<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Supplement to note on Brauer’s theorem of simple groups. II</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. 11(2) P.147–P.152</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1959</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/10.18910/8620">https://doi.org/10.18910/8620</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/8620</td>
</tr>
<tr>
<td><strong>rights</strong></td>
<td></td>
</tr>
</tbody>
</table>
Supplement to Note on Brauer's Theorem of Simple Groups. II

By Osamu NAGAI

The aim of this note is to complete the proof of the following theorem:

Let $G$ be a finite group which contains an element $P$ of prime order $p$ which commutes only with its own powers (condition (*)) and assume that $G$ is equal to its commutator-subgroup $G'$ (condition (**)). Then the order $g$ of $G$ is expressed as $g=p(p-1)(1+np)/t$, where $1+np$ is the number of conjugate subgroups of order $p$ and $t$ is the number of classes of conjugate elements of order $p$. If $n \leq p+2$ and $t \equiv 0 \pmod{2}$, then $p$ is of the form $2^k-1$ and $G \cong LF(2, 2^k)$.

In [3], the theorem was proved for the case $n=p+2$ and $t \equiv 0 \pmod{2}$: If $n \leq p+2$ and $t \equiv 0 \pmod{2}$, under (*), then $p$ is of the form $2^k-1$ and $G \cong LF(2, 2^k)$. In [4], the case $n=p+2$ and $t \equiv 0 \pmod{2}$ are discussed, but the equation in p. 230, line 6 is not correct. So the representation of degree $p+1$ may occur. Therefore, in this note, we shall assume that the irreducible representation of degree $p+1$ occurs besides the assumptions (*), (**), $n=p+2$ and $t \equiv 0 \pmod{2}$. Under these assumptions we shall prove that such a group does not exist.

We shall use the same notations as Brauer [1]. First of all, we shall assume that $n=p+2=F(p, 1, 2)=F(p, u, 1)$ with positive integer $u$. For, if $n$ does not have the expression $F(p, u, 1)$ with positive integer $u$, then the character-relations in $B(\rho)$ yields a contradiction easily. Simple computations show that the possible values of the irreducible characters in $B_i(\rho)$ are $1, \rho + 1, \rho + (u-1)p-1, (\rho + 1)/t$ and $(u-1)p-1)/t$. In order to consider such characters, we shall prove following lemmas, essentially due to Brauer.

Lemma 1. Under assumptions (*), (**), $n=p+2 \ t \equiv 0 \pmod{2}$, if $G$ has an irreducible character $A$ of degree $up+1(u>1)$, then for the element $I$ of order 2 in the normalizer $N(\Psi)$ of a $p$-Sylow subgroup $\Psi$.

---

1) W. F. Reynolds kindly pointed out this error and gave the author many useful suggestions. By this error, Theorem in [5] (p. 107) should be corrected as follows: If $2p-3 < n \leq 2p+3$, $t \equiv 0 \pmod{2}$ and $t>1$, then $2p+1$ is a prime power and $G \cong LF(2, 2p+1)$, unless the irreducible representation of degree $p+1$ occurs. But Theorem in [5] (p. 116) is valid.
\[
A(I) = \begin{cases} 
  u+1, & \text{if } u \text{ is even.} \\
  0, & \text{if } u \text{ is odd.}
\end{cases}
\]

The normalizer \( N(\mathfrak{P}) \) of a \( p \)-Sylow subgroup \( \mathfrak{P} \) is a metacyclic group \( \{P, Q\} \) of order \( pq = p(p-1)/t \) and has \( q \) linear characters \( \omega_\mu \) and \( t \) \( p \)-conjugate characters \( Y^{(t)} \) of degree \( q \). If we consider the character \( A \) in \( N(\mathfrak{P}) \), then \( A \) is decomposed into two parts \( \bar{A} \) and \( A_0 \), where \( \bar{A} \) is a sum of \( u+1 \) linear characters \( \omega_\mu \) and \( A_0 \) is a linear homogeneous combination of \( Y^{(t)} \). Now, as \( u \geq 1 \), \( n = p + 2 \) has an expression \( F(p, u, 1) = (up + u^2 + u + 1)/(u + 1) \). This implies \( p = u^2 - u - 1 \) and \( g = p q(u(p + 1)(p + u + 1))/(u + 1) \). Since \( gn(G)^{-1} \cdot (D_g A)^{-1} \cdot A(G) \) is an algebraic integer, where \( n(G) \) is the order of the normalizer of \( G \) in \( \mathfrak{P} \) and \( D_g A \) is the degree of \( A \), \( gn(Q)^{-1} \cdot (u(p + 1))^{-1} \cdot A(Q^j) \) is, and also \( A(Q^j)/(u + 1) \) is an algebraic integer.

But \( A(Q^j) = \bar{A}(Q^j) \) for \( j \equiv 0 \pmod{q} \). Then applying Burnside's method, we have \( \bar{A}(Q^j) = 0 \) or \( (u + 1) \omega \mu^j \) : that is, \( A(Q^j) = 0 \) or \( (u + 1) \omega \mu^j \) for \( j \equiv 0 \pmod{q} \). Assume \( \bar{A} = \alpha_1 \omega_\mu_1 + \alpha_2 \omega_\mu_2 + \cdots + \alpha_r \omega_\mu_r \) is a decomposition of \( \bar{A} \) in \( N(\mathfrak{P}) \). Let \( m \) be the least positive integer satisfying \( \bar{A}(Q^m) \equiv 0 \). Then \( m \) is a divisor of \( q \) and any integer \( x \) satisfying \( \bar{A}(Q^x) \equiv 0 \) is a multiple of \( m \). Now there exist \( q/m \) integers satisfying \( \bar{A}(Q^x) \equiv 0 \) from the orthogonality-relations, we have
\[
\sum_{j=0}^{q-1} \bar{A}(Q^j) \omega_\mu(j) \omega_\mu(j) = \alpha_i \cdot q.
\]

On the other hand, \( \sum_{j=0}^{q-1} \bar{A}(Q^j) \omega_\mu(j) = \sum_{i=1}^{q-1} \bar{A}(Q^m) \omega_\mu(j) = (u + 1) q/m \). Hence \( \alpha_i q = (u + 1) q/m \). This means \( \alpha_i = (u + 1)/m \) for \( i = 1, 2, \ldots, r \). Therefore \( \bar{A} = \frac{u + 1}{m} (\omega_\mu_1 + \omega_\mu_2 + \cdots + \omega_\mu_m) \). Furthermore \( \bar{A}(Q^m) \equiv 0 \) implies \( \omega_\mu_1 \omega_\mu = \omega_\mu_2 \omega_\mu = \cdots = \omega_\mu_m \). This means \( \mu_1 \equiv \mu_2 \equiv \cdots \equiv \mu_m \pmod{q/m} \). Then we can put \( \mu_1 = a, \mu_2 = a + q/m, \ldots, \mu_m = a + (m - 1) q/m \). Thus

(D) \[
A = \frac{u + 1}{m} (\omega_\mu + \omega_{a + q/m} + \cdots + \omega_{a + (m - 1)q/m}) + A_0.
\]

Next consider its determinant for \( Q^j \) for \( j \equiv 0 \pmod{q} \). This value must be 1.
\[
\text{Det}(A(Q^j)) = \omega^{ja(u + 1)} (-1)^{(j - 1)(u + 1)}.
\]

Suppose \( (u + 1)/m \equiv 0 \pmod{2} \), then \( \omega^{ja(u + 1)} = (-1)^j \). For \( j = 1 \), we have \( a(u + 1) \equiv q/2 \pmod{q} \), \( a(u + 1) \equiv 0 \pmod{q} \). These yield \( u - 2 \equiv 0 \pmod{2} \). This contradicts \( u + 1 \equiv 0 \pmod{2} \). Now we have \( (u + 1)/m \equiv 0 \pmod{2} \) and then \( a(u + 1) \equiv 0 \pmod{q} \). From (D),
Note on Brauer's Theorem II

\[ A(I) = \frac{u+1}{m}((-1)^a + (-1)^{a+q/m} + \cdots + (-1)^{a+(m-1)q/m}). \]

i) If \( u \) is even, then \( m \) is odd. And \( q/m \) must be even. From \( a(u+1) \equiv 0 \pmod{q} \), \( a \) is even. Thus \( A(I) = u+1 \).

ii) If \( u \) is odd, then \( \frac{q}{m} = \frac{u+1}{m} \frac{u-2}{t} \) is odd. Hence \( A(I) = 0 \). This proves lemma 1.

For other type of irreducible characters, similar results can be proved.

Lemma 2.\(^2\) Under the same assumptions as in Lemma 1, if \( \mathfrak{g} \) has an irreducible character \( B \) of degree \((u-1)p-1\), then for an involution \( I \) (the element of order 2) in \( \mathfrak{N}(\mathfrak{p}) \)

\[ B(I) = \begin{cases} 0, & \text{if } u \text{ is even} \\ u-2, & \text{if } u \text{ is odd} \end{cases} \]

Lemma 3.\(^3\) Under the same assumptions as in Lemma 1, if \( \mathfrak{g} \) has an irreducible character \( C \) of degree \((up+1)/t\), then for an involution \( I \) of \( \mathfrak{N}(\mathfrak{p}) \)

\[ C(I) = \begin{cases} (u+1)/t, & \text{if } u \text{ is even} \\ 0, & \text{if } u \text{ is odd} \end{cases} \]

Lemma 4.\(^4\) Under the same assumptions as in Lemma 1, if \( \mathfrak{g} \) has an irreducible character \( C \) of degree \(((u-1)p-1)/t\), then for an involution \( I \) of \( \mathfrak{N}(\mathfrak{p}) \)

\[ C(I) = \begin{cases} 0, & \text{if } u \text{ is even} \\ (u-2)/t, & \text{if } u \text{ is odd} \end{cases} \]

2) If \( u-2=1 \), then the Burnside's method yields nothing. But \( u-2=1 \) yields \( p=5 \). For \( p=5 \), \( g=5 \cdot 4 \cdot (1+7 \cdot 5)/t \). Since \( t \) is odd, \( t=1 \). Then \( B_1(5) \) consists of the principal character, \( x \) characters of degree 6, \( y \) characters of degree 16 and \( z \) characters of degree 9. And we have \( 1+x+y+z=5 \) and \( 1+6x+16y=9z \). This is a contradiction. Hence \( u-2>1 \).

3) Let \( u+1=t \). If the irreducible character of degree \( up+1 \) occurs, then \( q \equiv 0 \pmod{(u+1)} \). And \( u=2 \). This contradicts \((**\))\(^2\). Therefore \( B_1(p) \) may consists of the 1-character, \( x \) characters of degree \( p+1 \), \( y \) characters of degree \( (u-1)p-1 \) and \( t \) characters of degree \( (up+1)/t \). Then \( 1+x+y+(p-1)/t = u-2 \) and \( x+1=(u-1)y \). This is also a contradiction. Hence \( (u+1)/t \geq 1 \).

4) Let \( u-2=t \). If the irreducible character of degree \( (u-1)p-1 \) occurs, then \( q \equiv 0 \pmod{(u-2)} \). And either \( u=5 \) or \( u=3 \). If \( u=5 \), then \( p=19 \). \( B_1(19) \) may consist of the 1-character, \( x \) characters of degree 29, \( y \) characters of degree 96, \( z \) characters of degree 75 and \( t \) characters of degree 25. Then \( 1+x+y+z=6 \) and \( x+5y=4z+1 \). This is a contradiction. If \( u=3 \), then \( p=5 \). So \( B_1(5) \) may consists of the 1-character, \( x \) characters of degree 6, \( y \) characters of degree 16 and \( z \) characters of degree 9. Then \( 1+x+y+z=5 \) and \( 1+6x+19y=9z \). This is a contradiction. If the irreducible character of degree \( (u-1)p-1 \) does not occur, then \( B_1(p) \) may consist of the 1-character, \( x \) characters of degree \( p+1 \), \( y \) characters of degree \( up+1 \) and \( t \) characters of degree \( ((u-1)p-1)/(u-2) \). Then \( 1+x+y=u+1 \) and \( x+uy=1 \). This is a contradiction. Hence \( (u-2)/t \geq 1 \).
Lemma 5. Under the same assumptions as Lemma 1, let $X$ be an irreducible character of degree $p+1$, then for an involution $I$ of $R(\mathfrak{B})$

$$X(I) = \begin{cases} 0, & \text{if } q \equiv 0 \pmod{4}. \\ \text{either } +2 \text{ or } -2, & \text{if } q \equiv 0 \pmod{4}. \end{cases}$$

In the latter case, we denote by $y_1$ and $y_2$ respectively the numbers of characters whose values for $I$ are $+2$ and $-2$.

Now, we shall consider two cases.

Case I: $R$ contains an irreducible character of degree $(u-1)p$; Let $B_1(p)$ contain $x$ characters of degree $u+1$, $y$ characters of degree $p+1$, and $z$ characters of degree $(u-1)p-1$. From the character-relations in $B_1(p)$, we have

\begin{align*}
1 + x + y + z &= (p-1)/t, \\
xu + y + (u+1)/t &= (u-1)z, \\
p &= u^2 - u - 1.
\end{align*}

The character-relation which holds for $p$-regular elements shows for an involution $I$ that

(I) \[ 1 + \sum A(I) + \sum X(I) + C(I) = \sum B(I). \]

Eliminate $y$ and $p$, then $(u-1)x - (u-1)z + (u^2-1)/t = z + 1$. Put $z+1 = \alpha(u-1)$. Then $x = -(u+1)/t + \alpha u - 1$, $y = (u^2-1)/t - 2\alpha u + \alpha + 1$ and $z = \alpha u - \alpha - 1$. As $x \geq 0$, $\alpha \geq 1$. And $\alpha \geq 2$ for $t=1$.

Now consider (I) for even $u$ and for odd $u$ separately.

Case Ia: Case where $u$ is even; From (I), none of $X(I)$ can be zero. Hence we have

\[ 1 + x(u+1) + 2(y_1 - y_2) + (u+1)/t = 0. \]

But $y_2 - y_1 \leq y$. Then $1 + x(u+1) + (u+1)/t \leq 2y$. Substitute above values for $x$ and $y$, then we have

\[ \alpha(u+5u-2) - u - 2 \leq (3u^2 + u - 2)/t. \]

This inequality yields $\alpha = 0$ for $t = 1$ and $\alpha \leq 2$ for $t = 1$. Hence we have $t = 1$ and $\alpha = 2$.

Case Ib: Case where $u$ is odd; From (I), none of $X(I)$ can be zero. Hence we have

\[ 1 + 2(y_1 - y_2) = (u-2)z. \]

But $y_1 - y_2 \leq y$. Then $(u-2)z - 1 \leq 2y$. Substitute the above values for $y$ and $z$, then we have
Note on Brauer's Theorem II

\[ \alpha(u^2 + u) - u - 1 \leq 2(u^2 - 1)/t, \]
\[ \alpha u - 1 \leq 2(u - 1)/t. \]

This inequality yields \( \alpha = 0 \) for \( t = 1 \) and \( \alpha < 2 \) for \( t = 1 \). This is a contradiction.

Case II: \( \mathcal{C} \) contains an irreducible character of degree \( ((u-1)p-1)/t \); Let \( B_1(p) \) contain \( x \) characters of degree \( up+1 \), \( y \) characters of degree \( p+1 \), \( z \) characters of degree \( (u-1)p-1 \). From the character-relations in \( B_1(p) \),

\[ 1 + x + y + z = (p-1)/t, \]
\[ uz + y = (u-1)z + (u-2)/t, \]
\[ \rho = u^2 - u - 1, \]

\( (I') \)
\[ 1 + \sum A(I) + \sum X(I) = \sum B(I) + C(I). \]

Eliminate \( y \) and \( \rho \), then \( x + 1 = ux - uz + u(u-2)/t \). Put \( x + 1 = \alpha u \). Then
\[ z = (u-2)/t + \alpha u - \alpha - 1, y = u(u-2)/t - 2\alpha u + \alpha + 1 \quad \text{and} \quad x = \alpha u - 1. \]

Of course \( \alpha \) is a positive integer.

Case IIa: Case where \( u \) is even; As Case Ia, from \( (I') \), we have
\[ 1 + x(u+1) \leq 2y. \]

Substitute the above values for \( x \) and \( y \), then we have
\[ \alpha(u^2 + 5u - 2) - u - 2 \leq 2u(u - 2)/t. \]

This yields \( t = 1 \) and \( \alpha = 1 \).

Case IIb: Case where \( u \) is odd; We have from \( (I') \),
\[ 1 + 2(y_1 - y_2) = (u-2)z + (u-2)/t. \]

As Case Ib, we have
\[ (u-2)z + (u-2)/t - 1 \leq 2y, \]
\[ \alpha(u^2 + u) - u - 1 \leq (u-1)(u-2)/t, \]
\[ \alpha u - 1 \leq (u-2)/t. \]

This inequality yields \( \alpha < 1 \). This is a contradiction.

Combining the above cases, the only possible case occurs when \( t = 1 \) for even \( u \). In this case \( B_1(p) \) consists of the 1-character, \( u-1 \) characters of degree \( up+1 \), \( u^2 - 4u + 2 \) characters of degree \( p+1 \) and \( 2u-3 \) characters of degree \( (u-1)p-1 \).

Denote the sum of the elements in the conjugate class containing \( G \) by \( \langle G \rangle \). Now we consider the coefficient of \( \langle I \rangle \) in the group ring of its center. From the orthogonality relations the coefficient \( a_\rho \) of \( \langle P \rangle \) is
\[ a_\rho = gn(I)^{-2} \sum (D_g X)^{-1} X(I)^{\rho} \cdot \overline{X}(P), \]
where the summation ranges over all the irreducible characters of $\mathfrak{G}$. (cf. [2], §5). On the other hand this coefficient is equal to the number of pairs of conjugate elements $T$ and $S$ of $\langle I \rangle$ such that $TS = P$. If $TS = P$, then $TPT^{-1} = P^{-1}$. By condition (*), this number of pairs is $p$. Hence we get

$$p = gn(I)^{-2} \sum (D_gX)^{-1}X(I)^2\bar{X}(P),$$

where sum ranges over all irreducible characters of $\mathfrak{G}$.

Applying this, we have

$$n(I)^2p = g\{1+(u+1)^{-1}(u+1)(u-1)+(p+1)^{-1}4(u^2-4u+2)\}.$$

$$n(I)^2 = 2u(u-2)^2(u-1)(3u-2)(u+1).$$

Since $n(I)$ is a multiple of $p-1 = (u+1)(u-2)$ and $u$ is even, we have $u+1 = 5$. Hence $n(I)^2 = 52^23$. This number is not a square.

Thus for $n = p+2$ and $t \equiv 0 \pmod{2}$, such a group $\mathfrak{G}$ does not exist. This completes the proof of the theorem.

(Received September 17, 1959)

References


