

THE DEGREE AND CLASS OF MULTIPLY TRANSITIVE GROUPS*

BY

W. A. MANNING

If a group contains substitutions of degree μ but none that displace fewer letters, the identity excepted, μ is said to be its class.† The same term is unfortunately used with a different meaning in the theory of prime power groups.

In substitution group theory the two problems of the order and of the class of groups of given degree are in large measure interchangeable.‡ For this reason Bochert's inequalities, limiting the degree n of a multiply transitive group in terms of its class μ are second in importance only to Sylow's theorem.§ Bochert's theorem may be stated as follows.||

The class (> 3) of a substitution group of degree n exceeds $\frac{1}{3}n - \frac{2}{3}\sqrt{n}$ if it is doubly, $\frac{1}{3}n - 1$ if triply, $\frac{1}{2}n - 2$ if quadruply, transitive.

In the proof of this theorem Bochert introduces the condition that the class is a given number by means of the commutator of two non-commutative substitutions. Now the commutator is only one combination out of many that may be made from the substitutions of a group (G) and is by no means always one of the substitutions of lowest degree in G . In the hope of penetrating more deeply into this matter the author has assumed the presence of substitutions of order 2 among the substitutions of lowest degree in G and thereby gains the advantages that are afforded by the simplicity of structure of dihedral rotation groups. The principal result arrived at may be put thus:

1. THEOREM. *Let n be the degree and μ (> 2) the class of a group that contains a substitution of order 2 and degree μ ; then if it is*

doubly transitive,	$\mu > \frac{1}{2}n - \frac{1}{2}\sqrt{n} - 1,$
triply “ ,	$\mu \geq \frac{1}{2}n,$
4-ply “ ,	$\mu \geq \frac{1}{2}(n + 1),$
5-ply “ ,	$\mu \geq \frac{3}{5}n,$
6-ply “ ,	$\mu > \frac{3}{4}n,$
7-ply “ ,	$\mu \geq \frac{10}{13}n,$

* Presented to the Society, Nov. 25, 1916.

† Jordan, *Paris Comptes Rendus*, vol. 72 (1871), p. 384.

‡ See these *Transactions*, vol. 16 (1915), p. 139.

§ Jordan, *Journal de mathématiques*, ser. 5, vol. 1 (1895), p. 35.

|| Bochert, *Mathematische Annalen*, vol. 40 (1892), p. 176; vol. 49 (1897), p. 133.

more than $p_1 + p_2 + \cdots + p_r$ times transitive, where p_1, p_2, \cdots, p_r are distinct odd primes ($r > 1$),

$$\mu > \frac{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1) - 1}{(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)} n.$$

THE DIEDRAL GROUPS

2. The auxiliary theorem by means of which this will be proved is the following:

If the order of a group of class μ generated by two substitutions s and t of order 2 and degree μ is divisible by each of the odd primes p_1, p_2, \cdots, p_r , its degree n does not exceed $\mu + \mu/(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$; if the order N of st is odd or is divisible by 4, n does not exceed $\mu + 2\mu/N$; if $N (> 2)$ is twice an odd number, n is not greater than $\mu + 2\mu/N + 8\mu/N^2$.

If we erase from $\{s, t\}$, of degree n , the ξ letters of all the regular constituents of $\{s, t\}$ which involve letters displaced by both s and t the group in the remaining constituents is of degree $n - \xi$, of class $\mu - \xi$, and is generated by two similar substitutions of order 2 and degree $\mu - \xi$. Then if the theorem can be shown to be true for diedral groups satisfying the given conditions, but in which the regular constituents, if any, are of order 2 and exhibited by transpositions of s (or t) in letters fixed by t (or s), it is *a fortiori* true when regular constituents on letters common to s and t are present. It may be noted that if p^a is a Sylow divisor of N , i. e., the highest power of the prime p that divides the order of st , and if p^a divides the degree of a regular constituent of $\{s, t\}$ it must also divide the degree of some non-regular constituent of $\{s, t\}$. If this is not so, $(st)^{N/p}$ involves no letter not in a regular constituent of $\{s, t\}$ and is not the identity. Thus the degree of $(st)^{N/p}$ is at least μ and cannot exceed ξ ; but if $\xi = \mu$ the truth of the theorem is not in dispute. Consequently the deletion of the regular constituents from the group $\{s, t\}$ leaves a group of the same order. In what follows the group $\{s, t\}$ under discussion will be assumed free from any regular constituent on letters common to s and t .

The transitive constituents of $\{s, t\}$ may be enumerated as follows. In s there are m_1 cycles that displace letters not in t , and t has m_2 cycles that displace letters not in s ; let $m = m_1 + m_2$. There are y_j constituents of degree Y_j and order $2Y_j$, Y_j an odd number, $j = 1, 2, \cdots$. There are z'_k transitive constituents of degree Z_k and order $2Z_k$, Z_k even, $k = 1, 2, \cdots$, with the generator of degree Z_k in s and the generator of degree $Z_k - 2$ in t . In like manner there are z''_k constituents of the same order Z_k with $Z_k - 2$ letters in s and Z_k letters in t ; let $z_k = z'_k + z''_k$. The numbers Y_1, Y_2, \cdots are all the odd divisors of N , unity excepted, and the numbers Z_1, Z_2, \cdots

are all the even divisors of N , with the exception of 2. We recall that a non-regular transitive dihedral rotation group of degree n is of class $n - 1$ if n is odd, and is of class $n - 2$ if n is even. In the latter case the two generators of order 2 are not similar substitutions. Of course some of the numbers $y_1, y_2, \dots, z'_1, z'_2, \dots, z''_1, z''_2, \dots$ may be zero. The degree of s is

$$2m_1 + \sum y_j (Y_j - 1) + \sum z'_k Z_k + \sum z''_k (Z_k - 2),$$

and the degree of t is

$$2m_2 + \sum y_j (Y_j - 1) + \sum z'_k (Z_k - 2) + \sum z''_k Z_k.$$

The summations extend the subscripts through their entire range of values. With this understanding we may omit the subscripts j and k in future and introduce these abbreviations:

$$E_1 \equiv \sum y (Y - 1), \quad F_1 \equiv \sum z (Z - 1),$$

and similarly

$$\Gamma_a \equiv E_a + F_a \equiv \sum y (Y - a) + \sum z (Z - a).$$

Then the degree of $\{s, t\}$ is $2m + \Gamma_0$ which on the elimination of $2m$ becomes $2\mu - \Gamma_2$; for

$$\begin{aligned} -2\Gamma_1 + \Gamma_0 &= \sum yY - \sum (2yY - 2y) + \sum zZ - \sum (2zZ - 2z) \\ &= -\sum y(Y - 2) - \sum z(Z - 2) = -\Gamma_2. \end{aligned}$$

3. If st is of odd prime order it is obvious that $n = \mu + \mu/(p - 1)$.

Let st be of order p^α , p any prime and $\alpha > 1$. Let $\{s, t\}$ have x_i transitive constituents of degree p^i , $i = 1, 2, \dots, \alpha$. From $(st)^{p^{\alpha-1}}$ we get the equation,

$$p^\alpha x_\alpha = \mu + h_\alpha,$$

from $(st)^{p^{\alpha-2}}$,

$$p^{\alpha-1} x_{\alpha-1} + p^\alpha x_\alpha = \mu + h_{\alpha-1},$$

from $(st)^{p^{\alpha-3}}$,

$$p^{\alpha-2} x_{\alpha-2} + p^{\alpha-1} x_{\alpha-1} + p^\alpha x_\alpha = \mu + h_{\alpha-2},$$

.

from $(st)^p$,

$$p^2 x_2 + p^3 x_3 + \dots + p^\alpha x_\alpha = \mu + h_2,$$

while

$$px_1 + p^2 x_2 + \dots + p^\alpha x_\alpha = \mu + \delta,$$

and

$$(p - 1)x_1 + (p^2 - 1)x_2 + \dots + (p^\alpha - 1)x_\alpha = \mu.$$

Here $h_2, h_3, \dots, h_\alpha, \delta$, are positive integers or zero, and $\mu + \delta$ is the degree

of $\{s, t\}$. These $\alpha + 1$ equations are consistent, their eliminant must vanish, and when equated to zero and reduced it gives

$$\delta = \mu/p^{\alpha-1}(p-1) - \sum_{i=2}^{\alpha} h_i/p^{i-1}.$$

Then if st is of order p^α ($\alpha > 1$), the degree of $\{s, t\}$ does not exceed

$$\mu + \mu/p^{\alpha-1}(p-1).$$

4. Let $N = 2p^\alpha$, where p^α is a power of an odd prime. Let y and z be the number of transitive constituents of degrees p^α and $2p^\alpha$ respectively in $\{s, t\}$. Then from $(st)^{N/p}$ and $(st)^{N/2}$ we have

$$p^\alpha y + 2p^\alpha z = \mu + h,$$

$$2m + 2p^\alpha z = \mu + k - \bar{F}_0,$$

and

$$2m + p^\alpha y + 2p^\alpha z = \mu + \delta - \bar{\Gamma}_0,$$

with

$$m + (p^\alpha - 1)y + (2p^\alpha - 1)z = \mu - \bar{\Gamma}_1.$$

By \bar{F}_0 , $\bar{\Gamma}_0$, and $\bar{\Gamma}_1$ is meant the summation explained above but with the exclusion of constituents whose degree is divisible by p^α . The meaning of h , k , and δ is the same as before. They are positive integers or zero. The eliminant of m , y , and z is

$$\begin{vmatrix} 0 & p^\alpha & 2p^\alpha & \mu + h \\ 2 & 0 & 2p^\alpha & \mu + k - \bar{F}_0 \\ 2 & p^\alpha & 2p^\alpha & \mu + \delta - \bar{\Gamma}_0 \\ 1 & p^\alpha - 1 & 2p^\alpha - 1 & \mu - \bar{\Gamma}_1 \end{vmatrix} = 0.$$

This reduces to

$$(p^\alpha - 1)\delta = \mu - h(p^\alpha - 1) - k - (\bar{E}_0 + p^\alpha \bar{\Gamma}_2),$$

whence we conclude that *when the order of st is twice a power of an odd prime, its degree does not exceed $\mu + \mu/(p^\alpha - 1)$.*

5. Let $N = p_1 p_2 \cdots p_r$, the product of r distinct odd prime factors.

There is at once the equation

$$E_1 = \mu,$$

and there are $\sum_{i=1}^{i=r} C_i = 2^r - 1$ equations given by the $2^r - 1$ powers $(st)^{N/(p_i p_j \cdots)}$, which is in no case the identity but is of degree $\mu + h_{ij} \dots$, where the quantities $h_{ij} \dots$ are positive whole numbers or zero. Let $\delta \equiv h_{12 \dots r}$, a constantly recurring quantity since $\mu + \delta$ is the degree of st or of $\{s, t\}$. Now $(st)^{N/p_i p_j}$, say, involves letters from and only from those transitive con-

stituents of $\{s, t\}$ whose degree contains p_i or p_j as a factor, and so on for other combinations of the primes p_1, p_2, \dots . The equation given by $(st)^{N/p_1 p_2}$ when $r = 3$, for example, is

$$p_1 y_1 + p_2 y_2 + p_1 p_2 y_{12} + p_1 p_3 y_{13} + p_2 p_3 y_{23} + p_1 p_2 p_3 y_{123} = \mu + h_{12}.$$

There are $2^r - 1$ variables $y_1, \dots, y_{12}, \dots$ in the 2^r equations. Replace these equations by an equivalent system got by replacing the first, $E_1 = \mu$, by $E_0 - E_1 = \delta$ and the last $2^r - 2$ by themselves less the second, $E_0 = \mu + \delta$. The eliminant of these equations is

$$\begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & \delta \\ p_1 & p_2 & p_3 & \cdots & p_2 p_3 \cdots p_r & p_1 p_2 \cdots p_r & \mu + \delta \\ 0 & p_2 & p_3 & \cdots & p_2 p_3 \cdots p_r & p_1 p_2 \cdots p_r & -h_1 + \delta \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} = 0.$$

Multiply the first row of this determinant by $p_1 p_2 \cdots p_r$ and then divide the first column by p_1 , the second by p_2 , \dots , the $(r + 1)$ th by $p_1 p_2, \dots$. Then we have

$$\begin{vmatrix} p_2 p_3 \cdots p_r & p_1 p_3 \cdots p_r & \cdots & p_2 & p_1 & 1 & p_1 p_2 \cdots p_r \delta \\ 1 & 1 & \cdots & 1 & 1 & 1 & \mu + \delta \\ 0 & 1 & \cdots & 0 & 1 & 0 & -h_1 + \delta \\ 1 & 0 & \cdots & 1 & 0 & 0 & -h_2 + \delta \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix} = 0.$$

For the sake of convenience of reference we may call the row in which h_i, h_{ij}, \dots occur the h_i -row, the h_{ij} -row, and so forth. Then the law of the formation of the last $2^r - 2$ rows is evident: a term in the h_i -row (except $\delta - h_i$) is unity if the term above it in the first row contains p_i as a factor; a term in the h_{ij} -row is unity if the term in the first row above it contains $p_i p_j$ as a factor, and so on; otherwise it is zero. For wherever a zero is found in the h_{ijk} -row of the determinant there was a term $p_i p_j p_k y_{ijk}$ in the original equation, from which was subtracted $E_0 = \mu + \delta$, and this product $p_i p_j p_k$ we divided out from every term of the column corresponding to y_{ijk} , thus leaving $p_1 p_2 \cdots p_r / (p_i p_j p_k)$ in the first row directly above the zero in question. The present units correspond to zeros in the original equations. For the sake of clearness it may be well to write out the determinant for the case $r = 3$:

$$\begin{vmatrix}
 p_3 p_2 & p_3 p_1 & p_2 p_1 & p_3 & p_2 & p_1 & 1 & p_1 p_2 p_3 \delta \\
 1 & 1 & 1 & 1 & 1 & 1 & 1 & \mu + \delta \\
 0 & 1 & 1 & 0 & 0 & 1 & 0 & \delta - h_1 \\
 1 & 0 & 1 & 0 & 1 & 0 & 0 & \delta - h_2 \\
 1 & 1 & 0 & 1 & 0 & 0 & 0 & \delta - h_3 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & \delta - h_{12} \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & \delta - h_{13} \\
 1 & 0 & 0 & 0 & 0 & 0 & 0 & \delta - h_{23}
 \end{vmatrix} = 0.$$

Now multiply the second row by -1 , the h_i -row by $-(p_i - 1)$, the h_{ij} -row by $-(p_i - 1)(p_j - 1)$, \dots , and add them all to the first row. The sum in a typical column, the $y_{12\dots k}$ -column, is

$$\begin{aligned}
 p_1 p_2 \cdots p_k - & \left[1 + \sum_{i=1}^k (p_i - 1) + \sum_{i=1; j=i+1}^{i=k; j=k} (p_i - 1)(p_j - 1) + \cdots \right. \\
 & \left. + (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) \right] \\
 & = p_1 p_2 \cdots p_k - (p_1 - 1 + 1)(p_2 - 1 + 1) \cdots (p_k - 1 + 1) = 0.
 \end{aligned}$$

This gives zero in every term of the first row except one. From the addition of the elements of the last column we have

$$\begin{aligned}
 \delta [p_1 p_2 \cdots p_r - 1 - \sum (p_1 - 1) - \sum (p_1 - 1)(p_2 - 1) - \cdots \\
 - \sum (p_1 - 1)(p_2 - 1) \cdots (p_{r-1} - 1)] \\
 - \mu + \sum h_1 (p_1 - 1) + \sum h_{12} (p_1 - 1)(p_2 - 1) + \cdots = 0.
 \end{aligned}$$

Hence when the order of st is the product of r distinct odd primes p_1, p_2, \dots, p_r , the degree of $\{s, t\}$ does not exceed

$$\mu + \mu/(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

6. Let $N = 2pq$, where p and q are two distinct odd primes. The following five equations can be written down:

$$\begin{array}{ll}
 \text{from } s \text{ and } t \text{ jointly,} & m + \Gamma_1 = \mu, \\
 \text{from } st, & 2m + \Gamma_0 = \mu + \delta, \\
 \text{from } (st)^{p^q}, & 2m + F_0 = \mu + h, \\
 \text{from } (st)^{2q}, & \Gamma_0 - qy_2 - 2qz_2 = \mu + i, \\
 \text{from } (st)^{2p}, & \Gamma_0 - py_1 - 2pz_1 = \mu + j,
 \end{array}$$

where δ , h , i , and j are positive whole numbers or zero. The elimination of m , y_1 , z_1 , and z_3 gives

$$\begin{vmatrix} 1 & p-1 & 2p-1 & 2pq-1 & \mu - (q-1)y_2 - (pq-1)y_3 - (2q-1)z_2 \\ 2 & p & 2p & 2pq & \mu + \delta - qy_2 - pqy_3 - 2qz_2 \\ 2 & 0 & 2p & 2pq & \mu + h - 2qz_2 \\ 0 & p & 2p & 2pq & \mu + i - pqy_3 \\ 0 & 0 & 0 & 2pq & \mu + j - qy_2 - pqy_3 - 2qz_2 \end{vmatrix} = 0,$$

which reduces to

$$-\mu + q(p-1)\delta + qh + (p-1)qi + (q-1)j + q(pq-2p+1)y_2 + pq(q-1)y_3 + 2q(q-1)(p-1)z_2 = 0;$$

whence $\delta \leq \mu/q(p-1)$. If the order of st is twice the product of two distinct odd primes the degree of $\{s, t\}$ does not exceed

$$\mu + \mu/[q(p-1)].$$

This case is needed in the proof of our theorem only when one of the two odd primes is 3.

7. Now let N have at least two prime power factors the smaller of which is greater than 3. $N = p^a q^b \phi$, where p and q are distinct primes and ϕ is unity or a number relatively prime to p and q . We start from

$$\mu + \delta = 2\mu - \Gamma_2.$$

The powers $(st)^{N/p}$ and $(st)^{N/q}$ give

$$\Gamma_0(*, 0) + \Gamma_0(*, *) = \mu + h,$$

$$\Gamma_0(0, *) + \Gamma_0(*, *) = \mu + i,$$

where h and i are positive whole numbers or zero, and $\Gamma_a(*, 0)$ is to be understood as equal to $\sum y(Y-a) + \sum z(Z-a)$, the summation extending however only to those constituents of $\{s, t\}$ whose degrees are divisible by p^a and not by q^b . In $\Gamma_a(0, *)$ the summation extends to the constituents whose degrees are divisible by q^b and not by p^a , while in $\Gamma_a(*, *)$ the summation extends to constituents whose degrees are divisible by both p^a and q^b . Thus

$$\Gamma_a = \Gamma_a(*, *) + \Gamma_a(*, 0) + \Gamma_a(0, *) + \Gamma_a(0, 0).$$

Then

$$0 = -\mu - \frac{h+i}{2} + \frac{\Gamma_0(*, 0) + \Gamma_0(0, *)}{2} + \Gamma_0(*, *).$$

Multiply by $(p^a q^b - 2)/(p^a q^b)$ and add to

$$\mu + \delta = 2\mu - \Gamma_2(*, 0) - \Gamma_2(0, *) - \Gamma_2(*, *) - \Gamma_2(0, 0),$$

with the result (writing π for $p^a q^b$)

$$\mu + \delta = \mu + 2\mu/\pi - \frac{\pi - 2}{\pi} \frac{h + i}{2} - \frac{\pi + 2}{2\pi} \Gamma'_{4\pi/(\pi+2)} - \frac{2}{\pi} \Gamma''_{\pi} - \Gamma_2^{(0)}.$$

Here the new symbol $\Gamma_a^{(k)}$ is introduced ($k = 0, 1, 2, \dots$). It is to mean the sum $\Gamma_a(*, 0) + \Gamma_a(0, *)$ when $k = 1$, $\Gamma_a(*, *)$ when $k = 2$, $\Gamma_a(0, 0)$ when $k = 0$. It will presently be used when more than two prime powers are in question. Then $\Gamma_a^{(3)}$, for example, shall be the sum of all the quantities which, like $\Gamma_a(*, *, *, 0, \dots)$ contain three stars in the parenthesis. Returning to the proof of the last result,

$$\begin{aligned} \frac{\pi - 2}{2\pi} \Gamma_0(*, 0) - \Gamma_2(*, 0) &= \sum \left(\frac{\pi - 2}{2\pi} Y - Y + 2 \right) y \\ &+ \sum \left(\frac{\pi - 2}{2\pi} Z - Z + 2 \right) z = - \sum \left(\frac{\pi + 2}{2\pi} Y - 2 \right) y \\ &- \sum \left(\frac{\pi + 2}{2\pi} Z - 2 \right) z = - \frac{\pi + 2}{2\pi} \sum \left(Y - \frac{4\pi}{\pi + 2} \right) y \\ &- \frac{\pi + 2}{2\pi} \sum \left(Z - \frac{4\pi}{\pi + 2} \right) z = - \frac{\pi + 2}{2\pi} \Gamma_{4\pi/(\pi+2)}(*, 0); \end{aligned}$$

and similarly

$$\frac{\pi - 2}{\pi} \Gamma_0(*, *) - \Gamma_2(*, *) = - \frac{2}{\pi} \Gamma_{\pi}(*, *) = - \frac{2}{\pi} \Gamma''_{\pi}.$$

The summations \sum are to be taken in accordance with the symbol $\Gamma_0(*, 0)$ or $\Gamma_0(*, *)$. Hence in this case $n \leq \mu + 2\mu/\pi$.

8. If $q^b = 3$ and $p^a > 3$, we may proceed as follows:

$$\begin{aligned} n &= 2\mu - \Gamma_2 + \frac{4}{3p^a} (-\mu - h + \Gamma_0(*, 0) + \Gamma_0(*, *)) \\ &\quad + \frac{p^a - 2}{p^a} (-\mu - i + \Gamma_0(0, *) + \Gamma_0(*, 0)), \\ n &= 2\mu - \Gamma_2 + \frac{\pi - 6}{\pi} (-\mu - h + \Gamma_0(*, 0) + \Gamma_0(*, *)) \\ &\quad + \frac{4}{\pi} (-\mu - i + \Gamma_0(0, *) + \Gamma_0(*, 0)) \\ &= \mu + \frac{2\mu}{\pi} - \frac{\pi - 6}{\pi} h - \frac{4}{\pi} i - \frac{\pi}{6} \Gamma_{\pi/3}(*, 0) - \frac{\pi - 4}{\pi} \Gamma_{2\pi/(\pi-4)}(0, *) \\ &\quad - \frac{2}{\pi} \Gamma_{\pi}(*, *) - \Gamma_2(0, 0). \end{aligned}$$

Hence n is not greater than $\mu + 2\mu/\pi$.

9. Next, let N have at least r ($r > 2$) Sylow divisors each of which is greater than 2: $N = \pi\phi$, where $\pi = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, the product of powers of r distinct primes, and where ϕ is relatively prime to π . From the r substitutions $(st)^{N/p_k}$, $k = 1, 2, \dots, r$, we have r equations which when added together give

$$-r\mu - \sum_{k=1}^r h_k + \sum_{k=1}^r k\Gamma_0^{(k)} = 0.$$

Multiply this equation by $(\pi - 2)/r\pi$ and add to

$$n = 2\mu - \sum_{k=0}^r \Gamma_2^{(k)},$$

whence

$$n = \mu + \frac{2\mu}{\pi} - \sum_{k=0}^r \frac{2k + \pi(r-k)}{r\pi} \Gamma_{2r\pi/[2k+(r-k)\pi]}^{(k)} - \frac{\pi-2}{r\pi} \sum_{k=1}^r h_k.$$

If $k = 0$,

$$\frac{2r\pi}{2k + (r-k)\pi} = 2,$$

and if $k = r$,

$$\frac{2r\pi}{2k + (r-k)\pi} = \pi;$$

since $r > 2$, and $\pi - 2 < r\pi/3$, we have for $k = 1$,

$$\frac{2r\pi}{2 + (r-1)\pi} < 3.$$

When $1 < k < r$,

$$\frac{2r\pi}{2k + (r-k)\pi} < \frac{2r}{r-k} < 2(k+1) < 3 \cdot 4 \cdot 5 \cdots \text{to } k \text{ factors.}$$

It follows at once that the greatest possible value of n in this case is $\mu + 2\mu/\pi$. The results of the last three paragraphs may be stated thus:

If the order of st has r ($r > 1$) Sylow divisors, no one of which is the first power of 2, and whose product we call π , then the degree of $\{s, t\}$ does not exceed $\mu + 2\mu/\pi$.

10. There remains to be investigated the limit of n when N is twice an odd number (π) in which there are at least two prime power factors.

If $\pi = p^a \cdot 3$, we have already before us

$$n = \mu + \frac{2\mu}{\pi} - \frac{4i}{\pi} - \frac{\pi-6}{\pi} h - \frac{\pi-4}{\pi} \Gamma_{2\pi/(\pi-4)}(0, *) - \frac{6}{\pi} \Gamma_{\pi/3}(*, 0) - 2z - \Gamma_2(0, 0),$$

where z is the number of transitive constituents of degree 2π in $\{s, t\}$. Now $(st)^\pi$ gives

$$2m + F_0 = \mu + j,$$

where j is a positive integer or zero; expanding this,

$$2\pi z + F_0(*, 0) + F_0(0, *) + F_0(0, 0) = \mu + j - 2m.$$

Substitute this value of $2z$ in the expression for n above, and obtain

$$\begin{aligned} n = \mu + \frac{\mu}{\pi} + \frac{2m}{\pi} - \frac{6}{\pi} E_{\pi/3}(*, 0) - \frac{\pi-4}{\pi} E_{2\pi/(\pi-4)}(0, *) - E_2(0, 0) \\ - \frac{5}{\pi} F_{2\pi/5}(*, 0) - \frac{\pi-5}{\pi} F_{2\pi/(\pi-5)}(0, *) - \frac{\pi-1}{\pi} F_{2\pi/(\pi-1)}(0, 0) \\ - \frac{\pi-6}{\pi} h - \frac{4i}{\pi} - \frac{j}{\pi}. \end{aligned}$$

Now

$$2m + \Gamma_0 \leq \mu + \frac{2\mu}{\pi},$$

as has been proved, while $\Gamma_0 \geq \mu$. Hence

$$2m \leq \frac{2\mu}{\pi}, \quad \frac{2m}{\pi} \leq \frac{2\mu}{\pi^2},$$

and therefore

$$n \leq \mu + \frac{\mu}{\pi} + \frac{2\mu}{\pi^2}.$$

11. When $N = 2\pi$ is twice an odd number which is the product of two or more prime powers each of which is greater than 3 we may use the formula

$$n = \mu + \frac{2\mu}{\pi} - \frac{\pi-2}{r\pi} \sum_{k=1}^r h_k - \sum_{k=0}^{r-1} \frac{2k + \pi(r-k)}{r\pi} \Gamma_{2r\pi/[2k+(r-k)\pi]}^{(k)} - 2z,$$

where z is the number of transitive constituents in $\{s, t\}$ of degree 2π . From $(st)^\pi$ we have

$$-2\pi z = -\mu - j + 2m + \sum_{k=0}^{r-1} F_0^{(k)}$$

(j a positive integer or zero), which when substituted for $2z$ in the preceding expression gives

$$\begin{aligned} n = \mu + \frac{\mu}{\pi} + \frac{2m}{\pi} - \sum_{k=0}^{r-1} \frac{2k + \pi(r-k)}{r\pi} E_{2r\pi/[2k+(r-k)\pi]}^{(k)} \\ - \sum_{k=0}^{r-1} \frac{2k - r + \pi(r-k)}{r\pi} F_{2r\pi/[2k-r+\pi(r-k)]}^{(k)} - \frac{j}{\pi} - \frac{\pi-2}{r\pi} \sum_{k=1}^r h_k. \end{aligned}$$

It is necessary to show that

$$\frac{2r\pi}{2k - r + \pi(r - k)} < 2 \cdot 3 \cdot 5 \cdots \text{to } k + 1 \text{ factors.}$$

If $k = 0$, the difference $Z - 2\pi/(\pi - 1)$ is positive since 6 is the least possible value of Z . If $k = 1$, we must have $2r\pi/(2 - r + r\pi - \pi) < 6$, that is $2r\pi - 3r - 3\pi + 6 > 0$, or $2(r - 2)(\pi - \frac{3}{2}) + \pi > 0$, which is certainly true. Finally for $1 < k < r$,

$$\begin{aligned} \frac{r\pi}{2k - r + \pi(r - k)} &< \frac{\pi}{\pi - 1} \frac{r}{r - k} \\ &< \left(1 + \frac{1}{\pi - 1}\right)(k + 1) \\ &< 2(k + 1) < 3^k < 3 \cdot 5 \cdots \text{to } k \text{ factors.} \end{aligned}$$

Just as in the preceding paragraph we now draw the conclusion that

$$n \leq \mu + \frac{\mu}{\pi} + \frac{2\mu}{\pi^2}.$$

When the order of st is twice an odd number π divisible by two or more distinct primes the degree of $\{s, t\}$ is not greater than $\mu + \mu/\pi + 2\mu/\pi^2$.

12. This result is significant in the proof of the present theorem when π is the product of two or more distinct odd primes. In this event it gives a limit for n that is lower than the limit found when the order of st is $\prod_{k=1}^r p_k$, for

$$\frac{1}{\prod_{k=1}^r p_k} + \frac{2}{\prod_{k=1}^r p_k^2} < \frac{1}{\prod_{k=1}^r (p_k - 1)}.$$

In fact,

$$\frac{1}{\prod_{k=1}^r p_k} + \frac{2}{\prod_{k=1}^r p_k^2} < \frac{1}{(p_1 - 1) \prod_{k=2}^r p_k}.$$

It has now been proved that if the order of st is divisible by the odd primes p_1, p_2, \dots, p_r its degree is at most $\mu + \mu/(p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$, and that if its order is 2^α , $\alpha > 1$, its degree does not exceed $\mu + \mu/2^{\alpha-1}$. Then the theorem follows as stated even when $\{s, t\}$ has regular constituents in letters common to both s and t .

The general proposition that *the degree of a group of class μ generated by two non-commutative substitutions of order 2 and degree μ is at most $\frac{3}{2}\mu$* , is covered by this theorem.*

*Bulletin of the American Mathematical Society, vol. 20 (1914), p. 469.

MULTIPLY TRANSITIVE GROUPS

13. Let G be a p times transitive group, p an odd prime. By hypothesis there is in G a substitution s of order 2 and degree μ :

$$s = (a_0 a_2)(a_3 a_4) \cdots (a_{p-2} a_{p-1}) \cdots,$$

and by reason of the fact that G is more than $p - 1$ times transitive, there is in G a second substitution s' similar to s :

$$s' = (a_0 a_3)(a_2 a_5)(a_4 a_7) \cdots (a_{p-3} -) \cdots (a_{p-1}).$$

If the blank space that follows a_{p-3} in s' is filled by a letter new to s , the product ss' has at least one cycle of p letters. Transform s' by all the g_{p-1} substitutions of the transitive subgroup of G that leaves fixed the letters $a_0, a_2, \cdots, a_{p-1}$. Each of these g_{p-1} transforms s', s'', \cdots has in common with s the $p - 2$ letters $a_0, a_2, \cdots, a_{p-2}$, and x other letters. It is easy to calculate $\sum x$ for these g_{p-1} substitutions s', s'', \cdots . Any letter, not a_0, a_2, \cdots , or a_{p-1} , is found as often in the set as any other. There are in the cycle $(a_{p-3} -)$ and in the last $\frac{1}{2}\mu - \frac{1}{2}(p - 1)$ cycles of the substitutions of the set $s', s'', \cdots (\mu - p + 2)g_{p-1}$ such letters. Hence there are

$$\frac{(\mu - p + 2)g_{p-1}}{n - p + 1}$$

substitutions among s', s'', \cdots that contain a given letter (not $a_0, a_2, \cdots, a_{p-1}$). Therefore

$$(1) \quad \sum x = (\mu - p + 1) \frac{(\mu - p + 2)g_{p-1}}{n - p + 1} = (\mu - p + 1)(\mu - p + 2)g_p.$$

But in the set s', s'', \cdots there are exactly $(n - \mu)g_p$ substitutions which replace a_{p-3} by a letter new to s , and $(\mu - p + 1)g_p$ that replace a_{p-3} by a letter of s . Then

$$(2) \quad \sum_{(n-\mu)g_p} (p - 2 + x) \geq \frac{(p - 2)\mu}{p - 1} (n - \mu)g_p,$$

$$(3) \quad \sum_{(\mu-p+1)g_p} (p - 2 + x) \geq \frac{1}{2}\mu(\mu - p + 1)g_p.$$

A word of explanation should perhaps be added. Since all the substitutions s', s'', \cdots fix a_{p-1} , all are non-commutative with s . Moreover, when s' (say) replaces a_{p-3} by a letter new to s , ss' contains a cycle of degree p . It has been proved above that in the latter event s' has at most $\mu/(p - 1)$ letters new to s , whence it follows that the number of letters common to s' and s cannot be less than $\mu - \mu/(p - 1) = (p - 2)\mu/(p - 1)$. Then on the addition of (2) and (3),

$$\sum x \geq \left(\frac{(p - 2)\mu}{p - 1} - p + 2 \right) (n - \mu)g_p + \left(\frac{\mu}{2} - p + 2 \right) (\mu - p + 1)g_p;$$

put for $\sum x$ its value from (1),

$$(\mu - p + 1)(\mu - p + 2)g_p \cong \frac{p-2}{p-1}(\mu - p + 1)(n - \mu)g_p \\ + \left(\frac{\mu}{2} - p + 2\right)(\mu - p + 1)g_p,$$

or, on division by $(\mu - p + 1)g_p$, which is not zero because $\mu > p$,*

$$\mu - p + 2 \cong \frac{p-2}{p-1}(n - \mu) + \frac{\mu}{2} - p + 2,$$

$$\frac{\mu}{2} + \frac{p-2}{p-1}\mu \cong \frac{p-2}{p-1}n,$$

whence finally,

$$\mu \cong \frac{2p-4}{3p-5}n.$$

If $p = 3$, that is, if G is triply transitive,

$$\mu \cong \frac{n}{2}.$$

It will be recalled that the holomorph of the elementary abelian group of order 2^α ($\alpha > 1$) is a triply transitive group of class $2^{\alpha-1}$, in which all the substitutions of degree $2^{\alpha-1}$ are of order 2.

14. If $p = 5$, this limit is

$$\mu \cong \frac{3}{5}n.$$

Whenever μ is not divisible by 12, this may be replaced by

$$\mu \cong \frac{3n+4}{5}.$$

For those substitutions s', s'', \dots which replace a_{p-3} by a letter of s cannot have so many as $\mu/2$ letters in common with s unless such a product as ss' is of order 6. The three equations

$$m + 2y + 5z = \mu,$$

$$2m + 6z = \mu,$$

$$3y + 6z = \mu,$$

give on solution $z = \mu/12$. Hence if μ is not divisible by 12, no product ss', ss'', \dots is of order 6, and in consequence

$$\sum_{(\mu-4)g_5} (3+x) \cong \left(\frac{\mu}{2} + 1\right)(\mu - 4)g_5,$$

* Jordan, *Traité des substitutions*, 1870, p. 64.

whence

$$\mu \geq \frac{3n+4}{5}.$$

15. If $p = 7$, no product ss', ss'', \dots is of order less than 8 when $s' (s'', \dots)$ replaces a_4 by a letter of s . Then for the $(\mu - 6)g_7$ substitutions of the set s', s'', \dots which replace a_4 by a letter of s , we have

$$\sum_{(\mu-6)g_7} (5+x) \geq \frac{3}{4}\mu(\mu-6)g_7,$$

which added to

$$\sum_{(n-\mu)g_7} (5+x) \geq \frac{5}{8}\mu(n-\mu)g_7,$$

gives on reduction

$$\mu \geq \frac{1}{13}n.$$

16. Let it be assumed that G is more than p times transitive, p an odd prime. Then besides

$$s = (a_0 a_2)(a_3 a_4) \cdots (a_{p-2} a_{p-1}) \cdots (a_p)$$

we have

$$s' = (a_0 a_3)(a_2 a_5) \cdots (a_{p-3} a_p) \cdots (a_{p-1}).$$

The transitive subgroup G_p of degree $n - p$ transforms s' into a set of g_p substitutions s', s'', \dots such that all the products ss', ss'', \dots are of order p or a multiple of p . Hence

$$\sum_{g_p} (p-2+x) \geq \frac{p-2}{p-1} \mu g_p.$$

Any one of the last $\mu - p + 1$ letters of s is found in

$$\frac{(\mu - p + 1)g_p}{n-p} = (\mu - p + 1)g_{p+1}$$

of the substitutions s', s'', \dots . Then

$$(\mu - p + 1)^2 g_{p+1} \geq \frac{p-2}{p-1} \mu g_p - (p-2)g_p,$$

or

$$(\mu - p + 1)^2 g_{p+1} \geq \frac{p-2}{p-1} (n-p)(\mu - p + 1)g_{p+1},$$

whence

$$\mu \geq \frac{p-2}{p-1}n + \frac{1}{p-1}.$$

When applied to quadruply transitive groups this limit is

$$\mu \geq \frac{1}{2}n + \frac{1}{2},$$

and for sextuply transitive groups,

$$\mu \geq \frac{3}{4}n + \frac{1}{4}.$$

17. The general case may now be very briefly stated. Let the group G be more than σ times transitive, where σ is the sum of r (> 1) distinct odd primes, p_1, p_2, \dots, p_r . When the substitution s is given, s' , because G_σ is transitive, may be so written that the first r cycles of ss' are of the orders p_1, p_2, \dots, p_r . The substitutions s and s' have $\sum_{k=1}^r (p_k - 2)$ common letters in these first $\frac{1}{2} \sum_{k=1}^r (p_k - 1)$ cycles, and x other letters in common. Summing for all the g_σ substitutions s', s'', \dots

$$\sum x = \left(\mu - \sum_1^r (p_k - 1) \right)^2 g_{\sigma+1},$$

and

$$\sum_{g_\sigma} \left(\sum_1^r (p_k - 2) + x \right) \geq \frac{\prod_{k=1}^r (p_k - 1) - 1}{\prod_{k=1}^r (p_k - 1)} \mu g_\sigma,$$

whence, putting Π for $\prod_{k=1}^r (p_k - 1)$,

$$\left(\mu - \sum_1^r (p_k - 1) \right)^2 \geq \left[\frac{\Pi - 1}{\Pi} \mu - \sum_1^r (p_k - 2) \right] \left(n - \sum_1^r p_k \right),$$

whence

$$\mu - \sum_1^r p_k + r \geq \frac{\Pi - 1}{\Pi} \left(n - \sum_1^r p_k \right) + \frac{r(\Pi + 1) - \sum_1^r p_k}{\Pi} \cdot \frac{n - \sum_1^r p_k}{\mu - \sum_1^r (p_k - 1)}.$$

Since

$$n - \sum_1^r p_k > \mu - \sum_1^r (p_k - 1),$$

$$\mu > \frac{\prod_1^r (p_k - 1) - 1}{\prod_1^r (p_k - 1)} n + \frac{r}{\prod_1^r (p_k - 1)}.$$

Here the condition $r > 1$ must be taken into account because the coefficient of $(n - \sum_{k=1}^r p_k) / (\mu - \sum_{k=1}^r (p_k - 1))$ is zero when $r = 1$. Then if a group is more than 8 or more than 15 times transitive, μ exceeds $\frac{7}{8}n$ or $\frac{4}{3}n$. In connection with this result it might be well to note that a closer study of our group G when 16 times transitive has shown that instead of the limit $\frac{4}{3}n$, the class is actually greater than $\frac{6}{5}n$. Since this appears to be an isolated result depending on the three primes 3, 5, and 7, I omit the proof.

18. If G is exactly $\sigma = p_1 + p_2 + \cdots + p_r$ times transitive, p_1, p_2, \cdots, p_r being distinct odd primes in ascending order of magnitude, $r > 1$, we can prove in like manner that

$$\mu > \frac{\left(\prod_1^r (p_k - 1) - 1\right)n + r - 1}{\prod_1^r (p_k - 1) + p_1 - 2}.$$

19. Let G be doubly transitive.* The substitution s of order 2 and degree $\mu (> 3)$ is one of w conjugates. Any transposition occurs exactly

$$w\mu/n(n-1)$$

times in this set. The number of possible transpositions in which one letter is displaced by s and the other is fixed by s is $\mu(n-\mu)$, so that if y is the number of substitutions conjugate to s which are not commutative with s ,

$$y \cong \frac{2w\mu(n-\mu)}{n(n-1)}.$$

Since μ letters may be paired in $\mu(\mu-1)/2$ ways, the set has $w\mu(\mu-1)/2$ pairs, and $w\mu(\mu-1)/n(n-1)$ substitutions of the set have a given pair in common. Hence if x is the number of letters any one of the w substitutions has in common with s ,

$$\sum_w x = w\mu^2/n, \quad \sum_w x(x-1) = w\mu^2(\mu-1)^2/n(n-1).$$

It is assumed that μ is less than $n/2$. Neither y nor $w-y$ is zero. Now

$$\sum_w x^2 = \sum_w \left(x - \frac{1}{w} \sum_w x\right)^2 + \frac{1}{w} \left(\sum_w x\right)^2,$$

whence

$$\sum_w \left(x - \frac{\mu^2}{n}\right)^2 = \frac{w\mu^2(n-\mu)^2}{n^2(n-1)}.$$

Since

$$\sum_y x \cong y\mu/2,$$

$$\sum_y \left(x - \frac{\mu^2}{n}\right)^2 \cong y \left(\frac{\mu}{2} - \frac{\mu^2}{n}\right)^2,$$

and therefore

$$\sum_{w-y} \left(x - \frac{\mu^2}{n}\right)^2 \leq \frac{w\mu^2(n-\mu)^2}{n^2(n-1)} - y \left(\frac{\mu}{2} - \frac{\mu^2}{n}\right)^2.$$

* This page is a brief sketch of the reasoning given in full in the *Bulletin of the American Mathematical Society*, 2d series, vol. 20 (1914), pp. 471 ff., which see, as well as Bochert, l. c.

Now

$$\sum_{w-y} \left(x - \frac{\mu^2}{n} \right)^2 \cong \frac{1}{w-y} \left[\sum_{w-y} \left(x - \frac{\mu^2}{n} \right) \right]^2 \cong \frac{1}{w-y} \frac{y^2 \mu^2}{n^2} \left(\frac{n}{2} - \mu \right)^2,$$

so that

$$\frac{w\mu^2(n-\mu)^2}{n^2(n-1)} - y \left(\frac{\mu}{2} - \frac{\mu^2}{n} \right)^2 \cong \frac{1}{w-y} \frac{y^2 \mu^2}{n^2} \left(\frac{n}{2} - \mu \right)^2,$$

whence finally

$$\frac{n(n-\mu)}{2\mu} - \frac{(n-\mu)^2}{n-1} \cong \left(\frac{n}{2} - \mu \right)^2.$$

On solution this inequality gives

$$\mu > \frac{1}{2}n - \frac{1}{2}\sqrt{n} - 1.$$

STANFORD UNIVERSITY

August, 1916