Title	Note on Brauer's theorem of simple groups
Author(s)	Nagai, Osamu
Citation	Osaka Mathematical Journal. 1952, 4(2), p. 113-120
Version Type	VoR
URL	https://doi.org/10.18910/5720
rights	
Note	

Note on Brauer's Theorem of Simple Groups

By Osamu NAGAI

Using the theory of modular representations of groups, R. Brauer studied simple groups and obtained very interesting results[1] concerning a group which satisfies the following conditions:

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

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

By relaxing his conditions about the number of p-Sylow subgroups, we have the following theorem:

Theorem. *Let $\mathfrak{G}$ be a group of finite order which satisfies conditions (*) and (**). Then $g = p\,(p-1)\,(1+np)/t$ is the order of $\mathfrak{G}$, 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 in $\mathfrak{G}$. If $n < p+2$ and t is odd, then p is of the form $2^\mu - 1$ and $\mathfrak{G} \cong LF(2,2^\mu)$.*

It seems probable that the case $\mathfrak{G} \cong LF(3,3)$ will occur, when t is even. But it is still an open problem.

Brauer mentioned in his earlier paper[2] that if $\mathfrak{G}$ is a simple group of order $g = qp\,(1+np)$ with $q\,|\,p-1$ in which the elements of order p commute only with their own powers and if $n < (2p+7)/3$, then either (1) $\mathfrak{G}$ is cyclic, or (2) $\mathfrak{G} \cong LF(2, p)$ or (3) p is a prime of the form $p = 2^\mu \pm 1$, and $\mathfrak{G} \cong LF(2,2^\mu)$. (We can easily prove these facts by the slight modifications of his method).[3]

1. Preliminaries.

The former part of the theorem is obvious, so we shall prove only the latter half. In this paper we shall use the same notations as Brauer's and prove the theorem step by step with a little complicating numerical calculations.

---

1) R. Brauer, On permutation groups of prime degree and related classes of groups, Ann. of Math. 44 (1943), I refer to this paper as [1].

2) R. Brauer, On the representation of groups of finite order, Proc. Nat. Akad. Sci. 25 (1939).

3) Cf. the proof of [1], Theorem 10. In the proof of Lemma 8 of this paper, we shall show the outline of them.

Let $\mathfrak{G}$ be a group of finite order g which satisfies the condition (∗). Since g contains the prime p only to the first power, Brauer's results[4] can be applied. For the sake of convenience we first mention those facts which will be needed.

The ordinary irreducible representations of $\mathfrak{G}$ are of four different types: (I) Representations $\mathfrak{A}_\rho$ of a degree $a_\rho = u_\rho p + 1$. Denote by A_ρ the character of $\mathfrak{A}_\rho$. (II) Representations $\mathfrak{B}_\sigma$ of a degree $b_\sigma = v_\sigma p - 1$. Denote by B_σ the character of $\mathfrak{B}_\sigma$. (III) Representations $\mathfrak{C}$ of a degree c which is not congruent to $0, 1, -1 \pmod{p}$ for $t \neq 1$. There exist exactly t such representations $\mathfrak{C}^{(1)}, \mathfrak{C}^{(2)}, \cdots, \mathfrak{C}^{(t)}$ that are algebraically conjugate. Denote by $C^{(\nu)}$ the character of $\mathfrak{C}^{(\nu)}$. The degree c is of the form $c = (wp + \delta)/t$, $\delta = \pm 1$, where w is a positive integer. (These characters $C^{(\nu)}$ are called "exceptional" and characters A_ρ and B_σ are called "non-exceptional"). (IV) Representations $\mathfrak{D}_\tau$ of a degree $d_\tau = p x_\tau$. Denote by D_τ the character of $\mathfrak{D}_\tau$.

Because of the assumption (∗), $\mathfrak{G}$ has only one block $B_1(p)$ of lowest kind and some blocks of highest kind. If $B_1(p)$ has α characters $A_\rho (\rho = 1, 2, \cdots, \alpha)$ and β characters $B_\sigma (\sigma = 1, 2, \cdots, \beta)$, then the following relations hold:

(1) $$\alpha + \beta = (p-1)/t,$$

(2) $$\sum_\rho A_\rho(G) + \delta C^{(\nu)}(G) = \sum_{\sigma=1}^{\beta} B_\sigma(G) \quad \text{(for } p\text{-regular element } G \text{ of } \mathfrak{G}).$$
Putting $G = 1$, we have

(2)′ $$\sum_{\rho=1}^{\alpha} u_\rho + (\delta w + 1)/t = \sum_{\sigma=1}^{\beta} v_\sigma.$$

Since g is equal to the sum of squares of all the degrees of these representations, we obtain

(3) $$\sum_{\rho=1}^{\alpha} u_\rho{}^2 + \sum_{\sigma=1}^{\beta} v_\sigma{}^2 + w^2/t + \sum x_\tau{}^2 = (np - n + 1)/t.$$

Furthermore we quote the following results which are useful to determine the degrees of ordinary irreducible characters.

Theorem A.[5] *If $\mathfrak{G}$ is a group satisfying the condition* (∗), *then we find all representations of n in the form* $n = (h^{(\nu)} u^{(\nu)} p + u^{(\nu)2} + u^{(\nu)} + h^{(\nu)})/(u^{(\nu)} + 1)$ *with positive integers* $u^{(\nu)}$, $h^{(\nu)}$. *The degrees of the irreducible representations of $\mathfrak{G}$, as far as they are prime to p, can only have some of the values*

---

4) R. Brauer, On groups whose order contains a prime number to the first power I, II, Amer. Math. Soc. 54 (1942).

5) Cf. [I], Theorem 7.

$$a_\rho = 1, \qquad a_\rho = u^{(\nu)}p+1, \quad a_\rho = np+1,$$
$$b_\sigma = p-1, \qquad b_\sigma = v^{(\nu)}p-1,$$
$$c = (np+1)/t, \quad c = (u^{(\nu)}p+1)/t, \quad c = (p-1)/t, \quad c = (v^{(\nu)}p-1)/t$$

where $v^{(\nu)}$ is set equal to $(n-h^{(\nu)})/u^{(\nu)}$.

Theorem B.[6] *Let $\mathfrak{G}$ be a group satisfying the condition $(*)$. If $\mathfrak{G}$ possesses an irreducible representation of degree $p-1$, then either the number t is even or the index of the commutator subgroup $\mathfrak{G}'$ in $\mathfrak{G}$ is even.*

Theorem C.[7] *Let $\mathfrak{G}$ be a non-cyclic simple group satisfying the condition $(*)$. If the exceptional degree c in $B_1(p)$ satisfies condition $c \leq (p+1)/2$, then $\mathfrak{G} \simeq LF(2, p)$, $(p \neq 2, 3)$.*

If $\mathfrak{G}$ coincides with its commutator subgroup $\mathfrak{G}'$, then the 1-character A_1 is the only character of degree 1. It follows that $p-1 \neq t$, thus, in particular $p \neq 2$.

2. Proof of the theorem.

We may assume that $(p+3)/2 \leq n < p+2$, because Brauer proved[8] that, if $n < (p+3)/2$, t must be even.

Lemma 1. *Under assumptions $(*)$, $(**)$ and $n < p+2$, $\mathfrak{G}$ must be simple.*

Proof. This is a direct consequence of Theorem 5 and Corollary 6 in [1].

Lemma 2. *Under assumptions $(*)$ and $(p+3)/2 \leq n < p+2$, n is represented uniquely*

$$(4) \qquad n = (up+u^2+u+1)/(u+1),$$

where u is a positive integer.

Proof. We set $F(p, u^{(\nu)}, h^{(\nu)}) = (u^{(\nu)}h^{(\nu)}p+u^{(\nu)^2}+u^{(\nu)}+h^{(\nu)})/(u^{(\nu)}+1)$. For $h > 0$, $n = F(p, u, h)$ is monotone increasing in variable u.

Lemma 3. *Under the assumptions of the theorem, the degree b_σ of the representation $\mathfrak{B}_\sigma$ (if it may appear) must be equal to $(n-1)p/u-1$. And*

$$(5) \quad b_\sigma = (n-1)p/u-1 = (p+u)p/(u+1)-1 = (p-1)(p+u+1)/(u+1).$$

---

6) Cf. [I], Theorem 9.

7) Cf. H. F. Tuan, On groups whose orders contain a prime number to the first power, Ann. of Math. 45 (1944), Theorem 4.

8) Cf. [I], Theorem 10.

Proof. This is a direct consequence of Theorem A and B. According to (4), b_σ is decomposed as above.

Lemma 4. *Under assumptions* (∗), (∗∗) *and* $n < p+2$, *holds* $t \neq 1$, except the case $\mathfrak{G} \cong LF(2, 2^2)$.

Proof. Assume $t = 1$. Then we can choose $\mathfrak{C}$ among p irreducible representations of degree not divisible by p.

First we shall prove that $\mathfrak{G}$ does not possess the representation $\mathfrak{A}_\rho$ of degree $a_\rho = np + 1$.

If $\mathfrak{G}$ possesses at least two such representations $\mathfrak{A}_\rho$, then from (3)

$$2n^2 < np - n + 1, \quad 2n^2 \leq np - n, \quad n \leq (p-1)/2.$$ This is impossible under the assumption $t = 1$.

Hence, if $\mathfrak{G}$ possesses one such representation $\mathfrak{A}_\rho$ then other representations of type $\mathfrak{A}_\rho$ must have the degree $a_\rho = up + 1$ or 1. So, from (3),

$$n^2 + (p-y-2) u^2 + y(n-1)^2/u^2 + \sum x_\tau^2 = np - n + 1, \quad y = \beta \text{ or } \beta + 1.$$

Using (4), we obtain

$$y(p^2 + 2up - u^4 - 2u^3) \leq up^2 - (u^4 + 3u^3 + 2u^2 + u - 1) p + u^4 + u^3 - 2u^2 - 2u - 1.$$

Now we assume $y \geq u$. Then from $n < p+2$, we have $p > u^2$.[9] The above inequality implies

$$p(u^4 + 3u^3 + 4u^2 + u - 1) \leq u^5 + 3u^4 + u^3 - 2u^2 - 2u - 1,$$

hence

$$3u^3 + 3u^2 + u + 1 < 0.$$

This is impossible, so must hold $y < u$.

While, from (2)

$$1 + n + u(p-y-2) = y(p+u)/(u+1),$$

$$p(u^2 + 2u) - u^2 + 2 = y(p + u^2 + 2u).$$

Since

$$y < u, \quad p(u^2 + u) < u^3 + 3u^2 - 2.$$

This is impossible because $p > u+2$.

Thus, then, $B_1(p)$ consists of one 1-character A_1, $(p-y-1)$ characters $A_\rho(\rho \neq 1)$ of degree $a_\rho = up + 1$ and y characters B_σ of degree $b_\sigma = (p+u)p/(u+1) - 1$. Since $b_\sigma = (p-1)(p+u+1)/(u+1)$ and $p > u^2$, $p-1 \equiv 0 \pmod{(u+1)}$. And so $up + 1 \equiv 0 \pmod{(u+1)}$.

Furthermore, from assumption (∗)

$$g = p(p-1)(1+np) = p(p-1)(up+1)(p+u+1)/(p+1).$$

From (2), $1 + \sum_{\rho \neq 1} a_\rho = \sum_\sigma b_\sigma$, this means a_ρ and b_σ are relatively prime.

---

9) Since $n < p+2$ and from (4), we obtain $(up + u^2 + u + 1)/(u+1) \leq p + 1$. Then $p \geq u^2$. But the equality sign does not hold because p is a prime number.

Hence it follows that for any prime l dividing $up+1$ the characters $A_\rho(\rho \neq 1)$ are of highest kind. This implies

$$A_\rho(L) = 0 \quad \rho \neq 1 ,$$

for elements L of $\mathfrak{G}$ whose orders are divisible by l. For the prime m dividing b_σ the character B_σ are of highest kind. Hence

$$B_\sigma(M) = 0 ,$$

for elements M of $\mathfrak{G}$ whose orders are divisible by m.

On the other hand, the normalizer $\mathfrak{N}(\mathfrak{P})$ of a p-Sylow subgroup $\mathfrak{P}$ contains an element Q of order $p-1$. Since $(p-1)/(u+1)>1$,[10] and $(up+1)/(u+1)>1$, Q must be the element both of type L and of type M.

This contradicts relation (2). Thus $t \neq 1$ is proved.

Corollary 1. *Under the assumptions of the theorem, $\mathfrak{G}$ does not possess the representation $\mathfrak{A}_\rho$ of degree $np+1$.*

Proof. From the lemma, it is sufficient to prove this in the case $t \geq 3$. Then from (3)

$$n^2+1/t < (np+n+1)/t ,$$
$$n < (p-1)/t \leq (p-1)/3 .$$

This is impossible because $t \not\equiv 0 \pmod{2}$

Corollary 2. *Under the assumptions of the theorem, $p>3$, except $LF(2, 2^2)$.*

Proof. If $p=3$, then $(p-1)/t=2$ or 1, i. e. $t=1$ or $p-1=t$, this is a contradiction.

Lemma 5. *Under the assumptions of the theorem, $\mathfrak{G}$ does not possess the representation $\mathfrak{C}$ of degree $c = (up+1)/t$, for $p>3$.*

Proof. If $\mathfrak{G}$ possesses the representation $\mathfrak{C}$ of this degree, then $B_1(p)$ must consist of the followings: one 1-character A_1, $(p-1)/t-\beta-1$ characters $A_\rho(\rho \neq 1)$ of degree $a_\rho = up+1$, β characters B_σ of degree $b_\sigma = (n-1)p/u-1$ and t characters $C^{(\nu)}$ of degree $c = (up+1)/t$.

From (5), as in the proof of lemma 4, $p-1 \equiv 0 \pmod{(u+1)}$. We set $p-1 = q(u+1)$, then $a_\rho = up+1 = (u+1)(uq+1)$. Since, from (2)′, $u+1 \equiv 0 \pmod{t}$, we can set $u+1 = st$. Then $g = p(p-1)(up+1)$ $(p+u+1)/t(u+1) = (qst+1)qs(qst-q+1)(qst+st+1)$. But $a_\rho = st(qst$

---

10) If $p \leq u+2$, then $u^2 < p \leq u+2$. This means $u=1$. But $y < u^2+u$. This is the excepted case.

11) If all A_ρ, except $\rho=1$, do not appear in $B_1(p)$, then from (2)′ $(u+1)/t=(p-1)/t-1)(p+u)/(u+1)$. Substituting as above, $s=(qs-1)(q+1)$. This implies $s=2$ and $q=1$. We obtain $u+1=2t$ and $p-1=2t$, then $p=u+2$. On account of our foot-note 10), this is impossible.

$-q+1$) must divide $g^{11)}$, hence $q \equiv 0 \pmod{t}$. And we set again $q = kt$. On substituting these values in (2), we obtain

$$1+(\alpha-1)\,st\,(kst^2-kt+1)+s\,(kst^2-kt+1) = \beta\,kt\,(kst^2+st+1)\,.$$

This means $$(s, k) = 1\,, \quad (s, t) = 1\,.$$

On the other hand $\quad g = (kst^2+1)\,kst\,(kst^2-kt+1)\,(kst^2+st+1)\,.$

If $s \neq 1$, then the characters $A_\rho(\rho \neq 1)$ and $C^{(\nu)}$ are of highest kind for any prime l dividing s. This implies

$$A_\rho(L) = 0 \quad \text{for} \quad \rho \neq 1\,, \; C^{(\nu)}(L) = 0$$

for elements L of $\mathfrak{G}$ whose orders are divisible by l. For the prime m dividing t the characters B_σ are of highest kind. Hence

$$B_\sigma(M) = 0$$

for elements M of $\mathfrak{G}$ whose orders are divisible by m.

But the normalizer $\mathfrak{N}(\mathfrak{P})$ of a p-Sylow subgroup $\mathfrak{P}$ contains an element Q of order $(p-1)/t = kst$. Hence $A_\rho(Q) = 0$ $(\rho \neq 1)$, $C^{(\nu)}(Q) = 0$ and $B_\sigma(Q) = 0$. This contradicts (2).

If $s = 1$, then $u+1 = t$. On substituting these values in $(2)'$, we obtain

$$(\alpha-1)\,u+(u+1)/t = \beta\,(p+u)/(u+1)\,,$$

$$(\alpha-1)(t-1)+1 = \beta\,(kt+1)\,.$$

Then $(\alpha-1)(-1)+1 \equiv \beta \pmod{t}$ and this gives $2 \equiv \alpha+\beta \pmod{t}$. Since $\alpha+\beta = (p-1)/t = kt$, $2 \equiv 0 \pmod{t}$. This is a contradiction.

Lemma 6. *Under the assumptions of the theorem, $\mathfrak{G}$ does not possess the representation $\mathfrak{C}$ of degree $c = (np+1)/t$.*

Proof. If $\mathfrak{G}$ possesses the representation $\mathfrak{C}$ of this degree, then $B_1(p)$ must consist of the followings: one 1-character A_1, $(p-1)/t-\beta-1$ characters $A_\rho(\rho \neq 1)$ of degree $a_\rho = up+1$, β characters B_σ of degree $b_\sigma = (n-1)p/u-1$ and t characters $C^{(\nu)}$ of degree $c = (np+1)/t$.

From (5), as in the proof of lemma 5, we can set $p-1 = q\,(u+1)$. Then

$$g = (uq+u+1)\,q\,(u+1)\,(uq+1)\,(uq+q+u+2)/t\,,$$

$$a_\rho = (u+1)\,(uq+1)\,, \quad b_\sigma = q\,(uq+q+u+2) \quad \text{and}$$

$$c = (uq+1)\,(uq+q+u+2)/t\,.$$

If the character $A_\rho(\rho \neq 1)$ exists really, then a_ρ must divide g. Then, it follows that $uq+q+u+2 \equiv 0 \pmod{t}$.[12] From $(2)'$ $n+1 \equiv 0 \pmod{t}$.

---

12) From the form of c, we set $t=t_1t_2$, $uq+1=t_1t_1'$ and $uq+q+u+2=t_2t_2'$. Since a_p divides g, $qt_2' \equiv 0 \pmod{t_1}$. We get $t_2' \equiv 0 \pmod{t_1}$, because $(q, t_1)=1$. This means that $uq+q+u+2 \equiv 0 \pmod{t}$.

Hence $q \equiv 0$ (mod t). On the other hand, the character B_σ surely exists and its degree divides g. Hence $u+1 \equiv 0$ (mod t). This is a contradiction.

If the character $A_\rho(\rho \neq 1)$ does not exist, then taking the forms of b_σ and c in account, we obtain that $u+1 \equiv 0$ (mod t) and $uq+1 \equiv 0$ (mod t).[13] We set again $u+1 = kt$ and $uq+1 = st$. It follows from (2) that

$$1 + s(st + kt + q) = (qk-1) q (st + kt + q).$$

This is a contradiction. Thus we see that $\mathfrak{G}$ does not possess the representation $\mathfrak{C}$ of degree $(np+1)/t$, q. e. d.

From Theorem C, $\mathfrak{G}$ can not possess the exceptional characters of degree $c = (p-1)/t$, because t must be even in $LF(2, p)$. So from Theorem A, the following is the only possible case.

Lemma 7. *Under the asumptions of the theorem, $\mathfrak{G}$ possesses the representations $\mathfrak{C}$ of degree $c = \dfrac{(n-1)p/u-1}{t}$ and p is of the form $2^\mu-1$ and $\mathfrak{G} \cong LF(2, 2^\mu)$, for $p > 3$.*

Proof. If $\mathfrak{G}$ possesses the representation $\mathfrak{C}$ of this degree, then $B_1(p)$ consists of the followings: one 1-character A_1, $(p-1)/t - \beta - 1$ characters $A_\rho(\rho \neq 1)$ of degree $a_\rho = up+1$, β characters B_σ of degree $b_\sigma = (n-1)p/u-1$ and t characters $C^{(\nu)}$ of degree $c = \dfrac{(n-1)p/u-1}{t}$.

Applying analogous method as in the proof of Lemma 5, we shall conclude that $\beta = 0$. First we set $p-1 = kt(u+1)$. As b_σ divides g, we can set again $u+1 = st$. From (2), if $k \neq 1$, then the characters $A_\rho(\rho \neq 1)$ are of highest kind for any prime dividing t and the characters B_σ and $C^{(\nu)}$ are of highest kind for any prime dividing k. This contradicts that $\mathfrak{N}(\mathfrak{P})$ has an element Q of order $(p-1)/t$. If $k = 1$, then $p = st^2+1$ and $u = st-1$. Then from $n < p+2$, we obtain $t(s-1) < 2$. This is impossible.

Hence $\mathfrak{G}$ does not possess the representation $\mathfrak{B}_\sigma$. Then, we can set again $p-1 = kt(u+1)$. From (2)' $(k(u+1)-1)u = k$, this means $k(u^2+u-1) = u$. Then we can conclude $u = 1$ and $k = 1$. Substituting these values in n, we obtain $n = (p+3)/2$.

Thus, by the following lemma we have Lemma 7.

---

13) From the form of c, we can set $uq+1=t_1t_1'$, $t=t_1t_2$ and $uq+q+u+2=t_2t_2'$. But (2)' means $n+1\equiv0$ (*mod* t), then we set again $u_1+u+2=t't$. Comparing these, we find $q\equiv0$ (*mod* t_2) and $u+2\equiv0$ (*mod* t_2). Since b_σ divides g, we find $(u+1)t_1'\equiv0$ (*mod* t_2) and $t_1'\equiv0$ (*mod* t_2). This means $uq+1\equiv0$ (*mod* t). This contradicts $q\equiv0$ (*mod* t_2). Then t_2 must be equal to 1. Hence $uq+1\equiv0$ (*mod* t). On the other hand $p-1=q(u+1)\equiv0$ (*mod* t) and $(q, t)=1$, hence $u+1\equiv0$ (*mod* t).

Lemma 8. *Under the assumptions* (*), (**), $n = (p+3)/2$ *and* $t \not\equiv 0$ (mod 2), *p is of the form* $2^\mu - 1$ *and* $\mathfrak{G} \cong LF(2, 2^\mu)$.

Proof. We can prove this lemma in an analogous manner as in Brauer's main theorem.[14]

As we proved above, $\mathfrak{G}$ does not prossess the representation $\mathfrak{B}_\sigma$. Since $n = (p+3)/2$, we obtain easily $t = (p-1)/2$ and $g = p(p+1)(p+2)$. Furthermore $a_1 = 1$, $a_2 = p+1$ and $c = p+2$ are the full table of degrees of irreducible characters belonging to $B_1(\mathrm{p})$.

We can classify the elements of $\mathfrak{G}$ into four distinct sets: (I) the unit element, (II) the elements of order p, (III) the elements L whose orders are divisible by at least one prime factor of $p+1$, (IV) the elements M whose orders are divisible by at least one prime factor of $p+2$. Now we decompose each irreducible character of $\mathfrak{G}$ into the irreducible characters of $\mathfrak{N}(\mathfrak{P}) = \{P, Q\}$. Considering their linear characters only, we can conclude from the orthogonality relations for group characters that any L is conjugate with Q in $\mathfrak{G}$. Since Q has order 2, $p+1$ must be a power of 2, say $p+1 = 2^\mu$, $\mu > 2$. At the same time the 2-Sylow subgroup $\mathfrak{L}$ of $\mathfrak{G}$ must be an abelian group of type $(2, 2, \cdots, 2)$. We may assume that $\mathfrak{L}$ contains Q. Then we obtain that the normalizer $\mathfrak{N}(\mathfrak{L})$ has the index $p+2$ in $\mathfrak{G}$.

Hence it follows that $\mathfrak{G}$ possesses a permutation representation of degree $p+2$. As easily be seen, $\mathfrak{G}$ is three times transitive, then from a theorem of Zassenhaus,[15] $\mathfrak{G} \cong LF(2, p+1)$. This finishes the proof of Lemma 8.

By these facts proved in § 2, we can examine all the possible cases which may occur under those assumptions: (*), (**), $n < p+2$ and $t \not\equiv 0$ (mod 2). Thus our main theorem is proved completely.

<div align="center">(Received March, 16, 1952)</div>

---

14) Cf. [1], Theorem 10.

15) Cf. H. Zassenhaus: Kennzeichung endlicher linearer Gruppen als Permutationsgruppen, Hamb. Abh. 11 (1936).