<table>
<thead>
<tr>
<th>Title</th>
<th>On transitive groups that contain non-abelian regular subgroups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Nagai, Osamu</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Mathematical Journal. 13(1) P.199–P.207</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1961</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/5988">https://doi.org/10.18910/5988</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/5988</td>
</tr>
<tr>
<td>rights</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
On Transitive Groups that Contain Non-Abelian Regular Subgroups

By Osamu Nagai

1. In 1911 Burnside [2] proved the following celebrated theorem: If a permutation group \( \mathcal{G} \) of prime power degree \( p^m \) contains a cycle of order \( p^m(m > 1) \), then \( \mathcal{G} \) is doubly transitive or imprimitive. This result has been generalized by Schur and Wielandt. The best is due to Wielandt [11]. Before stating his result, we shall define a B-group (see Wielandt [13], p. 57). A group \( \mathcal{G} \) of order \( n \) is called a B-group (or Burnside-group) when every primitive permutation group of degree \( n \) which contains the regular representation of \( \mathcal{G} \) is doubly transitive. Then the result of Wielandt can be stated as follows: An abelian group of composite order in which at least one Sylow group is cyclic is a B-group. Another type of abelian B-group was obtained by Kochendörffer [6] and Manning [7] (at about the same time and by quite different methods): An abelian group of type \( (p^a, p^b) \), where \( a > b \), is a B-group. As for non-abelian B-group, in 1949 Wielandt [12] obtained the following remarkable result: A dihedral group is a B-group. But other type of non-abelian B-group is not known (at least to the author). Now in the present paper we shall show the following:

**Theorem.** Let \( p \) be a prime number of the form \( 2 \cdot 3^a + 1 \), where \( a > 2 \). Then a non-abelian group of order \( 3p \) is a B-group.

In the proof we do not use the ring-properties (due to Schur [9]) which are the useful weapons in studying the abelian case. Our proof is based largely on the investigation of the behavior of a \( p \)-Sylow subgroup.

2. First of all, we shall summarize some known results which are necessary for our purpose.

A. Theorem of Jordan. Let the integer \( n = p + k \), where \( p \) is a prime and \( k \geq 3 \). If a primitive permutation group \( \mathcal{G} \) of degree \( n \) contains a cycle of length \( p \), then \( \mathcal{G} \) contains the alternating group \( A_n \) (Jordan [5]).
B. Theorem of Manning. Let the integer \( n=2p+k \), where \( p \) is a prime \( \geq 5 \) and \( k \geq 2 \). If a primitive permutation group \( G \) of degree \( n \) contains an element of order \( p \) and of degree \( 2p \), then \( G \) contains the alternating group \( A_n \) (Manning [8]).

C. Let \( G \) be a transitive permutation group of degree \( n \). Then \( G \) can be represented as a matric group \( G^* \) of dimension \( n \) isomorphically. Let \( \sum \varepsilon_i \xi_i \) be the complete reduction of \( G^* \) into its irreducible constituents over the complex number field. And let the subgroup \( G_i \) fixing one letter have \( m \) transitive sets \( \Delta_i \) of length \( n_i \) (\( i=1, 2, \ldots, m \)).

CI. If \( G \) is primitive and if \( n_i=2 \) for some \( i \), then \( G \) contains a regular normal subgroup of index 2 (Wielandt [13], p. 43).

CII. \[ m = \sum \varepsilon_i^2 \xi_i \] \quad (Wielandt [13], p. 77).

CIII. Theorem of Frame. The number
\[ q = (n)^m-2 \prod_{i=1}^m n_i/\prod_{i=1}^k x_i^2 \]
is a rational integer, where \( x_i = Dg \xi_i \) (Frame [4]).

D. Theorems of Brauer. Suppose that a finite group \( G \) satisfies the condition: \((*)\) \( G \) contains an element \( P \) of order \( p \) which commutes only with its own powers \( P^i \). Then the order \( g \) of \( G \) is expressed as \( g = p(p-1)(1+np)/t \), where \( 1+np \) is the number of \( p \)-Sylow subgroups and \( t \) is the number of conjugate classes which contain an element of order \( p \). Furthermore, the ordinary irreducible representations of \( G \) can be classified into four different types:

I. The representations \( \mathfrak{A}_u \) of degree \( u \), \( p+1 \). Denote their characters by \( A_u \). Then, for an element \( P \) of order \( p \), \( A_p(P) = 1 \).

II. The representations \( \mathfrak{B}_v \) of degree \( v \), \( p-1 \). Denote their characters by \( B_v \). Then \( B_v(P) = -1 \).

III. The representations \( \mathfrak{C}_c \) of degree \( c = (wp+\delta)/t \) with \( \delta = \pm 1 \). Denote their characters by \( C_c \). Then \( C_c(P) = -\delta \sum \varepsilon^{rk} \). There are \( t \) such characters \( C_c \) and they are \( p \)-conjugate.

IV. The representations \( \mathfrak{D}_d \) of degree \( d \equiv 0 \) (mod \( p \)). Denote their characters by \( D_d \). Then \( D_d(P) = 0 \).

There are \( q = (p-1)/t \) characters of type I and type II in \( G \). These, together with \( t \) characters of type III, form the first \( p \)-block \( B_i(p) \).
Among their degrees holds the following relation:

\[(D) \sum_p DgA_p + \delta DgC^{(\gamma)} = \sum_q DgB_q.\]

It is easy to find all irreducible characters of the normalizer \(\mathfrak{N}(\mathfrak{P})\) of \(\mathfrak{P}\) in \(\mathfrak{S}\), which is generated by \(P\) and \(Q\) such that \(P^p = 1, Q^q = 1, Q^{-1}PQ = P^{qt}\), where \(\gamma\) is a primitive root (mod \(p\)), and \(tq = p - 1\). Let \(\omega\) be a primitive \(q\)-th root of unity. We then have \(q\) linear characters \(\omega_\mu\) \((\mu = 0, 1, 2, \ldots, q - 1)\) defined by

\[\omega_\mu(Q^j) = \omega^{\mu j}, \quad \omega_\mu(P^j) = 1\]

Besides, we have \(t\) conjugate characters \(Y^{(\nu)}\) of degree \(q\).

\[Y^{(\nu)}(Q^j) = 0 \quad \text{for } j \equiv 0 \pmod{q}.\]

**DI.** If we consider the characters of \(\mathfrak{S}\) only for elements \(N\) of the subgroup \(\mathfrak{N}(\mathfrak{P})\), then \(A_\mu(N)\) contains \(u_\mu + 1\) of the \(\omega_\mu(N)\), \(B(N)\) contains \(v_\mu - 1\) of the \(\omega_\mu(N)\), \(C^{(\nu)}(N)\) contains \((w + \delta)/t\) of the \(\omega_\mu(N)\) and \(D_\sigma(N)\) contains \(d_\sigma/p\) of the \(\omega_\mu(N)\).

**E.** Theorem of Tuan. Let \(\mathfrak{S}\) be a group of order \(g = pg'\), where \(p\) is a prime greater than 7 such that \((p, g') = 1\). Let \(\mathfrak{S}\) have no normal subgroup of order \(p\). Let \(\mathfrak{S}\) have a 1-1 irreducible representation of degree \(z < (2p + 1)/3\). Then the factor group of \(\mathfrak{S}\) by its center is isomorphic to \(LF(2, p)\). For \(p = 7\) and \(z = 4\), the factor group of \(\mathfrak{S}\) by its center is isomorphic to either \(LF(2, 7)\) or \(A_7\) (Tuan [10]).

3. Now, we shall prove our theorem. Let \(p = 2 \cdot 3^k + 1\). Let a group \(\mathfrak{S} = \{A, B | A^p = B^3 = 1, B^{-1}AB = A^2\}\). Suppose that \(\mathfrak{S}\) is a primitive permutation group of degree \(3p\) which is not of doubly transitive and contains \(\mathfrak{S}\) as its regular subgroup. Our purpose is to show that, under these circumstances, \(a \leq 2\).

(a). The order of \(\mathfrak{S}\) contains a prime \(p\) to the first power only. Let \(\mathfrak{P}\) be a \(p\)-Sylow subgroup of \(\mathfrak{S}\). Every element \(P \equiv 1\) of \(\mathfrak{P}\) is a product of \(p\)-cycles and 1-cycles (Here \(p\)-cycle means a cycle of length \(p\)). If \(P\) contains only one \(p\)-cycle, then from theorem of Jordan (see A) \(\mathfrak{S}\) is doubly transitive. If \(P\) contains just two \(p\)-cycles, then from the theorem of Manning (see B) \(\mathfrak{S}\) is doubly transitive. So \(P\) is a product of three \(p\)-cycles. Then the subgroup \(\mathfrak{P}_3\) of \(\mathfrak{P}\) leaving one letter fixed is trivial. This means the order of \(\mathfrak{P}\) is \(p\).

(b). The centralizer \(\mathfrak{C}(\mathfrak{P})\) of \(\mathfrak{P}\) in \(\mathfrak{S}\) coincides with \(\mathfrak{P}\). From (a),
we can assume $\mathfrak{S}$ is generated by $A = (a_1, a_2, \ldots, a_p) (a_{p+1}, \ldots, a_{2p}) (a_{2p+1}, \ldots, a_{3p})$. Now put $\Gamma_1 = \{a_1, a_2, \ldots, a_p\}$, $\Gamma_2 = \{a_{p+1}, \ldots, a_{2p}\}$ and $\Gamma_3 = \{a_{2p+1}, \ldots, a_{3p}\}$. Let $V$ be a $p$-regular element in $\mathcal{G}(\mathfrak{S})$ and let $v$ be its order. For an integer $v'$ satisfying $v'v \equiv 1 \pmod{p}$, we consider the element $S = VA^{v'}$. Then $S^v = A$. Hence the lengths of the cycles in $S$ must be the multiples of $p$. If $S$ is itself a cycle of length $3p$, then, by the theorem of Schur [9], $\mathfrak{S}$ is doubly transitive. So $S$ is either a product of a cycle of length $2p$ and that of length $p$ or a product of three $p$-cycles. Therefore the order $v$ of $V = S^p$ is at most 2. Since every element of $\mathcal{G}(\mathfrak{S})$ induces a permutation over $\{\Gamma_1, \Gamma_2, \Gamma_3\}$, $\mathcal{G}(\mathfrak{S})$ is homomorphic to a subgroup of $S_3$. Its kernel is $\mathfrak{S}$ itself. Since the order of an element of $\mathcal{G}(\mathfrak{S})/\mathfrak{S}$ is at most 2, the order $\mathcal{G}(\mathfrak{S})$ is at most $2p$. Suppose there is an element $V$ of order 2 in $\mathcal{G}(\mathfrak{S})/\mathfrak{S}$. Then we can assume that $V = (a_1, a_{p+i}) (a_2, a_{p+i}) \ldots (a_p, a_{p+i})$. Since $\mathfrak{S} = \{A, B\}$ is transitive over $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$, there is an element $X$ such that $a_i^X = a_{p+i}$. This $X$ must normalize $V$, because $\mathfrak{S}$ is contained in the normalizer $\mathfrak{K}(\mathfrak{S})$ of $\mathfrak{S} = \{A\}$. But $X^{-1} V X = V$. This is a contradiction. Therefore $V = E$, that is, $\mathcal{G}(\mathfrak{S}) = \mathfrak{S}$. Thus $\mathfrak{S}$ satisfies the condition $(\ast)$ (see D). And $g = p(p-1)/(1+np)/t$.

Now, we shall examine the decomposition of $\mathfrak{S}^*$ into its irreducible constituents (see C). Denote by $\Pi^*$ the character of $\mathfrak{S}^*$.

(c) $x_i = 1$ and $x_i > 1$ for $i \geq 2$. Since $\mathfrak{S}$ is transitive, $e_i = 1$. If $x_2 = 1$, then $\mathfrak{S}_2$ is linear. As $\mathfrak{S}$ is not abelian, $\mathfrak{S}_2$ is not faithful. Let $\mathfrak{K}$ be its kernel. Since $\mathfrak{S}$ is primitive, $\mathfrak{K}$ is transitive. Hence $\mathfrak{S}^*(\mathfrak{S})$ can be considered as the matric group $\mathfrak{S}^*$ corresponding to $\mathfrak{K}$. $\mathfrak{S}_2$, considered in $\mathfrak{K}$, is a unit representation. This contradicts the transitiveness of $\mathfrak{S}$.

(d) The irreducible representations of type III can not occur in the decomposition $\sum e_i \mathfrak{s}_i$ of $\mathfrak{S}^*$. If some $\mathfrak{s}_i$ is of type III, all of its $p$-conjugate representations must occur. Thus we have the following inequality: $3 \geq 1 + t(wp + \delta)/t \geq wp$. $3 \geq w$.

i) $w = 3$. Then $c = (3p-1)/t$. $3 - 1 \equiv 0 \pmod{t}$. If $t = 1$, such representation $\mathfrak{s}_i$ can be considered as that of type II. This will be discussed later (see (h)). If $t = 2$, then $\Pi^* = A_0 + C^{(1)} + C^{(2)}$. Decompose $C^{(2)}$ in $\mathfrak{K}(\mathfrak{S})$. Then $C^{(1)}$ contains only one linear character, say $\omega_\mu$. Since $C^{(2)}$ is $p$-conjugate to $C^{(1)}$, $C^{(2)}$ also contains the same $\omega_\mu$. For the element $B$, since $B$ does not fix any letter at all, we have $0 = 1 + 2\omega$. This is impossible.

ii) $w = 2$. Then $3p = 1 + 2p + \delta + x$. If $\delta = 1$, $x = p - 2$. This can not give the degree of the characters. Hence $\delta = -1$. $c = (2p-1)/t$. This
Transitive Groups

203

yields \( t=1 \). This case will be discussed later (see (h)).

ii) \( w=1 \). Then \( c=(p+1)/t \) or \( c=(p-1)/t \). If \( C^{(\gamma)} \) is not faithful, then the order of its kernel \( \mathfrak{K} \) is prime to \( p \) (Brauer [1], Theorem 4). On the other hand, since \( \mathfrak{S} \) is primitive, the normal subgroup \( \mathfrak{K} \) is transitive. So the order of \( \mathfrak{K} \) is a multiple of \( 3p \). This is a contradiction. Thus such representation \( C^{(\gamma)} \) is faithful. And by the theorem of Tuan (see E), \( p=7 \) or \( \mathfrak{S}=LF(2,p) \). In \( LF(2,p) \), since \( p-1 \equiv 0 \) (mod 3), the subgroup of index \( 3p \) must be contained either in a dihedral group of order \( p+1 \), or in \( A_4 \). But anyhow this means that \( p \leq 2 \cdot 3+1 \). This is the desired one.

(e). \( \Pi^* \), restricted in \( \mathfrak{N}(\mathfrak{S}) \), contains just three different linear characters of \( \mathfrak{N}(\mathfrak{S}) \), one of which is a principal character \( \omega_0 \). Set \( \Omega=\omega_0+\omega_1+\ldots+\omega_q-1 \). Then we have \( \Omega(1)=\Omega(P^j)=q, \Omega(Q^j)=0 \) for \( j \equiv 0 \) (mod \( q \)).

\[
\sum \Pi^*(N)\Omega(N) = \sum \Pi^*(P^i)\Omega(P^j) = 3pq
\]

with \( N \) in the sum ranging over the elements of \( \mathfrak{N}(\mathfrak{S}) \). From the orthogonality relations for the characters of \( \mathfrak{N}(\mathfrak{S}) \), \( \Pi^*(N) \) contains three of the \( \omega_{\mu}(N) \). Since \( \Pi^* \) contains a principal character of \( \mathfrak{S} \), at least one of the \( \omega_{\mu} \) is \( \omega_0 \). As (d) i), these \( \omega_{\mu} \) are different.

(f). \( q=(p-1)/t=3 \) or \( =6 \). From (b) we can assume that \( \mathfrak{N}(\mathfrak{S})=\{A, X|X^{3t}=1, X^t=B \text{ and } X^{-1}AX=A^t\} \), where \( \gamma \) is a primitive root modulo \( p \) and \( q=(p-1)/t=3l \). Since \( X^t=B \), the lengths of cycles in \( X \) are the multiples of \( 3 \). Let \( 3l_1, 3l_2, \ldots, 3l_s \) be the lengths of cycles in \( X \), where \( \sum l_i=p \). Then value of \( \Pi^*(X) \) must be zero. But as above \( \Pi^* \) contains only three different linear characters of \( \mathfrak{N}(\mathfrak{S}) \), say \( \omega_0, \omega_\mu \) and \( \omega_\nu \). This yields the equation \( \omega_0(X)+\omega_\mu(X)+\omega_\nu(X)=0 \). \( 1+\omega_0+\omega_\nu=0 \). From the theorem of Kronecker (Carmichael [3], p. 228), \( (\omega^\mu)^3=(\omega^\nu)^3=1 \). Thus the three different linear characters must be \( \omega_0, \omega_1 \) and \( \omega_{3t} \). Therefore

\[
\Pi^*(X^t) = 1+\omega^{it}+\omega^{3it} = \begin{cases} 0 & \text{for } i \equiv 0 \pmod{3}, \\ 3 & \text{for } i \equiv 0 \pmod{3}. \end{cases}
\]

Since \( \Pi^*(\mathfrak{S}) \) is the character corresponding to the permutation \( \mathfrak{S} \), every element of \( \mathfrak{N}(\mathfrak{S}) \) fixes either three letters or none of them. If \( l_i > l_j \), then \( X^{3l_j} \) leaves fixed at least \( 3l_j \) letters. This means \( l_j = 1 \). Since the order of \( X \) is \( 3l \), \( l_i=l_2=\cdots=l_s=1 \) and \( l_1=\cdots=l_{s-1}=1 \). Pick up the element \( X^3 \), then as above \( l_1=l_2=\cdots=l_{s-1}=1 \) and \( l_s = 1 \). Consider the cyclic subgroup generated by \( X^3 \). This group is a permutation group over \( 3p-3 \) letters and of order \( l \). But since the subgroup leaving one
letter fixed is trivial, $3p - 3 \equiv 0 \pmod{l}$. Since $X' = B$ fixes no letter, $l \equiv 0 \pmod{3}$. Thus

$$3(p-1) = 3 \cdot 3 \cdot l \cdot t = 2 \cdot 3^{a+1} \equiv 0 \pmod{l},$$

$$l \equiv 0 \pmod{3}.$$  

From these, $l = 1$ or $l = 2$. If $l = 1$, then $t = 2 \cdot 3^{a-1}$ and $(p-1)/t = 3$. If $l = 2$, then $t = 3^{a-1}$ and $(p-1)/t = 6$.

(g). $x_i \neq p$. Let $\Xi$ be the irreducible representation of degree $p$: $x_i = p$. Then its character contains only one linear (non-principal) character $\omega_p$. Consider the determinant of $\Xi(X)$. Then $\text{Det} (\Xi(X)) = \omega_p \cdot \omega_{f(1+2+\cdots+q-1)}$. If $(p-1)/t = 3$, then $\text{Det} (\Xi(X)) = \omega_p \cdot \omega^{(1+2)} = \omega^3$. The representation of $\Xi$ induced by

$$X \to \text{Det} (\Xi(X))$$

is linear and its kernel $\mathcal{K}$ has an index at least 3 in $\mathcal{G}$. By the theorem of Brauer (Theorem 2, [1]), $\mathcal{G} = \mathcal{G}'$ and $[\mathcal{G} : \mathcal{G}'] = 3$. This yields that the normalizer of $\mathcal{G}$ in $\mathcal{G}'$ is $\mathcal{G}$ itself. By the theorem of Burnside, $\mathcal{G}'$ contains a normal $p$-complement which is a characteristic subgroup of $\mathcal{G}'$. Hence this subgroup is normal in $\mathcal{G}$ which is not transitive. This contradicts the primitiveness of $\mathcal{G}$. If $(p-1)/t = 6$, then $\text{Det} (\Xi(X)) = \omega_p \cdot \omega^{(1+2+\cdots+5)} = (-1) \omega_p$. The representation of $\Xi$ induced by

$$X \to \text{Det} (\Xi(X))$$

is linear and its kernel $\mathcal{K}$ has an index at least 6 in $\mathcal{G}$. Then, as above, by the theorems of Brauer, $[\mathcal{G} : \mathcal{G}'] = 6$. And the normalizer of $\mathcal{G}$ in $\mathcal{G}'$ is $\mathcal{G}$ itself. Hence there exists a normal subgroup of $\mathcal{G}$ which is not transitive. This is a contradiction.

(h). Now, we can examine the decomposition of $\Pi^*$ explicitly. For convenience' sake, we shall denote by "x" the character of degree $x$.

i) $x_2 = up + 1$. Then $3p \geq 1 + up + 1$. If $u = 2$, then $3p - x_1 - x_2 = p - 2$. This shows that "$x_3" is of type III. This contradicts (d). If $u = 1$, then $3p - x_1 - x_2 = 2p - 2$. This shows that there are two more irreducible characters of degree $p - 1$ in $\Pi^*$. Then,

Case I. $\Pi^* = "1" + "p + 1" + "p - 1" + "p - 1"$.

ii) $x_2 = vp - 1$. Then $3 \geq v$. If $v = 3$, then $\Pi^* = "1" + "3p - 1"$. This shows that $\mathcal{G}$ is doubly transitive. If $v = 2$, then

$$\Pi^* = "1" + "2p - 1" + "p".$$
This contradicts (g). If \( v = 1 \), then \( 3\rho - x_1 - x_2 = 2\rho \). This yields several cases:

**Case II.** \( \Pi^* = \left\{ 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ 2\rho \right\} \),

**Case I.** \( \Pi^* = \left\{ 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ \rho + 1 \right\} \)
or

\( \Pi^* = \left\{ 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ \rho \right\} + \left\{ \rho \right\} \).

The last case does not occur (see (g)).

(i). **Case I does not occur.** Suppose on the contrary that Case I occurs: \( \Pi^* = \left\{ 1 \right\} + \left\{ \rho + 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ \rho - 1 \right\} \). We shall discuss two cases: \( q = 6 \), \( q = 3 \) separately.

i) \( q = (\rho - 1)/t = 6 \). Then since \( t \) is odd, by the theorem of Brauer (Theorem 9, [1]) \( \left[ \mathcal{G} : \mathcal{G}' \right] \equiv 0 \) (mod 2). Since \( \left[ \mathcal{G} : \mathcal{G}' \right] = 6 \) yields contradiction as above and since \( \left[ \mathcal{G} : \mathcal{G}' \right] \leq 6 \), \( \left[ \mathcal{G} : \mathcal{G}' \right] = 2 \). So by the theorem of Brauer (Corollary 5, [1]) the order \( g' \) of \( \mathcal{G}' \) is \( g' = \rho(\rho - 1)(1 + np)/t' = 3\rho(1 + np) \) and \( \mathcal{G} = \mathcal{G}' \). If \( \rho \pm 1 \) is reducible in \( \mathcal{G}' \), then its irreducible constituents should be of degree \( (\rho \pm 1)/t' \), where \( t' = 2t = 2 \cdot 3^{-1} \). If this character of \( \mathcal{G}' \) is not faithful, then its kernel \( \mathcal{K} \) is the unique maximal normal subgroup of an order prime to \( \rho \) (Brauer [1], Corollary 2). This shows \( \mathcal{K} \) is characteristic in \( \mathcal{G}' \). Therefore \( \mathcal{K} \) is normal in \( \mathcal{G} \). But this \( \mathcal{K} \) can not be transitive. Thus by the theorem of Tuan (see E), \( \rho = 7 \) or \( \mathcal{G} = LF(2, \rho) \). Then as (d) iii), we can assume both \( \left\{ \rho - 1 \right\} \) and \( \left\{ \rho + 1 \right\} \) are irreducible in \( \mathcal{G}' \). Since \( \mathcal{G}' = \mathcal{G}' \) and \( \mathcal{G}' \) satisfies condition (*), we can examine the degrees of the irreducible characters of \( \mathcal{G}' \) in its first \( \rho \)-block \( B_1(\rho) \). \( B_1(\rho) \) consists of \( \left\{ 1 \right\} \), \( \left\{ \rho + 1 \right\} \), \( \left\{ \rho - 1 \right\} \) and \( \left\{ (wp + \delta)/t' \right\} \). From (D),

\[
1 + \rho + 1 + \delta(wp + \delta)/t' = \rho - 1, \quad 3 + \delta(wp + \delta)/t' = 0.
\]

This yields \( \delta = -1 \), \( 3t' = wp - 1 \). But since \( 3t' = \rho - 1 \), we have \( w = 1 \). This yields that \( B_1(\rho) \) contains \( \left\{ (\rho - 1)/t' \right\} \). This is a contradiction (see (d) iii)).

ii) \( (\rho - 1)/t = 3 \). In this case, we can assume \( \mathcal{G} = \mathcal{G}' \). So the latter half of the above argument can be applied. Thus we can exclude Case I.

Now we shall consider the case II, which is the only possible case.

**Case II.** \( \Pi^* = \left\{ 1 \right\} + \left\{ \rho - 1 \right\} + \left\{ 2\rho \right\} \).

(i). \( n_i \vdash n \). Assume the contrary, then, from \( m = \sum_{i=1}^{k} e_i^2 \), we have
Applying the theorem of Frame, we can conclude that 
\[ q = \frac{3p(wp-1)}{8p(p-1)} \] must be a rational integer. We can put \( p-1=6s \). Then 
\[ q = \frac{(9s+1)^2}{4s} \] 
\[ 81s^2 + 18s + 1 = 0 \pmod{s} \] \( s = 1 \). This means \( p = 2 \cdot 3 + 1 \). This is the desired one.

(k). \( 4p = 3c^2 + 1 \) for an integer \( c \). Since \( n_3 = 2 \) is excluded in C1, we can assume \( 2 \leq n_3 \leq n_2 \). Put \( n_3 = v \). Applying the methods of Wielandt [14], we have two equalities:

(1) \[ v + 2pa + (p-1)b = 0, \]

(2) \[ v^2 + 2pa^2 + (p-1)b^2 = 3pv, \]

where \( a, b \) are integers.

From (1), \( v \equiv b \pmod{p} \). From (2),

\[ (p-1)b^2 < 3pv. \]

\[ b^2 < 3pv/(p-1) < 3p \cdot 3p/(p-1) = 9p^2/(p-1). \]

Since \( p \geq 7 \), we have \( b^2 < p^2 \). Then 1) \( b = v \) or 2) \( b = -p + v \) or 3) \( b = -2p + v \).

If \( b = v \), then \( 2a + b = 0 \). Substituting these in (2), we have

\[ b^2 + 2pa^2 + (p-1)b^2 = 3pb. \]

\[ 2a^2 + b^2 = 3b. \]

\[ 2a^2 + 4a^2 + 6a = 0. \]

This yields \( a = b = v = 0 \) or \( a = -1 \) and \( b = 2 \). This contradicts C1. If \( b = -p + v \), then \( a = -(b+1)/2 \). Substituting this in (2), we have \( 4p = 3b^2 + 1 \). If \( b = -2p + v \), then \( a = -(b+2)/2 \). Substituting this in (2), we have \( 4p = 3(b+1)^2 + 1 \).

(l). \( 4p = 3c^2 + 1 \) yields \( p = 2 \cdot 3^a + 1 \) with \( a \leq 2 \). From \( 4p = 3c^2 + 1 \) and \( p = 2 \cdot 3^a + 1 \), we have \( 8 \cdot 3^{a-1} = c^2 - 1 \). If \( c - 1 = 2 \cdot 3^b \), then \( c + 1 = 2 \cdot 3^b + 2 \). \( c^2 - 1 = 4 \cdot 3^b(3^b + 1) \). We have \( b = a - 1 \) and \( 3^b + 1 = 2 \). These imply \( b = 0 \).

Hence \( a = 1 \). If \( c - 1 = 2 \cdot 3^b \), then \( c + 1 = 4 \cdot 3^b + 2 \). \( c^2 - 1 = 8 \cdot 3^b(2 \cdot 3^b + 1) \).

We have \( 2 \cdot 3^b + 1 = 3 \). \( b = 0 \). Then \( c^2 - 1 = 8 \cdot 3 = 8 \cdot 3^{a-1} \). Hence \( a = 2 \). Thus our theorem is proved completely.

4. There exists a primitive not doubly transitive group of degree 21, which contains a non-abelian regular subgroup of order 21 (due to N. Ito).

Let \( \Omega \) be the set of unordered pairs \( \{a, b\} \) from the set of seven letters: \( \{1, 2, 3, \ldots, 6, 7\} \) such that \( a \neq b \). For an element \( G \) of the alternating group \( A_7 \), we consider the permutation \( G \) over \( \Omega \) such that
\{a, b\}^G = \{a^G, b^G\}. Thus we have a permutation group \(\bar{G}\) over \(\Omega\) which is isomorphic to \(A_7\). Since there is no element which maps \{1, 2\} to \{1, 2\} and \{1, 3\} to \{4, 5\}, \(\bar{G}\) is not doubly transitive. As is easily seen, \(\bar{G}_{(1,2)}\) is maximal. Hence \(\bar{G}\) is primitive. The permutations corresponding to the normalizer of a 7-Sylow subgroup are of order 21 and regular.

The above example shows that \(a | p| 1\) in \(p = 2 \cdot 3^a + 1\) is essential. But whether \(a | p| 2\) is essential or not is an open question.

(Received March 24, 1961)

References

[10] H. Tuan: On groups whose orders contain a prime number to the first power, Ann. of Math. 45 (1944), 110-140.