RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

D. HELD
J. HRABĚ DE ANGELIS

A block-theory-free characterization of M_{24}

Rendiconti del Seminario Matematico della Università di Padova, tome 82 (1989), p. 133-150
<http://www.numdam.org/item?id=RSMUP_1989__82__133_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 82 (1989)

A Block-Theory-Free Characterization of M_{24}.

D. HELD - J. HRABĚ DE ANGELIS (*)

In [5, § 5] a characterization of the Mathieu-group M_{24} as a simple group G having a central involution z such that the centralizer H of z in G is isomorphic to the centralizer of a central involution of M_{24} had been given. To distinguish M_{24} from the simple groups $L_5(2)$ and He, it was assumed that the normalizers in G of the two elementary abelian normal subgroups of order 16 of H are not isomorphic. The information about the local structure obtained had been enough to apply the order-formula of J. G. Thompson [3] to get the uniquely determined order of G which then is the order of M_{24}. Then, by a result of R. Stanton [8], who characterized M_{24} as a simple group having the same order as M_{24}, the group G could be identified with M_{24}.

Unfortunately, the Ph. D-thesis of R. Stanton, written under the supervision of Richard Brauer, had not been published, there is only the short summary [8] available in which he describes his methods which are heavily block theoretical and computational.

This was the reason that we tried to make § 5 of [5] free of Stanton's result. In [11], J. A. Todd gives generators and relations for the group M_{24}, and we succeeded in showing that the group G can be generated by elements satisfying the Todd-relations. Thus, without using Stanton's result, we are able to identify G with M_{24}. It is in this sense that our title should be understood.

Similar procedures allow to throw out character theory from Z. Janko's characterizations of M_{22} and M_{23} in [7]. Also, it seems

(*) Indirizzo degli A.A.: Fachbereich Mathematik (17) der Universität, D-6500 Mainz, R.F.T.

possible to eliminate character theory from characterizations of M_{11} and M_{12}. Moreover, theorems of B. Beisiegel [1] and V. Stingl [9] permit to prove Stanton's result without block theory.

1. Notations.

In the whole paper, G denotes a finite simple group having all the properties of the group G of [5; § 5]. We shall use the notation introduced in [5] with one exception: We do not use the letter H to denote the centralizer of z_1 in G. In addition, we put $S = \langle \pi, \tau, \mu, \lambda \rangle$ and $F = \langle z_1, z_3, \mu, \lambda \rangle$. The centralizer of the non-2-central involution $z_3 \pi$ in G is described in [5; § 5]. There, one finds also the structures of the normalizers of the elementary abelian groups R_1 and R_2 both of order 64 and of E of order 16 which — essentially — determined the fusion of the involutions of G. The multiplication table of $\mathbb{C}(z_1)$ is completely given in [5, § 1]; the relations of [6; § 1, p. 218] are satisfied inside $\mathbb{C}(z_1)$.

Put $H_1 = \mathbb{C}(z_1)$. Then, $E = \langle z_1, z_2, z_3, z_4 \rangle$ is an elementary abelian normal selfcentralizing subgroup of order 16 of H_1. The 2-group $T = E \langle \pi, \tau, \tau' \rangle \langle \mu, \mu', \lambda \rangle$ is a Sylow 2-subgroup of G. The two elementary abelian normal subgroups of order 64 of T are $R_1 = \langle z_1, z_3, z_4, \pi, \mu\tau, \mu'\tau' \rangle$ and $R_2 = \langle z_1, z_3, \pi, \mu, \tau, \lambda \rangle$. One has $\mathbb{N}(R_1) \cap H_1 = \langle T, \varrho \rangle$ and $\mathbb{N}(R_2) \cap H_1 = \langle T, u \rangle$. The element u of order 3 centralizes $\langle z_1, z_3 \rangle$ and operates on S fixed-point-free in the following way: $\pi \to \tau \to \pi\tau$, $\mu \to \lambda \to \mu\lambda$. Further, $[u, \tau'] = 1$. There is another elementary abelian normal subgroup $E_1 = \langle z_1, \pi, \tau, \tau' \rangle$ of H_1. We have to treat here the situation in which $\mathbb{N}(E_1) = H_1$ and $\mathbb{N}(E)/E \simeq A_8$.

2. Some facts about the subgroup structure of G.

In this paragraph we shall derive some results about the 3-structure of G and shall exhibit certain subgroups of $\mathbb{N}(E)$ and $\mathbb{N}(F)$ with which we are able to construct a subgroup of G isomorphic to $L_3(4)$.

(2.1) LEMMA. The group G has the following properties:

(*a*) A Sylow 3-subgroup of G is non-abelian of exponent 3.

(*b*) If k is an element of order 3 of $\boldsymbol{O}_{2,3}(\mathrm{N}(R_2))$ then k is conjugate to ϱ in G and $\mathrm{C}(\langle\varrho\rangle)/\langle\varrho\rangle \cong A_6$, $\mathrm{N}(\langle\varrho\rangle)/\langle\varrho\rangle \cong \Sigma_6$. Moreover, the element k acts fixed-point-free on R_2.

(*c*) If K is a Sylow 3-subgroup of $\mathrm{N}(R_2)$ and x is an element of K not in K' then $|\mathrm{C}(x) \cap R_2| = 4$.

(*d*) In G there are precisely two classes of elements of order 3.

(*e*) If v is an element of order 3 not conjugate to ϱ in G then $\mathrm{C}(v) = \langle v\rangle \times L_2(7)$.

(*f*) If x is an element of order 3 of G then all involutions of $\mathrm{C}(x)$ are conjugate in $\mathrm{C}(x)$.

PROOF. The structure of $\mathrm{N}(R_2)$ is described in lemmas (2.17) and (5.3) of [5]. From [5; § 5] we know that $\mathrm{C}(z_3\pi)$ is contained in $\mathrm{N}(R_2)$.

Let K be a Sylow 3-subgroup of $\mathrm{N}(R_2)$ containing the element u of order 3. If K was abelian then a subgroup of order 9 of K would centralize $\mathrm{C}(u) \cap R_2 = \langle z_1, z_3\rangle$. This, however, is not possible as the order of the centralizer of an involution of G is not divisible by 9. It follows that a Sylow 3-subgroup of G is nonabelian.

We have $T = R_2(\langle\tau'\rangle \times \langle z_3 z_4, \pi\mu'\tau'\rangle\langle z_2\rangle)$ and the commutator group of $\langle\tau'\rangle \times \langle z_3 z_4, \pi\mu'\tau'\rangle\langle z_2\rangle$ is $\langle z_3 z_4\rangle$. Thus, if k is an element of order 3 in $\boldsymbol{O}_{2,3}(\mathrm{N}(R_2))$, we get $[k, z_4] \in R_2$: It follows that k operates on the set $\langle z_1, z_3, \pi, \mu\tau\rangle z_4$ of all involutions of $R_2 z_4$. But there are only four 2-central involutions of G in $R_2 z_4$. It follows that $k \sim \varrho$, since $z_1 \sim z_4$. Frattini's argument yields $\mathrm{N}(R_2) = (\mathrm{N}(\langle k\rangle) \cap \mathrm{N}(R_2)) R_2$. Since the order of $\mathrm{N}(\langle k\rangle)$ is divisible by 3^3, application of [5; Lemma (2.10)] gives $\mathrm{N}(\langle k\rangle)/\langle k\rangle \cong \Sigma_6$. In particular, we see that k acts fixes-point-free on R_2.

Let $K' = \langle k\rangle$ and let x be an element of K not in K'. Then, $K_1 = \langle k, x\rangle$ is elementary abelian of order 9 and normalizes R_2. We apply [2; 5.3.16] and get $R_2 = \Pi \mathrm{C}(y)$, where y runs through all elements of $K_1^{\#}$. Assume that for such a y we had $|\mathrm{C}(y) \cap R_2| = 16$. Then y cannot centralize a conjugate of z_1 by the structure of $\mathrm{C}(\varrho)$. However, $F = \langle z_1, z_3, \mu, \lambda\rangle$ has only 2-central involutions and $|F \cap \cap \mathrm{C}(y) \cap R_2| \geqslant 4$; this yields a contradiction. It follows that for all y in $K_1^{\#}$ we have $|\mathrm{C}(y) \cap R_2| \leqslant 4$, and so, if y in $\langle k, x\rangle \setminus \langle k\rangle$, we must have $|\mathrm{C}(y) \cap R_2| = 4$. We have shown that every element of order 3 of G is centralized by an involution and this implies that G has precisely two classes of elements of order 3.

Put $H_2 = \mathbb{C}(z_3\pi)$. We know that H_2 lies in $\mathbb{N}(R_2)$. From [5; Lemma (5.4)] we get that $V = \langle z_3\pi, z_1\mu\tau\rangle$ is normal in H_2. Note that $H_2/R_2 \cong \Sigma_5$ and that $\mathbb{C}(V)/R_2 \cong A_5$. Denote by v an element of order 3 in H_2. We get that $\mathbb{C}(v) \cap H_2$ has order $2^3 \cdot 3$ and that a Sylow 2-subgroup of $\mathbb{C}(v)$ is dihedral of order 8. From [5; Lemmas (2.19) and (5.2)] we get that v is centralized by a subgroup isomorphic to $L_3(2)$ of G. Hence, $\mathbb{C}(v)$ has no subgroup of index 2, and since v is not 3-central, we see that $|\mathbb{C}(v)|$ is not divisible by 3^3. Application of the result of [4] yields that $\mathbb{C}(v) = \langle v\rangle \times L_3(2)$. All assertions of the lemma are proved.

(2.2) LEMMA. The group G contains a subgroup isomorphic to $L_3(4)$.

PROOF. Application of [5; Lemma (2.9)] yields that $|\mathbb{N}(\langle z_1, z_3\rangle)| = 2^{10}\cdot 3^2$. We know that $\mathbb{N}(\langle z_1, z_3\rangle)$ lies in $\mathbb{N}(R_2)$ and in $\mathbb{N}(E)$. We have $\mathbb{C}(\langle z_1, z_3\rangle) = ER_2\langle u, \mu'\tau'\rangle$. Denote by H a Sylow 3-subgroup of $\mathbb{N}(\langle z_1, z_3\rangle)$ such that $u \in H$. Then, $H = \langle u, \nu\rangle$, where ν is an element of order 3. The element u of order 3 acts fixed-point-free on $S = \langle \pi, \tau, \mu, \lambda\rangle$ and $[u, R_2] = S$. Therefore, we get that H normalizes S. The normalizer of an elementary abelian group of order 16 of A_8 does not contain the centralizer of a 2-central involution of A_8. Thus, under the action of H, the involution π has precisely 9 conjugates in S. It is easy to see that the conjugates of π in S under the action of H centralize subgroups of order 8 in E. The six elements μ, λ, $\mu\lambda$, $\pi\mu$, $\tau\lambda$, $\pi\tau\mu\lambda$ centralize only subgroups of order 4 in E. Clearly, $|H : H \cap \mathbb{C}(\mu)| = 3$, and we may and shall assume that $[\nu, \mu] = 1$. Since u acts on $\mathbb{C}_S(\nu)$, we get $\mathbb{C}_S(\nu) = \langle \mu, \lambda\rangle$. With respect to E we may call the 9 conjugates of π long and the 6 conjugates of μ short involutions. Then, u is a long and ν is a short element of order 3 with respect to E.

Clearly, H acts on E. But H acts also on $F = \langle z_1, z_3, \mu, \lambda\rangle$, since $[u, \nu] = 1$. We know that ν acts fixed-point-free on E, and so, we get $\langle z_1, z_3\rangle\langle\nu\rangle \cong \langle z_2, z_3 z_4\rangle\langle\nu\rangle \cong A_4$ as $\mathbb{C}_E(u) = \langle z_1, z_3\rangle$ and $[u, E] = \langle z_2, z_3 z_4\rangle$. It follows that $\langle z_2, z_3 z_4\rangle\langle\nu\rangle$ lies in $\mathbb{N}(R_2)'$; note that $\langle z_2, z_3 z_4\rangle\langle\nu\rangle$ normalizes F.

Now, $\langle \mu, \lambda\rangle\langle u\rangle \times \langle\nu\rangle$ normalizes E. From the structure of $\mathbb{N}(E)$ follows that $\mathbb{C}_{\mathbb{N}(E)}(\nu)$ acts faithfully on E as ν is short and that $\mathbb{C}_{\mathbb{N}(E)}(\nu) \cong Z_3 \times A_5$. Clearly, νu or $\nu^{-1}u$ acts fixed-point-free on E. So, interchanging ν and ν^{-1} if necessary, we may and shall assume that $u\nu$ acts fixed-point-free on E. It follows that $\langle \mu, \lambda\rangle\langle u\nu\rangle$ is contained in a subgroups A_E isomorphic to A_5 of $C_{N(E)}(\nu)$. Note that $E\langle\mu, \lambda\rangle$ is a Sylow 2-subgroup of $EC_{N(E)}(\nu)$.

We shall now study the normalizer of F in G. Clearly, $C(F) = R_2$, and so, $N(F) \subseteq N(R_2)$. We have $R_2 = V \times F$, where $V = \langle z_3\pi, z_1\mu\tau\rangle$; all involutions of F are 2-central but no involution of V is 2-central in G. There are precisely the following six subgroups of R_2 with the property that they have order 16 and possess only 2-central involutions:

1) $F = \langle z_1, z_3, \mu, \lambda\rangle$,

2) $\langle z_1, z_3, \pi\mu, \tau\lambda\rangle$,

3) $\langle \pi, \tau, \mu, \lambda\rangle$,

4) $\langle \pi, z_1\tau, z_1\mu, z_3\lambda\rangle$,

5) $\langle z_1\pi, \tau, z_1z_3\mu, z_1\lambda\rangle$,

6) $\langle z_1\pi, z_1\tau, z_3\mu, z_1z_3\lambda\rangle$.

Each of these six subgroups is a complement of V in R_2. The first two subgroups are conjugate via τ', and the last four subgroups are conjugate under the action of $\langle z_2, z_4\rangle$. Since $z_1 \sim \pi$ holds in $N(R_2)$, we see that under the action of $N(R_2)$ all six subgroups are conjugate to F.

It follows that $|N(R_2):N(F)| = 6$, and so, $N(F)$ has order $2^9\cdot 3^2\cdot 5$. Since $R_2\langle z_1z_3z_4, z_2\rangle\langle\mu'\rangle$ is a Sylow 2-subgroup of $N(F)$, we get that $N(F)$ splits over R_2. We know that $u\nu$ and $u\nu^{-1}$ act fixed-point-freely on F as $C_F(u) = \langle z_1, z_3\rangle$ and $C_F(\nu) = \langle\mu, \lambda\rangle$. From our above choice we get that $\langle z_2, z_3z_4\rangle\langle u\nu\rangle \cong A_4$ and that $\langle z_2, z_3z_4\rangle$ is centralized by $u\nu^{-1}$. We have $\langle z_2, z_3z_4\rangle\langle u\nu\rangle \subseteq C(u\nu^{-1})$. If $u\nu^{-1}$ was not fixed-point-free on R_2, then $u\nu^{-1}$ centralizes $\langle z_2, z_3z_4\rangle$ and would in addition centralize a four-subgroup of R_2; but no element of order 3 in G centralizes a group of order 16. Thus, $u\nu^{-1}$ operates fixed-point-free on R_2 and on F. It follows that $\langle z_2, z_3z_4\rangle\langle u\nu\rangle$ lies in a subgroup A_F isomorphic to A_5 of $C(u\nu^{-1}) \cap N(F)$.

We have obtained $A_E \times \langle\nu\rangle \subseteq N(E)$ and $A_F \times \langle u\nu^{-1}\rangle \subseteq N(F)$.

There is an involution r_1 in A_E which inverts $u\nu$, and there is an involution r_2 in A_F which also inverts $u\nu$. We have therefore

$$[r_1, \nu] = 1, \quad \langle u\nu, r_1\rangle \cong \Sigma_3, \quad r_1 \in A_E \subseteq N(E)$$

and

$$[r_2, uv^{-1}] = 1\,, \quad \langle uv, r_2\rangle \cong \Sigma_3\,, \quad r_2 \in A_F \subseteq \mathrm{N}(F), \quad \text{and} \quad [r_1 r_2, uv] = 1\,.$$

For the action of $\langle r_1, r_2\rangle$ on $H = \langle u, v\rangle$ we get:

$$\begin{aligned}
r_1&:\ v \to v\,,\\
r_1&:\ u \to u^{-1}v\,,\\
r_2&:\ v \to u^{-1},\\
r_2&:\ u \to v^{-1},\\
r_1 r_2&:\ u \to u^{-1}v \to v^{-1} \to u\,,\\
r_1 r_2&:\ v \to u^{-1} \to uv^{-1} \to v\,.
\end{aligned}$$

It follows that $(r_1 r_2)^3 \in \mathrm{C}(H)$. But $\mathrm{C}(H) = H$ by the structure of $\mathrm{C}(u)$. Clearly, $r_1 r_2 \notin H$. It follows $o(r_1 r_2) = 3$, since there are no elements of order 9 in G. Thus, $\langle r_1, r_2\rangle \cong \Sigma_3$. Put $N = H\langle r_1, r_2\rangle$ and $B = EF\langle u, v\rangle$. Then, $N/H \cong \Sigma_3$ and $|B| = 2^6 \cdot 3^2$. Moreover, $B \cap N = H$ as B is 2-closed, and no involution centralizes H. Put $N/H = W$.

We shall show that the following conditions of [10] are satisfied:

(i′) *$B \cup Br_iB$ is a subgroup of G for $i = 1, 2$;*

(iv) *if $l(r_1 w) \geqslant l(w)$ for some $w \in W$ in the generators r_1, r_2 then $B^w \subseteq B^{r_i w}B$ for $i = 1, 2$.*

We have that $B^{r_1} \cap B = EH$; note that H acts transitively on EF/E and that $r_1 \notin \mathrm{N}(B)$ as $r_1 \notin \mathrm{N}(EF)$. Similarly, one gets $B^{r_2} \cap B = FH$. It follows that the number of left cosets of B in Br_iB is equal to $[B : B^{r_i} \cap B] = 2^2$. Thus, $B \cup Br_1B = E(\langle v\rangle \times A_E)$ and $B \cup Br_2B = F(\langle uv^{-1}\rangle \cdot A_F)$ are subgroups of G. We have shown that (i′) holds.

Put $Z = E \cap F = \langle z_1, z_3\rangle$. If r_1 would normalize Z then r_1 would normalize EF and also $EFH = B$ which is not the case; use here the structure of $E(\langle v\rangle \times A_E)$. Similarly, we see that $r_2 \notin \mathrm{N}(Z)$. Thus, $Z^{r_i} \neq Z$ for $i = 1, 2$. Since H acts nontrivially on Z^{r_i} and on Z, we get $Z^{r_i} \cap Z = \langle 1\rangle$. Clearly, $Z^{r_1} \subseteq E$ and $Z^{r_2} \subseteq F$. It follows $E = ZZ^{r_1}$ and $F = ZZ^{r_2}$; hence $EF = ZZ^{r_1}Z^{r_2}$.

It is easy to see that $w \in \{r_2, r_2 r_1\}$ if $i = 1$, and that $w \in \{r_1, r_1 r_2\}$ if $i = 2$.

Case 1. Here, $i = 1$ and $w = r_2$. Compute:

$$B = Z Z^{r_1} Z^{r_2} H ,$$

$$B^{r_2} = Z^{r_2} Z^{r_1 r_2} Z H ,$$

$$B^{r_1 r_2} = Z^{r_1 r_2} Z^{r_2} Z^{r_2 r_1 r_2} H .$$

It follows $B^{r_2} \subseteq B^{r_1 r_2} B$.

Case 2. Here, $i = 1$ and $w = r_2 r_1$. Compute:

$$B^{r_2 r_1} = Z^{r_2 r_1} Z^{r_1 r_2 r_1} Z^{r_1} H ,$$

$$B^{r_1 r_2 r_1} = Z^{r_1 r_2 r_1} Z^{r_2 r_1} Z^{r_1 r_2} H .$$

It follows $B^{r_2 r_1} \subseteq B^{r_1 r_2 r_1} B$.

Case 3. Here, $i = 2$ and $w = r_1$ Compute:

$$B^{r_1} = Z^{r_1} Z Z^{r_2 r_1} H ,$$

$$B^{r_2 r_1} = Z^{r_2 r_1} Z^{r_1 r_2 r_1} Z^{r_1} H .$$

It follows $B^{r_1} \subseteq B^{r_2 r_1} B$.

Case 4. Here, $i = 2$ and $w = r_1 r_2$. Compute:

$$B^{r_1 r_2} = Z^{r_1 r_2} Z^{r_2} Z^{r_2 r_1 r_2} H ,$$

$$B^{r_2 r_1 r_2} = Z^{r_2 r_1 r_2} Z^{r_2 r_1} Z^{r_1 r_2} H .$$

It follows $B^{r_1 r_2} \subseteq B^{r_2 r_1 r_2} B$.

Application of [10] yields that $U = BNB$ is a subgroup of G. Another application of [10] gives $B^w \cap B \subset B$ for all $w \in W^\#$. Also, since H acts on $EF \cap (EF)^w$ without fixed-points, we get that $|B : B^w \cap B| = 2^i$, where i is even and greater than 1 for $w \neq 1$. Put

$$|U| = 2^6 \cdot 3^2 \cdot (1 + 2^2 + 2^2 + 2^{i_4} + 2^{i_5} + 2^{i_6})$$

and denote the bracket by n. Then, 5 divides n, and n is a divisor of $3\cdot 5\cdot 7\cdot 11\cdot 23$. One gets $i_4 = i_5 = 4$, and $i_6 = 6$. Thus,

$$|U| = 3\cdot|L_3(4)| = 2^6\cdot 3^3\cdot 5\cdot 7 .$$

Put $H^* = \langle uv\rangle$, $B^* = EFH^*$, and $N^* = H^*\langle r_1, r_2\rangle$. Then, $N^*\cap B^* = H^*$ as uv acts fixed-point-freely on E and on F and any involution of EF lies in E or in F; clearly, H^* is normal in N^*. Moreover, $B^*\cup B^* r_1 B^* = EA_E$ and $B^*\cup B^* r_2 B^* = FA_F$. Put $N^*/H^* = W^*$. Since $|B:B^w\cap B| = |B^*:B^{*v}\cap B^*|$ if w in W and v in W^* correspond to each other, we obtain in a similar way as before that in U there is a subgroup $L = B^*N^*B^*$ of order $|L_3(4)|$.

We show that L is a simple group. Note that EF is a Sylow 2-subgroup of L and that EF has order 2^6. We know that A_E acts transitively on E and that A_F acts transitively on F. Thus, L has precisely one class of involutions. Let K be a minimal normal subgroup of L. Then, by Frattini's argument, K cannot have odd order. It follows that EF lies in K. Since $L = K\mathrm{N}_L(EF)$, we get from the structure of $\mathrm{C}(z_1)$ that $5\cdot 7$ divides $|K|$. It follows that $\langle EA_E, FA_F\rangle$ lies in K and this implies $L = K$. We have shown that L is a simple group. Since L has only one class of involutions, we get $L \simeq L_3(4)$.

3. Adaption of Todd's presentation of M_{24} to the group G.

According to [11], the Mathieu-group M_{24} can be presented by the set $\{a, b, c, d, t, g, h, i, j, k\}$ together with the following relations:

(i) $a^2 = b^2 = c^2 = d^2 = 1,\quad a^b = a^c = a^d = a,\quad b^c = b^d = b,\quad c^d = c,$

(ii) $t^3 = 1,\quad a^t = cd,\quad b^t = ad,\quad c^t = bd,\quad d^t = abc,$

(iii) $g^2 = (ga)^3 = (gb)^3 = (gc)^3 = (gt)^2 = 1,$

(iv) $h^2 = 1,\quad a^h = a,\quad b^h = abd,\quad c^h = ac,\quad d^h = d,$
$t^h = t^{-1},\quad (gh)^3 = 1,$

(v) $i^2 = 1,\quad a^i = cd,\quad b^i = ad,\quad c^i = abcd,\quad d^i = bcd,$
$t^i = t^{-1},\quad g^i = tg,\quad (hi)^3 = 1,$

(vi) $j^2 = 1, \quad a^j = abc, \quad b^j = b, \quad c^j = c, \quad d^j = cd,$
$t^j = t^{-1}, \quad g^j = g, \quad h^j = th, \quad (ij)^3 = 1,$

(vii) $k^2 = 1, \quad a^k = ad, \quad b^k = cd, \quad c^k = bd, \quad d^k = d,$
$t^k = t^{-1}, \quad g^k = tg, \quad h^k = h, \quad i^k = i, \quad (jk)^3 = 1.$

The set $\{a, b, c, d\}$ together with (i) defines the elementary abelian group of order 16. The set $\{a, b, c, d, t\}$ together with (i) and (ii) defines a group of order 48. The set $\{a, b, c, d, t, g\}$ together with (i) to (iii) defines a group of order $2^6 \cdot 3 \cdot 5$ which is isomorphic to a parabolic subgroup of $L_3(4)$. The set $\{a, b, c, d, t, g, h\}$ together with (i) to (iv) defines $L_3(4)$. The set $\{a, b, c, d, t, g, h, i\}$ together with (i) to (v) defines M_{22}. Finally, the set $\{a, b, c, d, t, g, h, i, j\}$ together with (i) to (vi) defines M_{23}.

In § 2 we had constructed a subgroup L of G which is isomorphic to $L_3(4)$. Therefore, we are able to find elements $a, b, c, d, t, g,$ and h in L such that $L = \langle a, b, c, d, t, g, h\rangle$ and such that the relations (i) to (iv) are satisfied.

From the representation of M_{24} as a subgroup of A_{24} given in [11], we get that the element gd has order 5. The subgroup L has only one class of involutions and only one class of elements of order 3. By construction, the involutions of L are all 2-central in G, and from the order of L follows that the elements of order 3 are all 3-central in G.

The element t of order 3 of L acts fixed-point-freely on the elementary abelian group $\langle a, b, c, d\rangle$ of order 16, and we know that $\mathrm{N}(\langle t\rangle)/\langle t\rangle \cong \Sigma_6$ and $\mathrm{C}(t)/\langle t\rangle \cong A_6$ holds; remember that $\mathrm{C}(t)$ does not split over $\langle t\rangle$.

Put $X = \langle a, b, c, d\rangle$ and $P = \langle X, t, g\rangle$. We have that P has order $2^6 \cdot 3 \cdot 5$ and is isomorphic to a parabolic subgroup of L. Denote by Y the largest normal 2-subgroup of P. Then, Y is elementary abelian of order 16 and P is a transitive splitting extension of Y by A_5. Since $g \notin \mathrm{N}(X)$, we see that $X \neq Y$.

(3.1) LEMMA. The 2-group XY is a Sylow 2-subgroup of L, and $Y = \langle ab, ac, (ab)^g, (ac)^g\rangle$.

PROOF. We know that t acts fixed-point-freely on X and normalizes Y. Thus, t has no nontrivial fixed-points in $X \cap Y$. Therefore, $|X \cap Y| = 4$ and $|XY| = 2^6$. It follows that $XY \in \mathrm{Syl}_2(L)$. From the embedding of L in G, we see that X and Y are not conjugate in G.

The relations inside L describe the action of t on X in the following way:

$$\begin{aligned} t\colon \quad & a \to cd \to acd\,, \\ & b \to ad \to abd\,, \\ & c \to bd \to bcd\,, \\ & d \to abc \to abcd\,, \\ & ab \to ac \to bc\,. \end{aligned}$$

Now, $Y\langle g\rangle$ is a group of order 2^5, since $\langle t, g\rangle \simeq \Sigma_3$. Since ga, gb, and gc have order 3, and gd has order 5, we get that neither a, b, c, nor d is contained in Y. It follows that $X \cap Y = \langle ab, ac\rangle$.

We want to show that $\mathbf{C}(g) \cap \langle ab, ac\rangle = \langle 1\rangle$. Assume that $[g, ab] = 1$. Then,

$$1 = gab(ga)\,b = gab(agag)\,b = gbgagb\,, \quad \text{and so}\,, \quad bgbg = ga = gb$$

which is impossible as a is different from b; here, we have used the fact that both ga and gb have order 3. Similarly, one shows that g does not centralize ac and bc. It follows $\mathbf{C}(g) \cap \langle ab, ac\rangle = \langle 1\rangle$. Since g is an involution, we get that $\langle ab, ac\rangle \cap \langle ab, ac\rangle^g = \langle 1\rangle$. But g lies in $\mathbf{N}(Y)$, and so, $Y = \langle ab, ac, (ab)^g, (ac)^g\rangle$. The lemma is proved.

(3.2) Lemma. The element t of order 3 acts fixed-point-free on Y in the following way:

$$\begin{aligned} t\colon \quad & ab \to ac \to bc\,, \\ & gabg \to gbcg \to gacg\,. \end{aligned}$$

Proof. The assertion follows from the relations (i), (ii), and (iii) which hold in L.

(3.3) Lemma. We have $\mathbf{N}_L(X) = \langle XY, t, h\rangle$.

Proof. Since t acts fixed-point-freely on Y, we have $\langle XY, t\rangle/X \simeq A_4$. If N is the full normalizer of X in L then $N/X \simeq A_5$. Therefore, $\langle XY, t\rangle/X$ is a maximal subgroup of N/X. Since $\langle XY, t\rangle$ normalizes Y but h does not, the assertion follows.

From the structure of G and the embedding of L in G, we know that one of the two elementary abelian subgroups X and Y is self-centralizing in G whereas the centralizer of the other in G is elementary abelian of order 64. Now, L possesses an automorphism of order 2 which interchanges X and Y. Therefore, we may and shall assume that $X = \mathrm{C}(X)$ and $\mathrm{C}(Y) \supset Y$.

In what follows we change notation and put $E = X$ and $F = Y$ to be in conformity with § 2. Thus, $\mathrm{N}(E)$ is a splitting extension of E by A_8, and $\mathrm{N}(F)$ is a splitting extension of $\mathrm{C}(F)$ by a group of type $(Z_3 \times A_5)Z_2$ such that $Z_3Z_2 \cong \Sigma_3$ and $A_5Z_2 \cong \Sigma_5$.

Denote by C a complement of E in $\mathrm{N}(E)$ such that t lies in C. Clearly, as t is fixed-point-freely on E, we have that t corresponds to a short element of order 3 of C. Also, $\mathrm{N}_C(\langle t\rangle) = \mathrm{N}(\langle t\rangle) \cap \mathrm{N}(E)$ and this group is isomorphic to $\mathrm{N}(\langle(123)\rangle) \cap A_8$. Obviously, modulo $\langle t\rangle$, the element h corresponds to a transposition of $\mathrm{N}_C(\langle t\rangle)/\langle t\rangle \cong \Sigma_5$. We can find now involutions i, j, and k in $\mathrm{N}_C(\langle t\rangle)$ which satisfy all the relations (v), (vi), and (vii) with the possible exception of $igi = tg$, $jgj = g$, or $kgk = tg$.

The following easy lemma is helpful. We shall state it without proof.

(3.4) LEMMA. Let X be a group of type $(Z_3 \times A_5)Z_2$ such that $Z_3Z_2 \cong \Sigma_3$ and $A_5Z_2 \cong \Sigma_5$. Then, X possesses precisely one subgroup A isomorphic to A_5. If i is an involution of $X \setminus A$, then $A\langle i\rangle \cong \Sigma_5$.

(3.5) LEMMA. We have $\mathrm{N}(E) = \langle EF, t, h, i, j, k\rangle$.

PROOF. Note that $\langle EF, t, h\rangle/E \cong A_5$ and that $\langle E, t, h, i, j, k\rangle/E$ has the structure of the group X of lemma (3.4). Clearly,

$$\langle EF, t, h\rangle/E \cap \langle E, t, h, i, j, k\rangle/E \cong \Sigma_3 .$$

Thus, these two subgroups of $\mathrm{N}(E)/E$ generate a subgroup of order at least $(2^2\cdot 3\cdot 5)\cdot(2^3\cdot 3^2\cdot 5)/6$. But A_8 has no proper subgroup of index smaller or equal to 5. The lemma is proved.

In what follows, a matrix indexed by the letter E stands for the action of an element from $\mathrm{N}(E)$ on E with respect to the basis $\{a, b, c, d\}$ over $GF(2)$. Analogously, a matrix indexed by F is used to describe the action of an element on F with respect to the basis $\{ab, ac, gabg, gacg\}$ over $GF(2)$.

In the next lemma we shall derive more information about the multiplication table of $\mathrm{N}(E)$.

(3.6) LEMMA. With respect to the « basis » $\{a, b, c, d\}$ of the « vector space » E over $GF(2)$, the action on E of $gabg$ and $gacg$ is described by the following correspondences:

$$gabg \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{vmatrix}_E ,$$

$$gacg \to \begin{vmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{vmatrix}_E .$$

(For example, the first matrix shows that $a^{gabg} = b$, $b^{gabg} = a$, $c^{gabg} = abc$, $d^{gabg} = acd$.)

PROOF. We know that F normalizes E. Using the relations (i) and (iii), we get

$$(gabg)\,a(gabg) = gb(agaga)\,bg = gb(gaa)\,bg = gbgbg = bgg = b\,.$$

It follows

$$(gabg)\,b(gabg) = a\,.$$

Since $[gabg, ac] = 1$, we get

$$(gabg)\,ac(gabg) = ac = b(gabg)\,c(gabg)\,.$$

Hence,

$$(gabg)\,c(gabg) = abc\,.$$

Similarly, one computes

$$(gacg)\,a(gacg) = c, \ (gacg)\,c(gacg) = a \quad \text{and} \quad (gacg)\,b(gacg) = abc\,.$$

Finally, using lemma (3.2), we get

$$(gacg)\,d(gacg) = tt^{-1}(gacg)\,d(gacg)\,tt^{-1} = t(gabg)\,t^{-1}\,dt(gabg)\,t^{-1} =$$
$$= t(gabg)\,abc(gabg)\,t^{-1} = t(baabc)\,t^{-1} = tct^{-1} = bcd\,,$$

and similarly, we get

$$(gabg)\,d(gabg) = acd\,.$$

The lemma is proved.

4. A subgroup isomorphic to M_{22}.

(4.1) LEMMA. The involution i normalizes F, and its action on F is described by the following correspondence

$$i \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix}_F .$$

PROOF. Put $x = (ab)^g$ and $y = (ac)^g$. Consider the group $\langle x, y, i\rangle E/E$. The action of the involutions x, y, and i on E are known. *Modulo* E one gets $(xi)^4 = (yi)^2 = x^2 = y^2 = i^2 = 1$, and $(xi)^2 = y$. Note that $C(E) = E$. It follows that $\langle x, y, i\rangle E/E = \langle x, i\rangle E/E$ is a dihedral group of order 8 with center $\langle yE\rangle$. Thus, *modulo* E we have $ixi = xy$ and $iyi = y$. This implies $(EF)^i = EF$. Since $i \in N(E)$, we get $i \in N(F)$ as E and F are the only elementary abelian subgroups of order 16 of EF.

Clearly, $i(ab)\,i = ac$, $i(ac)\,i = ab$, and $i(gabg)\,i = ixi = xye_1$, and $i(gacg)\,i = iyi = ye_2$ with elements $e_1, e_2 \in E \cap F$. In this way we have found the correspondence

$$i \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & \beta & 1 & 1 \\ \gamma & \delta & 0 & 1 \end{vmatrix}_F$$

with $\alpha, \beta, \gamma, \delta \in GF(2)$.

The relations $i^2 = 1$ and $(it)^2 = 1$ force that we get only the following two possiblities:

Case 1. $\alpha = 0,\ \beta = \gamma = \delta = 1.$

Case 2. $\alpha = \beta = \gamma = \delta = 0.$

By way of contradiction, we assume that we are in the first case. We get

$$ig \to \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{vmatrix}_F ,$$

and $(gi)^3$ centralizes F. It is easy to see that there is no element in $\langle t \rangle$ which acts on F in the same way as gi does. But gi centralizes t. It follows that $\langle gi, t \rangle \mathbb{C}(F)/\mathbb{C}(F)$ is a Sylow 3-subgroup of $\mathbb{N}(F)/\mathbb{C}(F)$. In particular, $|\langle EF, t, g, i \rangle \mathbb{C}(F)/\mathbb{C}(F)|$ is divisible by 3^2. We know that $\langle EF, t, g \rangle \mathbb{C}(F)/\mathbb{C}(F) \simeq A_5$, and therefore, by lemma (3.4), we see that $\langle EF, t, g, i \rangle \mathbb{C}(F)/\mathbb{C}(F)$ is isomorphic to A_5 or Σ_5. But 3^2 does not divide 120. We have ruled out case 1. The lemma is proved.

(4.2) THEOREM. We have $(ig)^2 = t$ and $\langle E, t, g, h, i \rangle$ is isomorphic to M_{22}.

PROOF. For the action of ig on F we get the correspondence

$$ig \to \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix}_F .$$

It follows that $(ig)^2$ acts in the same way as t on F, and the order of ig is either 6 or 12; remember that $\mathbb{C}(F)$ is elementary abelian of order 2^6. Put $N = \mathbb{N}(\langle t\rangle)/\langle t\rangle$ and $C = \mathbb{C}(t)/\langle t\rangle$. Assume by way of contradiction that the order of ig was 12. Then, $ig\langle t\rangle$ is an element of order 4 of C, since both i and g invert t and A_6 does not contain elements of order divisible by 6. The involutions $i\langle t\rangle$ and $g\langle t\rangle$ lie in $N\setminus C$. Thus, it is not possible that $i\langle t\rangle$ and $g\langle t\rangle$ would be conjugate in N. We know that $(gh)^3 = (hi)^3 = 1$ holds. Hence, g, h, and i are conjugate to each other in $\mathbb{N}(\langle t\rangle)$. This is a contradiction. We have proved that the order of ig is equal to 6.

Since $\mathbb{C}(F)$ is elementary abelian, we have

$$1 = ((ig)^2 t^{-1})^2 = (ig)^4 t ,$$

and therefore,

$$(ig)^2 = t .$$

Application of the result of [11] proves the theorem.

5. A subgroup isomorphic to M_{23}.

(5.1) LEMMA. The involution j normalizes F. We have the correspondence

$$j \to \left|\begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{matrix}\right|_F .$$

PROOF. The action of j, $gabg$, and $gacg$ on E is known. Thus, we get that $j(gabg)j = gacg$ holds *modulo* E. Hence, j normalizes EF which implies that $j \in \mathbb{N}(F)$.

We have that $j(ab)j = ac$ and $j(ac)j = ab$. Further, there are elements $e_1, e_2 \in E \cap F$ such that

$$j(gabg)j = (gacg)e_1 \quad \text{and} \quad j(gacg)j = (gabg)e_2 .$$

Therefore, we obtain the correspondence

$$j \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & \beta & 0 & 1 \\ \gamma & \delta & 1 & 0 \end{vmatrix}_F$$

with $\alpha, \beta, \gamma, \delta \in GF(2)$.

The equations $j^2 = 1$ and $(jt)^2 = 1$ give precisely two possibilities:

Case 1. $\alpha = \delta = 1$, $\beta = \gamma = 0$.

Case 2. $\alpha = \beta = \gamma = \delta = 0$.

Suppose that we are in case 1. Then, we get

$$jg \to \begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix}_F .$$

Thus, $(jg)^3$ centralizes F. Since no element of $\langle t \rangle$ acts on F in the same way as jg, we see that $\langle jg, t \rangle \mathbb{C}(F)/\mathbb{C}(F)$ is a Sylow 3-subgroup of $\mathbb{N}(F)/\mathbb{C}(F)$. Now, the same argument as in the proof of (4.1) yields a contradiction. The lemma is proved.

(5.2) Theorem. We have $(jg)^2 = 1$ and $\langle E, t, g, h, i, j \rangle$ is isomorphic to M_{23}.

Proof. The previous result implies that the order of jg is either 2 or 4.

Assume by way of contradiction that the order of jg was 4. As in the proof of (4.2) we put $N = \mathbb{N}(\langle t \rangle)/\langle t \rangle$ and $C = \mathbb{C}(t)/\langle t \rangle$. Then, $jg\langle t \rangle$ is an element of order 4 in C. The involutions $j\langle t \rangle$ and $g\langle t \rangle$ of N lie in $N \setminus C$. Hence, $j\langle t \rangle$ and $g\langle t \rangle$ are not conjugate in N. We know that $(gh)^3 = (hi)^3 = (ij)^3 = 1$ holds, and therefore, the involutions g, h, i, and j are all conjugate in $\mathbb{N}(\langle t \rangle)$. This is a contradiction. We have shown that the order of jg is equal to 2. Now, application of the result of [11] proves the assertion of the theorem.

6. The identification of G with the Mathieu-group M_{24}.

(6.1) LEMMA. The involution k normalizes F. We have the correspondence

$$k \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{vmatrix}_F .$$

PROOF. As in the proof of (5.1) we get $k(gabg)k = gbcg$ *modulo* E. Hence, k normalizes EF and F. Thus,

$$k \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \alpha & \beta & 1 & 1 \\ \gamma & \delta & 0 & 1 \end{vmatrix}_F$$

with $\alpha, \beta, \gamma, \delta \in GF(2)$.

The equations $k^2 = 1$ and $(kt)^2 = 1$ give precisely two possibilities:

Case 1. $\alpha = 0$, $\beta = \gamma = \delta = 1$.

Case 2. $\alpha = \beta = \gamma = \delta = 0$.

In case 1, we obtain that $\langle kg, t\rangle \mathrm{C}(F)/\mathrm{C}(F)$ is a Sylow 3-subgroup of $\mathrm{N}(F)/\mathrm{C}(F)$. This produces a contradiction just as in the proof of (4.1). The lemma is proved.

(6.2) THEOREM. We have $(kg)^2 = t$, and the group G is isomorphic to M_{24}.

PROOF. From (6.1) we get that the order of kg is either 6 or 12. Assume by way of contradiction that the order of kg was 12. As in (4.2) we denote by N the factor group $\mathrm{N}(\langle t\rangle)/\langle t\rangle$ and put $C = \mathrm{C}(t)/\langle t\rangle$. Then, $kg\langle t\rangle$ is an element of order 4 of C, since both k and g invert t. The involutions $k\langle t\rangle$ and $g\langle t\rangle$ of N lie in $N \setminus C$.

Hence, $k\langle t\rangle$ and $g\langle t\rangle$ are not conjugate in N. We know that $(gh)^3 = (hi)^3 = (ij)^3 = (jk)^3 = 1$ holds. Hence, g, h, i, j, and k are all conjugate to each other in $\mathbb{N}(\langle t\rangle)$. This is a contradiction which proves that $o(kg) = 6$.

It is now easy to compute that $(kg)^2$ and t act in the same way on F. Using a similar argument as that in the proof of (4.2), we get that $(kg)^2 = t$.

We apply now the result of [11] and get that

$$\langle E, t, g, h, i, j, k\rangle \cong M_{24} .$$

As $|G| = |M_{24}|$, the theorem is proved.

REFERENCES

[1] B. Beisiegel, *Über endliche einfache Gruppen mit Sylow 2-Untergruppen der Ordnung höchstens* 2^{10}, Commun. Algebra, **5** (1977), pp. 113-170.

[2] D. Gorenstein, *Finite Groups*, Harper and Row Publishers, New York-Evanston-London (1968).

[3] D. Gorenstein, *Finite Simple Groups - An Introduction to their Classification*, Plenum Press, New York-London (1982).

[4] D. Gorenstein - J. H. Walter, *On finite groups with dihedral Sylow 2-subgroups*, Ill. J. Math., **6** (1962), pp. 553-593.

[5] D. Held, *The simple groups related to* M_{24}, J. Algebra, **13** (2) (1969), pp. 253-296.

[6] D. Held, *A characterization of the alternating groups of degrees eight and nine*, J. Algebra, **7** (2) (1967), pp. 218-237.

[7] Z. Janko, *A characterization of the Mathieu simple groups - I, II*, J. Algebra, **9** (1968), pp. 1-19, 20-41.

[8] R. G. Stanton, *The Mathieu-groups*, Can. J. Math., **3** (1951), pp. 164-174.

[9] V. Stingl, *Endliche, einfache Component-Type-Gruppen, deren Ordnung nicht durch* 2^{11} *geteilt wird*, Dissertation, Mainz (1976).

[10] J. Tits, *Théorème de Bruhat et sous-groupes paraboliques*, C. R. Acad. Sci. Paris, **254** (1962), pp. 2910-2912.

[11] J. A. Todd, *Abstract definitions for the Mathieu groups*, Quart. J. Math. Oxford, (2), **21** (1970), pp. 421-424.

Manoscritto pervenuto in redazione il 30 giugno 1988.