ON SIMPLE GROUPS OF FINITE ORDER. I

RICHARD BRAUER AND HSIO-FU TUAN

1. **Introduction.** Using the theory of representations of groups we have obtained a number of results for simple groups of certain types of orders. In the present paper, we shall prove the following result: If $\mathfrak{G}$ is a (non-cyclic) simple group of order $g=pq^bg^*$, where p and q are two primes and where b and g^* are positive integers with $g^*<p-1$, then either $\mathfrak{G}\cong LF(2, p)$[1] with $p=2^m\pm 1$, $p>3$, or $\mathfrak{G}\cong LF(2, 2^m)$ with $p=2^m+1$, $p>3$; conversely, these groups satisfy the assumptions. As an application, we determine all simple groups of order prq^b, where p, r, q are primes and where b is a positive integer. The only simple groups of this type are the well known groups of orders 60 and 168.

2. **Some known results concerning representations of groups.** 1. In this section, some known theorems are given without proof. Most of these results, which are needed in the following, have been obtained in the theory of modular representations of groups. However, all the statements are concerned with the *ordinary* group characters.[2]

2. If $\mathfrak{G}$ is a group of order g containing k classes $K_1, \cdots, K_\mu, \cdots, K_k$ of conjugate elements, then there exist exactly k distinct irreducible characters $\zeta_1(G), \cdots, \zeta_\mu(G), \cdots, \zeta_k(G)$, where G denotes a variable element of $\mathfrak{G}$. If we restrict G to a subgroup $\mathfrak{M}$ of order m of $\mathfrak{G}$, then each $\zeta_\mu(G)$ may be considered as a (reducible or irreducible) character of $\mathfrak{M}$. From the orthogonality relations for the characters of $\mathfrak{M}$, it follows that

$$\sum{}'\zeta_\mu(G) \equiv 0 \pmod{m}, \tag{2.1}$$

where the sum extends over all elements G of $\mathfrak{M}$. More generally, the same congruence holds, if ζ is a linear combination of the ζ_μ's with coefficients which are algebraic integers.

3. Let p be a prime number and let $\mathfrak{p}$ be a prime ideal divisor of p in the algebraic number field generated by all $\zeta_\mu(G)$. Denote by $h(G)$ the number of elements in the class K_μ containing G. If ζ_μ has degree z_μ, the number $h(G)\zeta_\mu(G)/z_\mu$ is an algebraic integer. Two characters ζ_μ and ζ_ν belong to the same *p-block*, if

Presented to the Society, September 17, 1945; received by the editors March 27, 1945.

[1] We use the notation of L. E. Dickson, *Linear groups*, Leipzig, 1901.

[2] The fundamental properties of group characters are given in a large number of books. Here we mention only: W. Burnside, *The theory of groups of finite order*, 2d ed., Cambridge, 1911.

$$h(G)\zeta_\mu(G)/z \equiv h(G)\zeta_\nu(G)/z \pmod{\mathfrak{p}}, \tag{2.2}$$

for all G in $\mathfrak{G}$. In this manner, the k characters are distributed into a certain number of p-blocks $B_1(p)$, $B_2(p)$, $\cdots$. The *first p-block* $B_1(p)$ will always be taken as the block containing the 1-character $\zeta_1(G)=1$ (for all G). If for all characters ζ_μ of $B_\sigma(p)$ the degree z_μ of ζ_μ is divisible by a power p^α while at least one of the degrees z_μ is not divisible by $p^{\alpha+1}$, then $B_\sigma(p)$ is a block of *type* α. In particular, $B_\sigma(p)$ is of the *lowest type* if $\alpha=0$.

An element G is *p-regular*, if its order is prime to p; and G is p-singular in the other case. For every p-block $B_\sigma(p)$ we have[3]

$$\sum_\mu \zeta_\mu(P)\zeta_\mu(Q) = 0, \tag{2.3}$$

where ζ_μ ranges over all characters of $B_\sigma(p)$ and where P is any p-singular element of $\mathfrak{G}$ and Q any p-regular element.

If we let ζ_μ range over all the k characters of $\mathfrak{G}$, then the orthogonality relations for group characters show that the sum in (2.3) vanishes for any two elements P and Q for which P and Q^{-1} are not conjugate. If P and Q^{-1} are conjugate, the sum does not vanish.

4. If we assume that the prime p divides g to the first power,[4] we can make more definite statements. It will be sufficient to restrict our attention to the first p-block $B_1(p)$. There exists a divisor t of $p-1$ such that $B_1(p)$ consists of $w=(p-1)/t$ "non-exceptional" characters $\zeta_1(G), \cdots, \zeta_w(G)$ and t "exceptional" characters $\zeta_{w+1}(G), \cdots, \zeta_{w+t}(G)$. The latter have all the same degree z_{w+1}. To each of these characters $\zeta_i(G)$, there belongs a certain sign $\delta_i=\pm 1$ such that the following relations hold:

$$z_i \equiv \delta_i \pmod{p} \qquad \text{for } i = 1, 2, \cdots, w; \tag{2.4}$$

$$tz_{w+1} \equiv \delta_{w+1} \pmod{p}; \tag{2.5}$$

$$\sum_{\mu=1}^{w+1} \delta_\mu z_\mu = 0 \qquad (\delta_1 = z_1 = 1). \tag{2.6}$$

Moreover, for p-singular elements P of G, we have

$$\zeta_i(P) = \delta_i \qquad (i = 1, 2, \cdots, w). \tag{2.7}$$

There exist elements of order $w=(p-1)/t$ in $\mathfrak{G}$, hence

---

[3] R. Brauer and C. Nesbitt, University of Toronto Studies, Mathematical Series, No. 4, 1937, Theorem VIII, p. 21.

[4] For the results quoted in this part, cf. R. Brauer, Amer. J. Math. vol. 64 (1942) pp. 401–420, especially p. 420, §8, and p. 417, Formula (47a).

$$g \equiv 0 \pmod{w}. \tag{2.8}$$

5. If $\mathfrak{G}$ coincides with its commutator subgroup $\mathfrak{G}'$, in particular if $\mathfrak{G}$ is simple and non-cyclic, then $\zeta_1 = 1$ is the only character of degree 1. It follows that the number w above must be larger than 1. Indeed, if we had $w = 1$, the equation (2.6) would read $\delta_1 z_1 + \delta_2 z_2 = 0$, and as $\delta_1 = 1$, $\delta_2 = \pm 1$, $z_1 = 1$, it would follow that the positive number z_2 must be 1 which is impossible. Thus, in particular, $p \neq 2$.

6. Finally we quote the following results obtained in previous papers which yield characterizations of certain groups $LF(2, m)$.

THEOREM A.[5] *If a non-cyclic simple group $\mathfrak{G}$ has an order which contains the prime p to the first power and if the exceptional degree z_{w+1} in the first p-block $B_1(p)$ satisfies the condition $z_{w+1} \leqq (p+1)/2$, then $\mathfrak{G} \cong LF(2, p)$ $(p \neq 2, 3)$.*

THEOREM B.[6] *If a non-cyclic simple group $\mathfrak{G}$ has an order g of the form*

$$g = (p^b - 1)p(1 + mp)/\tau,$$

where p is a prime and where τ and m are non-negative integers such that τ divides $p-1$ and $m < (p+3)/2$, then either $\mathfrak{G} \cong LF(2, p-1)$ and p is a prime of the form $p = 2^b + 1 > 3$, or $\mathfrak{G} \cong LF(2, p)$ and p is any prime larger than 3.

3. **Proof of the main result.** We now begin to prove the following theorem.

THEOREM 1. *If $\mathfrak{G}$ is a simple group of order*

$$g = pq^b g^*, \tag{3.1}$$

where p and q are two primes and where b and g^* are positive integers with

$$g^* < p - 1, \tag{3.2}$$

then either $\mathfrak{G} \cong LF(2, p)$ with $p = 2^m \pm 1$, $p > 3$, or $\mathfrak{G} \cong LF(2, 2^m)$ with $p = 2^m + 1$, $p > 3$. Conversely, these groups satisfy the assumptions.

REMARK. It may be added that for both alternatives we have $q = 2$ and m is the highest exponent of q dividing g.

PROOF. 1. If g as given by (3.1) is the order of a non-cyclic simple

---

[5] H. F. Tuan, Ann. of Math. vol. 45 (1944) pp. 110–140, especially p. 135, Theorem 4, and p. 139, Formulas (10.i) and (10.i′) for i = 1, · · · , 7. Notice that Formulas (10.2′) and (10.3′) are printed there in the wrong order.

[6] R. Brauer, Ann. of Math. vol. 45 (1944) pp. 57–79, especially p. 76, Theorem 11.

group $\mathfrak{G}$, then by (3.2) certainly $p \neq 2$ and without restriction we may assume that

$$(g^*, q) = 1. \tag{3.3}$$

The case $p = q$ is impossible on account of Sylow's theorem since the p-Sylow subgroup of a group $\mathfrak{G}$ of order $g = p^{b+1}g^*$ would be normal in $\mathfrak{G}$, if $g^* < p-1$. Hence $p \neq q$, and p divides g only to the first power. From (2.6) it follows that in the first p-block $B_1(p)$ we have a degree $n \neq 1$ which is prime to q. Then

$$n \mid g^*, \tag{3.4}$$

and hence $n < p-1$. This shows that n must be the exceptional degree $n = z_{w+1}$ (cf. (2.5)), since all the other degrees are congruent to ± 1 (mod p) according to (2.4).

2. If $n \leqq (p+1)/2$, Theorem A gives $\mathfrak{G} \cong LF(2, p)$, $p \neq 3$, and $g = p(p+1)(p-1)/2$. Hence

$$(p+1)(p-1) = 2q^b g^*.$$

As $p+1$ and $p-1$ have the greatest common divisor 2, it follows that one of the two numbers $p-1$ and $p+1$ is divisible by q^b. The other number then divides $2g^*$. But $p \pm 1 > g^*$ by (3.2) and we have one of the two cases

$$\text{(I)} \qquad p - 1 = q^b, \qquad p + 1 = 2g^*;$$

$$\text{(II)} \qquad p + 1 = q^b, \qquad p - 1 = 2g^*.$$

In either case, $q = 2$, and this leads to the first alternative of our theorem.

3. We may now assume that

$$p - 1 > n > (p+1)/2. \tag{3.5}$$

By (2.5), we have $nt \equiv \pm 1$ (mod p) where t divides $p-1$. It follows that $n \equiv \mp (p-1)/t$ (mod p), and (3.5) gives

$$n = p - (p-1)/t. \tag{3.6}$$

From (2.8), it follows that we may set

$$(p-1)/t = q^\beta h, \tag{3.7}$$

$$h \mid g^*, \tag{3.8}$$

where $\beta \leqq b$ is a non-negative integer. Combining (3.6) and (3.7), we obtain

$$n = p - q^\beta h, \tag{3.9}$$

which implies $(n, h)=1$. Now (3.4) and (3.8) give

$$nh \mid g^*. \tag{3.10}$$

The relations (3.6) and (3.7) also yield

$$1 + n = 1 + p - (p-1)/t = 1 + (1 + tq^\beta h) - q^\beta h,$$

$$1 + n = 2 + q^\beta h(t-1). \tag{3.11}$$

4. If $\beta=0$, then (3.9) gives $p=n+h$. On the other hand, (3.10) and (3.2) show that $nh \leqq g^* < p-1$. Hence $nh < n+h$, and then at least one of the two positive integers n, h must be 1. But we have $n \neq 1$, and therefore h must be equal to 1. However, this would lead to $n=p-1$, which contradicts (3.5). Thus,

$$\beta > 0. \tag{3.12}$$

5. From (3.6), it follows that $nt \equiv 1 \pmod{p}$. Since $n = z_{w+1}$, we have $\delta_{w+1}=1$ in (2.5). The relation (2.6) then has the form

$$(1 + n + \cdots) - (\cdots) = 0, \tag{3.13}$$

where the missing terms are the non-exceptional degrees greater than 1 of the first p-block $B_1(p)$.

If $q \neq 2$, then (3.11) shows that at least one of these degrees must be prime to q, and hence a divisor of $g^* < p-1$. But the only degree m with $1 < m < p-1$ is the exceptional degree (cf. (2.4)). This is a contradiction; we must have

$$q = 2. \tag{3.14}$$

6. Assume next that $\beta \geqq 2$. Then (3.11) shows that $1+n \equiv 2 \pmod 4$, and at least one of the missing degrees in (3.13) is not divisible by 4. This degree then has the form $m=\mu$ or $m=2\mu$ with $\mu \mid g^*$. Hence $m \leqq 2g^* < 2(p-1)$. On the other hand, we have $m \equiv \pm 1 \pmod{p}$ on account of (2.4). As $m \neq 1$, the only possibilities are $m = p \pm 1$. The number g^* is a multiple of $m/2$, and from (3.2) it now follows that $g^* = (p \pm 1)/2$. But then the divisor n of g^* is at most $(p \pm 1)/2$ which contradicts (3.5).

Hence the only possible case is the case $\beta = 1$.

7. For $q=2$, $\beta=1$, the equation (3.9) reads

$$n = p - 2h. \tag{3.15}$$

The number g^* now is odd and so are its divisors n and h. Combining (3.10), (3.2) and (3.15), we find

$$nh \leqq g^* < p - 1 < n + 2h. \tag{3.16}$$

If $h \neq 1$, then $h \geqq 3$ and (3.16) gives

$$n > (n-2)h \geqq 3n - 6,$$

which is impossible as n is odd and $n \neq 1$. This proves that $h = 1$. Now (3.15) reads $n = p-2$. The multiple g^* of n then must be $p-2$; we have

$$g^* = n = p - 2, \tag{3.17}$$

$$g = p2^b(p-2). \tag{3.18}$$

From (3.6), it follows that

$$w = (p-1)/t = 2.$$

In the equation (2.6) only three terms appear. The first two terms are 1 and $n = p-2$. The missing term therefore is $-(p-1)$ and (2.6) reads

$$1 + (p-2) - (p-1) = 0. \tag{3.19}$$

As the degree of an irreducible character, the number $p-1$ is a divisor of g. Then (3.18) shows that $p-1$ is a power of 2, say

$$p - 1 = 2^c, \qquad c \leqq b. \tag{3.20}$$

8. In order to finish the proof, we need three lemmas which we state here in a more general form than actually needed for our present purpose. The proof of these lemmas will be given in the next section.

LEMMA 1. *Let $\mathfrak{G}$ be a group which is identical with its commutator subgroup $\mathfrak{G}'$, and assume that the first p-block $B_1(p)$ contains an irreducible* 1-1 *representation $\mathfrak{Z}$ of degree $z < 2p$. Then the order of the centralizer $\mathfrak{C}(\mathfrak{P})$ of a p-Sylow subgroup $\mathfrak{P}$ of $\mathfrak{G}$ is a power of p.*

LEMMA 2. *If a group $\mathfrak{G}$ with center* 1 *has an irreducible* 1-1 *representation $\mathfrak{Z}$ of degree $z = p^r$ (p a prime) and if the center $\mathfrak{C}$ of the p-Sylow subgroup $\mathfrak{P}$ of $\mathfrak{G}$ has the order p^s, then $\mathfrak{Z}$ belongs to a p-block of type at least s. In particular, $r \geqq s$. Also, $s \geqq 1$ except when $\mathfrak{G} = 1$.*

LEMMA 3. *Let $\mathfrak{G}$ be a group of order $g = p^a q^b g^*$ where p and q are different primes and a, b and g^* are positive integers, $(g^*, pq) = 1$. Assume that $\mathfrak{G}$ does not contain elements of order pq. Then for every p-singular element P of $\mathfrak{G}$, we have*

$$\sum{}' z_\mu \zeta_\mu(P) \equiv 0 \pmod{q^b},$$

where the sum extends over all characters ζ_μ which belong simultaneously to a fixed p-block $B_\sigma(p)$ and to a fixed q-block $B_\tau(q)$. Here, z_μ denotes the degree of ζ_μ.

9. Assuming these lemmas, we conclude the proof of Theorem 1 as follows:

Lemma 1 shows that under the assumptions of the theorem, $\mathfrak{G}$ does not contain any element of order $2p$. From Lemma 2, it follows that the degree $p-1=2^c$ in (3.19) belongs to a 2-block $B_\tau(2)$ which is not of the lowest kind. Now apply Lemma 3 to the first p-block $B_1(p)$ and the 2-block $B_\tau(2)$. The only character in common to these two blocks is the character ζ of degree $p-1$ in (3.19), since the other degrees occurring in $B_1(p)$ are the odd numbers 1 and $p-2$ which therefore cannot occur in $B_\tau(2)$. Now the statement of Lemma 3 gives

$$z\zeta(P) = (p-1)\zeta(P) \equiv 0 \pmod{2^b}$$

for any p-singular element P of $\mathfrak{G}$. But (2.7) and (2.4) give $\zeta(P)=-1$, and hence $p-1\equiv 0 \pmod{2^b}$. Combining this with (3.20) and (3.18) we find

$$p - 1 = 2^b, \tag{3.21}$$

$$g = p(p-1)(p-2) = 2p(1 + p(p-3)/2). \tag{3.22}$$

Now Theorem B can be applied with $\tau=(p-1)/2$ and $m=(p-3)/2$. We have either $\mathfrak{G}\cong LF(2, p-1)$ with $p=2^b+1>3$ or $\mathfrak{G}\cong LF(2, p)$. In the second case, $g=p(p-1)(p+1)/2$. Comparison with (3.22) then gives $p=5$. In any case, $\mathfrak{G}$ is of the form stated in Theorem 1. As the converse is trivial, this finishes the proof.

4. **Proof of the lemmas.** To complete the proof of Theorem 1, it now remains to prove the three lemmas used and formulated in the preceding section.

Proof of Lemma 1. If ζ is the (irreducible) character of a 1-1 representation $\mathfrak{Z}$ of the first p-block $B_1(p)$, we have (cf. (2.2))

$$h(G)\zeta(G)/z \equiv h(G) \pmod{\mathfrak{p}}. \tag{4.1}$$

For all elements G of the centralizer $\mathfrak{C}(\mathfrak{P})$ of a p-Sylow subgroup $\mathfrak{P}$, the number $h(G)$ is prime to p and can therefore be cancelled in (4.1) and we have then

$$\zeta(G) \equiv z \pmod{\mathfrak{p}}. \tag{4.2}$$

Assume that the order of $\mathfrak{C}(\mathfrak{P})$ contains a prime factor $v\neq p$. Then $\mathfrak{C}(\mathfrak{P})$ contains a cyclic subgroup $\mathfrak{V}$ of order v. Now $\zeta(G)$ for G in $\mathfrak{V}$ may be considered as a (reducible) character of $\mathfrak{V}$ and the same is true for $\zeta^*(G)=z=1+1+\cdots+1$ (z terms). We cannot have $\zeta(G)=z$ for all G in $\mathfrak{V}$, as $\mathfrak{Z}$ then would represent every G in $\mathfrak{V}$ by the unit matrix while $\mathfrak{Z}$ is assumed to be a 1-1 representation. The

congruence (4.2) implies[7]

$$\zeta(G) = z_0 + p\theta(G), \tag{4.3}$$

where z_0 is the least non-negative residue of $z_0 \pmod{p}$ and where $\theta(G)$ is a reducible or irreducible character of $\mathfrak{V}$.

If the degree z of $\mathfrak{Z}$ is less than $2p$, the degree of $\theta(G)$ is 1. It follows that for every G in $\mathfrak{V}$, the matrix $\mathfrak{Z}(G)$ has z_0 characteristic roots 1, and p roots $\theta(G)$. If $\mathfrak{G}$ coincides with its commutator subgroup $\mathfrak{G}'$, every representation of $\mathfrak{G}$ represents elements of $\mathfrak{G}$ with matrices of determinant 1. Hence

$$1^{z_0} \cdot \theta(G)^p = 1.$$

But $\theta(G)$ is a vth root of unity with $(v, p) = 1$. It follows that $\theta(G) = 1$ and all characteristic roots of $\mathfrak{Z}(G)$ are 1. But this means that $\mathfrak{Z}(G) = I$ which gives a contradiction for $G \neq 1$. Hence, under the assumptions of Lemma 1, the order of $\mathfrak{C}(\mathfrak{P})$ cannot contain a prime factor $v \neq p$, and this proves Lemma 1.

PROOF OF LEMMA 2. Let $\mathfrak{Z}$ with the character ζ be an irreducible 1-1 representation of degree $z = p^r$ of $\mathfrak{G}$. If ζ belongs to a p-block $B = B(p)$ of type α, we may find a character ζ_0 of degree z_0 in B such that z_0 is divisible by p^α but not by $p^{\alpha+1}$. According to (2.2), we have for any element G of $\mathfrak{G}$,

$$h(G)\zeta(G)/z \equiv h(G)\zeta_0(G)/z_0 \pmod{\mathfrak{p}}. \tag{4.4}$$

Now, for any element G of the center $\mathfrak{C}$ of $\mathfrak{P}$, the number $h(G)$ is prime to p, and $z = p^r$ divides $\zeta(G)$ which is a sum of p^r roots of unity. A well known argument of Burnside[8] shows that either $\mathfrak{Z}(G)$ is a scalar multiple of I or $\zeta(G) = 0$. The first possibility cannot arise for $G \neq 1$, if the center of $\mathfrak{G}$ consists only of 1. In the case $\zeta(G) = 0$, (4.4) yields

$$\zeta_0(G) \equiv 0 \pmod{\mathfrak{p}p^\alpha} \qquad (\text{for } G \neq 1 \text{ in } \mathfrak{C}), \tag{4.5}$$

since $z_0 \equiv 0 \pmod{p^\alpha}$. On the other hand,

$$\zeta_0(1) = z_0. \tag{4.6}$$

Adding (4.6) and (4.5) for all elements $G \neq 1$ of $\mathfrak{C}$, we obtain

$$\sum \zeta_0(G) \equiv z_0 \pmod{\mathfrak{p}p^\alpha}, \tag{4.7}$$

[7] It follows from the orthogonality relations for group characters and (4.2) that $\zeta(G)$ contains every irreducible character of $\mathfrak{V}$ with a multiplicity divisible by p with the exception of the 1-character only. In the case of the 1-character, the multiplicity is congruent to $z \pmod{p}$.

[8] Burnside, p. 322, Theorem I.

where the sum extends over all elements G of $\mathfrak{C}$. The expression on the left side is divisible by the order p^s of $\mathfrak{C}$ (cf. (2.1)). Since $z_0 \not\equiv 0 \pmod{p^{\alpha+1}}$, the congruence (4.7) shows that $s \leqq \alpha$, and this proves the main assertion of Lemma 2. It is then clear that $r \geqq s$. If $s=0$, then g would be prime[9] to p and hence $r=0$, $z=1$. But then $\mathfrak{G}$ would be Abelian and would not have the center 1, except for $\mathfrak{G}=1$.

COROLLARY.[10] *If in Lemma 2 the p-Sylow subgroup is Abelian, then z must be the highest power of p which divides the order of $\mathfrak{G}$.*

PROOF OF LEMMA 3. Let P be a p-singular element of a group $\mathfrak{G}$, let $B_\sigma(p)$ be a fixed p-block of $\mathfrak{G}$ and set

$$\xi_\mu = \zeta_\mu(P) \quad \text{for} \quad \zeta_\mu \text{ in } B_\sigma(p), \qquad \xi_\mu = 0 \quad \text{for} \quad \zeta_\mu \text{ not in } B_\sigma(p). \tag{4.8}$$

The equation (2.3) can be written in the form

$$\sum_\mu \xi_\mu \zeta_\mu(Q) = 0. \tag{4.9}$$

Here Q is an arbitrary p-regular element of $\mathfrak{G}$, and we may let ζ_μ range over all characters of $\mathfrak{G}$. We can determine $a_1, a_2, \cdots, a_k$ from

$$\xi_\mu = \sum_\kappa a_\kappa \zeta_\mu(G_\kappa), \tag{4.10}$$

where $G_1, G_2, \cdots, G_k$ represent the different classes of $\mathfrak{G}$ (this because the determinant $|\zeta_\mu(G_\kappa)|$ $(\mu, \kappa = 1, 2, \cdots, k)$ does not vanish). Multiplication of (4.10) with $\zeta_\mu(Q)$ and addition over μ gives

$$\sum_\mu \xi_\mu \zeta_\mu(Q) = \sum_\kappa a_\kappa \sum_\mu \zeta_\mu(G_\kappa)\zeta_\mu(Q).$$

The expression on the left side vanishes on account of (4.9). The orthogonality relations for the group characters show that the inner sum on the right side is different from 0 only for that element G_κ which is conjugate to Q^{-1}. Hence $a_\kappa = 0$ when G_κ is conjugate to Q^{-1}. Now since Q^{-1} as well as Q may be any p-regular element, it follows that $a_\kappa = 0$ when G_κ is p-regular. It will consequently suffice to let G_κ in (4.10) range over all p-singular elements.

Take Q now as a q-singular element of $\mathfrak{G}$. Since $\mathfrak{G}$ does not contain elements of order pq, the element Q must be p-regular, and can therefore be used in (4.9). Applying (2.3) to the q-block $B_\tau(q)$ of $\mathfrak{G}$, we have for any q-regular element G_κ the equation

$$\sum_\rho {}^*\zeta_\rho(G_\kappa)\zeta_\rho(Q) = 0, \tag{4.11}$$

[9] Burnside, p. 119, Theorem I.

[10] R. Brauer, loc. cit. footnote 6, p. 78, Lemma 5.

where ζ_ρ ranges over all characters of $B_\tau(q)$. In particular, this will hold for p-singular elements G_κ, that is for all G_κ actually appearing in (4.10). Multiplication of (4.11) with a_κ and subsequent addition over all p-singular G_κ gives

$$\sum_\kappa \sum_\rho{}^* a_\kappa \zeta_\rho(G_\kappa)\zeta_\rho(Q) = 0.$$

On account of (4.10) this may be written in the form

$$\sum_\rho{}^* \xi_\rho \zeta_\rho(Q) = 0. \tag{4.12}$$

Set now

$$S(G) = \sum_\rho{}^* \xi_\rho \zeta_\rho(G) \tag{4.13}$$

for any G in $\mathfrak{G}$. Then $S(G)$ is a linear combination of the characters of $\mathfrak{G}$, the coefficients ξ_ρ are algebraic integers as follows from (4.8). On account of (4.12), $S(G)$ vanishes for all $G \neq 1$ belonging to a q-Sylow subgroup $\mathfrak{Q}$; we obtain

$$\sum S(G) = S(1) = \sum_\rho{}^* \xi_\rho z_\rho,$$

where G ranges over all elements of $\mathfrak{Q}$. The left side is a sum of the kind studied in (2.1) and hence it is divisible by the order q^b of $\mathfrak{Q}$. Consequently,

$$\sum{}^* \xi_\rho z_\rho \equiv 0 \pmod{q^b}.$$

Here, ρ ranges over those values for which ζ_ρ lies in $B_\tau(q)$. As defined in (4.8), ξ_ρ is 0 if ζ_ρ does not belong to $B_\sigma(p)$. We thus obtain

$$\sum{}' \zeta_\rho(P) z_\rho \equiv 0 \pmod{q^b},$$

here the sum extends over those values of ρ for which ζ_ρ belongs to both $B_\sigma(p)$ and $B_\tau(q)$. This proves Lemma 3.

COROLLARY. *If the order of a group $\mathfrak{G}$ is divisible by two different primes p and q, and if $\mathfrak{G}$ does not contain elements of order pq, then the first p-block $B_1(p)$ of $\mathfrak{G}$ and the first q-block $B_1(q)$ of $\mathfrak{G}$ have at least one character $\zeta_\mu \neq 1$ in common.*

5. **Simple groups of order prq^b.** We now prove the following theorem.

THEOREM 2.[11] *If a simple group $\mathfrak{G}$ has an order of the form $g = prq^b$*

[11] This result was announced without proof in R. Brauer, Proc. Nat. Acad. Sci. U. S. A. vol. 25 (1939) p. 290.

where p, q and r are primes and where b is a positive integer, then

$$\mathfrak{G} \cong LF(2, 5),\ g = 60, \quad \text{or} \quad \mathfrak{G} \cong LF(2, 7),\ g = 168.$$

PROOF. It follows from a well known theorem of Burnside[12] that the primes p, q, r must be distinct. As then both p and r must be odd, we may assume without restriction that $r<p-1$. Now Theorem 1 can be applied. Two cases are possible:

(I) $$g = prq^b = p(p-1)(p+1)/2, \qquad p = 2^b \pm 1;$$

(II) $$g = prq^b = p(p-1)(p-2), \qquad p = 2^b + 1;$$

with $q=2$ and $p\neq 3$. In both cases, g is divisible by 3 and hence $r=3$. In the first case, this gives

$$3\cdot 2^{b+1} = (p-1)(p+1).$$

Not both factors on the right are divisible by 4. Hence either $p+1$ or $p-1$ divides 6. Then $p=5$ or $p=7$ and this leads to $\mathfrak{G}\cong LF(2, 5)$ or $\mathfrak{G}\cong LF(2, 7)$. In the second case, we obtain

$$3\cdot 2^b = (p-1)(p-2).$$

It follows that the odd number $p-2$ must be 3 and this gives $p=5$, $\mathfrak{G}\cong LF(2, 4)\cong LF(2, 5)$. Thus Theorem 2 is proved.

UNIVERSITY OF TORONTO AND
PRINCETON UNIVERSITY

[12] Burnside, p. 323, Theorem I, Corollary 3.