THE SYLOW SUBGROUPS OF THE SYMMETRIC GROUP*

BY

WILLIAM FINDLAY

In the Sylow theorems† we learn that if the order of a group $\mathfrak{A}$ is divisible by p^α (p a prime integer) and not by $p^{\alpha+1}$, then $\mathfrak{A}$ contains one and only one set of conjugate subgroups of order p^α, and any subgroup of $\mathfrak{A}$ whose order is a power of p is a subgroup of some member of this set of conjugate subgroups of $\mathfrak{A}$. These conjugate subgroups may be called the Sylow subgroups of $\mathfrak{A}$. It will be our purpose to investigate the Sylow subgroups of the symmetric group of substitutions.

By means of a preliminary lemma the discussion will be reduced to the case where the degree of the symmetric group is a power (p^α) of the prime (p) under consideration.

A set of generators of the group having been obtained, they are found to set forth, in the notation suggested by their origin, the complete imprimitivity of the group. The various groups of substitutions upon the systems of imprimitivity, induced by the substitutions of the original group, are seen to be themselves Sylow subgroups of symmetric groups of degrees the various powers of p less than p^α. They are also the quotient groups under the initial group of an important series of invariant subgroups.

In terms of the given notation convenient exhibitions are obtained of the commutator series of subgroups and also of all subgroups which may be considered as the Sylow subgroups of symmetric groups of degree a power of p.

Enumerations are made of the substitutions of periods p and p^α and the conjugacy relations of the latter set of substitutions are discussed.

The subgroup consisting of all substitutions invariant under the main group is cyclic and of order p.

The full set of conjugate Sylow subgroups of the symmetric group on p^α letters fall into

$$\frac{p^\alpha!}{(p!)^\alpha} \qquad (\alpha = p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1)$$

classes each consisting of $\{(p-2)!\}^\alpha$ groups having the same complete system of imprimitivity.

* Presented to the Society February 27, 1904. Received for publication June 20, 1903.

† Mathematische Annalen, vol. 5 (1873), page 584.

§ 1. *Lemma.*

We define the function $\pi(n, p)$ of p any prime and n any integer, as the exponent of the highest power of p occurring as a factor of $n!$. If we impose the restriction that no power of p shall occur in the summation more than $p-1$ times, n is uniquely expressible in the form

$$n = \sum_{i=1}^{k} p^{a_i}, \qquad a_i \geqq 0.$$

We have the relation *

$$\pi(n, p) = \frac{n-k}{p-1}.$$

In particular

$$\pi(p^a, p) = \frac{p^a - 1}{p-1},$$

and therefore

$$\pi(n, p) = \sum_{i=1}^{k} \pi(p^{a_i}, p).$$

§ 2. *Reduction of the problem.*

Throughout this paper, German capitals will be used to denote groups and the corresponding Roman capitals to represent substitutions; thus, $\mathfrak{A}_a^\alpha$ represents a group of degree a and order α and its substitutions will in general be denoted by $A_1, A_2, \cdots$. The symmetric group of degree n will be denoted by $\mathfrak{S}^n$ and its Sylow subgroup of order a power of p, by $\mathfrak{P}^n$. The letter E, with suffixes, will be used for the elements of $\mathfrak{P}$ which are considered as its generators. Our main problem is to find one subgroup $\mathfrak{P}^n$ of $\mathfrak{S}_{n!}^n$ having order $p^{\pi(n,p)}$.

If $a < c$, any substitution, or group of substitutions on a letters — we will speak of the objects upon which the substitution is performed as *letters* — may properly be considered as an element or subgroup of $\mathfrak{S}^c$.

Given a number of groups

$$\mathfrak{A}_a^\alpha, \mathfrak{B}_\beta^b, \cdots, \mathfrak{K}_\kappa^k,$$

if we consider the letters of the different groups as wholly distinct and the groups as subgroups of $\mathfrak{S}^m$, $m = a + b + \cdots + k$, then their least common overgroup consists of the totality of products of the form

$$A \cdot B \cdots K$$

and its order is $\alpha \cdot \beta \cdots \kappa$.

By the lemma of § 1, we can find a set of powers of p, say

$$p^{a_1}, p^{a_2}, \cdots, p^{a_r},$$

such that

1) $$n = \sum_{i=1}^{r} p^{a_i},$$

* BACHMANN, *Zahlentheorie*, I, p. 33.

2) $$\pi(n, p) = \sum_{i=1}^{r} \pi(p^{a_i}, p).$$

Distributing the n letters of $\mathfrak{S}^n$ into r sets containing $p^{a_1}, p^{a_2}, \cdots, p^{a_r}$ letters, respectively, we see that $\mathfrak{P}^n$ is the least common overgroup of a set of Sylow subgroups *

$$\mathfrak{P}^{p^a} \qquad (i=1, 2, 3, \cdots, r).$$

Since it is also a subgroup of $\mathfrak{P}^{p^a}$, $p^a > n$, it may be considered sufficient to investigate only the case where n is a power of p.

§ 3. *Generation of a* $\mathfrak{P}^{p^a}_{p^{\pi(p^a, p)}}$. †

We shall obtain $\mathfrak{P}^{p^a}$ by an inductive process, assuming the knowledge of a $\mathfrak{P}^{p^{a-1}}$. Distribute the p^a letters into p corresponding sets each containing p^{a-1} letters. This we may indicate by the notation for the letters

$$\mathrm{L}_{i,j} \qquad (i=1, 2, \cdots, p\,;\ j=1, 2, 3, \cdots, p^{a-1}).$$

Let $\mathfrak{A}'$ be a $\mathfrak{P}^{p^{a-1}}$ on the letters $\mathrm{L}_{1,j}$. Transforming this by the p substitutions

$$\mathrm{S}_i = \begin{pmatrix} \mathrm{L}_{1,1}, & \mathrm{L}_{1,2}, & \cdots, & \mathrm{L}_{1,p^{a-1}} \\ \mathrm{L}_{i,1}, & \mathrm{L}_{i,2}, & \cdots, & \mathrm{L}_{i,p^{a-1}} \end{pmatrix} \qquad (i=1, 2, \cdots, p),$$

we obtain a series of groups $\mathfrak{A}', \mathfrak{A}'', \mathfrak{A}''' \cdots \mathfrak{A}^{(p)}$, whose least common overgroup $\mathfrak{Q}$ (§ 2) is of degree p^a and order

$$p^{p \cdot \pi(p^{a-1}, p)}.$$

Now

$$\pi(p^{a-1}, p) = p^{a-2} + p^{a-3} + \cdots + p + 1.$$

Therefore the degree of $\mathfrak{Q}$ is

$$p^{\pi(p^a, p)-1}.$$

The substitution

$$\mathrm{E} = \begin{pmatrix} \cdots & \mathrm{L}_{i,j} & \cdots \\ & \mathrm{L}_{h,j} & \end{pmatrix},$$

where $h \equiv i+1$, mod. p, $1 \leqq h \leqq p$, $i = 1, 2, 3, \cdots, p$, has the following properties:

1) $$\mathrm{E}^{-1} \mathrm{A}^{(i)} \mathrm{E} = \mathrm{A}^{(h)}.$$

Therefore the product of two substitutions of the form

$$\mathrm{Q}\mathrm{E}^k$$

may again be expressed in the same form.

---

* Cf. G. A. MILLER, *On the Transitive Substitution Groups whose order is a power of a Prime Number*, American Journal of Mathematics, vol. 23 (1901), p. 176.

† Cf. NETTO, *Theory of substitutions* (translated by COLE), § 39, page 41.

2) If Q changes L_{ij} into $L_{i,g}$, then QE^k will change L_{ij} to $L_{h,g}$ where $h \equiv i + k$, mod. p. Therefore

$$QE^k = Q'E^{k'}$$

if, and only if, $Q = Q'$ and $k \equiv k$, mod. p.

Hence it follows that the totality of substitutions of the form QE^k constitute a group of order

$$p^{\pi(p^a, p)},$$

which is therefore a $\mathfrak{P}^{p^a}$.

The process of induction obtained above is to be conceived of as beginning with $a = 1$. The Q in this case is the identity substitution. For the full application of the induction it is required that the original p^a letters be distributed into p sets, which we shall call the subsets of order one, then each of these into p subsets of order two, each of the latter subsets into p subsets of order three, and so on until finally we have the subsets of order a consisting of one letter each. The required correspondence between the letters in the p subsets of order $h + 1$ into which any subset of order h is divided is to be obtained by ordering the p subdivisions at each stage. For convenience the totality of the p^a letters will be spoken of as the subset of order 0.

All these requirements are met by the following a-partite suffix notation:

$$L_{\{b_1, b_2, \cdots, b_a\}},$$

where $1 \leqq b_i \leqq p$ $(i = 1, 2, \cdots, a)$.

The first g elements in the suffix define the subset of order g to which the letter belongs, the $(g + 1)$th suffix which of the p subsets of this division contains it and the remaining $a - g - 1$ elements serve to establish the required correspondence of these p subsets of order $g + 1$. Here g has the range $g = 0, 1, 2, \cdots, a - 1$.

The E required to obtain a particular $\mathfrak{P}^{p^{a-g}}$ $(0 \leqq g \leqq a - 1)$, (say that which acts upon the subset of order g whose letters have $c_1, c_2, \cdots, c_g$ as the first g elements in their suffix), from the $p\mathfrak{P}^{p^{a-g-1}}$ upon the p subsets of order $g + 1$ contained in the above, will be

$$E_{\gamma_g} \equiv E_{\{c_1, c_2, \cdots, c_g\}} \equiv \begin{pmatrix} \cdots, & L_{\{b_1, b_2, \cdots, b_a\}} \\ & L_{\{d_1, d_2, \cdots, d_a\}} \end{pmatrix}, \cdots,$$

where

$$d_{g+1} \equiv b_{g+1} + 1 \,(\text{mod. } p) \text{ if } b_i = c_i \; (i = 1, 2, \cdots, g),$$

$$d_{g+1} = b_{g+1}, \text{ if for some } i, \text{ in } i = 1, 2, \cdots, g, \; b_i \neq c_i,$$

$$d_j = b_j \qquad (j = 1, 2, \cdots, g, g+2, \cdots, a).$$

Hereafter we shall use α_g, β_g, γ_g, etc., as symbols for g-partite numbers with elements a_i, b_i, c_i, etc. The general g-partite number with elements having range $1, 2, 3, \cdots, p$ will be denoted by $\lambda_g \equiv \{l_1, l_2, \cdots, l_g\}$ and the totality

of these, p^g in number, will be denoted by Λ_g. For $g = 0$ we have but one E which we may denote by E_0.

The totality of E_{λ_g}'s ($g = 0, 1, \cdots, a-1$), in number

$$\pi(p^a, p) = \sum_{g=0}^{a-1} p^g,$$

constitute a system of generators of a $\mathfrak{P}^{p^a}$.

§ 4. *A normal form for the general* P.

We shall say that λ_g is contained in λ'_h if 1) $g < h$, 2) $l_i = l'_i$ ($i = 1, 2, \cdots, g$). If λ_g and λ'_h are not the same and neither one contains the other they will be said to be independent.

From the expression for the E's in § 3, it is seen that if λ_g is contained in λ_h, then

$$E_{\lambda_g}^{-1} E_{\lambda_h} E_{\lambda_g} = E_{\lambda'_h},$$

where

$$l'_{g+1} \equiv l_{g+1} + 1 \pmod{p},$$

$$l'_i = l_i \qquad (i = 1, 2, \cdots, g, g+2, \cdots, h),$$

and that if λ_g and λ'_h are independent,

$$E_{\lambda_g}^{-1} E_{\lambda'_h} E_{\lambda_g} = E_{\lambda'_h}.$$

These results may be generalized and stated in the following form:

a) If λ_g is contained in λ_h, then

$$E_{\lambda_h}^{b} \cdot E_{\lambda_g}^{c} = E_{\lambda_g}^{c} \cdot E_{\lambda'_h}^{b},$$

where

$$l'_{g+1} \equiv l_{g+1} + c \pmod{p},$$

$$l'_i = l_i \qquad (i = 1, 2, \cdots, g, g+2, \cdots, h).$$

b) If λ_g and λ'_g are independent, then

$$E_{\lambda_g}^{b} \cdot E_{\lambda'_h}^{c'} = E_{\lambda'_h}^{c'} \cdot E_{\lambda_g}^{b}.$$

By means of these formulas any product of the E's, that is, any substitution of $\mathfrak{P}^{p^a}$, can be expressed in the form

$$P = \prod_{g=0, 1, 2, \cdots, a-1} \prod_{\lambda_g | \Lambda_g} E_{\lambda_g}^{k_{\lambda_g}},$$

where $0 \leqq k_{\lambda_g} \leqq p-1$, and the symbol $\lambda_g | \Lambda_g$ indicate that λ_g takes all values in Λ_g. The arrangement of the terms in the inner product is immaterial since they are commutative with each other.

This we shall call the normal form of P in terms of the generators. The set of k's is uniquely determined.

§ 5. *Normal form* for* P^{p^n}.

It is desired to find the set of k''s such that

$$\mathrm{P}^{p^n} = \Pi\Pi \mathrm{E}_{\lambda_g}^{k'_{\lambda_g}}.$$

We shall conceive this normalized form to be obtained from the product of p^n factors each of which is P written in its normal form by assembling to the left first the E's with $g = 0$, next the E's with $g = 1$, then the E's with $g = 2$ and so on, making use of the formulas of § 4. Let

$$k_{\{i_{1,b},\, i_{2,b},\, \cdots,\, i_{g,b}\}} \qquad (1 \leqq b \leqq p^n)$$

be the exponent of E_{λ_g} in the bth factor of the product, numbering from the right, after all the E_{λ_h}, with $h < g$, have been assembled to the left. The exponents of the $(b+1)$th term differ from the corresponding ones in the bth term only in the effects produced by the parts of the bth term as they passed over. Therefore

$$l_{h+1,\, b+1} \equiv l_{h+1,\, b} - k_{\{i_{1,b},\, i_{2,b},\, \cdots,\, i_{h,b}\}} \pmod{p}.$$

Each $\mathrm{E}_{\lambda_g}^k$ is unaffected as it passes to the left, over the residues of terms, since the latter contain only $\mathrm{E}_{\lambda'_h}$ with $h \geqq g$. We have then

$$k'_{\lambda_g} \equiv \sum_{b=1}^{p^n} k_{\{i_{1,b},\, i_{2,b},\, \cdots,\, i_{g,b}\}} \pmod{p}.$$

§ 6. *The imprimitivity of* $\mathfrak{P}^{p^a}$.

The complex classification of the letters L_{λ_a} furnished by the a-partite suffix λ_a may be regarded as comprising $a-1$ simple classifications, viz., the distributions of the p^a letters into p^h subsets of order h, p^{a-h} in each subset $(h = 1, 2, \cdots, a-1)$.

THEOREM: Each of these simple classifications constitutes a division of the letters into sets of imprimitivity of the group.

This is equivalent to saying that, by a given substitution P, all letters having their first h suffixes the same in each will go into letters which agree in their first h suffixes.

The effect of P upon L_{λ_a} may be considered as produced by applying sucessively, beginning at the left, i. e., according to ascending values of g, the factors of the outer product in the normal form of P (§ 4). If P changes L_{λ_a} to $\mathrm{L}_{\lambda'_a}$ it will be seen that

1) The l_i's are changed one by one and in order according to ascending values of i.

2) $$l'_{g+1} \equiv l_{g+1} + k'_{\lambda_g} \pmod{p} \qquad (g = 0, 1, 2, \cdots, a-1),$$

when λ'_g is contained in λ'_a.

* This normal form seems worthy of note although no use is made of it in the sequel.

Hence if L_{β_a} and L_{γ_a} have $b_i = c_i$ $(i = 1, 2, \cdots, h)$, then their transforms by P, $L_{\beta'_a}$ and $L_{\gamma'_a}$, have $b'_i = c'_i$ $(i = 1, 2, \cdots, h)$, which proves the theorem, and in addition that

$$b'_{h+1} - b_{h+1} \equiv c'_{h+1} - c_{h+1} \pmod{p}.$$

THEOREM: The analysis of the imprimitivity of $\mathfrak{P}$, given above, is complete, in the sense that it contains every subdivision of the letters into sets of imprimitivity of $\mathfrak{P}$.

For suppose we have a division of the p^a letters L_λ into p^a/n classes of n each, indicated by the following schematic arrangement of their suffixes λ_a:

$$\begin{array}{cccccccc}
\alpha', & \alpha'', & \alpha''', & \cdots, & \alpha^{(i)}, & \cdots, & \alpha^{(n)}, \\
\beta', & \beta'', & \beta''', & . & . & . & ., & \beta^{(n)}, \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
\omega', & \omega'', & \omega''', & . & . & . & ., & \omega^{(n)}.
\end{array}$$

Suppose, in addition that the $n\alpha$'s agree in their first h elements $(0 \leqq h < a)$, but not in their $(h+1)$th elements, i. e., $a^{(j)}_i = a'_i$ $(i = 1, 2, \cdots, h$ and $j = 1, 2, \cdots, n)$, but in particular $a''_{h+1} \equiv a'_{h+1} + d$, mod. p, where $d \not\equiv 0$ mod. p.

A substitution P can be found which will transform $L_{\alpha'}$ into $L_{\beta'}$, and at the same time $L_{\alpha''}$ into any L_λ having $l_i = b'_i$ $(i = 1, 2, \cdots, h)$ and

$$l_{h+1} - b'_{h+1} \equiv a''_{h+1} - a'_{h+1} \pmod{p},$$

since

$$a''_{h+1} \neq a'_{h+1}.$$

Hence among the β's every λ must occur having $l_i = b'_i (i = 1, 2, \cdots, h)$, if the division of the letters be into sets of imprimitivity, and accordingly among the α's every λ must occur for which $l_i = a_i (i = 1, 2, \cdots, h)$. This establishes the theorem.

§ 7. *The induced groups on the sets of imprimitivity.*

The substitutions of $\mathfrak{P}^{p^a}$ give us a group of degree p^h of induced substitutions on the p^h sets of imprimitivity of $\mathfrak{P}^{p^a}$ of order h. The *letter* (L'_{μ_h}) of this group is, or corresponds to, the totality of L_{λ_a} in which $l_i = m_i (i = 1, 2, \cdots, h)$. The h-partite subscripts of the L''s classify them in a scheme corresponding to that of the L's. The substitution upon the L''s induced by E_{λ_g} on the L's is seen 1) if $g \geqq h$ to be the identity, 2) if $g < h$ to be exactly the corresponding generator E'_{λ_g}, of the Sylow subgroup of the symmetric group upon the p^h L''s, defined after the method of § 3, by the classification and ordering set up by the suffixes μ_h. Hence we have the

THEOREM. The totality of E_{λ_g}'s of $\mathfrak{P}^{p^a}$ $(g = 0, 1, 2, \cdots, h-1)$, generate a subgroup of $\mathfrak{P}^{p^a}$ which is isomorphic to the induced group on the sets of imprimitivity of $\mathfrak{P}^{p^a}$ of order h, and also to a Sylow subgroup of the symmetric group of degree p^h.

From this view-point $\mathfrak{P}^{p^a}$ itself is seen to be but a member of an unending series of intimately related Sylow subgroups of symmetric groups whose degrees are the ascending powers of p.

It is to be observed that E_{λ_g}, applied as a transformer to the totality of E_{λ_h}'s, makes upon them the same substitution as E'_{λ_g} upon the letters, L'_{λ_h}, of its group, $\mathfrak{P}^{p^h}$.

§ 8. *On the cyclic character of the substitutions of* $\mathfrak{P}$.

We proceed to establish relations between the cyclic character of a substitution P of $\mathfrak{P}^{p^a}$ and the various substitutions upon the sets of imprimitivity of $\mathfrak{P}^{p^a}$ induced by P, which we have seen may be thought of as substitutions of Sylow subgroups of symmetric groups whose degrees are the various powers of p less than p^a, or as substitutions upon the E_{λ_h}'s produced by transformation by the substitutions

$$\bar{P}_h = \prod_{g=0,1,\cdots,h-1} \prod_{\lambda_g | \Lambda_g} E_{\lambda_g}^{k_{\lambda_g}}.$$

In addition to the above it will be convenient to adopt the following notations for other portions of the normal expression of P:

$$P_h = \prod_{\lambda_h | \Lambda_h} E_{\lambda_h}^{k_{\lambda_h}},$$

$$\underline{P}_h = \prod_{k=h+1,\cdots,a-1} \prod E_{\lambda_k}^{k_{\lambda_k}}.$$

Thus

$$P = \bar{P}_h \cdot P_h \cdot \underline{P}_h.$$

The substitution upon the E_{λ_h}'s produced by $\bar{P}_h$ will be denoted by $\bar{P}'_h$.

If λ_h is contained in λ_{h+1}, then

$$\bar{P}_h^{-x} E_{\lambda_h} \bar{P}_h^{x} = E'_{\lambda_h},$$

$$\bar{P}_{h+1}^{-x} E_{\lambda_{h+1}} \bar{P}_{h+1}^{x} = E'_{\lambda_{h+1}},$$

where λ'_h is contained in λ'_{h+1} (§ 6). If E_{λ_h}, in the cyclic notation of P'_h, belongs to a cycle with p^b letters, then will

$$\bar{P}_{h+1}^{-p^b} E_{\lambda_{h+1}} \bar{P}_{h+1}^{p^b} = E''_{\lambda_{h+1}},$$

where

1) $$l''_i = l_i \qquad (i = 1, 2, \cdots, h),$$

2) $$l''_{h+1} \equiv l_{h+1} + \sum k_{\mu_h} \pmod{p},$$

the summation being for μ_h running through the suffixes of the E_{μ_h}'s belonging to the cycle of $\bar{P}'_h$ containing E_{λ_h}. If this sum is a multiple of p the cycle of $\bar{P}'_{h+1}$ containing $E_{\lambda_h \lambda_{h+1}}$ contains p^b E's. If it is not a multiple of p, the cycle will contain the p^{b+1} $E_{\mu_{h+1}}$'s whose suffixes contain the suffixes of the E_{μ_h}'s in the same cycle as E_{λ_h}. From this follows the

THEOREM. If $\bar{P}'_h$, written in cyclic notation, has a_i cycles each containing p^{b_i} E_{λ_h}'s $(i = 1, 2, \cdots, r)$* and if s_i of the a_i cycles are composed of E_λ's for which the sum of the p^{b_i} k_λ's is congruent to zero, modulo p, then $\bar{P}'_{h+1}$ has, corresponding to these, $p s_i$ cycles with p^{b_i} E's in each and $a_i - s_i$ cycles with p^{b_i+1} E's in each.

COROLLARY 1. If n_g denotes the total number of cycles in $\bar{P}'_g$, then in the above

$$n_h = \sum a_i,$$

$$n_{h+1} = n_h + (p-1)\sum_{i=1}^{r} s_i.$$

COROLLARY 2. Since $n_1 = 1$, or p, according as k_0 is not, or is, equal to zero therefore $n_h \equiv 1 \pmod{p-1}$ for all values of h.

If $\bar{P}'_g$ has order p^g and so consists of but one cycle, then every cycle in $\bar{P}'_h$ $(h = g, g+1, \cdots, a)$ will contain at least p^g letters. If P is also of order p^g, then every cycle in each of the $\bar{P}'_h$'s contains precisely p^g letters. Hence upon the choice of the exponents in P_h of such a $P(g \leqq h \leqq a-1)$, there are imposed p^{h-g} conditions giving in all $p^{p^h - p^{h-g}}$ choices of P_g for a given $\bar{P}_h$. From this we derive

COROLLARY 4. The total number of P's of order p^g and having a given $\bar{P}_g$ also of order p^g is p^m, where

$$m = (p^g - 1)\frac{p^{a-g} - 1}{p-1}.$$

COROLLARY 5. If we denote the order of $\bar{P}'_g$ by p^{π_g}, then $\pi_g \leqq g$; and if $g < h$ we have

$$0 \leqq \pi_h - \pi_g \leqq h - g.$$

Hence if P is of order p^a, the order of $\bar{P}'_g$ is p^g, and we have

COROLLARY 6. The necessary and sufficient condition that P has order p^a is that $\sum k_{\lambda_g} \not\equiv 0$, mod. p, $(g = 0, 1, \cdots, a-1)$, the summation being for λ_g running through Λ_g.

§ 9. *Certain normalizations.*

If $R = P^{-1}$, it can be proved that

$$R_h = (P_h^{-1})_{\bar{\pi}_h}.$$

* Thus $p^h = \sum_{i=1}^{r} a_i p^{b_i}$.

The symbol

$$A_B$$

is used for $B^{-1}AB$ and it is convenient in such expressions as the above to conceive the operation as performed by a substitution upon the E's, in this case the substitution which we have denoted by $\bar{R}'_h$. It is still better to conceive the effect to be produced by a substitution upon the exponents of the E's in P_h^{-1}.

In general if $R = P \cdot Q \cdot S \cdots T \cdot U$, then

$$R_h = (P_h)_{Q_h . S_h \ldots U_h} \cdot (Q_h)_{S_h \ldots U_h} \cdots (T_h)_{U_h} \cdot U_h .$$

If $R = Q^{-1}PQ$, then

$$R_h = (P_h)_{Q_h} \cdot (Q_h^{-1})_{\bar{R}_h} \cdot Q_h .$$

§ 10. *Invariant substitutions.*

Consider $R = E_{\lambda_g}^{-1} P E_{\lambda_g}$. We have

$$\bar{R}_g = \bar{P}_g ,$$

$$R_g = P_g \cdot (E_{\lambda_g}^{-1})_{P_g} \cdot E_{\lambda_g} .$$

Therefore in order that $R = P$ for every E_{λ_g}, it is necessary and sufficient that every E_{λ_g} should be invariant under $\bar{P}_g$. In particular, every $E_{\lambda_{a-1}}$ must be invariant under $\bar{P}_{a-1}$ and therefore $\bar{P}_{a-1} = I$ and $P = P_{a-1}$. From the transitivity of $\mathfrak{P}$ it follows that it is necessary (and sufficient) in order that

$$\prod_{\lambda_{a-1} | \Delta_{a-1}} E_{\lambda_{a-1}}^{k_{\lambda_{a-1}}}$$

is invariant under $\mathfrak{P}$, that the exponents k_λ are all equal. Thus we have the

THEOREM. The only invariant substitutions of $\mathfrak{P}^{p^a}$ are the p powers of

$$\prod_{\lambda_{a-1} | \Delta_{a-1}} E_{\lambda_{a-1}} .$$

§ 11. *Substitutions of orders p and p^a.*

It follows from § 8, corollary 6, that the number of elements of $\mathfrak{P}^{p^a}$ of order p^a is

$$\prod_{g=0, 1, \ldots, a-1} (p-1) p^{pg-1} = (p-1)^a p^{a-a} \qquad \left(a = \frac{p^a - 1}{p-1}\right).$$

The factor $p-1$ occurs because $p-1$ congruentially distinct values of

$$\sum_{\lambda_g | \Delta_g} k_{\lambda_g}$$

are admissible.

Let P be any substitution of order p^a and Q another, as yet undetermined, substitution of $\mathfrak{P}$. Let $R = Q^{-1} \cdot P \cdot Q$. Then (§ 9)

$$R_h = (P_h)_{\overline{Q}_h} \cdot (Q_h^{-1})_{\overline{R}_h} \cdot Q_h.$$

Let s_h be the least positive residue of the sum of the exponents of the E_{λ_h}'s in P_h, modulo p. We will assume $\overline{Q}_h$ to have been already selected, and therefore

$$(P_h)_{\overline{Q}_h} \qquad \text{and} \qquad \overline{R}_h$$

are determined.

Let

$$(P^h)_{\overline{Q}_h} = \prod_{\lambda_h | \Delta_h} E_{\lambda_h}^{v_{\lambda_h}}$$

and

$$\overline{R}_h' = (E_{\beta_h'}, E_{\beta_h''}, E_{\beta_h'''}, \cdots, E_{\beta_h^{(p^h)}}).$$

Since $\overline{R}_h'$ is conjugate to $\overline{P}_h'$, it will consist of but one cycle.

If now we denote Q_h, which we wish to determine, by

$$\prod_{\lambda_h | \Delta_h} E_{\lambda_h}^{y_{\lambda_h}},$$

and

$$(Q_h^{-1})_{\overline{R}_h} Q_h \qquad \text{by} \qquad \prod_{\lambda_h | \Delta_h} E_{\lambda_h}^{x_{\lambda_h}},$$

then the x's and the y's are related by the congruences

$$x_{\beta_h^{(i)}} \equiv y_{\beta_h^{(i)}} - y_{\beta_h^{(j)}} \pmod{p},$$

in which

$$j \equiv i - 1 \pmod{p^h}$$

and

$$i = 1, 2, 3, \cdots, p^h.$$

There is one, and only one, condition imposed upon the x's, viz., that their sum is congruent to zero, modulo p. This condition is fulfilled by the following choice of the x's:

$$x_{\beta_h^{(i)}} \equiv -v_{\beta_h^{(i)}} \pmod{p} \qquad (i = 2, 3, \cdots, p^h),$$

$$x_{\beta_h'} \equiv s_h - v_{\beta_h'} \pmod{p},$$

since

$$\sum v_{\beta_h} \equiv s_h \pmod{p}.$$

We can now solve the above congruences for the y's and so determine a Q_h such that

$$R_h = E_{\beta_h'}^{s_h}.$$

Proceeding thus for $h = 1, 2, \cdots, a-1$ we have finally

$$R = \prod_{h=0, 1, \cdots, a-1} E_{\beta_h}^{s_h},$$

where β_h is an arbitrarily selected number of Λ_h. No two of these R's for different sets of s_h's are conjugates and hence we have the

THEOREM. There are $(p-1)^a p^{a-a}$ substitutions in $\mathfrak{P}^{p^a}$ of order p^a, where $\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1$. They fall into $(p-1)^a$ sets of conjugates each set containing p^{a-a} substitutions and determined by the set of least positive residues, modulo p, of the various sums

$$\sum_{\lambda_h | \Delta_h} k_{\lambda_h} \qquad (h = 0, 1, 2, \cdots, a-1).$$

COROLLARY 1. A substitution of order p^a is invariant only under its own powers.

From this theorem and corollary 4 of § 8 we have

COROLLARY 2. There are

$$(p-1)^c p^{p^{a-1} \cdot \frac{p^c-1}{p-1} - c}$$

substitutions, P, in $\mathfrak{P}^{p^a}$ of order p^c and such that $\overline{\mathrm{P}}_c$ is also of order p^c.

In particular for $c = 1$ we have

COROLLARY 3. There are $(p-1)p^{p^{a-1}-1}$ substitutions of order p, for which $k_0 \not\equiv 0 \pmod{p}$.

Every substitution P of $\mathfrak{P}$ having $k_0 = 0$ is the product of p substitutions $\mathrm{P}', \mathrm{P}'', \mathrm{P}''', \cdots, \mathrm{P}^{(p)}$ chosen one from each of the p Sylow subgroups of the symmetric groups on the subsets of the letters of $\mathfrak{P}^{p^a}$, of order 1 (§ 3). If $\mathrm{P}^{p^a} = \mathrm{I}$ then $\mathrm{P}^{(i)p^a} = \mathrm{I}$ $(i = 1, 2, \cdots, p)$, and conversely. Therefore the total number of substitutions in $\mathfrak{P}^{p^a}$ whose orders are less than or equal to p^c and having $k_0 = 0$ is equal to the pth power of the number of substitutions in $\mathfrak{P}^{p^{a-1}}$ of orders less than or equal to p^c.

Hence, for $c = 1$, we have from corollary 3,

THEOREM. The total number of substitutions in $\mathfrak{P}^{p^a}$ of order p is the value of n_a determined by the following recursion formula:

$$n_h = (p-1)p^{p^{h-1}-1} + (n_{h-1}+1)^p - 1,$$

$$n_1 = p - 1.$$

§ 12. *The set of Sylow subgroups of* $\mathfrak{S}^{p^a}$.

Any substitution G of $\mathfrak{S}$ which transforms $\mathfrak{P}$ into itself must conform to the complete system of imprimitivity of $\mathfrak{P}$. For let

$$\begin{array}{cccccc} \alpha', & \alpha'', & \alpha''', & \cdots, & \alpha^{(p^h)} \\ \beta', & \beta'', & \beta''', & \cdots, & \beta^{(p^h)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

indicate a division of the letters L_{λ_α} into imprimitive sets (cf. § 6). The row $\alpha', \alpha'', \cdots$ consists of the totality of λ_α's agreeing with α' in their first p^{n-h} elements and similarly for each of the other rows. Suppose that G transforms this tactical arrangement of the letters into another having two letters from different rows above in the same row, e. g.,

$$\begin{array}{cccc} \alpha', & \beta', & \alpha''', & \cdots \\ \alpha'', & \gamma', & \cdots & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

Now $G^{-1}PG$ will transform this second arrangement in the same way that P transforms the first. Since α' and β' agree in their first g elements, where $g < a - h$, it is possible to find a P' which will transform $L_{\alpha'}$ into $L_{\alpha''}$ and $L_{\beta'}$ into any one of n letters where $n \geqq p^h$ and therefore $L_{\beta'}$ into a letter whose suffix does not occur in the same row of the second arrangement as α''. Taking $P = GP'G^{-1}$ we see that the hypothesis leads to a contradiction.

Hence the substitution G upon the letters L_{λ_α} may be thought of as produced by changing, first the initial elements of their suffixes, then the second elements, then the third and so on, the change produced in any one class of elements being a function of the preceding ones only. Let

$$\text{(I)} \qquad \begin{pmatrix} 1, & 2, & 3, & \cdots, & p \\ b_1, & b_2, & b_3, & \cdots, & b_p \end{pmatrix}$$

be the substitution upon the first elements of the suffixes induced by G. Then since $G^{-1}E_0G$ produces upon the L's, as rearranged by G, the same substitution as E_0 produced upon the preceding arrangement,

$$\text{(II)} \qquad b_2 - b_1 \equiv b_3 - b_2 \equiv \cdots \equiv b_1 - b_p \equiv k_0 \pmod{p},$$

where k_0 is the exponent of E_0 in the normal form of $G^{-1}E_0G$ (§ 4). The group $\mathfrak{P}$ is invariant under G_0, the substitution upon the L's induced by (I) where the b's are any solution of the congruences (II) k_0 being any one of the integers $1, 2, \cdots, p-1$. There are $p(p-1)$ solutions.

The substitution $G' = G_0^{-1}G$ will also leave $\mathfrak{P}$ invariant and is the product of p substitutions of degree p^{a-1} each of which may be discussed in relation to a $\mathfrak{P}^{p^{a-1}}$ as G has been in relation to $\mathfrak{P}^{p^a}$. In this way G is found to be the product of $1 + p + p + \cdots + p^{a-1}$ substitutions under each of which $\mathfrak{P}$ is invariant and for each of which there are $p(p-1)$ choices. Hence the total number of substitutions of $\mathfrak{S}^{p^a}$ under which $\mathfrak{P}^{p^a}$ is invariant is

$$\{p(p-1)\}^\alpha \qquad \left(\alpha = \frac{p^a - 1}{p-1}\right).$$

If in all the congruences (II) we take $k_0 = 1$ the G thus obtained is a substitution of $\mathfrak{P}$ and we so obtain all the substitutions of $\mathfrak{P}$. If $k_0 \neq 1$ the corresponding E, (E_0), is not invariant under G. If in § 9 we take $P = E_{\lambda_g}$ and Q any substitution of $\mathfrak{P}$, it is seen that the necessary and sufficient condition that the system of generators of $\mathfrak{P}$ should be invariant under Q is that Q_h should be invariant under every

$$E_{\lambda_g} \quad (g = 0, 1, \cdots, h-1;\ h = 1, 2, \cdots, a-1).$$

This requires that the exponents of the E's in Q_h shall be all equal. The subgroup of $\mathfrak{G}$, or of $\mathfrak{S}$, consisting of substitutions leaving the set of generators of $\mathfrak{P}$ invariant is of order p^a and consists of the subgroup of $\mathfrak{P}$ generated by the substitutions

$$\prod_{\lambda_g | \Lambda_g} E_{\lambda_g} \qquad (g = 0, 1, \cdots, a-1).$$

The subgroup of $\mathfrak{S}$ and overgroup of $\mathfrak{G}$ consisting of all the substitutions leaving invariant the complex classification of the letters given by the imprimitivity of $\mathfrak{P}$ is readily seen to be of order $(p!)^a$.

THEOREM. There are $p^a!/p^a(p-1)^a$ Sylow subgroups of the symmetric group, they fall into $p^a!/(p!)^a$ classes each containing $\{(p-2)!\}^a$ groups having the same system of imprimitivity. Each group has $p^{a-1}\cdot(p-1)^a$ systems of generators of the type used in this paper, where

$$\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1.$$

§ 13. *Sylow subgroups of lower degree contained in* $\mathfrak{P}$.

In obtaining $\mathfrak{P}^{p^a}$ we required and obtained (§ 3), as subgroups of it p^{a-h} Sylow subgroups of the symmetric groups of degree p^h on the various subsets of the letters of order $h\,(h = 1, 2, \cdots, a-1)$. They consist of the totality of substitutions of $\mathfrak{P}^a$ affecting only the letters of the corresponding subset of order h and are readily seen to be all conjugate and to form a complete system.

These are the only subgroups of $\mathfrak{P}^{p^a}$ which are Sylow subgroups of symmetric groups of degree p^h. For if such a subgroup, $\mathfrak{G}$, affected two letters L and L′ from different subsets of order h, because of its transitivity $\mathfrak{G}$ must contain a substitution G which transform L into L′. Then, on account of the imprimitivity of $\mathfrak{P}$, G must affect at least $2p^h$ letters. Therefore the degree of $\mathfrak{G}$ must be greater than or equal to $2p^h$ contrary to the assumption.

§ 14. *The maximal invariant abelian subgroup of* $\mathfrak{P}$ *and a series of invariant subgroups.*

In order that a group $\mathfrak{B}$ should be an invariant abelian subgroup of $\mathfrak{P}$ it is necessary that the division of the letters into subsets of order $a-1$ (§ 3) should

constitute a system of intransitivity of $\mathfrak{B}$. For if some B transforms L_{α_a} into L_{β_a} of a different subset of order $a-1$, i. e., α_a and β_a do not agree in their first $a-1$ elements, then

$$A = E_{\alpha_{a-1}}^{-1} B^{-1} E_{\alpha_{a-1}} \cdot B \cdot E_{\alpha_{a-1}}^{-1} B E_{\alpha_{a-1}} = B \cdot E_{\beta_{a-1}}^{-1} \cdot E_{\gamma_{a-1}} \cdot E_{\beta_{a-1}}^{-1} \cdot E_{\alpha_{a-1}} \neq B$$

and therefore $\mathfrak{B}$ is not an invariant abelian subgroup of $\mathfrak{P}$.

The group generated by the substitutions $E_{\lambda_{a-1}}$ $(\lambda_{a-1}|\Lambda_{a-1})$, and consisting of the totality of substitutions of $\mathfrak{P}$ having the particular system of imprimitivity of $\mathfrak{P}$, which has p letters in each division, as their system of intransitivity, is readily seen to be both invariant and abelian and therefore, by the above, the maximal invariant abelian subgroup of $\mathfrak{P}$. We will denote it by $\mathfrak{D}_{(a-1)}$. Its order is $p^{p^{a-1}}$. The substitutions of $\mathfrak{P}$ generated by the remaining E's constitute a system of left extenders of $\mathfrak{D}_{(a-1)}$ to $\mathfrak{P}$ (cf. § 4) and therefore the quotient group $\mathfrak{P}/\mathfrak{D}_{a-1}$ is simply isomorphic to a Sylow subgroup on p^{a-1} letters (L') obtained from $\mathfrak{P}$ by establishing a correspondence between the L''s and the subsets of order $a-1$ of the letters of $\mathfrak{P}$ (cf. § 7).

THEOREM. The series of subgroups $\mathfrak{D}_0 = \mathfrak{P}, \mathfrak{D}_{(1)}, \mathfrak{D}_{(2)}, \cdots, \mathfrak{D}_{(a-1)}, \mathfrak{D}_{(a)} = I$, in which $\mathfrak{D}_{(h)}$ consists of the totality of substitutions having the system of imprimitivity of $\mathfrak{P}$ containing p^{a-h} letters in each division as a system of intransitivity, or which, in their normal form (§ 4), have $k_{\lambda_g} = 0$ $(g = 0, 1, \cdots, h-1)$, are each contained in, and invariant under, every preceding one. The quotient group $\mathfrak{P}/\mathfrak{D}_{(h)}$ is simply isomorphic to a Sylow subgroup on p^h letters, the one derived in § 7, and $\mathfrak{D}_{(h-1)}/\mathfrak{D}_{(h)}$ is the maximal invariant abelian subgroup of $\mathfrak{P}/\mathfrak{D}_{(h)}$. In particular $\mathfrak{D}_{(a-1)}$ is the maximal invariant abelian subgroup of $\mathfrak{P}$.

§ 15. *The commutator series of subgroups.*

It has been proved* that, if $P_1, P_2, \cdots, P_k$ be a set of generators of group $\mathfrak{P}$ and $G_{ij} = P_i^{-1} P_j^{-1} P_i P_j$, as i and j have, independently, the range $1, 2, 3, \cdots, k$, generate a subgroup $\mathfrak{G}$, then the smallest invariant subgroup of $\mathfrak{P}$ containing $\mathfrak{G}$ is the first commutator subgroup of $\mathfrak{P}$. Applying this to the Sylow subgroup with the generators E_{λ_h} for the G's we have, besides the identity, products of the form

$$E_{\lambda_h'}^{-} E_{\lambda_h},$$

where $l_i' = l_i$ for all values of i from 1 to h excepting one, say d, and $l_d' \equiv l_d \pm 1$, mod. p. Also any product of this form can be obtained in this way.

By combinations of these products we can generate any substitution of $\mathfrak{P}$ whose normal form (§ 4) satisfies the a conditions

$$\sum_{\lambda_g|\Lambda_g} k_{\lambda_g} \equiv 0 \pmod{p} \qquad (g = 0, 1, 2, \cdots, a-1).$$

It is easily seen (cf. § 9) that any product of substitutions satisfying these con-

*MILLER, Bulletin, American Mathematical Society, vol. 4 (1898), p. 136.

ditions, and also the transform of such a substitution by any substitution of $\mathfrak{P}$, satisfy the same congruence. Hence the

THEOREM. The totality of substitutions whose normal forms satisfy the above congruences constitutes the first commutator subgroup of $\mathfrak{P}$, which we shall denote by $\mathfrak{C}_1$. The order of $\mathfrak{C}_1$ is $p^{\alpha-a}$ $(\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1)$.

The first commutator subgroup of $\mathfrak{P}$ is intransitive with the sets of imprimitivity of $\mathfrak{P}$ containing p^{a-1} letters in each as its sets of intransitivity. It is independently simply transitive within any $p-1$ of its sets of intransitivity.

Since in the normal form of $\mathfrak{C}_1$ we have $k_0 = 0$, it follows (cf. § 9) that when we normalize any product of commutators of $\mathfrak{C}_1$ the exponents in the result fulfil the $1 + p(a-1)$ conditions

$$k_0 = 0, \qquad \sum k_{\lambda_g} \equiv 0 \pmod{p} \quad (g = 1, 2, 3, \cdots, a-1),$$

the summation being for all the numbers of Λ_g with a chosen value for l_1. The group $\mathfrak{C}_2$, consisting of the totality of such substitutions of $\mathfrak{P}$, is the product of the first commutator subgroups of the various Sylow subgroups of degree p^{a-1} contained in $\mathfrak{P}$.

Among the substitutions of $\mathfrak{C}_1$ occur all the substitutions of the form

$$F = E_{\lambda_h}^{-1} \cdot E_{\lambda_h'},$$

where λ_h and λ_h' are any two numbers of Λ_h such that $l_1 \neq l_1'$ and $1 < h \leqq a-1$. From the above it follows that $\mathfrak{C}_1$ contains a substitution C such that:

$$C^{-1} E_{\lambda_h} C = E_{\lambda_h},$$

$$C^{-1} E_{\lambda_h'} C = E_{\lambda_h''},$$

where λ_h'' is any number of Λ_h subject to the one condition that $l_1'' = l_1'$.

Then

$$C^{-1} F^{-1} C F = E_{\lambda_h} E_{\lambda_h''}^{-1} E_{\lambda_h}^{-1} E_{\lambda_h'} = E'_{\lambda_h''} E'_{\lambda_h'}.$$

These last products, which are commutators of $\mathfrak{C}_1$, generate $\mathfrak{C}_2$, which is therefore the first commutator subgroup of $\mathfrak{C}_1$ or the second commutator subgroup of $\mathfrak{P}$.

By successive application of these results we obtain the

THEOREM. The dth commutator subgroup $(\mathfrak{C}_d)$ of $\mathfrak{P}$ is the product of the first commutator subgroups of the Sylow subgroups of degree p^{a-d+1} contained in $\mathfrak{P}$. It is also the product of the $(d-1)$th commutator subgroups of the p Sylow subgroups of degree p^{a-1} contained in $\mathfrak{P}$. The order of $\mathfrak{C}_d$ is p^δ, where

$$\delta = p^{a-1} + p^{a-2} + \cdots p^d - (a-d)p^{d-1}.$$

The cogredient subgroup of $\mathfrak{P}$ (§ 10) is a subgroup of each of the commutator subgroups $\mathfrak{C}_1, \mathfrak{C}_2, \cdots, \mathfrak{C}_{a-1}$.

COLUMBIA UNIVERSITY, NEW YORK.