THE DOUBLE TRANSITIVITY OF A CLASS OF PERMUTATION GROUPS

Thesis by

Ronald David Bercov

In Partial Fulfillment of the Requirements

For the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1962

ACKNOWLEDGMENTS

I wish to express my appreciation to my advisor Professor Marshall Hall Jr. for his interest and guidance.

I am grateful to the General Electric Foundation for a fellowship.

I would like also to thank Professor Helmut Wielandt for his help and encouragement.

ABSTRACT

In this thesis primitive finite permutation groups G with regular abelian subgroup H are studied. It is shown that if, for an odd prime p, H has a Sylow p-subgroup which is the direct product of two cyclic groups of different order, then G is doubly transitive.

I Introduction

The object of this thesis is to show that certain finite abelian groups cannot occur as regular subgroups of uniprimitive (primitive but not doubly transitive) permutation groups. Thus we conclude that primitive groups with such a regular abelian subgroup are necessarily doubly transitive.

The first result of this nature was obtained by Burnside who showed that cyclic groups of order p^m (p prime, $m > 1$) do not occur as regular subgroups of uniprimitive groups. The proof is given in [1] , p. 343.

For this reason Wielandt has chosen to call such abstract groups B-groups.

Burnside conjectured that every abelian group which is not elementary abelian is a B-group. This conjecture is not correct. A class of counter-examples was found by Dorothy Manning in 1936. This class of counter-examples has been generalized by Wielandt and will be given below. The first advance beyond Burnside's result was obtained by Schur [2] in 1933. He showed that every cyclic group of composite order is a B-group.

In 1935 Wielandt [3] generalized this result by showing that every abelian group of composite order which has at least one cyclic Sylow subgroup is a B-group.

In 1937 Kochendörffer [4] generalized the Burnside result in a different direction by showing that every abelian group of type (p^{α}, p^{β}) with $\alpha > \beta$ is a B-group.

This thesis is a simultaneous generalization of the results of Wielandt and Kochendörffer. We show that for any odd prime p every abelian group of composite order which has at least one Sylow subgroup of type (p^{α}, p^{β}) with $\alpha > \beta$ is a B-group.

We now give the Wielandt class of counter-examples to the Burnside conjecture.

Let $H = H_1 \times H_2 \dots \times H_d$ with $|H_1| = |H_2| = \dots = |H_d| = a > 2$ and $d > 1$ (where $|H_i|$ is the order of H_i).

Then H is not a B-group. Thus for any such H there exists a uniprimitive group with a regular subgroup isomorphic to H. No assumption is made on the structure of the H_i.

The proof is given in [5], an unpublished set of notes from lectures given by Wielandt at Tübingen in 1954.

We mention that two classes of non-abelian B-groups are known as well.

Wielandt [6] showed that every dihedral group is a B-group, and Scott [7] has shown that every generalized dicyclic group is a B-group.

This thesis is a direct generalization of [4] in the sense that the arguments apply whether or not the regular subgroup is a p-group or not. The case in which the Sylow subgroup is cyclic (i.e. $\beta = 0$) requires a slightly different argument, however. Thus we mention that the arguments given in this thesis can be adapted to give a somewhat different proof of Wielandt's result in the case $\beta = 0$, but for clarity of the presentation, we assume that the regular subgroup has a non-cyclic Sylow subgroup of type (p^{α}, p^{β}) with $\alpha > \beta$ (i.e. we assume that $\beta \neq 0$ holds).

II Notation, Definitions, and Theorems from the Theory of Schur Rings

Let G be a given permutation group on the letters $a_1, \ldots, a_n$ with regular subgroup H.

We denote the image of the letter a_i under the permutation $g \in G$ by a_i^g.

We regard G as a permutation group on H in the following way.

We distinguish the letter a_1.

Since H is regular there is a unique $h \in H$, which we call h_j, taking a_1 into a_j for $j = 1, \ldots, n$.

Clearly $h_1 = 1$, the identity element of H.

The one-to-one mapping $j \leftrightarrow h_j$ enables us to replace the letters $a_1, \ldots, a_n$ by the elements $h_1, \ldots, h_n$ of H.

To the permutation $g \in G$ (on $\{a_1, \ldots, a_n\}$) corresponds the permutation $\begin{pmatrix} h \\ h^g \end{pmatrix}$ (on H) where h^g is the element of H uniquely determined by the formula

$$a_1^{h^g} = a_1^{hg}$$

Let R(H) be the group ring of H over the ring of rational integers.

For $\eta = \sum_{h \in H} \gamma(h)\, h \in R(H)$ and any integer j we put $\eta^{(j)} = \sum_{h \in H} \gamma(h)\, h^j$, and $|\eta| = \left|\sum \gamma(h)\, h\right| = \sum \gamma(h)$.

With $K \subseteq H$ we associate $\underline{K} \in R(H)$ defined by

$$\underline{K} = \sum_{h \in H} \gamma(h)\, h \text{ where } \gamma(h) = \begin{cases} 1 \text{ if } h \in K \\ 0 \text{ if } h \notin K \end{cases}$$

Thus $|\underline{K}|$ is the number of elements in K.

Let G_1 be the subgroup of G (considered as a permutation group on H) consisting of those elements of G fixing 1, the identity element of H (thus G_1 corresponds to G_{a_1}).

Let $\{1\} = T^0, T^1, \ldots, T^k$ be the sets of transitivity of G_1, where $T^i \subseteq H$ for $i = 0, \ldots, k$.

Clearly the elements $\sum_{i=0}^{k} \gamma_i \underline{T}^i$ (γ_i integers) form an additive subgroup of R(H).

<u>Definition 1</u>:

A Schur-module (S-module) over H is an additive subgroup of R(H) which has a basis $\underline{K}_1, \ldots, \underline{K}_t$ where $K_i \subseteq H$ for $i = 1, \ldots, t$, $K_i \cap K_j = \emptyset$ for $1 \leq i < j \leq t$ and

$$\sum_{i=1}^{t} \underline{K}_i = \underline{H}.$$

Let $R(H, G_1)$ be the additive subgroup of R(H) spanned by the $\underline{T}^i$, $i = 0, \ldots, k$.

Then clearly $R(H,G_1)$ is an S-module.

<u>Definition 2</u>:

A Schur-ring (S-ring) over H is an S-module over H which is in addition a subring of R(H) containing the multiplicative identity $\underline{1}$ and containing $\eta^{(-1)} = \sum \gamma(h)h^{-1}$ whenever it contains $\eta = \sum \gamma(h)\, h$.

<u>Theorem 1</u>: (Schur, 1933)

$R(H,G_1)$ is an S-ring.

<u>Definition 3</u>:

An S-ring $\mathcal{S}$ is called <u>primitive</u> if K = 1 and K = H are the only subgroups K of H for which $\underline{K} \in \mathcal{S}$ holds.

Theorem 2:

G is a primitive group if and only if $R(H,G_1)$ is a primitive S-ring.

Theorem 3:

Let $\mathcal{S}$ be a primitive S-ring, $\eta \in \mathcal{S}$, $\eta \neq \gamma \cdot \underline{1}$.

Then the elements $h \in H$ actually appearing in η (i.e. with non-zero coefficient) generate H.

Theorem 4:

Let $\mathcal{S}$ be an S-ring over the abelian group H of order n. Let j be an integer. Let $\eta \in \mathcal{S}$.

Then:

(a) $(j, n) = 1 \implies \eta^{(j)} \in \mathcal{S}$.

(b) If $j = p$ is a prime divisor of n and if $\mathcal{S}$ is primitive, then

$$\eta^{(p)} \equiv \delta \cdot \underline{1} \pmod p$$

holds for an appropriate integer δ.

(The congruence is understood, of course, to hold for the coefficients.)

Proofs of theorems 1-4 are found in reference 2. They are given in terms of somewhat different, but equivalent, concepts.

Definition 4:

Let $\eta \in R(H)$.

If $(j,n) = 1$, $\eta^{(j)}$ is said to be conjugate to η.

Definition 5:

If $\eta = \eta^{(j)}$ for all j with $(j,n) = 1$, i.e. if η is its only conjugate, η is said to be rational.

Definition 6:

Let $\eta \in R(H)$

Then the sum of all (distinct) conjugates of η is called the trace of η, and is denoted by tr. (η).

Tr. (η) is obviously rational and by theorem 4(a) lies in the S-ring $\mathcal{S}$ whenever η lies in $\mathcal{S}$.

Definition 7:

For $h \in H$, the trace of $\underline{\{h\}}$ is called the elementary trace associated with h and is denoted by tr. (h).

Clearly if k has non-zero coefficient in the elementary trace associated with h, then the elementary traces associated with h and with k are identical.

It is also fairly easily seen that the conjugates of the $\underline{T}^i$ are again of this form:

Theorem 5:

$$(j,n) = 1 \Rightarrow \underline{T}^{i^{(j)}} = \underline{T}^q \text{ for some } q \text{ with } 0 \leq q \leq k.$$

Proof:

To see this we note that by theorems 1 and 4

$$\underline{T}^{i^{(j)}} = \sum_{s=0}^{k} \gamma_s \underline{T}^s \quad \text{where}$$

$\gamma_s = 0$ or 1 for $s = 0,\ldots,k$ since $(j,n) = 1$.

We proceed by induction on $|\underline{T}^i|$ (the statement obviously holding for $T^0 = \{1\}$).

Unless $\gamma_q = 1$ for some q and $\gamma_s = 0$ for all $s \neq q$, in which case $\underline{T}^{i^{(j)^q}} = \underline{T}^q$ as asserted, we have

$|\underline{T}^s| < |\underline{T}^i|$ for all s for which $\gamma_s \neq 0$, since in any case we have

$$\left|\underline{T}^{i^{(j)}}\right| = \left|\underline{T}^{i}\right|.$$

We therefore assume that $\left|\underline{T}^{s}\right| < \left|\underline{T}^{i}\right|$ holds for all s with $\gamma_s \neq 0$.

Now let j' satisfy $jj' \equiv 1\ (n)$.

Then $\underline{T}^{i} = \left[\underline{T}^{i^{(j)}}\right]^{(j')} = \sum_{s=0}^{k} \gamma_s \left[\underline{T}^{s}\right]^{(j')}$.

The $\left[T^{s}\right]^{(j')}$ are $\underline{T}^{q}$ for appropriate q by the induction hypothesis. We have thus expressed $\underline{T}^{i}$ as a linear combination of smaller $\underline{T}^{q}$ which is not possible since by definition $T^{i} \cap T^{q} = \emptyset$ for $i \neq q$.

Now tr. $(\underline{T}^{i})$ is a sum of distinct conjugates of $\underline{T}^{i}$ hence a sum of distinct $\underline{T}^{q}$.

Thus tr. $(\underline{T}^{i})$ has only coefficients 0 and 1 and tr. $(\underline{T}^{i}) = \underline{S}^{i}$ where $S^{i} \subseteq H$ is the set of elements of H with non-zero coefficient in tr. $(\underline{T}^{i})$.

We note first that the S^{i} need not in general be different. If necessary by renumbering the T^{i} we may assume without loss of generality that $S^{1},\ldots,S^{r}$ are distinct and that for any $j > r$ there is an $i \leq r$ with $S^{i} = S^{j}$.

Clearly $\underline{S}^{0} = \text{tr.}\ (\underline{T}^{0}) = \text{tr.}\ (\underline{1}) = \underline{1}$.

We now assert that for $i, j \leq r$, $i \neq j$ we have $S^{i} \cap S^{j} = \emptyset$.

Suppose the contrary, say $h \in S^{i} \cap S^{j}$. Then $h = x^{s} = y^{t}$ where $(s,n) = (t,n) = 1$, $x \in T^{i}$, $y \in T^{j}$.

Let t' satisfy $tt' \equiv 1\ (n)$.

Then $x^{st'} = y$, thus $\underline{T}^{i^{(st')}}$ and $\underline{T}^{j}$ have the element y in common, and $\underline{T}^{i^{(st')}} = \underline{T}^j$.

Thus we have $T^j \subseteq S^i$.

Now since $\underline{S}^i$ is rational we conclude that $S^j \subseteq S^i$. Since S^i and S^j here play symmetric roles we have $S^i \subseteq S^j$ by the same argument, hence $S^i = S^j$, which is in contradiction to the way we numbered the T^i.

The $S^i (i = 0,\dots,r)$ are therefore disjoint subsets of H, we clearly have $\sum_{i=0}^{r} \underline{S}^i = \underline{H}$, and therefore the $\underline{S}^i$ span an S-module over H.

Since $\underline{S}^0 = \underline{1}$ and $\underline{S}^{i^{(-1)}} = \underline{S}^i$ (since $\underline{S}^i$ is rational) for $i = 0,\dots,r$ the $\underline{S}^i$ generate on S-ring over H provided only that they generate a subring of R(H).

To show this we prove the following:

<u>Theorem 6:</u>

Let $1 \leq i,j \leq r$.

Then $\underline{S}^i \, \underline{S}^j = \sum_{t=o}^{r} \gamma_t \, \underline{S}^t$ for appropriately chosen integers γ_t.

<u>Proof:</u>

$$\underline{S}^i, \underline{S}^j \in R(H,G_1) \Longrightarrow \underline{S}^i \, \underline{S}^j = \sum_{q=0}^{k} \delta_q \, \underline{T}^q = \sum_{h \in H} \gamma(h) h.$$

We need show that if h, $k \in S^t$, $\gamma(h) = \gamma(k)$. We may then put $\gamma_t = \gamma(h) = \gamma(k)$.

Clearly it suffices to show that for $h \in T^t$, $k \in S^t$, $\gamma(h) = \gamma(k)$.

Clearly if $k \in T^t$ holds, we have $\gamma(h) = \gamma(k) = \delta_t$. Now $k \in S^t \Longrightarrow k = h^s$ for some $h \in T^t$, where $(s,n) = 1$.

$\gamma(h)$ is the number of ordered pairs (u,v) with $u \in S^i$, $v \in S^j$, $uv = h$.

For each such (u,v) the pair (u^s, v^s) satisfies $u^s v^s = h^s = k$ and conversely.

Moreover $u^s \in S^i \Leftrightarrow u \in S^i$, $v^s \in S^j \Leftrightarrow v \in S^j$ since $\underline{S}^i$ and $\underline{S}^j$ are rational.

Thus $(u,v) \longleftrightarrow (u^s,v^s)$ is a one-to-one correspondence between the $\gamma(h)$ pairs of solutions $uv = h$ and the $\gamma(k)$ pairs of solutions $uv = k$.

Thus $\gamma(h) = \gamma(k)$ and theorem 6 is proved. Since $\underline{S}^i$ is in $R(H,G_1)$ for $i = 0,\ldots,r$, it is clear that the S-ring generated by the $\underline{S}^i$ is a subring of $R(H,G_1)$.

We will use theorem 6 in the following weaker form:

<u>Theorem 6'</u>:

$$\text{Let } \left[\underline{S}^i\right]^2 = \sum_{h \in H} \sigma_i(h)\, h.$$

Then $h, k \in S^j \Rightarrow \sigma_i(h) = \sigma_i(k)$.

To assist in computing these coefficients we introduce the following notation:

Let $h \in H$, $R \subseteq H$.

Then $R(h) = \left\{ r \in R \mid r^{-1}h \in R \right\}$.

The coefficient of h in $\left[\underline{R}\right]^2$ is the number of solutions $r_1 r_2 = h$.

$r_1 \in R$ can occur in at most one such pair and it occurs in such a pair precisely when $r_2 = r^{-1} h \in R$ holds.

Thus $|\underline{R(h)}|$ is the coefficient of h in $\left[\underline{R}\right]^2$, and the elements of $R(h)$ are precisely those elements of R which "hit" other elements of R in such a way as to produce an h.

We introduce the following further notation.

For any set K, let $|K|$ be the number of elements in K.

$K \subseteq H$ means that K is a subset of H.

$\langle K \rangle$ is the smallest subgroup of H containing K and for $h \in H$,

$$\langle h \rangle = \langle \{h\} \rangle .$$

$K \leq H$ means that K is a subgroup of H.

We now state the two theorems proved in this thesis.

Theorem A:

Let G be a primitive permutation group of degree n.

Let p be an odd prime.

Let $H = A \times B \times C$ be a regular abelian subgroup of G, where

$A = \langle a \rangle$ is cyclic of order p^{α} (p prime)

$B = \langle b \rangle$ is cyclic of order p^{β}

$|C| = m$ where $(m,p) = 1$,

and $\alpha > \beta > 0$ holds.

Then G is doubly transitive.

Theorem B:

Let the hypotheses of theorem A hold.

In addition let $\{1\} = T^0, T^1, \ldots, T^k$ be the sets of transitivity of G_1 and let tr. $(\underline{T}^i) = \underline{H-1}$ for $i = 1, \ldots, k$. Then G is doubly transitive.

It is clear that theorem A includes theorem B. They are stated separately since we will first prove theorem B by a not too difficult counting argument, and then devote the greater part of the paper to the proof that under the hypotheses of theorem A, tr. $(\underline{T}^i)$ $= \underline{H-1}$ necessarily holds for $i = 1, \ldots, k$.

Throughout this thesis, k will denote the number of non-trivial (i.e. $\neq \{1\}$) sets of transitivity of G_1, and r will denote the number of distinct non-trivial traces of these $\underline{T}^i$.

Thus G is doubly transitive if and only if $k = 1$.

The additional hypothesis of theorem B is that $r = 1$.

Let $P = AB$.

Since $(|C|, p) = 1$, P is a Sylow p-subgroup of H.

We have $|A| = p^{\alpha}$

$$|B| = p^{\beta}$$

$$|P| = p^{\alpha+\beta}$$

Since H is regular we have

$$n = |H| = |PC| = |P|\,|C| = mp^{\alpha+\beta}.$$

We let $u = a^{p^{\alpha-1}}$.

Put $U = \langle u \rangle$. Thus $|\langle u\rangle| = p$.

Let $K \subseteq H$, $0 \leq \lambda \leq \beta$.

We may express $k \in K$ uniquely in the form

$k = a^{sp^{\nu}} b^{tp^{\lambda}} c$ where $(s,p) = (t,p) = 1$, $c \in C$.

Let $K_{X(\lambda)}$ be the set of all such $k \in K$ for which $\nu = 0$.

Let $K_{Y(\lambda)}$ be the set of all such $k \in K$ for which $\nu \neq 0$, but $\alpha - \nu > \beta - \lambda$.

Let $K_{Z(\lambda)}$ be the set of all such $k \in K$ for which $\alpha - \nu \leq \beta - \lambda$.

Let $K_X = \bigcup_{\lambda=0}^{\beta} K_{X(\lambda)}$

$$K_Y = \bigcup_{\lambda=0}^{\beta} K_{Y(\lambda)}$$

$$K_Z = \bigcup_{\lambda=0}^{\beta} K_{Z(\lambda)}$$

$$K_{(\lambda)} = K_{X(\lambda)} \cup K_{Y(\lambda)} \cup K_{Z(\lambda)}$$

$K_{(\lambda)}$ is then the subset of K consisting of all elements which have a power of b exactly divisible by p^{λ}.

$K_{X(\lambda)}$ is the subset of $K_{(\lambda)}$ consisting of elements of order divisible by p^{α}.

$K_{Y(\lambda)}$ is the subset of $K_{(\lambda)}$ consisting of the elements k not in $K_{X(\lambda)}$ for which $uC \cap \langle k \rangle \neq \emptyset$ holds.

$K_{Z(\lambda)}$ consists of the remaining elements of $K_{(\lambda)}$, the k for which $uC \cap \langle k \rangle = \emptyset$.

Without loss of generality we may assume that $u \in T^1$ holds. We put $S^1 = S$.

Let $C_o = \{ c \in C \mid ac \in S \}$.

We show that by appropriate choice of generators of P we may assume that $C_o \neq \emptyset$.

Since G is primitive, $\langle S \rangle = H$ by theorem 3.

Thus S must have an element of order divisible by p^{α}, say

$$a^s \, b^{tp^{\lambda}} \, c \quad \text{where } (s,p) = (t,p) = 1,\ c \in C.$$

Let $a_1 = a^s \, b^{tp^{\lambda}}$.

$$a_1^{\,p^{\alpha-1}} = a^{sp^{\alpha-1}} \, b^{tp^{\alpha-1+\lambda}} = a^{sp^{\alpha-1}}$$

since $\alpha - 1 \geq \beta \implies b^{p^{\alpha-1}} = 1$.

$u \in S \implies u^s = a_1^{\,p^{\alpha-1}} \in S$ since $\underline{S}$ is rational.

Obviously we have $P = \langle a_1 \rangle \times \langle b \rangle$.

Thus we may replace a by a_1 and put $u = a_1^{\,p^{\alpha-1}}$ to get $a_1 c \in S$ and $a_1^{\,p^{\alpha-1}} \in S$ as well.

We therefore assume that a has been chosen in such a way that C_o is non-empty.

III Preliminary Lemmas

We prove five preliminary lemmas; the first two of which to be used in the proof of theorem B and the remaining three to be used in the proof of theorem A.

Because of theorem 6' we know that in $[\underline{S}^i]^2$ certain coefficient equalities must hold. Lemmas 1-5 will tell us that such equalities can occur only if the S^i have a special structure. Repeated application of these lemmas shows that this structure is incompatible with the existence of more than one non-trivial S^i. We will therefore be able to show directly that $\underline{S} = \underline{H-1}$.

Lemma 1:

Let $x \in P$, $u \in \langle x \rangle$, $x \notin U$, $c \in C$. Then for any $j = 1,\ldots,p-1$ there exists v prime to n with $v \equiv 1 \ (p)$ such that $(xc)^v = u^j xc$.

Proof:

Since $x \in P$, we may write $x = a^{sp^{\nu}} b^{tp^{\lambda}}$

where $0 \leq \nu \leq \alpha$, $0 \leq \lambda \leq \beta$,

$(s,p) = (t,p) = 1$.

$u \in \langle x \rangle \Longrightarrow \alpha - \nu > \beta - \lambda$,

i.e. $x \in H_X \cup H_Y$, and $x \notin U \Longrightarrow \alpha \neq \nu - 1$

Choose s', m' satisfying $s's \equiv 1 \ (p^{\alpha})$

$m'm \equiv 1 \ (p^{\alpha})$

(where $m = |C|$).

Then,

$$u^j xc = a^{jp^{\alpha-1}} a^{sp^{\nu}} b^{tp^{\lambda}} c$$

$$= a^{sp^{\nu}(1+mm's'jp^{\alpha-\nu-1})} b^{tp^{\lambda}(1+mm's'jp^{\alpha-\nu-1})} c^{(1+mm's'jp^{\alpha-\nu-1})}$$

since $b^{p^{\alpha-\nu+\lambda-1}} = c^m = 1.$

Thus,

$$u^j(xc)\ (a^{sp^\nu}\ b^{tp^\lambda}\ c)^{1+mm's'jp^{\alpha-\nu-1}} = (xc)^v$$

where $v = 1 + mm's'jp^{\alpha-\nu-1}$

Now $\alpha-\nu > \beta-\lambda \Longrightarrow \nu \neq \alpha$

and $x \notin U \Longrightarrow \nu \neq \alpha-1,$

thus $p \mid p^{\alpha-\nu-1}$ and we have $v \equiv 1\ (p).$

Clearly $v \equiv 1\ (m)$, thus $(v, n) = 1$ as asserted.

<u>Lemma 2</u>:

Let $K \subseteq H$.

Let $h \in H$ such that $hK = K$. Then in $\underline{K}\ \underline{K}^{(-1)}$ h has coefficient $|K|$.

<u>Proof</u>:

In $\underline{K}\ \underline{K}^{(-1)}$, 1 has coefficient $|K|$. Thus in $h\ \underline{K}\ \underline{K}^{(-1)} = \underline{hK}\ \underline{K}^{(-1)}$ $= \underline{K}\ \underline{K}^{(-1)}$ h has coefficient $|K|$.

<u>Lemma 3</u>:

Let $R \subseteq H$ such that $\underline{R}$ is rational.

Let $R^* = (R_X \cup R_Y) - UC$

Then $R^* \subseteq R(u^j)$ for $j = 1,\dots,p-1$.

<u>Proof</u>:

$\underline{R}$ rational $\Longrightarrow \underline{R_X}, \underline{R_Y}, \underline{R \cap UC}$ rational $\Longrightarrow R^*$ rational.

$\underline{R^*}$ rational $\Longrightarrow \underline{R^*} = \underline{R^*}^{(-1)}$, thus $r \in R^* \Longleftrightarrow r^{-1} \in R^*$. Moreover by Lemma 1,

$$r^{-1} \in R^* \Longrightarrow r^{-1}u^j \in R^*.$$

Thus $r \in R^* \Longrightarrow r^{-1} \in R^* \Longrightarrow r^{-1}u^j \in R^* \Longrightarrow r \in R(u^j).$

and $R^* \subseteq R(u^j),$

We are now in a position to prove the important.

<u>Lemma 4</u>:

Let $x \in H_X$ (i.e. let x be of order divisible by p^{α}).

Let $R \subseteq H$ such that $\underline{R}$ is rational.

Then $|R(x)| \leq |R(u^j)|$ holds for $j = 1,\ldots,p-1$ and $|R(x)| = |R(u^j)|$ for every $j = 1,\ldots,p-1$ only if

$$h \in R(u^i) - R(x) \Longrightarrow \begin{cases} \text{(i)} & h \in H_X, \\ \text{(ii)} & h^{-1}x \in H_Z \\ \text{and (iii)} & u^{-j}h \in R(x) \text{ for } j = 1,\ldots,p-1 \end{cases}$$

<u>Proof</u>:

Let $j \in \{1,\ldots,p-1\}$. To each element $z \in R(x)-R(u^j)$ we wish to associate in a 1-1 fashion an element of $R(u^j)-R(x)$.

$z \in R(x)-R(u^j) \Longrightarrow z^{-1}x \in R, \quad z^{-1}u^j \notin R.$

By lemma 3,

$$z \notin R(u^j) \Longrightarrow z \notin R^* = (R_X \cup R_Y) - UC$$

Now if $z = u^i c$ $(c \in C)$, $u^i \neq u^j$ we have

$z^{-1} = u^{-i} c^{-1} \in R$ (since $\underline{R}$ is rational) and

$z^{-1} u^j = u^{j-i} c^{-1} \in R$ since we can always simultaneously satisfy the congruences

$$v \equiv q \ (p) \qquad q \in \{1,\ldots,p-1\}$$
$$v \equiv 1 \ (m)$$

since $(m,p) = 1$.

This would violate $z \notin R(u^j)$.

Thus $z \notin R(u^j) \Longrightarrow z \notin (R_X \cup R_Y) - u^jC$,

i.e. $z \in R_Z \cup (R \cap u^jC)$

Now $z \in R(x) \Longrightarrow z^{-1}x \in R$,

thus $z^{-1}x \in R_X$.

Now by lemma 1, we may conclude that

$u^j z^{-1} x \in R$, indeed we have

$u^j z^{-1} x \in R_X \subseteq R^*$

Now by lemma 3, we have $u^j z^{-1} x \in R(u^j)$.

We claim that $u^j z^{-1} x \in R(u^j) - R(x)$.

Suppose the contrary, i.e.

$(u^j z^{-1} x)^{-1} x \in R$, thus $zu^{-j} \in R$.

Since $\underline{R} = \underline{R}^{(-1)}$ we have $z^{-1}\, u^j \in R$ contradicting $z \notin R(u^j)$.

Thus with each $z \in R(x) - R(u^j)$ we have associated $u^j\ z^{-1} x$ in $R(u^j) - R(x)$. This completes the proof that $|R(u^j)| \geq |R(x)|$ holds.

Now suppose $|R(u^i)| = |R(x)|$ for $i = 1, \ldots, p-1$. Then the only elements of $R(u^j) - R(x)$ can be the elements $u^j\ z^{-1} x$ where $z \in R(x) - R(u^j)$, thus $z \in R_Z \cup (R \cap u^j C)$. For such an $h = u^j z^{-1} x$, we have

(i) $h \in H_X$,

(iii) $u^{-j} h = z^{-1} x \in R(x)$

(since $(z^{-1} x)^{-1} x = z \in R$) and $h^{-1} x = u^{-j} z \in H_Z \cup (u^{-j} C)$.

Now $h \in H_X \Longrightarrow h \in R^* \Longrightarrow h \in R(u^i)$ for $i = 1, \ldots, p-1$. Thus from $h \in R(u^j) - R(x)$ for some j we conclude that

$h \in R(u^i) - R(x)$ for every $i = 1, \ldots, p-1$.

We conclude from $h^{-1} x \in H_Z \cup (u^{-i} C)$ for $i = 1, \ldots, p-1$ and $p > 2$ that

(ii) $h^{-1} x \in H_Z$

Lemma 4 says that if $|R(x)| = |R(u^j)|$ for every $j = 1, \ldots, p-1$, then in $[\underline{R}]^2$ only elements of H_X can "hit" some u^j but fail to "hit" x. Such elements h fail to "hit" x because the element $h^{-1} x$ which they must "hit" belongs to $H_Z - R$. For each such h there are p-1 other elements in tr. (h), the $u^j h$ ($j=1,\ldots,p-1$), which do "hit" x. In particular since all elements of $(R_X \cup R_Y) - UC$ do "hit" every u^j it follows that $R_Y - UC \subseteq R(x)$, and indeed if any element of R not in H_X "hits" any u^j it must hit x as well. Moreover, any element h of R_X which "hits" an element of H_Y to yield an x (i.e. an h for which $h^{-1}x \in H_Y$ holds) must belong to R(x). Thus for such an h we may conclude that $h^{-1}x \in R$ holds.

We now prove a further lemma which says essentially that every elementary trace of $P_{X(\lambda)}$ has some element "hitting" an element of any elementary trace of $P_{Y(\lambda)} \cup P_{Z(\lambda)}$ in such a way as to yield the element a. Thus if we know that there is a whole elementary trace of $P_{Y(\lambda)} \cup P_{Z(\lambda)}$ in R belonging to R(a), we will be able to conclude that every elementary trace of $P_{X(\lambda)}$ occurs in R.

<u>Lemma 5</u>:

Let $ab^{tp^\lambda} \in P_{X(\lambda)}$

Let $a^{p^\vee} b^{sp^\lambda} \in P_{Y(\lambda)} \cup P_{Z(\lambda)}$

Then there exist e,f with $(e,n) = (f,n) = 1$ such that

$$(ab^{tp^\lambda})^f = (a^{p^\vee} b^{sp^\lambda})^{-e} a$$

<u>Proof</u>:

For any integer j, let j' be an integer satisfying $jj' \equiv 1(p^\alpha)$.

Let $e \equiv t(tp^\vee - s)' \pmod{p^\alpha}$

$f \equiv s(tp^\vee - s)' \pmod{p^\alpha}$

Then $\left[(a^{p^\vee} b^{sp^\lambda})^{-e} a\right]^{f'} = (a^{p^\vee} b^{sp^\lambda})^{-ef'} a^{f'}$

$= (a^{p^\vee} b^{sp^\lambda})^{s't} a^{-s'(tp^\vee - s)} = a^{1+p^\vee(s't-s't)} b^{tp^\lambda} = ab^{tp^\lambda}$.

Thus we have $(a^{p^\vee} b^{sp^\lambda})^{-e} a = (ab^{tp^\lambda})^f$ as asserted.

We now proceed to the proof of theorem B, making use of lemmas 1 and 2. We will then make use of lemmas 3, 4 and 5 with $R = S$ (occasionally $R = S^i$ with $i > 1$) in order to show that $\underline{S} = \underline{H}-\underline{1}$ necessarily holds.

IV Proof of Theorem B

In this section we use lemmas 1 and 2 and a counting argument to show that $r = 1$ (i.e. tr. $(\underline{T}^i) = \underline{H} - \underline{1}$, $i = 1,\ldots,k$) implies $k = 1$.

Theorem B:

Let G be a primitive group with regular abelian subgroup $H = A \times B \times C$ where

$A = \langle a \rangle$ is of order p^{α}.

$B = \langle b \rangle$ is of order p^{β}, $\alpha > \beta > 0$.

$|C| = m$ where $(m,p) = 1$.

Let $\{1\} = T^0, T^1, \ldots, T^k$ be the sets of transitivity of G_1.

Let tr. $(\underline{T}^i) = \underline{H-1}$ for $i = 1,\ldots, k$.

Then $k = 1$, i.e. G is doubly transitive.

Proof:

Since U is a subgroup of H we have whenever $(v,n) = 1$ that $h^v \in U \iff h \in U$.

Since all elements appearing in Tr. $(\underline{T}^i) = \underline{H} - \underline{1}$ are obtained by taking such v^{th} powers of elements of T^i, it follows that $T^i \cap U \neq \emptyset$ for $i = 1,\ldots, k$.

Let $T = T^1$ be the set of transitivity of G_1 in which u occurs.

As we let j take on values congruent to 1 through p-1 modulo p and prime to n we have that the $\underline{T}^{(j)}$ run through sets of transitivity of G_1 (by theorem 5). All such sets of transitivity are obtained in this way since every element of U-1 appears in some such $\underline{T^{(j)}}$.

Now suppose T has s elements of U. Then each T^i has s elements of U, and we have $ks = |U-1| = p-1$.

We note that theorem B holds even in the case $p = 2$, since from what we have just shown it follows that $T^1 = S^1$.

Since the $\underline{T}^i$ are all conjugate to $\underline{T}$ $(i=1,\dots,k)$ we have that the $n-1$ elements of $H-1$ are divided by G_1 into k sets of transitivity, each with $\frac{n-1}{k}$ elements. It is easily seen that

$P_{X(\lambda)}$ consists of $\Phi(p^{\alpha})\ \Phi(p^{\beta-\lambda})$ elements for $\lambda = 0,\dots,\beta$.

$P_{Y(\lambda)}$ consists of $(p^{\alpha-1} - p^{\beta-\lambda})\ \Phi(p^{\beta-\lambda})$ elements for $\lambda = 0,\dots,\beta$.

Thus
$$|P_X| = \Phi(p^{\alpha})p^{\beta} = p^{\alpha+\beta-1}(p-1)$$
$$|P_Y| = p^{\alpha+\beta-1} - \frac{(p^{2\beta+1}+1)}{(p+1)}$$

Except for the $p-1$ elements, x, of $U-1$, for any element xc with $x \in P_X \cup P_Y$, $c \in C$ and for any $j \in \{1,\dots,p-1\}$, there exists $v \equiv 1(p)$ with $(v,n) = 1$ such that

$$u^j xc = (xc)^v.$$

But since $v \equiv 1\ (p)$ holds

$\underline{T}^{(v)}$ and $\underline{T}$ have s elements of U in common. Since distinct T^i are disjoint it follows that $\underline{T}^{(v)} = \underline{T}$ holds; thus $u^j xc \in T$.

Now taking v^{th} powers where $(v,n) = 1$ takes elements of $\left[(P_X \cup P_Y) - U\right]C$ into other such elements.

Therefore if we put

$$T^* = \left[(P_X \cup P_Y) - U\right]C \cap T \text{ we have that}$$
$$|T^*| = \frac{1}{k}\ \left|(P_X \cup P_Y) - U\right|\ |C|$$
$$= \frac{1}{k}\left[p^{\alpha+\beta-1}(p-1) + p^{\alpha+\beta-1} - \frac{(p^{2\beta+1}+1)}{(p+1)} - (p-1)\right] m$$

$$= \frac{m}{k}\left[p^{\alpha+\beta} - \frac{(p^{2\beta+1} + p^2)}{(p+1)}\right]$$

Now for $xc \in T^*$ we have $u^j xc \in T^*$, thus $u^j\ T^* \subseteq T^*$.

Now since T^* is a finite set it follows that

$$u^j\ T^* = T^* \quad \text{for } j = 1, \ldots, p-1.$$

Thus by lemma 2 we have that the coefficient of u^j in $\underline{T}^*\ \underline{T}^{*(-1)}$ is $|T^*|$.

Thus the coefficient of u^j in $\underline{T}\ \underline{T}^{(-1)}$ is $\geq |T^*|$. The coefficient of 1 in $\underline{T}\ \underline{T}^{(-1)}$ is $|T| \geq |T^*|$.

Now, since the Schur-ring $R(H, G_1)$ has the $\underline{T}^i$ as generators, it follows that

$$\underline{T}\ \underline{T}^{(-1)} = \sum_{i=o}^{k} \gamma_i\ \underline{T}^i.$$

Now each T^i $(i = 0, \ldots, k)$ has an element of U.

Thus we have $\gamma_i \geq |T^*|$ for $i = 0, \ldots, k$.

Thus we get the inequality,

$$|T|^2 = \left|\underline{T}\ \underline{T}^{(-1)}\right| = \left|\sum_{i=o}^{k} \gamma_i\ \underline{T}_i\right| \geq |T^*|\ \left|\sum_{i=o}^{k} \underline{T}_i\right| = |T^*|\ |H|$$

Now $|T| = \frac{n-1}{k} = \frac{mp^{\alpha+\beta} -1}{k}$

$$|H| = n = mp^{\alpha+\beta}.$$

Thus we have that

$$\left[\frac{mp^{\alpha+\beta} -1}{k}\right]^2 \geq \frac{m}{k}\left[p^{\alpha+\beta} - \frac{(p^{2\beta+1} + p^2)}{(p+1)}\right] mp^{\alpha+\beta}$$

$$\geq \frac{m}{k}\left[p^{\alpha+\beta} - \frac{(p^{2\beta+1} + p^2)}{(p+1)}\right](mp^{\alpha+\beta} -1)$$

thus

$$\frac{mp^{\alpha+\beta} -1}{k} \geq m\left[p^{\alpha+\beta} - \frac{(p^{2\beta+1} + p^2)}{(p+1)}\right]$$

Since $\beta > 0$ holds, we have

$$\frac{mp^{\alpha+\beta} -1}{k} \geq m\left[p^{\alpha+\beta} - \frac{(p^{2\beta+1} + p^{2\beta})}{(p+1)}\right] \geq m\left[p^{\alpha+\beta} - p^{2\beta}\right]$$

Thus

$$k \leq \frac{mp^{\alpha+\beta} - 1}{mp^{\alpha+\beta} - mp^{2\beta}}$$

Now

$2mp^{2\beta} - 1 < 2mp^{2\beta} \leq pmp^{2\beta} = mp^{\beta+1}\, p^{\beta} \leq mp^{\alpha+\beta}$

$\Longrightarrow mp^{\alpha+\beta} - 1 < 2mp^{\alpha+\beta} - 2mp^{2\beta}$.

Thus we have

$$k \leq \frac{mp^{\alpha+\beta} - 1}{mp^{\alpha+\beta} - mp^{2\beta}} < 2 \quad .$$

Thus k = 1, and theorem B is proved.

V Proof of Theorem A

#1

We now wish to show that S (the trace of the set of transitivity of G_1 in which u occurs) is all of H-1.

We first show that if $S_{X(\lambda)} \neq \emptyset$ we have that $S_{(\lambda)}$ consists of most of $P_{(\lambda)}$ $C(\lambda)$ where $C(\lambda)$ is a subset of C, and $C(\beta)$ $= C_o = \{ c \in C \mid ac \in S \}$.

We will then show in #2 that if μ is the smallest λ for which $S_{X(\lambda)} \neq \emptyset$ holds, we have that $S_{X(\lambda)} \neq \emptyset$ for $\lambda = \mu, \ldots, \beta$, that $C(\lambda) = C_o$ for $\lambda = \mu, \ldots, \beta$, that $S_{(\lambda)} = P_{(\lambda)} C_o$ for $\lambda = \mu, \ldots, \beta-1$, that $S_{(\beta)} = AC_o-1$, and that $\mu = 0$ or β must hold. In #3 we show that the hypothesis $\mu = \beta$ leads to a contradiction. In #4 we show that $C_o = C$. We are thus able to conclude that $S = PC -1 = H -1$.

We now prove two lemmas, the first dealing with the structure of the $S^i_{(\beta)}$ which have elements of order divisible by p^α, and the second dealing with the structure of the $S^i_{(\lambda)}$, $\lambda = 0, \ldots, \beta-1$, which have elements of order divisible by p^α.

Lemma 1.1

Let $1 \leq i \leq r$.

Let $C^i(\beta) = \{ d \in C \mid ad \in S^i_{(\beta)} \}$

Let $c \in C$.

Then the coefficient of ac in $\left[S^i_{(\beta)} \right]^2$ is less than or equal to the coefficient of u^j for $j = 1, \ldots, p-1$ and equality holds for every such j only if

(i) $\underline{S^i_{(\beta)}} = \dfrac{(A-1)\, C^i(\beta)}{} + \underline{C^*_i}$

where $C^*_i \subseteq C$.

(ii) $C^i(\beta)c = C^i(\beta)$

<u>Proof</u>:

Put $R = S^i_{(\beta)}$,

$D = C^i(\beta)$.

$\underline{S^i}$ rational $\Longrightarrow \underline{S^i_{(\beta)}}$ rational.

Thus since $ac \in H_X$ holds we may conclude immediately from lemma 4 that

$$|R(ac)| \leq |R(u^j)| \text{ holds for } j = 1,\ldots,p-1.$$

We now assume that $|R(ac)| = |R(u^j)|$ for $j = 1,\ldots,p-1$.

Since $(m,p) = 1$, for any s with $(s,p) = 1$

and any t with $(t,m) = 1$

we may find s', t' with

$s' \equiv s(p^\alpha)$, $s' \equiv 1\ (m)$

$t' \equiv 1(p^\alpha)$, $t' \equiv t\ (m)$.

Thus for $x \in P$, $d \in C$ we have tr. (xd) = tr. (x) tr. (d)

Thus R has every element of tr. (a) $\underline{D}$ and no other element of tr. (a) $\underline{C}$. Now tr. $(a) = \sum_{(s,p)=1} a^s$.

Again by lemma 4, the only elements x of tr. (a) $\underline{D}$ which might not satisfy $x^{-1}ac \in R$ must satisfy $x^{-1}ac \in H_Z$. Now $x \in AC \Longrightarrow x^{-1}ac$ in AC and $AC \cap H_Z = C$.

Thus the only elements x of tr. (a) $\underline{D}$ which might fail to satisfy $x^{-1}ac \in R$ are the elements of aD.

Now as we let x run through the elements $a^{1+pw}d$ of tr. (a) $\underline{D}$ $(w \neq o)$, the elements $x^{-1}ac$ that we get are the elements $a^{-pw}\, d^{-1}c$

which must all lie in R.

Now since D is inverse closed, we have that

$$R \geq A_Y Dc$$

Now, were R to have a further element, y, of $A_Y C$ it would satisfy $y^{-1}u \in R$ by lemma 3, thus

$$y^{-1}ac \in R \text{ by lemma 4.}$$

This is clearly not possible by the definition of D.

Hence the only elements of $A_Y C$ which can occur in R belong to $A_Y Dc$ and all such elements do occur.

Thus we have that

$$S^i_{(\beta)} = \underline{A_X D} + \underline{A_Y\ Dc} + \underline{C^*_i}.$$

Now, again by lemma 3 since $p > 2$ holds, we have

$(a^2 d)^{-1}\ u \in R$ for $d \in D$, hence by lemma 4,

$(a^2 d)^{-1} ac = a^{-1}\ d^{-1}\ c \in R$. But the only elements of $A_X C$ in R lie in $A_X D$.

Thus $d^{-1}c \in D$ holds for $d \in D$. Again since D is inverse closed we have $Dc = D$ as asserted.

Thus we have that

$$\underline{S^i_{(\beta)}} = \left[\underline{A_X} + \underline{A_Y}\right]\underline{D} + \underline{C^*_i} = \left[\underline{A - 1}\right]\underline{D} + \underline{C^*_i} = \left[\underline{A - 1}\right]\underline{C^i(\beta)} + \underline{C^*_i}\ .$$

We now assume that $\lambda < \beta$, and prove a lemma similar to lemma 1.1.

Lemma 1.2

Let $R = S^i_{(\lambda)}$ where $i \in \{1, \dots, r\}$, $\lambda < \beta$.

Let $R_X \neq \emptyset$.

Let $C^i(\lambda) = \left\{ d \in C \mid ab^{sp^\lambda}\ d \in R \text{ for some s with } (s,p) = 1 \right\}$

$$= \left\{ d_1, \dots, d_v \right\}.$$

Let $c \in C$.

Let $Z_j^*(\lambda)$ be the subset of $P_{Z(\lambda)}$ such that

$$Z_j^*(\lambda)\, d_j^{-1} c = R_Z \cap P\, d_j^{-1} c \text{ for } j = 1,\ldots, v.$$

Let $Z^{**}(\lambda) \subseteq H_Z$ such that $\underline{R_Z} = \sum_{i=1}^{v} \underline{Z_j^*(\lambda)}\, d_j^{-1}c + \underline{Z^{**}(\lambda)}$

Then the coefficient of ac in $[\underline{R}]^2$ is less than or equal to the coefficient of u^j in $[\underline{R}]^2$ for $j = 1,\ldots, p-1$. If equality holds for all such j then

(i) $R_X = P_{X(\lambda)}\, C^i(\lambda)$.

(ii) $R_Y = P_{Y(\lambda)}\, C^i(\lambda)$.

(iii) The coefficient of u^j in $[\,\underline{R_Z}\,]^2$ is

$$2 \sum_{i=1}^{v} \left|Z_j^*(\lambda)\right| - \left|P_{Z(\lambda)}\, C^i(\lambda)\right|$$

(iv) $C^i(\lambda)c = C^i(\lambda)$

<u>Proof</u>:

Again by Lemma 4 since $\underline{R} = \underline{S^i_{(\lambda)}}$ is rational, we have

$$|R(ac)| \leq |R(u^j)| \text{ for } j=1,\ldots,p-1.$$

We now assume that $|R(ac)| = |R(u^j)|$ for all j.

Put $D = C^i(\lambda)$.

Since $R_X \neq \emptyset$ holds there is some elementary trace say tr. $(ab^{wp^\lambda} d)$ in R_X. Then $a^{1-p}b^{w(1-p)p^\lambda} d \in R_X$ holds.

Now $(a^{1-p}b^{w(1-p)p^\lambda} d)^{-1} ac = a^p b^{-w(1-p)p^\lambda} d^{-1} c$ lies in H_Y unless we have $\lambda = 0$ and $\alpha = \beta + 1$. We exclude this case for the moment. Then by Lemma 4 we may conclude that $a^{1-p}b^{w(1-p)p^\lambda} d$ is in R(ac) since the only elements $h \in R_X$ such that $h \notin R(ac)$ satisfy $h^{-1}ac \in H_Z$. Thus we conclude that

$$\text{tr. } (a^p b^{-w(1-p)p^\lambda})\, d^{-1} c \text{ lies in } R.$$

Put $s = w(1-p)$. Again by Lemma 4 we have that $y \in R(ac)$ for every y occurring in tr. $(a^p b^{sp^\lambda}) d^{-1} c$.

By lemma 5 we have that as y runs through tr. $(a^p b^{sp^\lambda})$ the elements $y^{-1}a$ occur in every elementary trace of $P_{X(\lambda)}$. It thus follows that $P_{X(\lambda)} D \subseteq R$.

By the definition of $D = C^i(\lambda)$, no further elements of H_X can be in R. Thus we have that

$$\text{(i)} \qquad R_X = P_{X(\lambda)} C^i(\lambda).$$

We now turn to the case $\lambda = 0$, $\alpha = \beta + 1$.

Again from lemma 4 we have that p-1 of every p elements in every trace of $P_{X(\lambda)}$ occurring with $d_j \in D$ in R must lie in R(ac). From lemma 5 we have that as we let x run through such an elementary trace of $P_{X(\lambda)}$ the elements $x^{-1}ac$ lie in distinct traces of $P_{Z(\lambda)}$, indeed one in each trace of $P_{Z(\lambda)}$. It follows that we must have

$$|Z_j^*(\lambda)| > \tfrac{1}{2} |P_{Z(\lambda)}| \text{ for } j=1,\dots,v \text{ where}$$

$$D = \{d_1,\dots,d_v\}.$$

Now for some $z \in Z_j^*(\lambda)$ we must have $uz \in Z_j^*(\lambda)$ as well. Now

$$(uz)z^{-1} = u \implies uz \in R(u).$$

$$(uz)^s,\ z^{-s} \in Z_j^*(\lambda) \text{ hold if } (s,p) = 1.$$

Thus $(uz)^s \in R(u^s)$.

By lemma 4 since by hypothesis $|R(ac)| = |R(u^s)|$ for all such s we have that every element in tr. $(uz)\, d_j^{-1}c$ belongs to R(ac).

As we let x run through the elements of tr. $(uz)\, d_j^{-1}c$ we get that the elements $x^{-1}ac$ belong to every trace of $P_{X(\lambda)} d_j$.

It follows that $P_{X(\lambda)} D \subseteq R_X$ as before. Again from the definition of D we have

(i) $R_X = P_{X(\lambda)} D$.

We now show that in either case ($\lambda = 0$, $\alpha = \beta + 1$ or not) (ii) and (iii) hold.

Let $y \in P_{Y(\lambda)} Dc$.

Then we have $y^{-1}ac \in P_{X(\lambda)} D = R_X$.

By lemma 4 since $y \notin H_z$ we have $y^{-1}ac \in R(ac)$, thus $y \in R$.

We therefore have that $R_Y \supseteq P_{Y(\lambda)} Dc$.

If R_Y had any further element, it would necessarily be of the form xd, $x \in P$, $d \notin Dc$, and such an element cannot belong to R(ac) since $R_X = P_{X(\lambda)} D$.

Thus we conclude that

(ii) $R_Y = P_{X(\lambda)} Dc$.

It follows exactly as above that

$$|Z_j^*(\lambda)| = |P_{Z(\lambda)} d_j^{-1} c \cap R| > \tfrac{1}{2}|P_{Z(\lambda)}| \text{ for } j=1,\ldots,v.$$

Now it is not possible that $z \in R_Z$ belongs to R(u) but not to R(ac). Thus the coefficient of u in $[\underline{R_Z}]^2$ is

$|R(u) \cap R_Z| = |R(u) \cap R(ac) \cap R_Z|$.

(Elements of R_Z must be multiplied by other elements of R_Z to yield u since $R \subsetneq H_{(\lambda)}$ where $\lambda \neq \beta$.)

Only elements of PDc can belong to R(ac).

It is not possible that both z and uz be in $P_{Z(\lambda)}Dc - R_Z$ since then we would have

$z^{-1}ac$ and $(uz)^{-1}ac$ both belonging to $R(u) - R(ac)$

which is impossible by lemma 4.

Thus $z \in P_{Z(\lambda)}Dc - R_Z \Longrightarrow uz \in R(ac) - R(u)$. $uz \in R_Z - R(u)$ can only hold if $z^{-1} \notin R$ holds. Thus the coefficient of u in $[\underline{R_Z}]^2$ is

$$\left| P_{Z(\lambda)}{}^{Dc} \right| - \left| P_{Z(\lambda)}{}^{Dc} - R_Z \right| - \left| R_Z - R(u) \right|$$
$$= \left| P_{Z(\lambda)}{}^{Dc} \right| - 2\left| P_{Z(\lambda)}{}^{Dc} - R_Z \right|$$
$$= 2\left| R_Z \cap P_{Z(\lambda)}{}^{Dc} \right| - \left| P_{Z(\lambda)}{}^{D} \right|$$
$$= 2 \sum_{j=1}^{v} \left| Z_j^*(\lambda) \right| - \left| P_{Z(\lambda)}{}^{D} \right|$$

In addition since $p \neq 2$, we have $a^2 b^{p^\lambda} d_j \in R(ac)$ for $j=1,\ldots,v$ thus $(a^2 b^{p^\lambda} d_j)^{-1}\, ac \in R$, and $d_j^{-1} c \in D$ for $j=1,\ldots,v$.

Since D is inverse closed it follows that $D = Dc$.

This completes the proof of lemma 1.2.

We now put $i=1$ in lemmas 1.1 and 1.2 thus $S^i = S^1 = S$.

Since $\rho < \lambda \implies H_{(\rho)} H_{(\lambda)} \subseteq H_{(\rho)}$ it follows that $|S(h)| = \sum_{\lambda=0}^{\beta} |S_{(\lambda)}(h)|$ for $h \in AC$.

Now $|S_{(\lambda)}(ac)| \leq |S_{(\lambda)}(u^j)|$ holds for $\lambda = 0,\ldots,\beta$ and $|S(ac)| = \sum_{\lambda=0}^{\beta} |S_{(\lambda)}(ac)| = \sum_{\lambda=0}^{\beta} |S_{(\lambda)}(u^j)| = |S(u^j)|$ for $c \in C_o$ and $j=1,\ldots,p-1$ by theorem 6 since $u \in S \implies u^j \in S$ since $\underline{S}$ is rational, and C_o is by definition the subset of C satisfying $ac \in S$. Thus we conclude that for $c \in C_o$

$|S_{(\lambda)}(ac)| = |S_{(\lambda)}(u^j)|$ for all $j=1,\ldots,p-1$.

Let $C_o = \{c_1,\ldots, c_q\}$.

From lemma 1.1 we conclude that $\underline{S_{(\beta)}} = \underline{A - 1}\ \ \underline{C_o} + \underline{C^*}$.

Moreover, letting c run through the elements of C_o we have since $p \neq 2$, that $C_o c_i = C_o$ for $i=1,\ldots,q$, thus $C_o{}^2 = C_o$.

C_o was already known to be non-empty and inverse closed. Thus we have

<u>Lemma 1.3</u>

C_o is a <u>subgroup</u> of C.

By lemma 1.2 we have that $S_{X(\lambda)} \neq \emptyset \implies$

$$\underline{S_{X(\lambda)}} = \left[\underline{P_{X(\lambda)}}\ \underline{D}\right] + \left[\underline{P_{Y(\lambda)}}\ \underline{Dc_i}\right] + \sum_{j=1}^{v(\lambda)} \underline{Z_j^*(\lambda) d_j^{-1} c_i} + \underline{Z^{**}(\lambda)}$$

for $c_i \in C_o$ where $D = \{d_1, \ldots, d_{v(\lambda)}\}$, $Z^{**}(\lambda) \subseteq H_{Z(\lambda)}$ and $|Z_j^*(\lambda)| > \frac{1}{2} |P_{Z(\lambda)}|$.

Choosing $c_i = 1$ (since $1 \in C_o$ holds) we get from $Dc_i = Dc_j$ $(i,j=1,\ldots,q)$ that $D = Dc_j$ for $j=1,\ldots,q$, thus that D consists of full cosets of C_o. Choosing $c_1^\lambda, \ldots, c_{q(\lambda)}^\lambda$ as the coset representatives (thus $v(\lambda) = q(\lambda)q = q(\lambda)|C_o|$) we have that if $S_{X(\lambda)} \neq \emptyset$

$$\underline{S_{(\lambda)}} = \left[\underline{P_{X(\lambda)}} + \underline{P_{Y(\lambda)}}\right] \underline{C_o} \left[c_1^\lambda + \ldots + c_{q(\lambda)}^\lambda\right] + \sum_{i=1}^{q} \sum_{j=1}^{q(\lambda)} \underline{Z_{ij}^*(\lambda)} c_i c_j^\lambda$$
$$+ \underline{Z^{**}(\lambda)}$$

where $|Z_{ij}^*(\lambda)| > \frac{1}{2} |P_{Z(\lambda)}|$ holds for $i=1,\ldots,q$
$j=1,\ldots,q(\lambda)$

It also follows from lemma 1.2 that the coefficient of u in $\left[\underline{Z^{**}(\lambda)}\right]^2$ is zero.

#2

We now let μ be the smallest λ such that $S_{X(\lambda)} \neq \emptyset$ holds. We will show in this section that for any λ with $\mu \leq \lambda \leq \beta - 1$ we have

$$S_{(\lambda)} = P_{(\lambda)} C_o.$$

We will then show that $\mu = 0$, $C_o = C$ and that $S_{(\beta)} = P_{(\beta)} C_o - 1$, thus proving directly that $S = H - 1$.

By hypothesis, $S_{X(\mu)} \neq \emptyset$. Thus there is an element $ab^{tp^\mu} c$ in S where $(t,p) = 1$, $c \in C$. Now by theorem 6, we have $|S(ab^{tp^\mu} c)| = |S(u)|$. By lemma 4 we know that this can occur only if S has a special structure.

From #1 we have that for any λ we have either

$$S_{X(\lambda)} = \emptyset \quad \text{or}$$

$$\underline{S_{(\lambda)}} = \left[\underline{P_{X(\lambda)}} + \underline{P_{Y(\lambda)}}\right] \underline{C_o} \left[C_1^\lambda + \dots + C_{q(\lambda)}^\lambda\right]$$

$$+ \sum_{i=1}^{q} \sum_{j=1}^{q(\lambda)} \underline{Z^*_{ij}(\lambda)}\, C_i c_j^\lambda + \underline{Z^{**}(\lambda)}.$$

Lemma 2.1

Let $\mu \leq \lambda \leq \beta - 1$.

Then (i) $S_{X(\lambda)} \neq \emptyset$

(ii) $q(\lambda) = 1$

(iii) $C_1^\lambda \in C_o$

i.e. $S_{(\lambda)} = \left[\underline{P_{X(\lambda)}} + \underline{P_{Y(\lambda)}}\right] \underline{C_o} + \sum_{i=1}^{q} \underline{Z^*_i(\lambda)}\, c_i + \underline{Z^{**}(\lambda)}$

where $Z^*_i(\lambda)$ is the subset of $P_{Z(\lambda)}$ which we earlier denoted by $Z^*_{i1}(\lambda)$.

Proof:

We first note that if $\mu = \beta$ the lemma is vacuously true.

Thus we assume that $\mu < \beta$ holds. Let $ab^{tp^\mu} c \in S$, $((t,p) = 1,\ c \in C)$.

Let $0 < \nu < \beta - \mu$. Then since $\underline{S}$ is rational it follows that $(ab^{tp^\mu} c)^e \in S$ holds where e is chosen to satisfy the congruences

$$e \equiv 1 - p^\nu \quad (p^\alpha),$$

$$e \equiv 1 \quad (m)$$

By lemma 3, $(ab^{tp^\mu} c)^e \in S(u)$ holds. Now $(ab^{tp^\mu} c)^{-e}(ab^{tp^\mu} c)$ $= (ab^{tp^\mu})^{p^\nu} \notin H_Z$.

Thus we may conclude from lemma 4 that $(ab^{tp^\mu} c)^e$ cannot belong to $S(u) - S(ab^{tp^\mu} c)$, thus

$$(ab^{tp^{\mu}}c)^e \in S(ab^{tp^{\mu}}c) \text{ holds,}$$

i.e. $(ab^{tp^{\mu}}c)^{-e}(ab^{tp^{\mu}}c) \in S$.

Thus $(ab^{tp^{\mu}})^{p^{\nu}} \in S$ holds for $0 < \nu < \beta - \mu$.

But $ab^{tp^{\mu+\nu}} \in S^i \implies S^i \supseteq P_{X(\mu+\nu)} \cup P_{Y(\mu+\nu)}$ by lemma 1.2.

Thus $a^{p^{\nu}} b^{tp^{\mu+\nu}} \in S^i$ would also hold. Now $S \cap S^i = \emptyset$ or $S^i = S$. Thus we conclude that $S^i = S$, and that $ab^{tp^{\mu+\nu}} \in S$ holds for $0 < \nu < \beta - \mu$. $S_{X(\mu)} \neq \emptyset$ holds by hypothesis. Thus $S_{X(\lambda)} \neq \emptyset$ for $\mu \leq \lambda \leq \beta - 1$.

We have $(ab^{p^{\mu}})^{1-p^{\beta-\mu}} c_j^{\mu} \in S_{X(\mu)}$ for $j=1,\ldots,q(\mu)$.

We conclude from lemma 4 that

$$\left[ab^{p^{\mu}} c_1^{\mu}\right]\left[(ab^{p^{\mu}})^{1-p^{\beta-\mu}} c_j^{\mu}\right]^{-1} = a^{p^{\beta-\mu}} c_1^{\mu}(c_j^{\mu})^{-1} \in S \text{ holds.}$$

By the definition of C_o and by lemma 1.1 it follows that

$$c_j^{\mu} \in C_o\, c_1^{\mu} \text{ holds for } j=1,\ldots,q(\mu).$$

Since the c_j^{μ} were coset representatives it follows that $q(\mu) = 1$.

Now $y = a^p b^{p^{\lambda}} c_j^{\lambda} \in S_Y$ holds by lemma 1.2 for $\lambda = \mu+1,\ldots,\beta-1$.

By lemma 4 we conclude that $y \notin S(ab^{p^{\mu}} c_1^{\mu})$ must hold, thus $(a^p b^{p^{\lambda}} c_j^{\lambda})^{-1} ab^{p^{\mu}} c_1^{\mu} \in S$ holds.

Thus by what we have just shown, since this is clearly an element of $S_{X(\mu)}$, we have $(c_j^{\lambda})^{-1} \in C_o$ for $\lambda = \mu+1,\ldots,\beta-1$, $j=1,\ldots,q(\lambda)$.

Thus $q(\lambda) = 1$ for $\lambda = \mu+1,\ldots,\beta-1$ and we may choose $c_1^{\lambda} = 1$.

Since $p \neq 2$ have $a^2 b^{2p^{\mu}}(c_1^{\mu})^{-1} \in S_{X(\mu)}$, hence

$$(a^2 b^{2p^{\mu}}(c_1^{\mu})^{-1})^{-1} ab^{p^{\mu}} c_1^{\mu} = a^{-1} b^{-p^{\mu}}(c_1^{\mu})^2 \in S_{X(\mu)}.$$

Thus $(c_1^{\mu})^2 \in C_o\, c_1^{\mu}$, and $c_1^{\mu} \in C_o$.

Thus we may choose $c_1^{\mu} = 1$.

This completes the proof of lemma 3.1.

We now show that $Z_i^*(\lambda) = P_{Z(\lambda)}$ for $i=1,\dots,q$ $\lambda=\mu,\dots,\beta-1$.

The idea is to note that for $z \in P_{Z(\lambda)}$, $zc_i \notin S \implies zc_i \in S^j$ for some $j \geq 2$.

S^j would have to have some element xd ($x \in P$, $d \in C$) of order divisible by p^{α} since $\langle S^j \rangle = H$.

Then $|S(zc_i)| = |S(xd)|$ would have to hold by theorem 6.

We will use lemmas 4, 5 and 7 to show that such an equality cannot hold.

Lemma 2.2

$$S \supsetneqq \langle a \rangle \langle b^{p^{\mu}} \rangle C_o - 1$$

Proof:

Assume the contrary.

Let $K = \langle a \rangle \langle b^{p^{\mu}} \rangle C_o$.

We already know that $S \supseteq K_X$ by lemma 2.1. Thus there exists $k \in K_Y \cup K_Z - S$ with $k \neq 1$.

Let $k \in S^j$ and let $xd \in S^j$ be an element of order divisible by p^{α}, where $x \in P$, $d \in C$.

Since $xd \notin S$, we have either $x \in P_{X(\nu)}$ for some $\nu < \mu$ or $d \notin C_o$.

We treat these cases separately.

Case (i):

Let $x \in P_{X(\nu)}$ where $\nu < \mu$ holds. By the minimality of μ, $S_{X(\rho)} = \emptyset$ for $\rho < \mu$ and therefore in $\left[\underline{S_{(\rho)}}\right]^2$ xd has coefficient zero (since the a-exponent of every element occurring there is divisible by p and the a-exponent of x is prime to p).

Since in general, $\rho < \tau \Rightarrow H(\rho)H(\tau) \subseteq H(\rho)$, it follows that the only contribution to $|S(xd)|$ comes from $\underline{S_{(\nu)}}\ \underline{S_X}$, thus from $\underline{S_{(\nu)}}\left[\sum_{\lambda=\mu}^{\beta} \underline{P_{X(\lambda)}}\ \underline{C_o}\right]$.

Were z and uz both to belong to $S_{(\nu)}$ the coefficient of u in $\left[\underline{S_{(\nu)}}\right]^2$ would be greater than zero. This would contradict $|S(u)| = |S(a)|$ since $|S_{(\lambda)}(a)| \leq |S_{(\lambda)}(u)|$ holds for $\lambda = 0,\dots,\beta$ and $|S_{(\nu)}(a)| = 0$. Thus at most half of the elements z of $H_{Z(\nu)}$ which satisfy $z^{-1}xd \in H_{(\lambda)}$ can occur in $S_{(\nu)}$.

It therefore follows that for every element of K_X which belongs to S(xd) there is another element of K_X which does not belong to S(xd).

Now $h \in S_X = K_X \Rightarrow h^{-1} k \in K_X \subseteq S$

Thus we have that $S_X \subseteq S(k)$.

Thus there is a 1-1 correspondence between the elements of $S_{(\nu)}$ which belong to S(xd) and the elements of S_X which belong to S(xd) and since in this way we get at most one-half the elements of S_X it follows that

$$|S(xd)| \leq |S_X| \text{ holds.}$$

Moreover, we have just shown that $S(k) \supseteq S_X$. It not suffices to exhibit an element of S(k) which does not belong to S_X.

We claim that a^p is such an element. $a^p \in S$ holds by lemma 1.1, since $1 \in C_o$.

$$\nu < \mu \Rightarrow \mu \neq 0.$$

Thus since $k \in K_Y \cup K_Z$ holds, we have $k = a^{sp^\lambda} b^{tp^\tau} c$ where $\alpha - \lambda \leq \beta - \tau \leq \beta - \mu \leq \beta - 1$.

Thus we have $\lambda > 1$ and $a^{-p}k \in K_Y \subseteq S$.

Thus we have $a^p \in S(k) - S_X$.

This completes the proof that $|S(k)| > |S(xd)|$ holds, under the hypothesis $x \in P_{X(\nu)}$ where $\nu < \mu$.

<u>Case (ii)</u>:

We now suppose $x \in P_{X(\nu)}$ where $\nu \geq \mu$ holds, hence $d \notin C_o$.

The contribution to $|S(xd)|$ now comes from

$$2\left[\sum_{\lambda=\nu}^{\beta} \underline{P_{X(\lambda)}}\ \underline{C_o}\right] \underline{Z^{**}(\nu)} + 2\underline{P_{X(\nu)}}\ \underline{C_o}\left[\sum_{\lambda=\nu}^{\beta-1} \underline{Z^{**}(\lambda)}\right]$$

$$+\ 2\underline{P_{X(\nu)}}\ \underline{C_o}\ \underline{C^*} + 2 \sum_{\mu \leq \lambda < \nu} (\underline{P_{X(\lambda)}}\ \underline{C_o})\ (\underline{Z^{**}(\lambda)})$$

Now precisely as in case (i) we conclude that the contribution from the 1st, 2nd and 4th terms is

$$\leq \sum_{\lambda=\mu}^{\beta-1} |P_{Z(\lambda)}|\ |C_o|$$

Now only elements of the form xc_i may be multiplied by an element of C^* to yield an xd.

Thus the contribution from term 3 is at most $2|C_o| = 2q$.

Thus we have $|S(xd)| \leq \sum_{\lambda=\mu}^{\beta-1} |P_{Z(\lambda)}|\, q + 2q$.

Again as in case 1 we have $P_{X(\lambda)}\, C_o \subseteq S(k)$ for $\lambda = \mu, \ldots, \beta$.

Thus we have $|S(k)| \geq \sum_{\lambda=\mu}^{\beta} |P_{X(\lambda)}|\,|C_o|$, and

$$|S(k)| - |S(xd)| \geq \sum_{\lambda=\mu}^{\beta} |P_{X(\lambda)}|\, q - \sum_{\lambda=\mu}^{\beta-1} |P_{Z(\lambda)}|\, q - 2q$$

$$= q \sum_{\lambda=\mu}^{\beta-1} \left[\Phi(p^{\alpha})\,\Phi(p^{\beta-\lambda}) - p^{\beta-\lambda}\,\Phi(p^{\beta-\lambda})\right] + \Phi(p^{\alpha})q - 2q$$

$$= q \sum_{\lambda=\mu}^{\beta-1} \Phi(p^{\beta-\lambda})\left[p^{\alpha-1}(p-1) - p^{\beta-\lambda}\right] + q\left[p^{\alpha-1}(p-1) - 2\right]$$

$$\geq q \sum_{\lambda=\mu}^{\beta-1} \Phi(p^{\beta-\lambda})\left[p^{\beta} - p^{\beta-\lambda}\right] + q\left[p^{\alpha-1}(p-1) - 2\right] > 0$$

since the 1st term is ≥ 0 and the second term is > 0 since $\alpha > 1 \Longrightarrow p^{\alpha-1} \geq p \geq 3$.

This completes the proof that $k \in S$. We conclude that for $\lambda = \mu, \ldots, \beta-1$.

$\underline{S_{X(\lambda)}} = \underline{P_{(\lambda)}C_o} + \underline{Z^{**}(\lambda)}$ then follows:

Lemma 2.3

Let $\mu \neq \beta$.

Let $S = \sum_{\lambda=0}^{\mu-1} \underline{Z^{**}(\lambda)} + \sum_{\lambda=\mu}^{\beta-1} \left[\underline{P_{(\lambda)}C_o} + \underline{Z^{**}(\lambda)}\right] + \left[\underline{A-1}\right]\underline{C_o} + \underline{C^*}$.

Let $K = \langle a \rangle \langle b^{p^{\mu}} \rangle C_o$.

Then $Z^{**}(\lambda) = \emptyset$ for $\lambda = 0, \ldots, \beta-1$.

Proof:

We have that $K-1 \subseteq S$ and that $a \in K$ holds. $S_X = K_X$.

Since the coefficient of a in $\left[\underline{S_Y}\right]^2 + 2\underline{S_Y}\,\underline{S_Z} + \left[\underline{S_Z}\right]^2$ is clearly zero, the contribution to $|S(a)|$ comes solely from $\left[\underline{S_X}\right]^2 + 2\underline{S_X}\left[\underline{S_Y} + \underline{S_Z}\right]$.

Now since K is a subgroup of H, for $k \in K$ we may conclude from $kh = a$ that $h = k^{-1}a \in K$.

Thus the total contribution to $|S(a)|$ comes from $\left[\underline{K-1}\right]^2$.

It is easily seen that $\left[\underline{K-1}\right]^2 = (|K| - 2)\left[\underline{K-1}\right] + (|K|-1) \cdot \underline{1}$

Thus since $|S(a)| = |S(k)|$ for $k \in K-1$ by theorem 6, it follows that there can be no contribution to any $k \in K-1$ from any $\left[\underline{Z^{**}(\lambda)}\right]^2$.

Now let $zd \in Z^{**}(\lambda)$, $(z \in P,\ d \in C)$ where $0 \leq \lambda < \beta - 1$.

Then $z^{1-p^{\beta-\lambda-1}}d \in Z^{**}(\lambda)$ holds. Thus we have $(z^{1-p^{\beta-\lambda-1}}d)^{-1} \in Z^{**}(\lambda)$.

Thus in $\left[\underline{Z^{**}(\lambda)}\right]^2$, $(z^{1-p^{\beta-\lambda-1}}d)^{-1}zd = z^{p^{\beta-\lambda-1}}$ occurs with non-zero coefficient. It is in $P_{Z(\beta-1)}$.

$P_{Z(\beta-1)} \subseteq K$ holds since $\mu \neq \beta$.

Since $p \neq 2$ we have for $zd \in Z^{**}(\beta-1)$, $(z \in P, d \in C)$ that $z^2 d \in P_{Z(\beta-1)}$ holds, $z^{-2}(d)^{-1}zd = z^{-1} \in P_{Z(\beta-1)}$. We conclude that $Z^{**}(\beta-1) = \phi$ as well.

Now $S_{(o)} \neq \emptyset$ since $\langle S \rangle = H$ requires that S have an element whose b exponent is not divisible by p.

By what we have just shown, we have $\underline{S} = \sum_{\lambda=\mu}^{\beta-1} \underline{P_{(\lambda)}C_o} + [\underline{A}-\underline{1}]\underline{C_o}$ $+ \underline{C^*}$ unless $\mu = \beta$.

Thus there remain only two possibilities:

$$\text{(i)}\quad \mu = \beta, \quad \underline{S} = \sum_{\lambda=0}^{\beta-1} \underline{Z^{**}(\lambda)} + \underline{AC_o} - \underline{1} + \underline{C^*}$$

$$\text{(ii)}\quad \mu = 0, \quad \underline{S} = \sum_{\lambda=0}^{\beta-1} \underline{P_{(\lambda)}\,C_o} + \underline{AC_o} - \underline{1} + \underline{C^*}$$

#3

In this section we assume throughout that $\mu = \beta$. We will show that this leads to a contradiction.

<u>Lemma 3.1</u>

Let $h \in S^i$ where $i \geq 2$. Then $|S(h)| \leq 2$.

<u>Proof:</u>

S^i must contain some element x of order divisible by p^{α} since $\langle S^i \rangle = H$. Then $|S(h)| = |S(x)|$ must hold. $\underline{S} = \underline{S_X} + \underline{S_Y} + \underline{S_Z}$

$$[\underline{S}]^2 = [\underline{S_X} + \underline{S_Y}]^2 + 2\underline{S_X}\,\underline{S_Z} + 2\underline{S_Y}\,\underline{S_Z} + [\underline{S_Z}]^2.$$

Clearly x cannot occur in $2\underline{S_Y}\,\underline{S_Z} + [\underline{S_Z}]^2$ since such elements are products of elements with a exponent divisible by p.

Now $\underline{S_X} + \underline{S_Y} = [\underline{A} - \underline{1}]\underline{C_o}$.

In $[\underline{AC_o}]^2$ the only elements of H_X which occur belong to S.

Hence the only contribution to the coefficient of x (which does not belong to S) is from $2\,\underline{S_X}\,[\underline{S_Z - C_o}]$.

Suppose $s_1, s_2 \in S_Z - C_o$ such that $s_1^{-1}x \in S$, $s_2^{-1}x \in S$. Since $s_1, s_2 \in S_Z$ and $x \in H_X$ it follows that we have $s_1^{-1}x, s_2^{-1}x \in S_X \subseteq AC_o$. Thus we have $(s_1^{-1}x)^{-1}(s_2^{-1}x) = s_1 s_2^{-1} \in AC_o$.

In $[\underline{AC_o} - \underline{1}]^2$ the coefficient of $s_1 s_2^{-1}$ is $|AC_o| - 2$ which is the coefficient of a in $[\underline{S}]^2$.

Thus $s_1 \neq s_2 \implies |S(s_1 s_2^{-1})| > |S(a)|$ which cannot occur.

Thus there is at most one $s_1 \in S_Z - C_o$ satisfying $s_1^{-1}x \in S$ and if there exists such an s_1 we have

$$|S(x)| = 2 = |S(h)|.$$

Thus we have either $|S(h)| = 0$ or $|S(h)| = 2$ and lemma 3.1 is proved.

It now follows that $|S(h)| > 2 \implies h \in S$ if $h \neq 1$.

<u>Lemma 3.2</u>

Let $0 \leq \lambda \leq \beta - 1$.

Let $\underline{S_{(\lambda)}} = \sum_{j=1}^{v(\lambda)} \underline{Z_j^{**}(\lambda)}\, d_j^{\lambda}$ where $Z_j^{**}(\lambda) \subseteq P_{Z(\lambda)}$ for $j = 1, \ldots, v(\lambda)$. Then for all $1 \leq i, j \leq v(\lambda)$, we have that $Z_j^{**}(\lambda) = Z_i^{**}(\lambda)$ is a single elementary trace of $P_{Z(\lambda)}$.

<u>Proof</u>:

Let $a^x b^{p^\lambda} d_1^{\lambda}$, $a^y b^{p^\lambda} d_j^{\lambda} \in S$.

Then $[\underline{S_{(\lambda)}}]^2$ contributes to the coefficient of $a^{x-y} d_1^{\lambda} (d_j^{\lambda})^{-1}$.

Unless $x = y$, $d_1^{\lambda} = d_j^{\lambda}$ we cannot have $d_1^{\lambda}(d_j^{\lambda})^{-1} \in C_o$ since $|S(a^{x-y}c_i)| = qp^{\alpha} - 2 = |S(a)| = |S(a^{x-y}c_i) \cap AC_o|$ for

$c_i \in C_o$, $a^{x-y}c_i \neq 1$. Thus since $1 \in C_o$ holds it is clear that $Z_j^{**}(\lambda)$ cannot have two distinct elementary traces. Suppose we have $a^{x-y}(d_1^\lambda)(d_j^\lambda)^{-1} \in S^i$ for some $i \geq 2$.

By lemma 1.1 we have that $ad_1^\lambda (d_j^\lambda)^{-1} \in S^i$ must hold.

We have from lemma 3.1 that $|S(ad_1^\lambda (d_j^\lambda)^{-1})| = 0$ or 2.

$|S(ad_1^\lambda (d_j^\lambda)^{-1})| = 0$ contradicts $|S(a^{x-y}d_1^\lambda (d_j^\lambda)^{-1})| > 0$.

$|S(ad_1^\lambda (d_j^\lambda)^{-1})| = 2$ can occur only if C^* has an element of $C_o d_1^\lambda (d_j^\lambda)^{-1}$. In this case it follows that in $\left[\underline{S_{(\beta)}}\right]^2$ $a^{x-y} d_1^\lambda (d_j^\lambda)^{-1}$ occurs with coefficient 2 as well. Thus we get $|S(a^{x-y}d_1^\lambda (d_j^\lambda)^{-1})| > 2 = |S(ad_1^\lambda (d_j^\lambda)^{-1})|$. This contradiction is avoided only if $a^{x-y}d_1^\lambda (d_j^\lambda)^{-1} \in S^o = \{1\}$, thus $a^x = a^y$, $d_1^\lambda = d_j^\lambda$.

This completes the proof of lemma 3.2.

Since $S_{(o)} \neq \emptyset$ (because the elements of S generate H) we have that $\underline{S_{(o)}} = \underline{Z_1^{**}(0)}\left[d_1 + .. + d_v\right]$ where $d_i^o = d_i$ and $v(o) = v$.

<u>Lemma 3.3</u>

Let $\underline{Z_1^{**}}\,(o) = \text{tr.}\,(z)$, $D = \{d_1, \ldots, d_v\}$, hence $\underline{S_{(o)}} = \text{tr.}(z)\underline{D}$.

Then $S \supseteq \langle z \rangle D - 1$

<u>Proof</u>:

For $\lambda > 0$ and any of $\Phi(p^B)$ choices of s we have

$z^s\, d_i\, z^{-s+tp^\lambda}\, d_k = z^{tp^\lambda}\, d_i d_k$ with $z^{-s+tp^\lambda}\, d_k \in S_{(o)}$

since $\underline{S_{(o)}}$ is rational.

For $\lambda = 0$ there are $p^{\beta-1}(p-2)$ choices for s (excluding $s \equiv t\ (p)$).

Thus for $\beta > 1$ we have $|S(z^{tp^\lambda} d_i\, d_k)| \geq p^{\beta-1}(p-2) \geq p > 2$ for any t with $(t,p) = 1$, any $\lambda = 0,\ldots,\beta$ and any i,k between 1 and v.

Thus $z^{tp^\lambda} d_i\, d_k \in S$ unless $\beta = 1$. If $\beta = 1$ we have that $\underline{S} = \underline{AC_o}\text{-}\underline{1} + \underline{D\text{-}1} + \text{tr.}\,(z)\,\underline{D}$ since $\underline{S}^{(p)} \equiv \gamma \cdot \underline{1}$ (mod p) must hold.

Now from $\left[\underline{S_{(o)}}\right]^2$ we still get a contribution to $|S(z^t\, d_i d_k)|$ of at least $p^{\beta-1}(p-2) \geq 1$.

In addition if $d_i \neq 1$ we get a further contribution of at least 2 from $2\, \underline{S_{(o)}}\, \underline{S_{(1)}}$, namely from $2\,(z^t d_k) d_i$.

Thus we have $|S(z^t d_i d_k)| > 2$ unless $d_i = 1$.

This means $z^t d_i d_k \in S$ unless $d_i = 1$ in which case we have obviously $z^t d_i d_k = Z^t d_k \in S$.

We also have $z^{tp} d_i d_k = d_i d_k \in S$ in the case $\beta = 1$ unless $d_i d_k = 1$.

Now with $\lambda = 0$, $t = 1$, we get $z d_i d_k \in S$ for any i,k between 1 and v.

Thus $d_i d_k \in D$ for any $d_i, d_k \in D$.

We know since $\underline{S_{(o)}}$ is rational that D is inverse closed.

Thus D is a subgroup of C.

Now as we let t and λ vary through all possible values, we get $z^{tp^\lambda} d_i d_k \in S$, unless $\lambda = \beta$, $d_i = d_k^{-1}$, thus $S \supseteq \langle z \rangle D - 1$.
We now calculate $|S(z)|$. Since D is a subgroup we have $1 \in D$, hence $z \in S$.

$$\left[\underline{S}\right]^2 = \left[\underline{S_{(o)}} + \left(\sum_{\lambda=1}^{B} \underline{S_{(\lambda)}}\right)\right]^2 = \left[\underline{S_{(o)}}\right]^2 + 2\underline{S_{(o)}}\left[\sum_{\lambda=1}^{B} \underline{S_{(\lambda)}}\right]$$
$$+ \left[\sum_{\lambda=1}^{B} \underline{S_{(\lambda)}}\right]^2.$$

Elements of the 3rd term have b exponent divisible by p and $z \in S_{(o)}$ does not.

Thus the contribution to $|S(z)|$ comes only from the 1st two terms.

Since $S_{(o)}$ has only elements of $\langle z \rangle D$, and we have $y^{-1}z \notin \langle z \rangle D$ only for $y \in \langle z \rangle D$, the contribution to $|S(z)|$ comes only from $\left[\underline{\langle z \rangle D} - \underline{1}\right]^2$ and this contribution is clearly $|D|\, p^{\beta} - 2$ since z is of order p^{β} (since it is in $P_{Z(O)}$).

But $|S(a)| = qp^{\alpha}-2 = |C_o|\, p^{\alpha}-2$.

$|S(a)| = |S(z)| \Longrightarrow |D|\, p^{\beta}-2 = |C_o|\, p^{\alpha}-2$. Thus $|D| = |C_o|\, p^{\alpha-\beta}$.

But $\alpha > \beta \Rightarrow p \mid |D|$.

This is impossible since D is a subgroup of C which has order prime to p. Thus $\mu = \beta$ cannot occur, and we conclude that $\mu = 0$,

$$\underline{S} = \sum_{\lambda=0}^{\beta-1} \underline{P_{(\lambda)}C_o} + \underline{AC_o} - \underline{1} + \underline{C}^*$$

#4

To complete the proof of theorem A we need now only show that $C^* = \emptyset$ and $C_o = C$.

Lemma 4.1

$C^* = \emptyset$.

Proof:

Since $(|C|, p) = 1$, $\underline{C_o}^{(p)} = \underline{C_o}$.

Thus $\underline{C}^{*(p)}$ has no element of C_o.

1 occurs in S^o, hence not in S.

If $1 \neq c^* \in C^*$ held, $(c^*)^p$ would occur with coefficient 1 in $\underline{S}^{(p)}$.

This would contradict theorem 4.

We therefore conclude that $C^* = \emptyset$ and that $\underline{S} = \underline{PC_o} - \underline{1}$ where $C_o \leq C$ (since $A = P_{(\beta)}$).

Now $\langle S \rangle = H$ since G is primitive, but it is evident that $\langle S \rangle = PC_o$. Thus we have that $PC_o = PC = H$ and $S = H - 1$.

Since $S^o = 1$, $S = S^1 = H - 1$ and $S^i \cap S = \emptyset$ for $2 \leq i \leq r$, it follows that $r \geq 2$ cannot occur. Thus we conclude that $r = 1$, and with the help of theorem B, we have a complete proof of theorem A.

REFERENCES

1. Burnside, W.: Theory of Groups of finite order (1911) 2nd ed. Cambridge University Press.

2. Schur, I.: Zur Theorie der einfach transitiven Permutationsgruppen. Sitzungsberichte Preuss. Akad. Wiss., phys.-math. Kl. (1933) pp. 598-623.

3. Wielandt, H.: Zur Theorie der einfach transitiven Permutationsgruppen. Math. Zeitschrift (1935) vol. 40, pp. 582-587.

4. Kochendörffer, R.: Untersuchungen über eine Vermutung von W. Burnside. Schriften math. Sem. Inst. angew. Math. Univ. Berlin (1937), vol. 3, pp. 155-180.

5. Wielandt, H.: Permutationsgruppen (1954).

6. Wielandt, H.: Zur Theorie der einfach transitiven Permutationsgruppen II. Math. Zeitschrift (1949), vol. 52, pp. 384-393.

7. Scott, W. R.: Solvable Factorizable groups. Illinois Journal of Mathematics (1957), vol. 1, pp. 389-394.