The University of Osaka
Institutional Knowledge Archive

Title	On simple groups related to permutation-groups of prime degree. I
Author(s)	Nagai, Osamu
Citation	Osaka Mathematical Journal. 1956, 8(1), p. 107-117
Version Type	VoR
URL	https://doi.org/10.18910/12443
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

Osaka Mathematical Journal
Vol. 8, No. 1, June, 1956.

On Simple Groups Related to Permutation-Groups of Prime Degree I

By Osamu NAGAI

1. Let $\mathfrak{G}$ be a group which satisfies the following two conditions:

$(*)$ *$\mathfrak{G}$ contains an element P of prime order p which commutes only with its own powers P^i,*

$(**)$ *$\mathfrak{G}$ coincides with its own commutator-subgroup $\mathfrak{G}'$.*

Obviously the transitive permutation-group of degree p satisfies the condition $(*)$.

Using his brilliant theory of modular representations, R. Brauer investigated the structure of $\mathfrak{G}$ and proved the following interesting theorem ([2], Theorem 10): *The order of $\mathfrak{G}$ is expressed as $g=p(p-1)(1+np)/t$ where $1+np$ is the number of subgroups of order p in $\mathfrak{G}$ and t is the number of classes of conjugate elements of order p in $\mathfrak{G}$. Furthermore, if $n<(p+3)/2$, then either (1) $\mathfrak{G}\cong LF(2, p)$, or (2) p is a Fermat prime $2^{\mu}+1>3$ and $\mathfrak{G}\cong LF(2, 2^{\mu})$. If $n\geqq(p+3)/2$, then n has the form*

$$n=F(p, u, h)=(uhp+u^2+u+h)/(u+1)$$

where u and h are positive integers.

Recently R. Brauer studied $\mathfrak{G}$ for the case $n\leqq p+2$[1] and W. F. Reynolds extended these considerations to the case $p+2<n\leqq 2p-3$[2]. Their results are as follows: If $n\leqq p+2$, then (1) $\mathfrak{G}\cong LF(2, p)$, or (2) $p=2^{\mu}\pm 1$ and $\mathfrak{G}\cong LF(2, 2^{\mu})$, or (3) $\mathfrak{G}\cong LF(3, 3)$, or (4) $\mathfrak{G}\cong\mathfrak{M}_{11}$ (Mathieu group of order 7920). If $p+2<n\leqq 2p-3$, then $2p-1$ is a prime power and $\mathfrak{G}\cong LF(2, 2p-1)$.

Our purpose is to study the general nature of $\mathfrak{G}$. In the present note we extend Reynolds' enumerations to the case $2p-3<n\leqq 2p+3$ as follows:

Theorem. *If $2p-3<n\leqq 2p+3$, $t\not\equiv 0 \pmod 2$ and $t>1$, then (1) $2p+1$ is a prime power: $2p+1=l^a\geqq 23$, where $l=3$ for $a>1$, and (2) $\mathfrak{G}\cong LF(2, l^a)$.*

---

1) This result is not published yet. Cf. Math. Rev. **14**, p. 843 (1953).

2) This was reported in [4] without proof.

We shall prove Theorem step by step. In Section **2** we examine the case $2p-3<n<2p+3$ under the condition $t\not\equiv 0 \pmod 2$ and show that such a group does not exist. In Section **3** we treat the case $n=2p+3$ under conditions $t\not\equiv 0 \pmod 2$ and $t>1$. By a theorem of Brauer ([2], Theorem 7), we can determine all the degrees of the characters of $\mathfrak{G}$ belonging to the first p-block $B_1(p)$. In Section **4** we investigate the structure of $\mathfrak{G}$. By calculating the number of elements whose order is divisible by a prime divisor of $2p+1$, we show that $2p+1$ is a prime power l^a and the index of the normalizer of an l-Sylow subgroup in $\mathfrak{G}$ is equal to l^a+1. Therefore $\mathfrak{G}$ will be represented as a doubly transitive permutation-group on l^a+1 symbols in which each element is determined uniquely by the images of three symbols. By a method of Zassenhause [5], we can prove $\mathfrak{G}\cong LF(2, l^a)$. In Section **5** we shall show that the assumptions in above Theorem can be replaced by the assumptions $n=2p+3$ and $t=(p-1)/2$. In this case $LF(2, 7)$ and $LF(2, 11)$ may exist besides above $LF(2, l^a)$.

2. The case $2p-3<n<2p+3$.

If n has the form $n=F(p, u, 3)$, then $u=1$ and $p\leqq 7$ since $n<2p+3$. For $p\leqq 7$, $F(p, x, h)=F(p, 1, 3)$ does not have the positive integral solution x for both $h=2$ and $h=1$. By a theorem of Brauer ([2], Theorem 7), the possibilities of the degrees of the characters belonging to the first p-block $B_1(p)$ are as follows:

$$1,\ p+1,\ \frac{(3p-1)}{2}p-1,\quad \left(\frac{(3p-1)}{2}p-1\right)/t.$$

By the degree-relation in $B_1(p)$, the character of degree $p+1$ must exist. Then $(p-1)/t=2$[3]. Hence the character of degree $p+2$ must exist as an exceptional one. This is impossible because $\frac{3p-1}{2}p-1\neq(p+2)(p-1)/2$.

2.1. $t\not\equiv 0 \pmod 2$ and $t>1$.

Let us assume that n does not have the form $n=F(p, u, 3)$. If n has the form $F(p, u, 1)$, then $u-4+\frac{6}{u+2}<p<u+2$ since $2p-3<n<2p+3$. For those p, n can not be integers. Therefore n must have the form $F(p, u, 2)$ only. Then, since $2p-2\leqq n\leqq 2p+2$, $u^2-u\leqq 2p\leqq u^2+3u+4$. By a theorem of Brauer [2], the possibilities of the degrees of the characters belonging to $B_1(p)$ are as follows:

$$1,\ up+1,\ \frac{n-2}{u}p-1,\quad (up+1)/t,\ \left(\frac{n-2}{u}p-1\right)/t.$$

3) O. Nagai [3], p. 230.

For the sake of simplicity we denote the character of degree z by "z".

If "$up+1$" does not exist, then $B_1(p)$ must consist of one "1", $\frac{(p-1)}{t}-1$ characters "$\frac{(n-2)}{u}p-1$" and t "$(up+1)/t$". Then by a degree-relation in $B_1(p)$, $\frac{u+1}{t}=\left(\frac{p-1}{t}-1\right)\frac{n-2}{u}$. Since $(p-1)/t>1$ and $n=F(p,\ u,\ 2)<2p+3$,

$$\frac{u+1}{t}\geqq\frac{2p+u-1}{n+1}\geqq\frac{u^2-1}{u+1}+1=u-1.$$

This contradicts $t\geqq 3$.

If "$\frac{n-2}{u}p-1$" does not exist, then $B_1(p)$ must consist of one "1", $\frac{p-1}{t}-1$ "$up+1$" and t "$\left(\frac{n-2}{u}p-1\right)/t$". Again by a theorem of Brauer,

$$u\left(\frac{p-1}{t}-1\right)=\left(\frac{n-2}{u}-1\right)/t. \quad \frac{p-1}{t}-1=\frac{2(p-1)}{tu(u+1)}.$$

Let $2p-2=aut(u+1)$. Then, since $2p\leqq u^2+3u+4$, $atu(u+1)\leqq u^2+3u+2$. $atu(u+1)\leqq u^2+3u+2$. $atu\leqq u+2$. $3u\leqq u+2$. This means $n=F(p,\ u,\ 2)=p+2$. This is a contradiction.

Therefore $B_1(p)$ must contain "$up+1$" and "$\frac{n-2}{u}p-1$". Since $\frac{n-2}{u}p-1$ divides g, $u+1\equiv 0 \pmod{t}$. We consider the following five cases:

1) $n=2p-2$. This means $2p=u^2+3u+4$. Since $up+1$ divides g, $(p-1)(2p+u+1)\equiv 0\ \ (t(u+1))$. $(u^2+4u+5)(u+2)\equiv 0 \pmod{t}$. Since $u+1\equiv 0\ (t)$, $(1-4+5)\cdot 1\equiv 0\ (t)$. This contradicts our assumption $t>2$.

2) $n=2p-1$. This means $2p=u^2+2u+3$. Let $B_1(p)$ consist of one "1", x "$\frac{n-2}{u}p-1$", $\frac{(p-1)}{t}-x-1$ "$up+1$" and t "$(up+1)/t$". Then

$$u\left(\frac{p-1}{t}-x-1\right)+\frac{u+1}{t}=(u+2)x.$$

$$2(u+1)x=\frac{u+1}{2t}\cdot(u^2+u+2)-u.$$

Since $u+1\equiv 0\ (2t)$ and $u^2+u+2\equiv 0\ (2)$, $u\equiv 0\ (2)$. This contradicts $2p=u^2+2u+3$.

Let $B_1(p)$ consist of one "1", x "$\frac{n-2}{u}p-1$", $\frac{p-1}{t}-x-1$ "$up+1$" and t "$\left(\frac{n-2}{u}p-1\right)/t$". Then

$$u\left(\frac{p-1}{t}-x-1\right)=(u+2)x+\frac{u+1}{t}.$$

$$2(u+)x=\frac{u(u+1)^2}{2t}-\frac{u+1}{t}-u.$$

Since $u+1\equiv 0\ (2t)$, $u\equiv 2\ (2)$. This also contradicts $2p=u^2+2u+3$.

3) $n=2p$. This means $2p=u^2+u+2$. Since $up+1$ divides g, $(2p+u+1)(p-1)\equiv 0 \pmod{t(u+1)}$. $(u^2+2u+3)u\equiv 0\ (t)$. Since $u+1\equiv 0\ (t)$, $(1-2+3)\cdot(-1)\equiv 0\ (t)$. This contradicts $t>2$.

4) $n=2p+1$. This means $2p=u^2+1$. Since $up+1$ divides g, $(p-1)(2p+u+1)\equiv 0 \pmod{t(u+1)}$. $(u-1)(u^2+u+2)\equiv 0\ (2t)$. Since $u+1\equiv 0\ (t)$, $(-2)\cdot(1-1+2)\equiv 0\ (t)$. This contradicts $t>2$.

5) $n=2p+2$. This means $2p=u^2-u$. Since $up+1$ divides g, $(u-1)(u^2+1)\equiv 0 \pmod{2t}$. Since $u+1\equiv 0\ (t)$, $(-2)\cdot(1+1)\equiv 0\ (2t)$. This contradicts $t>2$.

2. 2. $t=1$.

As above n have the form $F(p, u, 2)$ only. Therefore the possibilities of degrees of the characters belonging to $B_1(p)$ are as follows:

$$1,\ up+1,\ \frac{n-2}{u}p-1, \quad \text{where} \quad u^2-u\leqq 2p\leqq u^2+3u+4\,.$$

Let $B_1(p)$ contain x characters of degree $\frac{n-2}{u}p-1$. Then $B_1(p)$ contains $p-x-1$ "$up+1$" since, for $t=1$, $B_1(p)$ contains just p characters. We examine the following five cases separately:

1) $n=2p-2$. This means $2p=u^2+3u+4$. Then $\frac{n-2}{u}p-1=\frac{2p-4}{u}p-1=(u+3)p-1$. By the degree-relation in $B_1(p)$,

$$u(p-1-x)+1=(u+3)x.$$
$$u(p-1)+1=x(2u+3).$$
$$u(2p-2)+2=2x(2u+3).$$
$$u(u^2+3u+2)+2=2(2u+3)x.$$
$$u^3+3u^2+2u+2=2(2u+3)x.$$
$$19\equiv 0\ (2u+3).$$
$$19=2u+3.\quad 2u=16.\quad u=8.\quad 2p=64+32+4=100.$$

50 is not a prime.

2) $n=2p-1$. This means $2p=u^2+2u+3$. Then $\frac{n-2}{u}p-1=\frac{2p-3}{u}up-1=(u-2)p-1$.

By the degree-relation in $B_1(p)$, we have

$$u(p-1-x)+1=(u+2)x.$$
$$u(p-1)+1=x(2u+2).$$
$$u(2p-2)+2=4x(u+1).\quad u(u^2+2u+1)+2=4x(u+1).$$

$$u^3+2u^2+u+2=4x(u+1).$$
$$-1+2-1+2\equiv 0\ (u+1).\quad 2\equiv 0\ (u+1).\quad u=1.\quad 6=8x.$$

Such an x can not be an integer.

3) $n=2p$. This means $2p=u^2+u+2$. Then $\frac{n-2}{u}p-1=(u+1)p-1$. By the degree-relation,

$$u(p-1-x)+1=(u+1)x.$$
$$u(p-1)+1=(2u+1)x.$$
$$u(2p-2)+2=2x(2u+1).$$
$$u(u^2+u)+2=2x(2u+1).$$
$$u^3+u+2=2x(2u+1).$$
$$17\equiv 0\ (2u+1).$$
$$17=2u+1.\quad u=8.\quad p=37\quad \text{and}\quad x=17.$$

Therefore $B_1(p)$ must consist of one "1", 19 "$8\cdot 37+1$" and 17 "$9\cdot 37-1$". But $8\cdot 37+1$ does not divide $g=2739$.

4) $n=2p+1$. This means $2p=u^2+1$. Then $\frac{n-2}{u}p-1=up-1$. By the degree-relation,

$$u(p-1-x)+1=ux$$
$$u(p-1)+1=2ux.$$
$$u(2p-2)+2=4ux.$$
$$u(u^2-1)+2=4ux.$$
$$u^3-u+2=4ux.$$
$$2\equiv 0\ (u).\quad u=2.\quad 2p=5.$$

5) $n=2p+2$. This means $2p=u^2-u$. Then $\frac{n-2}{u}p-1=(u-1)p-1$. By the degree-relation,

$$u(p-1-x)+1=x(u-1)$$
$$u(p-1)+1=x(2u-1)$$
$$u(2p-2)+2=2x(2u-1)$$
$$u(u^2-u-2)+2=2x(2u-1)$$
$$u^3-u^2-2u+2=2x(2u-1).$$
$$7\equiv 0\ (2u-1).\quad u=4.\quad 2p=12.$$

Consequently, we obtain the following

Proposition. *If t is odd, then such group $\mathfrak{G}$ does not exist for* $2p-3<n<2p+3$.

3. The case $n=2p+3$, $t\not\equiv 0 \pmod 2$ and $t>1$.

In this case n may have the forms $n=F(p, 1, 4)=F(p, 2, 3)=F(p, u, 2)$. Then $2p=u^2-2u-1$. Therefore the possibilities of degrees of characters belonging to $B_1(p)$ are as follows: 1, $p+1$, $2p+1$, $up+1$, p^2-1, $\frac{n-2}{u}p-1=(u-2)p-1$, $(up+1)/t$, $(2p+1)/t$, $(p^2-1)/t$, $((u-2)p-1)/t$.

We shall sieve these one by one.

If "$p+1$" exists, then $(p-1)/t=2$. Hence the exceptional character must be of degree $p+2$. This is impossible. If "p^2-1" exists, then $tp^2\leqq np-n+1=2p^2+p-2$. $p^2-p+2\leqq 0$. So we can omit "p^2-1". Since $B_1(p)$ contains only one exceptional family, it is sufficient to be considered the following four cases:

1) "$((u-2)p-1)/t$" exists. If "$(u-2)p-1$" exists, then its degree must divide g. So $(u+1)(u-1)(u-2)\equiv 0\ (2t)$. This contradicts $u\equiv 3\ (t)$. Thus $B_1(p)$ consists of one "1", $\frac{p-1}{t}-x-1$ "$2p-1$", x "$up+1$" and t "$((u-2)p-1)/t$". Then

$$
\begin{aligned}
ux+2\left(\frac{p-1}{t}-x-1\right) &= \frac{u-3}{t} \\
x(u-2)t &= (u-1-2p)+2t\,. \\
x(u-2)t &= -u(u-3)+2t\quad.
\end{aligned}
$$

This is a contradiction.

2) "$(p^2-1)/t$" exists. If "$(u-2)p-1$" exists, then $(u+1)(u-1)(u-2)\equiv 0\ (2t)$. Since $p-1=(u+1)(u-3)/2$ is divisible by t, we can set $t=t_1\cdot t_2$ such that $u+1\equiv 0\ (t_1)$, $u-3\equiv 0\ (t_2)$. $4\cdot 2\cdot 1\equiv 0\ (t_2)$. This means $t_2=1$ and $u+1\equiv 0\ (t)$. In this case "$up+1$" does not exist since $(u-3)u(u-1)\equiv 0\ (2t)$. Hence we can assume that $B_1(p)$ consists of one "1", $\frac{(p-1)}{t}-x-1$ "$2p+1$", x "$(u-2)p-1$" and t "$(p-1)/t$". Then

$$
\begin{aligned}
&2((p-1)/t-x-1 = (u-2)x+(p-1)/t. \\
&(p-1)/t-2 = ux\,. \\
&p-1 = t\ \ (ux+2)\,. \\
&(u+1)(u-3) = 2t(ux+2)\,. \\
&-3\equiv 4t(u)\,.
\end{aligned}
$$

Let $4t+3=au$ and $u+1=2kt$. Then we have $4t+3=2akt-a$. $2t(ak-2)=a+3$. $6(ak-2)\geqq a+3$. $a(6k-1)\leqq 15$. Hence we have $k=2$, $a=1$ or $k=1$, $a=3$. Neither of them gives an integral solution x.

If "$(u-2)p-1$" does not exist, then $B_1(p)$ consists of one "1",

$\frac{p-1}{t}-x-1$ "$2p+1$", x "$up+1$" and t "$(p-1)/t$". We have $ux+2\left(\frac{p-1}{t}-x-1\right)=\frac{p-1}{t}$. $x(u-2)=2-(p-1)/t$. This means $x=0$ and $p-1=2t$. Hence in this case $B_1(p)$ consists of one "1", one "$2p+1$" and $(p-1)/2$ "$2(p+1)$". We shall discuss this case in **4.**

3) "$(2p+1)/t$" exists. This means $t=3$.

If "$(u-2)p-1$" does not exist, then $B_1(p)$ must consist of one "1", $\frac{p-1}{3}-x-1$ "$2p+1$", x "$up+1$" and 3 "$(2p+1)/3$". Then we have

$$2\left(\frac{p-1}{3}-x-1\right)+ux=1\,.$$
$$3x(u-2)+2p-11=0\,.$$

This can not hold since $2p=u^2-2u-1$.

If "$(u-2)p-1$" exists, then we can assume $B_1(p)$ consists of one "1" $\frac{p-1}{3}\cdot x-1$ "$2p-1$" x "$(u-2)p-1$" and 3 "$(2p+1)/t$". Then we have

$$2\left(\frac{p-1}{3}-x-1\right)=ux-2x+1\,.$$
$$2p-2=3(ux+3)\,.$$
$$u^2-2u-3=3ux+9\,.$$
$$12\equiv 0\ \ (u)\,.$$

Since u is odd, u must be equal to 3. This contradicts $2p=u^2-2u-1$.

4) $c=(up+1)/t$. In this case "$up+1$" does not exist, as in **2.1.** 1), since $u+1\equiv 0\ \ (t)$. $B_1(p)$ consists of one "1", $\frac{p-1}{t}-x-1$ "$2p+1$", x "$(u-2)p-1$" and t "$(up+1)/t$". Then

$$2\left(\frac{p-1}{t}-x-1\right)=ux-2x+\frac{u+1}{t}\,.$$
$$2p-3-2t=uxt\,.$$
$$(u+1)(u-4)=(ux+2)t\,.$$

As u is odd, we can put $t+2=au$ and $u+1=2kt$. Then $t+2=2akt-a$. $(2ak-1)t=a+2$, $3(2ak-1)\leqq a+2$. $a(6k-1)\leqq 5$. Hence we have $u=1$, $k=1$. This does not give an integral solution x.

4. Continuation: The case $n=2p+3$ and $B_1(p)$ consists of one character A_1 of degree 1, one character A_2 of degree $2p+1$ and

t $(=(p-1)/2)$ p-conjugate characters $C^{(\lambda)}$ of degree $(p-1)/t$ $(=2(p+1))$. In this case the order of $\mathfrak{G}$ is expressed as $g=p(p-1)(1+np)/t$ $=2p(2p+1)(p+1)$. Since $(2p+1,\ 2p+2)=1$, the character A_2 is of highest kind for any prime l dividing $2p+1$. Hence $A_2(L)=0$ for elements L of $\mathfrak{G}$ whose order divisible by l. For the prime m dividing $2p+2$, the character $C^{(\lambda)}$ is of highest kind. Hence $C^{(\lambda)}(M)=0$ for elements M of $\mathfrak{G}$ whose order divisible by m. Of course such elements L and M are p-regular by the condition (*). Therefore $A_1(G)+A_2(G)$ $=C^{(\lambda)}(G)$ holds for $G=L$ and $G=M$. Thus $A_2(M)=-1$, $C^{(\lambda)}(L)=1$. From above relation, there is no such element G which is L and M at the same time. Therefore the elements of $\mathfrak{G}$ are distributed into four disjoint sets: (I) The unit element, (II) the elements of order p, (III) the elements of type L whose order is divisible by at least one prime factor l of $2p+1$, (IV) the elements of type M whose order is divisible by at least one prime factor m of $2p+2$.

Let r denote the number of elements of type L in $\mathfrak{G}$. Then by the well-known character-relations,

$$\sum_G C^{(1)}(G)+\sum C^{(2)}(G)+\cdots+\sum C^{(t)}(G)=0\,.$$

By the relation $A_1(G)+A_2(G)=C^{(\lambda)}(G)$ for p-regular G, we have $C^{(\lambda)}(1)$ $=2(p+1)$, $C^{(\lambda)}(L)=1$, $C^{(\lambda)}(M)=0$ and $\sum_\nu C^{(\lambda)}(G)=-1$. From these, it follows

$$\begin{aligned}&(p-1)(p+1)+(-1)(p-1)(2p+1)(p+1)+r\cdot(p-1)/2=0\,.\\&r=4p(p+1)\,.\end{aligned}$$

For any element L^* whose order divides $2p+1$, let us denote the normaliser of L^* in $\mathfrak{G}$ by $\mathfrak{N}(L^*)$ and its order by $n(L^*)$. If $\mathfrak{N}(L^*)$ contains an element M^* of type M, then there exists such an element L^*M^* of type L and of type M at the same time. Of course $n(L^*)$ does not contain the prime p. Hence $n(L^*)$ must contain the factors of $2p+1$ only. If $n(L^*)<2p+1$, then $n(L^*)\leqq(2p+1)/3$. Therefore the number of elements conjugate to L^* is greater than $4p(p+1)$. But $g/n(L^*)\leqq r$. This is a contradiction. Therefore we have $n(L^*)=2p+1$. This means that the number of elements in the conjugate class containing L^* is equal to $2p(p+1)$. If $2p+1$ is divisible by a prime l' different from l, then the element of order $l'l$ must exist. Therefore $r\geqq2p(p+1)+2p(p+1)$ $+2p(p+1)$. This is a contradiction.

Therefore $2p+1$ must be a prime power: $2p+1=l^a$. For $p=7$, $2p+1$ is not a prime power. For $p<7$, we have $t\equiv0$ (2) or $t=1$. Therefore we can assume $p\geqq11$, that is, $2p+1=l^a\geqq23$. For its exponent $a>1$, such l must be equal to 3, because $2p=(l-1)\ (l^{a-1}+\cdots+l+1)$. Denote the normaliser of an l-Sylow group $\mathfrak{L}$ by $\mathfrak{N}(\mathfrak{L})$ and its order by $n(\mathfrak{L})$. By a theorem of Sylow, $g/n(\mathfrak{L})\equiv 1 \pmod{l}$. Let $g/n(\mathfrak{L})=1+lx$. Of course $\mathfrak{G}$ is represented as a transitive permutation-group of degree $1+lx$. Denote this character by Π. We decompose Π into the irreducible characters of $\mathfrak{G}$. As is well known Π contains A_1 exactly once.

The following three cases must be considered.

1) Π contains $C^{(\lambda)}$. Then all p-conjugate $C^{(\lambda)}$ must be contained in Π, since $\Pi(G)$ is integral. Therefore $1+lx\geqq 1+(l^a+1)(l^a-3)/4=(l^a-1)^2/4$. Hence $n(\mathfrak{L})\leqq 2l^a+4+\frac{4}{l^a-1}$. Since $n(\mathfrak{L})\equiv 0\ (l^a)$ and $l^a\geqq 23$, $n(\mathfrak{L})$ is either l^a or $2l^a$. If $n(\mathfrak{L})=l^a$, then $\mathfrak{G}$ must have an l-Sylow complement[4]. Therefore the commutator-subgroup $\mathfrak{G}'$ does not coincide with $\mathfrak{G}$, contrary to (**). Hence $n(\mathfrak{L})=2l^a$. So $(1+lx)2l^a=l^a(l^a+1)(l^a-1)/2$. $4(1+lx)=(l^a-1)(l^a+1)$. Thus $5\equiv 0 \pmod{l}$. This is a contradiction.

2) Π contains only the characters of highest kind for p besides A_1. Then we have $1+lx\geqq 1+(l^a-1)/2=(l^a+1)/2$. Hence $n(\mathfrak{L})\leqq(l^a-1)l^a$. Since $1+lx\equiv 0\ ((l^a-1)/2)$, $n(\mathfrak{L})\equiv 0\ ((l^a-1)/2)$. Therefore $n(\mathfrak{L})$ is either $(l^a-1)l^a/2$ or $(l^a-1)l^a$. If $n(\mathfrak{L})=(l^a-1)l^a/2$, then $1+lx=1+l^a$ is not congruent modulo $(l^a-1)/2$. If $n(\mathfrak{L})=(l^a-1)l^a$, then $1+lx=(1+l^a)/2\not\equiv 1$ (mol l).

3) Therefore Π must contain character A_2. Since $\Pi(P)\geqq A_1(P)+A_2(P)>1$ for p-singular element P, there exists an element P^* belonging to a conjugate of $\mathfrak{N}(\mathfrak{L})$. This means $n(L)\equiv 0\ ((l^a-1)l^a/2)$. Hence $1+lx\leqq 1+l^a$. Thus we can conclude that index of $\mathfrak{N}(\mathfrak{L})$ in $\mathfrak{G}$ is equal to $1+l^a$ and $\Pi(G)=A_1(G)+A_2(G)$. Therefore $\Pi(1)=1+l^a$, $\Pi(P^i)=2$, $\Pi(L)=1$ and $\Pi(M)=0$. However, $\Pi(G)$ equals the number of letters not altered by the permutation-representation of $\mathfrak{G}$. Since $\Pi(G)=1+l^a$ only for $G=1$, we have a $(1-1)$ representation. From the above facts, $\mathfrak{G}$ is a doubly transitive permutation group on $1+l^a$ letters in which each element is determined uniquely by the images of three letters. Therefore by the method of Zassenhaus we can construct "almost-field" (Fastkörper) F corresponding to $\mathfrak{N}(\mathfrak{L})$ and its multiplier M corresponding to a p-Sylow subgroup. Since M is an abelian group of order $(l^a-1)/2$, F is considered as a "Teilfastköper" of Galois field $GF(l^a)$. In our case the order of M is not even, but it is prime. Therefore we can use the method of Zassenhaus [5]. Thus we have proved $\mathfrak{G}\cong LF(2, l^a)$.

---

4) Cf. H. Wielandt [6].

5. Remark

The conditions in our Theorem can be replaced by the conditions $n=2p+3$, $t=(p-1)/2$.

Theorem. *If $n=2p+3$ and $t=(p-1)/2$, then $2p+1$ is a prime power and $\mathfrak{G}\cong LF(2, 2p+1)$ including $LF(2, 7)$ and $LF(2, 11)$.*

Proof. Since, as in **3**, $n=2p+3$, the possibilities of degrees of of characters belonging to $B_1(p)$ are as follows:

1, $p+1$, $2p+1$, $up+1$, p^2-1, $\frac{n-2}{u}p-1=(u+2)p-1$, $p-1$, $(up+1)/t$, $(2p+1)/t$, $(p+1)/t$, $(p-1)/t$, $(p^2-1)/t$, $((u+2)p-1)/t$, where $2p=u^2-2u-1$.

Let $t=1$, then $p=3$. In this case n does not have the form $n=F(3, u, 2)$. Therefore $B_1(3)$ must consist of one "1", one "$2p+1$" and one "p^2-1". Since this is a special case in **4**, we have $\mathfrak{G}\cong LF(2, 7)$. But this group does not appear in former Theorem.

Let $t>1$. If "$(up+1)/t$" exists, then $u+1\equiv 0 \pmod{t}$. Since $2p=u^2-2u-1$, $2(p-1)=(u-3)(u+1)$. $(p-1)/2=(u-3)(u+1)/4=\frac{u-3}{4}(u+1)$. This means $\frac{u-3}{4}\leqq 1$. We have $u=5$ and $u=7$. For $u=5$, $p=7$ and $(up+1)/t=12$. Therefore $B_1(7)$ must contain "13". But this can not divide $g=1736$. For $u=7$, $p=17$ and $(up+1)/t=15$. Therefore $B_1(17)$ must contain "16". But this can not divide $g=17\cdot 2\cdot 35\cdot 18$.

If "$(2p+1)/t$" exists, then $3\equiv 0 \pmod{t}$. As $t>1$, $t=3$ and $p=7$. $B_1(7)$ must contain the character of degree x satisfying $1+(2\cdot 7+1)/3=x$. $x=6=p-1$. This means $t\equiv 0 \pmod 2$.

If "$(p+1)/t$" exists, then $2\equiv 0 \pmod{t}$. As $t>1$, $t=2$ and $p=5$. Since $(p+1)/t<(2p+1)/t$, by a theorem of Tuan ([5], Theorem 4) $\mathfrak{G}\cong LF(2, p)$. This contradicts $n=2p+3$.

If "$(p-1)/t$" exists, then $\mathfrak{G}\cong LF(2, p)$. This contradicts $n=2p+3$ too.

If "$((u+2)p-1)/t$" exists, then $u+1\equiv 0 \pmod{t}$. Since $2p=u^2-2u-1$, $2p-2=(u-3)(u+1)$. $u+1=\frac{4}{u-3}\frac{p-1}{2}$. $4\geqq u-3$. We have $u=5$ and $u=7$. For $u=5$, $p=7$ and $((u+2)p-1)/t=15$. Therefore $B_1(7)$ must contain "14". But this can not be $xp+1$. For $u=7$, $p=17$. $((u+2)p-1)/t=19$ does not divide $g=17\cdot 2\cdot 35\cdot 18$.

If "$(p^2-1)/t$" exists, then $B_1(p)$ must consist of one "1", one "$2p+1$" and t "$(p^2-1)/t$". Since $(p^2-1)/t=2p+2$, the proof in **4** is valid in this case. Thus we can conclude that $2p+1$ is a prime power and $\mathfrak{G}\cong LF(2, 2p+1)$.

This completes the proof of Theorem.

(Received April 11, 1956)

Bibliography

[1] R. Brauer: On groups whose order contains a prime number to the first power, Amer. J. Math. **54,** part I, 401–420, part II, 421–440 (1942).

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

[3] O. Nagai: Supplement to "Note on Brauer's Theorem of Simple Groups", Osaka Math. J. **5,** 227–232 (1953).

[4] W. F. Reynolds: On finite groups related to permutation groups of prime degree, Bull. Amer. Math. Soc. **61** (1955).

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

[6] H. Wielandt: p-Sylowgruppen und p-Faktorgruppen, Crelle J. 182 (1940).

[7] H. Zassenhaus: Kennzeichnung endlicher linearer Gruppen als Permutations gruppen, Abh. Math. Sem. Univ. Hamburg **11** (1936).