$ for $\varepsilon \in \hat{\mathbf{K}}$. Fix $\mu \in \hat{\mathbf{K}}$ so that $\mu^\varphi = -\mu$ (let $\mu = 1$ if $r = 2$). Let $\mathrm{Tr}: \tilde{\mathbf{K}} \to \mathbf{K}$ be the trace map.

(4.9) EXAMPLE. The group $\mathcal{T}_1 = \mathcal{T}^*(\hat{\mathbf{K}}/\mathbf{K})$.

For $u, v \in V_1 = \hat{\mathbf{K}}^+$ set

$$g_1(u, v) = \mathrm{Tr}(\mu(u^\varphi v - uv^\varphi)).$$

We let $\mathfrak{T}^*(\hat{\mathbf{K}}/\mathbf{K})$ be the subgroup of $\mathfrak{T}(\hat{\mathbf{K}}/\mathbf{K})$ fixing the form g_1. We set $\mathfrak{T}_1^0 = \hat{\mathbf{K}}^\times \cap \mathfrak{T}^*(\hat{\mathbf{K}}/\mathbf{K})$. This subgroup has order $r^m + 1$. The index is $[\mathfrak{T}_1 : \mathfrak{T}_1^0] = 2m$. If P is a p-Sylow subgroup of $\mathfrak{T}_1$ then P splits over $P \cap \mathfrak{T}_1^0$ unless $p = 2$. When $p = 2$, P is cyclic unless $4 | r^m + 1$ in which case P is generalized quaternion.

We shall prove these last facts now.

Let $\mathcal{G} = \mathcal{G}(\hat{\mathbf{K}}/\mathbf{K})$. Then $\mathfrak{T}_1$ is a subgroup of $\mathcal{G} \cdot \hat{\mathbf{K}}^\times$. In fact [3, (3.9)] $\mathfrak{T}_1/\mathfrak{T}_1^0 \simeq \mathcal{G}$ since $\mathfrak{T}_1^0\hat{\mathbf{K}}^\times = \mathcal{G} \cdot \hat{\mathbf{K}}^\times$. If p is an odd prime then $\mathfrak{T}_1^0$ contains the p-Sylow subgroup of $\hat{\mathbf{K}}^\times$. Therefore, an odd p-Sylow subgroup of $\mathfrak{T}_1$ is a p-Sylow subgroup of $\mathfrak{T}(\hat{\mathbf{K}}/\mathbf{K})$. These latter Sylow subgroups split over $\hat{\mathbf{K}}^\times$. So P splits over $P \cap \mathfrak{T}_1^0$ for odd primes p.

Suppose $p = 2$ and $2^t| \, |r^m + 1$ where $t \geqslant 2$. Choose $\nu \in \hat{\mathbf{K}}^\times$ of order 2^{t+1}. Then $\varphi\nu$ fixes g_1. Further, if $P_0 = P \cap \mathfrak{T}_1^0$ then $\langle \varphi\nu, P_0 \rangle$ is a 2-Sylow subgroup of $\mathfrak{T}_1$ and is generalized quaternion. Finally suppose $p = 2$ and $2^t| \, |r^m - 1$ where $t \geqslant 2$. Choose $\sigma \in \mathcal{G}$ of order 2^s where $2^s| \, |2m$. A 2-Sylow subgroup of $\mathfrak{T}_1$ will have order 2^{s+1}. By [3, (3.9)] $\sigma\nu \in \mathfrak{T}_1$ for $\nu \in \hat{\mathbf{K}}^\times$ will fix g_1 if and only if $\mu^\sigma\mu^{-1}\nu^\varphi\nu = 1$. We may choose ν to satisfy this identity. What is the order of $\sigma\nu$? Computing $(\sigma\nu)^{2^{s-1}} = \varphi\nu_0$ where $\nu_0 = \nu^{1+\sigma+\cdots+\sigma^{2^{s-1}-1}}$. This element fixes g_1 so that $1 = \mu^\varphi\mu^{-1}\nu_0^\varphi\nu_0 = -\nu_0^\varphi\nu_0$. Therefore, $\nu_0^\varphi = -\nu_0^{-1}$. We conclude that $(\sigma\nu)^{2s} = (\varphi\nu_0)^2 = -1$; and $\sigma\nu$ has order 2^{s+1}. Therefore, a 2-Sylow subgroup of $\mathfrak{T}_1$ is cyclic in this case.

(4.10) Example. The group $\mathfrak{T}_2 = \mathfrak{T}(\tilde{\mathbf{K}}/\mathbf{K})$.

Recall that $\tilde{\mathbf{K}} = \mathrm{GF}(r^m)$. Let e_1, e_2 be a $\tilde{\mathbf{K}}$-basis for a 2-dimensional vector space V_2. For $u = \alpha e_1 + \beta e_2$, $v = \alpha' e_1 + \beta' e_2$ where $\alpha, \alpha', \beta, \beta' \in \tilde{\mathbf{K}}$ set

$$g_2(u, v) = \mathrm{Tr}(\alpha'\beta - \alpha\beta').$$

We write semilinear transformations as matrices in the basis e_1, e_2.

$$\mathfrak{T}_2 = \mathfrak{T}^\dagger(\tilde{\mathbf{K}}/\mathbf{K}) = \left\langle \tau = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}, \begin{bmatrix} \sigma\nu & \\ & \sigma\nu^{-1} \end{bmatrix} \middle| \sigma \in \mathcal{G}(\tilde{\mathbf{K}}/\mathbf{K}), \nu \in \tilde{\mathbf{K}}^\times \right\rangle.$$

Then

$$\mathfrak{T}_2^0 = \left\langle \begin{bmatrix} \nu & \\ & \nu^{-1} \end{bmatrix} \middle| \nu \in \tilde{\mathbf{K}}^\times \right\rangle \simeq \tilde{\mathbf{K}}^\times$$

has order $r^m - 1$. This group fixes the form g_2. Let $\bar{\tau}$ be the inversion automorphism of $\tilde{\mathbf{K}}^\times$. Then $\bar{\tau}$ commutes with $\mathcal{G}(\tilde{\mathbf{K}}/\mathbf{K})$ upon $\tilde{\mathbf{K}}^\times$. Therefore:

(4.11) Lemma. *$\mathfrak{T}_2 \simeq (\langle \bar{\tau} \rangle \times \mathcal{G}(\tilde{\mathbf{K}}/\mathbf{K})) \cdot \tilde{\mathbf{K}}^\times$; and $\mathfrak{T}_2^0 \simeq \tilde{\mathbf{K}}^\times$.*

If P is a p-Sylow subgroup of $\mathfrak{T}_2$ then the isomorphism of (4.11) where $\mathfrak{T}_2^0 \simeq \tilde{\mathbf{K}}^\times$ makes it clear that P splits over $P \cap \mathfrak{T}_2^0$.

We reference the full description of $\mathfrak{T}_i$, $i = 1, 2$, just by (4.9) and (4.10). In using (4.11) we shall reference it directly.

Using these two group-module pairs we have the following theorem by [3, (3.10), (3.17)].

(4.12) THEOREM. *Assume* (4.1). *If M is a normal cyclic self-centralizing subgroup of H containing N then we may identify H, M, V, g respectively with H_0, M_0, V_i, g_i where $H_0 \leqslant \mathfrak{T}_i$ and $M_0 \leqslant \mathfrak{T}_i^0$ for $i = 1$ or 2 where* $\dim V_i = 2m$. *If $i = 2$ then H_0 (via* (4.11)) *does not lie in* $\mathcal{G}(\tilde{\mathbf{K}}/\mathbf{K}) \cdot \tilde{\mathbf{K}}^{\times}$.

Using our comments about Sylow subgroups of $\mathfrak{T}_i$ we may say the following.

(4.13) LEMMA. *If p is a prime and N contains a p-Sylow subgroup of $\mathfrak{T}_i^0$ then a p-Sylow subgroup P of H splits over $P \cap N$. In fact, for an appropriate conjugate of P, $P = (P \cap A)(P \cap N)$.*

We always get splitting unless $i = 1$ and $p = 2$. We need more than this. The group P may be chosen so that $P < A(P \cap N)$ since $AN = H$ and $P \cap N \triangle H$. Thus $P \cap [A(P \cap N)] = (P \cap A)(P \cap N)$. Since $(P \cap A) \cap (P \cap N) \leqslant A \cap N = 1$, we get the desired splitting.

The hypotheses of (4.13) are not difficult to satisfy.

(4.14) LEMMA. *If $\pi = \pi(C_A(N))$ is the set of prime divisors of $|C_A(N)|$ then for purposes of computing $\mathfrak{X}_\lambda|_A$ we may assume that N is a Hall π'-subgroup of $\mathfrak{T}_i^0$.*

Observe that the extension $(\mathfrak{T}_i^0 H)R$ exists. The group $\mathfrak{T}_i^0 H$ has order prime to r so that $\mathfrak{X}_\lambda(\mathfrak{T}_i^0 HR)$ exists. Thus $\mathfrak{X}_\lambda|_A = \mathfrak{X}_\lambda(\mathfrak{T}_i^0 HR)|_A$. Let N_0 be a Hall π'-subgroup of $\mathfrak{T}_i^0$. Consider the group $N_0 H$. With $H_0 = N_0 H = AN_0$ (since $N_0 \geqslant N$ by (4.8)(b)) H_0 satisfies the hypothesis (4.1). So (4.14) holds.

Actually, for computing $\mathfrak{X}_\lambda|_A$ the extension $(\mathfrak{T}_i^0 H)R$ need not be known to exist. As shown in §2, the values of $\mathfrak{X}_\lambda|_H$ depend only upon H, V, and g. Therefore, we may define $\mathfrak{X}_\lambda$ formally upon H_0 and observe that $\mathfrak{X}_\lambda|_A$ remains unchanged.

REMARK. For the rest of this section we assume that N is a Hall π'-subgroup of $\mathfrak{T}_i^0$.

Recall that $\bar{H} = H/C_H(N)$. We now prove that hypothesis (4.4) holds if $\bar{H}$ has fewer than three regular orbits upon N.

(4.15) LEMMA. *If $\bar{H}$ has fewer than three regular orbits upon N then* (4.4) *holds with $\bar{H} = K$ and $N = L$.*

Observe that $\bar{H} \leqslant \operatorname{Aut}(N)$. Since $\operatorname{Aut}(N)$ is regular upon generators of N we must have $[\operatorname{Aut}(N)\colon \bar{H}] \leqslant 2$. Now $\mathfrak{T}_i/\mathfrak{T}_i^0$ is isomorphic to $\mathcal{G}(\hat{\mathbf{K}}/\mathbf{K})$ if $i = 1$ and $\mathbf{Z}_2 \times \mathcal{G}(\tilde{\mathbf{K}}/\mathbf{K})$ if $i = 2$; The group $H/M \simeq H\mathfrak{T}_i^0/\mathfrak{T}_i^0$ is a subgroup of one of these. Since $[C_H(N)\colon M] = 1, 2$, $\bar{H} \simeq F$ or $\mathbf{Z}_2 \times F$ where F is cyclic. Therefore, (4.4) holds.

At this point (4.6) tells us something about the order of N. We now wish to bound the exponents of prime powers there. This is done by observing that $\bar{H}$ acts upon N like most of $\mathrm{Aut}(N)$. In particular, if $p^e \mid |N|$ for large e then $p \mid |\bar{H}|$. This double divisibility of primes is hard to carry off. So the exponents are limited.

(4.16) LEMMA. *Assume* (4.1). *Suppose p is a prime, $\sigma \in A$ has order p, T is a p-Sylow subgroup of N of order p^e where $e > 0$, and $[\sigma, N] \leqslant T$. Then $p = 2$ and $P = \langle \sigma, T\rangle$ is dihedral, semidihedral, or quaternion.*

Set $A = A_1 \times A_2$ where A_1 is a p-group and A_2 is a p'-group. Write $N = T \times N_2$ where N_2 is a p'-group. Now σ centralizes A_2 and N_2. Thus $\langle \sigma, A_2, N\rangle$ contains $\langle \sigma, C_A(N)N\rangle = \langle \sigma, M\rangle$ and is nilpotent. It is also normal in H since H/M is abelian. The group $P = \langle \sigma, T\rangle$ is a p-Sylow subgroup of $\langle \sigma, M\rangle$. Therefore P is normal in H. The group P is a split extension of T by $\langle \sigma \rangle$. Assume that if $p = 2$ then P is not dihedral, semidihedral or quaternion. Then $P_0 = \langle \sigma, \mho^1(T)\rangle$ is a characteristic abelian subgroup of P. In particular, it is normal in H. By (4.7) it is cyclic. Therefore, $\mho^1(T) = 1$. But now $\langle \sigma, T\rangle$ must be abelian. Again (4.7) applies to tell us that it is cyclic. So $T = 1$. But $|T| = p^e$ and $e > 0$. This contradiction concludes the proof of (4.16).

(4.17) LEMMA. *Assume* (4.1). *Suppose $\bar{H}$ has fewer than three regular orbits upon N. If $p^e \mid\, |N|$ then $e = 0, 1$ or $p = 2$ and $e = 0, 1, 2, 3$.*

Suppose the lemma is false. Recall that by (4.15), hypothesis (4.4) holds. In particular, $[\mathrm{Aut}(N): \bar{H}] \leqslant 2$. Let T be a p-Sylow subgroup of N. We may assume that $|T| = p^e$ where $e > 1$, or $e > 3$ if $p = 2$. If p is odd than $\mathrm{Aut}(N)$ contains a cyclic group of order $p^{e-1}(p-1)$. In particular, $\bar{H}$ contains an element $\bar{\sigma}$ of order p. If $p = 2$ then $\mathrm{Aut}(N)$ contains a copy of $\mathbf{Z}_2 \times \mathbf{Z}_{2^{e-2}}$. In this case $e > 3$ so that $\bar{H}$ will contain a copy of $\mathbf{Z}_{2^{e-3}}$ where $e - 3 > 0$. That is, we may choose $\bar{\tau} \in \mathrm{Aut}(N)$ so that $\bar{\tau}^2 = \bar{\sigma} \in \bar{H}$ has order 2. Further, $\bar{\tau}$ acts with order four upon T and $\bar{\sigma}$ acts with order p upon T.

By (4.13) we may choose a p-element $\sigma \in A$ so that $\sigma C_H(N) = \bar{\sigma}$. Now σ^p centralizes N and is in A. Therefore $\sigma^p \in C_A(N)$. By (4.8)(b) we conclude that $\sigma^p = 1$.

Next we prove that $[\sigma, N] \leqslant T$. Fix a prime q such that $q \neq p$ and $q^f \mid |N|$ where $f > 0$. Suppose σ is nontrivial upon a q-Sylow subgroup N_0 of N. That is, the image of σ in $\mathrm{Aut}(N_0)$ has order p. We now have $p \mid q - 1$. That is, $\mathbf{Z}_p \times \mathbf{Z}_p$ is a subgroup of $\mathrm{Aut}(T) \times \mathrm{Aut}(N_0)$ which, in turn, is a subgroup of $\mathrm{Aut}(N)$. Assume that $p > 2$. Then $\mathbf{Z}_p \times \mathbf{Z}_p$ resides in $\bar{H}$ since $[\mathrm{Aut}(N): \bar{H}] \leqslant 2$. But by (4.4) the odd part of $\bar{H}$ is cyclic. This contradiction proves that $[\sigma, N_0] = 1$. Since q was arbitrary, we conclude that $[\sigma, N] \leqslant T$ if p is odd.

We may now assume that $p = 2$. Since $|T| = 2^e$ and $e > 3$, $\mathrm{Aut}(T) \simeq \mathbf{Z}_2 \times \mathbf{Z}_{2^{e-2}}$ where $2^{e-2} \geqslant 4$. Further, $\mathrm{Aut}(N)$ contains $\mathrm{Aut}(T) \times \mathrm{Aut}(N_0)$. Now $\mathrm{Aut}(N)$ must contain $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_4$. From (4.5)(2) we find that $\mathrm{Aut}(N) \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times F_0$ where F_0 is cyclic of even order. From (4.6)(3) we discover that $|N| = 2^e q^f$ where $2|\,|q - 1$. At this point we are in trouble. Restricting $\bar{\tau}$ to N_0, $\bar{\tau}$ will have 2-power order. Since $2|\,|q - 1$, it has order one or two upon N_0. Therefore, $\bar{\tau}^2 = \bar{\sigma}$ is trivial upon N_0. Even when $p = 2$ we may conclude that $[\sigma, N_0] = 1$. So $[\sigma, N] \leqslant T$ for all possible p.

We have now satisfied the hypotheses of (4.16). In particular, $p = 2$ and $P = \langle \sigma, T \rangle$ is dihedral, semidihedral, or quaternion. That is, $\bar{\sigma}$ acts upon T as $x \to x^{-1}$ or $x \to x^{2^{e-1}-1}$. Neither of these automorphisms is a square in $\mathrm{Aut}(T)$. But restricting $\bar{\tau}$ to T gives an element of order four in $\mathrm{Aut}(T)$ whose square is $\bar{\sigma}$ restricted to T. That is, $\bar{\sigma}$ is both a square and a nonsquare on T. This final contradiction completes the proof of (4.17).

The two results (4.16) and (4.17) may be combined to yield the following:

(4.18) LEMMA. *Assume* (4.1). *Suppose $\bar{H}$ has at most two regular orbits upon N. Below are tabulated possible structures for N and $\bar{H}$. The following notations are used*: *c–cyclic*; *n–noncyclic*; *p,q,t–distinct odd primes. Further,*

$$(p - 1, q - 1) = (p - 1, t - 1) = (q - 1, t - 1) = 2, 4.$$

$\bar{H}$	$\mathrm{Aut}(N)$	$[\mathrm{Aut}(N){:}\ \bar{H}]$	$\lvert N\rvert$
c	c	1, 2	$p, 2p$
c	n	2	$4p, pq, 2pq$
n	n	1	$4p, pq, 2pq$
n	n	2	$4p, 8p, pq, 2pq, 4pq, pqt, 2pqt$

This table is derived from (4.5), (4.6), and (4.17). First observe that N is not a 2-group. Let A_1 be the 2-Sylow subgroup of A and A_2 the 2-complement. If N is a cyclic 2-group then $AN = A_2 \times (A_1 N)$ is nilpotent. This violates (4.1). By (4.17) if $p > 2$ and $p|\,|N|$ then $p|\,|\;|N|$. If $p = 2$ and $2|\,|N|$ then $16 \nmid |N|$. Combining this information with (4.5) and (4.6) yields the above table.

We may make one more remark.

(4.19) LEMMA. *Assume* (4.1). *If* $2|\,|N|$ *then* $|C_A(N)|$ *is odd and* $C_H(N)$ *is cyclic.*

By (4.8)(b) $|C_A(N)|$ is odd. Since N is cyclic and $C_H(N) = C_A(N)N$, (4.8)(b), (c) imply that $C_H(N)$ is cyclic.

We turn our attention now to the order of H/M. Recall that by (4.9), (4.10), and (4.11) we may view $\mathfrak{T}_i^0$ as a subgroup of the multiplicative group of the field $\hat{\mathbf{K}}$ or $\tilde{\mathbf{K}}$. Further, H/M acts upon $\mathfrak{T}_i^0$ as a subgroup of $\langle \bar{\tau} \rangle \times \mathfrak{G}$

where $\mathcal{G}$ is the Galois group of the field and $\bar{\tau}$ inverts the multiplicative group of the field. When $i = 1$ H/M acts as a subgroup of $\mathcal{G}$. So if $\bar{\sigma} \in H/M$ then $\bar{\sigma}$ or $\bar{\sigma}\bar{\tau}$ acts as an automorphism of the field. This fact will play a large role in our computations. We wish to limit the number of primes dividing $[H: M]$ and their exponents. First we need information about the structure of $A\mathcal{T}_i^0$.

(4.20) Lemma. *Assume* (4.1). *Suppose $\overline{H}$ has at most two regular orbits upon N. Let $\pi = \pi(C_A(N))$ be the set of prime divisors of $|C_A(N)|$. If M_π is a Hall π-subgroup of $\mathcal{T}_i^0$, and if $\bar{\sigma} \in H/M$ has order ξ^e for a prime ξ and exponent $e > 0$ then $\mathcal{T}_i^0 = M_\pi \times N$, AM_π is nilpotent, and $[\mathcal{T}_i^0: C_{\mathcal{T}_i^0}(\bar{\sigma})] = \xi^s[N: C_N(\bar{\sigma})]$ for some s.*

By (4.14) N is a Hall π'-subgroup of $\mathcal{T}_i^0$. Therefore, the cyclic group $\mathcal{T}_i^0$ equals $M_\pi \times N$. Suppose $p \in \pi$ and S is a p-Sylow subgroup of $\mathcal{T}_i^0$. Then $S_1 = S \cap A \neq 1$ since $p \in \pi$. Further, we may choose $\sigma \in A$ so that in H/M, $\sigma M = \bar{\sigma}$ where σ has ξ-power order. Thus $\langle \sigma, S_1 \rangle$ is contained in A and, therefore, is nilpotent. If $p \neq \xi$ then σ must centralize S_1. That is, σ must centralize S. This holds for all $p \in \pi$ and $\xi | [H: M]$. We now know that AM_π is nilpotent. But, in this case, $[M_\pi: C_{M_\pi}(\bar{\sigma})] = \xi^s$ is a power of ξ. Since M_π and N have relatively prime order and since $M = M_\pi \times N$ we conclude that $[M: C_M(\bar{\sigma})] = [M_\pi: C_{M_\pi}(\bar{\sigma})][N: C_N(\bar{\sigma})] = \xi^s[N: C_N(\bar{\sigma})]$. The proof is complete.

(4.21) Lemma. *Assume* (4.1). *Suppose $\overline{H}$ has at most two regular orbits upon N. Assume that $\bar{\sigma} \in H/M$ has order ξ^e for a prime ξ and exponent $e > 0$.*

(a) *If $\xi > 2$ then $e = 1$.*

(b) *If H is a subgroup of $\mathcal{T}_1$ and $\xi = 2$ then $|\mathcal{T}_1^0| = 2^b|N|$ and $e = 1$ unless $|N| = |\mathcal{T}_1^0| = 2q$ or $2|N| = |\mathcal{T}_1^0| = 2q$ for an odd prime q.*

(c) *If H is a subgroup of $\mathcal{T}_2$, $\xi = 2$, and $|N|$ has exactly ν odd prime divisors then $\nu \leqslant 3$ and $e \leqslant \nu + 1$.*

Suppose $e > 1$. By our previous remarks, $\bar{\sigma}$ or $\bar{\sigma}\bar{\tau}$ acts as a field automorphism. Further, we need only consider $\bar{\sigma}\bar{\tau}$ in part (c). Let $\bar{\sigma}^{\xi^{e-j}} = \bar{\sigma}_j$, $j = 0, \ldots, e$. If we are in part (c) and $\bar{\sigma}\bar{\tau}$ is the field automorphism we set $\bar{\sigma}_e = \bar{\sigma}\bar{\tau}$. Let $\mathbf{K}_j$ be the fixed field of $\bar{\sigma}_j$. Now $\mathbf{K}_j$ is a subfield of $\hat{\mathbf{K}}$ or $\tilde{\mathbf{K}}$ as $i = 1$ or 2. Let $\mathcal{H}_j = \mathcal{T}_i^0 \cap \mathbf{K}_j$. For this intersection we are viewing $\mathcal{T}_i^0$ as in $\hat{\mathbf{K}}$ or $\tilde{\mathbf{K}}$ (as in (4.11)). Observe that $\mathcal{H}_j$ is the centralizer of $\bar{\sigma}_j$ in $\mathcal{T}_i^0$. Therefore (4.20) applies to tell us that

$$[\mathcal{T}_i^0: \mathcal{H}_j] = \xi^{s_j}[N: C_N(\bar{\sigma}_j)]$$

for some s_j.

Turn now to (4.18). Suppose $|N| = 2^a q_1 \ldots q_\nu$ where $\nu < 3$ and $q_1, \ldots, q_\nu$ are odd primes. Then for $\alpha \neq \beta$ $(q_\alpha - 1, q_\beta - 1) = 2, 4$. By (4.5) and (4.6) the value of $(q_\alpha - 1, q_\beta - 1) = 4$ can only occur when $H \leqslant \mathcal{T}_2$ and $\nu = 2$.

Consider (a). Here $\bar{\sigma}_j$, $j > 0$, is trivial on all but one ($q_\beta = q$) q-Sylow subgroup of N. Thus $[N\colon C_N(\bar{\sigma}_j)] = q^f$ where $f = 0, 1$. Therefore,

$$\left[\mathfrak{T}_i^0\colon \mathcal{H}_e\right] = \xi^{s_e} q^f.$$

But then $[\mathfrak{T}_i^0\colon \mathcal{H}_1] = \xi^s$ for some s. Taking $\varepsilon = +1$ if $i = 1$ and $\varepsilon = -1$ if $i = 2$; and $m = \xi^e n$ we have $|\mathcal{H}_0| = |\mathfrak{T}_i^0| = r^{n\xi^e} + \varepsilon$. But then

$$\left[\mathfrak{T}_i^0\colon \mathcal{H}_1\right] = (r^{n\xi^e} + \varepsilon)/(r^{n\xi^{e-1}} + \varepsilon) = \xi^s.$$

If $e > 1$ and ξ is odd, this equation has no solution. We must have $\xi = 2$.

Consider (c). Assume now that $e > \nu + 1$. In this case $\mathcal{H}_j = \mathbf{K}_j^\times$. Now $[\mathfrak{T}_2^0\colon \mathcal{H}_{e-1}] = \Pi_j[\mathbf{K}_j^\times\colon \mathbf{K}_{j+1}^\times]$ over $j = 0, \ldots, e-1$. Set $[\mathbf{K}_j^\times\colon \mathbf{K}_{j+1}^\times] = \rho_j$. Then

$$\left[\tilde{\mathbf{K}}^\times\colon \mathbf{K}_{e-1}^\times\right] = \rho_0\rho_1 \ldots \rho_{e-2} = \left[\mathfrak{T}_2^0\colon C_{\mathfrak{T}_2^0}(\bar{\sigma}^2)\right]$$

divides $2^b q_1 \ldots q_\nu$ by (4.20) since $|N| = 2^a q_1 \ldots q_\nu$ and $\xi = 2$. There are $e - 1 > \nu$ values of ρ_j. So at least one ρ_j is a power of 2. Since $|\mathbf{K}_j^\times| = r^{n2^{e-j}} - 1$ where $m = n2^e$,

$$(r^{n2^{e-j}} - 1)/(r^{n2^{(e-j-1)}} - 1) = 2^c.$$

By (1.6) $n2^{(e-j-1)} = 1$ so that $e = j + 1$. But $j \leqslant e - 2$ or $e > j + 1$ since ρ_j has $j \leqslant e - 2$. This contradiction proves (c).

Finally we look at (b). The element $\bar{\sigma}$ is an automorphism in this case. Further, $\bar{\sigma}_1$ has order two. Thus $\bar{\sigma}_1$ is the automorphism of $\hat{\mathbf{K}} = \mathrm{GF}(r^{2m})$ of order two. But that automorphism sends $x \to x^{r^m}$. Here $x \in \mathfrak{T}_1^0$ so that $x^{r^m+1} = 1$ or $x^{r^m} = x^{\bar{\sigma}_1} = x^{-1}$. So $\bar{\sigma}_1$ inverts $\mathfrak{T}_1^0$. Recalling (4.20), $\mathfrak{T}_1^0 = M_\pi \times N$ and $\langle \sigma, M_\pi \rangle$ is nilpotent where $\sigma M = \bar{\sigma}$ and $\sigma \in A$ is a 2-element. Therefore, M_π is a 2-group, and $|\mathfrak{T}_1^0| = 2^b|N|$. By (4.5), (4.6) and (4.18), $|N| = 2^s, p, 2p, 4p, pq$, or $2pq$. Suppose $e > 1$. Then $2m = 2^e n$ so that $2|m$. In particular, $|\mathfrak{T}_1^0| = r^m + 1$ is twice an odd number. So $|\mathfrak{T}_1^0| = 2p, 2pq$. Therefore, $|N| = p, 2p, pq, 2pq$. By (4.6)(a), (b) if $pq|\,|N|$ then $(p-1, q-1) = 2$. Suppose $2|\,|p - 1$. So $\bar{\sigma}^2$ centralizes the p-Sylow subgroup of N. But $\bar{\sigma}^{2^{e-1}}$ inverts N. Since $e > 1$ we conclude that $pq \nmid |N|$. So if $e > 1$ then $|N| = 2p = |\mathfrak{T}_1^0|$ or $2|N| = 2p = |\mathfrak{T}_1^0|$ for an odd prime p. The proof of (4.21) is complete.

We have limited the exponents of primes dividing $[H\colon M]$. Next we limit the number of prime divisors in $[H\colon M]$ in terms of the number of prime divisors of $|N|$.

(4.22) LEMMA. *Assume* (4.1). *Suppose $\overline{H}$ has at most two regular orbits upon N. Suppose $p|\,|N|$ is an odd prime, and N_p is the p-Sylow subgroup of N. Let $H_p = H/C_H(N_p)$ be the restriction of H/M to N_p.*

(a) *If $\pi_0 = \pi(N)$ is the set of odd primes dividing $|N|$ and $p \in \pi_0$ then H_p is regular upon the elements of $N_p^\#$ with one possible exceptional p. For that one exception H_p has exactly two regular orbits upon the elements of $N_p^\#$.*

(b) *If H is a subgroup of $\mathfrak{T}_1$ then $|H_p| = 2^\alpha \xi$ for $\alpha \geqslant 0$ and $\xi = 1$ or ξ is an odd prime.*

(c) *If H is a subgroup of $\mathfrak{T}_2$ then $|H_p| = 2^\alpha$, ξ, or 2ξ where ξ is an odd prime. If $|H_p| = 2\xi$ then H_p contains an element inverting N_p.*

By (4.18) we know that $|N| = 2^s q_1 \dots q_\nu$ where $\nu \leqslant 3$. Let S_0 be the 2-Sylow and S_i the q_i-Sylow subgroup of N. Then

$$\operatorname{Aut}(N) = \operatorname{Aut}(S_0) \times \operatorname{Aut}(S_1) \times \cdots \times \operatorname{Aut}(S_\nu).$$

Now $[\operatorname{Aut}(N): \overline{H}] \leqslant 2$. Let $\overline{H}_0, \dots, \overline{H}_\nu$ be the projections of $\overline{H}$ into $\operatorname{Aut}(S_0), \dots, \operatorname{Aut}(S_\nu)$. Then $\overline{H} \leqslant \overline{H}_0 \times \cdots \times \overline{H}_\nu$. So $\overline{H}_i = \operatorname{Aut}(S_i)$ for all but possibly one value of i.

If $p = q_j$ then $N_p = S_j$. Therefore $H_p = \operatorname{Aut}(S_j)$ except for i if $i > 0$. If $p = q_i$, $i > 0$, then $[\operatorname{Aut}(S_i): H_p] = 2$. Since $\operatorname{Aut}(S_j)$, $j > 0$, is regular upon $S_j^{\#}$, part (a) follows.

For the next part, suppose $\gamma > \delta$ are two distinct prime divisors of $|H_p|$. Now $|N_p| = p$ is of prime order by (4.18). We have $|H_p| = \gamma^a \delta^b \cdot u$ where $(u, \gamma\delta) = 1$ and $a, b > 0$. Choose $\sigma_1 \in H_p$ of order γ and $\sigma_2 \in H_p$ of order δ (or δ^b if $\delta = 2$).

By (4.18) $(q_\alpha - 1, q_\beta - 1) = 2, 4$ for $\alpha \neq \beta$ where $|N| = 2^s q_1 \dots q_\nu$ and the q_j are odd primes. Thus $C_N(\sigma_i)$ contains all but one q_j-Sylow subgroup if σ_i has odd order. In particular,

$$[N: C_N(\sigma_1)] = p = q_{j_0} \quad \text{for some } j_0.$$

Suppose $\delta > 2$. Then $[N: C_N(\sigma_2)] = p$ also. By (4.20) we have

$$[\mathfrak{T}_i^0: C_{\mathfrak{T}_i^0}(\sigma_j)] = \gamma^\alpha p \ \text{ if } j = 1 \quad \text{or} \quad \delta^\beta p \ \text{ if } j = 2.$$

Let $\mathbf{K}_j$ be the fixed field of σ_j (recall that σ_j now acts as an automorphism of the underlying field). Set $\mathcal{H}_j = \mathbf{K}_j \cap \mathfrak{T}_i^0$. Then $\mathcal{H}_j = C_{\mathfrak{T}_i^0}(\sigma_j)$. Therefore p divides both $[\mathfrak{T}_i^0: \mathcal{H}_j]$ for $j = 1, 2$. So p divides $[\mathfrak{T}_i^0: \mathcal{H}_1\mathcal{H}_2]$. In particular, $[\mathcal{H}_1\mathcal{H}_2: \mathcal{H}_1] = \gamma^\omega$ is a power of γ. But then $[\mathcal{H}_1\mathcal{H}_2: \mathcal{H}_1] = [\mathcal{H}_2: \mathcal{H}_1 \cap \mathcal{H}_2] = \gamma^\omega$. Let $\varepsilon = 1$ if $i = 1$ and $\varepsilon = -1$ if $i = 2$. Then $|\mathcal{H}_2| = |\mathbf{K}_2 \cap \mathfrak{T}_i^0| = r^{m/\delta} + \varepsilon$ and $|\mathcal{H}_1 \cap \mathcal{H}_2| = |\mathbf{K}_1 \cap \mathbf{K}_2 \cap \mathfrak{T}_i^0| = r^{m/\gamma\delta} + \varepsilon$. So

$$(r^{n\gamma} + \varepsilon)/(r^n + \varepsilon) = \gamma^\omega$$

where $n = m/\gamma\delta$. By (1.6) we must have $\gamma^\omega = 3$, $\varepsilon = 1$, $n = 1$, and $r = 2$. By the same argument with δ in place of γ we obtain

$$[\mathcal{H}_1: \mathcal{H}_1 \cap \mathcal{H}_2] = \delta^\mu = (r^{n\delta} + \varepsilon)/(r^n + \varepsilon)$$

where $n = m/\gamma\delta$. By (1.6) we have $\delta^\mu = 3 = \gamma$. But $\gamma > \delta$. This proves that $|H_p|$ has at most one odd prime divisor.

Next we assume that $\delta = 2$. We now consider (c) since (b) holds. Further, we may assume that $|H_p| = 2^b\gamma$ where $b > 0$. Since $H_p \leqslant \operatorname{Aut}(N_p)$, it is cyclic. By (4.21) we know that $\gamma^a = \gamma$.

Since $\bar{H} < \mathrm{Aut}(N)$ and $|N| = 2^s q_1 \ldots q_\nu$ where $(q_\alpha - 1, q_\beta - 1) = 2, 4$ for $\alpha \neq \beta$ we must have $\gamma| \mid |\bar{H}|$. So we may choose $\bar{\sigma}_1 \in H/M$ of order γ so that $\bar{\sigma}_1 = \sigma_1$ in H_p. Further, we may choose $\bar{\sigma}_2 \in \mathrm{Aut}(N)$ of 2-power order so that $\bar{\sigma}_2$ is σ_2 in H_p. If $b \neq 1$ we may choose $\bar{\sigma}_2$ not inverting N_p. Let $\bar{\sigma}_2'$ be $\bar{\sigma}_2$ or $\bar{\sigma}_2\bar{\tau}$ whichever is a field automorphism. Then $\bar{\sigma}_2'$ is nontrivial upon N_p and acts upon N_p with order 2^b.

Let $\mathbf{K}_1$ and $\mathbf{K}_2$ respectively be the fixed fields of $\bar{\sigma}_1$ and $\bar{\sigma}_2'$. Now p divides $[\tilde{\mathbf{K}}^\times : \mathbf{K}_j^\times]$ for $j = 1, 2$. Thus $[\tilde{\mathbf{K}}^\times : \mathbf{K}_1^\times \mathbf{K}_2^\times]$ is divisible by p. But then since $[\tilde{\mathbf{K}}^\times : \mathbf{K}_1^\times] = [\mathfrak{T}_2^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma}_1)] = \gamma^\alpha p$ we have

$$\left[\mathbf{K}_1^\times \mathbf{K}_2^\times : \mathbf{K}_1^\times\right] = \left[\mathbf{K}_2^\times : \mathbf{K}_1^\times \cap \mathbf{K}_2^\times\right] = \gamma^\omega .$$

Now $[\mathbf{K}_2^\times : \mathbf{K}_1^\times \cap \mathbf{K}_2^\times] = (r^{n\gamma} - 1)/(r^n - 1) = \gamma^\omega$ where $m = n\gamma 2^b$. By (1.6) this cannot occur. Therefore $|H_p| = 2\gamma$ and σ_2 inverts N_p. This completes the proof of (c), and hence all of (4.22).

We may now complete the case where $H \leqslant \mathfrak{T}_1$.

(4.23) THEOREM. *Assume* (4.1). *Suppose* $\bar{H}$ *has at most two regular orbits upon* N, *and* $H < \mathfrak{T}_1$. *Then* $\bar{H} = H/M$ *and we have the following tabulated values*:

	r	m	$\|\bar{H}\|$	$\|N\|$	$\pi(A \cap M)$	# reg.orbits
(1)	2	1	2	3	$\varnothing$	1
(2)	2	2	2	5	$\varnothing$	2
(3)	2	2	4	5	$\varnothing$	1
(4)	2	4	8	17	$\varnothing$	2
(5)	2	5	5	11	3	2
(6)	3	2	2	5	2	2
(7)	3	2	4	5	2	1
(8)	3	3	3	7	2	2
(9)	3	3	6	7	2	1
(10)	5	3	3	7	2,3	2
(11)	$2^s \cdot 3 - 1$	1	2	3	2	1 ($s > 0$)
(12)	$2^s \cdot 5 - 1$	1	2	5	2	2 ($s > 0$)

By (4.18), $|N|$ is divisible by an odd prime. Further, an involution of H/M must invert $\mathfrak{T}_1^0$ by (4.9). Thus by (4.8)(c) $C_H(N) = M$.

Since $H < \mathfrak{T}_1$, H/M is cyclic and acts as field automorphisms of $\hat{\mathbf{K}}$. By (4.18) we have $|N| = p, 2p, 4p, pq, 2pq$. Now $[\mathrm{Aut}(N) : \bar{H}] < 2$. Therefore we may compute the order of $\bar{H}$. The possibilities $|N| = 2p$, $|\bar{H}| = (p - 1)/2$ and $|N| = 2pq$, $|\bar{H}| = (p - 1)(q - 1)/2$ do not occur. In both cases, $\bar{H}$ has two regular orbits upon the Hall $2'$-subgroup of N. The involution of N multiplied by orbit generators gives two more regular orbits. So there are four regular orbits. We therefore have the following table:

$$(*)\quad \begin{array}{cccccc} |N| & p & p & 2p & 4p & pq \\ |\bar{H}| & (p-1)/2 & (p-1) & (p-1) & (p-1) & (p-1)(q-1)/2 \end{array}$$

Since $\bar{H}$ is cyclic, when $|N| = pq$ we may assume that $2|\,|q-1$. By (4.22) we know that if $t|\,|N|$ is an odd prime then $|H_t| = 2^\alpha \xi$ where $\xi = 1$ or is an odd prime. Thus $t = 2^\beta \xi + 1$ where $\beta = \alpha$ or $\alpha + 1$. For p and q we may therefore write $p = 2^\beta \xi + 1$, $q = 2\zeta + 1$ where $\xi, \zeta = 1$ or are odd primes.

First assume that $|N|$ is divisible by a prime of the form $t = 2\xi + 1$ where $\xi > 1$. This will certainly occur for $|N| = pq$ unless $q = 2 + 1 = 3$. Choose $\bar{\sigma} \in \bar{H}$ of order ξ. By (4.20) $[\mathfrak{T}_1^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma})] = \xi^s t = \xi^s(2\xi + 1)$. Since ξ is odd $[\mathfrak{T}_1^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma})] = (r^{n\xi} + 1)/(r^n + 1)$ where $m = n\xi$. Thus

$$(r^{n\xi} + 1)/(r^n + 1) = \xi^s(2\xi + 1).$$

By (1.5) we know that $s = 0, 1$ since ξ is odd. But then by (1.4) we must have $n = 1$ and:

r	2	3	5
ξ	5	3	3
p	11	7	7

Since $|\bar{H}|$ divides $2m$ we have $|\bar{H}| = \xi, 2\xi$. This will lead to entries (5), (8), (9), and (10) of the table.

At this point we have $2m = 2\xi$ and $|\bar{H}|$ divides this number. If $|\bar{H}| = 2\xi$ then $\bar{H}$ contains an element of order two inverting $\mathfrak{T}_1^0$. Thus N contains the Hall $2'$-subgroup of $\mathfrak{T}_1^0$. By (4.9) a Sylow 2-subgroup of $\mathfrak{T}_1$ does not split over $\mathfrak{T}_1^0$ unless $r = 2$. So if $2|\,|\bar{H}|$ then N is the Hall $2'$-subgroup of $\mathfrak{T}_1^0$. Assume that $2|\,|\bar{H}|$. From this we obtain the values

r	2	3	5
m	5	3	3
$\lvert\bar{H}\rvert$	10	6	6
$\lvert N\rvert$	33	7	63

Since $63 = 3^2 \times 7$ and $|N|$ is not divisible by an odd square, the case $r = 5$ does not occur. With $r = 2$, $|\bar{H}| = 10$, $|N| = 33$, $\bar{H}$ has three regular orbits upon N. The remaining case with $r = 3$ is listed as (9).

Next suppose that $|\bar{H}| = \xi$. So $|N| = p$ and $|\bar{H}| = (p-1)/2$ by $(*)$. This leads to entries (5), (8), (10) of the table.

We now assume $|N|$ is not divisible by a prime $t = 2\xi + 1$ where $\xi > 1$, i.e. $\beta > 1$ and $\zeta = 1$. We have actually limited the remaining cases quite a bit. By (4.21)(b) we know that $\rho = 2\xi + 1$ and $q = 3$ if $|N| = pq$ since $|\bar{H}| = p - 1$ and $\bar{H}$ is cyclic. This rules out the possibility that $|N| = pq$. Further, if $|\bar{H}| = \xi$ is odd then by $(*)$ $\xi = (p-1)/2$ or $p = 2\xi + 1$. Again this case is ruled out. In particular, $|N| = p$, $2p$, $4p$ and $|\bar{H}|$ is even. By (4.21)(b), $|\mathfrak{T}_1^0| = 2^b|N|$. Thus $N = \mathfrak{T}_1^0$ or $|N| = p$ and $|\mathfrak{T}_1^0| = 2^bp$, $b > 0$. Since $|\bar{H}|$ is even and since the 2-Sylow subgroup of $\mathfrak{T}_1$ is not split over $\mathfrak{T}_1^0$ we conclude that $2| \, |C_A(N)|$ and $|N| = p$ is odd.

Now $|\mathfrak{T}_1^0| = 2^bp$ and $|N| = p$. Note that $|\bar{H}| = (p-1)$ or $(p-1)/2$. By (4.21)(b) $|\bar{H}| = 2^\alpha\xi$ where $\xi = 1$ or ξ is an odd prime. Thus $p = 2^\beta\xi + 1$ where $\beta = \alpha$ or $\alpha + 1$. We have already discussed the case where $\beta = 1$. So we know that $\beta > 1$.

Suppose $\xi > 1$. Choose $\bar{\sigma} \in \bar{H}$ of order ξ. By (4.20) $[\mathfrak{T}_1^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma})] = \xi^s p$. Since ξ is odd and $|\mathfrak{T}_1^0| = 2^bp$ we conclude that $s = 0$. Now $|\bar{H}|$ divides $2m$ so that $m = n\xi$. In particular,

$$\left[\mathfrak{T}_1^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma})\right] = p = (r^{n\xi} + 1)/(r^n + 1).$$

Therefore $r^n + 1 = 2^b$. This equation forces r to be odd and $n = 1$ by (1.7).

Note that $2m = 2\xi$. Since $|\bar{H}|$ is even, we conclude that $|\bar{H}| = 2\xi$. But $(p-1)/2 = 2^{\beta-1}\xi$ divides $|\bar{H}|$, thus $|\bar{H}| = 2^\beta\xi$ or $2^{\beta-1}\xi = 2\xi$. Since the case $\beta = 1$ has already been discussed we conclude that $\beta = 2$. Therefore, $p = 4\xi + 1$. Thus $(r^{n\xi} + 1)/(r^\xi + 1) = 4\xi + 1$. By (1.4) there are no solutions to this equation for r a prime and ξ odd. We conclude that $\xi = 1$.

Now $p = 2^\beta + 1$. Suppose $4| \, |\bar{H}|$. Then since $|\bar{H}|$ divides $2m$ we have $2|m$. If 2 divides $r^m + 1$ then $2| \, |r^m + 1$ since m is even. So $r^m + 1 = |\mathfrak{T}_1^0| = 2p = 2(2^\beta + 1)$ or $r^m = 2^{\beta+1} + 1$. By (1.7) the only solution to this equation is $r = 3$, $m = 2$, $\beta = 2$. In this case $p = 5$. Further $2m = 4$. Thus $|\bar{H}| = 4$. This all leads to entry (7) of the table. Suppose 2 does not divide $r^m + 1$. That is, $r = 2$. Now $2^m + 1 = p = 2^\beta + 1$. In particular, p is a Fermat prime and $m = \beta$ is a power of 2. Now $|\bar{H}| = (p-1)$ or $(p-1)/2$ so that $|\bar{H}| = 2^m$ or 2^{m-1}. But $|\bar{H}|$ divides $2m$. Therefore $2^{m-1} \leqslant 2m$ or $2^m \leqslant 2m$. The only powers of 2 which will work for m are $m = 2$ or $m = 4$. That is, $r = 2$, $m = 2$, $|\bar{H}| = 4$, $|N| = 5$ or $r = 2$, $m = 4$, $|\bar{H}| = 8$, $p = 17$. These account for entries (3) and (4) of the table.

We may now assume that $2| \, |\bar{H}|$. Since $|\bar{H}| = (p-1)$ or $(p-1)/2 = 2^\beta$ or $2^{\beta-1}$ we conclude that $\beta = 1, 2$. That is, $p = 3, 5$. Thus $r^m + 1 = 3, 5, 2^b \cdot 3, 2^b \cdot 5$ where $b > 0$. From $r^m + 1 = 3, 5$ we obtain entries (1) and (2). We are left with $r^m + 1 = 2^b \cdot 3, 2^b \cdot 5$ for $b > 0$. Now $p = 3, 5$ and $|\bar{H}| = (p-1)$ or $(p-1)/2$. So $|\bar{H}| = 2$.

Suppose an odd integer $\xi > 1$ divides m. Then $\mathfrak{T}_1/\mathfrak{T}_1^0$ contains an automorphism $\bar{\sigma}$ of order ξ. Clearly $\bar{\sigma}$ centralizes all elements of order 3 or 5 in $\mathfrak{T}_1^0$. Thus $[\mathfrak{T}_1^0 : C_{\mathfrak{T}_1^0}(\bar{\sigma})] = (r^{n\xi} + 1)/(r^n + 1) = 2^c$ where $n\xi = m$. Note that $r^m + 1 = 2^bp$ so that r is odd. By (1.6) we must have $\xi = 3$ and $r = 2$ since ξ is odd. We conclude that m is a power of 2. If m is even then when $r^m + 1 = 2p$ since $2| \, |r^m + 1$. Now $r^m + 1 = 6, 10$ so that $r^m = 5, 9$ and $m > 1$ is even.

This forces $r = 3$, $m = 2$, $p = 5$. This gives entry (6). We conclude that $m = 1$ so that $r = 2^b \cdot p - 1$. This leads to entries (11) and (12). The proof of (4.23) is complete.

We may turn now to the case where $H \leqslant \mathfrak{T}_2$. Recall that $\mathfrak{T}_2^0 \simeq \tilde{\mathbf{K}}^\times$ and H/M is isomorphic to a subgroup of $\langle\tau\rangle \times \mathcal{G}$ where τ inverts $\tilde{\mathbf{K}}^\times$ and $\mathcal{G}$ is the Galois group of $\tilde{\mathbf{K}}$. Further, $\mathcal{G}\mathfrak{T}_2^0$ is reducible upon V. Therefore, H/M contains an element $\tau\sigma$ for some $\sigma \in \mathcal{G}$.

(4.23′) Theorem. *Assume* (4.1). *Suppose* $H \leqslant \mathfrak{T}_2$ *and* $\bar{H}$ *has at most two regular orbits upon* N. *Then we must have the following values. In the last column* c *means* H/M *must be cyclic, and if* t *is an integer then* $\pi(t)$ *are the prime divisors of* t.

	r	m	$\lvert\bar{H}\rvert$	$[H: M]$	$\lvert N\rvert$	$\pi(A \cap M)$	# reg. orb.	*
(1)	2	2	2	2	3	$\varnothing$	1	c
(2)	2	3	6	6	7	$\varnothing$	1	c
(3)	2	4	2	2	3	5	1	c
(4)	2	4	4	4	$3 \cdot 5$	$\varnothing$	2	–
(5)	2	4	8	8	$3 \cdot 5$	$\varnothing$	1	–
(6)	2	4	4	4	5	3	3	$1c$
(7)	2	6	6	6	7	3	1	c
(8)	3	3	6	6	13	2	2	c
(9)	3	4	2	2	5	2	2	c
(10)	3	4	2	4	5	2	2	–
(11)	3	4	4	4	5	2	1	c
(12)	3	4	4	8	5	2	1	–
(13)	3	8	2	2	5	2, 41	2	c
(14)	5	2	2	2	3	2	1	c
(15)	5	2	2	4	3	2	1	–
(16)	5	4	2	2	3	2, 13	1	c
(17)	7	1	2	2	$2 \cdot 3$	$\varnothing$	2	c
(18)	7	2	2	2	3	2	1	c
(19)	7	2	2	4	3	2	1	–
(20)	7	4	2	2	3	2, 5	1	c
(21)	11	2	4	4	$3 \cdot 5$	2	2	–
(22)	31	2	4	4	$3 \cdot 5$	2	2	–
(23)	$2^s \cdot 3 + 1$	1	2	2	3	2	1	c
(24)	$2^s \cdot 3 + 1$	2	2	2	3	$\pi(r + 1)$	1	c
(25)	$2^s \cdot 5 + 1$	1	2	2	5	2	2	c
(26)	$2^s \cdot 5 + 1$	2	2	2	5	$\pi(r + 1)$	2	c

Suppose $\lvert N\rvert = 2^b q_1 \ldots q_\nu$ where the q_j are odd primes and $\nu \leqslant 3$. This follows from (4.18). Set $q_0 = 2$. Let N_j be the q_j-Sylow subgroup of N and H_j

the restriction of $\overline{H}$ to N_j. Suppose $j > 0$. By (4.22)(a) there is at most one j such that the restriction H_j of $\overline{H}$ to N_j is smaller than $\mathrm{Aut}(N_j)$. If such a j exists set that $j = \mu$. We may now determine the q_j's. For $j > 0$ we have $q_j - 1 = |H_j|$ if $j \neq \mu$ and $|H_\mu| = (q_\mu - 1)/2$. By (4.22)(c), $|H_j| = 2^{\alpha_j}, \xi_j$, or $2\xi_j$ where ξ_j is an odd prime. By (4.21)(c), since $\mathrm{Aut}(N_j)$ is cyclic we have $\alpha_j < \nu + 1 \leqslant 4$. We arrive at the following possibilities.

$$q_j = 3, 5, 17, 2\xi_j + 1 \quad \text{if } j \neq \mu$$

and

$$q_\mu = 3, 5, 17, 4\xi_\mu + 1.$$

First we settle the case where ξ_j occurs. That is, suppose $p = q_j$ for $j > 0$ and $p = 2^f\xi + 1$ where $f = 1, 2$ and ξ is an odd prime. Choose $\sigma \in H/M$ of order ξ. Since $(q_\alpha - 1, q_\beta - 1) = 1, 2, 4$ for $\alpha \neq \beta$ by (4.18), σ will centralize all N_j except the one of order $q_j = p$. Therefore, $[N: C_N(\sigma)] = p$. By (4.20) we then have

$$\left[\mathfrak{T}_2^0 : C_{\mathfrak{T}_2^0}(\sigma)\right] = \xi^s p = (r^{n\xi} - 1)/(r^n - 1)$$

where $m = n\xi$ since $\mathfrak{T}_2^0 \simeq \tilde{\mathbf{K}}^\times = \mathrm{GF}(r^m)^\times$, and since σ acts as an automorphism of $\tilde{\mathbf{K}}$. By (1.5) $s = 0, 1$. That is,

$$(r^{n\xi} - 1)/(r^n - 1) = (2\xi + 1), (4\xi + 1), \xi(2\xi + 1), \text{ or } \xi(4\xi + 1).$$

By (1.4) we must have the following values:

r	2	3	2
n	1	1	2
ξ	3	3	3
p	7	13	7

The number $|\overline{H}|/2$ divides m. Therefore $|\mathrm{Aut}(N)|/4$ (or $|\mathrm{Aut}(N)|/2$ if this is not an integer) divides m. Now $m = n\xi$ so that $n = 1, 2$ as tabulated above. Now $|\mathrm{Aut}(N)| = 2^{b-1}(2^f\xi)(q_2 - 1)\ldots(q_\nu - 1)$ where $p = 2^f\xi + 1 = q_1$. Since $\xi = 3$ we have $q_j = 3, 5, 17, 7, j \neq \mu$, and $q_\mu = 3, 5, 17, 13$. Running through the $|\mathrm{Aut}(N)|$ values ($\xi = 3$, $n = 1, 2$) we have: $|\mathrm{Aut}(N)| = 6, 12, 24$. We must now have:

$$|N| = 7, 2 \cdot 7, 4 \cdot 7, 3 \cdot 7, 2 \cdot 3 \cdot 7, 13, 2 \cdot 13, 8 \cdot 7,$$
$$4 \cdot 13, 3 \cdot 13, 2 \cdot 3 \cdot 13, 5 \cdot 7, 2 \cdot 5 \cdot 7.$$

Now $r = 2, 3$, $|N|$ divides $r^m - 1$, and by (4.14) $(r^m - 1, (r^m - 1)/|N|) = 1$. We must therefore have:

r	2	2	3	3
m	3	6	3	3
$\|N\|$	7	7	13	$2 \cdot 13$.

Let $\mathcal{G}$ be the Galois group of $\tilde{\mathbf{K}}$. Suppose $r = 2$, $m = 3$. Then τ is in H/M so that $H/M = \overline{H} \simeq \langle\tau\rangle \times \mathcal{G}$. Since $|N| = 7$ and $2^3 - 1 = 7$, $|A \cap M| = 1$. This is entry (2). Suppose $r = 2$, $m = 6$. Then $\mathcal{G} = \langle\sigma_1, \sigma_2\rangle$ where σ_1 has order three and σ_2 has order two. Here, again $|N| = 7$. Since N is in the fixed field of σ_2, σ_2 centralizes N. But N is a Hall subgroup of $\tilde{\mathbf{K}}^\times$ so that $3 \in \pi(A \cap M)$ by (4.14). The group of order nine in $\tilde{\mathbf{K}}^\times$ is inverted by σ_2. Now A is nilpotent and τ, σ_2 both invert $A \cap M$. Therefore $\tau, \sigma_2 \not\in H/M$. That is, $H/M = \overline{H} = \langle\tau\sigma_2\rangle \times \langle\sigma_1\rangle$. This gives entry (7). Finally, consider the case where $r = 3$, $m = 3$. Here $|N| = 13, 2 \cdot 13$. Further $\tau \in H/M$ so that $H/M = \overline{H} \simeq \langle\tau\rangle \times \mathcal{G}$. If $|N| = 2 \cdot 13$ then $\overline{H}$ has four regular orbits upon N. We conclude that $|N| = 13$ and $\pi(A \cap M) = 2$. This gives (8).

We may now assume that $q_j = 3, 5, 17$ for all j. Since $[\mathrm{Aut}(N): \overline{H}] \leqslant 2$ and $\overline{H}$ is cyclic or $\overline{H} \simeq \mathbf{Z}_2 \times F$ where F is cyclic we conclude that $\{q_1, \ldots, q_\nu\} = \{3\}, \{5\}, \{17\}, \{3, 5\}, \{3, 17\}, \{5, 17\}$. By (4.21) the exponent of $\overline{H}$, since $\overline{H}$ is now a 2-group, is less than or equal to $2^{\nu+1} \leqslant 2^3 = 8$. This fact with $\overline{H} \simeq \mathbf{Z}_2 \times F$ and $[\mathrm{Aut}(N): \overline{H}] \leqslant 2$ excludes the set $\{5, 17\}$.

At this point we know that $\overline{H}$ is a 2-group. Since H/M is a subgroup of $\langle\tau\rangle \times \mathcal{G}$ we know that there is a 2-power automorphism $\sigma \in \mathcal{G}$ of order 2^2 such that $H/M = \langle\tau\rangle \times \langle\sigma\rangle$ or $\langle\tau\sigma\rangle$. Let $\sigma_0 = \sigma^{2^{\alpha-1}}$ and suppose $\alpha > 1$. In particular, $\sigma_0 \in H/M$. Note that $2^\alpha | m$ so $m = 2n$ where n is even. Since σ_0 may be trivial in $\overline{H}$ (4.8), (4.14), and (4.20) tell us that

$$\begin{aligned}\left[\mathfrak{T}_2^0 : C_{\mathfrak{T}_2^0}(\sigma_0)\right] &= (r^{2n} - 1)/(r^{n-1}) = r^n + 1\\ &= 2^s, 2^s \cdot 3, 2^s \cdot 5, 2^s \cdot 3 \cdot 5, 2^s \cdot 3 \cdot 17.\end{aligned}$$

Since r is even (1.7) tells us that $2^s \neq r^n + 1$. Further, by (1.5) $s = 0, 1$. These values give rise to the following table:

r	n	$r^n + 1$	$r^m - 1$
2	2	5	$3 \cdot 5$
3	2	$2 \cdot 5$	$2^4 \cdot 5$

In both cases $m = 2^\alpha = 4$.

Suppose $r = 2$. In $\tau \in H/M$ then τ inverts the 3-elements of $\tilde{\mathbf{K}}^\times$ so by (4.14) $|N| = 3 \cdot 5$ and $H/M = \overline{H}$ has order 8. This is entry (5). The element σ inverts the 3-elements of $\tilde{\mathbf{K}}^\times$. Thus $\sigma\tau$ centralizes them. So $|N| = 5$ is possible when $H/M = \langle\sigma\tau\rangle$. If $|N| = 3 \cdot 5$ there are three regular orbits for $\overline{H} = H/M$ upon N. This gives entry (6).

Suppose $r = 3$. Since N is a Hall subgroup, $|N| = 5$ or $2^4 \cdot 5$. The latter case has too many regular orbits since $\langle\tau\rangle \times \langle\sigma\rangle$ acts as the full automorphism group on the 2-Sylow subgroup of $\tilde{\mathbf{K}}^\times$. Therefore $|N| = 5$. If $H/M = \langle\tau\sigma\rangle$ then $\overline{H} = H/M$. If $H/M = \langle\tau\rangle \times \langle\sigma\rangle$ then $\tau\sigma^2$ centralizes N. If T is a

2-Sylow subgroup of $\tilde{\mathbf{K}}^\times$ then $\langle \tau\sigma^2, T\rangle$ is semidihedral. These two possibilities lead to entries (11) and (12).

After the preceding, we may assume that $\alpha = 0, 1$. Suppose $\tau \in H/M$. Since τ inverts $\tilde{\mathbf{K}}^\times$ we must have $|\mathfrak{T}_2^0| = r^m - 1 = 2^s|N|$. That is, $r^m - 1 = 2^s \cdot 3, 2^s \cdot 5, 2^s \cdot 3 \cdot 5$. Since $\alpha = 0, 1$; 17 cannot be a factor of $|N|$. Suppose $\tau \notin H/M$. Then $H/M = \langle \tau\sigma\rangle$ where σ has order two. In particular, $m = 2n$. Let $\mathbf{K}'$ be the fixed field of σ. Then $\tau\sigma$ inverts $\mathbf{K}'^\times$ so that $\mathbf{K}'^\times/\mathbf{K}'^\times \cap N$ is a 2-group. Therefore, $r^n - 1 = 2^t, 2^t \cdot 3, 2^t \cdot 5$. The value $2^t \cdot 3 \cdot 5$ cannot occur since $|\bar{H}| = 2$. In either case $r^n - 1 = 2^s, 2^s \cdot 3, 2^s \cdot 5, 2^s \cdot 3 \cdot 5$ where $m = n$ or $2n$. By (1.8) we must have the following values if $n > 1$:

r	n	$r^n - 1$	$r^{2n} - 1$
2	2	3	$3 \cdot 5$
2	4	$3 \cdot 5$	$3 \cdot 5 \cdot 17$
3	2	2^3	$2^4 \cdot 5$
3	4	$2^4 \cdot 5$	$2^5 \cdot 5 \cdot 41$
5	2	$2^3 \cdot 3$	$2^4 \cdot 3 \cdot 13$
7	2	$2^4 \cdot 3$	$2^5 \cdot 3 \cdot 5^2$
11	2	$2^3 \cdot 3 \cdot 5$	$2^4 \cdot 3 \cdot 5 \cdot 61$
31	2	$2^6 \cdot 3 \cdot 5$	$2^7 \cdot 3^3 \cdot 5 \cdot 19$

Assume that $\bar{H} = H/M = \langle \tau\sigma\rangle$. Then m-$2n$ and $|\bar{H}| = 2$. In particular $3 \cdot 5 \nmid |N|$. Further, if $5 \mid |N|$ then $2 \nmid |N|$, and if $3 \mid |N|$ then $4 \nmid |N|$. If $x \in \tilde{\mathbf{K}}^\times$ order $r^n + 1$ then $\tau\sigma$ centralizes x. Since $\tau\sigma$ does not centralize the odd part of N, we conclude that $|N \cap \mathbf{K}'|$ is divisible by 3 or 5. Inspecting our table we have the following possibilities with $n > 1$:

r	m	$\lvert\bar{H}\rvert$	$[H{:}\, M]$	$\lvert N\rvert$	$\pi(A \cap M)$	# reg.orb.	*
2	4	2	2	3	5	1	c
3	8	2	2	5	2, 41	2	c
5	4	2	2	3	2, 13	1	c
7	4	2	2	3	2, 5	1	c

These entries lead to (3), (13), (16), and (20).

We conclude that $n = 1$. As remarked above, $\tau\sigma$ centralizes the elements of order dividing $r + 1$. Thus $|N| = 3, 5, 2 \cdot 3$ and the odd part of $|N|$ divides $r - 1$. That is, $r - 1 = 2^t \cdot 3, 2^t \cdot 5$. Now N is a Hall subgroup and $4 \mid r^2 - 1 = r^m - 1$ so that $|N| = 3, 5$. These considerations lead to the following:

r	m	$\lvert\bar{H}\rvert$	$[H{:}\, M]$	$\lvert N\rvert$	$\pi(A \cap M)$	# reg.orb.	*
$2^s \cdot 3 + 1$	2	2	2	3	$\pi(r + 1)$	1	c
$2^s \cdot 5 + 1$	2	2	2	5	$\pi(r + 1)$	1	c

These give entries (24) and (26).

We now assume that $\tau \in H/M$ and $m > 1$. With $m = n$ in our table we obtain:

	r	m	$\lvert\bar{H}\rvert$	$[H: M]$	$\lvert N\rvert$	$\pi(A \cap M)$	# reg.orb.	*
(1)	2	2	2	2	3	$\varnothing$	1	c
(4)	2	4	4	4	$3 \cdot 5$	$\varnothing$	2	–
(9)	3	4	2	2	5	2	2	c
(10)	3	4	2	4	5	2	2	–
(14)	5	2	2	2	3	2	1	c
(15)	5	2	2	4	3	2	1	–
(18)	7	2	2	2	3	2	1	c
(19)	7	2	2	4	3	2	1	–
(21)	11	2	4	4	$3 \cdot 5$	2	2	–
(22)	31	2	4	4	$3 \cdot 5$	2	2	–

The corresponding entries are noted at the left of the table. In entry (1), $\tau\sigma$ centralizes H. The irreducibility of H forces $\sigma \notin H/M$.

We are now reduced to $m = 1$, $\alpha = 0$, and $H/M = \bar{H} = \langle\tau\rangle$. But then $|N| = 2 \cdot 3, 3, 5$ and $r - 1 = 2^s \cdot 3, 2^s \cdot 5$. We must have the following list.

	r	m	$\lvert\bar{H}\rvert$	$[H: M]$	$\lvert N\rvert$	$\pi(A \cap M)$	# reg.orb.	*
(17)	7	1	2	2	$2 \cdot 3$	$\varnothing$	2	c
(23)	$2^s \cdot 3 + 1$	1	2	2	3	2	1	c
(25)	$2^s \cdot 5 + 1$	1	2	2	5	2	2	c

The proof of (4.23) is complete.

II. Condition B. Look back at (4.2). We have found all exceptions to Condition (A). We turn our attention to Condition (B) now. We must determine the structure of $C_H(N) = C_A(N) \times N$. In particular, where is $[C_H(N): M] = 2$?

(4.24) Lemma. *Assume* (4.1). *Also assume that* (4.14) *holds. Suppose that* $[C_H(N): M] = 2$. *Then* $H \leqslant \mathfrak{T}_2$; $\tilde{\mathbf{K}} = \mathrm{GF}(r^{2n})$; *and*

(1) $r = 3$, $n = 2$, *and* $|N| = 5$;

(2) $r - 1 = 2^s$, $n = 1$, *and* $|N| = (r + 1)/2$; *or*

(3) $r + 1 = 2^s$, $n = 1$, *and* $|N| = (r - 1)/2$.

Suppose $H \leqslant \mathfrak{T}_1$. Suppose $\sigma \in H/M$ has order two and centralizes N. Now $M \leqslant \mathfrak{T}_1^0$ and σ inverts $\mathfrak{T}_1^0$. Thus $|N| = 1, 2$. But H is not nilpotent. We conclude that $H \leqslant \mathfrak{T}_2$.

Since τ inverts $\tilde{\mathbf{K}}^\times$, if there is an element of order two in H/M centralizing N it must be σ or $\tau\sigma$ where σ is an automorphism of order two upon $\tilde{\mathbf{K}}$.

Assume that $\tau\sigma$ centralizes N. That is, σ inverts N. But this means $|N|$ $| r^n + 1$ where $m = 2n$. But $\tau\sigma$ inverts $\mathrm{GF}(r^n)^\times$. That is, $r^n - 1 = 2^s$. So we have $n = 1$ or $r = 3$, $n = 2$, and $s = 3$. Since N is a Hall subgroup $|N| = 5$ if $n > 1$. This proves (1). Assume that $n = 1$. Then $r - 1 = 2^s$. Now N is a Hall subgroup so that $|N|$ must be the odd part of $r + 1$. That is, $|N| = (r + 1)/2$. This proves (2). In both cases, the 2-Sylow subgroup of $C_{\mathfrak{T}_2}(N)$ is semidihedral.

Assume that σ centralizes N. That is, $|N|\ |r^n - 1$ where $m = 2n$. But σ inverts the elements of order dividing $r^n + 1$ in $\tilde{\mathbf{K}}^{\times}$ so that $2^s = r^n + 1$. In particular, $n = 1$. As before, $|N| = (r - 1)/2$ and the 2-Sylow subgroup of $C_{\mathfrak{T}_2}(N)$ is semidihedral. The proof of (3) is complete.

We turn now to the character theory of $\mathfrak{X}_\lambda(HR)|_{C_H(N)}$ as required by Condition (B).

(4.25) LEMMA. *Assume* (4.1). *Suppose that* $C_A(N) \leqslant M$. *Then* $\mathfrak{X}_\lambda(HR)|_{C_H(N)}$ *satisfies Condition* (B) *of* (4.2) *with* $b > 2$ *except as tabulated below*:

i	1	1	2	2
$[\mathfrak{T}_i^0 : M]$	1	2	1	2
b	1	2	1	2

Note that in this case, $C_H(N) = M \leqslant \mathfrak{T}_i^0$ is cyclic. If $i = 1$ then (3.8)(i)(b) applies to $B = \mathfrak{T}_1^0$. Thus

$$\mathfrak{X}_\lambda(\mathfrak{T}_1^0 R)|_{\mathfrak{T}_1^0} = \rho - \mu$$

where ρ is the regular $\mathfrak{T}_1^0$-character and μ is a character of order 1 or 2. Looking back at Condition (B) we see that $\rho - \mu|_M$ satisfies it if and only if $\rho|_M$ does also. But $\rho|_M = [\mathfrak{T}_i^0 : M]\rho_M$. From this, the tabulated values for $i = 1$ follow immediately.

If $i = 2$ then $\mathfrak{T}_2^0$ fixes $V_1 = \tilde{\mathbf{K}}e_1$ of (4.10), a maximal isotropic subspace of V. Let R_1 be the inverse image in R of V_1. Then $R_1 \simeq V_1 \times Z(R)$. Extend λ from $Z(R)$ to $(\mathfrak{T}_2^0 V_1) \times Z(R)$ by making it trivial upon $\mathfrak{T}_2^0 V_1$. The extended character λ^* induces $\mathfrak{X}_\lambda(\mathfrak{T}_2^0 R)\nu$ for some linear character ν of order 1 or 2. Thus

$$\mathfrak{X}_\lambda(\mathfrak{T}_2^0 R)\big|_{\mathfrak{T}_2^0} = \nu^{-1} \sum \lambda^{*x}\big|_{(\mathfrak{T}_2^0 V_1 \times Z(R))^{x^{-1}} \cap \mathfrak{T}_2^0}\big|^{\mathfrak{T}_2^0}$$

where the sum is over all $\mathfrak{T}_2^0 \times (\mathfrak{T}_2^0 V_1 \times Z(R))$ double cosets in R. Since $\mathfrak{T}_2^0 \simeq \tilde{\mathbf{K}}^{\times}$ and since $R/R_1 \simeq \tilde{\mathbf{K}}^{+}$ we have

$$\mathfrak{X}_\lambda(\mathfrak{T}_2^0 R)\big|_{\mathfrak{T}_2^0} = \nu^{-1}(1_{\mathfrak{T}_2^0} + \rho) = \nu^{-1} + \rho$$

where ρ is the regular $\mathfrak{T}_2^0$-character. Since ν^{-1} has order 1 or 2 the argument is exactly as for $i = 1$. The proof of (4.25) is now complete.

We turn next to the case where $C_A(N) \nleqslant M$. That is, we assume the hypotheses of (4.24) hold.

(4.26) Lemma. *Assume that the hypotheses and conclusion* (1) *or* (2) *of* (4.24) *hold. Then Condition* (B) *of* (4.2) *with* $b > 2$ *holds except as tabulated below*:

$[\mathfrak{T}_2^0 : M]$	1	2	2	4	4
b	0	0	1	1	2
$C_A(N)$	semidihedral	dihedral	quaternion	dihedral	quaternion

Let Q_0 be the 2-Sylow subgroup of $\mathfrak{T}_2^0$. Since $|N| = 5$ or $(r + 1)/2$, $NQ_0 = \mathfrak{T}_2^0$. Because $[C_A(N): M] = 2$, $\tau\sigma \in H/M$ where σ is an automorphism of $\tilde{\mathbf{K}}$ of order two and τ inverts $\tilde{\mathbf{K}}^{\times}$. But $C_A(N)Q_0 = C_A(N)$ so that

$$\begin{bmatrix} & 1 \\ -1 & \end{bmatrix}\begin{bmatrix} \sigma & \\ & \sigma \end{bmatrix} = \begin{bmatrix} & \sigma \\ -\sigma & \end{bmatrix} \in C_A(N)\mathfrak{T}_2^0.$$

Looking back at (3.6) we see that $C_A(N)\mathfrak{T}_2^0 = B = Q \times D$. Choosing a conjugate of A in H, if necessary, we may assume that $C_A(N)Q_0 = Q$ of (3.6). From here (3.8)(iv)(b) applies to give:

$$\mathfrak{X}_\lambda|_B = \sum_{\chi(1)>1} \chi + (1_Q + \mu_1)\delta + \mu_2$$

where μ_1 has dihedral and μ_2 has quaternion kernel upon Q. Let ρ be the regular character of N and ρ_T the regular character of a group T. Then

$$\mathfrak{X}_\lambda|_B = \rho\left[\tfrac{1}{2}(\rho_Q - 1_Q - \mu_2 - \mu_3) + 1_Q + \mu_1\right] + \mu_2$$

where μ_3 is nontrivial upon Q and has cyclic kernel.

Let Q_1 be a maximal dihedral subgroup of Q. Let μ_3' be the linear character of Q_1 with cyclic kernel. Let $B_1 = Q_1N$. Then

$$\mathfrak{X}_\lambda|_{B_1} = \rho\left[\rho_{Q_1} + 1_{Q_1} - \mu_3'\right] + \mu_3'.$$

Suppose Q_2 is a maximal dihedral subgroup of Q_1 and μ_3'' is linear with cyclic kernel. Let $B_2 = NQ_2$ so that

$$\mathfrak{X}_\lambda|_{B_2} = \rho\left[2\rho_{Q_2} + 1_{Q_2} - \mu_3''\right] + \mu_3''.$$

Clearly, restricting further to subgroups of Q_2 will give rise to at least 3-regular characters.

Let Q_3 be a maximal quaternion subgroup of Q. Let ν_3' be a linear character with cyclic kernel upon Q_3. Then with $B_3 = Q_3N$,

$$\mathfrak{X}_\lambda|_{B_3} = \rho\rho_{Q_3} + 1_{Q_3}.$$

The pattern for further restrictions is obvious here. Thus we have sufficient information to prove (4.26).

(4.27) Lemma. *Assume that the hypotheses and conclusion* (3) *of* (4.24) *hold. Then Condition* (B) *of* (4.2) *with* $b > 2$ *holds except as tabulated below*:

$[\mathfrak{T}_2 : M]$	1	2	2	4	4
b	0	0	1	1	2
$C_A(N)$	semidihedral	dihedral	quaternion	dihedral	quaternion

Again let Q_0 be the 2-Sylow subgroup of $\mathfrak{T}_2^0$. Now $\mathfrak{T}_2^0 = NQ_0$. Further, $\sigma \in H/M$ where σ is an automorphism of $\tilde{\mathbf{K}}$ of order two. But now, looking back at (4.10) we have

$$C_H(N)Q_0 = \left\langle \begin{bmatrix} \sigma & \\ & \sigma \end{bmatrix}, \begin{bmatrix} \nu & \\ & \nu^{-1} \end{bmatrix} \middle| \nu \in \tilde{\mathbf{K}}^\times \right\rangle.$$

In particular, $B = C_H(N)Q_0$ fixes the subspace $V_1 = \tilde{\mathbf{K}}e_1$. In R, the inverse image in BR of B and V_1 takes the form $(BV_1) \times Z(R)$. Extending λ to this group by making it trivial upon BV_1 gives a character λ^*. We then have $\mathfrak{X}_\lambda \mu = \lambda^*|^{BR}$ where μ has order one or two. Then

$$\begin{aligned} \mathfrak{X}_\lambda|_B &= \mu(1_B + 1_{\langle\sigma\rangle})|^B \\ &= \mu\rho\left(\tfrac{1}{2}(\rho_Q - 1_Q - \mu_1 - \mu_2 - \mu_3) + 1_Q + \mu_1\right) + \mu \end{aligned}$$

where $Q = \langle [{}^\sigma{}_\sigma], Q_0 \rangle$, ρ is regular upon N, ρ_Q is regular upon Q, μ_1 has dihedral kernel, μ_2 has quaternion kernel, and μ_3 has cyclic kernel. This character looks exactly like the one arising in (4.26). From here, the analysis and answers are the same.

III. THE FINAL RESULT. We are not in a position to apply (4.3). We shall tabulate exceptional numbers. For purposes of clarity, we restate the hypotheses of this section.

(4.1) HYPOTHESIS. (a) Suppose $H = AN$ is not nilpotent where $N \triangle H$ is cyclic, A is nilpotent, and $A \cap N = 1$. Let r be a prime not dividing $|H|$, and $G = HR$ where R is a normal extraspecial r-group, $Z(R) \leqslant Z(G)$, and $R/Z(R)$ is a faithful minimal H-module.

(b) Let $\mathbf{k}$ be a finite extension of the rational field containing all $|G|$th roots of unity. Let λ be a nontrivial linear character of $Z(R)$ in $\mathbf{k}$ and $\mathfrak{X}_\lambda(G) = \mathfrak{X}_\lambda$, the unique character of (2.2).

Recall that $|R| = r^{2m+1}$ and H embeds in one of the groups of (4.9) or (4.10). In our theorem i denotes $H \leqslant \mathfrak{T}_i$; S_2 denotes the 2-Sylow subgroup of $C_A(N)$; $*$ denotes $A/C_A(N)$; and # reg. denotes a lower bound for the number of copies of the regular A-character in $\mathfrak{X}_\lambda|_A$. We have used letters as follows: c–cyclic, n–noncyclic, d–dihedral, s–semidihedral, and q–quaternion.

(4.28) THEOREM. *Assume* (4.1) *where* $|R| = r^{2m+1}$. *Suppose* $\mathfrak{X}_\lambda|_A$ *does not contain at least three copies of the regular A-character. We then have the following tabulated data. The exponent* $s > 0$:

	r	m	$\lvert C_A(N)\rvert$	S_2	$[A: C_A(N)]$	$*$	$\lvert N\rvert$	i	# reg.
(1)	3	4	2^5	s	–	–	–	2	0
(2)	3	4	2^4	d	–	–	–	2	0
(3)	$2^s + 1$	2	2^{s+2}	s	–	–	–	2	0
(4)	$2^s + 1$	2	2^{s+1}	d	–	–	–	2	0

(5)	$2^s - 1$	2	2^{s+2}	s	–	–	–	2	0
(6)	$2^s - 1$	2	2^{s+1}	d	–	–	–	2	0
(7)	2	1	1	c	2	c	3	1	1
(8)	2	2	1	c	2	c	3	2	1
(9)	2	2	1	c	4	c	5	1	1
(10)	2	3	1	c	6	c	7	2	1
(11)	2	4	5	c	2	c	3	2	1
(12)	2	4	1	c	8	n	$3 \cdot 5$	2	1
(13)	2	4	3	c	4	c	5	2	1
(14)	2	6	9	c	6	c	7	2	1
(15)	3	2	2	c	4	c	5	1	1
(16)	3	3	4	c	6	c	7	1	1
(17)	3	4	16	c	4	c	5	2	1
(18)	3	4	8	d	4	c	5	2	1
(19)	3	4	16	q	4	c	5	2	1
(20)	5	2	8	c	2	c	3	2	1
(21)	5	2	8	q	2	c	3	2	1
(22)	5	4	$16 \cdot 13$	c	2	c	3	2	1
(23)	7	2	16	c	2	c	3	2	1
(24)	7	2	8	d	2	c	3	2	1
(25)	7	2	16	q	2	c	3	2	1
(26)	7	4	$32 \cdot 25$	c	2	c	3	2	1
(27)	$2^s \cdot 3 - 1$	1	2^s	c	2	c	3	1	1
(28)	$2^s \cdot 3 + 1$	1	2^s	c	2	c	3	2	1
(29)	2	2	1	c	2	c	5	1	2
(30)	2	4	1	c	4	n	$3 \cdot 5$	2	2
(31)	2	4	1	c	8	c	17	1	2
(32)	2	5	3	c	5	c	11	1	2
(33)	3	2	2	c	2	c	5	1	2
(34)	3	2	1	c	4	c	5	1	2
(35)	3	3	4	c	3	c	7	1	2
(36)	3	3	2	c	6	c	13	2	2
(37)	3	3	2	c	6	c	7	1	2
(38)	3	4	16	c	2	c	5	2	2
(39)	3	4	8	d	2	c	5	2	2
(40)	3	4	16	q	2	c	5	2	2
(41)	3	4	8	c	4	c	5	2	2
(42)	3	4	8	q	4	c	5	2	2
(43)	3	8	$32 \cdot 41$	c	2	c	5	2	2
(44)	5	2	4	c	2	c	3	2	2
(45)	5	3	$2 \cdot 9$	c	3	c	7	1	2

(46)	5	4	$8 \cdot 13$	c	2	c	3	2	2
(47)	7	1	1	c	2	c	6	2	2
(48)	7	2	8	c	2	c	3	2	2
(49)	7	2	8	q	2	c	3	2	2
(50)	7	4	$16 \cdot 25$	c	2	c	3	2	2
(51)	11	2	8	c	4	n	15	2	2
(52)	31	2	64	c	4	n	15	2	2
(53)	$2^s \cdot 3 - 1$	1	2^{s-1}	c	2	c	3	1	2
(54)	$2^s \cdot 5 - 1$	1	2^s	c	2	c	5	1	2
(55)	$2^s \cdot 3 + 1$	1	$2^s - 1$	c	2	c	3	2	2
(56)	$2^s \cdot 3 + 1$	2	$2^{s-1}(r + 1)$	c	2	c	3	2	2
(57)	$2^s \cdot 5 + 1$	1	2^s	c	2	c	5	2	2
(58)	$2^s \cdot 5 + 1$	2	$2^s(r + 1)$	c	2	c	5	2	2

These tables are produced by using (4.3). From (4.23) and (4.24) we obtain a number a giving the cases where $a \leqslant 2$ and $\bar{H} = H/C_H(N) \simeq A/C_A(N)$ has exactly a regular orbits in its action upon N. From (4.24), (4.25), (4.26), and (4.27) we obtain the number $b \leqslant 2$ used in Condition (B) of (4.2). We itemize all cases where $ba \leqslant 2$. A few remarks are in order. In (4.14) we assumed that N was a Hall subgroup of $\mathfrak{T}_i^0$. So the results described above yield an upper bound for $|N|$. But $\bar{H}$ must be faithful upon N. In all but case (47) this forces the order $|N|$ to be equal to the upper bound. The other possible situations corresponding to $|N| = 6$ in (47) are catalogued as (28) and (55) with $s = 1$.

Further, $[\mathfrak{T}_i^0 \colon M]$ is bounded by (4.25), (4.26), and (4.27). These bounds allow us to determine $|C_A(N)|$ when $C_A(N) \leqslant M$. In all other cases $[C_A(N)\colon A \cap M] = 2$ so that $[H\colon M] = 2|\bar{H}|$. That is, (10), (12), (15), (19) of (4.23) hold if $b > 0$. These entries with (4.26) and (4.27) lead to table entries (18), (19), (21), (24), (25), (39), (40), (42), and (49) giving the order and structure of $C_A(N)$.

Finally, (4.24), (4.26), (4.27) give all the information available when $b = 0$.

The table has not been checked to see whether "# reg." gives exactly the number of regular A-characters in $\mathfrak{X}_\lambda|_A$. The number "# reg." is a lower bound. This is more than enough for most applications.

We now prove some corollaries.

(4.28) Corollary. *Assume* (4.1). *Let t be the number of regular A-characters contained in $\mathfrak{X}_\lambda|_A$.*

(a) *If A is $\mathbf{Z}_2 \wr \mathbf{Z}_2$ free then $t \geqslant 1$.*

(b) *If $|A|$ is odd then $t \geqslant 3$ unless $t = 2$, $|R| = 2^{11}$, $|N| = 11$, $|C_A(N)| = 3$, and $[A\colon C_A(N)] = 5$.*

For (a) we need only check the entries of (4.27) for which "# reg." is 0. But in all these $C_A(N)$ is dihedral or semidihedral. Therefore A involves $\mathbf{Z}_2 \wr \mathbf{Z}_2$ in these cases.

In (b) $|C_A(N)|$ is even if "# reg." is 0. Further, $[A: C_A(N)]$ is even except for entries (32), (35), and (45). In all these $|C_A(N)|$ is even except for entry (32). This entry gives the only case where $t = 2$. Direct computation shows that $t = 2$ is the correct answer in this exceptional case.

References

1. T. R. Berger, *Class two p-groups as fixed point free automorphism groups*, Illinois J. Math. **14** (1970), 121–149. MR **41** #336.

2. ———, *Hall-Higman type theorems*. I, Canad. J. Math. **26** (1974), 513–531.

3. ———, *Hall-Higman type theorems*. II, Trans. Amer. Math. Soc. **205** (1975), 47–69.

4. ———, *Hall-Higman type theorems*. V, Pacific J. Math. (to appear).

5. ———, *Hall-Higman type theorems*. VI (to appear).

6. C. W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1962. MR **26** #2519.

7. P. X. Gallagher, *Group characters and normal Hall subgroups*, Nagoya Math. J. **21** (1962), 223–230. MR **26** #240.

8. Daniel Gorenstein, *Finite groups*, Harper and Row, New York, 1968. MR **38** #229.

9. B. Huppert, *Endliche Gruppen*. I, Springer-Verlag, Berlin and New York, 1967. MR **37** #302.

10. I. M. Isaacs, *Characters of solvable and symplectic groups*, Amer. J. Math. **95** (1973), 594–635.

Department of Pure Mathematics, The Australian National University, Box 4, P. O., Canberra, A. C. T., Australia, 2600

Current address: Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455