THE MATHIEU GROUPS

R. G. STANTON

1. Introduction. An enumeration of known simple groups has been given by Dickson [17]; to this list, he made certain additions in later papers [15], [16]. However, with but five exceptions, all known simple groups fall into infinite families; these five unusual simple groups were discovered by Mathieu [21], [22] and, after occasioning some discussion [20], [23], [27], were relegated to the position, which they still hold, of freakish groups without known relatives. Further interest is attached to these Mathieu groups in virtue of their providing the only known examples (other than the trivial examples of the symmetric and alternating groups) of quadruply and quintuply transitive permutation groups.

Basically, the two important Mathieu groups are the group $\mathfrak{M}_{12}$ of order $m_{12} = 95040$ and the group $\mathfrak{M}_{24}$ of order $m_{24} = 244823040$. The other three Mathieu groups are subgroups of these two; $\mathfrak{M}_{11}$ is a subgroup of index 12 in $\mathfrak{M}_{12}$ whereas $\mathfrak{M}_{23}$ is a subgroup of index 24 in $\mathfrak{M}_{24}$ and $\mathfrak{M}_{22}$ is a subgroup of index 23 in $\mathfrak{M}_{23}$. Since the Mathieu groups are exceptional both in their simplicity and their multiple transitivity, it should be of interest to investigate whether they are the unique simple groups of their orders. Hence we shall consider the two groups $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$ and prove the following

MAIN THEOREM. *The only simple group of order m_{12} is the Mathieu group $\mathfrak{M}_{12}$; the only simple group of order m_{24} is the Mathieu group $\mathfrak{M}_{24}$.*

2. Definition of the Mathieu groups. A brief summary of the history of the Mathieu groups is provided by Witt [30]; we shall ignore the older permutation definition and give a more combinatorial one which is also due to Witt. This necessitates the introduction of the concept of a Steiner system [31].

A Steiner system $\mathfrak{S}(l, m, n)$ is defined to be a set of $\binom{n}{l}/\binom{m}{l}$ m-member clubs formed from n individuals who are subject to the proviso that every l persons must meet together in one club and one club only. Clearly one person will occur in $m\rho/n$ clubs, ρ denoting the total number of clubs. Such a Steiner system is identical with the "complete 1-l-m configuration" of tactical arrangement [13], [24], [25].

The Steiner group of $\mathfrak{S}(l, m, n)$ is the group of all those permutations of the n individuals which leaves the set of clubs invariant; such a group will be l-fold transitive. We now define the two fundamental Mathieu groups $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$ as the groups of the two Steiner systems $\mathfrak{S}(5, 6, 12)$ and $\mathfrak{S}(5, 8, 24)$.

Received March 6, 1950.

This paper contains the substance of a thesis prepared under the supervision of Professor Richard Brauer and submitted for a Ph.D. degree at the University of Toronto in May 1948.

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

If we consider all the clubs of $\mathfrak{S}(l, m, n)$ which contain a fixed individual, these clubs will in turn form another Steiner system $\mathfrak{S}(l\text{-}1, m\text{-}1, n\text{-}1)$. The systems $\mathfrak{S}(4, 5, 11)$ and $\mathfrak{S}(4, 7, 23)$, $\mathfrak{S}(3, 6, 22)$ can thus be obtained from the two systems given in the preceding paragraph. Their groups, which we call $\mathfrak{M}_{11}$, $\mathfrak{M}_{23}$, and $\mathfrak{M}_{22}$, are the other three Mathieu groups and occur as subgroups of the two larger groups $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$.

The orders of $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$ may be obtained from the given definitions; thus $\mathfrak{M}_{12}$ is 5-fold transitive and so has order m_{12} equal to 12.11.10.9.8.k, where k is the order of the subgroup leaving five persons invariant. Since every permutation other than the identity of an l-fold transitive group must alter at least $2l - 2$ symbols, it is necessary that k be unity and so $m_{12} = 95040$. A slightly more intricate combinatorial analysis yields $m_{24} = 24.23.22.21.20.48 = 244823040$.

We may now amplify the statement of our problem. Dickson [17] has shown that there are infinitely many group orders g with the property that there exists two simple groups of order g; the lowest such value of g is 20160. We shall here study simple groups of orders m_{12} and m_{24}; it is first shown that the character tables for simple groups of these two orders are unique and are consequently identical with the character tables already known [18], [19] for $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$. Thence it is possible to demonstate the theorem stated in the introduction.

3. Modular characters of groups. Since the assumption of the existence of simple groups of order m_{12} and m_{24} is a rather meagre one with which to start, we must attack the problem by local methods. These are provided by the theory of modular group characters for a fixed prime p. We briefly sketch here some of the more fundamental results which we shall employ from this theory.

Consider a group $\mathfrak{G}$ of order $g = p^a q^b r^c \ldots$ where p, q, and r are distinct primes. Let k denote the number of classes of conjugate elements. If a class contains elements of order prime to p, it is called a p-regular class; otherwise it is termed p-singular. It is well known that if $\mathfrak{G}$ is represented by matrices with coefficients in a field K of characteristic prime to the order g of $\mathfrak{G}$, then the ordinary Frobenius-Schur theory of representation holds and there are k irreducible representations over K [14] with corresponding irreducible characters $\zeta_1, \zeta_2, \ldots, \zeta_k$ [12], [26], [28]. But if K has characteristic p, where p divides g, this theory is no longer valid; the ordinary irreducible representations, when their coefficients are taken in such a modular field K, break up further into modular-irreducible representations and the number of these is equal to the number of p-regular classes of conjugate elements. This splitting actually corresponds to the fact that the group algebra Γ of $\mathfrak{G}$ is not semi-simple when taken as an algebra over the field K. The traces of the modular-irreducible representations are, after an isomorphic mapping upon the roots of unity in the complex field, referred to as the modular-irreducible characters.

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

This splitting-up, in the field K, of the ordinary irreducible representations into modular-irreducible representations allows us to make a very significant grouping of the ordinary representations. A set of ordinary irreducible representations is said to form a *block for the prime p* if they can be written down in some chain order such that each representation has a modular-irreducible constituent in common with both the preceding and the following representations (for brevity, we also say that the corresponding characters belong to the same block of characters). Such blocks may run the whole gamut of possibilities from blocks made up of a single ordinary representation to blocks consisting of all the ordinary representations. The theory of modular characters and blocks is developed in detail in [1], [2], [3], [6], [7], [8], [10], [11].

We shall denote the various blocks by the notation $B_\mu(p)$ and agree that $B_1(p)$ shall refer to that block containing the unit representation. The *type* of a block is defined as the minimal power of p dividing the degrees of all representations in that block; it may range from 0 to a and is always 0 for $B_1(p)$. At the present state of our knowledge, the most useful blocks are those of type a-1; we refer to these as *standard blocks.*

4. Structure of the blocks. If an ordinary irreducible representation has degree divisible by p^a, then it remains modular-irreducible and forms a block by itself. In particular, if $g = pg'$, where $(p, g') = 1$, we have an especially simple situation which has been extensively studied in [4], [5], [29]; all representations are either individual blocks or else fall into standard blocks of representations whose degrees are all prime to p.

In this particular case where p divides g to the first power only, the group order g may be written in the form

$$g = p\,\frac{p-1}{t}\,v(1+np) \tag{1}$$

where pv is the order of the normalizer of the element P of order p, t is the number of different classes of conjugate elements of $\mathfrak{G}$ appearing in the Sylow subgroup $\{P\}$, and $1 + np$ is the number of Sylow subgroups of order p. The standard blocks $B_\mu(p)$ consist of $(p - 1)/t_\mu$ ordinary characters (t_μ being a divisor of $p - 1$) and a family of t_μ p-conjugate characters, that is, characters which differ only in a permutation of the p-th roots of unity, the g'-th roots of unity remaining unaltered. In particular, $t_1 = t$.

The normalizer of P can be written as $\{P\} \times \mathfrak{B}$ where $\mathfrak{B}$ is a group of order v, this order usually being small. If the characters of $\mathfrak{B}$ are known, then we can find all the characters of $\mathfrak{G}$ itself insofar as they lie in standard blocks [4]. In particular, all the characters of $B_1(p)$ have degrees which are congruent to ± 1 modulo p except for one exceptional family of t p-conjugate characters whose members have degrees congruent to $\pm\,(p - 1)/t$ modulo p. The other blocks $B_\mu(p)$ contain characters whose degrees are congruent to $\pm a_\mu$ modulo p and a family of t_μ p-conjugate characters whose members have degrees con-

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

gruent to $\pm a_\mu(p - 1)/t_\mu$ modulo p. In any one of these blocks we may consider the characters to be of two kinds; those with degrees congruent to a_μ (including the exceptional family if its t_μ members have degrees congruent to $-a_\mu(p-1)/t_\mu$) are said to be of positive type, and those with degrees congruent to $- a_\mu$ (including the exceptional family if its members have degrees congruent to $a_\mu(p - 1)/t_\mu$) are said to be of negative type. If we set the sum of all characters of positive type equal to the sum of all characters of negative type, we obtain a character relation which is valid for the p-regular classes of elements. This relation will be our most powerful tool.

5. Block relationships for two primes. In this section we shall briefly enumerate some of the most useful theorems on blocks and block-intersections. We use, as before, p and q to denote two primes which divide the group order g.

LEMMA 1. *If a relation*

$$\sum_{\mu=1}^{k} a_\mu \zeta_\mu(S) = 0$$

holds for all p-singular elements S of $\mathfrak{G}$, a_μ being independent of S, then the relation still holds if the summation is performed only over characters of some fixed block B, that is,

$$\sum_{\zeta_\mu \varepsilon B} a_\mu \zeta_\mu(S) = 0.$$

Proof. Determine numbers b_G such that $a_\mu = \sum_{G \varepsilon \mathfrak{G}} b_G \zeta_\mu(G)$. The orthogonality relations for ordinary characters show that $b_G = 0$ for p-singular elements G. Hence $a_\mu = \sum_R b_R \zeta_\mu(R)$ where R ranges over the p-regular elements of G. Then

$$\sum_{\zeta_\mu \varepsilon B} a_\mu \zeta_\mu(S) = \sum_R b_R \sum_{\zeta_\mu \varepsilon B} \zeta_\mu(R)\zeta_\mu(S) = 0.$$

(Cf. [10], Theorem 8).

LEMMA 2. *If $\mathfrak{G}$ contains no elements of order pq and if*

$$\sum_{\mu=1}^{k} a_\mu \zeta_\mu(G) = 0$$

for all p-regular elements G, then

$$\sum_{\zeta_\mu \varepsilon B} a_\mu \zeta_\mu(H) = 0$$

for all q-singular elements H, the summation being performed over the characters of a fixed q-block B. Furthermore, if E is the identity in $\mathfrak{G}$, then

$$\sum_{\zeta_\mu \varepsilon B} a_\mu \zeta_\mu(E) \equiv 0 \bmod q^b.$$

Proof. (The a_μ denote algebraic integers). Every q-singular H is p-regular and so the hypothesis gives $\sum_{\mu=1}^{k} a_\mu \zeta_\mu(H) = 0$. Apply Lemma 1 for the prime q

and we have $\sum_{\zeta_\mu \epsilon B} a_\mu \zeta_\mu(H) = 0$. In particular, the expression $S(X) = \sum_{\zeta_\mu \epsilon B} a_\mu \zeta_\mu(H)$ vanishes for all elements, except the identity, of a Sylow q-group $\mathfrak{Q}$. Express $S(X)$ as a linear combination of the irreducible characters of $\mathfrak{Q}$, for X in $\mathfrak{Q}$. The coefficient of the principal character of $\mathfrak{Q}$ is $q^{-b}S(E)$; as this number is an algebraic integer, $S(E) \equiv 0 \bmod q^b$, that is, $\sum_{\zeta_\mu \epsilon B} a_\mu \zeta_\mu(E) \equiv 0 \bmod q^b$.

Lemma 3. *If a character ζ belongs to the first p-block, so do all its algebraically conjugate characters.*

Proof. The necessary and sufficient condition for ζ to belong to the first p-block is

$$\frac{g}{n(G)} \frac{\zeta(G)}{\zeta(E)} \equiv \frac{g}{n(G)} \bmod \mathfrak{p}$$

for all G in $\mathfrak{G}$, where $\mathfrak{p}$ is a prime ideal dividing p and $n(G)$ is the order of the normalizer of G. An algebraically conjugate character ζ' can be obtained by replacing G by G^a where $(a, g) = 1$. Then $n(G^a) = n(G)$ and, using this condition, with the relation already given, for the element G^a, we have

$$\frac{g}{n(G)} \frac{\zeta'(G)}{\zeta'(E)} \equiv \frac{g}{n(G)} \bmod \mathfrak{p}.$$

This shows ζ' is in the first p-block.

In the following lemmas, we consider groups of orders divisible by a prime p to the first power only, that is, a decomposition of g exists in the form (1).

Lemma 4. *If $v > 1$, the degrees z of all characters other than the* 1*-character belonging to* $1 - 1$ *representations in the first p-block satisfy the inequality* $z \geqslant 1 + 2p$. (In this lemma, we assume $\mathfrak{G} = \mathfrak{G}'$).

Proof. We have g written in the form (1) with $v > 1$. Let ζ be a character of the first p-block; then $\zeta(V) \equiv \zeta(PV) = \zeta(P) \equiv z \bmod \mathfrak{p}$. If we consider ζ as a character of $\mathfrak{V}$, we have $\zeta(\mathfrak{V}) = a(1) + \sum c_\nu \theta_\nu$ where the θ_ν are irreducible characters of $\mathfrak{V}$ with $\theta_\nu \neq (1)$, $a \geqslant 0$, $c \geqslant 0$, a and c rational integers. Then $\zeta(\mathfrak{V}) \equiv z \bmod \mathfrak{p}$.

Now the order v is prime to p and so $a \equiv z \bmod p$, $c_\nu \equiv 0 \bmod p$. Then $\zeta(\mathfrak{V}) = a(1) + p \sum b_\nu \theta_\nu$ and $z = a + p \sum b_\nu = a + pb$. Since $z \not\equiv 0 \bmod p$, $a > 0$; also, if $b = 0$, all $b_\nu = 0$. In this case, $\zeta(\mathfrak{V}) = a(1)$ and $\mathfrak{V}$ is represented by the identity; thus $b \geqslant 1$.

If $b = 1$, then the representation corresponding to ζ is composed of the identity of order a along with p repetitions of a linear representation $\mathfrak{F}$, that is,

$$Z(\mathfrak{V}) = \begin{pmatrix} I_a & \\ & p \times \mathfrak{F} \end{pmatrix}.$$

Then $\det Z(\mathfrak{V}) = \{\det \mathfrak{F}(\mathfrak{V})\}^p$. At this stage, we make the assumption that $\mathfrak{G}$ is identical with its derived group $\mathfrak{G}'$. Then $\det Z$ is a linear character of

$\mathfrak{G}$ and so is unity; hence det $\mathfrak{F}(\mathfrak{V}) = 1$. But $\mathfrak{F}(\mathfrak{V})$ is linear and so $\mathfrak{F}(\mathfrak{V}) = 1$; this is impossible. Thus $b \geqslant 2$ and so

$$z = a + pb \geqslant 2p + 1$$

for all characters of $1 - 1$ representations in the first p-block (when $\mathfrak{G} = \mathfrak{G}'$).

Lemma 5. *Suppose that p occurs in g to the first power only, as in* (1); *Let the decomposition* (1) *for a second prime p' be $g = p'\left(\frac{p'-1}{t'}\right)v'(1 + n'p')$. Let the group $\mathfrak{V}'$ of order v' intersect $\mathfrak{V}$ in a group $\mathfrak{W}$ of order w. Then, if $w \neq 1$, every representation in $B_1(p) \cap B_1(p')$ has a degree z satisfying the inequality $z \geqslant 1 + 2pp'$.*

Proof. The proof parallels closely that of Lemma 4. Let W be an element of $\mathfrak{W} = \mathfrak{V} \cap \mathfrak{V}'$. Then, by the argument of Lemma 4, we have

$$\zeta(\mathfrak{W}) = a(1) + p\omega(\mathfrak{W})$$

where ω is a character, reducible or irreducible, of $\mathfrak{W}$. In a similar manner,

$$\zeta(\mathfrak{W}) = a'(1) + p'\omega'(\mathfrak{W}).$$

These two expressions for $\zeta(\mathfrak{W})$ may then be equated. Now let ω_0 be a character of $\mathfrak{W}$, other than the principal character, which appears in ω; its multiplicity must be divisible by pp'. Then

$$\zeta(\mathfrak{W}) = \mathfrak{a}(1) + pp'\omega_1(\mathfrak{W}).$$

Taking degrees, and using the same sort of determinantal argument as in Lemma 4, we obtain the inequality

$$z \geqslant \mathfrak{a} + 2pp'$$

where $\mathfrak{a} > 0$, $\mathfrak{a} \equiv a \bmod p$, $\mathfrak{a} \equiv a' \bmod p'$.

Lemma 6. *As in Lemma 5, assume that p and p' are distinct primes which divide g to the first power only and that there are no elements of order pp'. Let a_{ij} be the number of characters in $B_1(p) \cap B_1(p')$ which are of type i for p and type j for p', the indices i and j being zero or unity according as the character type, defined at the end of* §4, *is positive or negative. Then*

$$a_{00} + a_{11} = a_{01} + a_{10}. \tag{2}$$

Proof. Let a character ζ be in common to the first p-block and the first p'-block; three cases may arise. First ζ may be non-exceptional for both p and p'; in this case the degree z of ζ is congruent to ± 1 for both p and p'. Secondly, ζ may be exceptional for p', that is, $z \equiv \pm 1 \bmod p$, $z \equiv \mp \frac{p'-1}{t'} \bmod p'$. Thirdly, ζ may be exceptional for p, that is, $z \equiv \pm 1 \bmod p'$, $z \equiv \mp \frac{p-1}{t} \bmod p$. ζ can not be exceptional for both p and p'.

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

Now consider the degree relation for the first block $B_1(p)$ and take the degrees modulo p'. The degrees which are of positive type for p' will then contribute 1 to the congruence; those which are of negative type will contribute -1. In this way we obtain the congruence

$$a_{00} - a_{01} \equiv a_{10} - a_{11} \mod p'.$$

If $t' > 1$, the sum $a_{00} + a_{01} + a_{10} + a_{11} \leqslant \frac{p'-1}{t'}$ and so the above congruence must be an equality. If $t' = 1$, then $a_{00} + a_{01} + a_{10} + a_{11} \leqslant p'$ and the congruence must again be an equality. Thus we have the block-intersection theorem

$$a_{00} + a_{11} = a_{01} + a_{10}.$$

LEMMA 7. *Let p, p', w have the same significance as in Lemma* 5. *Assume now that p' divides $\frac{p-1}{t}$ and that $w = 1$. Then $v \equiv 1 \mod p'$ and the number of elements of $\mathfrak{V}$ of a fixed order other than* 1 *is also congruent to* 1 mod p'.

Proof. Let $\mathfrak{M}$ denote the normalizer of $\{P\}$ and let P' denote an element of order p'. Since $\mathfrak{V}$ is normal in $\mathfrak{M}$, P' must transform $\mathfrak{V}$ into itself. Also $w = 1$; hence 1 is the only invariant element and this implies that v is congruent to 1 mod p'.

Consider now a class of conjugate elements, other than the identity, in $\mathfrak{V}$; P' will transform this class into another class. If this second class were not distinct from the first, then the number of elements in it would have to be congruent to zero mod p'. This is not possible, under the assumptions of the lemma, since p' can not divide v. Thus P' carries a class of $\mathfrak{V}$ into a distinct class and this completes the Lemma.

COROLLARY; *Under the assumptions of Lemma* 7, *but without insisting that $w = 1$, we have $w \equiv v$* mod p'.

In concluding this section, it might be well to emphasize that, while we are here applying the powerful local methods of modular theory to the Mathieu groups, the same general approach could be used on any members of the rather large class of groups which contain a prime (or preferably several primes) to the first power only.

6. The blocks in the Mathieu groups.

It is not possible to give here[1] the considerable numerical calculations necessary to find the degrees of the characters of simple groups of orders m_{12} and m_{24}. We shall content ourselves with indicating briefly the process for the case of the prime 23 in a simple group of order m_{24}. We know that there is a decomposition (1) of m_{24} and, by considering the factors of m_{24} mod 23, the number $1 + np$ of Sylow 23-

[1] The details of numerical calculation are available in the author's thesis in the University of Toronto library.

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

groups is found to lie in the set 24, 70, 231, 576, 990, 1680, 3520, 5544, 13824, 19712, 23760, 40320, 84480, 133056, 967680. Also, the number t can, for a simple group, be only 1, 2, or 11. The possibility $t = 11$ can be excluded almost immediately and this in turn eliminates some of the numbers in the list of possible Sylow groups. From there on, numerical work with Lemmas 4, 5, 6, and 7 is necessary. The block-intersection theorem that there must be a character other than the 1-character in $B_1(23) \cap B_1(11)$ finally allows us to eliminate all cases except $t = 2$, $1 + np = 967680$. Thus the decomposition (1) for the prime 23 is

$$m_{24} = 23.11.1.967680.$$

The decomposition of m_{24} in the form (1) for the other primes 11, 7, and 5 which appear in the group order to the first power requires an even more extended numerical sieving of possible degrees in block-intersections such as $B_1(23) \cap B_1(5)$, etc. When completed, the decompositions are

$$\begin{array}{lll} m_{24} = 11.10.1.1225664 & & \text{for } 11, \\ m_{24} = 5.4.12(23.11.7.576) & & \text{for } 5, \\ m_{24} = 7.3.6(23.11.5.1536) & & \text{for } 7. \end{array}$$

The groups $\mathfrak{B}$ of orders 12 and 6 which appear associated with the primes 5 and 7 are just the alternating group on 4 symbols and the symmetric group on three symbols. From the groups $\mathfrak{B}$ we see that there exists a 23-block, an 11-block, 3 5-blocks, and 3 7-blocks. Such a large number of blocks makes for smooth working of the block-intersection theorem and we give the results of its application in the form of block relations (asterisks denote the families of p-conjugate characters; also, we use the convention that the number a shall mean "the character whose degree is a"):

$B_1(23)$ $\quad 1 + 231' + 231'' + 990' + 990'' + 3520 + 5544$
$\qquad\qquad = 770^* + 45' + 45'' + 252 + 10395,$

$B_1(11)$ $\quad 1 + 45' + 45'' + 1035 + 1035' + 1035'' + 23 + 3312$
$\qquad\qquad = 252 + 483 + 5796,$

$B_1(7)$ $\quad 1 + 2024 = 990^* + 1035,$

$B_2(7)$ $\quad 3312 + 253 = 3520 + 45^*,$

$B_3(7)$ $\quad 23 + 2277 = 1035^* + 1265,$

$B_1(5)$ $\quad 1 + 5796 + 1771 = 2024 + 5544,$

$B_2(5)$ $\quad 252 + 231^* = 483,$

$B_3(5)$ $\quad 23 + 253 + 5313 = 3312 + 2277.$

During the course of the block determination, it also appeared that there were four standard 3-blocks, which were very helpful in finding the character relations, namely:

$B_2(3)$ $\quad 5796 = 252 + 5544,$

$B_3(3)$ $\quad 990' + 45' = 1035',$

$B_4(3)$ $\quad 990'' + 45'' = 1035'',$

$B_4(3)$ $\quad 2277 + 1035 = 3312.$

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press

In the twelve blocks which have just been given there occur 26 degrees; finding the sum of their squares, we check that it is equal to m_{24} and so we have found all the characters. The complete character table can then be constructed by using these block relations, together with the results of [4] concerning the expression of the characters of $\mathfrak{G}$ in terms of those of $\mathfrak{B}$. It turns out that this table can be formed in a unique way, that is, we have

THEOREM 1. *The character table for any simple group of order m_{24} is unique and hence is identical with that for $\mathfrak{M}_{24}$.*

The analogous result for $\mathfrak{M}_{12}$, namely, that the character table for a simple group of order m_{21} is unique, has already been given in [5]. However, we should here give the decomposition (1), which is:

$$m_{12} = 11.5.1.1728 \qquad \text{for } 11,$$
$$m_{12} = 5.4.2.2376 \qquad \text{for } 5.$$

Thus there is an 11-block and 2 5-blocks; in order for them to fit together, we we find that the block relations must be:

$B_1(11)$ $\quad 1 + 45 + 144 = 16^* + 54 + 120,$
$B_1(5)$ $\quad 1 + 66 + 176 = 99 + 144,$
$B_2(5)$ $\quad 16' + 16'' + 11' + 11'' = 54.$

There is also a standard 3-block and a 2-block type 4; these are given by:

$B_2(3)$ $\quad 45 + 99 = 144,$
$B_3(2)$ $\quad 16' + 16'' + 144 = 176.$

The fifteen degrees which occur in these block relations suffice to fill up the group order 95040 and, as in the case of m_{24}, the character table can be uniquely constructed from the block relations.

7. Uniqueness of the Mathieu groups. It is a well-known fact that two distinct groups of a given order g may possess the same character table; we now seek to show that this can not be the case for m_{12} or m_{24}. Suppose that we consider the character table for $\mathfrak{M}_{12}$ (for a reproduction of this table, cf. [19]). Let the corresponding group be represented as a group of linear substitutions in 11 variables x_i; by a rather lengthy discussion of the canonical matric form of the elements of order 11 and order 5, one can show that the invariance group of the variable x_1 is a group of order 7920. When this is done, the proof runs smoothly; the group under consideration must have a subgroup of index 12 and hence a permutation representation of degree 12. Split this permutation representation into irreducible constituents; the only possible splitting is a splitting into the unit representation and a representation of degree 11. This is, however, a necessary and sufficient condition for the double transitivity of the group. An exactly similar discussion of a simple group of order m_{24} can be carried out using the representation of degree 23; the invariance group of x_1 will have index 24 in this case. Hence we obtain

THEOREM II. *A simple group of order m_{12} is doubly transitive on* 12 *symbols; a simple group of order m_{24} is doubly transitive on* 24 *symbols.*

By consulting the tables of primitive groups, we could immediately identify the group on 12 symbols as $\mathfrak{M}_{12}$; however, these tables do not extend as far as degree 24 and so it is better to proceed by writing down permutation representations for the group elements of these doubly transitive groups. When these are obtained, they turn out to be identical with the known permutation representations of $\mathfrak{M}_{12}$ and $\mathfrak{M}_{24}$ [13], [20], [27]. This result, combined with Theorems I and II, yields the main theorem, as given at the end of §1.

REFERENCES

[1] R. Brauer, *On the Cartan Invariants of Groups of Finite Order*, Ann. of Math., vol. 42 (1941), 53-61.

[2] ———, *On the Connection Between the Ordinary and the Modular Characters of Groups of Finite Order*, Ann. of Math., vol. 42 (1941), 926-935.

[3] ———, *Investigations on Group Characters*, Ann. of Math., vol. 42 (1941), 936-958.

[4] ———, *On Groups whose Order Contains a Prime Number to the First Power*, Am. J. of Math., vol. 64 (1942), 401-440.

[5] ———, *On Permutation Groups of Prime Degree and Related Classes of Groups*, Ann. of Math., vol. 44 (1943), 57-79.

[6] ———, *On the Arithmetic in a Group Ring*, Proc. Nat. Acad. Sciences, vol. 30 (1944), 109-114.

[7] ———, *On Blocks of Characters of Groups of Finite Order*, Proc. Nat. Acad. Sciences, vol. 32 (1946), 182-186 and 215-219.

[8] ———, *On Modular and p-adic Representations of Algebras*, Proc. Nat. Acad. Sciences, vol. 25 (1939), 252-258.

[9] ———, *On the Representation of a Group of Order g in the Field of the g-th Roots of Unity*, Am. J. of Math., vol. 67 (1945), 461-471.

[10] R. Brauer and C. Nesbitt, *On the Modular Representations of Groups of Finite Order*, Univ. of Toronto Studies, No. 4 (1937).

[11] ———, *On the Modular Characters of Groups*, Ann. of Math., vol. 42 (1941), 556-590.

[12] W. Burnside, *The Theory of Groups of Finite Order*, Cambridge (1911).

[13] R. Carmichael, *An Introduction to the Theory of Groups of Finite Order*, Boston (1937).

[14] L Dickson, *On the Group Defined for any Given Field by the Multiplication Table of any Finite Group*, T.A.M.S., vol. 3 (1902), 285-301.

[15] ———, *Theory of Linear Groups in an Arbitrary Field*, T.A.M.S., vol. 2 (1901), 363-394.

[16] ———, *A new System of Simple Groups*, Math. Ann., vol. 60 (1905), 137-150.

[17] ———, *Linear Groups*, Leipzig (1901).

[18] G. Frobenius, *Über die Charactere der Symmetrischen Gruppe*, Sitz. Preuss. Akad. Wissen. (1900), 516-534.

[19] ———, *Über die Charactere der Mehrfach transitiven Gruppen*, Sitz. Preuss. Akad. Wissen. (1904), 558-571.

[20] C. Jordan, *Traité des Substitutions*, Paris (1870).

[21] E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités*, Jour. de Math., 2me Série, vol. 6 (1861), 241-323.

[22] ———, *Sur la fonction cinq fois transitive de* 24 *quantités*, Jour. de Math., 2me Série, vol. 18 (1873), 25-46.

[23] G. Miller, *On the Supposed Five-fold Transitive Function of* 24 *Elements,* Mess. of Math., vol. 27 (1898), 187-190.

[24] E. Moore, *Tactical Memoranda,* Am. J. of Math., vol. 18 (1896), 268-275.

[25] E. Netto, *Lehrbuch der Kombinatorik,* Leipzig (1927).

[26] I. Schur, *Neue Begründung der Theorie der Gruppencharactere,* Sitz. Preuss. Akad. Wissen. (1905), 406-432.

[27] J. de Séguier, *Theorie des Groupes Finis,* Paris (1904).

[28] A. Speiser, *Die Theorie der Gruppen,* New York (1945).

[29] H. Tuan, *On Groups whose Orders Contain a Prime to the First Power,* Ann. of Math., vol. 45 (1944), 110-140.

[30] E. Witt, *Die* 5*-fach Transitiven Gruppen von Mathieu,* Abhand. Math. Sem. Hamb., Band 12 (1938), 256-264.

[31] ———, *Über Steinersche Systeme,* Abhand. Math. Sem. Hamb., Band 12 (1938), 265-275.

The University of Toronto

https://doi.org/10.4153/CJM-1951-021-6 Published online by Cambridge University Press