<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>On simple groups related to permutation-groups of prime degree. I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Nagai, Osamu</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Mathematical Journal. 8(1) P.107-P.117</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1956-06</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/12443">https://doi.org/10.18910/12443</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/12443</td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
</tbody>
</table>

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/repo/ouka/all/

Osaka University
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 \( g = p(p-1) \frac{1 + np}{t} \) 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 \( n < \frac{(p+3)}{2} \), then either (1) \( \mathfrak{G} \cong LF(2, p) \), or (2) \( p \) is a Fermat prime \( 2^n + 1 \geq 3 \) and \( \mathfrak{G} \cong LF(2, 2^n) \). If \( n \geq \frac{(p+3)}{2} \), then \( n \) has the form

\( n = F(p, u, h) = (u + w^2 + u + h) / (u + 1) \)

where \( u \) and \( h \) are positive integers.

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

**Theorem.** If \( 2p - 3 < n \leq 2p + 3 \), \( t \equiv 0 \pmod{2} \) and \( t > 1 \), then (1) \( 2p + 1 \) is a prime power: \( 2p + 1 = l^a \geq 23 \), where \( l = 3 \) for \( a > 1 \), and (2) \( \mathfrak{G} \cong LF(2, l^a) \).

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 $t \equiv 0 \pmod{2}$ and show that such a group does not exist. In Section 3 we treat the case $n = 2p+3$ under conditions $t \equiv 0 \pmod{2}$ 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 $B_{\lambda}(p)$. 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 $l^w$ and the index of the normalizer of an $l$-Sylow subgroup in $\mathfrak{G}$ is equal to $l^w+1$. Therefore $\mathfrak{G}$ will be represented as a doubly transitive permutation-group on $l^w+1$ symbols in which each element is determined uniquely by the images of three symbols. By a method of Zassenhause [5], we can prove $\mathfrak{G} \simeq LF(2, l^w)$. 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 $LF(2, l^w)$.

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

If $n$ has the form $n = F(p, u, 3)$, then $u = 1$ and $p \leq 7$ since $n < 2p+3$. For $p \leq 7$, $F(p, x, h) = F(p, 1, 3)$ 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 $B_{\lambda}(p)$ are as follows:

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

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

2.1. $t \equiv 0 \pmod{2}$ 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 $2p-2 \leq n \leq 2p+2$, $u^2 - u \leq 2p \leq u^2 + 3u + 4$. By a theorem of Brauer [2], the possibilities of the degrees of the characters belonging to $B_{\lambda}(p)$ are as follows:

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

3) O. Nagai [3], p. 230.
For the sake of simplicity we denote the character of degree \( z \) by \( "z" \).

If \( \frac{u}{t}p+1 \) does not exist, then \( B_1(\phi) \) 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 \( B_1(\phi) \),

\[
\frac{u+1}{t} = \left(\frac{p-1}{t} - 1\right) \frac{n-2}{u}.
\]

Since \( (p-1)/t \geq 1 \) and \( n = F(p, u, 2) < 2p + 3 \),

\[
\frac{u+1}{t} \geq \frac{2p+u-1}{n+1} \geq \frac{u^2-1}{u+1} + 1 = u-1.
\]

This contradicts \( t \geq 3 \).

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

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

Let \( 2p-2 = \text{aut}(u+1) \). Then, since \( 2p \leq u^2 + 3u + 4 \), \( \text{aut}(u+1) \leq u^2 + 3u + 2 \).

\( auu(u+1) \leq u^2 + 3u + 2 \). \( auu \leq u + 2 \). This means \( n = F(p, u, 2) = p + 2 \). This is a contradiction.

Therefore \( B_1(\phi) \) must contain \( "up+1" \) and \( "n-2/p-1" \). 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 \( g \), \( (p-1)(2p+u+1) \equiv 0 \pmod{t} \). \( (u^2 + 4u + 5)(u+2) \equiv 0 \pmod{t} \). Since \( u+1 \equiv 0 \pmod{t} \), \((1-4+5) \cdot 1 \equiv 0 \pmod{t} \). This contradicts our assumption \( t \geq 2 \).

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

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

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

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

Let \( B_1(\phi) \) consist of one \( "1", x \ "(n-2)/u/p-1" \), \( (p-1)/t \) - 1 \( "up+1" \) and \( t\ "(n-2)/u/p-1" \). Then

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

\[
2(u+1) = \frac{u(u+1)^2}{2t} - \frac{u+1}{t} - u.
\]
Since \( u + 1 = 0 \) \((2t)\), \( u = 2 \) \((2)\). This also contradicts \( 2p = u^2 + 2u + 3 \).

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

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

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 \( u + 1 \equiv 0 \pmod{t} \), \((-2)(1 + 1) \equiv 0 \pmod{2t} \). This contradicts \( t \geq 2 \).

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 \( B_i(p) \) are as follows:

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

Let \( B_i(p) \) contain \( x \) characters of degree \( \frac{n - 2}{u} p - 1 \). Then \( B_i(p) \) contains \( p - x - 1 \) \( "up + 1" \) since, for \( t = 1 \), \( B_i(p) \) 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 \( B_i(p) \),

\[
\begin{align*}
&u(p - 1 - x) + 1 = (u + 3)x . \\
&u(p - 1) + 1 = x(2u + 3) . \\
&u(2p - 2) + 2 = 2x(u + 3) . \\
&u(u^2 + 3u + 2) + 2 = 2(2u + 3)x . \\
&u^2 + 3u + 2u + 2 = 2(2u + 3)x . \\
&19 \equiv 0 \pmod{2u + 3} . \\
&19 = 2u + 3 . \\
&2u = 16 . \\
&u = 8 . \\
&2p = 64 + 32 + 4 = 100 .
\end{align*}
\]

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 \( B_i(p) \), we have

\[
\begin{align*}
&u(p - 1 - x) + 1 = (u + 2)x . \\
&u(p - 1) + 1 = x(2u + 2) . \\
&u(2p - 2) + 2 = 4x(u + 1) . \\
&u(u^2 + 2u + 1) + 2 = 4x(u + 1) .
\end{align*}
\]
Such an $x$ cannot 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,

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

Therefore $B,(p)$ must consist of one “1”, 19 “8·37+1” and 17 “9·37-1”. But 8·37+1 does not divide $g = 2739$.

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

By the degree-relation,

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

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,

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

Consequently, we obtain the following

**Proposition.** *If $t$ is odd, then such group $\mathcal{G}$ does not exist for $2p-3 < n < 2p+3$.***
3. The case \( n=2p+3, \) \( t \equiv 0 \pmod{2} \) 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 \( B_p(p) \) are as follows: \( 1, p+1, 2p+1, up+1, p^2-1, \) \( n \) \( \underbrace{u \cdots u}_{2} \) \( p-1=(u-2)p-1, (up+1)/t, (2p+1)/t, (p^2-1)/t, ((u-2)p-1)/t. \)

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 \( tp^2 \le n(p-n+1)=2p^2-p-2. \) \( p^2-p+2 \le 0. \) So we can omit \( "p^2-1". \) Since \( B_p(p) \) 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 \( (u+1)(u-1)(u-2) \equiv 0 \pmod{2}. \) This contradicts \( u \equiv 3 \pmod{t}. \) Thus \( B_p(p) \) consists of one \( "1", \) \( \frac{p-1}{t} - x - 1 "2p+1", x "up+1" \) and \( t "((u-2)p-1)/t". \) Then

\[
ux + 2 \left( \frac{p-1}{t} - x - 1 \right) = \frac{u-3}{t} \\
x(u-2)t = (u-1-2p)+2t \\
x(u-2)t = -u(u-3)+2t.
\]

This is a contradiction.

2) \( "(p^2-1)/t" \) exists. If \( "(u-2)p-1" \) exists, then \( (u+1)(u-1)(u-2) \equiv 0 \pmod{2}. \) Since \( p-1=(u+1)(u-3)/2 \) is divisible by \( t, \) we can set \( t=t_1t_2 \) such that \( u+1 \equiv 0 \pmod{t_1}, u-3 \equiv 0 \pmod{t_2}. \) \( 4 \cdot 2 \cdot 1 \equiv 0 \pmod{t_2}. \) This means \( t_1=1 \) and \( u+1 \equiv 0 \pmod{t_2}. \) In this case \( "up+1" \) does not exist since \( (u-3)(u-1) \equiv 0 \pmod{2}. \) Hence we can assume that \( B_p(p) \) consists of one \( "1", \) \( \frac{p-1}{t} - x - 1 "2p+1", x "(u-2)p-1" \) and \( t "(p-1)/t". \) Then

\[
2((p-1)/t-x-1 = (u-2)x+(p-1)/t. \\
(p-1)/t-2 = ux. \\
p-1 = t \ (ux+2). \\
(u+1)(u-3) = 2t(ux+2) . \\
-3 \equiv 4t(u).
\]

Let \( 4t+3 = au \) and \( u+1 = 2kt. \) Then we have \( 4t+3 = 2akt-a. \) \( 2t(ak-2) = a+3. \) \( 6(ak-2) \ge a+3. \) \( a(6k-1) \le 15. \) 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 \( B_p(p) \) consists of one \( "1", \)
On Simple Groups Related to Permutation-Groups of Prime Degree I

We have \[ u(x-2) = \frac{1}{t} (p-1) / t \]. This means \( x = 0 \) and \( p - 1 = 2t \). Hence in this case \( B_i(p) \) 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 \( B_i(p) \) must consist of one "1", \( \frac{p-1}{3} x-1 "2p+1", x "up+1" and 3 "(2p+1)/3". Then we have

\[
2\left(\frac{p-1}{3} - x - 1\right) + ux = 1.
\]

This can not hold since \( 2p = u^2 - 2u - 1 \).

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

\[
2\left(\frac{p-1}{3} - x - 1\right) = ux - 2x + 1.
\]

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). \( B_i(p) \) consists of one "1", \( \frac{p-1}{t} x-1 "2p+1", x "(u-2)p-1" and t "(up+1)/t". Then

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

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

4. Continuation: The case \( n = 2p+3 \) and \( B_i(p) \) consists of one character \( A_i \) of degree 1, one character \( A_z \) of degree 2p+1 and
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 $A_S$ is of highest kind for any prime $l$ dividing $2p+1$. Hence $A_S(L) = 0$ 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,

$$\sum C^{(\lambda)}(G) + \sum C^{(\lambda)}(G) + \cdots + \sum C^{(\lambda)}(G) = 0.$$ 

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

$$(p-1)(p+1) + (-1)(p-1)(2p+1)(p+1) + r \cdot (p-1)/2 = 0.$$ 

$$r = 4p(p+1).$$

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 $n(L^*) \leq (2p+1)/3$. Therefore the number of elements conjugate to $L^*$ is greater than $4p(p+1)$. But $g/n(L^*) \leq r$. 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 $r \geq 2p(p+1) + 2s(p+1) + 2p(p+1)$. 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 $t=0$ (2) or $t=1$. Therefore we can assume $p \geq 11$, that is, $2p+1 = l^a \geq 23$. For its ex-
ponent \(a \geq 1\), such \(l\) must be equal to 3, because \(2p = (l - 1) \cdot (l^{a-1} + \cdots + 1)\). Denote the normaliser of an \(l\)-Sylow group \(\mathfrak{S}\) by \(\mathfrak{R}(\mathfrak{S})\) and its order by \(n(\mathfrak{S})\). By a theorem of Sylow, \(g/n(\mathfrak{S}) = 1 \pmod{h}\). Let \(g/n(\mathfrak{S}) = 1 + lx\). Of course \(\mathfrak{S}\) is represented as a transitive permutation-group of degree \(1 + lx\). Denote this character by \(\Pi\). We decompose \(\Pi\) into the irreducible characters of \(\mathfrak{S}\). As is well known \(\Pi\) contains \(A_1\) exactly once.

The following three cases must be considered.

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

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

3) Therefore \(\Pi\) must contain character \(A_2\). Since \(\Pi(P) \geq A_1(P) + A_2(P) > 1\) for \(p\)-singular element \(P\), there exists an element \(P^*\) belonging to a conjugate of \(\mathfrak{R}(\mathfrak{S})\). This means \(n(L) = 0 ((l^a - 1)l^a/2)\). Hence \(1 + lx \leq 1 + l^a\). Thus we can conclude that index of \(\mathfrak{R}(\mathfrak{S})\) in \(\mathfrak{S}\) is equal to \(1 + l^a\) and \(\Pi(G) = A_1(G) + A_2(G)\). Therefore \(\Pi(1) = 1 + l^a\), \(\Pi(P) = 2\), \(\Pi(L) = 1\) and \(\Pi(M) = 0\). However, \(\Pi(G)\) equals the number of letters not altered by the permutation-representation of \(\mathfrak{S}\). Since \(\Pi(G) = 1 + l^a\) only for \(G = 1\), we have a \((1 - 1)\) representation. From the above facts, \(\mathfrak{S}\) 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 \(\mathfrak{R}(\mathfrak{S})\) 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 "Teilfastkörper" 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 \(\mathfrak{S} \cong LF(2, l^a)\).

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 \( \mathfrak{S} \cong LF(2, 2p + 1) \) including \( LF(2, 7) \) and \( LF(2, 11) \).

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

1. \( p + 1 \), \( 2p + 1 \), \( up + 1 \), \( p^2 - 1 \), \( \frac{n - 2}{u} p - 1 \), \( p - 1 \), \( (up + 1)/t \), 
2. \( (2p + 1)/t \), \( (p + 1)/t \), \( (p - 1)/t \), \( (p^2 - 1)/t \), \( (up + 1)/t - 1 \), \( (u + 2)p - 1)/t \), 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 \( \mathfrak{S} \cong LF(2, 7) \). 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 \( 2p = u^2 - 2u - 1 \), \( 2(p - 1) = (u - 3)(u + 1) \). \( (p - 1)/2 = (u - 3)(u + 1)/4 = \frac{u^2 - 3}{4}(u + 1) \). This means \( \frac{u^2 - 3}{4} \leq 1 \). 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 cannot divide \( g = 1736 \). For \( u = 7 \), \( p = 17 \) and \( (up + 1)/t = 15 \). Therefore \( B_1(17) \) must contain “16”. But this cannot 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 \( 1 + (2 \cdot 7 + 1)/3 = x \).

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) \( \mathfrak{S} \cong LF(2, p) \). This contradicts \( n = 2p + 3 \).

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

If “\( (u + 2)p - 1)/t \)” exists, then \( u + 1 \equiv 0 \pmod{t} \). Since \( 2p = u^2 - 2u - 1 \), \( 2p - 2 = (u - 3)(u + 1) \). \( u + 1 = \frac{4}{u - 3} - 1 \). \( 4 \geq u - 3 \). 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 cannot 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 \( \mathfrak{S} \cong LF(2, 2p + 1) \).

This completes the proof of Theorem.

(Received April 11, 1956)
Bibliography


