THE SYLOW SUBGROUPS OF THE SYMMETRIC GROUPS

A. J. WEIR

The aim of this paper is to give a direct approach to the study of the Sylow $p^n$-subgroups $S_n$ of the symmetric group of degree $p^n$. [We assume throughout that $p \neq 2$.] Many of the results are already known and are treated in a paper by Kaloujnine where he uses a particular representation by means of "reduced polynomials." It has seemed worth while to restate some of his results using the concept of complete product $L \circ M$ of two permutation groups $L, M$ which he and Krasner have recently emphasised. This elementary notion is of great importance in the theory of finite groups and it appears in the literature in different forms. A simple interpretation is given in §2 in terms of permutation matrices which shows the strong connection between the operation $\circ$ and imprimitivity. The associative rule for $\circ$ follows from the associative law of matrix multiplication and we show that $S_n \cong C \circ C \circ \cdots \circ C (n \text{ factors})$ where $C$ is cyclic of order $p$; various expressions of $S_{n+n}$ as $S_n \circ S_n$ allow us to express $S_{n+n}$ as a split extension and to investigate many properties of $S_{n+n}$ by an inductive process. Since the Sylow $p^n$-subgroups of the classical groups (general linear, symplectic, orthogonal and unitary) over a finite field with characteristic prime to $p$ are direct products of the basic subgroups $S_n \cong \overline{C} \circ C \circ \cdots \circ C (n \text{ factors})$ where $\overline{C}$ is cyclic of order $p^r (r \geq 1)$, it is hoped that the treatment here may also suggest ways in which these groups $S_n$ may be studied.

$S_{n+1} \cong C \circ S_n$ and so $S_{n+1} \cong A^n \cdot S_n$ where $A^n$ is elementary abelian of order $p^{n^2}$. We show that all the factors of the series $A^n > (A^n, S_n) > (A^n, S_n, S_n) > \cdots$ are cyclic of order $p$ and this leads naturally to a description of certain subgroups of $S_n$ in terms of partition diagrams. The main result of the paper is to show finally that the characteristic subgroups are precisely the normal partition subgroups.*

This material was largely the content of Chapter 3 of my Cam-

Received by the editors April 5, 1954.

1 See [2] and [3, part I, p. 212, note 5].

2 See [3] and [4] (summary of results contained in [3]).

3 [5, §172] gives an inductive construction of $S_n$ which is essentially the same as ours. The complete product is the Kranz group of Pólya [6, p. 178]. See also [7].

4 [9].

5 There is a strong similarity between the partition subgroups treated here and the partition subgroups in [8].

534
bridge Ph.D. thesis and it is a great pleasure to acknowledge the encouragement and kindness of Professor Philip Hall who supervised my research in Cambridge during the years 1949–1952.

1. Retractions and lower central series. A retraction \( \phi \) of a group \( G \) is a homomorphism of \( G \) into itself for which \( \phi^2 = \phi \).

\( \phi \) has kernel \( H \) and image \( L \), say. Clearly \( \phi \) acts as the identity on \( L \).

I. If \( x \in H \cap L \), then \( \phi(x) = 1 \) and \( \phi(x) = x \).

II. \( HL = G \). If \( g \in G \) put \( \phi(g) = x \) and \( g = xy \). Then \( x = \phi(y)x \), so that \( \phi(y) = 1 \) and \( y \in H \).

Conversely if \( G \) is a split extension \( G = HL \), \( H \cap L = 1 \), \( H \) normal in \( G \), then each element of \( G \) is uniquely expressible in the form \( yx \) (\( y \in H \), \( x \in L \)) and \( \phi : yx \rightarrow x \) is a retraction.

There is a (1–1) correspondence between retractions of \( G \) and expressions of \( G \) as a split extension.

Under a retraction \( \phi \) the lower central series \( G' \supset G'' \supset \cdots \) of \( G \) maps onto the lower central series \( L' \supset L'' \supset \cdots \) of \( L \) and \( \phi_k = \phi \mid G_k \)

is clearly a retraction of \( G_k \). If \( H_k \) is defined inductively: \( H_1 = H \), and \( H_{k+1} = (H_k, G) \), we shall show that \( H_k \) is the kernel of \( \phi_k \) and hence

**Theorem 1.** \( G_k = H_k L_k \) (\( k = 1, 2, \cdots \)).

Suppose \( H_r \) is the kernel of \( \phi_r \) then the kernel \( K \) of \( \phi_{r+1} \) certainly contains \( (H_r, G) \) and \( (G_r, H) \), since \( \phi(H) = 1 \). Now \( \phi(y,x_r, yx) = (x_r, x) \) and so by expanding the commutator we see that \( K \) is in any normal subgroup of \( G \) containing \( (H_r, G) \) and \( (G_r, H) \). The result now follows by the

**Lemma 1.** If \( P \) is a normal subgroup of \( G \) and we define by induction \( P_1 = P \), \( P_{r+1} = (P_r, G) \), then \( (G_k, P) \subset (P_k, G) \).

The lemma is true for \( k = 1 \); assume \( (G_{r-1}, P) \subset P_r \), for all \( P \). Now \( (G_r, P) = (G_{r-1}, G, P) \). Also \( (G, P, G_{r-1}) = (P_2, G_{r-1}) \supset (P_r, G) = P_{r+1} \) by the induction hypothesis applied to \( P_2 \), and \( (P, G_{r-1}, G) \subset (P_r, G) = P_{r+1} \) by the induction hypothesis. Hence \( (G_r, P) \subset P_{r+1} \).

**Remark.** If \( H \) is abelian we may simplify \( (H_k, G) \) to the form \( (H_k, L) \).

2. Complete products. If \( G \) is a permutation group of degree \( r \) we apply \( \sigma \in G \) to the columns of \( 1 \), and obtain a matrix \( M(\sigma) \). Post-

multiplication of an \((r \times r)\) matrix by \( M(\tau) \) permutes the columns by

\*If \( A, B, C \) are any subgroups of \( G \), then any normal subgroup which contains \((A, B, C)\) and \((B, C, A)\) also contains \((C, A, B)\). See [10, p. 47] or [11, Chap. II, §6, Theorem 14].
τ and so in particular $M(\tau)M(\tau) = M(\sigma\tau)$. It follows that $\sigma \rightarrow M(\sigma)$ is a faithful representation of $G$. Premultiplication of an $(r \times r)$ matrix by $M(\sigma^{-1})$ applies a permutation to the rows which must be $\sigma$ since $M(\sigma^{-1})M(\sigma) = 1$.

Let $G$ be imprimitive with systems of imprimitivity $1, \ldots, m$; $m+1, \ldots, 2m$; $\cdots$; $mn$. Any $\sigma \in G$ induces a permutation $\sigma'$ of these systems. In matrix notation $\sigma'$ becomes an $(n \times n)$ matrix $M'(\sigma')$ of $(m \times m)$ blocks obtained by applying $\sigma'$ to the “columns” of $1_{mn}$. [This is just the usual $M(\sigma')$ magnified $m$ times.] If $\sigma' = 1$, $\sigma$ permutes the systems of imprimitivity inside themselves and so may be written $\sigma = \tau_1 \cdots \tau_n$ where the $\tau_i$ commute among themselves. These considerations suggest the following definition:

Given permutation groups $A$, $B$ of degrees $m$, $n$ respectively, the group of all

$$\begin{bmatrix}
A_1 & \cdots \\
\vdots & \\
A_n
\end{bmatrix}$$

where $A_i \in M(A)$ and $B* \in M*(B)$ is denoted by $A \circ B$ and is called the complete product of $A$ and $B$.

$A \circ B$ has degree $mn$, and may again be viewed as a permutation group. If $B*$ represents the permutation $b \in B_i$, transformation by $B*$ applies $b$ to the rows and columns and so

$$B^{*-1}\begin{bmatrix}
A_1 & \\
\vdots & \\
A_n
\end{bmatrix}B* = \begin{bmatrix}
A_{b(1)} & \\
\vdots & \\
A_{b(n)}
\end{bmatrix}.$$ 

If $S_m$ is the symmetric group of degree $m$ then the above construction shows that $G$ is an imprimitive permutation group if and only if $G$ is a subgroup of some $S_m \circ S_n$.

If $G = A \circ B$ the homomorphism $\phi : \sigma \rightarrow \sigma'$ is clearly a retraction of $G$ onto $B$ with kernel $(A)^n$ (direct product), and so $G$ is expressed as a split extension

$$(A)^n \cdot B, \quad (A)^n \cap B = 1.$$ 

Since matrix multiplication is associative it follows that $A \circ (B \circ C) \cong (A \circ B) \circ C$ for any three permutation groups $A$, $B$, $C$. We may thus write down without ambiguity such expressions as $S_n \cong C \circ C \circ \cdots \circ C$ ($n$ factors) where $C$ is cyclic of order $p$. This $S_n$ is a permutation group of degree $p^n$ and order $p^{1+p+p^2+\cdots+p^{n-1}}$ and so is a Sylow $p$-subgroup of $S_{p^n}$. A Sylow $p$-subgroup of any $S_r$ is a direct product
of such basic $S_n$ so we shall restrict our discussion to them.

3. **The special case** $S_2$. $S_2$ may be expressed in terms of generators $x; z_1, \cdots, z_p$ each of order $p$, such that the $z$’s commute and $x^{-1}z_i x = z_{i+1}$ (suffixes mod $p$).

$A$ is the elementary abelian subgroup generated by $z_1, \cdots, z_p$.

We define a new basis of $A$ as follows:

$y_0 = z_1, \quad (y_i, x) = y_{i+1}$ \quad ($i = 0, 1, \cdots$).

Then $y_0 = z_1, \quad y_1 = z_2 z_1^{-1}, \cdots, y_k = z_{k+1} z_k^{-1} \cdots z_1^{(-1)^k}$ and so in particular $y_{p-1} = z_1 \cdots z_p$ and $y_p = 1$ ($p \neq 2$).

We may take $y_0, \cdots, y_{p-1}$ as basis of $A$. The chain $A > (A, S_1) > \cdots$ written $A_0 > A_1 > \cdots$ is given by the rule $A_i = [y_i, y_{i+1}, \cdots]$.

We notice the important fact that each factor has order $p$. The lower central series is $S_2 > A_1 > A_2 > \cdots > A_p = 1$ so $S_2$ has class $p$.

The upper and lower central series coincide.\(^8\)

If $a \in A$ we define $a_0 = a$, $(a_i, x) = a_{i+1}$ and then

$$(xa)^2 = x^2 a z a = x^2 a^2 a_1$$

$$(xa)^k = x^k a z_{k-1} \cdots a z_{1} = x^k a z_{1} a_{1} \cdots a_{k-1}$$

and so

$$(xa)^p = a^1 z_2 \cdots z_{k-1} = a_p^{-1}.$$ 

If $a = z_1^{a_1} \cdots z_p^{a_p}$, $(xa)^p = (z_1 \cdots z_p)^\sigma$ where $\sigma = \sum_1^p a_i$. The group generated by the $p$th powers of the elements of $S_2$ is $A_{p-1}$, the centre. Also $(xa)^p = 1$ if and only if $a \in A_1$.

The proper normal subgroups of $S_2$ are just the $A_i$ and the subgroups of index $p$. Of the latter $A$ and $B = [x, y_1, \cdots, y_{p-1}]$ are characteristic. $A$ is the unique maximal abelian normal subgroup of $S_2$ and $B$ is the only other normal subgroup of $S_2$ of index $p$ whose elements are all of order $p$ or 1.

4. **The partition subgroups** of $S_n$. The natural retraction of $S_{n+1}$ onto $S_n$ gives the split extension $S_{n+1} \cong A^n S_n$ where $A^n$ is elementary abelian of order $p^n$.

**Theorem 2.** The factors of $A^n > (A^n, S_n) > (A^n, S_n, S_n) > \cdots$ are all of order $p$.\(^9\)

We write the above series as $A^n_0 > A^n_1 > \cdots$. As a Sylow $p$-subgroup

\(^7\) Introduction to [1] and [2].

\(^8\) See [5, §172, Ex. 2].

\(^9\) This corresponds to Lemmas 1 and 2 in [2].
of \( S_{p^n} \), \( S_n \) clearly contains a cycle \( x \) of order \( p^n \).\(^{10}\) By suitable numbering we may take \( z_1, \ldots, z_{p^n} \) as generators of \( A^n \) and \( x^{-1}z_ix = z_{i+1} \) (suffixes mod \( p^n \)). Define \( y_0 = z_1, \ (y_i, x) = y_{i+1} \). As before, \( y_{p^n-1} = z_1z_2 \cdots z_{p^n}, \ y_{p^n} = 1 \). A fortiori \( A^n_{p^n-1} > 1 \) and the theorem follows.

This result shows that any normal subgroup \( H \) of \( S_{n+1} \) contained in \( A^n \) is of the form \( A^n_\mu \) \( [y_i \in H \implies y_{i+1} \in H] \).

**Remark.** \( S_{n+1} \cong (S_n)^p \cdot C \) and so \( A^{n-1} \) in \( S_n \) corresponds to \( A^n \) in \( S_{n+1} \). Also \( A^n_{p-1} \) in \( S_n \) corresponds to a normal subgroup of \( S_{n+1} \) of index \( p^p \) in \( A^n \), viz. \( A^n_p \). (Normal, since \( C \) merely permutes the direct factors.) Hence \( C \) transforms \( A^n \) mod \( A^n_p \) in the same way as \( A^1 \) (in \( S_2 \)).

The product of a subgroup and a normal subgroup is again a subgroup, so \( P = A^n_0 A^n_1 \cdots A^n_{n-1} \) is a subgroup of \( S_{n+1} \). We may draw a diagram with \( n+1 \) columns with \( p^i \) squares in the \( j+1 \)th column and then \( P \) is represented by a partition \( |P| \) of this diagram. We call \( P \) a partition subgroup.

**Theorem 3.** The lower central series \( H_0 > H_1 > \cdots \) of \( S_n \) is obtained by removing successive rows from the top of the partition diagram.

This follows immediately from Theorems 1 and 2 by induction.

We put \( T_m = A^n_0 A^n_1 \cdots A^n_{m-1} A^n_m \) and say that an element or subgroup has depth \( m \) if it is contained in \( T_m \) but not in \( T_{m+1} \).

**Lemma 2.** If \( x \) has depth \( m \), the least normal subgroup of \( S_{n+1} \) containing \( (A^n, x) \) is \( A^n_{p^m} \).\(^{11}\)

\( S_{n+1} \cong T_m S_m; \ T_m \cong (S_k)^{p^m} \ (k = n - m + 1) \). Now \( (A^n, x) \) in \( T_m \) corresponds to \( (A^{n-m}, x_1) \times \cdots \times (A^{n-m}, x_{p^m}) \) where for some \( j \), \( x_j \in S_k \) has depth 0. The lemma is true for \( m = 0 \) by Theorem 2 so this direct product contains \( 1 \times \cdots \times 1 \times A^{n-m}_1 \times 1 \cdots \times 1 \). We may permute the factors by transforming by the cycle in \( S_m \), so any normal subgroup of \( S_{n+1} \) containing \( (A^n, x) \) must contain \( A^n_{p^m} \).

**Remark.** (If \( x \) has depth \( m \)) we may apply the same argument with \( A^{n-m}_1 \) of \( S_k \) instead of \( A^{n-m} \) and see that the least normal subgroup of \( S_{n+1} \) containing \( (A^n_{p^m}, x) \) is \( A^{n_{p^m}}_{2^m} \).

**Theorem 4.** A necessary and sufficient condition for a partition subgroup \( P \) of depth \( s \) to be normal is \( i_r \leq p^s \) (all \( r \)).

We write \( P = HL, H \subseteq A^n, L \subseteq S_n \). Then \( (P, S_{n+1}) \subseteq P \) if and only if \( (L, S_n) \subseteq L \) and \( (L, A^n) \subseteq H \). This last condition is equivalent to \( i_r \leq p^s \) by Lemma 2 so the theorem is obvious by induction.

\(^{10}\) [5, §172, Ex. 1].

\(^{11}\) This corresponds to Lemmas 3 and 4 of [2].
If \( N'_i \) is the least normal subgroup of \( S_{n+1} \) containing \( A'_i \) \((i < p^*)\) then \( N'_i \cap S_{k+1} \) is normal in \( S_{k+1} \) and so by Lemma 2 must contain \( A'_k \) \((k \leq n)\). By the above theorem \( A'_k \theta_{k+1} \) is a normal subgroup so \( N'_k = A'_k \theta_{k+1} \). Here we write \( \theta_{k+1} \) for \( H_{p^*} \) (and in fact \( \theta_0 > \theta_1 \cdots \) is the derived series).

Given two distinct squares \((i, j), (u, v)\) in \(|S_n|\); we shall say \((i, j)\) covers \((u, v)\) if \((u, v) \in |N'_i| \). When \(|P|\) is a normal partition we shall say \(|P|\) covers \((u, v)\) if some square of \(|P|\) does. If \((u, v)\) covers some square outside \(|P|\) we shall say \((u, v)\) avoids \(|P|\).

When \(P\) is a normal partition subgroup of \(S_n\) we define \(P' = (P, S_n)\) and \(P^*\) where \(P^*/P = \)centre of \(S_n/P\). Then \(P'\) and \(P^*\) are again (normal) partition subgroups:

Theorem 5. (i) \(|P'\)| consists of the squares covered by \(|P|\).
(ii) \(|P^*|\) consists of the squares which do not avoid \(|P|\).

(i) If \(P = HL, H \subseteq A^r, L \subseteq S_r, P'\) is the least normal subgroup of \(S_{r+1}\) containing \((H, S_r), (L, A^r)\), and \(L'\). The first two are precisely the parts of \(A^r\) covered by \(H\) and \(L\) respectively so (i) follows by induction on \(r\).

(ii) Let \(|\overline{P}|\) be the set of squares which do not avoid \(|P|\). By (i), \((\overline{P}, S_n) \subseteq P\). If \(x \in \overline{P}\) then any normal subgroup of \(S_n\) containing \(x\) must contain some \(A'_i\) where \((i, j)\) avoids \(|P|\). Hence \(\overline{P}\) is the greatest normal subgroup of \(S_n\) for which \((\overline{P}, S_n) \subseteq P\).

As an immediate application we have:

Corollary. The upper and lower central series of \(S_n\) coincide.

5. The characteristic subgroups of \(S_n\). Transforming \(S_n\) by ele-

* See [2].
ments of the normalizer of $S_n$ in $S_p$ produces certain diagonal automorphisms as well as the inner automorphisms. These do not give the whole automorphism group but we shall see that they are sufficient to "cut out" all the characteristic subgroups. The "diagonal" nature of these automorphisms is perhaps most clearly seen in the Kaloujnine tableau notation.\textsuperscript{13} We shall merely quote the elementary fact that there is such an automorphism $uv \rightarrow u^2v$ of $S_r$ ($p \neq 2$) where $u \in A^*$, $v \in S_r$.

**Lemma 3.** Every characteristic subgroup of $S_n$ is a normal partition subgroup.

[We shall prove by induction that any subgroup invariant under inner and diagonal automorphisms is a normal partition subgroup.]

Suppose $K$ is a characteristic subgroup of $S_{r+1}$, $L = K \cap S_r$, $H = K \cap A^r$. $L$ is invariant under inner and diagonal automorphisms of $S_r$ and so is a normal partition subgroup of $S_r$ by the induction hypothesis.

$H$ is normal in $S_{r+1}$ and $H \subseteq A^r$, so $H = A_1^r$ for some $i$. If $uv \in K$, where $u \in A^r$, $v \in S_r$, then $u^2v \in K$ (by the above remark) and so $u, v \in K$. Finally $K = HL$.

**Theorem 6.** $A^n$ is the unique maximal abelian normal subgroup of $S_{n+1}$.

Put $H = A_{p-1}^n$ and $G =$ centralizer of $H$. $A^n$ is abelian and so $A^n \subseteq G$. If $x \in A^n$, $x$ has depth $\leq n - 1$ and so $(H, x) \in A_{2p^{n-1}+1}^n$ (Lemma 2, Remark). But $p^n > 2p^{n-1} + 1$ ($p \neq 2$), and so $x \in G$. Hence $A^n = G$.

If $B$ is any abelian normal subgroup of $S_{n+1}$, then $B \cap A^n = A_1^n$ for some $i$. If $B$ contains $x$ of depth $\leq n - 1$, then $B$ is a normal subgroup of $S_{n+1}$ containing $(A^n, x)$ and so $B \supseteq H$. But $B$ is abelian and so $B \subseteq A^n$, contradiction. Hence in any case $B \subseteq A^n$.

By this result we see that there is a dual of the derived series and hence $A^n, A^nA^{n-1}, \ldots$ are characteristic in $S_{n+1}$. This shows incidentally that the depth of an element is invariant under automorphisms.

We know for $S_2$ that the elements of order $p$ and depth 0 all lie in $A^0\theta_1$. Suppose we have proved this for $S_n$. Let $xy$ be an element of order $p$ and depth 0 in $S_{n+1}$ where $x \in S_n$, $y \in A^n$. Clearly $x^p = 1$ (working mod $A^n$), and so $x \in A^0\theta_1$ in $S_n$. Also $C$ transforms $A^n/A_p^n$ and $A_1^n$ in the same way (Remark, Theorem 2). Thus $(xy)^p \equiv y_{p-1} \pmod{A_p^n}$ and $y \in A_1^n$, i.e. $xy \in A^0\theta_1$ in $S_{n+1}$.

\textsuperscript{13} See [2].
Suppose now that $x$ is an element of order $p$ and depth $m$ in $S_n$, then $x$ corresponds to an element $(x_1, x_2, \cdots, x_{pm})$ of $S_{n-m}$ of order $p$. If each $x_i$ has depth 0 in $S_{n-m}$ it follows that $x_i \in A^m \theta_1$ and $x \in A^m \theta_{m+1}$.

In $S_2$, $x$ has depth 0 if and only if the group of elements of $A^1$ which commute with $x$ has order $p$.

$$(S_2)^p \cong T_{m}/T_{m+3}. \text{ Hence } x_1, \cdot \cdot \cdot, x_{pm} \text{ all have depth 0 if and only if the group of elements of } T_{m+1} \text{ which commute with } x \text{ mod } T_{m+3} \text{ has order } p^m. \text{ This condition is invariant under automorphisms.}$$

If $z_1, \cdot \cdot \cdot, z_{pm}$ are the generators of $A^m$, the least normal subgroup of $S_{m+1}$ containing $z_1$ also contains the other $z$'s and so is $A^m$ itself. $z_1 z_2 \cdot \cdot \cdot z_{pm} \in A^m_{m-1}$. The least normal subgroup of $S_n$ containing $x = z_1 z_2 \cdot \cdot \cdot z_{pm}$ is therefore $A^m \theta_{m+1}$. Since $p \neq 2$, the "parts" of $x$ are all of depth 0. Hence under an automorphism $A^m \theta_{m+1}$ maps into itself, i.e. $A^m \theta_{m+1}$ is characteristic.

All normal partition subgroups are obtained by commuting these $A^m \theta_{m+1}$ with $S_n$ and taking products. Hence in conjunction with Lemma 3 we have finally:

**Theorem 7.** The characteristic subgroups of $S_n$ are precisely the normal partition subgroups.

**Bibliography**