Nagai, Osamu
Osaka Math. J.
13 (1961), 199-207.

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 $\mathfrak{G}$ of prime power degree p^m contains a cycle of order $p^m(m>1)$, then $\mathfrak{G}$ 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 $\mathfrak{H}$ 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 $\mathfrak{H}$ 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 $k\geqq 3$. If a primitive permutation group $\mathfrak{G}$ of degree n contains a cycle of length p, then $\mathfrak{G}$ contains the alternating group A_n (Jordan [5]).

B. Theorem of MANNING. Let the integer $n=2p+k$, where p is a prime $\geqq 5$ and $k\geqq 2$. If a primitive permutation group $\mathfrak{G}$ of degree n contains an element of order p and of degree $2p$, then $\mathfrak{G}$ contains the alternating group A_n (Manning [8]).

C. Let $\mathfrak{G}$ be a transitive permutation group of degree n. Then $\mathfrak{G}$ can be represented as a matric group $\mathfrak{G}^*$ of demension n isomorphically. Let $\sum_{i=1}^{k} e_i\mathfrak{X}_i$ be the complete reduction of $\mathfrak{G}^*$ into its irreducible constituents over the complex number field. And let the subgroup $\mathfrak{G}_1$ fixing one letter have m transitive sets Δ_i of length n_i $(i=1, 2, \cdots, m)$.

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

CII. $m = \sum_{i=1}^{k} e_i^2$ (Wielandt [13], p. 77).

CIII. Theorem of FRAME. The number

$$q = (n)^{m-2} \prod_{i=1}^{m} n_i / \prod_{i=1}^{k} x_i^{e_i^2}$$

is a rational integer, where $x_i = Dg\mathfrak{X}_i$ (Frame [4]).

D. Theorems of BRAUER. Suppose that a finite group $\mathfrak{G}$ satisfies the condition: (*) $\mathfrak{G}$ contains an element P of order p which commutes only with its own powers P^i. Then the order g of $\mathfrak{G}$ 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 $\mathfrak{G}$ can be classified into four different types:

I. The representations $\mathfrak{A}_\rho$ of degree $u_\rho p+1$. Denote their characters by A_ρ. Then, for an element P of order p, $A_\rho(P)=1$.

II. The representations $\mathfrak{B}_\sigma$ of degree $v_\sigma p-1$. Denote their charcters by B_σ. Then $B_\sigma(P)=-1$.

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

IV. The represntations $\mathfrak{D}_\tau$ of degree $d_\tau\equiv 0 \pmod p$. Denote their characters by D_τ. Then $D_\tau(P)=0$.

There are $q=(p-1)/t$ characters of type I and type II in $\mathfrak{G}$. These, together with t characters of type III, form the first p-block $B_1(p)$.

Among their degrees holds the following relation:

(D) $$\sum_{\rho} DgA_{\rho}+\delta DgC^{(\nu)} = \sum_{\sigma} DgB_{\sigma}\,.$$

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

$$Y^{(\nu)}(Q^j) = 0 \qquad \text{for} \quad j \not\equiv 0 \pmod{q}.$$

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

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

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

(a). *The order of* $\mathfrak{G}$ *contains a prime* p *to the first power only.* Let $\mathfrak{P}$ be a p-Sylow subgroup of $\mathfrak{G}$. Every element $P\neq 1$ 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) $\mathfrak{G}$ is doubly transitive. If P contains just two p-cycles, then from the theorem of Manning (see B) $\mathfrak{G}$ is doubly transitive. So P is a product of three p-cycles. Then the subgroup $\mathfrak{P}_1$ 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* $\mathfrak{G}$ *coincides with* $\mathfrak{P}$. From (a),

we can assume $\mathfrak{P}$ is generated by $A=(a_1, a_2, \cdots, a_p)(a_{p+1}, \cdots, a_{2p})(a_{2p+1}, \cdots, a_{3p})$. Now put $\Gamma_1=\{a_1, a_2, \cdots, a_p\}$, $\Gamma_2=\{a_{p+1}, \cdots, a_{2p}\}$ and $\Gamma_3=\{a_{2p+1}, \cdots, a_{3p}\}$. Let V be a p-regular element in $\mathfrak{C}(\mathfrak{P})$ 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], $\mathfrak{G}$ 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 $\mathfrak{C}(\mathfrak{P})$ induces a permutation over $\{\Gamma_1, \Gamma_2, \Gamma_3\}$, $\mathfrak{C}(\mathfrak{P})$ is homomorphic to a subgroup of S_3. Its kernel is $\mathfrak{P}$ itself. Since the order of an element of $\mathfrak{C}(\mathfrak{P})/\mathfrak{P}$ is at most 2, the order $\mathfrak{C}(\mathfrak{P})$ is at most $2p$. Suppose there is an element V of order 2 in $\mathfrak{C}(\mathfrak{P})$. Then we can assume that $V=(a_1, a_{p+i_1})(a_2, a_{p+i_2})\cdots(a_p, a_{p+i_p})$. Since $\mathfrak{H}=\{A, B\}$ is transitive over $\Gamma_1\cup\Gamma_2\cup\Gamma_3$, there is an element X such that $a_1^X=a_{2p+j}$. This X must normalize V, because $\mathfrak{H}$ is contained in the normalizer $\mathfrak{N}(\mathfrak{P})$ of $\mathfrak{P}=\{A\}$. But $X^{-1}VX\neq V$. This is a contradiction. Therefore $V=E$, that is, $\mathfrak{C}(\mathfrak{P})=\mathfrak{P}$. Thus $\mathfrak{G}$ satisfies the condition (*) (see D). And $g=p(p-1)(1+np)/t$.

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

(c). $x_1=1$ *and* $x_i>1$ *for* $i\geqq 2$. Since $\mathfrak{G}$ is transitive, $e_1=1$. If $x_2=1$, then $\mathfrak{X}_2$ is linear. As $\mathfrak{G}$ is not abelian, $\mathfrak{X}_2$ is not faithful. Let $\mathfrak{K}$ be its kernel. Since $\mathfrak{G}$ is primitive, $\mathfrak{K}$ is transitive. Hence $\mathfrak{G}^*(\mathfrak{K})$ can be considered as the matric group $\mathfrak{K}^*$ corresponding to $\mathfrak{K}$. $\mathfrak{X}_2$, considered in $\mathfrak{K}$, is a unit representation. This contradicts the transitiveness of $\mathfrak{K}$.

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

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

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

iii) $w=1$. Then $c=(p+1)/t$ or $c=(p-1)/t$. If $C^{(\nu)}$ is not faithful, then the order of its kernel $\mathfrak{R}$ is prime to p (Brauer [1], Theorem 4). On the other hand, since $\mathfrak{G}$ is primitive, the normal subgroup $\mathfrak{R}$ is transitive. So the order of $\mathfrak{R}$ is a multiple of $3p$. This is a contradiction. Thus such representation $C^{(\nu)}$ is faithful. And by the theorem of Tuan (see E), $p=7$ or $\mathfrak{G}=LF(2,p)$. In $LF(2,p)$, since $p-1\equiv 0 \pmod 3$, the subgroup of index $3p$ must be contained either in a dihedral group of order $p+1$, or in A_5. But anyhow this means that $p\leqq 2\cdot 3+1$. This is the desired one.

(e). Π^*, *restricted in* $\mathfrak{N}(\mathfrak{P})$, *contains just three different linear characters of* $\mathfrak{N}(\mathfrak{P})$, *one of which is a principal character* ω_0. Set $\Omega=\omega_0+\omega_1+\cdots+\omega_{q-1}$. Then we have $\Omega(1)=\Omega(P^j)=q$, $\Omega(Q^j)=0$ for $j\not\equiv 0 \pmod q$.

$$\sum \Pi^*(N)\Omega(N) = \sum \Pi^*(P^i)\Omega(P^i) = 3pq$$

with N in the sum ranging over the elements of $\mathfrak{N}(\mathfrak{P})$. From the orthogonality relations for the characters of $\mathfrak{N}(\mathfrak{P})$, $\Pi^*(N)$ contains three of the $\omega_\mu(N)$. Since Π^* contains a principal character of $\mathfrak{G}$, at least one of the ω_μ is ω_0. As (d) i), these ω_μ are different.

(f). $q=(p-1)/t=3$ *or* $=6$. From (b) we can assume that $\mathfrak{N}(\mathfrak{P})=\{A, X \mid X^{3l}=1, X^l=B$ and $X^{-1}AX=A^{\gamma^t}$, where γ is a primitive root modulo p and $q=(p-1)/t=3l\}$. Since $X^l=B$, the lengths of cycles in X are the multiples of 3. Let $3l_1, 3l_2, \cdots, 3l_s$ be the lengths of cycles in X, where $\sum_{i=1} l_i=p$. Then value of $\Pi^*(X)$ must be zero. But as above Π^* contains only three different linear characters of $\mathfrak{N}(\mathfrak{P})$, say ω_0, ω_μ and ω_ν. This yields the equation $\omega_0(X)+\omega_\mu(X)+\omega_\nu(X)=0$. $1+\omega^\mu+\omega^\nu=0$. From the theorem of Kronecker (Carmichael [3], p. 228), $(\omega^\mu)^3=(\omega^\nu)^3=1$. Thus these three different linear characters must be ω_0, ω_l and ω_{2l}. Therefore

$$\Pi^*(X^i) = 1+\omega^{il}+\omega^{2il} = \begin{cases} 0 & \text{for } i\not\equiv 0 \pmod 3, \\ 3 & \text{for } i\equiv 0 \pmod 3. \end{cases}$$

Since $\Pi^*(\mathfrak{G})$ is the character corresponding to the permutation $\mathfrak{G}$, every element of $\mathfrak{N}(\mathfrak{P})$ 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 $3l$, $l_1=l_2=\cdots=l_i=l$ and $l_{i+1}=l_{i+2}=\cdots=l_s=1$. Pick up the element X^3, then as above $l_1=l_2=\cdots=l_{s-1}=l$ 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 $X^l=B$ fixes no letter, $l\not\equiv 0 \pmod 3$. Thus

$$3(p-1) = 3\cdot 3\cdot l\cdot t = 2\cdot 3^{a+1} \equiv 0 \pmod{l}.$$
$$l \not\equiv 0 \pmod 3.$$

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 $\mathfrak{D}$ be the irreducible representation of degree p: $x_i=p$. Then its character contains only one linear (non-principal) character ω_μ. Consider the determinant of $\mathfrak{D}(X)$. Then $\mathrm{Det}\,(\mathfrak{D}(X))=\omega^\mu\cdot\omega^{t(1+2+\cdots+q-1)}$. If $(p-1)/t=3$, then $\mathrm{Det}\,(\mathfrak{D}(X))=\omega^\mu\cdot\omega^{t(1+2)}=\omega^\mu$. The representation of $\mathfrak{G}$ induced by

$$X \to \mathrm{Det}\,(\mathfrak{D}(X))$$

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

$$X \to \mathrm{Det}\,(\mathfrak{D}(X))$$

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

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

i) $x_2=up+1$. Then $3p\geqq 1+up+1$. $2\geqq u$. 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 Π^*. Then,

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

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

$$\Pi^* = \text{"1"}+\text{"}2p-1\text{"}+\text{"}p\text{"}.$$

This contradicts (g). If $v=1$, then $3p-x_1-x_2=2p$. This yields several cases:

Case II. $\Pi^* = \text{“1”}+\text{“}p-1\text{”}+\text{“}2p\text{”}$,

Case I. $\Pi^* = \text{“1”}+\text{“}p-1\text{”}+\text{“}p-1\text{”}+\text{“}p+1\text{”}$

or

$$\Pi^* = \text{“1”}+\text{“}p-1\text{”}+\text{“}p\text{”}+\text{“}p\text{”}.$$

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

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

i) $q=(p-1)/t=6$. Then since t is odd, by the theorem of Brauer (Theorem 9, [1]) $[\mathfrak{G}:\mathfrak{G}']\equiv 0 \pmod 2$. Since $[\mathfrak{G}:\mathfrak{G}']=6$ yields contradiction as above and since $[\mathfrak{G}:\mathfrak{G}']\leqq 6$, $[\mathfrak{G}:\mathfrak{G}']=2$. So by the theorem of Brauer (Corollary 5, [1]) the order g' of $\mathfrak{G}'$ is $g'=p(p-1)(1+np)/t'=3p(1+np)$ and $\mathfrak{G}'=\mathfrak{G}''$. If “$p\pm 1$” is reducible in $\mathfrak{G}'$, then its irreducible constituents should be of degree $(p\pm 1)/t'$, where $t'=2t=2\cdot 3^{a-1}$. If this character of $\mathfrak{G}'$ is not faithful, then its kernel $\mathfrak{N}$ is the unique maximal normal subgroup of an order prime to p (Brauer [1], Corollary 2). This shows $\mathfrak{N}$ is characteristic in $\mathfrak{G}'$. Therefore $\mathfrak{N}$ is normal in $\mathfrak{G}$. But this $\mathfrak{N}$ can not be transitive. Thus by the theorem of Tuan (see E), $p=7$ or $\mathfrak{G}\cong LF(2, p)$. Then as (d) iii), we can assume both “$p-1$” and “$p+1$” are irreducible in $\mathfrak{G}'$. Since $\mathfrak{G}'=\mathfrak{G}''$ and $\mathfrak{G}'$ satisfies condition (*), we can examine the degrees of the irreducible characters of $\mathfrak{G}'$ in its first p-block $\tilde{B}_1(p)$. $\tilde{B}_1(p)$ consists of “1”, “$p+1$”, “$p-1$” and t' “$(wp+\delta)/t'$”. From (D),

$$1+p+1+\delta(wp+\delta)/t' = p-1\,.\quad 3+\delta(wp+\delta)/t'=0\,.$$

This yields $\delta=-1$, $3t'=wp-1$. But since $3t'=p-1$, we have $w=1$. This yields that $\tilde{B}_1(p)$ contains “$(p-1)/t'$”. This is a contradiction (see (d) iii)).

ii) $(p-1)/t=3$. In this case, we can assume $\mathfrak{G}=\mathfrak{G}'$. 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. $\Pi^* = \text{“1”}+\text{“}p-1\text{”}+\text{“}2p\text{”}$.

(j). $n_2 \neq n_3$. Assume the contrary, then, from $m=\sum_{i=1}^{k} e_i^2$, we have

$n_1=1$ and $n_2=n_3=(3p-1)/2$. Applying the theorem of Frame, we can conclude that $q=3p(wp-1)^2/8p(p-1)$ must be a rational integer. We can put $p-1=6s$. Then $q=(9s+1)^2/4s$. $81s^2+18s+1\equiv 0 \pmod{s}$. We have $s=1$. This means $p=2\cdot 3+1$. This is the desired one.

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

$$v+2pa+(p-1)b = 0, \tag{1}$$

$$v^2+2pa^2+(p-1)b^2 = 3pv, \tag{2}$$

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 $p\geqq 7$, 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 CI. 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* $a\leqq 2$. 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 $c-1=2^2\cdot 3^b$, 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 Ω be the set of unordered pairs $\{a, b\}$ from the set of seven letters: $\{1, 2, 3, \cdots, 6, 7\}$ such that $a\neq b$. For an element G of the alternating group A_7, we consider the permutation $\bar{G}$ over Ω such that

$\{a, b\}^{\bar{G}} = \{a^G, b^G\}$. Thus we have a permutation group $\overline{\mathfrak{G}}$ over Ω which is isomorphic to A_7. Since there is no element which maps $\{1, 2\}$ to $\{1, 2\}$ and $\{1, 3\}$ to $\{4, 5\}$, $\overline{\mathfrak{G}}$ is not doubly transitive. As is easily seen, $\overline{\mathfrak{G}}_{\{1,2\}}$ is maximal. Hence $\overline{\mathfrak{G}}$ is primitive. The permutations corresponding to the normalizer of a 7-Sylow subgroup are of order 21 and regular.

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

(Received March 24, 1961)

References

[1] R. Brauer: On permutation groups of prime degree and related classes of groups, Ann. of Math. **44** (1943), 57-79.

[2] W. Burnside: Theory of groups of finite order. 2 ed. Cambridge Univ. Press (1911).

[3] R. D. Carmichael: Introduction to the theory of groups of finite order. Boston (1937).

[4] J. S. Frame: The double cosets of a finite group, Bull. Amer. Math. Soc. **47** (1941), 458-467.

[5] C. Jordan: Traité des substitutions et des équations algébriques, Paris. Gauthiers-Villars (1870).

[6] R. Kochendörffer: Untersuchungen über eine Vermutung von W. Burnside, Schriften Math. Sem. Inst. Angew. Math. Univ. Berlin **3** (1937), 155-180.

[7] D. Manning: On simply transitive groups with transitve abelian subgroups of the same degree, Trans. Amer. Math. Soc. **40** (1936), 324-342.

[8] W. A. Manning: On the order of primitive groups, Trans. Amer. Math. Soc. **10** (1909), 247-258.

[9] I. Schur: Zur Theorie der einfach transitiven Permutationsgruppen, Sitz. Preuss. Akad. Wiss. Berlin. phys.-math. KI. (1933), 598-623.

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

[11] H. Wielandt: Zur Theorie der einfach transitiven Permutationsgruppen, Math. Z. **40** (1935), 582-587.

[12] ————: Zur Theorie der einfach transitiven Permutationsgruppen II, Math. Z. **52** (1950), 384-393.

[13] ————: Vorlesungen über Permutationsgruppen (Ausarbeitung von J. André.) Tübingen 1955.

[14] ————: Primitive Permutationsgruppen von Grad $2p$, Math. Z. **63**, (1956), 478-485.