Pacific Journal of Mathematics

CHAPTER V, FROM SOLVABILITY OF GROUPS OF ODD ORDER, PACIFIC J. MATH., VOL. 13, NO. 3 (1963

WALTER FEIT AND JOHN GRIGGS THOMPSON

Vol. 13, No. 3 May 1963

CHAPTER V

27. Statement of the Result Proved in Chapter V

The following result is proved in this chapter.

THEOREM 27.1. *Let $\mathfrak{G}$ be a minimal simple group of odd order. Then $\mathfrak{G}$ satisfies the following conditions:*

(i) *p and q are odd primes with $p > q$. $\mathfrak{G}$ contains elementary abelian subgroups $\mathfrak{P}$ and $\mathfrak{Q}$ with $|\mathfrak{P}| = p^a$, $|\mathfrak{Q}| = q^b$. $\mathfrak{P}$ and $\mathfrak{Q}$ are* T.I. *sets in $\mathfrak{G}$.*

(ii) *$N(\mathfrak{P}) = \mathfrak{P}\mathfrak{U}\mathfrak{Q}^*$, where $\mathfrak{P}\mathfrak{U}$ and $\mathfrak{U}\mathfrak{Q}^*$ are Frobenius groups with Frobenius kernels $\mathfrak{P}$, $\mathfrak{U}$ respectively. $|\mathfrak{Q}^*| = q$, $|\mathfrak{U}| = (p^a - 1)/(p - 1)$, $\mathfrak{Q}^* \subseteq \mathfrak{Q}$ and $((p^a - 1)/(p - 1), p - 1) = 1$.*

(iii) *If $\mathfrak{P}^* = C_{\mathfrak{P}}(\mathfrak{Q}^*)$, then $|\mathfrak{P}^*| = p$ and $\mathfrak{P}^*\mathfrak{Q}^*$ is a self-normalizing cyclic subgroup of $\mathfrak{G}$. Furthermore, $C(\mathfrak{P}^*) = \mathfrak{P}\mathfrak{Q}^*$, $C(\mathfrak{Q}^*) = \mathfrak{Q}\mathfrak{P}^*$, and $\mathfrak{P}^* \subseteq N(\mathfrak{Q})$.*

(iv) *$C(\mathfrak{U})$ is a cyclic group which is a* T.I. *set in $\mathfrak{G}$. Furthermore, $\mathfrak{Q}^* \subseteq N(\mathfrak{U}) = N(C(\mathfrak{U}))$, $N(\mathfrak{U})/C(\mathfrak{U})$ is a cyclic group of order pq and $N(\mathfrak{U})$ is a Frobenius group with Frobenius kernel $C(\mathfrak{U})$.*

In this chapter we take the results stated in Section 14 as our starting point. The notation introduced in that section is also used. There is no reference to any result in Chapter IV which is not contained in Section 14. The theory of group characters plays an essential role in the proof of Theorem 27.1. In particular we use the material contained in Chapter III.

Sections 28–31 consist of technical results concerning the characters of various subgroups of $\mathfrak{G}$. In Section 32 the troublesome groups of type V are eliminated. In Section 33 it is shown that groups of type I are Frobenius groups. By making use of the main theorem of [10] it is then easy to show that the first possibility in Theorem 14.1 cannot occur. The rest of the chapter consists of a detailed study of the groups $\mathfrak{S}$ and $\mathfrak{T}$ until in Section 36 we are able to supply a proof of Theorem 27.1.

28. Characters of Subgroups of Type I

Hypothesis 28.1.

(i) *$\mathfrak{X}$ is of Frobenius type with Frobenius kernel $\mathfrak{H}$ and complement $\mathfrak{E}$.*

(ii) *$\mathfrak{E} = \mathfrak{A}\mathfrak{B}$, where $\mathfrak{A}$ is abelian, $\mathfrak{B}$ is cyclic, and $(|\mathfrak{A}|, |\mathfrak{B}|) = 1$.*

(iii) $\mathfrak{E}_0$ *is a subgroup of* $\mathfrak{E}$ *with the same exponent as* $\mathfrak{E}$ *such that* $\mathfrak{E}_0\mathfrak{H}$ *is a Frobenius group with Frobenius kernel* $\mathfrak{H}$.

LEMMA 28.1. *Under Hypothesis* 28.1, $\mathfrak{X}$ *has an irreducible character of degree* $|\mathfrak{E}_0|$ *which does not have* $\mathfrak{H}$ *in its kernel.*

Proof. If $\mathfrak{A}$ is cyclic, then $\mathfrak{X}$ is a Frobenius group and the lemma is immediate. We may assume that $\mathfrak{A}$ is non cyclic.

Let $\mathfrak{H}_1/\boldsymbol{D}(\mathfrak{H})$ be a chief factor of $\mathfrak{A}\mathfrak{H}$ with $\mathfrak{H}_1 \subseteqq \mathfrak{H}$. Let $\mathfrak{A}_1 = \boldsymbol{C}_{\mathfrak{A}}(\mathfrak{H}_1/\boldsymbol{D}(\mathfrak{H}))$. Then $\mathfrak{A}/\mathfrak{A}_1$ is cyclic. Since $\mathfrak{X}$ is of Frobenius type, the exponent of $\mathfrak{A}/\mathfrak{A}_1$ is the exponent of $\mathfrak{A}$. Hence, $|\mathfrak{E}:\mathfrak{A}_1| = |\mathfrak{E}_0|$. Let $\mathfrak{A}_2$ be the normal closure of $\mathfrak{A}_1$ in $\mathfrak{E}$. Then $\mathfrak{A}_2$ is abelian. Let μ be a non principal linear character of $\mathfrak{H}_1/\boldsymbol{D}(\mathfrak{H})$. Then $\mathfrak{I}(\mu) = \mathfrak{H}\mathfrak{A}_1$, so Lemma 4.5 completes the proof.

LEMMA 28.2. *Suppose* $\mathfrak{L}$ *is of type* I, *and* $\mathfrak{L} = \mathfrak{X}$ *satisfies Hypothesis* 28.1. *Suppose further that* $\boldsymbol{Z}(\mathfrak{E})$ *contains an element* E *such that* $\boldsymbol{C}_{\mathfrak{H}}(E) \not\subseteqq \mathfrak{H}'$ *and* $\boldsymbol{C}_{\mathfrak{H}}(E) \neq \mathfrak{H}$. *Then the set* $\mathscr{S}$ *of irreducible characters of* $\mathfrak{L}$ *which do not have* $\mathfrak{H}$ *in their kernel is coherent.*

Proof. By Lemmas 28.1 and 4.5, it follows that Hypothesis 11.1 and (11.4) are satisfied if we take $\mathfrak{H}_0 = 1$, $\mathfrak{K} = \mathfrak{L}$, $d = |\mathfrak{E}_0|$ and let $\mathscr{S}$ play the role of $\mathscr{S}$.

Since E is in the center of $\mathfrak{E}$, it follows that $\mathfrak{H}'\boldsymbol{C}_{\mathfrak{H}}(E) \lhd \mathfrak{L}$. Thus, by assumption, $\mathfrak{H}/\mathfrak{H}'$ is not a chief factor of $\mathfrak{L}$. Therefore,

$$|\mathfrak{H}:\mathfrak{H}'| > 4|\mathfrak{E}_0|^2 + 1 . \tag{28.1}$$

Let $\mathscr{S}(\mathfrak{H}') = \{\lambda_{is} \mid s = 1, \cdots, n_i;\ i = 1, \cdots, k\}$, where the notation is chosen so that $\lambda_{is}(1) = \lambda_{jt}(1)$ if and only if $i = j$, and where $\lambda_{11}(1) < \cdots < \lambda_{k1}(1)$. By (28.1) we get that (11.5) holds with $\mathfrak{H}_1 = \mathfrak{H}'$ and by Theorem 11.1 the lemma will follow as soon as it is shown that $\mathscr{S}(\mathfrak{H}')$ is coherent.

Set $e_i = \lambda_{i1}(1)/d$ for $1 \leqq i \leqq k$. Then each e_i is an integer and $1 = e_1 < \cdots < e_k$. By Theorem 10.1, the coherence of $\mathscr{S}(\mathfrak{H}')$ will follow once inequality (10.2) is established. Suppose (10.2) does not hold. Then for some m with $1 < m \leqq k$,

$$\sum_{i=1}^{m-1} e_i^3 n_i \leqq 2e_m . \tag{28.2}$$

Every character in $\mathscr{S}(\mathfrak{H}')$ is a constituent of a character induced by a linear character of $\mathfrak{H}$. Therefore,

$$e_k \leqq |\mathfrak{E}:\mathfrak{E}_0| . \tag{28.3}$$

Let $\bar{\mathfrak{H}} = \mathfrak{H}/\mathfrak{H}'$ and let $\bar{\mathfrak{H}}_1 = \boldsymbol{C}_{\bar{\mathfrak{H}}}(E)$, $\bar{\mathfrak{H}}_2 = [\bar{\mathfrak{H}}, E]$. Thus, $\bar{\mathfrak{H}} = \bar{\mathfrak{H}}_1 \times \bar{\mathfrak{H}}_2$

and $\bar{\mathfrak{H}}_i \neq 1$, $i = 1, 2$. If $\mathfrak{H}_i$ is the inverse image of $\bar{\mathfrak{H}}_i$ in $\mathfrak{H}$, then $\mathfrak{E}\mathfrak{H}_i$ is of Frobenius type and satisfies Hypothesis 28.1. Two applications of Lemma 28.1 imply that $n_1 \geqq 4\,|\,\mathfrak{E} : \mathfrak{E}_0\,|$. Hence, (28.2) does not hold for any m, $1 < m \leqq k$. The proof is complete.

29. Characters of Subgroups of Type III and IV

The following notation will be used.

$\mathfrak{S} = \mathfrak{S}'\mathfrak{Q}^*$ is a subgroup of type II, III, or IV. $\mathfrak{Q}^*$ plays the role of $\mathfrak{W}_1$ in the definition of subgroups of type II, III, and IV given in Section 14. $\mathfrak{H}$, $\mathfrak{U}$, and $\mathfrak{W}_2$ have the same meaning as in these definitions. $\mathfrak{T} = \mathfrak{T}'\mathfrak{W}_2$ is a subgroup of type II, III, IV, or V whose existence follows from Theorem 14.1 (ii) (b), (e).

Let $\pi(\mathfrak{H}) = \{p_1, \cdots, p_t\}$ and for $1 \leqq i \leqq t$, let $\mathfrak{P}_i$ be the S_{p_i}-subgroup of $\mathfrak{H}$. Define

$$\mathfrak{C}_i = \mathfrak{U} \cap C(\mathfrak{P}_i)\,, \qquad 1 \leqq i \leqq t\,,$$

$$\mathfrak{C} = \bigcap_{i=1}^{t} \mathfrak{C}_i\,.$$

Let $|\,\mathfrak{H}\,| = h$, $|\,\mathfrak{U}\,| = u$, $|\,\mathfrak{Q}^*\,| = q$, $|\,\mathfrak{C}_i\,| = c_i$, $1 \leqq i \leqq t$, and $|\,\mathfrak{C}\,| = c$. By definition, q is a prime.

$\mathscr{S}_0$ is the set of characters of $\mathfrak{S}$ which are induced by nonprincipal irreducible characters of $\mathfrak{S}'/\mathfrak{H}$.

$\mathscr{S}$ is the set of characters of $\mathfrak{S}$ which are induced by irreducible characters of $\mathfrak{S}'$ that do not have $\mathfrak{H}$ in their kernel.

The purpose of this section is to prove the following result.

THEOREM 29.1.

(i) *If* $\mathfrak{S}$ *is of type* III *then* $\mathscr{S} \cup \mathscr{S}_0$ *is coherent except possibly if* $|\,\mathfrak{H}\,| = p^q$ *for some prime* p *and* $\mathfrak{C} = 1$.

(ii) *If* $\mathfrak{S}$ *is of type* IV, *then* $\mathscr{S} \cup \mathscr{S}_0$ *is coherent except possibly if* $|\,\mathfrak{H}\,| = p^q$ *for some prime* p, $\mathfrak{C} = \mathfrak{U}'$ *and* $\mathscr{S}_0$ *is not coherent.*

Hypothesis 29.1.

$\mathfrak{S}$ *is a subgroup of type* III *or* IV.

Throughout this section, Hypothesis 29.1 will be assumed. Thus, by Theorem 14.1 (ii) (d), $\mathfrak{T}$ is of type II. Consequently, $\mathfrak{W}_2$ has prime order p. Let $p = p_1$, $\mathfrak{P} = \mathfrak{P}_1$, and $\mathfrak{W}_2 = \mathfrak{P}^*$. Thus, by 3.16 (i), $\mathfrak{U} \subseteq C(\mathfrak{P}_i)$ for $2 \leqq i \leqq t$. Since $\mathfrak{U} \not\subseteq C(\mathfrak{H})$, this yields that $\mathfrak{U} \not\subseteq C(\mathfrak{P})$. As $\mathfrak{U}$ does not act trivially on $\mathfrak{P}/D(\mathfrak{P})$, Lemma 4.6 (i) implies that $C_{\mathfrak{U}}(\mathfrak{P}^*) = \mathfrak{C}_1 \subset \mathfrak{U}$.

For any subgroup $\mathfrak{H}_1$ of $\mathfrak{H}\mathfrak{C}$, let $\mathscr{S}(\mathfrak{H}_1)$ denote the set of characters in $\mathscr{S}_0 \cup \mathscr{S}$ which have the same degree and the same weight as some character in $\mathscr{S}_0 \cup \mathscr{S}$ that has $\mathfrak{H}_1$ in it kernel.

LEMMA 29.1. *Hypothesis* 11.1 *is satisfied if* $\mathscr{S}$ *in that hypothesis is replaced by* $\mathscr{S}_0 \cup \mathscr{S}$, $\mathfrak{H}$ *is replaced by* $\mathfrak{H}\mathfrak{C}$, $\mathfrak{H}_0$ *is taken as* $\langle 1 \rangle$, $\mathfrak{L}$ *is replaced by* $\mathfrak{S}$, $\hat{\mathfrak{L}}$ *and* $\mathfrak{R}$ *are replaced by* $\mathfrak{S}'$, *and* $d = 1$.

Proof. By Theorem 14.2, Condition (i) is satisfied. Condition (ii) follows from the fact that $\mathfrak{S}$ is a three step group. Condition (iii) is immediate and Condition (vi) is simply definition (consistent with the present definition). Since $\mathfrak{U}\mathfrak{Q}^*$ is a Frobenius group, $\mathscr{S}_0$ contains an irreducible character of degree q. Hence, Condition (iv) is satisfied. The group $\mathfrak{S}$ satisfies Hypothesis 13.2. Hence, by Theorem 14.2, Hypothesis 13.3 is satisfied with $\mathfrak{L} = \mathfrak{S}$, $\mathfrak{X} = \mathfrak{G}$, and $\hat{\mathfrak{L}} = \mathfrak{R} = \mathfrak{S}'$, and with $\mathscr{S}$ replaced by $\mathscr{S}_0 \cup \mathscr{S}$. By Lemmas 13.7, 13.9, and 13.10, Condition (v) of Hypothesis 11.1 is satisfied. The proof is complete.

LEMMA 29.2. *If* $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ *is coherent, then* $\mathscr{S}_0 \cup \mathscr{S}$ *is coherent.*

Proof. As $\mathfrak{U} \not\subseteq \boldsymbol{C}(\mathfrak{P})$, $\mathfrak{U}$ does not act trivially on $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$. Since $\mathfrak{U}\mathfrak{Q}^*$ is a Frobenius group, 3.16 (iii) yields that $|\mathfrak{P} : \boldsymbol{D}(\mathfrak{P})| \geqq p^q$. As either $p \geqq 3$ and $q \geqq 5$ or $p \geqq 5$ and $q \geqq 3$, (5.9) yields that

$$\mathfrak{H}\mathfrak{C} : (\mathfrak{H}\mathfrak{C})' | \geqq |\mathfrak{P} : \boldsymbol{D}(\mathfrak{P})| \geqq p^q > 4q^2 + 1 = 4|\mathfrak{S} : \mathfrak{S}'|^2 + 1 .$$

Hence, (11.5) is satisfied with $\mathfrak{H}_1 = (\mathfrak{H}\mathfrak{C})'$. By Lemma 29.1, Theorem 11.1 may be applied. This implies the required result.

LEMMA 29.3. *If* $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ *is not coherent, then* $\mathfrak{S}'' = \mathfrak{H}\mathfrak{C}$.

Proof. Let $b = |\mathfrak{H}\mathfrak{C} : \mathfrak{S}''|$. We have $\mathfrak{P}^* \subseteq \mathfrak{S}''$, as $\mathfrak{P}^* \subseteq \mathfrak{S}'$ and $\mathfrak{Q}^*$ centralizes $\mathfrak{P}^*$. Hence, $\mathfrak{S}/\mathfrak{S}''$ is a Frobenius group. Let $d_1 < \cdots < d_k$ be all the degrees of characters in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ and let $\nu_m = d_m/q$ for $1 \leqq m \leqq k$. Then for each m, ν_m is an integer and $\nu_1 = 1$. Every character of $\mathfrak{S}/\mathfrak{S}''$ is a constituent of a character induced by a linear character of $\mathfrak{H}\mathfrak{C}$. Thus, $\nu_m \leqq u/c$ for $1 \leqq m \leqq k$. There are at least

$$\frac{\left(\frac{u}{c}b - 1\right)}{q}$$

irreducible characters of degree q in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$. Thus, if $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent, inequality (10.2) must be violated for some m. In particular, this implies that

$$\frac{\left(\frac{u}{c}b - 1\right)}{q} \leqq 2\nu_m \leqq 2\frac{u}{c}$$

Therefore, $b - (c/u) \leqq 2q$, so $b < 2q + 1$, since $c < u$. As $\mathfrak{H}\mathfrak{C}/\mathfrak{S}''$ is a normal subgroup of the Frobenius group $\mathfrak{S}/\mathfrak{S}''$, we have $b \equiv 1 \pmod{q}$. Since b and q are both odd, this implies that $b = 1$ as required.

LEMMA 29.4. *If $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent, then $\mathfrak{H} = \mathfrak{P}$, $\mathfrak{P}' = \boldsymbol{D}(\mathfrak{P})$, $|\mathfrak{P} : \mathfrak{P}'| = p^q$, $\mathfrak{P}^* \cap \boldsymbol{D}(\mathfrak{P}) = 1$ and $\mathfrak{C} = \mathfrak{U}'$.*

Proof. By Lemma 29.3, $\mathfrak{S}'' = \mathfrak{H}\mathfrak{C}$. If $2 \leqq i \leqq t$, then $\mathfrak{U}\mathfrak{H} \subsetneqq \mathfrak{P}_i\boldsymbol{C}(\mathfrak{P}_i)$, so that $p_i \mid |\mathfrak{S}' : \mathfrak{S}''|$. Hence, $t = 1$ and $\mathfrak{H} = \mathfrak{P}$. $\mathfrak{C} = \mathfrak{U}'$ follows directly from the fact that $\mathfrak{H}\mathfrak{C} = \mathfrak{S}'' \subsetneqq \mathfrak{H}\mathfrak{U}'$. If $|\mathfrak{P} : \boldsymbol{D}(\mathfrak{P})| > p^q$, then since $\boldsymbol{C}_{\mathfrak{P}}(\mathfrak{Q}^*) = \mathfrak{P}^*$ is cyclic, Lemma 4.6 (i) implies that some non identity element of $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$ is in the center of $\mathfrak{P}\mathfrak{U}/\boldsymbol{D}(\mathfrak{P})$. Thus, p divides $|\mathfrak{U}\mathfrak{H} : \mathfrak{S}''|$ which is not the case. Since $\mathfrak{U}$ does not act trivially on $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$, 3.16 (iii) now implies that $|\mathfrak{P} : \boldsymbol{D}(\mathfrak{P})| = p^q$. Since $\mathfrak{P}^*$ has prime order and lies outside $\boldsymbol{D}(\mathfrak{P})$, we get that $\boldsymbol{D}(\mathfrak{P})\mathfrak{U}\mathfrak{Q}^*$ is a Frobenius group. Hence, by 3.16 (i), $\boldsymbol{D}(\mathfrak{P})\mathfrak{U}$ is nilpotent. Consequently, $\boldsymbol{D}(\mathfrak{P})/\mathfrak{P}'$ is in the center of $\mathfrak{P}\mathfrak{U}/\mathfrak{P}'$. As the fixed points of $\mathfrak{U}$ on $\mathfrak{P}/\mathfrak{P}'$ are a direct factor of $\mathfrak{P}/\mathfrak{P}'$, and since $\mathfrak{U}$ has no fixed points on $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$, we have $\mathfrak{P}' = \boldsymbol{D}(\mathfrak{P})$. The lemma is proved.

LEMMA 29.5. *If $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent then $\mathfrak{P}$ is an elementary abelian p-group of order p^q.*

Proof. In view of Lemma 29.4 it suffices to show that $\mathfrak{P}' = 1$. By 3.16 (i), $\mathfrak{U} \subseteq \boldsymbol{C}(\mathfrak{P}')$. Thus, if $\mathfrak{P}' \neq 1$, there exists a subgroup $\mathfrak{P}_0$ of $\mathfrak{P}'$ such that $\mathfrak{P}_0 \lhd \mathfrak{P}\mathfrak{U}$ and $|\mathfrak{P}' : \mathfrak{P}_0| = p$. If $\mathfrak{U}$ acts irreducibly on $\mathfrak{P}/\mathfrak{P}'$, then $\mathfrak{P}'/\mathfrak{P}_0 = \boldsymbol{Z}(\mathfrak{P}/\mathfrak{P}_0)$. Hence, $\mathfrak{P}/\mathfrak{P}_0$ is an extra special p-group and $|\mathfrak{P} : \mathfrak{P}'| = p^{2b}$ for some integer b contrary to Lemma 29.4.

Suppose that $\mathfrak{U}$ acts reducibly on $\mathfrak{P}/\mathfrak{P}'$. Since the irreducible constituents of this representation are conjugate under the action of $\mathfrak{Q}^*$, all constituents have the same dimension. As $|\mathfrak{P} : \mathfrak{P}'| = p^q$ and q is a prime, this yields that they must all be one dimensional. Therefore, there exist elements $P_1, \cdots, P_q$ in $\mathfrak{P}$ such that

$$\mathfrak{P}/\mathfrak{P}' = \langle P_1\mathfrak{P}'/\mathfrak{P}'\rangle \times \cdots \times \langle P_q\mathfrak{P}'/\mathfrak{P}'\rangle$$

and

$$U^{-1}P_i\mathfrak{P}'U = P_i^{s_i(U)}\mathfrak{P}', \quad U \in \mathfrak{U}, \quad 1 \leqq i \leqq q,$$

where $s_1, \cdots, s_q$ are linear characters of $\mathfrak{U} \pmod{p}$ with $s_{i+1}(U) = s_1(Q^{-i}UQ^i)$ for $U \in \mathfrak{U}$ and a suitably chosen generator Q of $\mathfrak{Q}^*$. Since $|\mathfrak{Q}^*\mathfrak{U}|$ is odd, $s_is_j \neq 1$ for any i, j with $1 \leqq i, j \leqq q$. Hence, if i, j are given, there exists $U \in \mathfrak{U}$ such that $s_i(U)s_j(U) \neq 1$. For $1 \leqq k \leqq q$ let P_k' be an element of $\mathfrak{P}'$ such that

$$U^{-1}P_k\mathfrak{P}_0U = P_k^{s_k(U)}P_k'\mathfrak{P}_0 .$$

Since $\mathfrak{P}'/\mathfrak{P}_0 \subseteq Z(\mathfrak{P}/\mathfrak{P}_0)$, we get that

$$\begin{aligned}[P_i, P_j] &\equiv U^{-1}[P_i, P_j]U \equiv [P_i^{s_i(U)}P_i', P_j^{s_j(U)}P_j'] \\ &\equiv [P_i^{s_i(U)}, P_j^{s_j(U)}] \equiv [P_i, P_j]^{s_i(U)s_j(U)} (\mathrm{mod}\ \mathfrak{P}_0) .\end{aligned}$$

Since $s_i(U)s_j(U) \neq 1$, this yields that $[P_i, P_j] \in \mathfrak{P}_0$ for $1 \leqq i, j \leqq q$. Since $\mathfrak{P} = \langle P_1, \cdots, P_q \rangle$, we get that $\mathfrak{P}' \subseteq \mathfrak{P}_0$ contrary to construction. Thus, $\mathfrak{P}' = 1$ as required.

LEMMA 29.6. *If $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent and $\mathfrak{C} \neq 1$, then $\mathscr{S}_0$ is not coherent.*

Proof. Suppose that $\mathfrak{C} \neq 1$. Assume that $\mathscr{S}_0$ is coherent. Let $\mathscr{S}_1 = \mathscr{S}_0$. Let $\mathscr{S}_2, \cdots, \mathscr{S}_k$ be the equivalence classes of $\mathscr{S}((\mathfrak{H}\mathfrak{C})') - \mathscr{S}_0$ chosen so that every character in $\mathscr{S}_m$ has degree $\nu_m q$ for $2 \leqq m \leqq k$, and $\nu_2 \leqq \cdots \leqq \nu_k$. Suppose $\bigcup_{i=1}^{k} \mathscr{S}_i$ is not coherent. By Hypothesis 11.1, and Lemma 29.1, all parts of Hypothesis 10.1 are satisfied except possibly inequality (10.2). Since $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent, inequality (10.2) must be violated for some m.

Every character in $\bigcup_{i=1}^{k} \mathscr{S}_i$ is a constituent of a character induced by a linear character of $\mathfrak{H}\mathfrak{C}$. Thus $\nu_m \leqq (u/c)$ for $1 < m \leqq k$. Hence, violation of inequality (10.2) yields that

$$\frac{u-1}{q} \leqq 2\nu_m \leqq 2\frac{u}{c} .$$

Since $c \equiv 1 \pmod{2q}$ and $c \neq 1$, this implies that

$$u - 1 \leqq 2q\frac{u}{c} = \frac{(2q+1)}{c}u - \frac{u}{c} \leqq u - \frac{u}{c} < u - 1 .$$

Hence $\bigcup_{i=1}^{k} \mathscr{S}_i$ is coherent. Since $\mathscr{S}((\mathfrak{H}\mathfrak{C})') = \bigcup_{i=1}^{k} \mathscr{S}_i$, the proof is complete.

The proof of Theorem 29.1 is now immediate. Lemmas 29.2, 29.4 and 29.5 imply statement (i). Lemmas 29.2, 29.4, 29.5, and 29.6 imply statement (ii).

30. Characters of Subgroups of Type II, III and IV

The notation introduced at the beginning of Section 29 is used in this section. The main purpose of this section is to prove the following result.

THEOREM 30.1. *Let $\mathfrak{S}$ be a subgroup of type* II, III *or* IV. *Then $\mathcal{S}$ is coherent except possibly if $\mathfrak{S}$ is of type* II, $\mathfrak{H}$ *is a non abelian* 3*-group, $\mathfrak{H}\mathfrak{U}/\mathfrak{C}$ is a Frobenius group with Frobenius kernel $\mathfrak{H}\mathfrak{C}/\mathfrak{C}$, $u < 3^{q/2}$, $|\mathfrak{H}:\mathfrak{H}'| = 3^q$ and $\mathfrak{T}$ is a subgroup of type* V.

All lemmas in this section will be proved under the following assumption.

Hypothesis 30.1.
(i) $\mathfrak{S}$ *is a subgroup of type* II, III, *or* IV.
(ii) $\mathcal{S}$ *is not coherent except possibly if $\mathfrak{S}$ is of type* II.
(iii) $\mathfrak{U}/\mathfrak{U}'$ *has exponent* a.

For any subgroup $\mathfrak{H}_1$ of $\mathfrak{S}'$ let $\mathcal{S}(\mathfrak{H}_1)$ be the set of characters in $\mathcal{S}$ which have $\mathfrak{H}_1$ in their kernel. Notice that this notation differs from that used in Section 29.

LEMMA 30.1. *The degree of every character in $\mathcal{S}$ is divisible by aq.*

Proof. Every character in $\mathcal{S}$ is a constituent of a character of $\mathfrak{S}$ induced by a nonprincipal character of $\mathfrak{H}$. For any character θ of $\mathfrak{H}$ let $\tilde{\theta}$ be the character of $\mathfrak{H}\mathfrak{U}$ induced by θ. Set $\mathfrak{U}_1 = \mathfrak{I}(\theta) \cap \mathfrak{U}$. Let $|\mathfrak{U}:\mathfrak{U}_1| = b$. If $\mathfrak{S}$ is of type II or III, then by Lemma 4.5 it suffices to show that if $\theta \neq 1_{\mathfrak{H}}$, then $a \mid b$.

Let $\mathfrak{K}$ be the kernel of θ and let $H \in \mathfrak{H} - \mathfrak{K}$ such that $H\mathfrak{K} \in \boldsymbol{Z}(\mathfrak{H}/\mathfrak{K})$. Then $\mathfrak{K} \lhd \mathfrak{H}\mathfrak{U}_1$ and $U^{-1}H\mathfrak{K}U = H\mathfrak{K}$ for $U \in \mathfrak{U}_1$. As $(u, h) = 1$, if $U \in \mathfrak{U}_1$, then U centralizes some element in $H\mathfrak{K}$. Hence, $\mathfrak{U}_1 \subseteqq \hat{\mathfrak{S}}$. Let $\mathfrak{U}_0 = \{U^b \mid U \in \mathfrak{U}\}$. Then $\mathfrak{U}_0$ char $\mathfrak{U}$ and $\mathfrak{U}_0 \subseteqq \mathfrak{U}_1 \subseteqq \hat{\mathfrak{S}}$.

Suppose $\mathfrak{U}_0 \neq 1$. If $\mathfrak{S}$ is of type II, then $\hat{\mathfrak{S}}$ is a T.I. set in $\mathfrak{G}$ by Theorem 14.2. Hence, $N(\mathfrak{U}) \subseteqq N(\mathfrak{U}_0) \subseteqq \mathfrak{S}$ contrary to definition. If $\mathfrak{S}$ is of type III, then by Theorem 29.1, $\mathfrak{U}\Omega^*$ is represented irreducibly on $\mathfrak{H}$. Since $\mathfrak{U}_0 \lhd \mathfrak{U}\Omega^*$, $\mathfrak{U}_0$ is in the kernel of this representation. Thus, $\mathfrak{U}_0 \subseteqq \boldsymbol{C}(\mathfrak{H})$ contrary to Theorem 29.1. Thus, $\mathfrak{U}_0 = 1$. Therefore $U^b = 1$ for $U \in \mathfrak{U}$ and so $a \mid b$ in case $\mathfrak{S}$ is of type II or III.

If $\mathfrak{S}$ is of type IV, we will show that Hypothesis 11.1 and (11.2) are satisfied with $\mathfrak{H}_0$ in that hypothesis being taken as our present $\mathfrak{H}$, $\mathfrak{L}$ being taken as $\mathfrak{S}/\mathfrak{H}$, $\mathfrak{H}$ and $\mathfrak{K}$ being taken as $\mathfrak{S}'/\mathfrak{H}$, and $\hat{\mathfrak{L}}_0$ being taken as $\mathfrak{S}'$. Certainly (i) is satisfied. Since $\mathfrak{S}/\mathfrak{H}$ is a Frobenius group with Frobenius kernel $\mathfrak{S}'/\mathfrak{H}$, (ii) and (11.2) are satisfied, and the remaining conditions follow immediately from the fact that $\mathfrak{S}/\mathfrak{H}$ is a

Frobenius group. The present $\mathscr{S}_0$ plays the role of $\mathscr{S}$ in Hypothesis 11.1 (iii).

Notice now that Hypothesis 11.2 is satisfied. By Lemma 11.2 and the fact that $\mathscr{S}_0$ is not coherent it follows that $\mathfrak{S}'/\mathfrak{P}$ is a non abelian r-group for some prime r whose derived group and Frattini subgroup coincide. But $\mathfrak{U} \cong \mathfrak{S}'/\mathfrak{P}$. Since $\mathfrak{C} = \mathfrak{U}'$, $\mathfrak{U}/\mathfrak{C}$ is of exponent r, so $a = r$. As $\mathfrak{U}$ has no fixed points on $\mathfrak{P}^\#$, it follows readily that every non linear character of $\mathfrak{S}'$ has degree divisible by r, as required.

LEMMA 30.2. *For $1 \leqq i \leqq t$, $|\mathfrak{P}_i : \boldsymbol{D}(\mathfrak{P}_i)| = p_i^q$ and $\mathfrak{U}/\mathfrak{C}_i$ has exponent a.*

Proof. If $\mathfrak{S}$ is of type III or IV, the result follows from Theorem 29.1. Suppose $\mathfrak{S}$ is of type II. Then $\hat{\mathfrak{S}}$ is a T.I. set in $\mathfrak{G}$ by Theorem 14.2. Let a_i be the exponent of $\mathfrak{U}/\mathfrak{C}_i$ for $1 \leqq i \leqq t$. Let $\mathfrak{U}_i = \{U^{a_i} \mid U \in \mathfrak{U}\}$. Then $\mathfrak{U}_i \subseteq \mathfrak{C}_i \subseteq \hat{\mathfrak{S}}$ and $\mathfrak{U}_i$ char $\mathfrak{U}$. Thus, if $\mathfrak{U}_i \neq 1$, then $N(\mathfrak{U}) \subseteq N(\mathfrak{U}_i) \subseteq \mathfrak{S}$, contrary to definition of subgroups of type II.

Suppose $|\mathfrak{P}_i : \boldsymbol{D}(\mathfrak{P}_i)| > p_i^q$ for some i with $1 \leqq i \leqq t$. Since $C_{\mathfrak{P}_i}(\mathfrak{Q}^*)$ is cyclic, this implies the existence of a subgroup $\mathfrak{P}_1$ with $\mathfrak{W}_2 \subseteq \mathfrak{P}_1 \subset \mathfrak{P}$ such that $\mathfrak{P}/\mathfrak{P}_1$ is a chief factor of $\mathfrak{S}$. By 3.16 (i), $\mathfrak{P}\mathfrak{U}/\mathfrak{P}_1$ is nilpotent. Thus, $\mathfrak{U} \subseteq \hat{\mathfrak{S}}$ and $N(\mathfrak{U}) \subseteq \mathfrak{S}$, contrary to definition.

LEMMA 30.3. *For $1 \leqq i \leqq t$, either $a \mid (p_i - 1)$ or $a \mid (p_i^q - 1)$ and $(a, p_i - 1) = 1$. In the first case, $\mathfrak{P}_i/\boldsymbol{D}(\mathfrak{P}_i)$ is the direct product of q groups of order p_i, each of which is normalized by $\mathfrak{U}$. In the second case, $\mathfrak{U}/\mathfrak{C}_i$ is cyclic of order a and acts irreducibly on $\mathfrak{P}_i/\boldsymbol{D}(\mathfrak{P}_i)$.*

Proof. By Lemma 30.2, $\mathfrak{U}\mathfrak{Q}^*$ is represented irreducibly on $\mathfrak{P}_i/\boldsymbol{D}(\mathfrak{P}_i)$. As $\mathfrak{U} \lhd \mathfrak{U}\mathfrak{Q}^*$, the restriction of this representation to $\mathfrak{U}$ breaks up into a direct sum of irreducible representations all of which have the same degree d. By Lemma 30.2, $d \mid q$ and so $d = 1$ or $d = q$.

If $d = 1$, the order of every element in $\mathfrak{U}/\mathfrak{C}_i$ divides $(p_i - 1)$. Hence, by Lemma 30.2, $a \mid (p_i - 1)$.

If $d = q$, then $\mathfrak{U}$ acts irreducibly on $\mathfrak{P}_i/\boldsymbol{D}(\mathfrak{P}_i)$. Thus, $\mathfrak{U}/\mathfrak{C}_i$ is cyclic. By Lemma 30.2, $|\mathfrak{U} : \mathfrak{C}_i| = a$. Therefore, $a \mid (p_i^q - 1)$. Let $\mathfrak{U}/\mathfrak{C}_i = \langle U \rangle$. Then the characteristic roots of U are algebraically conjugate over $GF(p)$. Hence, this is also the case for every power of U. If $(a, p_i - 1) \neq 1$, then some power $U_1 \neq 1$ of U has its characteristic roots in $GF(p)$ and thus is a scalar. This violates the fact that $\mathfrak{U}\mathfrak{Q}^*$ is a Frobenius group.

LEMMA 30.4. *Suppose $(a, p_i - 1) = 1$ for some i, $1 \leqq i \leqq t$. Let*

$$\mathfrak{H}_1 = \mathfrak{P}_i' \prod_{j \neq i} \mathfrak{P}_j ,$$

and let $|\mathfrak{P}_i : \mathfrak{P}_i'| = p_i^{m_i'}$. *Then* $m_i' = m_i q$ *for some integer* m_i. *Furthermore,* $\mathscr{S}(\mathfrak{H}_1)$ *contains at least*

$$\frac{1}{q}\left\{\frac{(p_i^{qm_i} - 1)c_i}{a} - (p^{m_i} - 1)\right\}$$

irreducible characters of degree aq *and at least* $(p_i^{m_i} - 1)$ *characters of weight* q *and degree* aq.

Proof. By Lemma 30.3, $\mathfrak{U}/\mathfrak{C}_i$ is cyclic. By Theorem 29.1, $\mathfrak{S}$ is not of type IV, so $\mathfrak{U}$ is abelian. Hence, $\mathfrak{H}\mathfrak{U}/\mathfrak{H}_1\mathfrak{C}_i$ is a Frobenius group. By Lemma 30.2, $|\mathfrak{U} : \mathfrak{C}_i| = a$. Furthermore, since $\mathfrak{U}\mathfrak{Q}^*$ acts irreducibly on $\mathfrak{P}_i/\boldsymbol{D}(\mathfrak{P}_i)$, $\bar{\mathfrak{H}} = \mathfrak{H}/\mathfrak{H}_1$ is the direct product of q cyclic groups of the same order $p_i^{m_i}$. Thus, $qm_i = m_i'$, and $|C_{\bar{\mathfrak{H}}}(\mathfrak{Q}^*)| = p_i^{m_i}$. By 3.16 (iii) every non principal irreducible character of $\mathfrak{H}\mathfrak{C}_i/\mathfrak{H}_1\mathfrak{C}_i$ induces an irreducible character of $\mathfrak{H}\mathfrak{U}/\mathfrak{H}_1\mathfrak{C}_i$ of degree a. Since $\mathfrak{U}$ is abelian, this implies that every irreducible character of $\mathfrak{H}\mathfrak{C}_i/\mathfrak{H}_1$ which does not have $\bar{\mathfrak{H}}$ in its kernel induces an irreducible character of $\mathfrak{H}\mathfrak{U}/\mathfrak{H}_1$ of degree a. Hence, $\mathfrak{H}\mathfrak{U}/\mathfrak{H}_1$ has at least

$$\frac{(p_i^{m_i q} - 1)c_i}{a}$$

distinct irreducible characters of degree a.

Since $\mathfrak{S}/\mathfrak{H}_1$ satisfies Hypothesis 13.2, Lemma 13.7 implies that all but $p^{m_i} - 1$ non principal irreducible characters of $\mathfrak{H}\mathfrak{U}/\mathfrak{H}_1$ induce irreducible characters of $\mathfrak{S}$. The result now follows.

LEMMA 30.5. *Suppose that* $a \mid (p_i - 1)$ *for some* i *with* $1 \leqq i \leqq t$. *Let*

$$\mathfrak{H}_1 = \mathfrak{P}_i' \prod_{j \neq i} \mathfrak{P}_j$$

and let $|\mathfrak{P}_i : \mathfrak{P}_i'| = p_i^{m_i'}$. *Then* $m_i = m_i'/q$ *is an integer and* $\mathscr{S}(\mathfrak{H}_1)$ *contains at least*

$$\frac{(p_i^{m_i} - 1)}{a}\,\frac{u}{au'}$$

irreducible characters of degree aq, *where* $|\mathfrak{U}'| = u'$.

Proof. For any subgroup $\mathfrak{X}$ of $\mathfrak{S}$, let $\bar{\mathfrak{X}} = \mathfrak{X}\mathfrak{H}_1/\mathfrak{H}_1$. By Lemma 30.3, $\bar{\mathfrak{H}}$ contains a cyclic subgroup $\mathfrak{P}_{i1}$ which is normalized by $\mathfrak{U}$ such that

$$|\mathfrak{P}_{i1}| = p_i^{m_i}$$

and such that $\bar{\mathfrak{H}} = \mathfrak{P}_{i1} \times \mathfrak{H}_0$ for some subgroup $\mathfrak{H}_0$ which is normalized by $\mathfrak{U}$. Since $\mathfrak{U}\Omega^*$ acts irreducibly on $\mathfrak{P}_i/D(\mathfrak{P}_i)$, it follows that $m_i = m_i'/q$. Let $\mathfrak{U}_1$ be the kernel of the representation of $\mathfrak{U}$ on $\mathfrak{P}_{i1}$. Then $\mathfrak{U}/\mathfrak{U}_1$ is cyclic and so $|\mathfrak{U} : \mathfrak{U}_1| \leqq a$. There are at least

$$\frac{(p_i^{m_i} - 1)}{u'} |\mathfrak{U}_1|$$

distinct linear characters of $\bar{\mathfrak{H}}\bar{\mathfrak{U}}_1/\mathfrak{H}_0$ which do not have $\mathfrak{P}_{i1}$ in their kernel. Each of these induces an irreducible character of $\bar{\mathfrak{H}}\bar{\mathfrak{U}}$ of degree $|\mathfrak{U} : \mathfrak{U}_1|$. Thus, by Lemma 30.1, $|\mathfrak{U} : \mathfrak{U}_1| = a$ and there are at least

$$\frac{(p_i^{m_i} - 1) \cdot u}{a \cdot a \cdot u'}$$

distinct irreducible characters of $\mathfrak{H}\mathfrak{U}$ of degree a which have $\mathfrak{H}_1$ in their kernel, and as characters of $\bar{\mathfrak{S}}'$ have $\mathfrak{H}_0$ in their kernel. If one of these induced a reducible character of $\mathfrak{S}$ or two of these induced the same character of $\mathfrak{S}$, then Ω^* would normalize $\mathfrak{H}_0$, contrary to the fact that $\mathfrak{U}\Omega^*$ acts irreducibly on $\mathfrak{P}_i/D(\mathfrak{P}_i)$.

LEMMA 30.6. *If $\mathscr{S}$ contains no irreducible character of degree aq, then $t = 1$, $\mathfrak{P}_1' = D(\mathfrak{P}_1)$, $a = u = (p_1^q - 1)/(p_1 - 1)$, and $c = c_1 = 1$. Furthermore, $\mathscr{S}(\mathfrak{H}')$ is coherent.*

Proof. By Lemmas 30.3 and 30.5, $(a, p_i - 1) = 1$ and a divides $(p_i^q - 1)/(p_i - 1)$ for $1 \leqq i \leqq t$. Suppose that for some i,

$$\frac{(p_i^{qm_i} - 1)c_i}{a} - (p_i^{m_i} - 1) \leqq 0 .$$

Then

$$\frac{(p_i^{qm_i} - 1)}{(p_i^{m_i} - 1)} c_i \leqq a .$$

Therefore, $c_i = 1$, $m_i = 1$, and $a = (p_i^q - 1)/(p_i - 1)$. Thus,

$$\frac{(p_i^{qm_i} - 1)c_i}{a} - (p_i^{m_i} - 1) = 0 . \tag{30.1}$$

Now Lemma 30.4 implies that (30.1) holds for $1 \leqq i \leqq t$. Thus, $t = 1$. Hence, $c = c_1 = 1$, $u = a = (p^q - 1)/(p - 1)$, $p = p_1$. Also, $m_1 = 1$, and

so $\mathfrak{P}_1' = D(\mathfrak{P}_1)$.

If a character θ in $\mathscr{S} \cup \mathscr{S}_0$ is equivalent to a character in $\mathscr{S}(\mathfrak{H}')$, then its degree is prime to $|\mathfrak{H}|$, so $\mathfrak{H}' \subseteq \ker \theta$. Thus, the equivalence relation in Hypothesis 11.1 has the property that the present set $\mathscr{S}(\mathfrak{H}')$ is a union of equivalence classes. Therefore, $\mathscr{S}(\mathfrak{H}')$ consists of $(p-1)$ reducible characters of degree aq. Theorem 14.2 implies that Hypothesis 13.3 is satisfied. Hence, Lemma 13.9 implies that $\mathscr{S}(\mathfrak{H}')$ is coherent.

The remaining lemmas in this section will be proved under the following stronger assumption.

Hypothesis 30.2.
(i) *Hypothesis* 30.1 *is satisfied.*
(ii) $\mathscr{S}$ *is not coherent.*

LEMMA 30.7. *If* $\mathscr{S}(\mathfrak{H}')$ *is not coherent, then* $\mathfrak{H} = \mathfrak{P}_1$, $\mathfrak{C}_1 = 1$, $a = (p-1)/2$, $p = p_1$, $u \neq a$, *and* $D(\mathfrak{P}_1) = \mathfrak{P}_1'$. *The degree of every character in* $\mathscr{S}(\mathfrak{H}')$ *is either* aq *or* uq, *and* $\mathscr{S}(\mathfrak{H}')$ *contains exactly* $2u/a$ *irreducible characters of degree* aq.

Proof. Let $d_1 < \cdots < d_k$ be all the degrees of characters in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$. Define $\nu_i = d_i/aq$ for $1 \leqq i \leqq k$. By Lemmas 13.10, 30.1 and 30.6, all the assumptions of Theorem 10.1 are satisfied except possibly inequality (10.2). Every character in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is a constituent of a character of $\mathfrak{S}$ which is induced by a linear character of $\mathfrak{H}\mathfrak{C}$. Hence, $d_k \leqq qu/c$, and so $\nu_k \leqq u/ac$.

Choose the notation so that $a \mid (p_i - 1)$ for $1 \leqq i \leqq t_0$ and $(a, p_i - 1) = 1$ for $t_0 + 1 \leqq i \leqq t$. If $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is not coherent then inequality (10.2) is violated. Lemmas 30.2 and 30.3 imply that for $t_0 + 1 \leqq i \leqq t$, $c_i = u/a$. Thus by Lemmas 30.4 and 30.5, there exists m with $1 < m \leqq k$, such that

$$\sum_{i=1}^{t_0} \frac{u}{a} \cdot \frac{(p_i^{m_i} - 1)}{au'} + \sum_{i=t_0+1}^{t} \left\{ \frac{u}{a} \cdot \frac{(p_i^{q_{m_i}} - 1)}{qa} - \frac{(p_i^{m_i} - 1)}{q} \right\} + \sum_{i=t_0+1}^{t} \frac{(p_i^{m_i} - 1)}{q} \leqq 2\nu_m \leqq \frac{2u}{ca}.$$

Therefore,

$$\sum_{i=1}^{t_0} \frac{(p_i^{m_i} - 1)}{au'} + \sum_{i=t_0+1}^{t} \frac{(p_i^{q_{m_i}} - 1)}{qa} \leqq 2\nu_m \frac{a}{u} \leqq \frac{2}{c} \leqq 2. \tag{30.2}$$

For

$$1 \leqq i \leqq t_0, \ \frac{(p_i^{m_i} - 1)}{a} \geqq 2p^{(m_i - 1)} .$$

By Theorem 29.1, $c \geqq u'$. Thus, (30.2) implies that

(30.3) $\qquad t_0 \leqq 1.$ If $t_0 = 1$, then $m_1 = 1$, $t = 1$.

Assume first that $t_0 = 0$. If $t = 1$, then since $q < p_1^q$ and $a \leqq (p_1^q - 1)/(p_1 - 1)$, (30.2) yields $m_1 = 1$. Thus, every character in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ has degree aq. Therefore the definition of subcoherence implies directly that $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is coherent contrary to assumption. Suppose now that $t \geqq 2$. Then (30.2) yields that $(p_1 - 1) + (p_2 - 1) \leqq 2q$. Therefore,

(30.4) $\qquad p_i \not\equiv 1 \pmod{q}, \quad i = 1, 2 .$

Further, (30.2) also implies that

(30.5) $$\frac{1}{a}\frac{(p_1^q - 1)}{(p_1 - 1)} + \frac{1}{a}\frac{(p_2^q - 1)}{(p_2 - 1)} \leqq q .$$

It follows from (30.4) that

(30.6) $$\frac{1}{a}\frac{(p_1^q - 1)}{(p_1 - 1)} \equiv \frac{1}{a} \equiv \frac{1}{a}\frac{(p_2^q - 1)}{(p_2 - 1)} \pmod{q} .$$

Each term on the left of (30.5) is an integer. Hence, if $p_1 > p_2$, (30.6) yields that

$$\frac{1}{a}\frac{(p_1^q - 1)}{(p_1 - 1)} \geqq q + \frac{1}{a}\frac{(p_2^q - 1)}{(p_2 - 1)} ,$$

contrary to (30.5). Consequently, $t_0 \neq 0$.

Now (30.2) and (30.3) imply that $t = 1$, so that $\mathfrak{H} = \mathfrak{P}_1$. We also conclude that $m_1 = 1$, so that $D(\mathfrak{P}_1) = \mathfrak{P}_1'$. Furthermore, $c = c_1 = u'$, and $(p_1 - 1)/a \leqq 2$. Since ap_1 is odd, we have $p_1 - 1 = 2a$. Finally we get that $\nu_m = u/ac$ and so $m = k$. If $k = m > 2$, or if $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ contains more than $2u/a$ irreducible characters of degree qa, then (30.2) is replaced by a strict inequality which is impossible as $(p_1 - 1)/a = 2$. Thus, $k = m = 2$, and so $d_2 = uq/c$ and the degree of a character in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is either aq or uq/c. If $\mathfrak{S}$ is of type II or III, then $(\mathfrak{H}\mathfrak{C})' = \mathfrak{H}'$ and the result is proved.

Suppose that $\mathfrak{S}$ is of type IV. Since the degree of any character in $\mathscr{S}((\mathfrak{H}\mathfrak{C})')$ is either aq or uq/c, $\mathfrak{U}/\mathfrak{C}$ is generated by two elements. Since $\mathfrak{C} = \mathfrak{U}'$, $\mathfrak{U}$ is generated by two elements. Thus, if we set $\mathfrak{H}_0 = \mathfrak{H}$, replace $\mathfrak{H}$ and $\mathfrak{N}$ by $\mathfrak{S}'/\mathfrak{H}$, and replace $\mathfrak{L}$ by $\mathfrak{S}$ in Hypothesis 11.2, then by Lemma 29.1, Hypothesis 11.2 holds and by Lemma 11.3 and Theorem 29.1, we conclude that $\mathscr{S} = \mathscr{S}(\mathfrak{H}')$ is coherent, contrary to

assumption.

LEMMA 30.8. *$\mathscr{S}(\mathfrak{P}')$ is coherent.*

Proof. By Lemma 30.7, it may be assumed that $\mathfrak{P} = \mathfrak{P}$ is a p-group for some prime p, that $D(\mathfrak{P}) = \mathfrak{P}'$, and that $\mathfrak{C} = 1$. Suppose that $\mathscr{S}(\mathfrak{P}')$ is not coherent. Let $\mathscr{S}_1$ be the set of irreducible characters in $\mathscr{S}(\mathfrak{P}')$ of degree aq. Then by Lemma 30.7

$$|\mathscr{S}_1| = \frac{2u}{a}, \qquad a = \frac{(p-1)}{2}. \tag{30.7}$$

Let $\mathscr{S}_2$ be the set of irreducible characters in $\mathscr{S}(\mathfrak{P}')$ of degree uq. The group $\mathfrak{S}/\mathfrak{P}'$ satisfies Hypothesis 13.2. Hence, by Lemmas 13.5, 13.7 and 30.7, there are $(p-1)$ reducible characters in $\mathscr{S}$ of weight q and degree uq which have $\mathfrak{P}'$ in their kernel. As the sum of the squares of degrees of irreducible characters of $\mathfrak{S}/\mathfrak{P}'$ is $p^q uq$, we get that

$$uq + |\mathscr{S}_1| q^2a^2 + (p-1)qu^2 + |\mathscr{S}_2| q^2u^2 = p^q uq . \tag{30.8}$$

Since $\mathfrak{U}$ is abelian and is generated by two elements, we also have

$$u \leqq a^2 . \tag{30.9}$$

Now (30.7), (30.8) and (30.9) yield that

$$\begin{aligned} |\mathscr{S}_2| &\geqq \frac{p^q - (p-1)u - 2qa - 1}{uq} \\ &\geqq \frac{1}{a^2q}\left\{(p^q - 1) - (p-1)q - \frac{(p-1)^3}{4}\right\}. \end{aligned} \tag{30.10}$$

Hence, by (5.8), $\mathscr{S}_2$ is non empty.

Let $\mathscr{S}_i = \{\lambda_{is} \mid 1 \leqq s \leqq n_i\}$ for $i = 1, 2$. The character λ_{11} is induced by a linear character of some subgroup $\mathfrak{S}_0$ of index a in $\mathfrak{S}'$. Define

$$\alpha = (\tilde{1}_{\mathfrak{S}_0} - \lambda_{11}), \tag{30.11}$$

where $\tilde{1}_{\mathfrak{S}_0}$ is the character of $\mathfrak{S}$ induced by $1_{\mathfrak{S}_0}$. Since $\mathfrak{S}_0 \lhd \mathfrak{S}'$, it follows that $1_{\mathfrak{S}_0}$ induces $\rho_{\mathfrak{S}'/\mathfrak{S}_0}$ on $\mathfrak{S}'$. Since Ω^* does not normalize $\mathfrak{S}_0$, (30.11) is seen to imply that

$$\|\alpha\|^2 = a + 1 + (q-1)\frac{a^2}{u} .$$

Since $\hat{\mathfrak{S}}$ is tamely imbedded in $\mathfrak{G}$ and α vanishes on $\mathfrak{S} - \hat{\mathfrak{S}}$, we get that

$$\|\alpha^r\|^2 = \|\alpha\|^2 = a + 1 + (q-1)\frac{a^2}{u}. \tag{30.12}$$

Furthermore,

$$(\alpha^r, \lambda_{2i}^r - \lambda_{2j}^r) = (\alpha, \lambda_{2i} - \lambda_{2j}) = 0$$

for all values of i and j.

Suppose that $(\alpha^r, \lambda_{2i}) \neq 0$ for some i. Then $(\alpha^r, \lambda_{2i}^r) \neq 0$ for all i. Hence (30.10) and (30.12) imply that

$$\frac{p^q-1}{qa^2} - \frac{(p-1)}{a^2} - \frac{(p-1)}{q} \leqq a + 1 + (q-1)\frac{a^2}{u}$$
$$= \frac{p-1}{2} + 1 + (q-1)\frac{a^2}{u}.$$

Thus

$$2\{1 + \cdots + p^{q-1}\} = \frac{p^q-1}{a} \tag{30.13}$$
$$\leqq q\frac{(p-1)}{2}\left\{\frac{2}{a} + \frac{p^q-1}{q} + \frac{p-1}{2} + 1 + (q-1)\frac{a^2}{u}\right\}$$
$$\leqq q\frac{(p-1)}{2}\left(p + q\frac{a^2}{u}\right)$$
$$< q\frac{(p-1)}{2}\left(p + q\frac{p}{2}\right).$$

Therefore

$$4p^{q-2} < 4\frac{p^{q-1}-1}{p-1} < pq\left(1 + \frac{q}{2}\right).$$

Hence

$$3^{q-2} < 4p^{q-3} < q\left(1 + \frac{q}{2}\right) < q^2.$$

Thus $q = 3$ by (5.1). Now (30.13) becomes

$$2(1 + p + p^2) \leqq \frac{3}{2}(p-1)\left\{\frac{4}{p-1} + \frac{5}{6}(p-1) + 1 + \frac{2a^2}{u}\right\}.$$

Thus

$$\frac{4}{3}(1 + p + p^2) \leqq 4 + p - 1 + \frac{5}{6}(p-1)^2 + \frac{2a^2}{u}(p-1).$$

This implies that

$$\frac{4}{3}p^2 \leqq p + \frac{5}{6}p^2 + \frac{2a^2}{u}p.$$

Therefore $(1/2)p^2 \leqq p(1 + (2a^2/u))$, or equivalently $(1/2)p \leqq 1 + (2a^2/u)$. Thus (30.7) yields that

$$u \leqq \frac{2a^2}{\frac{1}{2}p - 1} = \frac{4a^2}{p-2} \leqq \frac{(p-1)^2}{(p-2)} < p + 1 < 3a.$$

This is impossible since $a \mid u$, $a \neq u$ and both a and u are odd. Thus,

$$(\alpha^\tau, \lambda_{2i}^\tau) = 0 \quad \text{for} \quad \lambda_{2i} \in \mathscr{S}_2 . \tag{30.14}$$

Define $\beta = (u/a)\lambda_{11} - \lambda_{21} \in \mathscr{S}_0(\mathscr{S})$. Suppose that $(\beta^\tau, \lambda_{11}^\tau) = (u/a) - b$. As τ is an isometry on $\mathscr{S}_0(\mathscr{S})$, this yields that

$$(\beta^\tau, \lambda_{1i}^\tau) = \frac{u}{a}\delta_{i1} - b \quad \text{for all } i .$$

Therefore,

$$\beta^\tau = \left(\frac{u}{a} - b\right)\lambda_{11}^\tau - b\sum_{i\neq 1}\lambda_{1i}^\tau + \Gamma + \Delta , \tag{30.15}$$

where Γ is a linear combination of elements in $\mathscr{S}_2{}^\tau$ and Δ is orthogonal to $\mathscr{S}_1{}^\tau \cup \mathscr{S}_2{}^\tau$. Since $(\beta^\tau, \lambda_{21}^\tau - \overline{\lambda}_{21}^\tau) \neq 0$, it follows that $\| \Gamma \|^2 \geqq 1$. Since

$$\| \beta^\tau \|^2 = \| \beta \|^2 = \left(\frac{u}{a}\right)^2 + 1 , \tag{30.16}$$

(30.7) and (30.16) yield

$$\| \Delta \|^2 + \left(\frac{u}{a} - b\right)^2 + \left(2\frac{u}{a} - 1\right)b^2 \leqq \left(\frac{u}{a}\right)^2 .$$

This implies that

$$\| \Delta \|^2 + 2\frac{u}{a}b^2 - 2\frac{u}{a}b \leqq 0 ,$$

or $b^2 \leqq b$. Since b is an integer, $b = 0$ or 1 and $\Delta = 0$.

Suppose $b = 1$. Then (30.15) becomes

$$\beta^\tau = \left(\frac{u}{a} - 1\right)\lambda_{11}^\tau - \sum_{i\neq 1}\lambda_{1i}^\tau + \Gamma . \tag{30.17}$$

As α, β vanish on $\mathfrak{S} - \hat{\mathfrak{S}}$, we have

$$(\alpha^\tau, \beta^\tau) = (\alpha, \beta) = -\frac{u}{a} . \tag{30.18}$$

Since $(\alpha^\tau, \lambda_{11}^\tau - \lambda_{1i}^\tau) = -1$, we get that

$$\alpha^r = (x-1)\lambda_{11}^r + x\sum_{i\neq 1}\lambda_{1i}^r + \Delta_0\,, \tag{30.19}$$

for some integer x and some Δ_0 which is orthogonal to $\mathscr{S}_1$. Now (30.14), (30.17), (30.18) and (30.19) yield that

$$-\frac{u}{a} = \left(\frac{u}{a}-1\right)(x-1) - x\left(2\frac{u}{a}-1\right).$$

Reading this equality mod u/a, we get

$$0 \equiv -(x-1) + x \equiv 1 \left(\operatorname{mod}\frac{u}{a}\right).$$

Thus $u = a$, contrary to Lemma 30.7. Hence, $b = 0$. Consequently $\beta^r = (u/a)\lambda_{11}^r + \Gamma$, and so $\Gamma = \pm\lambda_{2j}^r$ for some j. Since $(\beta^r, \lambda_{21}^r - \bar{\lambda}_{21}^r) \neq 0$, $\lambda_{2j} = \lambda_{21}$ or $\bar{\lambda}_{21}$. This implies directly that $\mathscr{S}_1 \cup \mathscr{S}_2$ is coherent. Lemma 13.10 and Theorem 10.1 now yield that $\mathscr{S}(\mathfrak{P}')$ is coherent. The proof is complete.

LEMMA 30.9. *$\mathfrak{S}$ is of type* II.

Proof. If $\mathfrak{S}$ is of type III or IV, then Theorem 29.1 yields that $\mathfrak{P}' = 1$. Thus, by Lemma 30.8, $\mathscr{S}$ is coherent. Hence, Hypothesis 30.2 implies that $\mathfrak{S}$ is of type II.

LEMMA 30.10. *If $\mathscr{S}$ contains an irreducible character of degree aq, then Hypothesis* 11.1 *is satisfied with $\mathfrak{P}_0 = 1$, $\mathfrak{L} = \mathfrak{S}$, $\hat{\mathfrak{L}} = \hat{\mathfrak{S}}$, $\mathfrak{R} = \mathfrak{S}'$ and $d = a$.*

Proof. By Theorem 14.2, Condition (i) is satisfied. Condition (ii) follows from the definition of three step group. Conditions (iii) and (vi) are immediate, while Condition (iv) holds by assumption. The group $\mathfrak{S}$ satisfies Hypothesis 13.2. Hence, by Theorem 14.2 Hypothesis 13.3 is satisfied with $\mathfrak{X} = \mathfrak{G}$, $\mathfrak{L} = \mathfrak{S}$, $\hat{\mathfrak{L}} = \hat{\mathfrak{S}}$ and $\mathfrak{R} = \mathfrak{S}'$. By Lemmas 13.7, 13.9 and 13.10, Hypothesis 10.1 is satisfied. Thus, Lemma 10.1 yields that Condition (v) of Hypothesis 11.1 is satisfied. The proof is complete.

LEMMA 30.11. *If $\mathscr{S}$ contains an irreducible character of degree aq, then*

$$|\mathfrak{P} : \mathfrak{P}'| \leqq 4a^2q^2 + 1\,.$$

Proof. By Hypothesis 30.2, $\mathscr{S}$ is not coherent. Thus, Lemmas 30.8, 30.9, and 30.10, together with Theorem 11.1 yield the result.

LEMMA 30.12. *For* $1 \leqq i \leqq t$, $(a, p_i - 1) = 1$ *and* $\mathfrak{P}_i\mathfrak{U}/\mathfrak{C}_i$ *is a Frobenius group.*

Proof. Suppose that $a \mid (p_i - 1)$ for some i. Then Lemmas 30.2 and 30.11 yield that $p_i^q \leqq 4a^2q^2 + 1 \leqq (p_i - 1)^2q^2 + 1$. Thus, $p_i^{q-2} < q^2$. Therefore, (5.1) implies that $q = 3$. Hence, $p_i = 5$ or 7. Thus, a divides 4 or 6. As a is odd and $(a, q) = 1$, this implies that $a = 1$ which is not the case. Therefore, by Lemma 30.3, $\mathfrak{U}/\mathfrak{C}_i$ is cyclic of order a for $1 \leqq i \leqq t$. If $\mathfrak{P}_i\mathfrak{U}/\mathfrak{C}_i$ were not a Frobenius group, then for some $b < a$, $\{U^b \mid U \in \mathfrak{U}\} = \mathfrak{U}_0$ would lie in $\hat{\mathfrak{S}}$. Since $\mathfrak{U}_0 \neq 1$ and $\mathfrak{U}_0$ char $\mathfrak{U}$, this implies that $N(\mathfrak{U}) \subseteqq N(\mathfrak{U}_0) \subseteqq \mathfrak{S}$, contrary to Lemma 30.9.

LEMMA 30.13. $t = 1$, $p_1 = 3$, $a < 3^{q/2}$ *and* $\mathfrak{P}_1' = D(\mathfrak{P}_1)$.

Proof. By Lemma 30.8, $\mathfrak{P}' \neq 1$. Choose the notation so that $\mathfrak{P}_1' \neq 1$. Let $\mathfrak{P}_1 = \mathfrak{P}_{11} \supset \mathfrak{P}_{12} \cdots \supset \mathfrak{P}_{1n} = \mathfrak{P}_1' \supset \mathfrak{P}_{1,n+1}$, where $\mathfrak{P}_{1i}/\mathfrak{P}_{1,i+1}$ is a chief factor of $\mathfrak{S}$ for $1 \leqq i \leqq n$. Thus, $\mathfrak{P}_1/\mathfrak{P}_{1,n+1}$ is of class two and so is a regular p-group. By Lemma 4.6 (i) $\mathfrak{Q}^*$ centralizes an element of $\mathfrak{P}_{1i} - \mathfrak{P}_{1,i+1}$ for $1 \leqq i \leqq n$. Since $C_{\mathfrak{P}_1}(\mathfrak{Q}^*)$ is cyclic, this implies that $\mathfrak{P}_1/\mathfrak{P}_{1,n+1}$ has exponent p^n. Let $\mathfrak{U}/\mathfrak{C}_i = \langle U \rangle$. Then the regularity of $\mathfrak{P}_1/\mathfrak{P}_{1,n+1}$ yields that U has the same minimal polynomial on $\mathfrak{P}_1/D(\mathfrak{P}_1)$ as on $\mathfrak{P}_1'/\mathfrak{P}_{1,n+1}$. Hence, by Lemma 6.2, $a < 3^{q/2}$. Now Lemma 30.11 implies that if $|\,\mathfrak{P}_1 : \mathfrak{P}_1'\,| = p_1^{mq}$, then

$$p_1^{mq} \prod_{i=2}^{t} p_i^q \leqq 4.3^q q^2 + 1 . \tag{30.20}$$

Since $3 \leqq p_1$, (30.20) implies that

$$p_1^{(m-1)q} \prod_{i=2}^{t} p_i^q \leqq 4q^2 + 1 .$$

Hence, by (5.9), $m = 1$ and $t = 1$. Thus, (30.20) becomes

$$p_1^q \leqq 4.3^q q^2 + 1 . \tag{30.21}$$

If $p_1 \geqq 11$, (30.21) implies that

$$3^q < \left(\frac{p_1}{3}\right)^q \leqq 4q^2 + 1 .$$

Thus, $3^{q-2} < q^2$ and so $q < 5$ by (5.1). Hence $q = 3$ and (30.21) yields $1331 = 11^3 < 4.3^5 + 1 < 1000$, which is not the case. If $p_1 = 7$, then (30.21) and (5.6) imply that $q < 7$. Thus, $q = 5$ or $q = 3$. If $q = 3$, then

$$\frac{p_1^q - 1}{p_1 - 1} = 57$$

and $a < 3^{q/2} < 9$. Since $(q, a) = 1$ and $a \mid 57$, this cannot be the case. If $q = 5$, then

$$\frac{p_1^q - 1}{p_1 - 1} = 2801$$

is a prime. Thus $2801 = a < 3^{q/2} < 27$. Suppose now that $p_1 = 5$. Then by (5.7), $q < 13$. Thus, $q = 3, 7$, or 11. Let r be a prime factor of a. Then $r < 3^{q/2}$ and $5^q \equiv 1 \pmod{r}$. Thus, $r \equiv 1 \pmod{2q}$. If $q = 3$, then $r \equiv 1 \pmod 6$ and $r < 3^{3/2}$, which is impossible. If $q = 7$, then $r < 3^{7/2} < 50$ and $r \equiv 1 \pmod{14}$. Thus $r = 29$ or 43. Since $5^7 \equiv -1 \pmod{29}$ and $5^7 \equiv -6 \pmod{43}$, these cases cannot occur. If $q = 11$, then $r < 3^{11/2} < 437$ and $r \equiv 1 \pmod{22}$. Thus, $r = 23, 67, 89, 199, 331, 353, 397$, or 419. Since $5^{11} \equiv 1 \pmod r$, the quadratic reciprocity theorem implies that $(r \mid 5) = 1$, so that $r \equiv \pm 1 \pmod 5$. Thus, $r = 89, 199, 331$ or 419. Since $5^{11} \equiv 55 \pmod{89}$, $5^{11} \equiv 92 \pmod{199}$, $5^{11} \equiv -2 \pmod{331}$, $5^{11} \equiv -40 \pmod{419}$, these cases cannot occur. Hence, $p_1 = 3$, and the lemma is proved.

If $\mathscr{S}$ is not coherent, then Lemmas 30.8 and 30.12 imply that $|\mathfrak{W}_2|$ is not a prime. Hence, $\mathfrak{T}$ is of Type V. The other statements in Theorem 30.1 follow directly from Lemmas 30.9 and 30.13.

31. Characters of Subgroups of Type V

In this section $\mathfrak{T} = \mathfrak{T}'\mathfrak{W}_2$ is a subgroup of type V. Let $\mathfrak{S}$ be the subgroup of $\mathfrak{G}$ which satisfies condition (ii) of Theorem 14.1. By Theorem 14.1 (ii) (d) $\mathfrak{S}$ is of type II. The notation introduced at the beginning of Section 29 will be used.

$\mathscr{T}$ is the set of all characters of $\mathfrak{T}$ which are induced by non principal irreducible characters of $\mathfrak{T}'$. For any class function α of $\mathfrak{T}'$ let $\tilde{\alpha}$ be the class function of $\mathfrak{T}$ induced by α.

For $0 \leqq i \leqq q-1$, $0 \leqq j \leqq w_2 - 1$ let η_{ij} be the generalized characters of $\mathfrak{G}$ defined by Lemma 13.1 and let ν_{ij} be the characters of $\mathfrak{T}$ defined by Lemma 13.3.

Hypothesis 13.2 is satisfied with $\mathfrak{L} = \mathfrak{T}$, $\mathfrak{N} = \mathfrak{T}'$ and $\mathfrak{W}_1$ replaced by $\mathfrak{W}_2$. By Lemma 13.7 $\mathfrak{T}'$ has exactly q irreducible characters which induce reducible characters of $\mathfrak{T}$. Denote these by ν_i for $0 \leqq i \leqq q-1$, where $\nu_0 = 1_{\mathfrak{T}'}$. Let $\zeta_i = \tilde{\nu}_i$ for $0 \leqq i \leqq q-1$. Since q is a prime the characters ν_i are algebraically conjugate for $1 \leqq i \leqq q-1$. Therefore

$$\nu_i(1) = \nu_1(1) \quad \text{for } 1 \leqq i \leqq q-1 .$$

LEMMA 31.1. *$\mathscr{S}(\mathfrak{P}')$ contains an irreducible character of $\mathfrak{S}$ except possibly if w_2 is a prime and $\mathfrak{P}\mathfrak{U}$ is a Frobenius group.*

Proof. If $\mathfrak{S}'$ is not a Frobenius group then there are strictly more than w_2 classes of $\mathfrak{S}'/\mathfrak{P}'$ whose order is not relatively prime to $|\mathfrak{P}|$. The result now follows from Lemma 13.7.

Suppose that $\mathfrak{S}'$ is a Frobenius group. By Lemma 6.2 and 3.16 (iii) $\mathfrak{P}$ is abelian and $|\mathfrak{P}| = w_2^q$ if the result is false. Then Lemma 13.7 implies that $\mathfrak{S}'$ contains exactly $w_2 - 1$ conjugate classes which are in $\mathfrak{P}^\sharp$. Therefore

$$\frac{|\mathfrak{P}| - 1}{u} = w_2 - 1 .$$

Hence

$$u = \frac{|\mathfrak{P}| - 1}{w_2 - 1} = \frac{|\mathfrak{P}| - 1}{|\mathfrak{P}|^{1/q} - 1} > \sqrt{|\mathfrak{P}|} .$$

This implies that $\mathfrak{P}$ is an elementary abelian p-group for some prime p. Since $\mathfrak{W}_2$ is cyclic w_2 is a prime as required.

LEMMA 31.2. *Let*

$$a_{ij} = ((\nu_1(1)\tilde{1}_{\mathfrak{T}'} - \zeta_i)^r, \eta_{0j}) .$$

Then $a_{ij} \neq 0$ for $1 \leqq i \leqq q-1$, $0 \leqq j \leqq w_2 - 1$.

Proof. Lemma 10.3 implies that by Lemma 9.4

$$(\nu_1(1)\tilde{1}_{\mathfrak{T}'} - \zeta_i, \eta_{0j|\mathfrak{T}}) = ((\nu_1(1)\tilde{1}_{\mathfrak{T}'} - \zeta_i)^r, \eta_{0j}) = a_{ij} . \tag{31.1}$$

Since η_{01} is rational on $\mathfrak{T}'$ by Lemma 13.1, $a_{ij} = a_j$ is independent of i. Thus (31.1) implies that

$$\eta_{0j|\mathfrak{T}'} = b\rho_{\mathfrak{T}'} - a_j \sum_{i=1}^{q-1} \nu_{i0|\mathfrak{T}'} + \alpha_{|\mathfrak{T}'} , \tag{31.2}$$

for some integer b, where α is an integral linear combination of irreducible characters of $\mathfrak{T}$ each of which vanishes on $\hat{\mathfrak{W}}$.

Let $Q \in \mathfrak{Q}^{*\sharp}$. Let p be a prime dividing w_2, let P be an element of order p in $\mathfrak{W}_2$ and let $\mathfrak{p}$ be a prime divisor of p in the ring of integers of $\mathscr{O}_{|\mathfrak{G}|}$. Let ω_{ij} have the same meaning as in Hypothesis 13.1. Thus by Lemmas 13.1 and 13.3

$$\eta_{0j}(PQ) = \omega_{0j}(PQ) , \quad \alpha(PQ) = 0 , \quad \nu_{i0}(PQ) = \varepsilon\omega_{i0}(PQ) , \tag{31.3}$$

where $\varepsilon = \pm 1$ is independent of i. Therefore

$$\sum_{i=1}^{q-1} \nu_{i0}(PQ) = \varepsilon \sum_{i=1}^{q-1} \omega_{i0}(PQ) = \varepsilon \sum_{i=1}^{q-1} \omega_{i0}(Q) = -\varepsilon \,. \tag{31.4}$$

In view of Lemma 4.2 (31.3) and (31.4) imply that

$$\begin{aligned} &\eta_{0j}(Q) \equiv \eta_{0j}(PQ) \equiv \omega_{0j}(PQ) \equiv \omega_{0j}(Q) \equiv 1 \pmod{\mathfrak{p}} \\ &\sum_{i=1}^{q-1} \nu_{i0}(Q) \equiv -\varepsilon \pmod{\mathfrak{p}} \\ &\alpha(Q) \equiv \alpha(PQ) \equiv 0 \pmod{\mathfrak{p}} \,. \end{aligned} \tag{31.5}$$

Thus (31.2) and (31.5) yield that $1 \equiv \varepsilon a_j \pmod{\mathfrak{p}}$. Thus $a_j \neq 0$ as required.

The main purpose of this section is to prove that $\mathscr{T}$ is coherent. Theorem 12.1 will play an important role in the proof of this fact. The lemmas in this section will from now on satisfy the following assumption.

Hypothesis 31.1.
$\mathscr{T}$ is not coherent.

By Grün's theorem $\mathfrak{T}/\mathfrak{T}''$ is a Frobenius group. Hence by Lemma 11.2 $\mathfrak{T}' = \mathfrak{Q}$ is a q-group. Define

$$|\mathfrak{Q} : \mathfrak{Q}'| = q^b \,, \qquad |\mathfrak{T} : \mathfrak{Q}| = w_2 = e \,. \tag{31.6}$$

Let $1 = q^{f_0} < q^{f_1} < \cdots$ be all the integers which are degrees of irreducible characters of $\mathfrak{Q}$. Let

$$\nu_1(1) = q^{f_n} \,, \qquad n > 0 \,. \tag{31.7}$$

By Lemma 13.10 Hypothesis 12.1 is satisfied. Let $\mathscr{T}_s$ be defined by (12.3) for $0 \leqq s \leqq t$.

LEMMA 31.3. *Suppose that $b = 2c$ for some integer c. Then e is not a prime power.*

Proof. Suppose that $e = p^h$ for some prime p. Then by Lemma 11.5 $q^c + 1 = 2p^h$, $f_1 = c$ and $\mathfrak{Q}$ contains a subgroup $\mathfrak{Q}_1$ which is normal in $\mathfrak{T}$ and satisfies $|\mathfrak{Q}' : \mathfrak{Q}_1| = q$ and $\mathfrak{Q}^* \subseteqq \mathfrak{Q} - \mathfrak{Q}_1^\sharp$. Therefore $n = 1$ and $\mathscr{T}$ contains $2(q^c - 1)$ irreducible characters $\lambda_1, \lambda_2, \cdots$ of degree e. Define

$$\alpha = \tilde{1}_{\mathfrak{Q}} - \lambda_1 \,, \qquad \beta = q^c \lambda_1 - \zeta_1 \,.$$

By Lemma 9.4 we have that

$$\|\alpha^\tau\|^2 = e + 1 \,, \quad \|\beta^\tau\|^2 = q^{2c} + e \,, \quad (\alpha^\tau, \beta^\tau) = -q^c \,. \tag{31.8}$$

Furthermore

$$(31.9)\qquad \begin{aligned}(\alpha^r, \lambda_i^r - \lambda_j^r) &= \delta_{j1} - \delta_{i1}\,,\\ (\beta^r, \lambda_i^r - \lambda_j^r) &= q^c(\delta_{i1} - \delta_{j1})\,.\end{aligned}$$

Suppose that $(\alpha^r, \lambda_i^r) \neq 0$ for some i with $2 \leqq i \leqq 2(q^c - 1)$. Then (31.8) and (31.9) imply that

$$\frac{q^c + 1}{2} + 1 = e + 1 = \| \alpha^r \|^2 \geqq 1 + 2(q^c - 1) - 1\,.$$

Hence $q^c + 3 \geqq 4q^c - 4$, or $7 \geqq 3q^c$ which is not the case. Therefore

$$(31.10)\qquad \alpha^r = 1_{\mathfrak{G}} - \lambda_1^r + \Gamma\,,\quad (\Gamma, \lambda_i^r) = 0 \quad \text{for } 1 \leqq i \leqq 2(q^c - 1)\,.$$

Equation (31.9) also yields that for some integer x

$$(31.11)\qquad \beta^r = q^c\lambda_1^r - x\sum_{i=1}^{2(q^c-1)} \lambda_i^r + \Delta\,,$$
$$(\lambda_i^r, \Delta) = 0 \text{ for } 1 \leqq i \leqq 2(q^c - 1)\,.$$

Furthermore Lemma 13.8 implies that for $2 \leqq s \leqq q - 1$,

$$(31.12)\qquad (\Delta, \zeta_s^r - \zeta_1^r) = (\beta^r, \zeta_s^r - \zeta_1^r) = (\beta, \zeta_s - \zeta_1) = e\,.$$

Since β^r vanishes on $\hat{\mathfrak{W}}$ and $(\beta^r, 1_{\mathfrak{G}}) = 0$ Lemma 13.2 yields that

$$(31.13)\qquad \Delta = \sum_{i=1}^{q-1} a_{i0} \sum_{j=0}^{e-1} \eta_{ij} + \sum_{j=1}^{e-1} a_{0j} \sum_{i=0}^{q-1} \eta_{ij} + \Delta_0\,,$$

where $(\Delta_0, \eta_{ij}) = 0$ for $0 \leqq i \leqq q - 1$, $0 \leqq j \leqq e - 1$. Now (31.12) and (31.13) imply that

$$a_{s0} - a_{10} = \pm 1 \quad \text{for } 2 \leqq s \leqq q - 1\,.$$

Define $a = a_{20}$. Then (31.13) implies that

$$(31.14)\qquad (a \pm 1)^2 + (q - 2)a^2 + \sum_{j=1}^{e-1} a_{0j}^2$$
$$+ \sum_{j=1}^{e-1} \{(a \pm 1 + a_{0j})^2 + (q - 2)(a + a_{0j})^2\} \leqq \| \Delta \|^2\,.$$

For any value of j the term in the last summation in (31.14) is non zero. Furthermore $(a \pm 1)^2 + (q - 2)a^2 \neq 0$. Thus (31.14) implies that if there are exactly k values of j with $a_{0j} \neq 0$, then

$$(31.15)\qquad k + e \leqq \| \Delta \|^2\,,\quad k \text{ is even.}$$

The last statement follows from the fact that $(\eta_{0j}, \Delta) = (\bar{\eta}_{0j}, \Delta)$ since β^r and thus Δ has its values in $\mathscr{C}_{|\mathfrak{Q}|}$. By definition

$$(q^c\tilde{1}_{\mathfrak{Q}} - \zeta_1)^r = q^c(\tilde{1}_{\mathfrak{Q}} - \lambda_1)^r + (q^c\lambda_1 - \lambda_1)^r = q^c\alpha^r + \beta^r\,.$$

Lemma 31.2 implies that for any value of j with $1 \leqq j \leqq e - 1$

(31.16) $$(\alpha^r, \eta_{0j}) \neq 0 \quad \text{or} \quad (\beta^r, \eta_{0j}) \neq 0 .$$

Now (31.8), (31.11) and (31.15) yield that

$$(q^e - x)^2 + x^2\{2(q^e - 1) - 1\} \leqq q^{2e} ,$$

or

$$2(q^e - 1)x^2 \leqq 2q^e x .$$

Therefore

$$0 \leqq x \leqq \frac{q^e}{q^e - 1} < 2 .$$

Suppose that $x \neq 0$, then $x = 1$. Now (31.8) and (31.11) imply that $\| \Delta \|^2 \leqq q^{2e} + e - \{(q^e - 1)^2 + 2(q^e - 1) - 1\} = e + 2$. By (31.15) this implies that $k = 0$ or $k = 2$. Assume first that $k = 0$, then (31.10) implies that $\| \Gamma \|^2 \leqq e - 1$. Hence by (31.16)

$$\Gamma = \sum_{j=1}^{e-1} \pm \eta_{0j} .$$

This implies that $(\beta^r, \Gamma) = 0$. Consequently (31.8), (31.10) and (31.11) yield that

$$-q^e = (\alpha^r, \beta^r) = (-\lambda_1^r, \beta^r) = x - q^e = 1 - q^e$$

which is not the case.

Assume now that $k = 2$. Choose $1', 2'$ with $1 \leqq 1' < 2' \leqq e - 1$ so that $a_{0j} \neq 0$ for $j = 1', 2'$. Thus $\eta_{01'} = \overline{\eta_{02'}}$, $a_{01'} = a_{02'} = \pm 1$ and by (31.16)

$$\alpha^r = 1_{\mathfrak{G}} - \lambda_1^r + \sum_{j \neq 1', 2', 0} \pm \eta_{0j} + \Gamma_0 , \quad \| \Gamma_0 \|^2 = 2 .$$

Since β^r has its values in $\mathscr{O}_{|\mathfrak{Q}|}$ and $\eta_{01'}$ has its values in $\mathscr{O}_e$, $(\eta_{0j}, \beta^r) \neq 0$ for any algebraic conjugate η_{0j} of $\eta_{01'}$. By Lemma 13.1 $\eta_{01'}$ has at least $(p - 1)$ algebraic conjugates. Hence $p = 3$, therefore $q \neq 3$. Since α^r vanishes on $\hat{\mathfrak{B}}$ Lemma 13.1 implies that for $1 \leqq s \leqq q - 1$

$$0 = (\alpha^r, 1_{\mathfrak{G}} - \eta_{s0} - \eta_{01'} + \eta_{s1'}) = 1 + (\Gamma_0, - \eta_{s0} + \eta_{s1'}) - (\Gamma_0, \eta_{01'}) .$$

Hence if $(\Gamma_0, \eta_{01'}) = 0$ then

$$2 = \| \Gamma_0 \|^2 \geqq (q - 1) > 2 .$$

Therefore $(\Gamma_0, \eta_{01'}) \neq 0$. Hence

$$\Gamma = \sum_{j=1}^{e-1} \pm \eta_{0j} .$$

Consequently (31.8), (31.10) and (31.11) yield that

$$-q^e = (\alpha^r, \beta^r) = (-\lambda_1^r, \beta^r) \pm 2 = x - q^e \pm 2 = 1 - q^e \pm 2 .$$

The assumption that $x \neq 0$ has led to a contradiction in all cases. Therefore (31.8), (31.11) and (31.15) imply that

$$\beta^r = q^e\lambda_1^r + \Delta , \qquad \|\Delta\|^2 = e .$$

Thus $a_{0j} = 0$ for $1 \leqq j \leqq e-1$. Thus (31.14) implies that

$$(a \pm 1)^2 e + (q-2)a^2 e \leqq e .$$

Hence $a = 0$ or $q = 3$ and $a \pm 1 = 0$. Thus $\beta^r = q^e\lambda_1^r - \zeta_1^r$ or $q = 3$ and $\beta^r = q^e\lambda_1^r + \zeta_2^r$. In either case this implies that the set of characters consisting of λ_i, $1 \leqq i \leqq 2(q^e-1)$ and ζ_s, $1 \leqq s \leqq q-1$ is coherent. This includes all characters in $\mathscr{T}$ which have $\mathfrak{Q}_1$ in their kernel. Since $|\mathfrak{Q} : \mathfrak{Q}_1| = q^{3c+1} > 4p^{2b}$ the result now follows from Theorem 11.1 with $\mathfrak{H} = \hat{\mathfrak{L}} = \mathfrak{K} = \mathfrak{Q}$, $\mathfrak{H}_1 = \mathfrak{Q}_1$ and $\mathfrak{L} = \mathfrak{T}$.

LEMMA 31.4. *$\mathscr{S}$ is coherent.*

Proof. By Theorem 30.1 w_2 is a power of 3 if $\mathscr{S}$ is not coherent. By Lemma 31.3 b is odd. Thus the lemma follows from Lemma 11.6.

LEMMA 31.5. *For $0 \leqq i \leqq n-1$ let λ_i be an irreducible character of $\mathfrak{T}$ with $\lambda_i(1) = eq^{f_i}$. Let $\mathfrak{Q}_0$ be the normal closure of $\mathfrak{Q}^*$ in $\mathfrak{T}$. Let $1 = q^{g_0} < \cdots < q^{g_m}$ be all the degrees of irreducible characters of $\mathfrak{Q}/\mathfrak{Q}_0$. Then $\mathfrak{T}/\mathfrak{Q}_0$ is a Frobenius group. For any value of j with $0 \leqq j \leqq m$ let θ_j be an irreducible character of $\mathfrak{T}/\mathfrak{Q}_0$ of degree eq^{g_j}. Define*

$$\alpha = \tilde{1}_{\mathfrak{Q}} - \lambda_0 ,$$
$$\beta_i = q^{f_i - f_{i-1}}\lambda_{i-1} - \lambda_i \quad \text{for } 1 \leqq i \leqq n-1 ,$$
$$\gamma_j = q^{g_j - g_{j-1}}\theta_{j-1} - \theta_j \quad \text{for } 1 \leqq j \leqq m .$$

Then

$$(\beta_i^r, \eta_{0t}) = 0 \quad \text{for } 0 \leqq t \leqq e-1,\ 1 \leqq i \leqq n-1 ,$$
$$(\gamma_j^r, \eta_{0t}) = 0 \quad \text{for } 0 \leqq t \leqq e-1,\ 1 \leqq j \leqq m .$$

Furthermore if e is a prime then one of the following possibilities must occur:

$$\alpha^r = 1_{\mathfrak{G}} - \lambda_0^r + \sum_{t=1}^{e-1} \eta_{0t} ,$$

$$\alpha^r = 1_{\mathfrak{G}} + \bar{\lambda}_0^r + \sum_{t=1}^{e-1} \eta_{0t} \text{ and } 2e+1 = |\mathfrak{Q} : \mathfrak{Q}'| ,$$

$$\alpha^r = 1_{\mathfrak{G}} + \sum_{s=1}^{q-1} \eta_{s0} + \Gamma ,$$

with $(\Gamma, \eta_{st}) = 0$ *for* $0 \leqq s \leqq q-1$, $0 \leqq t \leqq e-1$.

Proof. For $1 \leqq i \leqq n-1$, $1 \leqq j \leqq m$ let

$$\alpha^r = \Gamma_{00} + \Delta_{00}\,, \quad \beta_i^r = \Gamma_{i0} + \Delta_{i0}\,, \quad \gamma_j^r = \Gamma_{0j} + \Delta_{0j}\,,$$

where each Δ_{ij} is a linear combination of the generalized characters η_{st} and each Γ_{ij} is orthogonal to each of these generalized characters. Since for $1 \leqq s \leqq q-1$, $(\zeta_s - \zeta_1)^r$ is orthogonal to α^r, β_i^r and γ_j^r and all of these vanish on $\hat{\mathfrak{B}}$, Lemma 13.2 implies that

$$\Delta_{ij} = a_{00}1_{\mathfrak{B}} + a\sum_{s=1}^{q-1}\sum_{t=0}^{e-1}\eta_{st} + \sum_{t=1}^{e-1}a_{0t}\sum_{s=0}^{q-1}\eta_{st} - a_{00}\sum_{s=1}^{q-1}\sum_{t=1}^{e-1}\eta_{st}\,, \tag{31.17}$$

where $\{a\} \cup \{a_{st}\}$ is a set of integers depending on (i, j). Since $(\lambda_0^r - \bar{\lambda}_0^r, \alpha^r) \neq 0$, $\|\Delta_{00}\|^2 \leqq e$. Since $(\lambda_i^r - \bar{\lambda}_i^r, \beta_i^r) \neq 0$, $(\theta_j^r - \bar{\theta}_j^r, \gamma_j^r) \neq 0$, Theorem 12.1 implies that

$$\|\Delta_{ij}\|^2 \leqq e \quad \text{for all } (i, j)\,. \tag{31.18}$$

Assume first that $(i, j) \neq (0, 0)$. Then $a_{00} = 0$. Thus (31.17) and (31.18) imply that

$$(q-1)a^2 + (q-1)\sum_{t=1}^{e-1}(a + a_{0t})^2 + \sum_{t=1}^{e-1}a_{0t}^2 \leqq e\,.$$

If $a \neq 0$ then for each value of t either $a_{0t} \neq 0$ or $a + a_{0t} \neq 0$. Thus $(q-1)a^2 \leqq 1$ which is not the case. Hence $a = 0$ and so

$$\Delta_{ij} = \sum_{t=1}^{e-1}a_{0t}\sum_{s=0}^{q-1}\eta_{st}\,. \tag{31.19}$$

As $\mathscr{I}_0(\mathscr{S})^r$ is orthogonal to $\mathscr{I}_0(\mathscr{T})^r$ Lemma 31.4 yields that for all (i, j)

$$(\xi_k(1)\xi_{k'}^r - \xi_{k'}(1)\xi_k^r, \Delta_{ij}) = 0 \quad \text{for } 1 \leqq k,\ k' \leqq e-1\,.$$

By (31.19) $(\Delta_{ij}, \xi_k^r) = \pm a_{0k}q$. Hence

$$\xi_k(1)a_{0k'} - \xi_{k'}(1)a_{0k} = 0\,.$$

Suppose now that $a_{0t} \neq 0$ for some t. Then $a_{0t} \neq 0$ for all t with $1 \leqq t < e$. Hence (31.18) and (31.19) imply that

$$q(e-1) \leqq q\sum_{t=1}^{e-1}a_{0t}^2 \leqq e$$

which is not the case. The result is proved in case $(i, j) \neq (0, 0)$.

Let $(i, j) = (0, 0)$. Then $a_{00} = 1$. By assumption $\xi_k(1) = \xi_1(1)$ for $1 \leqq k \leqq e-1$, since e is a prime. By (31.17)

$$(\Delta_{00}, \xi_k^\tau) = \pm\{a(q-1) + a_{0k}q - a_{00}(q-1)\}\,, \quad \text{for } 1 \leqq k \leqq e-1$$

where the sign is independent of k. Since $(\Delta_{00}, \xi_k^\tau - \xi_1^\tau) = 0$ this yields that $a_{0k} = a_{01}$ for $1 \leqq k \leqq e-1$. Hence (31.17) and (31.18) imply that

$$(q-1)a^2 + (e-1)a_{01}^2 + (e-1)(q-1)(a + a_{01} - 1)^2 \leqq e-1\,.$$

If $a_{01} \neq 0$ this yields that $a = 0$ and $a_{01} = 1$ and the result follows. If $a_{01} = 0$ then we get that

$$(q-1)a^2 + (e-1)(q-1)(a-1)^2 \leqq e-1\,.$$

Hence $a = 1$ and the result is proved also in this case.

LEMMA 31.6. *Let $\lambda = \lambda_{n-1}$ have the same meaning as in Lemma 31.5. Define*

$$\beta_n = \beta = q^{f_n - f_{n-1}}\lambda - \zeta_1\,.$$

Then $(\beta^\tau, \eta_{0t}) = 0$ for $0 \leqq t \leqq e-1$.

Proof. Let $\mathscr{T}_b$ be the equivalence class in $\mathscr{T}$ defined by (12.3) which contains λ. If ζ_1 is in $\mathscr{T}_b$ then the result follows from the coherence of $\mathscr{T}_b$. For any i, let a_i/e be the number of characters of degree $q^{f_i}e$ in $\mathscr{T}_b$ and define c as in (12.4) by

$$c = \sum_i a_i q^{2(f_i - f_m)}\,, \tag{31.20}$$

where $q^{f_m}e$ is the minimum degree of any character in $\mathscr{T}_b$.

Let

$$\beta^\tau = \Delta_0 + \Delta + \Gamma\,, \tag{31.21}$$

where $\Delta_0 \in \mathscr{I}(\mathscr{T}_b^\tau)$, Δ is an integral linear combination of the generalized characters η_{st} and Γ is orthogonal to $\mathscr{T}_b^\tau$ and to every η_{st}. Theorem 12.1 yields that

$$\|\Delta\|^2 + \|\Gamma\|^2 \leqq 2e\,. \tag{31.22}$$

β^τ vanishes on $\hat{\mathfrak{B}}$ and $(\beta^\tau, 1_{\mathfrak{B}}) = 0$. Furthermore $(\zeta_s^\tau - \zeta_1^\tau, \Delta) = e$ for $2 \leqq s \leqq q-1$. Therefore Lemma 13.2 implies that

$$\Delta = \varepsilon \sum_{t=0}^{e-1} \eta_{1t} + a_{10} \sum_{s=1}^{q-1} \sum_{t=0}^{e-1} \eta_{st} + \sum_{t=1}^{e-1} a_{0t} \sum_{s=0}^{q-1} \eta_{st}\,, \tag{31.23}$$

where $\varepsilon = \pm 1$.

Since $\mathscr{S}_0(\mathscr{S})^\tau$ is orthogonal to $\mathscr{S}_0(\mathscr{T})^\tau$ Lemma 31.4 yields that

$$(\xi_k(1)\xi_{k'}^\tau - \xi_{k'}(1)\xi_k^\tau, \Delta) = 0 \quad \text{for } 1 \leqq k,\ k' \leqq e-1\,.$$

By (31.23)

$$(\xi_k^{\mathfrak{x}}, \Delta) = \pm\{\varepsilon + (q-1)a_{10} + qa_{0k}\} ,$$

where the sign is independent of k. Therefore

$$\xi_k(1)\{\varepsilon + (q-1)a_{10} + qa_{0k'}\} = \xi_{k'}(1)\{\varepsilon + (q-1)a_{10} + qa_{0k}\}$$

for $1 \leqq k,\ k' \leqq e$. By (31.22) and (31.23) we see that

$$\sum_{t=1}^{e-1} a_{0t}^2 + (a_{10}+\varepsilon)^2 + (q-2)a_{10}^2 + \sum_{t=1}^{e-1}(\varepsilon + a_{10} + a_{0t})^2 + (q-2)\sum_{t=1}^{e-1}(a_{10}+a_{0t})^2 = \|\Delta\|^2 \leqq 2e . \tag{31.24}$$

If $a_{10} \neq 0$ and $a_{10} + \varepsilon \neq 0$ then for each t at most one of a_{0t}, $a_{10} + a_{0t}$ $\varepsilon + a_{10} + a_{0t}$ vanishes. Hence (31.24) yields that

$$(a_{10}+\varepsilon)^2 + (q-2)a_{10}^2 \leqq 2 .$$

This is impossible as either a_{10} or $a_{10} + \varepsilon$ is even. If $a_{10} \neq 0$ then (31.24) implies that

$$2\sum_{t=1}^{e-1} a_{0t}^2 + (q-2) + (q-2)\sum_{t=1}^{e-1}(a_{0t}-\varepsilon)^2 \leqq 2e .$$

If $q \neq 3$, then $2\,a_{0t}^2 + (q-2)(a_{0t}-\varepsilon)^2 \geqq 2$ for $1 \leqq t < e$. Hence $q - 2 \leqq 2$ which is not the case. Thus $a_{10} = 0$ or $q = 3$ and $a_{10} + \varepsilon = 0$. Thus we get

$$\begin{aligned} &(\xi_k, \Delta) = \pm\{\pm\varepsilon + qa_{0k}\} \\ &\xi_k(1)\{\pm\varepsilon + qa_{0k'}\} = \xi_{k'}(1)\{\pm\varepsilon + qa_{0k}\} \quad \text{for } 1 \leqq k,\ k' < e . \end{aligned} \tag{31.25}$$

Assume that the result is false. Then $a_{0t} \neq 0$ for some value of t. We will next show that $a_{0t} \neq 0$ for $1 \leqq t < e$. If this is false then there exists j such that $a_{0j} = 0$. If γ is any character in $\mathscr{S}$ then $(\gamma(1)\xi_j^{\mathfrak{x}} - \xi_j(1)\gamma^{\mathfrak{x}},\ \Delta + \Gamma) = 0$. Thus (31.25) implies that

$$(\gamma^{\mathfrak{x}}, \Delta + \Gamma) = \frac{\pm\gamma(1)}{\xi_j(1)} . \tag{31.26}$$

Thus $\xi_j(1) \mid \gamma(1)$ for every γ in $\mathscr{S}$. Let a be the exponent of $\mathfrak{U}$. By Lemmas 30.1, 30.4 and 30.5 $\xi_j(1) = aq$. Thus $\mathfrak{P}'$ is in the kernel of ξ_j. Define

$$\sigma = \{t \mid 1 \leqq t < e,\ \xi_t(1) \neq \xi_j(1)\} .$$

By (31.25)

$$a_{0t} = \frac{\pm\{\xi_t(1) - \xi_j(1)\}}{q\xi_j(1)} \quad \text{for } 1 \leqq t < e .$$

Thus (31.22), (31.23) and (31.26) yield that

$$2e(aq)^2 \geqq \Sigma\,\gamma(1)^2 + \frac{1}{q^2}\sum_{t=1}^{e-1}\{\xi_t(1) - \xi_j(1)\}^2 \geqq \sum \gamma(1)^2 + \frac{x}{q^2}\sum_{t\in\sigma}\xi_t(1)^2\,,$$

where $x = 4/9$ if $q \neq 3$ and $x = 16/25$ if $q = 3$, and γ ranges over the irreducible characters in $\mathscr{S}$. By Lemma 13.7 there exist irreducible characters μ_t of $\mathfrak{S}'$ which induce the characters ξ_t for $1 \leqq t < e$. Consequently

$$2ea^2q \geqq \sum \chi(1)^2 + x\sum_{t\in\sigma}\mu_t(1)^2 \geqq x\left\{\sum \chi(1)^2 + \sum_{t\in\sigma}\mu_t(1)^2\right\}$$

where χ ranges over the irreducible characters of $\mathfrak{S}'$ which are distinct from all μ_t and do not have $\mathfrak{P}$ in their kernel. Therefore $C(\mathfrak{P}) \subseteqq \mathfrak{P}$ otherwise since $|\mathfrak{S}|$ is odd there are at least $2eq$ characters χ of degree at least a. Furthermore

$$2ea^2q \geqq x\{u(h-1) - a^2(e-1)\}\,.$$

This implies that

$$yeqa^2 \geqq \left\{\frac{2eq}{x} + e - 1\right\}a^2 \geqq u(h-1)\,, \tag{31.27}$$

where $y = 4$ if $q = 3$ and $y = 5$ otherwise. Let $1 \subset \mathfrak{P}_1 \subset \mathfrak{P}$, where $\mathfrak{P}_1 \lhd \mathfrak{S}$. Let $h_1 = |\mathfrak{P}_1|$, $h_2 = |\mathfrak{P}:\mathfrak{P}_1|$, $e_1 = |C_{\mathfrak{P}_1}(\mathfrak{Q}^*)|$ and $e_2 = |C_{\mathfrak{P}/\mathfrak{P}_1}(\mathfrak{Q}^*)|$. Since $\mathfrak{S}$ is of type II $ae_1 < 2h_1$ and $a \leqq u$. Thus (31.27) implies that $h_2 - 1 \leqq 2yqe_2$. Since $h_2 \geqq p^{q-1}e_2$ for some prime p dividing h_2 we get that $p^{q-1} \leqq 2yq$. Thus $q = 3$ by (5.1). Hence $p^2 \leqq 24$ which is not the case as $p \geqq 5$. Hence no such group $\mathfrak{P}_1$ exists. Thus $\mathfrak{P}$ is an elementary abelian p-group for some prime. Therefore $e = p$ is a prime and $\xi_t(1) = \xi_1(1)$ for $1 \leqq t < e$. Consequently $a_{0t} = a_{0j} = 0$ for $1 \leqq t < e$ contrary to assumption.

Returning to (31.24) we see that

$$\sum_{t=1}^{e-1} a_{0t}^2 \leqq e + 1\,.$$

Therefore $a_{0t}^2 = 1$ for $1 \leqq t \leqq e-1$. Thus

$$a_{0t} = \pm 1 \quad \text{for } 1 \leqq t \leqq e-1\,. \tag{31.28}$$

Now (31.24) implies that

$$\begin{aligned}(a_{10} + \varepsilon)^2 &+ (q-2)a_{10}^2 \\ &+ (e-1)\{(a_{10} + \varepsilon + a_{01})^2 + (q-2)(a_{10} + a_{01})^2\} \\ &\leqq e + 1\,,\end{aligned} \tag{31.29}$$

Suppose that $q \neq 3$. Thus $q \geqq 5$ and $a_{10} = 0$. Then (31.29) implies that $(e-1)(q-2) \leqq e+1$. As $q \geqq 5$ this implies that $3e - 3 \leqq e + 1$ or $e \leqq 2$ which is not the case. Therefore

$$q = 3 . \tag{31.30}$$

By (31.29) either $a_{10} = 0$, $a_{01} = -(a_{10} + \varepsilon)$ or $a_{10} + \varepsilon = 0$, $a_{01} = -a_{10}$. Now (31.23) and (31.28) imply that

$$\Delta = \pm\left\{\sum_{t=0}^{e-1} \eta_{1t} - \sum_{t=1}^{e-1}\sum_{s=0}^{2} \eta_{st}\right\}$$

or

$$\Delta = \pm\left\{\sum_{t=0}^{e-1} \eta_{2t} - \sum_{t=1}^{e-1}\sum_{s=0}^{2} \eta_{st}\right\} .$$

This is equivalent to

$$\Delta = \pm\left\{\eta_{10} - \sum_{t=1}^{e-1} (\eta_{0t} + \eta_{2t})\right\}$$

or

$$\Delta = \pm\left\{\eta_{20} - \sum_{t=1}^{e-1} (\eta_{0t} + \eta_{1t})\right\} . \tag{31.31}$$

Since $(\beta^x - \bar{\beta}^x, \Gamma) = 0$, Γ is a real valued generalized character. Thus $\| \Gamma \|^2 \neq 1$. By (31.31) $\| \Delta \|^2 = 2e - 1$, hence by (31.22) $\Gamma = 0$. Now (31.21) implies that

$$\beta^x = q^{f_n - f_{n-1}} \lambda^x - x \sum_{i=m}^{n-1} \sum_{j=1}^{a_i/e} q^{f_i - f_m} \lambda_{ij}^x + \Delta , \tag{31.32}$$

where for $m \leqq i \leqq n-1$, λ_{ij} ranges over the characters of degree eq^{f_i} in $\mathscr{T}_b$.

Suppose that $\mathscr{S}$ contains an irreducible character γ. Then by Lemma 31.4

$$(\gamma(1)\xi_t^x - \xi_t(1)\gamma^x, \beta^x) = 0 \quad \text{for } 1 \leqq t \leqq e-1 .$$

As γ^x is rational valued on elements of Ω, $\gamma^x \neq \lambda_{ij}^x$ for all i, j. Thus (31.31) and (31.32) imply that

$$\pm 2\gamma(1) = (\gamma(1)\xi_t^x, \beta^x) = (\xi_t(1)\gamma^x, \beta^x) = 0 .$$

Therefore $\mathscr{S}$ contains no irreducible characters. Hence by Lemma 31.1

$$e = p , \quad p \text{ a prime.} \tag{31.33}$$

Now Lemma 31.3 implies that b is odd, where b is defined in (31.6). As $\| \Delta \|^2 = 2p - 1 > 2p - 2$ Theorem 12.1 implies that if c is

defined in (31.20) then

$$c \equiv 0 \pmod{q} \quad \text{or} \quad c \geqq p^2 . \tag{31.34}$$

Assume first that $m \neq 0$ in (31.32). Let α be defined as in Lemma 31.5. Suppose that

$$\alpha^\tau = 1_{\mathfrak{G}} \pm \lambda_0^\tau + \sum_{i=1}^{p-1} \eta_{0i} .$$

Then (31.31) and (31.32) yield that

$$0 = (\alpha^\tau, \beta^\tau) = \pm(p-1) .$$

Thus by Lemma 31.5

$$\alpha^\tau = 1_{\mathfrak{G}} \pm \lambda_0^\tau + \sum_{s=1}^{2} \eta_{s0} + \Gamma_0 , \quad \|\Gamma_0\|^2 \leqq p-3 . \tag{31.35}$$

Then

$$\Gamma_0 = \Gamma_{00} + y \sum_{i=m}^{n-1} \sum_{j=1}^{a_i/p} q^{f_i - f_m} \lambda_{ij}^\tau , \tag{31.36}$$

where $(\Gamma_{00}, \lambda_{ij}^\tau) = 0$ for $m \leqq i \leqq n-1$, $1 \leqq j \leqq (a_i/p)$. Suppose that $y = 0$. Then (31.31), (31.32) and (31.36) yield that $0 = (\alpha^\tau, \beta^\tau) = \pm 1$. Hence $y \neq 0$. Thus by (31.35) and (31.36)

$$(p-3) \geqq y^2 \frac{c}{p} \geqq \frac{c}{p} .$$

Thus (31.34) yields that

$$c \equiv 0 \pmod{q} . \tag{31.37}$$

Equations (31.31), (31.32), (31.35) and (31.36) imply that

$$0 = (\alpha^\tau, \beta^\tau) = \pm 1 + y q^{f_n - f_{n-1}} q^{f_{n-1} - f_m} - xy \frac{c}{p} .$$

Hence (31.37) implies that $0 \equiv \pm 1 \pmod{q}$. This contradiction arose from assuming $m \neq 0$.

Assume now that $m = 0$. Then

$$c = q^b - 1 + \sum_{i=1}^{n-1} a_i q^{2f_i} .$$

Hence $c \not\equiv 0 \pmod{q}$. Thus (31.34) and 3.15 imply that

$$c \geqq p^2 , \quad c + 1 \equiv 0 \pmod{q^{2f_n}} . \tag{31.38}$$

Now (31.31) and (31.32) yield that

$$q^{2(f_n-f_{n-1})} + p = ||\beta^r||^2 = q^{2(f_n-f_{n-1})} - 2xq^{f_n} + x^2\frac{c}{p} + 2p - 1 .$$

Therefore

$$x^2c + p(p-1) = 2xq^{f_n}p . \tag{31.39}$$

By (31.38), $(c+1) > pq^{f_n}$. Thus (31.39) yields that

$$f(x) = x^2(pq^{f_n} - 1) - 2xq^{f_n}p + p(p-1) < 0 .$$

It is easily verified that $f(x)$ is a monotone increasing function for $x \geqq 2$ and $f(2) = p(p-1) - 4 > 0$. Thus $x < 2$. By (31.39) $x > 0$. Hence $x = 1$. Now (31.39) becomes

$$c + p(p-1) = 2q^{f_n}p ,$$

or equivalently

$$p^2 - p(1 + 2q^{f_n}) + c = 0 . \tag{31.40}$$

Therefore $(1 + 2q^{f_n})^2 - 4c \geqq 0$, hence

$$4c \leqq 4q^{2f_n} + 4q^{f_n} + 1 < 8q^{2f_n} .$$

Thus $c < 2q^{2f_n}$. As c is even, (31.38) now yields that $c = q^{2f_n} - 1$. Now (31.40) becomes

$$q^{2f_n} - 2q^{f_n}p + p^2 - p - 1 = 0 ,$$

or

$$(q^{f_n} - p - 1)(q^{f_n} - p + 1) = p .$$

As p is a prime one of the factors is ± 1 and the other is $\pm p$. As the factors differ by 2 this implies that $p \pm 1 = 2$. Hence $p = 3$. Since $p \neq q$ (31.30) implies that $p \neq 3$. This contradiction establishes the lemma in all cases.

THEOREM 31.1. *$\mathscr{T}$ is coherent.*

Proof. Suppose that $\mathscr{T}$ is not coherent so that Hypothesis 31.1 is assumed. Let $\alpha, \beta_i, \gamma_j, \lambda_i, \theta_j$ have the same meaning as in Lemmas 31.5 and 31.6. Choose $\lambda_0 = \theta_0$. Then

$$(q^{f_n}\tilde{1}_\Omega - \zeta_1)^r = q^{f_n}\alpha^r + \sum_{i=1}^{n} q^{f_n-f_i}\beta_i^r . \tag{31.41}$$

$$(q^{f_n}\lambda_0 - \zeta_1)^r = \sum_{i=1}^{n} q^{f_n-f_i}\beta_i^r . \tag{31.42}$$

$$(q^{g_j}\theta_0 - \theta_j)^r = \sum_{s=1}^{j} q^{g_j-g_s}\gamma_s^r \quad \text{for } 1 \leqq j \leqq m . \tag{31.43}$$

Lemmas 31.2, 31.5 and 31.6 together with (31.41) imply that

$$\alpha^{\tau} = 1_{\mathfrak{G}} - \lambda_0^{\tau} + \sum_{t=1}^{e-1} \eta_{0t}$$

or

$$\alpha^{\tau} = 1_{\mathfrak{G}} + \bar{\lambda}_0^{\tau} + \sum_{t=1}^{e-1} \eta_{0t}$$

and $2e + 1 = |\mathfrak{Q} : \mathfrak{Q}'|$. If the latter possibility occurs then by Lemma 10.1 it may be assumed after changing notation that in any case

$$\alpha^{\tau} = 1_{\mathfrak{G}} - \lambda_0^{\tau} + \sum_{t=1}^{e-1} \eta_{0t} . \tag{31.44}$$

Now Lemma 31.5, (31.43) and (31.44) imply that

$$\begin{aligned} -q^{\varrho s} &= (\alpha^{\tau}, (q^{\varrho s}\theta_0 - \theta_s)^{\tau}) \\ &= (-\theta_0^{\tau}, (q^{\varrho s}\theta_0 - \theta_s)^{\tau}) , \quad \text{for } 1 \leqq s \leqq m . \end{aligned} \tag{31.45}$$

Since $\| (q^{\varrho s}\theta_0 - \theta_s)^{\tau} \|^2 = q^{2\varrho s} + 1$ and $((q^{\varrho s}\theta_0 - \theta_s)^{\tau}, (\theta_s^{\tau} - \bar{\theta}_s^{\tau})) = -1$, (31.45) implies that

$$(q^{\varrho s}\theta_0 - \theta_s)^{\tau} = q^{\varrho s}\theta_0^{\tau} - \theta_s^{\tau} \quad \text{for } 1 \leqq s \leqq m . \tag{31.46}$$

Lemmas 31.2 and 31.5 and equations (31.42) and (31.44) yield that

$$-q^{f n} = ((q^{f n}\lambda_0 - \zeta_1)^{\tau}, \alpha^{\tau}) = ((q^{f n}\lambda_0 - \zeta_1)^{\tau}, -\lambda_0^{\tau}) . \tag{31.47}$$

By Lemma 13.10 $\{\zeta_i \mid 1 \leqq i \leqq q-1\}$ is subcoherent in $\mathscr{T}$. Since $\| (q^{f n}\lambda_0 - \zeta_1)^{\tau} \|^2 = q^{2f n} + e$ it follows from (31.47) that

$$(q^{f n}\lambda_0 - \zeta_1)^{\tau} = q^{f n}\lambda_0^{\tau} - \zeta_1^{\tau} . \tag{31.48}$$

Let $\mathfrak{Q}_0$ have the same meaning as in Lemma 31.5. Then there exists a subgroup $\mathfrak{Q}_1$ of $\mathfrak{Q}_0$ such that $\mathfrak{Q}_0/\mathfrak{Q}_1$ is a chief factor of $\mathfrak{T}$ and $|\mathfrak{Q}_0 : \mathfrak{Q}_1| = q$. Let $\mathscr{T}(\mathfrak{Q}_0)$ be the irreducible characters of $\mathfrak{T}$ of degree $eq^{\varrho j}$, $0 \leqq j \leqq m$. Then (31.46) implies directly that $\mathscr{T}(\mathfrak{Q}_0)$ is coherent. Hypothesis 11.1 is satisfied with $\mathfrak{H} = \hat{\mathfrak{L}} = \mathfrak{N} = \mathfrak{Q}$ and $\mathfrak{T} = \mathfrak{L}$. If $\mathscr{T}$ is not coherent then Theorem 11.1 implies that $|\mathfrak{Q} : \mathfrak{Q}_0| < 4e^2 + 1$. As $\mathfrak{T}/\mathfrak{Q}_0$ is a Frobenius group this implies that $\mathfrak{Q}_0 = \mathfrak{Q}'$. Therefore $\mathfrak{Q}/\mathfrak{Q}_1$ is an extra special q-group. Thus $|\mathfrak{Q} : \mathfrak{Q}'| = q^{2c}$ for some integer c. Define

$$\mathscr{T}(\mathfrak{Q}_1) = \mathscr{T}(\mathfrak{Q}_0) \cup \{\zeta_i \mid 1 \leqq i \leqq q-1\} .$$

Then $\mathscr{T}(\mathfrak{Q}_1)$ consists of all characters in $\mathscr{T}$ having the same weight and degree as some character in $\mathscr{T}$ which has $\mathfrak{Q}_1$ in its kernel. By (31.48) $\mathscr{T}(\mathfrak{Q}_1)$ is coherent. Thus if $\mathscr{T}$ is not coherent Theorem 11.1 implies that

(31.49) $$q^{2e+1} = |\mathfrak{Q} : \mathfrak{Q}_1| \leqq 4e^2 + 1 .$$

Lemma 13.6 applied to the group $\mathfrak{W}_2\mathfrak{Q}/\mathfrak{Q}_1$ implies that $e \mid q^e + 1$ or $e \mid q^e - 1$ and $|\mathfrak{W}_2| = e$. As e is odd this yields that $2e \leqq q^e + 1$ in any case. Thus by (31.49)

$$q^{2e+1} \leqq 4e^2 + 1 \leqq (q^e + 1)^2 + 1 < 2q^{2e} .$$

This contradiction suffices to prove Theorem 31.1.

COROLLARY 31.1.1. *If λ_0 is an irreducible character of $\mathfrak{T}$ of degree w_2 then*

$$(\tilde{1}_{\mathfrak{T}'} - \lambda_0)^{\mathfrak{r}} = 1_{\mathfrak{G}} - \lambda_0^{\mathfrak{r}} + \sum_{t=1}^{w_2-1} \eta_{0t} .$$

Proof. Let $\alpha = \tilde{1}_{\mathfrak{T}'} - \lambda_0$ and let $a_t = (\alpha^{\mathfrak{r}}, \eta_{0t})$. By Theorem 31.1

(31.50) $$\begin{aligned}(\nu_1(1)\tilde{1}_{\mathfrak{T}'} - \zeta_1)^{\mathfrak{r}} &= \nu_1(1)\alpha^{\mathfrak{r}} + (\nu_1(1)\lambda_0 - \zeta_1)^{\mathfrak{r}} \\ &= \nu_1(1)\lambda_0^{\mathfrak{r}} - \zeta_1^{\mathfrak{r}} + \nu_1(1)\alpha^{\mathfrak{r}} .\end{aligned}$$

As η_{0t} is rational on $\mathfrak{T}'$, $(\eta_{0t}, \lambda_0^{\mathfrak{r}}) = 0$. By Lemma 13.9 $(\eta_{0t}, \zeta_1^{\mathfrak{r}}) = 0$. Thus (31.50) implies that

$$((\nu_1(1)\tilde{1}_{\mathfrak{T}'} - \zeta_1)^{\mathfrak{r}}, \eta_{0t}) = a_t\nu_1(1) \quad \text{for } 1 \leqq t \leqq w_2 - 1 .$$

Hence by Lemma 31.2 $(\alpha^{\mathfrak{r}}, \eta_{0t}) \neq 0$ for $1 \leqq t \leqq w_2 - 1$. As $|\mathscr{T}| > 2$, $(\alpha^{\mathfrak{r}}, 1_{\mathfrak{G}}) = 1$, $(\alpha^{\mathfrak{r}}, \lambda_0^{\mathfrak{r}} - \bar{\lambda}_0^{\mathfrak{r}}) = -1$ and $\|\alpha^{\mathfrak{r}}\|^2 = w_2 + 1$ we get that

$$\alpha^{\mathfrak{r}} = 1_{\mathfrak{G}} - \lambda_0^{\mathfrak{r}} + \sum_{t=1}^{w_2-1} \pm\eta_{0t} .$$

As $\alpha^{\mathfrak{r}}$ vanishes on $\hat{\mathfrak{W}}$ Lemma 13.2 now implies the required result.

COROLLARY 31.1.2. *$\mathfrak{S}'$ is a Frobenius group and w_2 is a prime.*

Proof. Suppose that $\mathscr{S}$ contains an irreducible character θ. Choose ξ_j in $\mathscr{S}(\mathfrak{P}')$. Then $(\theta(1)\xi_j^{\mathfrak{r}} - \xi_j(1)\theta^{\mathfrak{r}}) \in \mathscr{S}_0(\mathscr{S})$. If $\mathscr{S}$ is not coherent θ may be chosen in $\mathscr{S}(\mathfrak{P}')$ by Theorem 30.1 and Lemma 31.1. Hence by Corollary 31.1.1 and Lemmas 13.9 and 30.8,

$$\begin{aligned}0 &= (\theta(1)\xi_j^{\mathfrak{r}} - \xi_j(1)\theta^{\mathfrak{r}}, (\tilde{1}_{\mathfrak{T}'} - \lambda_0)^{\mathfrak{r}}) \\ &= \theta(1)\Big(\pm\sum_{i=0}^{q-1} \eta_{ij}, \sum_{t=1}^{w_2-1} \eta_{0t}\Big) = \pm\theta(1) .\end{aligned}$$

Therefore $\mathscr{S}$ contains no irreducible characters. Lemma 31.1 now implies that $\mathfrak{S}'$ is a Frobenius group and w_2 is a prime.

32. Subgroups of Type V

THEOREM 32.1. *$\mathfrak{G}$ contains no subgroup of type V.*

Proof. Suppose that the result is false and $\mathfrak{T}$ is a subgroup of type V. $\mathfrak{T}'$ is tamely imbedded in $\mathfrak{G}$ by Theorem 14.2. For $0 \leqq i \leqq n$ let $\mathfrak{L}_i$ have the same meaning as in Definition 9.1 and let $\mathfrak{A}_L$ be defined by (9.2). Let $\mathfrak{G}_1$ be the set of elements in $\mathfrak{G}$ which are conjugate to some element of $\mathfrak{A}_L$ for $L \in \bigcup_{i=0}^{n} \mathfrak{L}_i$. By Lemma 9.5

$$\frac{1}{|\mathfrak{G}|}|\mathfrak{G}_1| = \frac{1}{|\mathfrak{G}|}\sum_{\mathfrak{G}_1} 1_{\mathfrak{G}}(G) = \frac{1}{|\mathfrak{T}|}\sum_{\mathfrak{T}'^{\sharp}} 1_{\mathfrak{G}}(T) = \frac{1}{w_2}\left(1 - \frac{1}{|\mathfrak{T}'|}\right). \tag{32.1}$$

Let λ be an irreducible character of degree w_2 in $\mathscr{T}$. By Theorem 31.1 and Lemmas 10.3 and 9.4

$$\lambda^{\mathfrak{r}}(T) = a + \lambda(T) \quad \text{for } T \in \mathfrak{T}'^{\sharp}, \tag{32.2}$$

where a is independent of T. Now Theorem 31.1 and Corollary 31.1.1 imply that $a = 0$ in (32.2). Thus $\lambda^{\mathfrak{r}}(T) = \lambda(T)$ for $T \in \mathfrak{T}'^{\sharp}$. Hence Theorem 31.1 and Lemmas 10.3 and 9.5 imply that

$$\frac{1}{|\mathfrak{G}|}\sum_{\mathfrak{G}_1}|\lambda^{\mathfrak{r}}(G)|^2 = \frac{1}{|\mathfrak{T}|}\sum_{\mathfrak{T}'^{\sharp}}|\lambda(G)|^2 = 1 - \frac{w_2}{|\mathfrak{T}'|}. \tag{32.3}$$

Let $\mathfrak{W}$ be defined by Theorem 14.1 (ii) (a) and let $\hat{\mathfrak{W}} = \mathfrak{W} - \mathfrak{W}_2 - \Omega^*$. Define

$$\mathfrak{G}_2 = \bigcup_{G \in \mathfrak{G}} G^{-1}\hat{\mathfrak{W}}G .$$

Thus Theorem 14.2 (ii) (a) implies that

$$\frac{1}{|\mathfrak{G}|}|\mathfrak{G}_2| = 1 - \frac{1}{w_2} - \frac{1}{q} + \frac{1}{qw_2} . \tag{32.4}$$

Let $\mathfrak{G}_3$ be the set of elements in $\mathfrak{G}$ which are conjugate to some element of $\mathfrak{H}^{\sharp}$. Since $\mathfrak{H}$ is a T.I. set in $\mathfrak{G}$,

$$\frac{1}{|\mathfrak{G}|}|\mathfrak{G}_3| = \frac{1}{qu|\mathfrak{H}|}(|\mathfrak{H}| - 1) . \tag{32.5}$$

Define

$$\mathfrak{G}_0 = \mathfrak{G} - \mathfrak{G}_1 - \mathfrak{G}_2 - \mathfrak{G}_3 .$$

Then (32.1), (32.4) and (32.5) imply that

$$\begin{aligned}\frac{1}{|\mathfrak{G}|}|\mathfrak{G}_0| &\geqq 1-\left(1-\frac{1}{w_2}-\frac{1}{q}+\frac{1}{qw_2}\right)-\left(\frac{1}{w_2}-\frac{1}{w_2|\mathfrak{T}'|}\right)\\ &\quad -\left(\frac{1}{qu}-\frac{1}{qu|\mathfrak{H}|}\right)=\frac{1}{q}-\frac{1}{w_2q}-\frac{1}{qu}+\frac{1}{w_2|\mathfrak{T}'|}\\ &\quad +\frac{1}{qu|\mathfrak{H}|}>\frac{1}{q}-\frac{1}{3q}-\frac{1}{3q}=\frac{1}{3q}.\end{aligned} \tag{32.6}$$

By (32.3)

$$\frac{1}{|\mathfrak{G}|}\sum_{\mathfrak{G}_0}|\lambda^r(G)|^2 \leqq 1-\left(1-\frac{w_2}{|\mathfrak{T}'|}\right)=\frac{w_2}{|\mathfrak{T}'|}. \tag{32.7}$$

By Corollary 31.1.2 w_2 is a prime and $\mathfrak{HU}$ is a Frobenius group. Hence by Lemma 13.1 $\eta_{01}, \cdots, \eta_{0,w_2-1}$ are algebraically conjugate characters whose values lie in $\mathscr{O}_{w_2}$. Every element whose order is divisible by w_2 lies in $\mathfrak{G}_2 \cup \mathfrak{G}_3$. Thus $\eta_{0j}(G)=\eta_{01}(G)$ is a rational integer for $G \in \mathfrak{G}_0$ and $1 \leqq j \leqq w_2-1$. Now Corollary 31.1.1 implies that $1-\lambda^r(G)+(w_2-1)\eta_{01}(G)=0$ for $G \in \mathfrak{G}_0$. Hence $\lambda^r(G) \equiv 1 \pmod 2$ for $G \in \mathfrak{G}_0$. Therefore $|\lambda^r(G)| \geqq 1$ for $G \in \mathfrak{G}_0$. Now (32.6) and (32.7) imply that

$$\frac{w_2}{|\mathfrak{T}'|}>\frac{1}{3q}$$

or

$$3qw_2 > |\mathfrak{T}'|. \tag{32.8}$$

Since $\mathfrak{T}'' \neq 1$, (32.8) yields that $3w_2 > |\mathfrak{T}' : \mathfrak{T}''|$ and $|\mathfrak{T}''| = q$. Thus, $\mathfrak{W}_2$ acts irreducibly on $\mathfrak{T}'/\mathfrak{T}''$. Therefore $\mathfrak{T}'$ is an extra special group. Let $|\mathfrak{T}' : \mathfrak{T}''| = q^{2c}$. Then by Lemma 13.6, $w_2 \leqq (q^c+1)/2$. Thus (32.8) implies that $q^{2c} < (3/2)(q^c+1) < 2q^c$. Hence $q^c < 2$ which is not the case. The proof is complete.

COROLLARY 32.1.1. *Let $\mathfrak{S}$ be a subgroup of type* II, III *or* IV. *Let $\mathscr{S}$ have the same meaning as in Section 29. Then $\mathscr{S}$ is coherent.*

Proof. This is an immediate consequence of Theorems 30.1 and 32.1.

33. Subgroups of Type I

LEMMA 33.1. *Let $\mathfrak{L}$ be a maximal subgroup of $\mathfrak{G}$ and let $\hat{\mathfrak{L}}$ have the same meaning as in section* 14. *If $\mathfrak{L}$ is of type* I *with Frobenius*

kernel $\mathfrak{H}$ *let* $\mathscr{L}$ *be the set of all irreducible characters of* $\mathfrak{L}$ *which do not have* $\mathfrak{H}$ *in their kernel. If* $\mathfrak{L}$ *is of type* II, III *or* IV *let* $\mathscr{L}$ *be the set of characters of* $\mathfrak{L}$ *each of which is induced by a non principal irreducible character of* $\mathfrak{L}'$ *which vanishes outside* $\hat{\mathfrak{L}}$. *Let* $\mathfrak{L}_i$ *have the same meaning as in section* 9 *and let* $\mathfrak{A}_L$ *be defined by* (9.2). *If* $\lambda \in \mathscr{L}$ *then* λ^r *can be defined. Furthermore* λ^r *is constant on* $\mathfrak{A}_L$ *for* $L \in \bigcup_{i=0}^{r} \mathfrak{L}_i$.

Proof. Since $|\mathfrak{G}|$ is odd Lemmas 10.1 and 13.9 imply that λ^r can always be defined as $\{\lambda, \bar{\lambda}\}$ is coherent.

If $L \in \mathfrak{L}_0$ then $\mathfrak{A}_L = \{L\}$ and there is nothing to prove. If $L \in \mathfrak{L}_i$ with $i \neq 0$ let $\mathfrak{H}_i$ be a supporting subgroup of $\hat{\mathfrak{L}}$ such that $C(L) \subseteq \mathfrak{N}_i = N(\mathfrak{H}_i)$. If $\mathfrak{N}_i$ is of type I then the result follows from Lemmas 4.5 and 10.3. By definition $\mathfrak{N}_i$ cannot be of type III or IV. If $\mathfrak{N}_i$ is of type II then the result is a simple consequence of Corollary 32.1.1.

The main purpose of this section is to prove

THEOREM 33.1. *Every subgroup of type* I *is a Frobenius group.*

All the remaining lemmas in this section will be proved under the following assumption.

Hypothesis 33.1.
$\mathfrak{G}$ *contains a subgroup of type* I *which is not a Frobenius group.*

If Hypothesis 33.1 is satisfied the following notation will be used.

σ is a set of primes defined as follows: $p_i \in \sigma$ if and only if $\mathfrak{G}$ contains a subgroup $\mathfrak{M}_i$ of type I with Frobenius kernel $\mathfrak{K}_i$ such that a S_{p_i}-subgroup of $\mathfrak{M}_i/\mathfrak{K}_i$ is not cyclic.

$p = p_k$ is the smallest prime in σ. $\mathfrak{M} = \mathfrak{M}_k$; $\mathfrak{K} = \mathfrak{K}_k$.

$\mathfrak{P}_0$ is a S_p-subgroup of $\mathfrak{M}$.

$\mathfrak{P}$ is a S_p-subgroup of $\mathfrak{G}$ with $\mathfrak{P}_0 \subseteq \mathfrak{P}$.

$\mathfrak{L}$ is a maximal subgroup of $\mathfrak{G}$ such that $N(\Omega_1(\mathfrak{P}_0)) \subseteq \mathfrak{L}$.

$\mathscr{L}$ has the same meaning as in Lemma 33.1.

If $\mathfrak{L}$ is of type I let $\mathfrak{U}$ be the Frobenius kernel of $\mathfrak{L}$. Let $\mathfrak{L} = \mathfrak{U}\mathfrak{E}$ with $\mathfrak{U} \cap \mathfrak{E} = 1$.

If $\mathfrak{L}$ is of type II, III or IV let $\mathfrak{H}$ be the maximal normal nilpotent S-subgroup of $\mathfrak{L}$. Let $\mathfrak{U}$ be a complement of $\mathfrak{H}$ in $\mathfrak{L}'$ and let $\mathfrak{W}_1$ be a complement of $\mathfrak{L}'$ in $\mathfrak{L}$ with $\mathfrak{W}_1 \subseteq N(\mathfrak{U})$.

LEMMA 33.2. $\mathfrak{L}$ *is the unique maximal subgroup of* $\mathfrak{G}$ *which contains* $N(\Omega_1(\mathfrak{P}_0))$. *Furthermore* $\mathfrak{L}$ *is either a Frobenius group or* $\mathfrak{L}$ *is of type* III *or* IV *and* $\mathfrak{P}$ *can be chosen to lie in* $\mathfrak{U}$.

Proof. By Theorem 32.1 $\mathfrak{L}$ is not of type V. If $\mathfrak{L}$ is of type II, III or IV then $\mathfrak{P}_0 \subseteq \mathfrak{L}'$ since $\mathfrak{P}_0$ is not cyclic. Since $\mathfrak{H}$ is a T.I. set in $\mathfrak{G}$ it may be assumed that $\mathfrak{P}_0 \subseteq \mathfrak{U}$.

There exists $P \in \Omega_1(\mathfrak{P}_0)$ such that $C(P) \subseteq \mathfrak{M}$. Thus either $\mathfrak{P} = \mathfrak{P}_0$ or $Z(\mathfrak{P})$ is cyclic and $Z(\mathfrak{P}) \subseteq \mathfrak{P}_0$. If a S_p-subgroup of $\mathfrak{U}$ is abelian then $\mathfrak{P}_0$ is the S_p-subgroup of $\mathfrak{U}$. Hence $\Omega_1(\mathfrak{P}_0)$ char $\mathfrak{U}$ and so $N(\mathfrak{U}) \subseteq N(\Omega_1(\mathfrak{P}_0)) \subseteq \mathfrak{L}$. Therefore $\mathfrak{L}$ is of type III or IV and $\mathfrak{P} = \mathfrak{P}_0 \subseteq \mathfrak{U}$. By definition $\mathfrak{L}$ is the unique maximal subgroup which contains $N(\Omega_1(\mathfrak{P}_0))$. If the S_p-subgroup of $\mathfrak{U}$ is not abelian then $\mathfrak{L}$ is of type IV and it may be assumed that $\mathfrak{P} \subseteq \mathfrak{U}$. Then $\Omega_1(\mathfrak{P}_0) \subseteq \hat{\mathfrak{L}}$ and in this case also $\mathfrak{L}$ is the unique maximal subgroup of $\mathfrak{G}$ which contains $N(\Omega_1(\mathfrak{P}_0))$.

Suppose that $\mathfrak{L}$ is of type I. Let $\mathfrak{P}_1$ be a S_p-subgroup of $\mathfrak{L}$ with $\mathfrak{P}_0 \subseteq \mathfrak{P}_1$. If $p \in \pi(\mathfrak{E})$, then $\mathfrak{P}_1$ is abelian. Thus, $\mathfrak{P}_0 = \mathfrak{P}_1$ and so $\mathfrak{P}_0 = \mathfrak{P}$. Hence, $\mathfrak{P}$ is an abelian S_p-subgroup of $\mathfrak{G}$. By construction, $N(\mathfrak{P}) \subseteq \mathfrak{L}$. Hence, $\mathfrak{P} \subseteq \mathfrak{L}'$, by Burnside's transfer theorem. Since $|\mathfrak{L}|$ is odd, if an element of $N(\mathfrak{P})$ induces an automorphism of $\mathfrak{P}$ of prime order q, then $q < p$. By the minimal nature of p, a S_q-subgroup of $\mathfrak{L}$ is cyclic. Let $\mathfrak{P}^* = \mathfrak{P} \cap C(\mathfrak{U})$. Since $\mathfrak{L}$ is of type I, $\mathfrak{P}^*$ is cyclic. We can now find a prime q such that some element $N(\mathfrak{P})$ induces an automorphism of order q on $\mathfrak{P}/\mathfrak{P}^*$. Let $\mathfrak{Q}$ be a S_q-subgroup of $\mathfrak{E}$ permutable with $\mathfrak{P}$. Since $q < p$, $\mathfrak{Q}$ normalizes $\mathfrak{P}$, and $\mathfrak{Q}$ is cyclic. Since $\mathfrak{Q}\mathfrak{U}$ is a Frobenius group, $\Omega_1(\mathfrak{Q})$ centralizes $\mathfrak{P}/\mathfrak{P}^*$. Let $\mathfrak{P}_0^* = C_{\mathfrak{P}}(\Omega_1(\mathfrak{Q}))$. Then $\mathfrak{P} = \mathfrak{P}^*\mathfrak{P}_0^*$, and $[\mathfrak{Q}, \mathfrak{P}_0^*] \not\subseteq \mathfrak{P}^*$.

Let $\mathfrak{L}^*$ be a maximal subgroup containing $N(\Omega_1(\mathfrak{Q}))$. The minimal nature of p implies that $\mathfrak{Q} \subseteq \mathfrak{L}^{*\prime}$. Hence, by Lemma 8.13, $\mathfrak{Q}$ centralizes every chief p-factor of $\mathfrak{L}^*$, so $\mathfrak{Q}$ centralizes $\mathfrak{P}_0^*$, which is not the case. We conclude that $p \notin \pi(\mathfrak{E})$. Therefore $p \in \pi(\mathfrak{U})$. Hence $\mathfrak{P} \subseteq \mathfrak{U}$. $\mathfrak{U}$ is not a T.I. set since $\mathfrak{P}$ is not a T.I. set in $\mathfrak{G}$. This yields that either $p \in \pi_1^*$ or $m(\mathfrak{U}) = 2$. In either case this implies that every prime divisor of $|\mathfrak{E}|$ is less than p. The minimal nature of p now implies that $\mathfrak{L}$ is a Frobenius group.

The previous parts of the lemma imply that if $\mathfrak{L}_1$ is a maximal subgroup of $\mathfrak{G}$ which contains $N(\Omega_1(\mathfrak{P}_0))$ then $\mathfrak{L}_1$ is a Frobenius group and p divides the order of the Frobenius kernel of $\mathfrak{L}_1$. If $\mathfrak{P}$ is abelian then $\mathfrak{P} = \mathfrak{P}_0$ and $\mathfrak{L} = \mathfrak{L}_1 = N(\Omega_1(\mathfrak{P}_0))$. If $\mathfrak{P}$ is non abelian then $\mathfrak{L} = \mathfrak{L}_1 = N(Z(\mathfrak{P}))$. The uniqueness of $\mathfrak{L}$ is proved.

LEMMA 33.3. *There exists an irreducible character $\lambda \in \mathscr{L}$ which does not have $\mathfrak{P}$ in its kernel such that $\lambda(1) \mid (p-1)$ or $\lambda(1) \mid (p+1)$.*

Proof. Let λ be a character of $\mathfrak{L}$ which does not have $\mathfrak{P}$ in its kernel and is induced by a linear character of $\mathfrak{U}$ if $\mathfrak{L}$ is a Frobenius group and by a linear character of $\mathfrak{L}'$ if $\mathfrak{L}$ is of type III or IV.

Either $\mathfrak{P} = \mathfrak{P}_0$ and so $m(\mathfrak{P}) = 2$, or $Z(\mathfrak{P})$ is cyclic. In either case this implies that if $q \in \pi\,(N(\mathfrak{P})/C(\mathfrak{P}))$, $q \neq p$ then $q \mid (p+1)$ or $q \mid (p-1)$. If $\mathfrak{L}$ is of type III or IV then $\lambda(1) = |\mathfrak{W}_1|$ is a prime and the result follows. Suppose that $\mathfrak{L}$ is a Frobenius group. If $p \in \pi_1^*$ then $|\mathfrak{E}| = \lambda(1)$ has the required properties by assumption. If $p \notin \pi_1^*$ then $\mathfrak{H}$ is abelian since $\mathfrak{H}$ is not a T.I. set in $\mathfrak{G}$. Thus $\mathfrak{P} = \mathfrak{P}_0$ and $m(\mathfrak{P}) = 2$. Suppose that $q_1, q_2 \in \pi(\mathfrak{E})$ where $q_1 \mid (p-1)$ and $q_2 \mid (p+1)$. Then an element of $\mathfrak{E}$ of order q_1 acts as a scalar on $\mathfrak{P}$. There exists $P \in \mathfrak{P}^\sharp$ such that $N(\langle P \rangle) \subseteqq \mathfrak{M}$. Thus $\mathfrak{M}$ contains a Frobenius group of order pq_1 which is not the case. Therefore every prime in $\pi(\mathfrak{E})$ divides $(p-1)$ or every prime in $\pi(\mathfrak{E})$ divides $(p+1)$. Since $(p+1, p-1) = 2$ this yields that $|\mathfrak{E}| \,|\, (p+1)$ or $|\mathfrak{E}| \,|\, (p-1)$. The lemma follows since $\lambda(1) = |\mathfrak{E}|$.

LEMMA 33.4. *Let λ be the character defined in Lemma 33.3. Then*

$$\lambda^x(L) = \lambda(L) \quad \textit{for } L \in \hat{\mathfrak{L}}^\sharp$$

Proof. Set $e = |\mathfrak{L} : \mathfrak{L}'|$. Observe that if $\mathfrak{L}$ is a Frobenius group, then since $p \in \pi^*$, it follows that $\mathfrak{L}' = \mathfrak{U}$, so that $\lambda(1) = e$. This equality also holds if $\mathfrak{L}$ is of type III or IV.

Set $\alpha = (\tilde{1}_{\mathfrak{L}'} - \lambda)$ so that $\alpha^x = 1_{\mathfrak{G}} - \lambda^x + \Delta$, where Δ is a generalized character of $\mathfrak{G}$ orthogonal to $1_{\mathfrak{G}}$. Let $\lambda = \lambda_1, \cdots, \lambda_f$ be the characters in $\mathscr{L}$ of degree e. Since e divides $(p+1)/2$ or $(p-1)/2$, it follows that $f > e+1$, and so $(\Delta, \lambda_i^x) = 0$, $1 \leqq i \leqq f$.

We next show that $\mathscr{L}$ is coherent. If $\mathfrak{L}$ is a Frobenius group, the coherence of $\mathscr{L}$ follows from Lemma 11.1 and the fact that $\mathfrak{L}$ is of type I.

Suppose $\mathfrak{L}$ is of type III or IV. Then Hypothesis 11.1 and (11.2) are satisfied with the present $\mathfrak{L}$ in the role of $\mathfrak{L}_0$, $\mathfrak{H}$ in the role of $\mathfrak{H}_0$, and $\mathfrak{L}'/\mathfrak{H}$ in the role of $\mathfrak{H}$. By Lemma 11.1, we may assume that $|\mathfrak{L}' : \mathfrak{L}''| \leqq 4\,|\mathfrak{L} : \mathfrak{L}'|^2 + 1$. Hence, $|\mathfrak{L}' : \mathfrak{L}''| = p^2$ and $e = (p+1)/2$, so that $\mathfrak{P} = \mathfrak{U}$. If $\mathfrak{P}$ is non abelian, then e divides $(p-1)/2$. Hence, we may assume that $\mathfrak{P}$ is abelian of order p^2 and $\mathfrak{L}$ is of type III. By Theorem 29.1 (i), no element of $\mathfrak{P}^\sharp$ centralizes $\mathfrak{H}$. This implies that if $\mu_1, \cdots, \mu_{f'}$ are the characters in $\mathscr{L}$ of degree pe, then $f' \geqq 2p$. Hence, $(\Delta, \mu_j^x) = 0$, $1 \leqq j \leqq f'$.

Let $\beta = (p\lambda_1 - \mu_1)$, so that $\beta^x = p\lambda_1^x - x\sum_i \lambda_i^x - \mu_1^x + \Delta_1$, with $(\Delta_1, \lambda_i^x) = 0$. If $x = 0$, the coherence of $\mathscr{L}$ follows from Theorem 30.1. As $\|\beta^x\|^2 = p^2 + 1$, and $f = 2(p-1)$, it follows that $0 \leqq x < 2$, and $\|\Delta_1\|^2 \leqq 2$. Hence, $x = 1$ and $(\Delta_1, \mu_j^x) = 0$. But now $(\alpha^x, \beta^x) = (\alpha, \beta) = -p = -(p-1) + (\Delta, \Delta_1)$, so that $(\Delta, \Delta_1) = -1$. This is not the case as Δ and Δ_1 are real valued generalized characters of $\mathfrak{G}$

orthogonal to $1_{\mathfrak{G}}$. The coherence of $\mathscr{L}$ is proved in all cases.

Since $(\Delta, \lambda^r) = 0$, the lemma follows from Lemmas 9.4 and 33.1.

LEMMA 33.5. *Let λ be the character defined in Lemma* 33.3. *Then*

$$\frac{1}{|\mathfrak{M}|} \Sigma_{\mathfrak{K}^\sharp} |\lambda^r(K)|^2 < \frac{\lambda(1)^2}{|\mathfrak{L}|}.$$

Proof. Let $\mathfrak{G}_0$ be the set of all elements in $\mathfrak{G}$ which are conjugate to an element of $\mathfrak{A}_L$ for some $L \in \hat{\mathfrak{L}}^\sharp$. Let $\mathfrak{G}_1$ be the set of all elements in $\mathfrak{G}$ which are conjugate to an element of $\mathfrak{A}_K$ for some $K \in \mathfrak{K}^\sharp$. No subgroup of $\mathfrak{G}$ can be a supporting subgroup for both $\hat{\mathfrak{L}}$ and $\hat{\mathfrak{M}}$. If $\mathfrak{L}$ were a supporting subgroup of $\hat{\mathfrak{M}}$ then p would not be minimal in the set σ. Thus $\mathfrak{G}_0$ is disjoint from $\mathfrak{G}_1$. Therefore by Lemmas 9.5, 4.5, 10.3, 33.1 and 33.4

$$\begin{aligned}\frac{1}{|\mathfrak{M}|} \Sigma_{\mathfrak{K}^\sharp} |\lambda^r(K)|^2 &= \frac{1}{|\mathfrak{G}|} \Sigma_{\mathfrak{G}_1} |\lambda^r(G)|^2 < 1 - \frac{1}{|\mathfrak{G}|} \Sigma_{\mathfrak{G}_0} |\lambda^r(G)|^2 \\ &= 1 - \frac{1}{|\mathfrak{L}|} \Sigma_{\hat{\mathfrak{L}}^\sharp} |\lambda^r(G)|^2 = 1 - \frac{1}{|\mathfrak{L}|} \Sigma_{\hat{\mathfrak{L}}^\sharp} |\lambda(G)|^2 \\ &= 1 - \left(1 - \frac{\lambda(1)^2}{|\mathfrak{L}|}\right) = \frac{\lambda(1)^2}{|\mathfrak{L}|}.\end{aligned}$$

LEMMA 33.6. *Let $\mathfrak{M} = \mathfrak{K}\mathfrak{F}$ where $\mathfrak{F} = \mathfrak{M} \cap \mathfrak{L}$. Then there exists F in $(\mathfrak{P}_0 \cap Z(\mathfrak{F}))^\sharp$ such that $C_{\mathfrak{K}}(F) \not\subseteq \mathfrak{K}'$. Furthermore $\mathfrak{M}$ satisfies Hypothesis* 28.1.

Proof. If $\mathfrak{L}$ is of type I, then $\mathfrak{F} \subseteq \mathfrak{U}$. Thus, $\mathfrak{F}$ is nilpotent and hence abelian. The result follows from 3.16 (ii) and the fact that $\mathfrak{P}_0$ is not cyclic.

Suppose $\mathfrak{L}$ is not of type I. If $\mathfrak{F} \not\subseteq \mathfrak{U}\mathfrak{H}$, then we may assume that $\mathfrak{W}_1 \subseteq \mathfrak{F}$. Then $\mathfrak{W}_1\mathfrak{P}_0$ is a Frobenius group and $\mathfrak{W}_1\mathfrak{P}_0 \subseteq \mathfrak{F}$. By 3.16 (ii), $\mathfrak{W}_1$ centralizes an element of $\mathfrak{K}^\sharp$. Since $|\mathfrak{W}_1|$ is a prime, this contradicts the fact that $\mathfrak{M}$ contains a Frobenius group of order $|\mathfrak{W}_1\mathfrak{K}|$. Thus, $\mathfrak{F} \subseteq \mathfrak{U}\mathfrak{H}$. Let $\mathfrak{F}_1 = \mathfrak{F} \cap \mathfrak{H}$. Since $\mathfrak{H}$ is a T.I. set in $\mathfrak{G}$, we get that $\mathfrak{F}_1$ is a cyclic normal S-subgroup of $\mathfrak{F}$. If $\mathfrak{F}_1 = 1$, then $\mathfrak{F}$ is abelian and the result follows from 3.16 (ii).

Assume now that $\mathfrak{F}_1 \neq 1$. We may assume that $\mathfrak{F} = \mathfrak{F}_1(\mathfrak{F} \cap \mathfrak{U})$. If $\Omega_1(\mathfrak{P}_0)$ does not centralize $\mathfrak{F}_1$, then there exists $\mathfrak{P}^* \subseteq \Omega_1(\mathfrak{P}_0)$ such that $\mathfrak{F}_1\mathfrak{P}^*$ is a Frobenius group. Hence, $C_{\mathfrak{K}}(\mathfrak{P}^*) \neq 1$ by 3.16 (ii). But in this case, $\mathfrak{P}^*$ lies in no normal abelian subgroup of $\mathfrak{F}$ contrary to the definition of groups of Frobenius type. Thus, $\Omega_1(\mathfrak{P}_0)$ centralizes $\mathfrak{F}_1$. Since $\mathfrak{F} \cap \mathfrak{U}$ is abelian and $\mathfrak{F} = \mathfrak{F}_1(\mathfrak{F} \cap \mathfrak{U})$, this implies that $\Omega_1(\mathfrak{P}_0) \subseteq$

$Z(\mathfrak{F})$. The lemma now follows from 3.16 (ii).

LEMMA 33.7. *Let $\mathscr{M}$ be the set of all irreducible characters of $\mathfrak{M}$ which do not have $\mathfrak{K}$ in their kernel. Let λ be the character defined in Lemma 33.3. If $\mathscr{M}$ is coherent then λ^r is constant on $\mathfrak{K}^\sharp$.*

Proof. Let $\mathfrak{H}_1, \cdots \mathfrak{H}_s$ be a set of supporting subgroups of $\hat{\mathfrak{M}}$ in $\mathfrak{G}$, and let $\mathfrak{N}_i = N_{\mathfrak{G}}(\mathfrak{H}_i)$. By definition,

$$\hat{\mathfrak{M}} = \bigcup_{K \in \mathfrak{K}^\sharp} C_{\mathfrak{M}}(K) .$$

Suppose $M \in \hat{\mathfrak{M}}^\sharp$ and $C_{\mathfrak{G}}(M) \not\subseteq \mathfrak{M}$. We will show that $M \in \mathfrak{K}$. For otherwise, some power of M is $\mathfrak{M}$-conjugate to an element A of $\mathfrak{F}^\sharp$. Since $\mathfrak{K}$ is a supporting subgroup of some tamely imbedded subset of $\mathfrak{G}$, it follows that $C_{\mathfrak{G}}(A) \subseteq \mathfrak{M}$. Hence, M is in $\mathfrak{K}^\sharp$.

We next show that $\mathfrak{N}_i$ is of type I or II, $1 \leqq i \leqq s$. Suppose $\mathfrak{N}_i$ is not of type I. Then $\mathfrak{N}_i = \mathfrak{H}_i(\mathfrak{N}_i \cap \mathfrak{M})$, and we assume that $\mathfrak{N}_i \cap \mathfrak{M} = (\mathfrak{N}_i \cap \mathfrak{K})(\mathfrak{N}_i \cap \mathfrak{F})$. Since $\mathfrak{H}_i$ is a supporting subgroup of $\hat{\mathfrak{M}}$, we may choose M in $\hat{\mathfrak{M}}$ so that $C_{\mathfrak{G}}(M) \subseteq \mathfrak{N}_i$, $C_{\mathfrak{G}}(M) \not\subseteq \mathfrak{M}$. By the first paragraph, $M \in \mathfrak{K}^\sharp$. Hence, $\mathfrak{N}_i \cap \mathfrak{K} \neq 1$. If $N_{\mathfrak{G}}(\mathfrak{N}_i \cap \mathfrak{K}) \subseteq \mathfrak{N}_i$, then by a well known property of nilpotent groups, we have $\mathfrak{K} = \mathfrak{N}_i \cap \mathfrak{K}$, so that $\mathfrak{M} \subseteq \mathfrak{N}_i$, which is not the case. Hence, $N_{\mathfrak{G}}(\mathfrak{N}_i \cap \mathfrak{K}) \not\subseteq \mathfrak{N}_i$, so $\mathfrak{N}_i$ is not of type III or IV; $\mathfrak{N}_i$ is of type II.

Let a be the least common multiple of the orders of all elements of $\hat{\mathfrak{L}}$. We will show that $(a, |\mathfrak{K}|) = (a, |\mathfrak{H}_i|) = 1, 1 \leqq i \leqq s$. If $\mathfrak{L}$ is of type I, then $\mathfrak{L}$ is a Frobenius group, so a divides $|\mathfrak{U}|$, and we only need to verify that $\mathfrak{L}$ is not conjugate to $\mathfrak{M}$ or $\mathfrak{N}_i, 1 \leqq i \leqq s$. As none of the groups $\mathfrak{M}, \mathfrak{N}_1, \cdots, \mathfrak{N}_s$ is a Frobenius group, this is clear. Suppose $\mathfrak{L}$ is of type III of IV, so that $\mathfrak{L} = \mathfrak{H}\mathfrak{U}\mathfrak{W}_1$, $\hat{\mathfrak{L}} = \mathfrak{H}\mathfrak{U}$. Since none of $\mathfrak{M}, \mathfrak{N}_1, \cdots, \mathfrak{N}_s$ is of type III or IV, we have $(|\mathfrak{H}|, |\mathfrak{K}|) = (|\mathfrak{H}|, |\mathfrak{H}_i|) = 1, 1 \leqq i \leqq s$. Since $N_{\mathfrak{G}}(\mathfrak{U}) \subseteq \mathfrak{L}$, it is trivial that $(|\mathfrak{U}|, |\mathfrak{K}|) = (|\mathfrak{U}|, |\mathfrak{H}_i|) = 1$.

We appeal to Lemma 10.4 and conclude that λ^r is rational on $\mathfrak{K}$ and on every supporting subgroup of $\hat{\mathfrak{M}}$.

Let $\mathfrak{H}_i$ be a supporting subgroup of $\hat{\mathfrak{M}}$ and let α be a character of $\mathfrak{H}_i$ with $(\alpha, 1_{\mathfrak{H}_i}) = 0$. Let μ_1, μ_2 be irreducible characters of $\mathfrak{N}_i$ with $\mu_{1|\mathfrak{H}_i} = \mu_{2|\mathfrak{H}_i} = \alpha$. Then $\|(\mu_1 - \mu_2)^*\|^2 = 2$ and no irreducible character of $\mathfrak{G}$ appearing in $(\mu_1 - \mu_2)^*$ is rational on $\mathfrak{H}_i$. Thus, $(\lambda^r, (\mu_1 - \mu_2)^*) = 0$. If $\mathfrak{N}_i$ is of type I, then Hypothesis 10.2 is satisfied with our present $\hat{\mathfrak{M}}$ in the role of $\mathfrak{L}$. If $\mathfrak{N}_i$ is of type II, then a complement to $\mathfrak{H}_i$ in $\mathfrak{N}_i'$ is abelian, and again Hypothesis 10.2 is satisfied. Hence, by Lemma 10.2, λ^r is constant on the cosets of $\mathfrak{H}_i$ in $\mathfrak{N}_i - \mathfrak{H}_i$, and in particular is constant on all the sets $\mathfrak{A}_M, M \in \hat{\mathfrak{M}}$. As $\mathscr{M}$ is assumed coherent, an appeal to Lemma 10.5 completes the proof of this lemma.

Theorem 33.1 will now be proved by showing that Hypothesis 33.1 leads to a contradiction.

Choose $P \in \mathfrak{P}_0^\sharp$ and $K \in C(P) \cap \mathfrak{R}^\sharp$. By Lemmas 33.1 and 33.4

$$\lambda^r(KP) = \lambda^r(P) = \lambda(P) . \tag{33.2}$$

Let $\mathfrak{p}$ be a prime divisor of p in $\mathscr{O}_{|\mathfrak{G}|}$. By Lemma 4.2

$$\lambda^r(K) \equiv \lambda^r(PK) \pmod{\mathfrak{p}} \tag{33.3}$$

$$\lambda(P) \equiv \lambda(1) \pmod{\mathfrak{p}} . \tag{33.4}$$

Now (33.2), (33.3) and (33.4) yield that

$$\lambda^r(K) \equiv \lambda^r(PK) \equiv \lambda(P) \equiv \lambda(1) \pmod{\mathfrak{p}} .$$

By Lemma 10.4 $\lambda^r(K)$ is rational. Thus

$$\lambda^r(K) \equiv \lambda(1) \pmod{p} .$$

Since $\lambda(1) \leqq (p+1)/2$ by Lemma 33.3, we get that

$$|\lambda^r(K)| \geqq \lambda(1) - 1 \quad \text{for } K \in \mathfrak{R}^\sharp, \quad C_{\mathfrak{P}_0}(K) \neq 1 . \tag{33.5}$$

If every element in $\mathfrak{R}^\sharp$ commutes with an element of $\mathfrak{P}_0^\sharp$ then (33.5) implies that

$$|\lambda^r(K)| \geqq \lambda(1) - 1 \quad \text{for } K \in \mathfrak{R}^\sharp . \tag{33.6}$$

If not every element in $\mathfrak{R}^\sharp$ commutes with an element of $\mathfrak{P}_0^\sharp$ then λ^r is constant on $\mathfrak{R}^\sharp$ by Lemmas 28.2, 33.6 and 33.7. As (33.5) holds for at least one element in $\mathfrak{R}^\sharp$ we get that (33.6) holds in any case. Now Lemma 33.5 and (33.6) imply that

$$\frac{\lambda(1)^2}{|\mathfrak{L}|} > \frac{\{|\mathfrak{R}| - 1\}}{|\mathfrak{M}|} \{\lambda(1) - 1\}^2 .$$

This can be written as

$$\frac{|\mathfrak{M} : \mathfrak{R}|}{|\mathfrak{L}|} > \frac{\{|\mathfrak{R}| - 1\}}{|\mathfrak{R}|} \left(\frac{e-1}{e}\right)^2, \quad \text{where } e = \lambda(1) . \tag{33.7}$$

Since $|\mathfrak{L} : \mathfrak{L} \cap \mathfrak{M}| > 1$ and $\mathfrak{L} \cap \mathfrak{M}$ is a complement to $\mathfrak{R}$ in $\mathfrak{M}$, (33.7) yields that

$$\frac{1}{3} > \frac{\{|\mathfrak{R}| - 1\}}{|\mathfrak{R}|} \left(1 - \frac{1}{e}\right)^2 \geqq \frac{\{|\mathfrak{R}| - 1\}}{|\mathfrak{R}|} \left(\frac{2}{3}\right)^2 .$$

Hence $3|\mathfrak{R}|/4 > |\mathfrak{R}| - 1$ or $|\mathfrak{R}| < 4$. Thus $|\mathfrak{R}| = 3$ and a S_3-subgroup of $\mathfrak{G}$ is cyclic contrary to the simplicity of $\mathfrak{G}$ and the fact that $|\mathfrak{G}|$

is odd. This contradiction completes the proof of Theorem 33.1.

THEOREM 33.2. *$\mathfrak{G}$ contains a subgroup of type* II.

Proof. Suppose false. Then by Theorems 14.1 and 33.1, every maximal subgroup of $\mathfrak{G}$ is a Frobenius group. Let $\mathfrak{M}$ be a maximal subgroup of $\mathfrak{G}$ and let $\mathfrak{E}$ be a complement to the Frobenius kernel of $\mathfrak{M}$. We will show that $\mathfrak{E}$ is abelian. Suppose false.

Let σ be the set of primes p such that for some maximal subgroup $\mathfrak{M}_1$ with Frobenius kernel $\mathfrak{H}_1$ and complement $\mathfrak{E}_1$, a S_p-subgroup of $\mathfrak{E}_1$ is not in $Z(\mathfrak{E}_1)$. Let p be the least prime in σ. We may suppose that a S_p-subgroup $\mathfrak{P}$ of $\mathfrak{E}$ is not contained in $Z(\mathfrak{E})$. Then $\mathfrak{P} \cap \mathfrak{E}' = 1$. Let $\mathfrak{M}_1$ be a maximal subgroup of $\mathfrak{G}$ containing $N(\Omega_1(\mathfrak{P}))$. Since $\Omega_1(\mathfrak{P}) \subseteq Z(\mathfrak{E})$, $\mathfrak{E} \subseteq \mathfrak{M}_1$. If $\mathfrak{P}$ is contained in the Frobenius kernel $\mathfrak{R}$ of $\mathfrak{M}_1$, then so is $[\mathfrak{P}, \mathfrak{E}] \neq 1$. This is impossible as $\mathfrak{E}$ does not centralize $\mathfrak{P}$, while $\mathfrak{R}$ is nilpotent. Hence $\mathfrak{E} \cap \mathfrak{R} = 1$. Since $\mathfrak{M}_1'' \subseteq \mathfrak{R}$, it follows that $\mathfrak{P}$ is not contained in $\mathfrak{M}_1'$, and that a S_p-subgroup of $\mathfrak{M}_1$ is cyclic. Hence, by Burnside's transfer theorem, $\mathfrak{G}$ is not simple. Since this is not possible, $\mathfrak{E}$ is abelian.

Let $G \in \mathfrak{G}^\sharp$. Let $\mathfrak{M}$ be a maximal subgroup of $\mathfrak{G}$ containing $C(G)$. It follows that $C(G)$ is nilpotent. Hence, $\mathfrak{G}$ is solvable by the main theorem of [10]. The proof is complete.

34. The Subgroups $\mathfrak{S}$ and $\mathfrak{T}$

By Theorems 32.1 and 33.2 $\mathfrak{G}$ contains two subgroups $\mathfrak{S}$ and $\mathfrak{T}$, each of which is of type II, III or IV and which satisfy Condition (ii) (b) of Theorem 14.1. The following notation will be used throughout the rest of this chapter. This differs slightly from that introduced previously.

$$\mathfrak{S} = \mathfrak{Q}^*\mathfrak{S}', \quad \mathfrak{T} = \mathfrak{P}^*\mathfrak{T}', \quad |\mathfrak{Q}^*| = q, \quad |\mathfrak{P}^*| = p.$$

Thus p and q are both primes. Let $\mathfrak{P}$ be the S_p-subgroup of $\mathfrak{S}$ and let $\mathfrak{Q}$ be the S_q-subgroup of $\mathfrak{T}$. Then $\mathfrak{P}^* \subseteq \mathfrak{P}$, $\mathfrak{Q}^* \subseteq \mathfrak{Q}$. Let

$$\mathfrak{W} = \mathfrak{P}^*\mathfrak{Q}^*, \qquad \hat{\mathfrak{W}} = \mathfrak{W} - \mathfrak{P}^* - \mathfrak{Q}^*.$$

Let $\mathfrak{U}$ be a complement of $\mathfrak{P}$ in $\mathfrak{S}'$ and let $\mathfrak{V}$ be a complement of $\mathfrak{Q}$ in $\mathfrak{T}'$. By 3.16 (i) $\mathfrak{U}$ and $\mathfrak{V}$ are nilpotent, thus

$$\bigcup_{P \in \mathfrak{P}^\sharp} C(P) = \hat{\mathfrak{S}},$$

if $\mathfrak{S}$ is of type II and

$$\bigcup_{Q \in \mathfrak{Q}^\sharp} C(Q) = \hat{\mathfrak{T}},$$

if $\mathfrak{T}$ is of type II. Let

$$\mathfrak{C} = C_{\mathfrak{U}}(\mathfrak{P}), \qquad \mathfrak{D} = C_{\mathfrak{B}}(\mathfrak{Q}).$$

If $\mathfrak{S}$ is of type III or IV let $\mathfrak{U}^* = \mathfrak{U}$. If $\mathfrak{S}$ is of type II then a maximal subgroup $\mathfrak{M}$ which contains $N(\mathfrak{U})$ is not conjugate to $\mathfrak{T}$ since $\mathfrak{M}$ is not q-closed. Hence by Theorem 33.1 $\mathfrak{M}$ is a Frobenius group. Let $\mathfrak{U}^*$ be the Frobenius kernel of $\mathfrak{M}$. Thus $\mathfrak{U} \subseteq \mathfrak{U}^*$. Define $\mathfrak{V}^*$ similarly. Let

$$|\mathfrak{C}| = c, \quad |\mathfrak{D}| = d, \quad |\mathfrak{U}| = uc, \quad |\mathfrak{V}| = vd,$$
$$|\mathfrak{U}^*| = u^*c, \quad |\mathfrak{V}^*| = v^*d, \quad |\mathfrak{G}| = g.$$

$\mathscr{S}$ is the set of characters of $\mathfrak{S}$ which are induced by irreducible characters of $\mathfrak{S}'$ which do not have $\mathfrak{P}$ in their kernel.

$\mathscr{T}$ is the set of characters of $\mathfrak{T}$ which are induced by irreducible characters of $\mathfrak{T}'$ which do not have $\mathfrak{Q}$ in their kernel.

The set $\mathscr{S}$ as defined here is a subset of the $\mathscr{S}$ as defined in Section 29. Thus by Corollary 32.1.1 $\mathscr{S}$ and $\mathscr{T}$ are coherent.

$\mathscr{U}_0$, $\mathscr{V}_0$ are the sets of irreducible characters of $N(\mathfrak{U}^*)$, $N(\mathfrak{V}^*)$ respectively which do not have $\mathfrak{U}^*$, $\mathfrak{V}^*$ respectively in their kernel.

For $0 \leqq i \leqq q-1$, $0 \leqq j \leqq p-1$, η_{ij} are the generalized characters of $\mathfrak{G}$ defined by Lemma 13.1; μ_{ij} are the characters of $\mathfrak{S}$ defined by Lemma 13.3; ν_{ij} are the characters of $\mathfrak{T}$ defined by Lemma 13.3. For $0 \leqq j \leqq p-1$, ξ_j is the character of $\mathfrak{S}$ defined by Lemma 13.5. For $0 \leqq i \leqq q-1$, ζ_i is the character of $\mathfrak{T}$ defined by Lemma 13.5.

If $\mathfrak{G}_1 \subseteq \mathfrak{G}_2 \subset \mathfrak{G}$, where $\mathfrak{G}_2$ is a maximal subgroup of $\mathfrak{G}$ and if α is a class function of $\mathfrak{G}_1$ then $\tilde{\alpha}$ denotes the class function of $\mathfrak{G}_2$ induced by α. Whenever this notation is used $\mathfrak{G}_2$ will be uniquely determined by the context.

Throughout this section no distinction is made between $\mathfrak{S}$ and $\mathfrak{T}$. Any result in this section about one of these groups is automatically valid for the other by symmetry.

LEMMA 34.1. *Either*

$$u \Big| \frac{p^q - 1}{p - 1}$$

and $\mathfrak{U}/\mathfrak{C}$ is cyclic or $\mathfrak{U}/\mathfrak{C}$ is the product of at most $q-1$ cyclic groups and $u \mid (p-1)^{q-1}$. For $1 \leqq j \leqq p-1$ ξ_j is induced by a linear character of $\mathfrak{P}\mathfrak{C}$, $\xi_j(1) = uq$. Either $\mathfrak{P}\mathfrak{U}$ is a Frobenius group with $|\mathfrak{P}| = p^q$ and

$$u = \frac{p^q - 1}{p - 1}$$

or $\mathscr{S}$ contains an irreducible character of degree uq which is induced by a linear character of $\mathfrak{PC}$.

Proof. If $\mathfrak{P}^* \leqq \boldsymbol{D}(\mathfrak{P})$ then by 3.16(i) $\mathfrak{PU}/\boldsymbol{D}(\mathfrak{P})$ is nilpotent. Thus $\mathfrak{PU}$ is nilpotent contrary to assumption. Hence $\mathfrak{P}$ contains a subgroup $\mathfrak{P}_0$ such that $\mathfrak{P}^* \cap \mathfrak{P}_0 = 1$ and $\mathfrak{P}/\mathfrak{P}_0$ is a chief factor of $\mathfrak{S}$. Hence $\mathfrak{U}\mathfrak{Q}^*$ is represented on the elementary abelian group $\mathfrak{P}/\mathfrak{P}_0$. By 3.16 (i) $\mathfrak{P}_0\mathfrak{U}$ is nilpotent. Therefore $\mathfrak{U}\mathfrak{Q}^*/\mathfrak{C}$ is faithfully and irreducibly represented on $\mathfrak{P}/\mathfrak{P}_0$. By 3.16 (iii) $|\mathfrak{P} : \mathfrak{P}_0| = p^q$.

Let $\mathfrak{P}/\mathfrak{P}_0 = \mathfrak{P}_0\mathfrak{P}^*/\mathfrak{P}_0 \times \mathfrak{P}_1/\mathfrak{P}_0$, where $\mathfrak{Q}^* \leqq \boldsymbol{N}(\mathfrak{P}_1)$. By Lemma 4.6 (i) $\boldsymbol{N}_{\mathfrak{U}}(\mathfrak{P}_1) \leqq \boldsymbol{C}_{\mathfrak{U}}(\mathfrak{P}_1/\mathfrak{P}_0)$. Thus $\boldsymbol{N}_{\mathfrak{U}}(\mathfrak{P}_1) \leqq \boldsymbol{C}_{\mathfrak{U}}(\mathfrak{P}) = \mathfrak{C}$. Hence any non principal linear character of $\mathfrak{PC}/\mathfrak{P}_1\mathfrak{C}$ induces ξ_j for some j with $1 \leqq j \leqq p-1$. As p is a prime the characters ξ_j are algebraically conjugate for $1 \leqq j \leqq p-1$. Thus $\xi_j(1) = uq$ for $1 \leqq j \leqq p-1$. Let $\xi_j = \tilde{\psi}_j$ for ψ_j a linear character of $\mathfrak{PC}/\mathfrak{P}_1\mathfrak{C}$.

Suppose that $|\mathfrak{PC}: \boldsymbol{D}(\mathfrak{PC})| > p^q$. Then $\mathfrak{PC}$ contains a subgroup $\mathfrak{H} \neq \mathfrak{P}_0\mathfrak{C}$ such that $\mathfrak{PC}/\mathfrak{H}$ is a chief factor of $\mathfrak{S}$. Let λ be a non principal linear character of $\mathfrak{PC}/\mathfrak{H}$. Then $\psi_1\lambda$ induces an irreducible character of $\mathfrak{S}$ of degree uq.

Suppose that $\mathfrak{U}$ is represented reducibly on $\mathfrak{P}/\mathfrak{P}_0$. Since $\mathfrak{U} \lhd \mathfrak{U}\mathfrak{Q}^*$ the irreducible constituents of this representation all have the same dimension. This dimension is 1 since q is a prime. Thus $\mathfrak{U}/\mathfrak{C}$ is the direct product of k cyclic subgroups for some integer k, each of which has order dividing $(p-1)$. No element of $\mathfrak{U}/\mathfrak{C}$ is represented as a scalar as $\mathfrak{U}\mathfrak{Q}^*$ is a Frobenius group. Therefore $k < q$ and $u \mid (p-1)^{q-1}$. The irreducible constituents of the representation of $\mathfrak{U}/\mathfrak{C}$ on $\mathfrak{P}/\mathfrak{P}_0$ are distinct since $\mathfrak{U}\mathfrak{Q}^*$ is irreducibly represented on $\mathfrak{P}/\mathfrak{P}_0$. Let $\mathfrak{P}/\mathfrak{P}_0 = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_q$ where $\mathfrak{P}_{i+1} = Q^{-i}\mathfrak{P}_1 Q^i$ for some generator Q of $\mathfrak{Q}^*$ and such that $\mathfrak{U}$ normalizes each $\mathfrak{P}_i$. Let

$$P = \prod_{i=1}^{q} P_i$$

with $P_1 \in \mathfrak{P}_1^\sharp$, $P_2 = Q^{-1}P_1^{-1}Q$ and $Q^{-i}P_1Q^i = P_{i+1}$ for $2 \leqq i \leqq q \quad 1$. Suppose $U \in \mathfrak{U}$ and UQ^j centralizes P for some j. Let $U^{-1}P_iU \quad P_i^{a_i}$ then

$$P \quad (UQ^j)^{-1}P(UQ^j) = Q^{-j}\prod_{i=1}^{q} P_i^{a_i}Q^j .$$

Then $Q^{-j}P_2^{a_2}Q^j = P_{2+j}$. If $j \neq q$ then P_{2+j} is conjugate to P_1. Hence $P_2^{a_j}$ is conjugate to P_2^{-1} which is impossible as $|\mathfrak{U}\mathfrak{Q}|$ is odd. Therefore $j = q$. Then $U^{-1}P_iU = P_i$ for $1 \leqq i \leqq q$ and so $U \in \mathfrak{C}$. This proves that no element of $(\mathfrak{U}\mathfrak{Q}/\mathfrak{C})^\sharp$ leaves P fixed. Let μ_1 be a non principal linear character of $\mathfrak{P}/\mathfrak{P}_0$ with $\ker \mu_1 = \mathfrak{P}_2 \times \cdots \times \mathfrak{P}_q$. Let $\mu_i = \mu_1^{q^{i-1}}$; then $\mu = \mu_1\mu_2^{-1}\mu_3 \cdots \mu_q$ induces an irreducible character of $\mathfrak{S}$ of degree uq.

Assume now that $\mathfrak{U}$ is irreducibly represented on $\mathfrak{P}/\mathfrak{P}_0$. Then $\mathfrak{U}/\mathfrak{C}$ is cyclic since $\mathfrak{U}/\mathfrak{C}$ is abelian. If a subgroup of $\mathfrak{U}/\mathfrak{C}$ acts reducibly on $\mathfrak{P}/\mathfrak{P}_0$ then it is represented by scalar matrices. As $\mathfrak{U}\Omega^*$ is a Frobenius group every non identity subgroup of $\mathfrak{U}/\mathfrak{C}$ acts irreducibly on $\mathfrak{P}/\mathfrak{P}_0$. Thus $\mathfrak{U}/\mathfrak{C}$ permutes the subgroups of order p in $\mathfrak{P}/\mathfrak{P}_0$ and no element of $(\mathfrak{U}/\mathfrak{C})^*$ leaves any such subgroup fixed. Hence

$$u \Big| \frac{p^q - 1}{p - 1}.$$

Suppose now that $\mathscr{S}$ contains no irreducible character of degree uq. By an earlier part of the lemma this implies that $|\mathfrak{P}\mathfrak{C} : \boldsymbol{D}(\mathfrak{P}\mathfrak{C})| = p^q$. Thus $\mathfrak{C} = 1$ and $|\mathfrak{P} : \boldsymbol{D}(\mathfrak{P})| = p^q$. Since $\boldsymbol{D}(\mathfrak{P}) \cap \mathfrak{P}^* = 1$, we must have $\boldsymbol{D}(\mathfrak{P}) = \mathfrak{P}'$. By 3.16 (i) $\mathfrak{P}'\mathfrak{U}$ is nilpotent. If $\mathfrak{P}' \neq 1$ then there exists a subgroup $\mathfrak{P}_1$ of $\mathfrak{P}'$ such that $|\mathfrak{P}' : \mathfrak{P}_1| = p$. Hence $\mathfrak{P}'/\mathfrak{P}_1$ is the center of $\mathfrak{P}/\mathfrak{P}_1$ since $\mathfrak{U}$ acts irreducibly on $\mathfrak{P}/\mathfrak{P}'$. Thus $\mathfrak{P}/\mathfrak{P}_1$ is an extra special p-group. This implies that q is even which is not the case. Thus $\mathfrak{P}' = 1$. Hence $\mathfrak{P}\mathfrak{U}$ is a Frobenius group. Consequently $\mathfrak{P}\mathfrak{U}$ contains $(p^q - 1)/u$ irreducible characters of degree u. Lemma 13.7 now implies that

$$u = \frac{p^q - 1}{p - 1}.$$

LEMMA 34.2. *Either* $\mathfrak{P}\mathfrak{U}$ *is a Frobenius group with* $|\mathfrak{P}| = p^q$ *and*

$$u = \frac{p^q - 1}{p - 1}$$

or $\Omega\mathfrak{B}$ *is a Frobenius group with* $|\Omega| = q^p$ *and*

$$v = \frac{q^p - 1}{q - 1}.$$

Proof. If the result is false then Lemma 34.1 implies that $\mathscr{S}$ contains an irreducible character λ of degree uq and $\mathscr{T}$ contains an irreducible character θ of degree vp. Every character in $\mathscr{T}^{\mathfrak{r}}$ is rational valued on $\mathfrak{P}$ by Lemma 10.4. Since $|\mathfrak{G}|$ is odd this implies that every generalized character of weight 1 in $\mathscr{S}^{\mathfrak{r}}$ is orthogonal to $\mathscr{T}^{\mathfrak{r}}$. Define

$$\alpha = \lambda - \xi_1, \quad \beta = \theta - \zeta_1.$$

Then $\alpha(1) = \beta(1) = 0$ and $(\alpha^{\mathfrak{r}}, \beta^{\mathfrak{r}}) = 0$. Thus

$$0 = (\lambda^{\mathfrak{r}} - \xi_1^{\mathfrak{r}}, \theta^{\mathfrak{r}} - \zeta_1^{\mathfrak{r}}) = \Big(\pm \sum_{i=0}^{q-1} \eta_{i1}, \pm \sum_{j=0}^{p-1} \eta_{1j}\Big)$$
$$= \pm(\eta_{11}, \eta_{11}) = \pm 1.$$

This proves the lemma.

LEMMA 34.3. *For* $1 \leqq j \leqq p-1$

$$\sum_{x \in (\mathfrak{P}\mathfrak{C})^\#} |\eta_{0j}(X)|^2 \geqq uc|\mathfrak{P}| - u^2 .$$

Proof. Since $\mathfrak{P}\mathfrak{C}$ is a T.I. set in $\mathfrak{G}$ and $\mathscr{S}$ is coherent the Frobenius reciprocity theorem implies that for $1 \leqq j \leqq p-1$

$$\eta_{0j}(X) = \varepsilon(\mu_{0j}(X) + \alpha(X)) \quad \text{for } X \in (\mathfrak{P}\mathfrak{C})^\# ,$$

where α is a generalized character of $\mathfrak{S}'/\mathfrak{P}$, and $\varepsilon^2 = 1$. Therefore

$$\sum_{(\mathfrak{P}\mathfrak{C})^\#} |\eta_{0j}(X)|^2 = \sum_{(\mathfrak{P}\mathfrak{C})^\#} \{\mu_{0j}(X)\overline{\alpha(X)} + \overline{\mu_{0j}(X)}\alpha(X)\} + \sum_{(\mathfrak{P}\mathfrak{C})^\#} |\mu_{0j}(X)|^2 + \sum_{(\mathfrak{P}\mathfrak{C})^\#} |\alpha(X)|^2 .$$

This implies that

$$\sum_{(\mathfrak{P}\mathfrak{C})^\#} |\eta_{0j}(X)|^2 = -2\mu_{0j}(1)\alpha(1) + cu|\mathfrak{P}| - u^2 + |\mathfrak{P}| \sum_{\sigma \in \mathfrak{C}} |\alpha(C)|^2 - \alpha(1)^2 . \tag{34.1}$$

By Lemma 34.1, $2u + 1 \leqq |\mathfrak{P}|$, thus

$$\begin{aligned} -2\mu_{0j}(1)\alpha(1) + |\mathfrak{P}| \sum_{\mathfrak{C}} |\alpha(C)|^2 - \alpha(1)^2 &\geqq |\mathfrak{P}| \sum_{\mathfrak{C}} |\alpha(C)|^2 - (2u+1)\alpha(1)^2 \\ &\geqq |\mathfrak{P}| \sum_{\mathfrak{C}^\#} |\alpha(C)|^2 \geqq 0 . \end{aligned}$$

The result now follows from (34.1).

LEMMA 34.4. *For* $1 \leqq i \leqq q-1$

$$\sum_{x \in \mathfrak{P}\mathfrak{C}-\mathfrak{C}} |\eta_{i0}(X)|^2 \geqq \{|\mathfrak{P}| - 1\} c .$$

Proof. Since $\mathfrak{P}\mathfrak{C}$ is a T.I. set in $\mathfrak{G}$ the coherence of $\mathscr{S}$ and the Frobenius reciprocity theorem imply that $\eta_{i0}(X) = \alpha(X)$ for $X \in \mathfrak{P}\mathfrak{C} - \mathfrak{C}$, where α is a generalized character of $\mathfrak{S}'/\mathfrak{P}$. Therefore for $1 \leqq i \leqq q-1$

$$\begin{aligned} \sum_{x \in \mathfrak{P}\mathfrak{C}-\mathfrak{C}} |\eta_{i0}(X)|^2 &= \sum_{x \in \mathfrak{P}\mathfrak{C}-\mathfrak{C}} |\alpha(X)|^2 \\ &= \{|\mathfrak{P}| - 1\} \sum_{\mathfrak{C}} |\alpha(C)|^2 . \end{aligned} \tag{34.2}$$

If $P \in \mathfrak{P}^{*\#}$, $Q \in Q^{*\#}$ and q is a prime divisor of q in $\mathscr{C}_{pq}$ then by Lemma 4.2

$$\eta_{i0}(P) \equiv \eta_{i0}(PQ) \equiv 1 \pmod{q} .$$

Thus the expression in (34.2) is non zero. The result now follows from the fact that

$$\sum_{\mathfrak{C}} |\alpha(C)|^2 \equiv 0 \pmod{c} .$$

LEMMA 34.5. *Suppose that $\mathscr{S}$ contains an irreducible character λ of degree uq which is induced by a character of $\mathfrak{P}\mathfrak{C}$. Then*

$$\sum_{x \in (\mathfrak{P}\mathfrak{C})^\#} |\lambda^r(X)|^2 > uqc\,|\mathfrak{P}| - (uq)^2 - 2uq^2 .$$

Proof. As $\mathfrak{P}\mathfrak{C}$ is a T.I. set in $\mathfrak{G}$ the coherence of $\mathscr{S}$ and the Frobenius reciprocity theorem imply that

$$\lambda^r(X) = \lambda(X) + \alpha(X) \quad \text{for } X \in (\mathfrak{P}\mathfrak{C})^\# ,$$

for some generalized character α of $\mathfrak{S}'/\mathfrak{P}$. Therefore

$$\begin{aligned} \sum_{(\mathfrak{P}\mathfrak{C})^\#} |\lambda^r(X)|^2 &= \sum_{(\mathfrak{P}\mathfrak{C})^\#} |\lambda(X)|^2 + \sum_{(\mathfrak{P}\mathfrak{C})^\#} \{\lambda(X)\alpha(\overline{X}) + \lambda(\overline{X})\alpha(X)\} \\ &\quad + \sum_{(\mathfrak{P}\mathfrak{C})^\#} |\alpha(X)|^2 \geqq uqc\,|\mathfrak{P}| - (uq)^2 - 2\lambda(1)\alpha(1) \\ &\quad + \{|\mathfrak{P}| - 1\} \sum_{\mathfrak{C}} |\alpha(C)|^2 + \sum_{\mathfrak{C}^\#} |\alpha(C)|^2 . \end{aligned} \tag{34.3}$$

If $|\alpha(1)| \geqq q$ then by Lemma 34.1

$$2\lambda(1)|\alpha(1)| = 2uq|\alpha(1)| \leqq 2u\alpha(1)^2 \leqq \{|\mathfrak{P}| - 1\}\alpha(1)^2 .$$

Hence the result follows from (34.3) in this case. If $|\alpha(1)| < q$ then $2\lambda(1)|\alpha(1)| < 2uq^2$ thus (34.3) also implies the result in this case.

LEMMA 34.6. *Let $\mathfrak{G}_0$ be the set of elements in $\mathfrak{G}$ which are not conjugate to any element of $\mathfrak{P}\mathfrak{C}$, $\mathfrak{Q}$ or $\hat{\mathfrak{W}}$. Suppose that $\mathscr{S}$ contains an irreducible character λ of degree uq. Define*

$$\begin{aligned} \mathfrak{A}_1 &= \{G \mid G \in \mathfrak{G}_0,\ \lambda^r(G) \neq 0\} \\ \mathfrak{A}_2 &= \{G \mid G \in \mathfrak{G}_0,\ \eta_{10}(G) \neq 0\} \\ \mathfrak{A}_3 &= \{G \mid G \in \mathfrak{G}_0,\ \eta_{01}(G) \neq 0,\ \eta_{01}(G) \equiv 0 \pmod{(q-1)}\} . \end{aligned}$$

Then

$$\mathfrak{G}_0 = \mathfrak{A}_1 \cup \mathfrak{A}_2 \cup \mathfrak{A}_3 .$$

Proof. Suppose that $G \in \mathfrak{G}_0 - (\mathfrak{A}_1 \cup \mathfrak{A}_2)$. Let $\alpha = \xi_1 - \lambda$. Then $(\xi_1 - \lambda)^r(G) = 0$ and

$$(\xi_1 - \lambda)^r = \pm \sum_{i=0}^{q-1} \eta_{i1} - \lambda^r .$$

Since $G \in \mathfrak{G}_0$, $\eta_{i1}(G)$ is rational. Thus $\eta_{i1}(G) = \eta_{11}(G)$ for $1 \leqq i \leqq q-1$. As $G \notin \mathfrak{A}_1 \cup \mathfrak{A}_2$ we must have that

$$0 \equiv \sum_{i=0}^{q-1} \eta_{i1}(G) \equiv \eta_{01}(G) + (q-1)\eta_{11}(G) \equiv \eta_{01}(G) \pmod{(q-1)}. \tag{34.4}$$

Suppose that $\eta_{01}(G) = 0$. Then since $\alpha^r(G) = 0$ we must have that $\eta_{i1}(G) = 0$ for $0 \leqq i \leqq q-1$. Hence by Lemma 13.1

$$0 = (1_{\mathfrak{G}} - \eta_{10} - \eta_{01} + \eta_{11})(G) = 1 - \eta_{10}(G)$$

contradicting the fact that $G \notin \mathfrak{A}_2$. Hence $\eta_{01}(G) \neq 0$ and by (34.4) $G \in \mathfrak{A}_3$ as required.

LEMMA 34.7.

(i) *If* $q \geqq 5$ *then* $|\mathfrak{P}| = p^q$ *and* $u/c > 9p^{q-1}/20q$.

(ii) *If* $p, q \geqq 5$ *then* $c = 1$ *and* $u \geqq (13/20)\, p^{q-1}/q$.

(iii) *If* $p = 3$ *and* $c \neq 1$ *then* $u = 121$, $q = 5$, $c = 11$.

(iv) *If* $q = 3$ *then* $c = 1$ *or* $c = 7$. *Furthermore* $u > (p^2 + p + 1)/13$.

(v) *If* $q = 3$ *then* $\mathfrak{P}$ *is an elementary abelian p-group and* $|\mathfrak{P}| = p^3$ *or* $p = 7$, $c = 1$ *and* $|\mathfrak{P}| = 7^4$.

(vi) *If* $q = 3$ *and* $c = 7$ *then* $u > (p^2 + p + 1)/2$.

Proof. If $\mathfrak{P}\mathfrak{U}$ is a Frobenius group with $|\mathfrak{P}| = p^q$, $u = (p^q - 1)/(p-1)$ then all the statements in the lemma are immediate. Suppose that this is not the case. Then by Lemma 34.1 $\mathscr{S}$ contains an irreducible character λ which is induced by a linear character of $\mathfrak{P}\mathfrak{C}$. By Lemma 34.2 $\mathfrak{Q}\mathfrak{B}$ is a Frobenius group with $|\mathfrak{Q}| = q^p$, $v = (q^p - 1)/(q-1)$, $d = 1$.

$\mathfrak{P}\mathfrak{C}$, $\mathfrak{Q}$ and $\hat{\mathfrak{B}}$ are T.I. sets. Let $\mathfrak{G}_0, \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3$ have the same meaning as in Lemma 34.6. Then

$$\begin{aligned}\frac{1}{g}|\mathfrak{G}_0| &= 1 - \left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) \\ &\quad - \frac{1}{quc|\mathfrak{P}|}\{|\mathfrak{P}|c - 1\} - \frac{1}{pv|\mathfrak{Q}|}\{|\mathfrak{Q}| - 1\} \\ &= \frac{1}{p} + \frac{1}{q} - \frac{1}{pq} - \frac{1}{qu} - \frac{1}{pv} + \frac{1}{quc|\mathfrak{P}|} + \frac{1}{pvq^p}.\end{aligned} \tag{34.5}$$

Since λ^r is rational valued on $\mathfrak{G}_0$ by Lemma 10.4, Lemma 34.5 implies that

$$\begin{aligned}\frac{1}{g}|\mathfrak{A}_1| &\leqq \frac{1}{g}\sum_{\mathfrak{A}_1}|\lambda^r(X)|^2 \leqq 1 - \frac{1}{|\mathfrak{P}|ucq}\sum_{(\mathfrak{P}\mathfrak{C})^\#}|\lambda^r(X)|^2 \\ &< \frac{uq}{|\mathfrak{P}|c} + \frac{2q}{|\mathfrak{P}|c}.\end{aligned} \tag{34.6}$$

If Lemma 34.3 is applied to $\mathfrak{T}$ then Lemmas 13.1 and 34.4 yield that

$$\begin{aligned}\frac{1}{g}|\mathfrak{A}_2| &\leqq \frac{1}{g}\sum_{\mathfrak{A}_2}|\eta_{10}(X)|^2 \\ &\leqq 1-\left(1-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq}\right)-\frac{1}{pvq^p}\{vq^p-v^2\}-\frac{1}{|\mathfrak{P}|uqc}\{|\mathfrak{P}|-1\}c \\ &= \frac{1}{q}-\frac{1}{pq}+\frac{v}{pq^p}-\frac{1}{uq}+\frac{1}{|\mathfrak{P}|uq}.\end{aligned} \tag{34.7}$$

Lemmas 13.1 and 34.3 also imply that

$$\begin{aligned}\frac{1}{g}|\mathfrak{A}_3| &\leqq \frac{1}{(q-1)^2}\frac{1}{g}\sum_{\mathfrak{A}_3}|\eta_{01}(X)|^2 \\ &\leqq \frac{1}{(q-1)^2}\left\{1-\left(1-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq}\right)\right. \\ &\qquad\left.-\frac{1}{quc|\mathfrak{P}|}(uc|\mathfrak{P}|-u^2)\right\} \\ &= \frac{1}{(q-1)^2}\left\{\frac{(q-1)}{pq}+\frac{u}{qc|\mathfrak{P}|}\right\}.\end{aligned} \tag{34.8}$$

Lemma 34.6 and (34.5), (34.6), (34.7) and (34.8) now imply that

$$\begin{aligned}\frac{1}{p}+\frac{1}{quc|\mathfrak{P}|}-\frac{1}{pvq^p}(q^p-1)+\frac{1}{q}-\frac{1}{pq}-\frac{1}{qu} &\leqq \frac{uq}{|\mathfrak{P}|c} \\ &+\frac{2q}{|\mathfrak{P}|c}+\frac{1}{|\mathfrak{P}|uq}+\frac{v}{pq^p}+\frac{1}{q}-\frac{1}{pq}-\frac{1}{qu} \\ &+\frac{1}{pq(q-1)}+\frac{u}{qc|\mathfrak{P}|(q-1)^2}.\end{aligned}$$

Since $v=(q^p-1)/(q-1)$, this can be simplified to

$$\begin{aligned}\frac{1}{p} &\leqq \frac{(u+2)q}{|\mathfrak{P}|c}+\frac{(c-1)}{|\mathfrak{P}|quc}+\frac{1}{p(q-1)}-\frac{1}{pq^p(q-1)} \\ &\quad+\frac{(q-1)}{pq^p}+\frac{1}{pq(q-1)}+\frac{u}{qc|\mathfrak{P}|(q-1)^2} \\ &= \frac{(u+2)q}{|\mathfrak{P}|c}+\frac{(c-1)}{|\mathfrak{P}|quc}+\frac{u}{qc|\mathfrak{P}|(q-1)^2} \\ &\quad+\frac{(q+1)}{pq(q-1)}+\frac{(q-1)^2-1}{pq^p(q-1)}.\end{aligned} \tag{34.9}$$

By Lemma 34.1 $u \leqq (p^q - 1)/(p-1)$ and $|\mathfrak{P}| \geqq p^q$; thus (34.9) implies that

$$\frac{1}{p} \leqq \frac{(u+2)q}{|\mathfrak{P}|\,c} + \frac{(q+1)}{pq(q-1)} + \frac{1}{c(p-1)\,q(q-1)^2} + \frac{1}{p^q q} + \frac{1}{pq^{p-1}}. \tag{34.10}$$

Let $|\mathfrak{P}| = p^q x$ then

$$x \equiv c \equiv 1 (\mathrm{mod}\, 2q)\,. \tag{34.11}$$

Suppose first that $p, q \geqq 5$. Then (34.10) implies that

$$\frac{1}{p} \leqq \frac{uq}{p^q xc} + \frac{2q}{p^q xc} + \frac{3}{10p} + \frac{1}{80(p-1)} + \frac{2}{5^4 p}.$$

Hence by (5.2)

$$\frac{1}{p} < \frac{uq}{p^q xc} + \frac{1}{40p} + \frac{3}{10p} + \frac{3/2}{80p} + \frac{1/2}{80p}.$$

Therefore

$$\frac{q}{xc}\frac{u}{p^q} > \frac{13}{20p}. \tag{34.12}$$

Therefore

$$\frac{1}{xc}u > \frac{13p^{q-1}}{20q} > \frac{p^{q-1}}{2q}. \tag{34.13}$$

Suppose that $cx \neq 1$. Then by (34.11) $cx > 2q$. Thus (34.12) implies that

$$\frac{13}{20p} < \frac{1}{2}\frac{u}{p^q} < \frac{1}{2}\frac{1}{(p-1)}.$$

Thus $13(p-1) < 10p$ or $3p < 13$ which is not the case. Hence $c = x = 1$ and (34.13) completes the proof of statement (ii) of the lemma.

Suppose now that $p = 3$. Hence (34.10) yields that

$$\frac{1}{3} \leqq \frac{(u+2)q}{cx3^q} + \frac{(q+1)}{3q(q-1)} + \frac{1}{2q(q-1)^2} + \frac{1}{3^q q} + \frac{1}{3q^3}. \tag{34.14}$$

As $q \geqq 5$ this implies that

$$\frac{1}{3} \leqq \frac{q}{cx}\frac{u}{3^q} + \frac{1}{10} + \frac{1}{160} + \frac{(2q^2+1)}{3^q q} + \frac{1}{75}.$$

Hence by (5.3)

$$\frac{q}{cx}\frac{u}{3^q} \geqq \frac{1}{3} - \frac{1}{10} - \frac{1}{160} - \frac{1}{20} - \frac{1}{75}$$
$$> \frac{160 - 48 - 3 - 24 - 10}{480} = \frac{75}{480} > \frac{3}{20}.$$

Thus

$$\frac{u}{cx} > \frac{3}{20} \cdot \frac{3^q}{q}. \tag{34.15}$$

This yields that

$$\frac{2q}{cx} > \frac{9}{10} \cdot \frac{3^{q-1}}{u} > \frac{3}{5}.$$

Hence $4q > cx$.

Assume that $cx \neq 1$. Then (34.11) implies that

$$cx = 2q + 1. \tag{34.16}$$

Suppose first then $q \geqq 11$. Then (34.14) implies that

$$\frac{1}{3} \leqq \frac{q}{cx}\frac{u}{3^q} + \frac{2}{55} + \frac{1}{2.10^3} + \frac{1}{10.3^{10}} + \frac{2q}{cx}\frac{1}{3^{10}} + \frac{1}{300}.$$

Hence

$$\frac{q}{cx}\frac{u}{3^q} > \frac{1}{3} - \frac{2}{55} - \frac{1}{60} > \frac{1}{3} - \frac{3}{54} = \frac{5}{18}.$$

Therefore

$$\frac{q}{cx} > \frac{3^q}{u}\frac{5}{18} > \frac{2.5}{18} > \frac{1}{2}$$

contrary to (34.16). Suppose that $q = 7$. Then $cx = 15$ by (34.16). Thus $x = 3$ and $c = 5$ since x is a power of 3 and $(c, 3) = 1$. This contradicts (34.11). Hence $q = 5$. Thus by (34.16) $cx = 11$. Hence $x = 1$ and $c = 11$ since x is a power of 3. Thus statement (i) of the lemma follows from (34.15) and statement (ii). If $c \neq 1$ then $q = 5$ and $c = 11$. By (34.15)

$$u > \frac{11.3^5}{100} > 2^4 = (p-1)^{q-1}. \tag{34.17}$$

Hence by Lemma 34.1 $u \mid (3^5 - 1)/2 = 121$. Thus $u = 121$ by (34.17). This completes the proof of statement (iii) of the lemma.

Assume now that $q = 3$. Let $y = (p^2 + p + 1)/u$. (y is not necessarily integral) Then (34.9) implies that

$$\frac{1}{p} < \frac{3(p^2+p+1)}{cxyp^3} + \frac{6}{cxp^3} + \frac{1}{3p^3u} + \frac{(p^2+p+1)}{12cxyp^3} + \frac{2}{3p} + \frac{1}{2p3^{p-1}}.$$

Therefore

$$\frac{1}{3p} < \frac{37(p^2+p+1)}{12cxyp^3} + \frac{6}{cxp^3} + \frac{1}{3p^3u} + \frac{1}{2p3^{p-1}},$$

or

$$1 < \frac{37(p^2+p+1)}{4cxyp^2} + \frac{18}{cxp^2} + \frac{1}{p^2u} + \frac{1}{2\cdot 3^{p-2}}. \tag{34.18}$$

Suppose that $cxy \geqq 13$. Then (34.18) implies that

$$\frac{37}{52}\frac{(p^2+p+1)}{p^2} > 1 - \frac{19}{p^2} - \frac{1}{52}.$$

Therefore $37(p^2+p+1) > 51p^2 - 52\cdot 19$, or

$$14p^2 - 37p - 52\cdot 19 - 37 < 0.$$

Therefore, $p < 11$. Hence $p = 5$ or $p = 7$. Since $(6, u) = 1$, Lemma 34.1 now implies that $u \mid p^2+p+1$. Thus $u \mid 31$ if $p = 5$ and $u \mid 57$ if $p = 7$. Hence one of the following must occur:

$$p = 5, \quad u = 31, \quad y = 1, \quad cx \geqq 13$$

or

$$p = 7, \quad u = 19, \quad y = 3, \quad cx \geqq 5.$$

By (34.11)

$$cx = 7, \quad p = 7 \text{ or } cx \geqq 13.$$

If $cx \geqq 13$ then by (34.18)

$$1 < \frac{37}{52}\frac{(p^2+p+1)}{p^2} + \frac{19}{13p^2} + \frac{1}{52}.$$

Hence $p < 5$, which is not the case. Therefore we have shown that either $cxy < 13$ or $p = 7, u = 19, y = 3$ and $cx = 7$. If $cxy < 13$, then $y < 13$, and by (34.11) $cx = 7$ or $cx = 1$. Thus in any case

$$u > \frac{p^2+p+1}{13}, cx = 1 \text{ or } cx = 7. \tag{34.19}$$

This proves statement (iv) of the lemma.

If $x \neq 1$ then (34.19) implies that $c = 1$ and $x = 7$, hence $p = 7$ and $|\mathfrak{P}| = 7^4$. Since $(u, 6) = 1$, Lemma 34.1 implies that $u \mid 57$, thus $u = 19$. If $\boldsymbol{D}(\mathfrak{P}) \neq 1$ then $\mathfrak{U}$ acts irreducibly on $\mathfrak{P}/\boldsymbol{D}(\mathfrak{P})$ and centralizes $\boldsymbol{D}(\mathfrak{P})$. If $\mathfrak{P}$ is non abelian this implies that $\boldsymbol{D}(\mathfrak{P}) = \boldsymbol{Z}(\mathfrak{P})$. Hence $\mathfrak{P}$ is an extra special p-group contrary to the fact that $|\mathfrak{P}:\boldsymbol{D}(\mathfrak{P})| = p^3$. Thus $\mathfrak{P}$ is abelian. Hence $|\mathfrak{P}:\Omega_1(\mathfrak{P})| \leqq p$. If $\Omega_1(\mathfrak{P}) \neq \mathfrak{P}$ this implies that $\mathfrak{U}\mathfrak{Q}$ is represented on $\Omega_1(\mathfrak{P})$ and so $\mathfrak{U}$ acts irreducibly on $\Omega_1(\mathfrak{P})$ contrary to $\boldsymbol{D}(\mathfrak{P}) \subseteqq \Omega_1(\mathfrak{P})$ and $\mathfrak{U} \subseteqq \boldsymbol{C}(\boldsymbol{D}(\mathfrak{P}))$. Thus $\mathfrak{P}$ is elementary abelian. Statement (v) of the lemma is proved.

Suppose that $c = 7$ and $y \geqq 2$; then (34.18) implies that

$$1 < \frac{37}{56}\frac{(p^2 + p + 1)}{p^2} + \frac{19}{7p^2} + \frac{1}{54}.$$

Therefore, $p < 5$ which is impossible. Hence if $c = 7$ then $y < 2$. This proves statement (vi) of the lemma and completes the proof of Lemma 34.7.

LEMMA 34.8. *If $q \geqq 5$ then $\mathfrak{P}\mathfrak{U}/\mathfrak{C}$ is a Frobenius group and $u \mid (p^q - 1)/(p - 1)$.*

Proof. By Lemma 34.7 (i) $|\mathfrak{P}| = p^q$. Thus if $\mathfrak{P}\mathfrak{U}/\mathfrak{C}$ is not a Frobenius group then by Lemma 34.1 $u \mid [(p - 1)/2]^{q-1}$. Thus by Lemma 34.7 (i)

$$\frac{p^{q-1}}{2^{q-1}} > u > \frac{9 \cdot p^{q-1}}{20q}.$$

Therefore $q > 2^{q-3} \cdot (9/10)$ which is not the case, since $q \geqq 5$.

LEMMA 34.9. *If $p, q \geqq 5$ then $c = 1$, $|\mathfrak{P}| = p^q$ and either $u = (p^q - 1)/(p - 1)$ or $p \equiv 1 \pmod{q}$ and $u = 1/q\,[(p^q - 1)/(p - 1)]$.*

Proof. By Lemma 34.7(ii) $c = 1$. Lemma 34.8 implies that $|\mathfrak{P}| = p^q$ and $u \mid (p^q - 1)/(p - 1)$. Let $ux = (p^q - 1)/(p - 1)$. If $p \not\equiv 1 \pmod{q}$ then

$$u \equiv \frac{p^q - 1}{p - 1} \equiv 1 \pmod{2q}.$$

Thus $x \equiv 1 \pmod{2q}$. If $p \equiv 1 \pmod{q}$ then $(p^q - 1)/(p - 1) \equiv 0 \pmod{q}$. Hence $x \equiv 0 \pmod{q}$ as $(u, q) = 1$. Thus in any case $x \geqq 2q$ if the result is false. Now Lemma 34.7 (ii) implies that

$$\frac{p^q - 1}{p - 1} = ux \geqq 2qu \geqq \frac{13}{10}\,p^{q-1}.$$

Hence

$$p^q > p^q - 1 \geqq \frac{13}{10} p^q - \frac{13}{10} p^{q-1} .$$

Thus $13 > 3p$ contrary to the fact that $p \geqq 5$.

LEMMA 34.10.

$$\begin{aligned} |N(\mathfrak{V}^*):\mathfrak{V}^*C(\mathfrak{V}^*)| &= p \text{ or } pq && \text{if } p, q \geqq 5 \text{ or } p = 3, q \geqq 7 \\ &= 3 \text{ or } 15 \text{ or } 33 && \text{if } p = 3, q = 5 \\ &= p, 3p \text{ or } 7p && \text{if } q = 3. \end{aligned}$$

Proof. Let $\mathfrak{E}$ be a complement of $\mathfrak{V}^*C(\mathfrak{V}^*)$ in $N(\mathfrak{V}^*)$ which contains $\mathfrak{P}^*$. Every Sylow subgroup of $\mathfrak{E}$ is cyclic and every subgroup of prime order is normal in $\mathfrak{E}$ by 3.16 (ii) and Theorem 33.1. Thus $\mathfrak{E} \subseteqq N(\mathfrak{P}^*) = \mathfrak{Q}^*\mathfrak{P}\mathfrak{C}$. Hence $\mathfrak{E} = \mathfrak{P}^*$ or $|\mathfrak{E}| = pq$ or $\mathfrak{E} \subseteqq \mathfrak{P}^*\mathfrak{C}$. The result now follows from Lemma 34.7.

By Theorem 33.1 $\mathfrak{U}^*$ is tamely imbedded in $\mathfrak{G}$ unless $\mathfrak{U}^* = \mathfrak{U}$ and $C_{\mathfrak{P}}(\mathfrak{U}) \neq 1$. By Lemma 34.7 this can only happen if $p = 7$ and $q = 3$. In that case let $\mathscr{U}$ be the set of characters of $\mathfrak{S}$ which are induced by non principal irreducible characters of $\mathfrak{S}'/\mathfrak{P}$. In all other cases let $\mathscr{U}_0 = \mathscr{U}$. Define $\mathscr{V}$ similarly. Then $\mathscr{I}_0(\mathscr{U})^r$ and $\mathscr{I}_0(\mathscr{V})^r$ are always defined.

LEMMA 34.11. *Suppose that $\mathscr{V}$ is coherent and $p > q$. If*

$$\frac{dv^* - 1}{|N(\mathfrak{V}^*):\mathfrak{V}^*|} > \frac{v - 1}{p}$$

and

$$\frac{dv^* - 1}{|N(\mathfrak{V}^*):\mathfrak{V}^*|} > \frac{u - 1}{q}$$

then $|N(\mathfrak{V}^*):\mathfrak{V}^*| \geqq pq$. If furthermore $|N(\mathfrak{V}^*):\mathfrak{V}^*| = pq$ then $1/p \leqq pq/v^*d$.

Proof. Let $e = |N(\mathfrak{V}^*):\mathfrak{V}^*|$. Let $\psi \in \mathscr{V}$ with $\psi(1) = e$. Let $\alpha = \tilde{1}_{\mathfrak{V}^*} - \psi$. Then $\|\alpha^r\|^2 = \|\alpha\|^2 = e + 1$. Define

$$\beta_{\mathfrak{S}} = \tilde{1}_{\mathfrak{Q}^*\mathfrak{P}\mathfrak{C}} - \mu_{01} , \quad \beta_{\mathfrak{T}} = \tilde{1}_{\mathfrak{P}^*\mathfrak{Q}\mathfrak{D}} - \nu_{10} .$$

$\beta_{\mathfrak{S}}, \beta_{\mathfrak{T}}$ vanish on $\mathfrak{S} - \hat{\mathfrak{S}}_1, \mathfrak{T} - \hat{\mathfrak{T}}_1$ respectively. As $\hat{\mathfrak{S}}_1$ and $\hat{\mathfrak{T}}_1$ are T.I. sets in $\mathfrak{G}$

$$(34.20) \quad \|\beta_{\mathfrak{S}}^*\|^2 = \|\beta_{\mathfrak{S}}\|^2 = \frac{u - 1}{q} + 2 , \quad \|\beta_{\mathfrak{T}}^*\|^2 = \|\beta_{\mathfrak{T}}\|^2 = \frac{v - 1}{p} + 2 .$$

Furthermore by Lemma 13.8

$$(34.21) \qquad \beta_{\mathfrak{S}}^* = 1_{\mathfrak{G}} \pm \eta_{01} + \Gamma_{\mathfrak{S}} , \qquad \beta_{\mathfrak{T}}^* = 1_{\mathfrak{S}} \pm \eta_{10} + \Gamma_{\mathfrak{T}}$$

where $\Gamma_{\mathfrak{S}}, \Gamma_{\mathfrak{T}}$ are real valued generalized characters of $\mathfrak{G}$ which are orthogonal to $1_{\mathfrak{G}}$. The assumed inequalities and (34.20) imply that $(\psi^r, \beta^*_{\mathfrak{S}}) = 0 = (\psi^r, \beta^*_{\mathfrak{T}})$. Thus if $\alpha^r = 1_{\mathfrak{G}} \pm \psi^r + \Gamma_{\mathfrak{B}}$ then

$$0 \equiv (\alpha^r, \beta^*_{\mathfrak{S}}) \equiv 1 + (\eta_{01}, \Gamma_{\mathfrak{B}}) \pmod 2$$
$$0 \equiv (\alpha^r, \beta^*_{\mathfrak{T}}) \equiv 1 + (\eta_{10}, \Gamma_{\mathfrak{B}}) \pmod 2 .$$

Since $\Gamma_{\mathfrak{B}}$ is rational valued on $\hat{\mathfrak{W}}$ this implies that

$$(\eta_{i0}, \Gamma_{\mathfrak{B}}) \equiv (\eta_{0j}, \Gamma_{\mathfrak{B}}) \equiv 1 \pmod 2$$

for $1 \leqq i \leqq q-1$, $1 \leqq j \leqq p-1$. Hence by Lemma 13.1

$$(1_{\mathfrak{G}} - \eta_{i0} - \eta_{0j} + \eta_{ij}, \alpha^r) \equiv 1 + (\eta_{i0}, \Gamma_{\mathfrak{B}}) + (\eta_{0j}, \Gamma_{\mathfrak{B}}) + (\eta_{ij}, \Gamma_{\mathfrak{B}}) \pmod 2 .$$

Thus $(\eta_{ij}, \Gamma_{\mathfrak{B}}) \neq 0$ for $1 \leqq i \leqq q-1$, $1 \leqq j \leqq p-1$. Hence

$$e + 1 = \| \alpha^r \|^2 \geqq pq + 1 .$$

Suppose now that $e = pq$ then

$$\alpha^r = 1_{\mathfrak{G}} \pm \psi^r \pm \sum_{i=1}^{q-1} \eta_{i0} \pm \sum_{j=1}^{p-1} \eta_{0j} \pm \sum_{i=1}^{q-1} \sum_{j=1}^{p-1} \eta_{ij} . \tag{34.22}$$

Let $\mathfrak{G}_0$ be the set of elements in $\mathfrak{G}$ which are conjugate to some element of $\mathfrak{A}_V$ with $V \in \mathfrak{V}^{*\sharp}$. Since $\mathscr{Y}$ is coherent by assumption, (34.22) Lemmas 33.1 and 9.4 imply that $\psi^r(VC) = \psi(V)$ for $VC \in \mathfrak{A}_V$, $V \in \mathfrak{V}^{*\sharp}$. Furthermore Lemma 9.5 and (34.22) imply that

$$\frac{1}{g} \sum_{\mathfrak{G}_0} |\psi^r(G)|^2 = \frac{1}{pqv^*d} \sum_{\mathfrak{V}^{*\sharp}} |\psi(G)|^2 = 1 - \frac{pq}{v^*d} . \tag{34.23}$$

By Lemma 9.5

$$\frac{1}{g} |\mathfrak{G}_0| = \frac{1}{g} \sum_{\mathfrak{G}_0} 1_{\mathfrak{G}}(G) = \frac{1}{pqv^*d} \sum_{\mathfrak{V}^{*\sharp}} 1_{\mathfrak{G}}(G) = \frac{(dv^* - 1)}{dv^*pq} . \tag{34.24}$$

Let $\mathfrak{G}_1$ be the set of elements in $\mathfrak{G} - \mathfrak{G}_0$ which are not conjugate to any element of $\hat{\mathfrak{W}}$, $\mathfrak{PC}$ or $\mathfrak{QD}$. Now (34.22) implies that if $G \in \mathfrak{G}_1$ then $\psi^r(G)$ is rational and

$$0 \equiv \alpha^r(G) \equiv 1 + \psi^r(G) \pmod 2 .$$

Thus $|\psi^r(G)|^2 \geqq 1$ for $G \in \mathfrak{G}_1$. Hence (34.23) implies that

$$\frac{pq}{v^*d} \geqq \frac{1}{g} |\mathfrak{G}_1| \geqq 1 - \frac{(vd^* - 1)}{pqv^*d} - \left(1 - \frac{1}{p} - \frac{1}{q} + \frac{1}{pq}\right) - \frac{|\mathfrak{PC}| - 1}{qu\,|\mathfrak{P}|c} - \frac{|\mathfrak{QD}| - 1}{pv\,|\mathfrak{Q}|d} .$$

Therefore

$$\frac{pq}{v^*d} \geqq \frac{1}{p} + \frac{1}{q} - \frac{1}{pq} - \frac{1}{pq} + \frac{1}{pqv^*d} - \frac{1}{qu} + \frac{1}{qu\,|\,\mathfrak{P}\,|\,c} - \frac{1}{pv} + \frac{1}{pv\,|\,\mathfrak{Q}\,|\,d}.$$

Since $u > 2q$, $v > 2p$ and $p > q \geqq 3$

$$\frac{1}{pq} + \frac{1}{pq} + \frac{1}{qu} + \frac{1}{pv} < \frac{3}{q^2} \leqq \frac{1}{q};$$

thus the required inequality follows.

LEMMA 34.12. *If* $\mathfrak{U}^*$ *is cyclic then* $\mathfrak{U}^*$ *is a* T.I. *set in* $\mathfrak{G}$ *unless* $\mathfrak{U}^* = \mathfrak{U}$ *and* $N(\mathfrak{U}) \subseteqq \mathfrak{S}$.

Proof. Since $\mathfrak{U}^*$ is a cyclic S-subgroup in $N(\mathfrak{U}^*)$, $\mathfrak{U}^*$ is a S-subgroup of $\mathfrak{G}$. Suppose that $\mathfrak{U}^*$ is not a T.I. set in $\mathfrak{G}$ and let $1 \neq \mathfrak{U}^* \cap G^{-1}\mathfrak{U}^*G = \mathfrak{U}_0 \subseteqq \mathfrak{U}^*$. Then $\{N(\mathfrak{U}^*), N(G^{-1}\mathfrak{U}^*G)\} \subseteqq N(\mathfrak{U}_0)$. Since $N(\mathfrak{U}^*)$ is a maximal subgroup of $\mathfrak{G}$ this implies that $\{\mathfrak{U}^*, G^{-1}\mathfrak{U}^*G\} \subseteqq N(\mathfrak{U}^*)$. Thus $G^{-1}\mathfrak{U}^*G = \mathfrak{U}^*$ and $\mathfrak{U}^*$ is a T.I. set in $\mathfrak{G}$.

35. Further Results About $\mathfrak{S}$ and $\mathfrak{T}$

The notation of Section 34 is used in this section. However we will destroy the symmetry of $\mathfrak{S}$ and $\mathfrak{T}$ by choosing the notation so that

$$q < p. \tag{35.1}$$

The next three lemmas are restatements of Lemmas 34.7, 34.8, 34.9 and 34.10.

LEMMA 35.1. *If* $q \geqq 5$ *then* $c = d = 1$, $v = (q^p - 1)/(q - 1)$, $|\,\mathfrak{P}\,| = p^q$ *and* $|\,\mathfrak{Q}\,| = q^p$. *Either* $u = (p^q - 1)/(p - 1)$ *or* $p \equiv 1 \pmod{q}$ *and* $u = 1/q\,[(p^q - 1)/(p - 1)]$. *Furthermore* $\mathfrak{P}\mathfrak{U}$ *and* $\mathfrak{Q}\mathfrak{V}$ *are Frobenius groups.*

$$|\,N(\mathfrak{U}^*) : \mathfrak{U}^*\,| = q \text{ or } pq \text{ and } |\,N(\mathfrak{V}^*) : \mathfrak{V}^*\,| = p \text{ or } pq.$$

LEMMA 35.2. *Suppose that* $q = 3$. *Then* $|\,\mathfrak{Q}\,| = 3^p$,

$$\frac{v}{d} > \frac{9}{20} \cdot \frac{3^{p-1}}{p}$$

and $\mathfrak{Q}\mathfrak{V}/\mathfrak{D}$ *is a Frobenius group with* $v\,|\,(3^p - 1)/2$. *Either* $d = 1$ *or* $d = 11$, $p = 5$ *and* $v = 121$. *Furthermore* $\mathscr{Y} = \mathscr{Y}_0$ *and*

$$|\,N(\mathfrak{V}^*) : \mathfrak{V}^*\,| = p, 3p \text{ or } 7p.$$

LEMMA 35.3. *Suppose that* $q = 3$. *Then*

$$|N(\mathfrak{U}^*):\mathfrak{U}^*C(\mathfrak{U}^*)| = 3 \text{ or } 3p \quad \text{if } p \geqq 7$$
$$= 3, 15 \text{ or } 33 \quad \text{if } p = 5 .$$

Furthermore one of the following possibilities occurs:

(i) $c = 1, u > (p^2+p+1)/13$, $\mathfrak{P}$ *is an elementary abelian* p*-group with* $|\mathfrak{P}| = p^3$ *or* $|\mathfrak{P}| = 7^4$.

(ii) $c = 7, u > (p^2+p+1)/2$, $\mathfrak{P}$ *is an elementary abelian* p*-group with* $|\mathfrak{P}| = p^3$.

LEMMA 35.4. *Either* $q = 3, p = 5, v = 11, u = 31$ *or*

$$\frac{v-1}{p} > \frac{u-1}{q} .$$

Proof. By (5.12)

$$q^2\frac{(q^{p-1}-1)}{q-1} > p^2\frac{(p^{q-1}-1)}{p-1} .$$

Therefore if $v = (q^p-1)/(q-1)$ then by Lemma 34.1

$$\frac{v-1}{p} = \frac{1+\cdots+q^{p-1}-1}{p} = \frac{q(q^{p-1}-1)}{p(q-1)}$$
$$> \frac{p(p^{q-1}-1)}{q(p-1)} = \frac{\dfrac{p^q-1}{p-1}-1}{q} \geqq \frac{u-1}{q} .$$

Suppose now that $v \neq (q^p-1)/(q-1)$. Then $q = 3$ by Lemma 35.1. By Lemma 35.2 $v \mid (3^p-1)/2$ and $v > 9/20\cdot(3^{p-1}/p)$. Thus if $(v-1)/p \leqq (u-1)/q$ then by Lemma 34.2

$$\frac{\dfrac{9}{20}\cdot\dfrac{3^{p-1}}{p}-1}{p} \leqq \frac{p^2+p}{3} .$$

Hence $p < 11$. Thus $p = 5$ or $p = 7$. If $p = 7$ then $v \mid (3^7-1)/2 = 1093$. As 1093 is a prime this implies that $v = (3^7-1)/2$ and the result follows from the first part of the lemma. If $p = 5$ then $v \mid (3^5-1)/2 = 121$. Thus $v = 11$ and $u \mid 31$. Thus $u = 31$. The proof is complete.

LEMMA 35.5. $\mathscr{Y}$ *is coherent.*

Proof. Suppose that $\mathscr{Y}$ is not coherent. Then by Lemma 11.2 v^*d is a power of some prime r. As $\mathfrak{B}/\mathfrak{D}$ is cyclic $r \equiv 1 \pmod{p}$. Thus

$$r > 2p > 2q \,. \tag{35.2}$$

Let $|\mathfrak{V}^* : D(\mathfrak{V}^*)| = r^n$, then $n \geqq 3$ by Lemma 11.3. By Lemma 11.1

$$r^n \leqq 4\,|N(\mathfrak{V}^*) : \mathfrak{V}^*|^2 + 1 \,. \tag{35.3}$$

Suppose that $|N(\mathfrak{V}^*) : \mathfrak{V}^*| = 7p$. Then $p \neq 7$ and (35.2) and (35.3) imply that $r^n \leqq 200p^2 \leqq 50r^2$. If $n \geqq 4$ this yields that $r \leqq 7$. Then $p = 3$ by (35.2) which is not the case as $p > q$. Hence $n = 3$. Thus Lemma 11.4 implies that $r^3 \leqq 2r(7p) + 1$. Hence by (35.2) $r^2 \leqq 14p < 7r$ and so $r < 7$ which is impossible.

By Lemmas 35.1 and 35.2 we may assume now that $|N(\mathfrak{V}^*) : \mathfrak{V}^*| \leqq pq$. Thus (35.2) and (35.3) imply that

$$r^n \leqq 4p^2q^2 + 1 < (2p)^4 < r^4 \,,$$

thus $n = 3$. Hence Lemma 11.4 implies that

$$r^3 \leqq 2rpq + 1 < \frac{r^3}{2} \,.$$

This completes the proof in all cases.

LEMMA 35.6. *$d = 1$. If $|N(\mathfrak{V}^*) : \mathfrak{V}^*| \leqq pq$ then $v^* = v$ or $p = 5$, $q = 3$, $v = 11$, $v^* = 121$.*

Proof. If $|N(\mathfrak{V}^*) : \mathfrak{V}^*| > pq$ then $c \neq 1$. Hence $d = 1$ by Lemma 34.2. Assume now that $|N(\mathfrak{V}^*) : \mathfrak{V}^*| \leqq pq$.

Assume first that $d \neq 1$. By Lemmas 35.1 and 35.2 $d = 11$, $q = 3$, $p = 5$ and $v = 121$. By Lemma 34.2 $u = (5^3 - 1)/(5 - 1) = 31$. Thus

$$\frac{dv^* - 1}{|N(\mathfrak{V}^*) : \mathfrak{V}^*|} \geqq \frac{11^3 - 1}{15} > \frac{11^2 - 1}{5} = \frac{v - 1}{p}$$

and

$$\frac{dv^* - 1}{|N(\mathfrak{V}^*) : \mathfrak{V}^*|} \geqq \frac{11^3 - 1}{15} > \frac{31 - 1}{3} = \frac{u - 1}{q} \,.$$

Hence by Lemmas 35.5 and 34.11 $1/p \leqq pq/v^*d$.
Thus

$$11^3 \leqq v^*d \leqq p^2q = 75 \,.$$

Therefore $d = 1$.

Assume now that $q = 3$, $p = 5$, $v = 11$, $u = 31$. Let $v^* = vx$. $x \equiv 1 \pmod{10}$ as $v \equiv v^* \equiv 1 \pmod{10}$. If $v^* \neq 11$ and $v^* \neq 121$, then $x \geqq 21$. Thus $v^* \geqq 21.11$.

$$\frac{v^*-1}{|N(\mathfrak{V}^*):\mathfrak{V}^*|} \geqq \frac{21.11-1}{15} > \frac{11-1}{5} = \frac{v-1}{p}$$

and

$$\frac{v^*-1}{|N(\mathfrak{V}^*):\mathfrak{V}^*|} \geqq \frac{21.11-1}{15} > \frac{31-1}{3} = \frac{u-1}{q}.$$

Thus Lemmas 35.5 and 34.11 imply that $1/p \leqq pq/v^*$. Thus $21.11 \leqq v^* \leqq p^2q = 75$ which is not the case. Therefore $v = v^* = 11$ or $v^* = 121$, and we are done in this case.

By Lemma 35.4 it may now be assumed that $(v-1)/p > (u-1)/q$. If $v^* = vx$, then $x \equiv 1 \pmod{2p}$ since $v^* \equiv v \equiv 1 \pmod{2p}$. Thus

$$v^* = xv,\ x > 2p > 2q \quad \text{if } x \neq 1. \tag{35.4}$$

Therefore

$$\frac{v^*-1}{|N(\mathfrak{V}^*):\mathfrak{V}^*|} \geqq \frac{v^*-1}{pq} > \frac{2vq-1}{pq} > \frac{v-1}{p} > \frac{u-1}{q}.$$

Hence by Lemmas 35.5 and 34.11 $1/p < pq/v^*$. Hence (35.4) and Lemmas 35.1 and 35.2 imply that

$$q^{p-1} < \frac{20}{9}pv \leqq \frac{10}{9}v^* \leqq \frac{10}{9}p^2q.$$

Thus $q^{p-2} < 2p^2$. Hence $p < 7$ by (5.4). Thus $p = 5$. Hence $x \geqq 11$, $q = 3$ and $v \mid 121$. By assumption $v \neq 11$, hence $v = 121$. Thus $11^3 \leqq v^* \leqq p^2q = 75$. This completes the proof in all cases.

LEMMA 35.7.

$$|N(\mathfrak{U}^*):\mathfrak{U}^*C(\mathfrak{U}^*)| = q \text{ or } pq.$$

Proof. This follows directly from Lemmas 35.1, 35.2, 35.3 and 35.6.

THEOREM 35.1. *If $N(\mathfrak{U}^*)$ is conjugate to $N(\mathfrak{V}^*)$ then the conclusions of Theorem 27.1 hold.*

Proof. By Lemma 35.6 if $\mathfrak{V}^* \neq \mathfrak{V}$ then $p = 5$, $q = 3$ and $v^* = 121$. Thus $u = 31$. Hence u does not divide v^*. Thus by Lemmas 35.1 and 35.2, $\mathfrak{V}^* = \mathfrak{V}$ is cyclic. By Theorem 33.1 $N(\mathfrak{V}^*)$ is a Frobenius group with Frobenius kernel $\mathfrak{V}^*$. Hence by Lemma 34.12 $\mathfrak{V}^*$ is a T.I. set in $\mathfrak{G}$. Since $\mathfrak{D}^* \subseteq N(\mathfrak{U}^*)$ and $p \mid\mid N(\mathfrak{V}^*):\mathfrak{V}^*|$ Lemma 35.7 implies that $N(\mathfrak{U}^*)/\mathfrak{U}^*$ is a cyclic group of order pq. Thus condition (iv) of Theorem 27.1 holds. Since $\mathfrak{V}^*$ is cyclic so is $\mathfrak{U}$. Thus $\mathfrak{C}$ char $\mathfrak{U}$. Hence if $\mathfrak{C} \neq 1$ then $N(\mathfrak{U}) \subseteq \mathfrak{S}$ which is not the case. Hence

$c = 1$. By Lemma 35.6 $d = 1$. Thus $C(\mathfrak{Q}^*) = \mathfrak{Q}\mathfrak{P}^*$ and $C(\mathfrak{P}^*) = \mathfrak{P}\mathfrak{Q}^*$. Hence condition (iii) of Theorem 27.1 holds. If $|\mathfrak{P}| \neq p^q$ or $|\mathfrak{Q}| \neq q^p$, then $N(\mathfrak{U}) \subseteq \mathfrak{S}$ or $N(\mathfrak{B}) \subseteq \mathfrak{T}$ respectively. This implies that $\mathfrak{P}$ is elementary abelian of order p^q and $\mathfrak{Q}$ is elementary abelian of order q^p. Hence condition (i) of Theorem 27.1 holds.

Since $\mathfrak{U}$ is cyclic and $\mathfrak{C} = 1$, $\mathfrak{P}\mathfrak{U}$ and $\mathfrak{U}\mathfrak{Q}^*$ are Frobenius groups and $N(\mathfrak{P})' = \mathfrak{S}' = \mathfrak{P}\mathfrak{U}$. Since $\mathfrak{U}^*$ is cyclic every divisor x of $|\mathfrak{U}^*|$ satisfies $x \equiv 1 \pmod{pq}$. Thus $(|\mathfrak{U}|, p-1) = 1$. Hence by Lemma 34.1 $|\mathfrak{U}| \,|\, (p^q - 1)/(p-1)$. Let $(p^q - 1)(p-1) = y|\mathfrak{U}|$. Suppose that $p \not\equiv 1 \pmod{q}$. Then $y \equiv 1 \pmod{pq}$ since

$$\frac{p^q - 1}{p-1} \equiv |\mathfrak{U}| \equiv 1 \pmod{pq} .$$

Thus if $y \neq 1$, then $y > 2pq$. Furthermore Lemma 35.1 implies that in this case $q = 3$. Thus by Lemma 35.3 (i)

$$13 > \frac{p^2 + p + 1}{|\mathfrak{U}|} = y > 2pq = 6p$$

which is impossible as $p > 3$. Thus $y = 1$ and so $|\mathfrak{U}| = (p^q - 1)/(p-1)$. Suppose that $p \equiv 1 \pmod{q}$. Then $q \,|\, (p^q - 1)/(p-1)$. Hence $u \,|\, 1/q\,[(p^q - 1)/(p-1)]$ since $(u, q) = 1$. As $q < p$ and $u \equiv (p^q - 1)/(p-1) \equiv 1 \pmod{p}$ we see that $u \neq 1/q\,[(p^q - 1)/(p-1)]$. Thus if $y \neq 1$, Lemma 35.1 yields that $q = 3$. Since $c = 1$, Lemma 35.3 (i) implies that $u > (p^2 + p + 1)/13$. This is impossible since $u \equiv 1 \pmod{3p}$. This verifies condition (ii) of Theorem 27.1 and completes the proof of the theorem.

36. The Proof of Theorem 27.1

In this section the study of the groups $\mathfrak{S}$ and $\mathfrak{T}$ is continued. All the lemmas in this section will be proved under the following assumption.

Hypothesis 36.1

(i) $q < p$.

(ii) $N(\mathfrak{U}^*)$ *is not conjugate to* $N(\mathfrak{B}^*)$.

The following notation is used in addition to that introduced in Section 34.

$$\phi \in \mathscr{U} , \quad \psi \in \mathscr{V}$$

and

$$\phi(1) = |N(\mathfrak{U}^*) : \mathfrak{U}^* C(\mathfrak{U}^*)| , \quad \psi(1) = |N(\mathfrak{B}^*) : \mathfrak{B}^*| .$$

If $\phi_i \in \mathscr{U}$ then $\phi_i^{\mathfrak{S}}$ is defined since $|\mathfrak{S}|$ is odd. Let $\mathscr{U}^{\mathfrak{T}} = \{\phi_i^{\mathfrak{S}} \mid \phi_i \in \mathscr{U}\}$. Then

$$(\tilde{1}_{\mathfrak{U}^*} - \phi)^\tau = 1_{\mathfrak{G}} - \phi^\tau + \Gamma_{\mathfrak{U}} + \Xi_{\mathfrak{U}}, \quad \text{if } \mathscr{U} = \mathscr{U}_0$$
$$(\tilde{1}_{\mathfrak{S}'} - \phi)^\tau = 1_{\mathfrak{G}} - \phi^\tau + \Gamma_{\mathfrak{U}} + \Xi_{\mathfrak{U}} \quad \text{if } \mathscr{U} \neq \mathscr{U}_0 \tag{36.1}$$

$$(\tilde{1}_{\mathfrak{B}^*} - \psi)^\tau = 1_{\mathfrak{G}} - \psi^\tau + \Gamma_{\mathfrak{B}} + \Xi_{\mathfrak{B}} \tag{36.2}$$

$$(\tilde{1}_{\mathfrak{P}\mathfrak{S}\mathfrak{Q}^*} - \mu_{0j})^* = 1_{\mathfrak{G}} \pm \eta_{0j} + \Gamma_{\mathfrak{P}} + \Xi_{\mathfrak{P}} \quad \text{for } 1 \leqq j \leqq p-1\,, \tag{36.3}$$

$$(\tilde{1}_{\mathfrak{Q}\mathfrak{P}^*} - \nu_{i0})^* = 1_{\mathfrak{G}} \pm \eta_{i0} + \Gamma_{\mathfrak{Q}} + \Xi_{\mathfrak{Q}} \quad \text{for } 1 \leqq i \leqq q-1\,, \tag{36.4}$$

where $\Xi_{\mathfrak{U}}, \Xi_{\mathfrak{B}}$ are in $\mathscr{S}(\mathscr{U}^\tau), \mathscr{S}(\mathscr{V}^\tau)$ respectively, $\Gamma_{\mathfrak{U}}, \Gamma_{\mathfrak{B}}$ are orthogonal to $\mathscr{U}^\tau, \mathscr{V}^\tau$ respectively. $\Xi_{\mathfrak{P}}, \Xi_{\mathfrak{Q}}$ are linear combinations of the generalized characters η_{st} and $\Gamma_{\mathfrak{P}}, \Gamma_{\mathfrak{Q}}$ are orthogonal to each η_{st}. Then $\Gamma_{\mathfrak{U}}, \Gamma_{\mathfrak{B}}, \Gamma_{\mathfrak{P}}$ and $\Gamma_{\mathfrak{Q}}$ are real valued generalized characters each of which is orthogonal to $1_{\mathfrak{G}}$. Thus

$$(\Gamma_{\mathfrak{U}}, \eta_{01}) + (\Gamma_{\mathfrak{P}}, \phi^\tau) \not\equiv 0 \pmod 2\,, \tag{36.5}$$

$$(\Gamma_{\mathfrak{B}}, \eta_{01}) + (\Gamma_{\mathfrak{B}}, \psi^\tau) \not\equiv 0 \pmod 2\,. \tag{36.6}$$

$$(\Gamma_{\mathfrak{U}}, \eta_{10}) + (\Gamma_{\mathfrak{Q}}, \phi^\tau) \not\equiv 0 \pmod 2\,. \tag{36.7}$$

It is a simple consequence of Lemma 13.1 that

$$(\Gamma_{\mathfrak{U}}, \eta_{01}) + (\Gamma_{\mathfrak{U}}, \eta_{10}) + (\Gamma_{\mathfrak{U}}, \eta_{11}) \not\equiv 0 \pmod 2\,. \tag{36.8}$$

$$(\Gamma_{\mathfrak{B}}, \eta_{01}) + (\Gamma_{\mathfrak{B}}, \eta_{10}) + (\Gamma_{\mathfrak{B}}, \eta_{11}) \not\equiv 0 \pmod 2\,. \tag{36.9}$$

By Hypothesis 36.1 (ii) $\mathscr{U}^\tau$ is orthogonal to $\mathscr{V}^\tau$. Thus

$$(\Gamma_{\mathfrak{U}}, \psi^\tau) + (\Gamma_{\mathfrak{B}}, \phi^\tau) \not\equiv 0 \pmod 2\,. \tag{36.10}$$

Since τ is an isometry (36.1), (36.2), (36.3) and (36.4) yield that

$$\|\Gamma_{\mathfrak{U}}\|^2 \leqq |N(\mathfrak{U}^*):\mathfrak{U}^* C(\mathfrak{U}^*)| - 1 \tag{36.11}$$

$$\|\Gamma_{\mathfrak{B}}\|^2 \leqq |N(\mathfrak{B}^*):\mathfrak{B}^*| - 1 \tag{36.12}$$

$$\|\Gamma_{\mathfrak{P}}\|^2 \leqq \frac{u-1}{q} \tag{36.13}$$

$$\|\Gamma_{\mathfrak{Q}}\|^2 \leqq \frac{v-1}{p}\,. \tag{36.14}$$

LEMMA 36.1. *$\mathscr{U}$ is coherent.*

Proof. If $\mathfrak{S}$ is of type IV then by Lemmas 35.2 and 35.3 $c = 1$ or 7 so by Lemma 11.1 the result follows from Theorem 29.1. If $\mathfrak{S}$ is of type III then $\mathfrak{U} = \mathfrak{U}^*$ is abelian and the result follows from Lemma 11.2. Suppose that $\mathscr{U}$ is not coherent. Then $\mathscr{U} = \mathscr{U}_0$ and by Lemma 11.2 $\mathfrak{U}^*$ is an r-group for some prime r. Furthermore $\mathfrak{S}$ is of type II. Let $e = |N(\mathfrak{U}^*):\mathfrak{U}^*|$ then by Lemmas 11.1, 11.3 and

11.4 $\mathfrak{U}^{*\prime} = D(\mathfrak{U}^*) \neq 1$,

(36.15) $$|\mathfrak{U}^*:\mathfrak{U}^{*\prime}| = r^n \quad \text{with } n \geqq 3\,,$$

(36.16) $$r^n \leqq 4e^2 + 1, n \geqq 4 \quad \text{or } r^3 \leqq 2re + 1 \text{ and } n = 3\,.$$

Suppose first that $\mathfrak{U}$ is not cyclic. Then by Lemma 35.1 $q = 3$. If $c \neq 1$, then by Lemma 35.3 $\mathfrak{C}$ is cyclic and

$$u > \frac{p^2 + p + 1}{2} > \left(\frac{p-1}{2}\right)^2.$$

Thus by Lemma 34.1 $\mathfrak{U}/\mathfrak{C}$ is cyclic. Hence $\mathfrak{U}$ is generated by two elements. If $c = 1$ then Lemma 34.1 implies that $\mathfrak{U}$ is generated by two elements. Thus $\mathfrak{U} \neq \mathfrak{U}^*$. As $\mathfrak{S}$ is of type II $\hat{\mathfrak{S}}$ is a T.I. set in $\mathfrak{G}$. Consequently there exists an element R of order r such that $\mathfrak{U} = C_{\mathfrak{U}^*}(R)$. Thus $Z(\mathfrak{U}^*)$ is cyclic. Hence $r \equiv 1 \pmod{e}$. This contradicts (36.15) and (36.16).

Suppose now that $\mathfrak{U}$ is cyclic. Thus $r \equiv 1 \pmod{q}$. By (36.16) $N(\mathfrak{U}^*)/\mathfrak{U}^*$ is irreducibly represented on $\mathfrak{U}^*/D(\mathfrak{U}^*)$. Thus $\mathfrak{Q}^*$ acts as a group of scalar matrices on $\mathfrak{U}^*/D(\mathfrak{U}^*)$. Hence by Lemma 6.4 $\mathfrak{U}^*$ has prime exponent. Since $\mathfrak{U}$ is a cyclic subgroup of $\mathfrak{U}^*$ this implies that

(36.17) $$|\mathfrak{U}| = r\,.$$

If $q > 3$ then Lemmas 35.1, 35.7 and (36.15) and (36.16) imply that

$$\left(\frac{p^{q-1}}{q}\right)^3 \leqq |\mathfrak{U}|^3 < 4e^2 + 1 \leqq 4p^2q^2 + 1\,.$$

Hence $p^{3q-5} \leqq 5q^5$ and so

$$5^{3q-10} \leqq q^{3q-10} < p^{3q-10} < 5\,.$$

Thus $3q - 10 < 1$ which is not the case.

Suppose that $q = 3$: If $n \geqq 4$ then (36.16) and Lemmas 35.3 and 35.7 imply that

$$\frac{(p^2 + p + 1)^4}{13^4} < |\mathfrak{U}|^4 \leqq 36p^2 + 1\,.$$

Hence

$$p^8 < (p^2 + p + 1)^4 < 13^4(36p^2 + 1) < 3.13^5p^2\,.$$

Thus $p^6 < 3.13^5$. Hence $p < 13$. If $n = 3$ then (36.16) and Lemmas 35.3 and 35.7 imply that

$$\frac{(p^2 + p + 1)^3}{13^3} < |\mathfrak{U}|^3 \leqq 6p\,.$$

Hence

$$p^4 < (p^2 + p + 1)^2 < 13^2 \cdot 6p < 13^3 p .$$

Therefore $p < 13$ in this case also. Thus $p = 5, 7$ or 11. By Lemma 34.1 and (36.17) either $|\mathfrak{U}| \,|\, (p-1)$ or $|\mathfrak{U}| \,|\, p^2 + p + 1$. If $|\mathfrak{U}| \,|\, (p-1)$ then $p = 11$ and $|\mathfrak{U}| = 5$ since $(|\mathfrak{U}|, 6) = 1$. However in this case

$$\frac{(p^2 + p + 1)}{13} > 10 > |\mathfrak{U}|$$

which is impossible by Lemma 35.1. Thus $|\mathfrak{U}| \,|\, p^2 + p + 1$. Hence by (36.17) if $p = 5$, $|\mathfrak{U}| = 31$, if $p = 7$, $|\mathfrak{U}| = 19$ and if $p = 11$ then $|\mathfrak{U}| = 7$ or $|\mathfrak{U}| = 19$. If $p = 5$ then (36.16) and (36.17) imply that

$$31^3 \leqq 36.25 + 1$$

which is not the case. If $p = 7$ then (36.16) and (36.17) imply that

$$19^3 < 36.49 + 1 < 1800 .$$

Thus $19^2 < 100$ which is not the case. If $p = 11$ and $|\mathfrak{U}| = 19$ then (36.16) and (36.17) imply that

$$15.360 < 19^3 < 36.121 + 1 < 4800$$

which is not the case.

Assume now that $p = 11$ and $|\mathfrak{U}| = r = 7$. Then (36.15) and (36.16) imply that

(36.18) $$7^n \leqq 36.11^2 + 1 , \quad 7^n \equiv 1 \pmod{11} .$$

Since

$$7^5 > 10^4 > 5000 > 36.11^2 + 1$$

we must have $n \leqq 4$. However

$$7^2 \equiv 5, 7^3 \equiv 2, 7^4 \equiv 3 \pmod{11}$$

contrary to (36.18). The proof is complete.

LEMMA 36.2. $q = 3$.

Proof. Suppose that $q \neq 3$. Then by (36.10) either $(\Gamma_{\mathfrak{U}}, \psi^\tau) \neq 0$ or $(\Gamma_{\mathfrak{B}}, \phi^\tau) \neq 0$. If $u = 1/q\,[(p^q - 1)/(p-1)]$, then $u \not\equiv 1 \pmod{p}$. Hence by Lemmas 35.1, 35.5 and 36.1,

$$\frac{\dfrac{q^p - 1}{q - 1} - 1}{pq} \leqq pq - 1 \quad \text{or} \quad \frac{\dfrac{p^q - 1}{p - 1} - q}{pq} \leqq pq - 1 .$$

Therefore by (5.11) $p^{q-1} < (p^q - 1)/(p-1) < p^2 q^2$. Hence $p^{q-3} < q^2 < p^3$

which is impossible for $q \geqq 5$.

LEMMA 36.3. *$c = 1$, $|N(\mathfrak{B}^*):\mathfrak{B}^*| = p$ or $3p$.*

Proof. If $c \neq 1$ then $c = 7$ and $u > (p^2 + p + 1)/2$ by Lemma 35.3. Since $[(p-1)/2]^2 < (p^2+p+1)/2$ Lemma 34.1 implies that $u \mid p^2 + p + 1$. Thus $u = p^2 + p + 1$. By Lemma 34.2 $v = (3^p - 1)/2$.

Suppose first that $|N(\mathfrak{U}^*):\mathfrak{U}^*| = 3$. Then by (36.8) $\Gamma_{\mathfrak{U}} = \pm(\eta_{10} + \eta_{20})$. Thus $(\Gamma_{\mathfrak{U}}, \eta_{01}) = 0$. Hence $(\Gamma_{\mathfrak{B}}, \phi^r) \neq 0$ by (36.5). Since $\mathscr{U}$ is coherent (36.13) implies that

$$\frac{7u^* - 1}{3} \leqq ||\Gamma_{\mathfrak{B}}||^2 \leqq \frac{u - 1}{3} \leqq \frac{u^* - 1}{3},$$

which is not the case.

Suppose now that $|N(\mathfrak{U}^*):\mathfrak{U}^*| \neq 3$. Then by Lemma 35.7 $|N(\mathfrak{U}^*):\mathfrak{U}^*| = 3p$. Let $cu^* = xu = x(1 + p + p^2)$. Then $x \equiv 1 \pmod{6p}$ since

$$cu^* \equiv u \equiv 1 \pmod{6p}.$$

As $1 < c \leqq x$ this implies that $x \geqq 6p + 1$. Hence by Lemma 35.2 and (36.12)

$$\frac{cu^* - 1}{3p} > \frac{6pu}{3p} \geqq 2u > 7p - 1 \geqq ||\Gamma_{\mathfrak{B}}||^2. \tag{36.19}$$

Since $\mathscr{U}$ is coherent this implies that $(\Gamma_{\mathfrak{B}}, \phi^r) = 0$. Thus by (36.10)

$$(\Gamma_{\mathfrak{U}}, \psi^r) \neq 0. \tag{36.20}$$

Since $\mathscr{U}$ is coherent (36.13) and (36.19) imply that $(\Gamma_{\mathfrak{B}}, \phi^r) = 0$. Thus by (36.5)

$$(\Gamma_{\mathfrak{U}}, \eta_{01}) \not\equiv 0 \pmod{2}. \tag{36.21}$$

Since $\mathscr{V}$ is coherent (36.11), (36.20) and (36.21) imply that

$$(p - 1) + \frac{v^* - 1}{|N(\mathfrak{B}^*):\mathfrak{B}^*|} \leqq 3p - 1.$$

Hence by Lemma 35.2

$$\frac{3^p - 1}{2} - 1 = v - 1 \leqq v^* - 1 \leqq 2p\,|N(\mathfrak{B}^*):\mathfrak{B}^*| \leqq 14p^2.$$

Therefore $3^p - 3 \leqq 28p^2$. Hence $p = 5$ by (5.5). Thus $u = 31$ and $v = 121$. If the S_7-subgroup of $\mathfrak{U}^*$ has order 7^n, then $7^n \equiv 1 \pmod 5$. Thus $n \geqq 4$. Therefore

$$\frac{u^* - 1}{3p} \geqq \frac{7^4.31 - 1}{15} > 24 = \frac{v - 1}{p} .$$

Thus the coherence of $\mathscr{Z}$ implies that $(\Gamma_{\mathfrak{Q}}, \phi^r) = 0$. Hence (36.7) yields that $(\Gamma_{\mathfrak{U}}, \eta_{10}) \not\equiv 0 \pmod 2$. Therefore (36.8), (36.11) and (36.21) imply that

$$\Gamma_{\mathfrak{U}} = \pm \sum_{i=1}^{q-1} \eta_{i0} \pm \sum_{j=1}^{p-1} \eta_{0j} \pm \sum_{i=1}^{q-1} \sum_{j=1}^{p-1} \eta_{ij}$$

contrary to (36.20). Thus $c = 1$ and consequently $|N(\mathfrak{B}^*) : \mathfrak{B}^*| = p$ or $3p$.

LEMMA 36.4. $|N(\mathfrak{U}^*) : \mathfrak{U}^* C(\mathfrak{U}^*)| = 3p$.

Proof. If the result is false then $|N(\mathfrak{U}^*) : \mathfrak{U}^* C(\mathfrak{U}^*)| = 3$ by Lemma 35.7. Thus (36.8) implies that $\Gamma_{\mathfrak{U}} = \pm(\eta_{10} + \eta_{20})$. Therefore by (36.5) and (36.10) $(\Gamma_{\mathfrak{B}}, \phi^r) \neq 0$ and $(\Gamma_{\mathfrak{B}}, \phi^r) \neq 0$. Since $u^* \geqq u$ (36.13) implies that $u^* = u$ and

$$\Gamma_{\mathfrak{B}} = \pm \sum_i \phi_i^r , \tag{36.22}$$

where ϕ_i ranges over $\mathscr{Z}$. Thus by (36.6) $(\Gamma_{\mathfrak{B}}, \eta_{01})$ is odd. Hence by Lemma 36.3 and (36.12)

$$\Gamma_{\mathfrak{B}} = b \sum \phi_i^r \pm \sum_{j=1}^{p-1} \eta_{0j} + \Delta_{\mathfrak{B}} ,$$

where b is odd and $\Delta_{\mathfrak{B}}$ is orthogonal to all ϕ_i^r, η_{0j}. Therefore by (36.22)

$$0 = (\widetilde{1}_{\mathfrak{B}\mathfrak{Q}^*} - \mu_{01})^*, (\widetilde{1}_{\mathfrak{B}^*} - \psi)^r) = 1 \pm 1 \pm b\frac{(u-1)}{3} .$$

Since $b \neq 0$ this implies that $|b|(u-1)/3 = 2$. Hence $u = 7$. Thus by Lemma 35.3 (i) $7 \geqq (p^2 + p + 1)/13$, hence $p < 10$. Hence $p = 5$ or $p = 7$. In either of these cases $u \mid (p^2 + p + 1)$ by Lemma 34.1 since $(u, 6) = 1$. Thus $7 \mid 31$ or $7 \mid 57$ which is not the case.

LEMMA 36.5. $|\mathfrak{P}| = p^q$.

Proof. If $|\mathfrak{P}| \neq p^q$ then $N(\mathfrak{U}) \subseteqq \mathfrak{S}$ as $\mathfrak{P}$ is a T.I. set in $\mathfrak{G}$. This contradicts Lemma 36.4.

LEMMA 36.6. $\mathfrak{U}$ *is cyclic.*

Proof. By Lemma 34.1 if $\mathfrak{U}$ is not cyclic then $\mathfrak{U} = \mathfrak{U}_1 \times \mathfrak{U}_2$, where each $\mathfrak{U}_i$ is cyclic and $|\mathfrak{U}_i| \,|\, (p-1)/2$. Let $|\mathfrak{U}_i| = (p-1)/2y_i$ for $i = 1, 2$. If $y_1 y_2 \geqq 4$ then Lemma 35.3 (i) implies that

$$\frac{p^2}{13} < \frac{p^2+p+1}{13} < \frac{(p-1)^2}{4y_1y_2} \leqq \frac{(p-1)^2}{16} < \frac{p^2}{16}$$

which is not the case. Thus $y_1y_2 < 4$. If $y_1y_2 = 2$ then $p \equiv 1 \pmod 4$ and so $|\mathfrak{U}| = (p-1)^2/8$ is even. If $y_1y_2 = 3$ then $p \equiv 1 \pmod 3$ and so $3 \mid u$ which is not the case. Thus $y_1y_2 = 1$ and $u = [(p-1)/2]^2$. Therefore $((p-1)/2, 6) = 1$. Thus $p \geqq 11$. Furthermore $u \equiv 1/4 \pmod p$. Since $u^* \equiv 1 \pmod p$ by Lemma 36.4 we have that $u^* = ux$ and $x \equiv 4 \pmod p$. By Lemma 34.2 $v = (3^p - 1)/2$. Hence Lemma 36.3 and (36.10), (36.11) and (36.12) imply that

$$\text{(36.23)} \qquad \frac{\frac{3^p-1}{2} - 1}{3p} \leqq 3p - 1 \quad \text{or} \quad \frac{u^* - 1}{3p} < 3p - 1 .$$

The first possibility implies that $3^p - 3 \leqq 18p^2 - 6p$. Thus $3^{p-2} \leqq 2p^2$. Hence $p < 7$ by (5.4). The second possibility in (36.23) yields that

$$\frac{(p-1)^2}{4} x - 1 \leqq 9p^2 - 3p .$$

Therefore

$$(p-1)^2 x \leqq 36p^2 - 12p + 4 < 36p^2 .$$

As $p \geqq 11$ this implies that

$$\text{(36.24)} \qquad x < 36\left(\frac{p}{p-1}\right)^2 = 36\left(1 + \frac{1}{p-1}\right)^2 \leqq 36\left(\frac{121}{100}\right) < 45 .$$

Let $x = 4 + zp$ for some integer z. Then since $p \geqq 11$ (36.24) yields that $z < 4$. Furthermore

$$\text{(36.25)} \qquad p < 41 ; \quad \text{if} \quad z \geqq 2 , \quad p < 20 ; \quad \text{if} \quad z = 3 , \quad p < 14 .$$

As $p < 41$ and $((p-1)/2, 6) = 1$, $p = 11$ or $p = 23$. If $p = 23$ then by (36.25) $x = 27$ which is impossible as $x \equiv 1 \pmod 3$. If $p = 11$, then $x = 15$, 26 or 37. As $x \equiv 1 \pmod 6$ this implies that $x = 37$. Then $u = 25$ and so $37 \equiv 1 \pmod{11}$ by Lemma 36.4 which is not the case.

LEMMA 36.7. *$u = p^2 + p + 1$ or $u = (p^2 + p + 1)/3$ or $u = (p^2 + p + 1)/7$.*

Proof. If $u \mid [(p-1)/2]^2$ then by Lemmas 34.1 and 36.6 $u \mid (p-1)/2$. Thus by Lemma 35.3 (i) $(p-1)/2 > (p^2 + p + 1)/13$. Hence $2p^2 - 11p + 15 < 0$ which implies that $p < 5$. Therefore by Lemma 34.1 $p^2 + p + 1 = uy$, y an integer. By Lemma 35.3 (i) $y < 13$. If r is a prime such that $p^2 + p + 1 \equiv 0 \pmod r$ then either $r = 3$ or

$r \equiv 1 \pmod 3$. Hence $y = 1, 3, 7$ or 9. If $y = 9$ then $p^2 + p + 1 \equiv 0 \pmod 9$. Hence $p \equiv 1 \pmod 3$. Thus $p \equiv 1, 4$ or $7 \pmod 9$. In none of these cases is $p^2 + p + 1 \equiv 0 \pmod 9$. Hence $y = 1, 3$ or 7.

LEMMA 36.8. $u = u^* = p^2 + p + 1$.

Proof. Let $u^* = ux$. Assume that $x \neq 1$. $u^* \equiv 1 \pmod{6p}$ by Lemma 36.4. If $u = p^2 + p + 1$, then $u \equiv u^* \equiv 1 \pmod{6p}$, thus $x \equiv 1 \pmod{6p}$ and so $x \geqq 1 + 6p$. If $u = (p^2 + p + 1)/3$, then $x \equiv 3 \pmod p$. Furthermore $x \equiv 1 \pmod 6$ since $u \equiv u^* \equiv 1 \pmod 6$ and $p \equiv 1 \pmod 6$ since $p^2 + p + 1 \equiv 0 \pmod 3$. Thus if $x = 3 + zp$ then $1 \equiv 3 + z \pmod 6$. Hence $x \geqq 3 + 4p$. If $u = (p^2 + p + 1)/7$ then $x \equiv 7 \pmod p$. If $x = 7$ then by Lemma 36.6 the S_7-subgroup of $\mathfrak{U}^*$ is generated by two elements. Hence $7^2 - 1 \equiv 0 \pmod p$ by Lemma 36.4. However $7^2 - 1 = 48$ and $(p, 48) = 1$. Thus $x \neq 7$. Let $x = 7 + zp$. Then $p^2 + p + 1 \equiv u \equiv 1 \pmod 6$. Hence $p \equiv 5 \pmod 6$. Thus $1 \equiv x \equiv 7 + 5z \pmod 6$, hence $z \equiv 0 \pmod 6$. Therefore $x \geqq 7 + 6p$. Thus in any case

$$u^* = ux\,, \qquad x \geqq 4p + 3\,. \tag{36.26}$$

Therefore $(u^* - 1)/3p > (u - 1)/3$. Hence by (36.13) and the coherence of $\mathscr{U}$

$$(\phi^\tau, \Gamma_{\mathfrak{B}}) = 0\,. \tag{36.27}$$

Assume first that $(\phi^\tau, \Gamma_{\mathfrak{B}}) \neq 0$, then by (36.12) and the coherence of $\mathscr{U}$

$$\frac{u^* - 1}{3p} \leqq 3p - 1\,. \tag{36.28}$$

Suppose now that $(\phi^\tau, \Gamma_{\mathfrak{B}}) = 0$. Then by (36.10) $(\psi^\tau, \Gamma_{\mathfrak{U}}) \neq 0$. Hence the coherence of $\mathscr{V}$ and (36.11) imply that

$$\frac{v^* - 1}{3p} \leqq 3p - 1\,. \tag{36.29}$$

By (36.27) and (36.5) $(\eta_{01}, \Gamma_{\mathfrak{U}}) \not\equiv 0 \pmod 2$. If also $(\eta_{10}, \Gamma_{\mathfrak{U}})$ were odd then by (36.8) $(\eta_{ij}, \Gamma_{\mathfrak{U}}) \neq 0$ for $1 \leqq i \leqq q - 1$, $1 \leqq j \leqq p - 1$. Thus by (36.11) $(\psi^\tau, \Gamma_{\mathfrak{U}}) = 0$ contrary to what has been proved. Therefore $(\eta_{10}, \Gamma_{\mathfrak{U}}) \equiv 0 \pmod 2$. Hence by (36.7) $(\Gamma_{\mathfrak{Q}}, \phi^\tau) \neq 0$. Thus by (36.14) and (36.29)

$$\frac{u^* - 1}{3p} \leqq \frac{v - 1}{p} \leqq \frac{v^* - 1}{p} < 9p - 3\,.$$

Now (36.28) implies that in any case

$$\frac{u^* - 1}{9p} \leqq 3p - 1 . \tag{36.30}$$

For any prime r let $\mathfrak{U}_r$ be the S_r-subgroup of $\mathfrak{U}^*$.

Suppose first that $u = p^2 + p + 1$, then $x > 6p$. Hence (36.30) implies that

$$6(p^2 + p + 1) - 1 \leqq 27p - 9 .$$

Therefore $2p^2 - 7p + 4 \leqq 0$ which is impossible for $p \geqq 5$.

Suppose now that $u = (p^2 + p + 1)/3$ then $x \geqq 4p + 3$ by (36.26). Hence (36.30) implies that

$$4(p^2 + p + 1) < 81p .$$

Thus $4p < 81$ or $p < 22$. Since $p \equiv 1 \pmod 3$ this yields that $p = 7$, $p = 13$ or $p = 19$.

If $p = 7$ then $u = 19$. If $|\mathfrak{U}_{19}| = 19^n$ then $n \geqq 6$ as $|\mathfrak{U}_{19}| \equiv 1 \pmod 7$. Thus (36.30) implies that $19^6 \leqq 27.7^2 \leqq 19^4$. If $p = 13$ then $u = 61$. Let $|\mathfrak{U}_{61}| = 61^n$, then $n \geqq 3$ as $|\mathfrak{U}_{61}| \equiv 1 \pmod{13}$. Hence (36.30) implies that $61^3 \leqq 27.13^2 < 61^3$. If $p = 19$ then $u = 127$. Let $|\mathfrak{U}_{127}| = 127^n$, then $n \geqq 3$ as $|\mathfrak{U}_{127}| \equiv 1 \pmod{19}$. Hence (36.30) implies that $127^3 \leqq 27.19^2 < 127^3$.

Assume finally that $u = (p^2 + p + 1)/7$ then $x \geqq 6p + 1$. Thus (36.30) implies that

$$\frac{6(p^2 + p + 1)}{7} \leqq 27p .$$

Therefore $6p < 27.7$, so $p < 32$. Since $p^2 + p + 1 \equiv 0 \pmod 7$, $p \equiv 2 \pmod 7$ or $p \equiv 4 \pmod 7$. Thus $p = 11$ or $p = 23$.

If $p = 11$ then $u = 19$. Let $|\mathfrak{U}_{19}| = 19^n$; then $n \geqq 3$ as $|\mathfrak{U}_{19}| \equiv 1 \pmod{11}$. Hence (36.30) implies that $19^3 \leqq 27.11^2 = 287.11 < 19^3$. If $p = 23$ then $u = 79$. As $|\mathfrak{U}_{79}| \equiv 1 \pmod{23}$, $|\mathfrak{U}_{79}| \geqq 79^3$. Hence (36.30) implies that $79^3 \leqq 27.23^2 < 79^3$.

Therefore $u = u^*$ in all cases. Hence $u \equiv 1 \pmod p$ by Lemmas 36.4 and 36.5. Since $(p, 6) = 1$, $7 \not\equiv 1 \pmod p$ and $3 \not\equiv 1 \pmod p$. Hence by Lemma 36.7 $u = p^2 + p + 1$.

The proof of Theorem 27.1 under Hypothesis 36.1 is now immediate.

Let $q = 3$ and p have the same meaning as in the earlier part of this section. By Lemma 35.2 $|\mathfrak{Q}| = q^p$. By Lemma 36.5 $|\mathfrak{P}| = p^q$. The other properties of Condition (i) follow from the structure of $\mathfrak{S}$ and $\mathfrak{T}$ and Theorem 14.1. Thus Condition (i) is verified. By Lemma 35.6 $C(\mathfrak{Q}) \leqq \mathfrak{Q}$. Hence $C(\mathfrak{Q}^*) = \mathfrak{P}^*\mathfrak{Q}$. By Lemma 36.3 $C(\mathfrak{P}) \leqq \mathfrak{P}$, hence $C(\mathfrak{P}^*) = \mathfrak{P}\mathfrak{Q}^*$ by Lemma 36.5. The other properties of Condi-

tion (iii) follow from the structure of $\mathfrak{S}$ and $\mathfrak{T}$. Thus Condition (iii) is verified. Lemmas 36.6 and 36.8 imply that $\mathfrak{U} = C(\mathfrak{U})$ is cyclic. By Lemmas 34.12 and 36.4 $\mathfrak{U} = \mathfrak{U}^*$ is a T.I. set in $\mathfrak{G}$. Hence Lemma 36.4 completes the verification of Condition (iv).

Lemmas 34.1, 36.3, 36.5 and 36.8 imply that $\mathfrak{N}\mathfrak{U}$ is a Frobenius group. Lemma 36.8 implies that $|\mathfrak{U}| = (p^q - 1)/(p - 1)$. Lemmas 36.4, 36.6 and 36.8 imply that if $u_0 \,||\, |\mathfrak{U}|$ then $u_0 \equiv 1 \pmod{pq}$. Thus $(|\mathfrak{U}|, p - 1) = 1$. The other statements in Condition (ii) follow from the structure of $\mathfrak{S}$ and $\mathfrak{T}$.

By Theorem 35.1 this completes the proof of Theorem 27.1 in all cases.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is $18.00; single issues, $5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $8.00 per volume; single issues $2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2 chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies

Pacific Journal of Mathematics
Vol. 13, No. 3 May, 1963