Osaka Mathematical Journal
Vol. 5, No. 2, December, 1953

Supplement to "Note on Brauer's Theorem of Simple Groups"

By Osamu NAGAI

Using the modular representation theory of groups, R. Brauer obtained very interesting results[1] concerning a finite group satisfying the following conditions:

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

($**$) *The commutator subgroup* $\mathfrak{G}'$ *of* $\mathfrak{G}$ *is equal to* $\mathfrak{G}$.

Namely;

Theorem. If $\mathfrak{G}$ is a group of finite order g satisfying the conditions ($*$) and ($**$), then $g=p(p-1)(1+np)/t$, where n and t are integers, and t divides $p-1$. The group $\mathfrak{G}$ contains exactly $1+np$ subgroups of order p and t classes of conjugate elements of order p. Moreover, if $n<(p+7)/3$, then either (1) $\mathfrak{G}\cong LF(2, p)$ or (2) p is a prime of the form $2^{\mu}\pm 1$ and $\mathfrak{G}\cong LF(2, 2^{\mu})$.

In a previous note[2], we considered the case $n<p+2$ and $t\not\equiv 0 \pmod 2$, and proved that p is of the form $2^{\mu}-1$ and $\mathfrak{G}\cong LF(2, 2^{\mu})$. In this supplement we shall prove that, including the case $n=p+2$, the previous result is valid; that is,

Theorem. *Let* $\mathfrak{G}$ *be a group of finite order satisfying conditions* ($*$) *and* ($**$). *If* $n\leq p+2$ *and* t *is odd, then* p *is of the form* $2^{\mu}-1$ *and* $\mathfrak{G}\cong LF(2, 2^{\mu})$.

Before the proof, we shall mention Brauer's results[3] which is needed in the sequel. Under the condition ($*$), the order of $\mathfrak{G}$ contains p to the first power only. So the ordinary irreducible representations of $\mathfrak{G}$ are of

---

1) R. Brauer, "On the representation of groups of finite order," Proc. Nat. Akad. Sci., vol. 25 (1939) p. 291; R. Brauer, "On permutation groups of prime degree and related classes of groups," Ann. of Math., vol. 44 (1943) pp. 57-79, especially p. 70, Theorem 10. I refer to this paper as [B].

2) O. Nagai, "Note on Brauer's Theorem of Simple Groups," Osaka Math. J., vol. 4 (1952) pp. 113-120.

3) [B] and R. Brauer, "On groups whose order contains a prime number to the first power I, II," Amer. J. of Math., vol. 54 (1942).

four different types: (I) Representations $\mathfrak{A}_\rho$ of a degree $a_\rho = u_\rho p+1$. (II) Representations $\mathfrak{B}_\sigma$ of a degree $b_\sigma = v_\sigma p-1$. (III) Representations $\mathfrak{C}^{(\nu)}$ of a degree $c=(wp+\delta)/t$, where $\delta = \pm 1$ and w is a possitive integer. There exist exactly t such representations that are algebraically conjugate. (IV) Representations $\mathfrak{D}_\tau$ of a degree $d_\tau = px_\tau$. Denote by A_ρ, B_ρ, $C^{(\nu)}$ and D_τ the characters of $\mathfrak{A}_\rho$, $\mathfrak{B}_\sigma$, $\mathfrak{C}^{(\nu)}$ and $\mathfrak{D}_\tau$ respectively.

If we have x characters A_ρ, $\rho=1, 2, \dots, x$, and y characters B_σ, $\sigma = 1, 2, \dots, y$, then we have

$$x+y=(p-1)/t. \tag{1}$$

Furthermore, for elements G of order prime to p, we have

$$\sum A_\rho(G)+\delta\, C^{(\nu)}(G)=\sum B_\sigma(G). \tag{2}$$

In particular, for $G=1$, this gives

$$\sum a_\rho+\delta\, c=\sum b_\sigma, \text{ or } \sum u_\rho+(\delta w+1)/t=\sum v_\sigma. \tag{2'}$$

Since g is equal to the sum of the squares of all the degrees, we have

$$\begin{aligned}&\sum u_\rho^2+\sum v_\sigma^2+w^2/t+\sum x_\tau^2=(pn-n+1)/t,\\ &\sum u_\rho^2+\sum v_\sigma^2+w^2/t+\sum x_\tau^2=(p^2+p-1)/t \text{ (in the case } n=p+2).\end{aligned} \tag{3}$$

Since the first p-block $B_{\_}(p)$ is of the only lowest kind of $\mathfrak{G}$, the full number of irreducible representations of $\mathfrak{G}$ whose degrees are prime to p is $(p-1)/t+t$.

Proof.

It is sufficient to prove that such group does not exist in the case $n=p+2$, for the case $n<p+2$ was discussed in the previous note[2].

Let $n=p+2$.

First of all, we shall prove that such group $\mathfrak{G}$ must be simple. Let $\mathfrak{G}$ have a proper normal subgroup $\mathfrak{H}$ of order h. From [B], Theorem 3 and Theorem 4, $\mathfrak{G}/\mathfrak{H}$ also satisfies condition (*) and at the same time $h\equiv 1 \pmod p$ and $(1+np)\equiv 0 \pmod h$. Since $n=p+2$, we have $(p+1)^2\equiv 0 \pmod h$, $h\equiv 1 \pmod p$ and $g=p(p-1)(p+1)^2/t$. We put $h=1+\alpha p$ and $(p+1)^2=\beta h$, then $(p+1)^2=\beta(1+\alpha p)$. So $\beta\equiv 1 \pmod p$. We put $\beta=1+\gamma p$. Then $(p+1)^2=(1+\alpha p)(1+\gamma p)$. This gives $p+2=\alpha\gamma\, p+\alpha+\gamma$. If $\gamma=0$, then $\alpha=p+2$. We have $h=(p+1)^2$. Since $\mathfrak{G}/\mathfrak{H}$ also satisfies condition (**), $\mathfrak{G}/\mathfrak{H}$ can not be a metacyclic group of order $p(p-1)/t$. If $\gamma\neq 0$, then, since $\alpha\neq 0$, we have $\alpha=1$ and $\gamma=1$. So we have $h=p+1$. This means $g/h=p(p-1)(p+1)/t$.

From [B], Theorem 10, t must be even[4]. This is a contradiction.

Then, we shall examine the degrees of the irreducible representations of $\mathfrak{G}$. In the case $n=p+2$, n is represented as $n=F(p, u^{(\nu)}, h^{(\nu)})$[5] in two kinds such that $\begin{cases} u^{(\nu)}=u \\ h^{(\nu)}=1 \end{cases}$ and $\begin{cases} u^{(\nu)}=1 \\ h^{(\nu)}=2 \end{cases}$. So from [$B$], Theorem 7, the degrees of the irreducible representations of $\mathfrak{G}$, as far as they are prime to p, can only have some of the values

$$\begin{aligned} a_\rho &= 1\,,\ np+1\,,\ up+1\,,\ p+1\,, \\ b_\sigma &= p-1\,,\ ((n-1)/u)p-1\,,\ (n-2)p-1\,, \\ c &= (np+1)/t\,,\ (up+1)/t\,,\ (p+1)/t\,,\ (p-1)/t\,, \\ & \left(\left(\frac{n-1}{u}\right)p-1\right)/t\,,\ ((n-2)p-1)/t\,. \end{aligned}$$

Since $n=p+2$ is represented as $n=\dfrac{up+u^2+u+1}{u+1}$, we have $p=u^2-u-1$ (this means $u\geqq 3$). Using these relations of n and p, we can simplify some of above values such that

$$\begin{aligned} a_\rho &= 1\,,\ np+1\,,\ up+1\,,\ p+1\,, \\ b_\sigma &= p-1\,,\ ((n-1)/u)p-1=(p+u)p/(u+1)-1=(u-1)p-1\,, \\ &\quad (n-2)p-1=p^2-1\,, \\ c &= (np+1)/t\,,\ (up+1)/t\,,\ (p+1)/t\,,\ (p-1)/t\,, \\ &\quad \left(\frac{n-1}{u}p-1\right)/t=((u-1)p-1)/t\,, \\ &\quad ((n-2)p-1)/t=(p^2-1)/t\,. \end{aligned}$$

Now we shall eliminate the above values of degrees one by one.

If $\mathfrak{G}$ possesses the irreducible representations $\mathfrak{Z}$ of degree $p+1$, then we can decompose the character ς of $\mathfrak{Z}$ in the normalizer $\mathfrak{N}(\mathfrak{P})=\{P, Q\}$ of p-Sylow subgroup $\mathfrak{P}$ into its irreducible constituents. But it is easy to find all irreducible characters of the group $\mathfrak{N}(\mathfrak{P})$ of order $p(p-1)/t=pq$. Let ω be a primitive q-th root of unity. We then have q linear characters ω_μ, $(\mu=0, 1, 2, \ldots, q-1)$ defined by

$$\omega_\mu(Q^J)=\omega^{\mu J}\,,\ \omega_\mu(P^J)=1\,.$$

4) Furthermore, by considering the automorphism of $\mathfrak{H}$ induced by the element of $\mathfrak{T}$, we can find $p+1=2^\mu$ and $\mathfrak{H}$ must be an abelian group of type $(2, 2, \cdots\cdots, 2)$. Thus in the case $t\equiv 0 \pmod 2$, the structure of the non-simple group $\mathfrak{G}$ is determined: that is, $\mathfrak{G}$ contains an abelian normal subgroup of type $(2, 2, \cdots\cdots, 2)$ and the factor-group $\mathfrak{G}/\mathfrak{H}\cong LF(2, p)$ and $p=2^\mu-1$. This remark is due to Mr. N. Itô.

5) Cf. [B], Theorem 7.

Besides, we have t conjugate characters $Y^{(\tau)}$ of degree q such that $Y^{(\tau)}(Q^j)=0$ for $j \not\equiv 0 \pmod q$.

By [B], Lemma 3, $\varsigma(N)$ (N in $\mathfrak{N}(\mathfrak{P})$) contains only two linear characters: $\varsigma(N)=\omega_\mu(N)+\omega_\nu(N)+\sum Y^{(\tau)}(N)$. So the determinant of $\mathfrak{Z}(Q^j)$ ($j \not\equiv 0 \pmod q$) has the value

$$\omega^{j(\mu+\nu)}\cdot\omega^{t(1+2+\cdots+q-1)}=\omega^{j(\mu+\nu)}\cdot(-1)^{(q+1)t}=\omega^{j(\mu+\nu)}\cdot(-1)^t$$

Since t is odd, we have $|\mathfrak{Z}(Q^j)|=-\omega^{j(\mu+\nu)}$. But since the determinant of $\mathfrak{Z}(G)$ (G in $\mathfrak{G}$) forms a representation of degree 1 of $\mathfrak{G}$, this value must be equal to 1 for all $j \not\equiv 0 \pmod q$. This is obviously impossible, except the case $q=(p-1)/t=2$. But in this excluded case, if $\mathfrak{G}$ possesses the irreducible representation of degree $p+1$, then by (2)$'$

$$c=((u-1)p-1)/t \text{ or } (p^2-1)/t\,.$$

If $c=((u-1)p-1)/t$, then by (2)$'$, $1=(u-2)/t$. But since $p-1=u^2-u-2$ and $(p-1)/t=2$, we have $u+1=2$. This is impossible. If $c=(p^2-1)/2$, then by (2)$'$, $1=(p-1)/t$. This is impossible.

Thus $\mathfrak{G}$ does not possess the irreducible representation of degree $p+1$.

Since t is odd, $\mathfrak{G}$ does not possess the representations of degree $p-1$, $(p-1)/t$ and $(p+1)/t$[6]. Furthermore, according to the relation (3), $\mathfrak{G}$ does not possess the irreducible representations of degree $np+1$ and $(np+1)/t$.

If $\mathfrak{G}$ possesses the representations of degree p^2-1, then we can assume that the first p-block $B_1(p)$ contains one character of degree 1, x characters of degree $up+1$, y_1 characters of degree $(u-1)p-1$, y_2 characters of degree p^2-1 and t conjugate characters of degree $(wp+\delta)/t$. From (3), we have

$$u^2x+(u-1)^2y_1+p^2y_2+w^2/t \leqq (p^2+p-1)/t\,.$$

Now it is sufficient to draw a contradiction only in the case $t=1$. For, if $t \geqq 3$, then above inequality shows $p^2y_2 \leqq (p^2+p-1)/3$. This is impossible.

Let $t=1$. In this case the character $C^{(\nu)}(G)$ is considered as one of those $A_\rho(G)$ ($\rho \neq 1$) or $B_\sigma(G)$. So we again assume that $B_1(p)$ consists of one character of degree 1, x characters of degree $up+1$, y characters of degree $(u-1)p-1$ and y_2 characters of degree p^2-1, where $1+x+y_1+y_2=p$. From (3), we have

6) Cf. The relation (2)$'$.

$$u^2 x+(u-1)^2 y_1+p^2 y_2 \leqq p^2+p-1 .$$

From (2), $x \neq 0$. Then we have

$$u^2+y_1+p^2 \leqq p^2+p-1 ,$$
$$u^2+y_1 \leqq p-1 = u^2-u-2 .$$

This is impossible.

Thus $\mathfrak{G}$ does not possess the irreducible representations of degree p^2-1. Furthermore, above calculations show that $\mathfrak{G}$ does not possess the representations of degree $(p^2-1)/t$.

Then, it remains only the following cases to be considered; $B_1(p)$ consists of one character of degree 1, x characters of degree $up+1$, y characters of degree $(u-1)p-1$ and either t characters of degree $(up+1)/t$ or those of degree $((u-1)p-1)/t$.

Case A: $B_1(p)$ contains the characters of degree $(up+1)/t$.

If $x=0$, then from (2)$'$

$$(u+1)/t = y(u-1) .$$

But from the relations $1+x+y=(p-1)/t$ and $p=u^2-u-1$, we have

$$(u+1)/t=(u^2-u-2)\ (u-1)/t-(u-1) ,$$
$$t(u-1)=(u+1)\ (u^2-3u+1) ,$$
$$(u+1)/t=(u-1)/(u^2-3u+1) .$$

Since $(u+1)/t \geqq 1$, $u-1 \geqq u^2-3u+1$. Hence $u=3$. But $u+1 \equiv 0 \pmod{t}$. This contradicts $t \not\equiv 0 \pmod{2}$[7]. Thus we can assume $x \geqq 1$.

The degree a_ρ must divide the order g of $\mathfrak{G}$. But using $p=u^2-u-1$, a_ρ and g are decomposed into the forms:

$$a_\rho = up+1 = (u-1)^2\ (u+1) ,$$
$$g = p(p-1)\ (p+1)^2/t = (u^2-u-1)\ (u-2)\ (u+1)\, u^2\, (u-1)^2/t .$$

This gives $(u-2)\,u^2 \equiv 0 \pmod{t}$. But since $u+1 \equiv 0 \pmod{t}$, $t=3$ or $t=1$.

If $t=1$, then by (2)$'$ and by (1), we have

$$ux+u+1 = y(u-1) \text{ and } 1+x+y=p-1 .$$

So

$$u(u^2-u-3-y)+u+1 = y(u-1) ,$$
$$y(2u-1) = u^3-u^2-2u+1 .$$

---

7) If $t=1$, then the character of type C may be considered as one of those of type A_ρ or of type B_σ. So even in this case $B_1(p)$ contains the character of degree up+1.

Since $((u^3-u^2-2u+1), (2u-1))=1$, such y cannot be a rational integer.

If $t=3$, then we have

$$ux+(u+1)/3=y(u-1) \text{ and } 1+x+y=(p-1)/3.$$

So

$$u((u^2-u-2)/3-y-1)+(u+1)/3=y(u-1),$$
$$3y(2u-1)=u^3-u^2-4u+1.$$

But $8(u^3-u^2-4u+1)=(2u-1)(4u^2-2u-17)-9$. This means $9\equiv 0 \pmod{(2u-1)}$. Hence $u=5$. So $y=3$, $p=19$ and $x=2$. Thus $g=2^5\cdot 3\cdot 5^2\cdot 19$, $a_1=1$, $a_2=2^5\cdot 3$, $b_\sigma=5^2\cdot 3$ and $c=2^5$. Since the characters $A_2(G)$ and $C^{(\nu)}(G)$ are of highest kind for 2 and since $B_\sigma(G)$ is of highest kind for 3 and furthermore since the normalizer $\mathfrak{N}(\mathfrak{P})$ of p-Sylow subgroup $\mathfrak{P}$ contains an element Q of order $(p-1)/t=6$, we have

$$A_1(Q)=1,\ A_2(Q)=0,\ B_\sigma(Q)=0 \text{ and } C^{(\nu)}(Q)=0.$$

This contradicts (2).

Case B: $B(p)$ contains the characters of degree $((u-1)p-1)/t$.

If $y=0$, then from (1) and (2)'

$$u((p-1)/t-1)=(u-2)/t,$$
$$u^3-u^2-3u+2=ut.$$

So $2\equiv 0 \pmod{u}$. This is impossible. Thus we can assume $y\geqq 1$.

As in the case A, since $b_\sigma=(u-1)p-1=u(u-2)$ must divide the order g of $\mathfrak{G}$, we have $t=3$ or $t=1$.

If $t=1$, then from (2)' and (1), we have

$$ux=y(u-1)+u-2 \text{ and } 1+x+y=p-1.$$

So

$$u(u^2-u-3-y)=y(u-1)+u-2,$$
$$y(2u-1)=u^3-u^2-4u+2.$$

But such y cannot be a rational integer.

If $t=3$, then we have

$$ux=y(u-1)+(u-2)/3 \text{ and } 1+x+y=(p-1)/3.$$

So

$$3u((p-1)/3-y-1)=3y(u-1)+u-2,$$
$$3y(2u-1)=u^3-u^2-6u+2.$$

But such y cannot be a rational integer.

Thus, in the case $n=p+2$, such group can not exist.

Combining this with the previous result, we get the Theorem.

(Received September 21, 1953)