Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 121-144

Combinatorial methods for determining subgroup structures of finite groups

CAFER CALISKAN – S. S. MAGLIVERAS –L. C. YU

Dedicated to Prof. Marialuisa J. de Resmini

Abstract: *In this paper we discuss methods that might be employed in determining the subgroup structure of a finite group G. These methods have a particularly combinatorial flavor connected with graphs, designs and the combinatorial nature of presentations of groups. In particular, the methods are illustrated for the case of the simple group $U_3(5) = PSU_3(5^2)$ whose maximal subgroups are determined up to conjugacy.*

1 – Introduction

This paper is devoted to a discussion of some methods that might be employed in determining the subgroup structure of a finite group G. The methods have a strong combinatorial flavor and are illustrated here for the case of the simple group $U_3(5) = PSU_3(5^2)$ whose maximal subgroups are determined up to conjugacy. This example possesses a measure of difficulty suitable for exemplifying these methods. The reader is assumed to be acquainted with the elements of the theory of finite groups, including finite permutation groups as for example discussed in [8], [12], [19], [20], [22]. He is also assumed to have knowledge of the rudiments of the theory of strongly regular graphs and association schemes as

Key Words and Phrases: *Finite groups – Subgroup structure – Combinatorial methods*
A.M.S. Classification: 20E32, 20E28, 05E30.

discussed in [2], [3], [9], [10], [11]. Finally, the reader should have some knowledge of the beautiful Frobenius theory of ordinary characters [6], [7], [13], [16].

2 – The controlling viewpoint

The question of whether a list of subgroups is complete for a given group G can most effectively be dealt with if anticipated. Since the minimal normal subgroups of a group are characteristically simple, every subgroup M of a finite group G normalizes some subgroup of the form $A^r = A \times A \times \cdots \times A$ with A simple. This suggests that a systematic approach to determining the subgroups structure of G could consist of determining, up to conjugacy, all characteristically simple subgroups of G and subsequently determining their normalizers. The above observation allows us to "control" the process of determining the subgroups of G, and affords a way of verifying completeness.

We usually advance with the above procedure in two stages: First, we obtain the class Λ of *local* subgroups of G, *i.e.* the normalizers of the elementary abelian subgroups of G. Subsequently, we determine the class Ξ of normalizers of the non-soluble characteristically simple groups in G. The maximal subgroups of G must clearly occur in $\Xi \cup \Lambda$. Of course, we often have that $\Xi \cap \Lambda \neq \emptyset$.

3 – Matrices belonging to subgroups

Let G be a finite group acting transitively on a set Ω, and let Γ be the graph induced on Ω by a non-trivial, self-paired orbital of G on $\Omega \times \Omega$ [9], [21], [22]. Since the orbital is self-paired and non-trivial the graph is undirected and irreflexive. If $x \in \Omega$ and r is a non-negative integer, the *circle of radius* r about x is defined to be the set

$$S_r(x) = \{y \in \Omega \ : \ d(x,y) = r\}$$

where d is the usual distance function in the graph Γ.

If $\{\Delta_1, \ldots, \Delta_\ell\}$ is a partition of Ω we denote by $[\Delta_1, \Delta_2, \ldots, \Delta_\ell]$ the collection of all subgroups of G fixing each of the Δ_i setwise. Furthermore, if $k_1, \ldots, k_\ell$ are positive integers such that

$$\sum_{i=1}^{\ell} k_i = |\Omega|,$$

we denote by $[k_1, k_2, \ldots, k_\ell]$ the collection of all subgroups of G which have orbits of lengths $k_1, k_2, \ldots, k_\ell$.

If $H \leq G$, and H has orbits $\Delta_1, \ldots, \Delta_\ell$ on Ω, for $x \in \Delta_i$ we put $a_H(i,j) = |S_1(x) \cap \Delta_j|$. We call the matrix $A_H = (a_H(i,j))$ *the matrix belonging to the subgroup* H.

Let $M = (m_{i,j})$ be an $n \times n$ matrix with non-negative integral entries and constant row sums. The *domain* of M, $\mathcal{D}(M)$ is defined to be the collection of all partitions $P = \{\Delta_i\}_{i=1}^{k}$ of $\Omega = \{1, 2, \dots , n\}$ for which $x, y \in \Delta_i$ implies that

$$\sum_{q \in \Delta_j} m_{x,q} = \sum_{q \in \Delta_j} m_{y,q} = \overline{m_{i,j}}$$

for each pair of indices i, j, $1 \le i, j \le k$. We set $M(P) = \overline{(m_{i,j})}$.

If $N = M(P)$ for some $P \in \mathcal{D}(M)$ we say that N *covers* M and write $M \le N$. We note that if $M \le N$ then N is a $k \times k$ matrix with non-negative entries, constant row sums, and $k \le n$. We write $\int M$ for the collection of all covers of M and call $\int M$ *the cover* of M. We omit the proof of the following easy consequence:

PROPOSITION 3.1. *If H, K are subgroups of G and $H \le K$, then $A_H \le A_K$.*

Thus, the mapping $H \to A_H$ is an isotone function from the lattice of subgroups of G to the partially ordered set of all covers of the adjacency matrix of Γ.

The connection of the above concept with the concepts developed by D.G. Higman [10], [11], and also by Kramer and Mesner [14], [15], is apparent. The authors wish to emphasize the utility of the concept in investigations involving the determination of subgroup structures. We give below a hint of the way in which the matrices A_H are used and use the method more extensively in the $U_3(5)$ example.

When the adjacency matrix A of the graph Γ is given, one can calculate $\int A$. If H is any subgroup of G which is intransitive on Ω, then it corresponds to a cover of A. In particular, the covers determine which partitions of Ω are stabilized by intransitive subgroups of G. To obtain a focusing effect, and ignore duplication due to conjugacy, we may select a certain cyclic subgroup H of G, determine its matrix A_H and calculate $\int A_H$. This process is especially useful when we are seeking the non-soluble simple subgroups of G which contain H or a partial normalizer of H. Usually, only very few such covers exist, and these point to partitions whose stabilizers are the desired simple subgroups. If one knows the number of orbits of a sought subgroup, or even better, the vector of orbit lengths, the number of partitions of the given type corresponding to covers of A_H is even smaller. Sometimes, other small subgroups can be used in place of cyclic groups. For example, minimal simple groups which are known to be contained in G and whose orbit structure on Ω as well as corresponding matrices are easy to obtain.

The method can be used to determine whether some intransitive subgroup H of known matrix A_H is contained in any intransitive subgroup K, thus contributing to questions of maximality of a given subgroup.

The method is, of course, useful for the study of intransitive subgroups of G, however, its effectiveness is limited to relatively small $|\Omega|$. Transitive subgroups can be handled if one considers simultaneously several transitive permutation representations of G.

4 – Two-generator subgroups

Interest in two-generator subgroups becomes justified in view of the fact that there is evidence to support a conjecture that every finite non-abelian simple group is a 2-generator group. Even if the conjecture is false, all known simple groups except possibly for a few sporadic ones, are known to be 2-generator groups. For example, all $PSL_2(q)$ can be generated by two elements, one of which is an involution [1]. If $q \neq 9$, furthermore, $PSL_2(q)$ can be generated by two elements, one of order 2 and one of order 3. It is convenient to use the following notation: the conjugacy classes of G are denoted by $K_1 = \{1\}$, $K_2, \dots, K_c$.

If x is an element of G then $C(x) = C_G(x)$ denotes the centralizer of x in G. Furthermore σ_x denotes the order of $C(x)$. If $G|\Omega$ is a group action, the *meta-rank*, $\rho(G|\Omega)$, is defined to be the number of G-orbits on Ω. We write:

(4.1) $$[K_i \times K_j \to K_k] \;=\; \{(a,b) \in K_i \times K_j \mid ab \in K_k\}, i,j,k \in \{1,\dots,c\}$$

We denote $|\,[K_i \times K_j \to K_k]\,|$ by $|K_i \times K_j \to K_k|$.

(4.2) $$\langle K_i \times K_j \to K_k\rangle \;=\; \{\langle a,b\rangle \mid (a,b) \in [K_i \times K_j \to K_k]\,\}$$

Here, $\langle a,b\rangle$ denotes the subgroup of G generated by a and b.

(4.3) $$\sigma_i \;=\; |C_G(x)|, \quad x \in K_i\,;$$

For $x_1, x_2, \dots, x_\ell \in G$,

(4.4) $$\sigma_{x_1,\dots,x_\ell} \;=\; |\bigcap_{i=1}^{\ell} C_G(x_i)| = |C_G\langle x_1,\dots,x_\ell\rangle|$$

The structure constants of the center of the group algebra are denoted by $a_{i,j,k}$; thus,

(4.5) $$K_iK_j \;=\; \sum_{k=1}^{c} a_{i,j,k}K_k \quad i,j \in \{1,\dots,c\}\,;\ \text{also,}$$

(4.6) $$a_{i,j,k} \;=\; \frac{|G|}{\sigma_i\sigma_j}\sum_{t=1}^{c}\frac{\chi_t(i)\chi_t(j)\overline{\chi_t(k)}}{\chi_t(1)}$$

where $\chi_t(i)$ is the value of the irreducible ordinary character χ_t of G on the elements of the class K_i.

We also introduce the symmetric rational constants:

$$\beta_{i,j,k} = \frac{a_{i,j,k}}{\sigma_k}, \quad i,j,k \in \{1,\dots,c\}. \tag{4.7}$$

Consider the action of G on $K_i \times K_j$ by conjugation and define the mapping

$$\begin{aligned} \phi :\ & K_i \times K_j \to G \\ \phi :\ & (x,y) \mapsto xy\,, \end{aligned}$$

then, $(x',y') \in (x,y)^G$ implies that $\phi(x',y')$ is conjugate to $\phi(x,y)$ in G. Furthermore, if z is G-conjugate to $xy \in K_i \times K_j$, then there exists $(x',y') \in (x,y)^G$ such that $\phi(x',y') = z$. Hence, ϕ is a surjection onto a union of classes of G and $[K_i \times K_j \to K_k]$ is a union of G-orbits of $K_i \times K_j$. We have that:

$$|(x,y)^G| = [G : C(x) \cap C(y)] = \frac{|G|}{\sigma_{x,y}},$$

furthermore,

$$|(x,y)^G \cap \phi^{-1}(xy)| = [C(xy) : C(x) \cap C(y)] = \frac{\sigma_{xy}}{\sigma_{x,y}}, \tag{4.8}$$

an invariant of the orbit $(x,y)^G$. Given a fixed element $z \in K_k$, $a_{i,j,k} = |\phi^{-1}(z)|$. If the G-orbits $\Omega_1, \Omega_2, \dots, \Omega_m$ of $K_i \times K_j$ and no others are carried by ϕ into K_k, choose $(x_i,y_i) \in \Omega_i$ such that $\phi(x_i,y_i) = x_iy_i = z$, we get:

$$a_{i,j,k} = \sum_{i=1}^{m} |\Omega_i \cap \phi^{-1}(z)| = \sum_{i=1}^{m} \sigma_z/\sigma_{x_i,y_i}$$

hence,

$$\beta_{i,j,k} = \sum_{i=1}^{m} \frac{1}{\sigma_{x_i,y_i}}. \tag{4.9}$$

Since $\sigma_{x_i,y_i} = \sigma_{x_i,y_i,x_iy_i}$, we obtain:

$$\sigma_{x_i,y_i} | gcd(\sigma_i, \sigma_j, \sigma_{x_iy_i}) \tag{4.10}$$

If the induced characters $\theta_i = 1_{C(x)} \uparrow^G$, $\theta_j = 1_{C(y)} \uparrow^G$, $(x,y) \in K_i \times K_j$ are known, then

$$\rho(G| K_i \times K_j) = (\theta_i, \theta_j), \tag{4.11}$$

and conditions (4.9), (4.10) and (4.11) are usually sufficient to determine the number of orbits of G on $[K_i \times K_j \to K_k]$ for each $k \in \{1, \dots, c\}$.

Now, if $(x', y') = (x, y)^g$, then $\langle x', y' \rangle = \langle x, y \rangle^g$. Hence, if we are interested in $\{\langle x, y \rangle \mid (x, y) \in K_i \times K_j\}$ up to conjugacy, it suffices to consider one pair from each G-orbit of $K_i \times K_j$. We must, however, observe that it is possible for (x, y), (x', y') to belong to different G-orbits yet $\langle x, y \rangle$ to be G-conjugate to $\langle x', y' \rangle$. Thus,

$$\rho(G| \langle K_i \times K_j \to K_k \rangle) \leq \rho(G| [K_i \times K_j \to K_k]) . \tag{4.12}$$

To determine what orbit fusion is induced when we pass from the group action $G| [K_i \times K_j \to K_k]$ to the group action $G| \langle K_i \times K_j \to K_k \rangle$, in addition to standard group action conditions we use a certain combinatorial technique which roughly speaking, involves counting the number of ways in which a fixed two-generator subgroup is generated by pairs of elements of $K_i \times K_j$. More specifically, we introduce mappings of the sort

$$f : [K_i \times K_j \to K_k] \to \langle K_i \times K_j \to K_k \rangle$$
$$f : (x, y) \to \langle x, y \rangle$$

and determine the uniform sizes of preimages $f^{-1}(\langle x, y \rangle)$. The $U_3(5)$ example involves several applications of the above ideas.

5 – Compound Characters

Let G be a finite group whose irreducible ordinary characters are $1_G, \chi_2, \chi_3, \dots, \chi_c$. If $x \in G$, $H \leq G$, then we write $g_x = |[x]|$, and $h_x = |[x] \cap H|$, where $[x] = x^G$ is the G-conjugacy class containing x.

If θ and ψ are two ordinary characters of G, we denote by (θ, ψ) their inner product in the algebra of class functions of G. If ϕ is an ordinary character of G, then $\phi = \sum_{i=1}^{c} a_i \chi_i$, with $a_i \in \mathbb{Z}^+ = \{0, 1, 2, \dots\}$. Since the collection $\{\chi_i\}_{i=1}^{c}$ forms an orthonormal basis for the algebra of class functions of G, we have that $a_i = (\phi, \chi_i)$.

If $H \leq G$, then the character θ of the transitive permutation representation

$$\pi : G \to \mathcal{S}_m \, m = [G \ : \ H]$$
$$g \to \pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$$

is the induced character $1_H \uparrow^G$ of the principle character of H to G [7], [16].

It is immediate that the following necessary conditions are satisfied by θ :

(i) $(\theta, 1_G) = 1$

(ii) $\theta(x) \in \mathbb{Z}^+$, for each $x \in G$

(iii) $(\theta, \chi_i) \leq \chi_i(1) = n_i$

(iv) $\theta(x^k) \geq \theta(x)$, for $x \in G$, $k \in \mathbb{Z}^+$

(v) $\theta(1) = [G : H]$, hence $\theta(1)$ divides $|G|$

(vi) $\theta(x) = \theta(1) \cdot (h_x/g_x)$ and therefore $\theta(1)$ divides $\theta(x) \cdot g_x$.

(vii) $(\theta, \chi_i) = (\theta, \overline{\chi_i})$, where $\overline{\chi_i}$ is the complex conjugate character of χ_i.

By a *compound character* of G we mean here any character of G satisfying conditions *(i)* to *(vii)*. Thus, the character of every transitive permutation representation of G is a compound character but there may exist compound characters which are not the characters of any transitive permutation representation of G and therefore which correspond to no subgroup H of G.

In investigating the subgroup structure of a group G whose character table is known the following question arises: "*Are there any subgroups of G of index δ?* " More generally, if it is known that G possesses a subgroup H with associated compound character θ, what are the compound characters ϕ corresponding to subgroups K of G subject to $H \leq K \leq G$? If such an intermediate subgroup exists, then

$$\theta = 1_H \uparrow^G = 1_H \uparrow^K \uparrow^G, \quad \text{and } (1_H \uparrow^K, 1_K) = 1$$

imply that:

$$\text{(viii)} \qquad (\theta, \chi_i) \geq (\phi, \chi_i), \ i \in \{1, \ldots, c\}.$$

i.e. the multiplicities of the irreducible characters of G in θ are greater than or equal to those in ϕ. Thus, there is an order inverting homomorphism from the lattice of subgroups of G into the cone $(\mathbb{Z}^+)^c$, each subgroup mapping onto a vector of multiplicities $\overline{a} = (a_1, \ldots, a_c)$ of the associated compound character. The authors, and undoubtedly others, have algorithms which answer the above question by investigating all partitions of δ :

$$\delta = 1 + \sum a_i \chi_i(1) \quad \text{for each } \delta \mid |H|, \ |H| \mid \delta,$$

and testing that the corresponding character

$$\theta = [1] + \sum a_i \chi_i$$

satisfies (i) to (viii). Such programs can be made quite efficient if the algorithms incorporate knowledge of special numerical conditions in the given character table.

6 – The Maximal Subgroups of $U_3(5)$

In this section we illustrate the methods discussed on the simple group $U_3(5)$. We obtain the following result :

Theorem 6.1. *There are eight conjugacy classes of maximal subgroups of $U_3(5)$ as follows : a) Local: $C_G(z) \cong \langle z\rangle \setminus \mathcal{S}_5$, z is an involution in G; for $Q \in Syl_5(G)$, $N_G(Q) = N_G\langle 5_1\rangle \cong Q\setminus\mathbb{Z}_8$. b) Non-local : Three conjugacy classes of self normalizing A_7's ; Three conjugacy classes of M_{10}'s each normalizing a subgroup of G isomorphic to A_6. The classes of A_7's and the classes of M_{10}'s are distinguished by the G-class of elements of order five they contain.*

LOCAL ANALYSIS

6.1 – Local 2-Subgroups

There is one conjugacy class of involutions in G, and the Sylow-2 subgroup of G is quasidihedral. Thus, the only possible elementary abelian 2-groups of order greater than 2 that can occur in G are Klein four groups $V_4 \cong C_2 \times C_2$.

Lemma 6.1. *There is exactly one conjugacy class of V_4's in G.*

Proof. $a_{2,2,2} \neq 0$ implies that there exist V_4's in G. $|C_G(z)| = 240$, $[G : C_G(z)] = 525$, and from the fusion map $C_G(z) \to G$ we compute the character of the action $G|K_2$ as

$$\theta_{525} = 1_{C(z)} \uparrow^G = [1] + [28]_1 + [28]_2 + [28]_3 + [84] + [105] + [125] + [126].$$

Hence, $\rho(G|K_2 \times K_2) = (\theta_{525}, \theta_{525}) = 8$. Computation of the $a_{2,2,k}$ (See Table 1) shows that the 8 orbits of $G|K_2 \times K_2$ are already differentiated by the class in which k lies. *i.e.* There are precisely 8 $a_{2,2,k} \neq 0$ for k lying in 8 distinct conjugacy classes, and consequently the orbits are $[K_2 \times K_2 \to K_j]$ for those j for which $a_{2,2,j} \neq 0$. Thus $[K_2 \times K_2 \to K_2]$ is a G-orbit, and there exists one conjugacy class of V_4's. □

Table 1

k	:	1	2	4	8_1	8_2	3	6	5_1	5_2	5_3	5_4	10	7_+	7_-
$a_{2,2,k}$	:	525	20	4	0	0	18	6	0	5	5	5	0	0	0
$\langle 2,2,k\rangle$	:	$\langle z\rangle$	V_4	D_4	-	-	$\mathcal{S}_3$	D_6	-	D_{5_2}	D_{5_3}	D_{5_4}	-	-	-
$\lvert\langle 2,2,k\rangle\rvert$	:	2	4	8	-	-	6	12	-	10	10	10	-	-	-

Let z be an involution of G. It is easy to verify that $C_G(z)$ acts primitively on fix(z) with kernel $\langle z\rangle$. Thus $C_G(z) \cong \langle z\rangle \setminus \mathcal{S}_5$.

Proposition 6.1. *$C_G(z)$, $|z| = 2$, is maximal in G.*

Proof. From the proof of Lemma 6.1

$$\theta_{525} = 1_{C(z)} \uparrow^G = [1] + [28]_1 + [28]_2 + [28]_3 + [84] + [105] + [125] + [126].$$

Suppose $C(z)$ is not maximal, then there exists $H \leq G$ such that $C(z) \lneqq H \lneqq G$ and $[G : H] \mid 3 \cdot 5^2 \cdot 7$. By considering compound characters of degrees $\delta \mid 3 \cdot 5^2 \cdot 7$, we rule out all but one case, namely the case $[G : H] = 175$. In this case H would be a group of order $720 = 2^4 \cdot 3^2 \cdot 5$, $[G : H] = 175$, and $\theta_{175} = 1_H \uparrow^G = [1] + [125] + [21] + [28]_i$ for $i \in \{1, 2, 3\}$. We note that character [21] does not appear in $1_{C(z)} \uparrow^G$, a contradiction to 5.(viii). Hence $C(z)$ is maximal. □

6.1.1 – $C_G(V_4)$, $N_G(V_4)$

$a_{2,2,2} = 20$ implies that $\beta_{2,2,2} = 20/240 = 1/12$; but the number of orbits of G on $[K_2 \times K_2 \to K_2]$ is 1. Therefore $\beta_{2,2,2} = \frac{1}{|C(V_4)|} \Rightarrow |C(V_4)| = 12$. $N(V_4)/C(V_4) \overset{\sim}{\leq} Aut V_4 \cong GL_2(2) \cong \mathcal{S}_3 \Rightarrow |N(V_4)|$ divides $6 \cdot 12 = 72$. Consider an A_7 inside G, and represent A_7 in its canonical representation. Let $V_4 = [1, (12)(34), (13)(24), (14)(23)] \leq A_7$, then $C_{A_7}(V_4) = V_4 \times \langle\sigma\rangle$ where $\sigma = (567)$. Therefore $C_G(V_4) = C_{A_7}(V_4) \cong V_4 \times \mathbb{Z}_3$. The elements $\rho = (23)(56)$, $z = (234)$ normalize V_4 in A_7; thus $\langle V_4, \sigma, \rho, z\rangle \subseteq N_{A_7}(V_4) \subseteq N_G(V_4)$. But $|\langle V_4, \sigma, \rho, z\rangle| = 72$ implies that $|N_G(V_4)| = 72$ and $N_G(V_4) = N_{A_7}(V_4)$. Therefore, $N_G(V_4) \leq A_7$, *i.e.* $N_G(V_4)$ is not maximal. It follows from the above that the structure of $N(V_4)$ is $(V_4 \times \mathbb{Z}_3) \setminus \mathcal{S}_3$; in fact, since $\langle\rho, z\rangle \leq N(V_4)$, $\langle\rho, z\rangle \cong \mathcal{S}_3$ and $\langle\rho, z\rangle \cap \langle V_4, \sigma\rangle = 1$, the extension splits.

6.2 – Local 3-groups

Clearly, there is one conjugacy class of $\mathbb{Z}_3$'s and one class of $\mathbb{Z}_3 \times \mathbb{Z}_3$'s in G. We will now investigate the structures of $C_G(\mathbb{Z}_3)$, $N_G(\mathbb{Z}_3)$, $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$, $N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

LEMMA 6.2. *Let* $\sigma \in G$, $|\sigma| = 3$, *then* $C_G(\sigma) \cong \mathbb{Z}_3 \times A_4$.

PROOF. Take $\sigma \in 3 \cdot 1^4$ in A_7, then $C_{A_7}(\sigma) = \mathbb{Z}_3 \times A_4 \leq A_7$, but $|C_G(\sigma)| = 36$, therefore $C_G(\sigma) \cong \mathbb{Z}_3 \times A_4$. □

REMARK 6.1 Since $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \subseteq C_G(\mathbb{Z}_3) \cong \mathbb{Z}_3 \times A_4 \leq A_7$, neither of $C_G(\mathbb{Z}_3)$, $C_G((\mathbb{Z}_3 \times \mathbb{Z}_3))$ are maximal. Since there is exactly one conjugacy class of elts of order 3, $|N_G(\mathbb{Z}_3)| = 2|C_G(\mathbb{Z}_3)|$, hence $|N_G(\mathbb{Z}_3)| = 2^3 \cdot 3^2$ and $N_G(\mathbb{Z}_3) \cong C_G(\mathbb{Z}_3) \setminus \mathbb{Z}_2$.

LEMMA 6.3. *If* $\sigma = (123)(4)(5)(6)(7) \in A_7 \leq G$, *then* $N_G\langle\sigma\rangle = N_{A_7}\langle\sigma\rangle$.

PROOF. $C_{A_7}(\sigma) = \langle\sigma\rangle \times A_4$ with A_4 on $\{4, 5, 6, 7\}$; furthermore, $\nu = (23)(45)$ normalizes $\langle\sigma\rangle = \{1, \sigma, \sigma^2\}$. Hence, $\langle C_{A_7}(\sigma), \nu\rangle \subseteq N_{A_7}(\sigma)$, but $|\langle C_{A_7}(\sigma), \nu\rangle| = 72$; therefore, $N_G(\langle\sigma\rangle) = N_{A_7}(\langle\sigma\rangle) = \langle C_{A_7}(\sigma), \nu\rangle \leq A_7$. □

COROLLARY 6.1. $N_G(\mathbb{Z}_3)$ *is not maximal in* G.

LEMMA 6.4. *The Sylow-*3 *subgroups in* G *are self-centralizing in* G.

PROOF. $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \subseteq C_G(\mathbb{Z}_3) = C_{A_7}(3 \cdot 1^4) \cong \mathbb{Z}_3 \times A_4$. It suffices to find $C_{C_3 \times A_4}(\mathbb{Z}_3 \times \mathbb{Z}_3)$. But easily, $C_{\mathbb{Z}_3 \times A_4}(\mathbb{Z}_3 \times \mathbb{Z}_3) = \mathbb{Z}_3 \times \mathbb{Z}_3$. □

In 6.9 we prove that there exists a subgroup S of G with $S \cong M_{10}$, M_{10} the Mathieu group on 10 letters. M_{10} is transitive on the 10 letters and the order of the stabilizer of a point, M_{10_x}, is 72. Let $H = M_{10_x}$; the values of the induced character $1_H \uparrow^{M_{10}}$ on the conjugacy classes yield that there will be exactly 8 elements of order 3 in H and 63 elements of 2-power orders 2^a. Therefore, if $T \in Syl_3(G)$, $|N_G(T)| \geq 72$. Now,

$$N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)/C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \mathrel{\tilde{\leq}} Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$$

implies that

$$|N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)| \textit{ divides } 9 \cdot |GL_2(3)| = 3^3 \cdot 2^4.$$

Therefore, $|N| = 72$ or $2 \cdot 72$. But by Sylow's Theorem, $2 \cdot 72$ is ruled out. Hence, $|N| = 72$, and

$$N_G(\mathbb{Z}_3 \times \mathbb{Z}_3) = N_{M_{10}}(\mathbb{Z}_3 \times \mathbb{Z}_3) \leq M_{10}.$$

COROLLARY 6.2. $N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$ *is not maximal in* G.

6.3 – Local 5-groups

Since $Q \in Syl_5(G)$ is non-abelian of order 5^3 and contain no elements of order 25, Q must have the presentation:

$$Q = \langle \alpha, \beta, \gamma \mid \alpha^5 = \beta^5 = \gamma^5 = 1,\ \alpha^\gamma = \alpha,\ \beta^\gamma = \beta,\ [\alpha, \beta] = \gamma \rangle.$$

The elements of Q can be written in the form $\alpha^k \beta^l \gamma^m$; $k, l, m \in \mathbb{Z}_5$, and $\mathbb{Z}(Q) = \langle \gamma \rangle$. Since $\alpha^\beta = \alpha^4\gamma$, $\beta^\alpha = \beta\gamma^4$, the conjugacy class in Q of a non-central element x is the coset $\langle \gamma \rangle x$. Thus Q contains 24 non-central classes each of size 5.

Lemma 6.5. *The central element γ must belong to 5_1 and Q consists of exactly*

1. *the identity*
2. 4 *elements of type* 5_1
3. 40 *elements of each of types* 5_2*,* 5_3*,* 5_4*.*

Proof. $Q \trianglelefteq N_G(Q)$, $\theta_{126} = 1_{N_G(Q)} \uparrow^G = [1] + [125]$ and $\theta_{126}(5_2) = \theta_{126}(5_3) = \theta_{126}(5_4)$, $|C_G(5_i)| = 25$, $i = 1, 2, 3, 4$ imply that Q contains exactly 40 elements of each 5_i, $i \in \{1, 2, 3, 4\}$. ∎

From the character table of G follows that $|C_G(\gamma)| = 2 \cdot 5^3$. But $\langle \gamma \rangle$ is a characteristic subgroup of Q which implies that $N_G(Q) \leq N_G(Y)$. Therefore $|N_G(Q)| \mid 4 \cdot |C_G(Y)| = 2^3 \cdot 5^3$. By Sylow's Theorem, it follows that $|N_G(Q)| = 2^3 \cdot 5^3$. By [18], $N_G(Q) \cong Q \setminus \mathbb{Z}_8$ and every element of order 5 is conjugate to its powers. Thus there are exactly four conjugacy classes of $\mathbb{Z}_5$'s in G, namely $\langle 5_1 \rangle$, $\langle 5_2 \rangle$, $\langle 5_3 \rangle$, $\langle 5_4 \rangle$.

The structure and maximality of $N\langle 5_1 \rangle$.

Since $|\sigma| = 5 \Rightarrow \sigma \sim \sigma^k$, $k = 1, 2, 3, 4$, we have that $|N\langle 5_i \rangle| = 4 \cdot |C\langle 5_i \rangle|$. Hence $|N\langle 5_1 \rangle| = 1000$; $|N\langle 5_i \rangle| = 100$ if $i \in \{2, 3, 4\}$. Hence, $N(Q) = N\langle 5_1 \rangle \cong Q \setminus \mathbb{Z}_8$.

Proposition 6.2. *$N\langle 5_1 \rangle$ is maximal in G.*

Proof. $[G : N\langle 5_1 \rangle] = \frac{126000}{1000} = 126$. The character of the transitive permutation representation of G on the right cosets of $N_G\langle 5_1 \rangle$ is $\theta_{126} = 1_{N\langle 5_1 \rangle} \uparrow^G = [1] + [125]$; therefore, the representation is doubly-transitive, hence it is primitive and consequently, the stabilizer of a point, namely $N\langle 5_1 \rangle$ is maximal. ∎

Lemma 6.6. *$i \in \{2,3,4\} \Rightarrow \langle 5_1, 5_i \rangle$ contains exactly*

1. *the identity*
2. *4 elements of type 5_1*
3. *20 elements from class 5_i.*

Proof. Let $\gamma \in 5_1$ and $\sigma \in 5_i$, $i \neq 1$, such that $\sigma^\gamma = \sigma$. Also let $Q \in Syl_5(G)$ such that $\langle \gamma, \sigma \rangle \leq Q$. Then $y \in \langle \gamma \rangle x \Rightarrow y$ is Q-conjugate to $x \Rightarrow y$ is G-conjugate to x. But also, $x \sim x^k$ for any $k \not\equiv 0$ $(mod\ 5)$. □

Proposition 6.3. *$N\langle 5_i \rangle \leq \langle 5_1 \rangle$ if $i \in \{1,2,3,4\}$. Consequently, for $i \neq 1$ $N\langle 5_i \rangle$ are not maximal.*

Proof. Obvious for $i = 1$. Consider now the case where $i > 1$. If $\sigma \in N\langle 5_i \rangle$, then σ normalizes $C(5_i) = \langle 5_1, 5_i \rangle$. Let $\gamma \in 5_1 \cap C(5_i)$, then by Lemma 6.6 $\gamma^\sigma \in \langle \gamma \rangle \Rightarrow \langle \gamma \rangle^\sigma = \langle \sigma \rangle$, *i.e.* σ normalizes $\langle 5_1 \rangle$. Therefore $N\langle 5_i \rangle \leq N\langle 5_1 \rangle$. □

Corollary 6.3. *$N\langle 5_1, 5_i \rangle \leq N\langle 5_1 \rangle$, $i \neq 1$.*

Proof. Let $\sigma \in N\langle 5_1, 5_i \rangle$ and let $\sigma \in 5_1 \cap \langle 5_1, 5_i \rangle$, then $\gamma^\sigma \in 5_1 \cap \langle 5_1, 5_i \rangle$, therefore by Lemma 6.6, $\langle \gamma \rangle^\sigma = \langle \gamma \rangle$. □

Thus, we have the following :

Proposition 6.4. *There is exactly one up to conjugacy 5-local maximal subgroup of G; it is $N\langle 5_1 \rangle = N(Q)$ of order 1000.*

6.4 – Local 7-groups

It is immediate that $N_G(\mathbb{Z}_7) \cong \mathbb{Z}_7^3$. Furthermore, since $N_{A_7}(\mathbb{Z}_7) \cong \mathbb{Z}_7^3$, we have that $N_G(\mathbb{Z}_7) \leq A_7$ and consequently $N_G(\mathbb{Z}_7)$ is not maximal.

6.5 – Non-local Subgroups

Proposition 6.5. *If $H \leq G$, H non-abelian simple group, then H is isomorphic to one of the following: A_5, $PSL_2(7)$, A_6, A_7.*

PROOF. No simple groups not occurring in L.E.Dickson's list are found in the Higman-Sims group [18]. Hence, since $G \leq HS$, the only possible simple groups contained in G must occur in Dickson's list. By consideration of order, the possible non-abelian simple groups are: A_5, A_6, A_7, $PSL_2(7)$, $PSL_2(8)$. However $PSL_2(8) \nleq HS$, therefore, $PSL_2(8) \nleq G$. ∎

REMARK 6.2. Each of above indeed occurs in G. To see this we note that $A_7 \overset{\sim}{\leq} G$ and therefore A_6, A_5, $PSL_2(7)$ which are contained in A_7 are subgroups of G. There remains to determine the number of conjugacy classes of each of the above, and their normalizers.

6.6 – The set $[K_2 \times K_3 \to K_7]$

From $|K_2 \times K_3| = \frac{|G|}{240} \cdot \frac{|G|}{36} = 2^2 \cdot 3 \cdot 5^5 \cdot 7^2$, $|K_2 \times K_3 \to K_{7_+}| = a_{2,3,7_+} \cdot \frac{|G|}{7} = 3 \cdot |G|$, $|K_2 \times K_3 \to K_{7_-}| = 3 \cdot |G|$, $a_{2,3,7_+}|_{L_2(7)} = 7$, $|K_2 \times K_3 \to K_{7_+}|_{L_2(7)}| = 168$, we have:

$$\#L_2(7)'s = \frac{|K_2 \times K_3 \to K_7|}{2 \cdot 168} = 2250.$$

Let Ω be the set of all $L_2(7)$'s in G and consider the group action $G|\Omega$ by conjugation. The length of an orbit, say L^G, $L \in \Omega$, is $|L^G| = [G : G_L]$ where $G_L = N_G(L)$. Hence, if there are k orbits with representatives L_i, $i = 1, 2, \dots, k$, we have

$$\sum_{i=1}^{k} [G : G_{L_i}] = 2 \cdot 3^2 \cdot 5^3.$$

Therefore, $2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot \sum_{i=1}^{k} \frac{1}{|N_G(L_i)|} = 2 \cdot 3^2 \cdot 5^3 \Rightarrow\ 2^3 \cdot 7 \cdot \sum_{i=1}^{k} \frac{1}{|N(L_i)|} = 1$. Now since $L \in \Omega$ implies that $C_G(L) = 1$, if we write $|\frac{N(L_i)}{L_i}| = \ell_i$ we have:

$$\frac{1}{168} \sum_{i=1}^{k} \frac{1}{\ell_i} = \frac{1}{2^3 \cdot 7}.$$

Hence, in particular $\sum_{i=1}^{k} \frac{1}{\ell_i} = 3$ and $k \geq 3$. Consider the group action $G|[K_2 \times K_3 \to K_{7_+}]$ by conjugation. We have the following:

LEMMA 6.7. *The number of G orbits on $[K_2 \times K_3 \to K_{7_+}]$ is three.*

PROOF. Since $g.c.d(\sigma_2, \sigma_3, \sigma_7) = 1$, $\rho(G|[K_2 \times K_3 \to K_{7_+}]) = \beta_{2,3,7_+} = \frac{a_{2,3,7_+}}{7} = \frac{21}{7} = 3$. ∎

Every $\langle x,y\rangle$ such that $|x|=2$, $|y|=3$, $|xy|=7$ can be thought of as a $(2,3,7_+)$; for either $xy\in 7_+$ in which case $(x,y)\in[K_2\times K_3\to K_{7_+}]$ or else $xy\in 7_-$ in which case $y^{-1}x^{-1}\in 7_+$ and $\langle x,y\rangle=\langle x^{-1},y^{-1}\rangle\in(2,3,7_+)$.

If (x,y), $(x',y')\in\ [K_2\times K_3\to K_{7_+}]$ and (x,y) is G-conjugate to (x',y'), then clearly $\langle x,y\rangle$ is G-conjugate to (x',y'). Therefore, if $\Omega=\{H\leq G\mid H\cong L_2(7)\}$, then $\rho(G|\Omega)\leq\rho(G|[K_2\times K_3\to K_{7_+}])=3$.

Corollary 6.4. *$k=3$, $\ell_i=1$ for $i\in\{1,2,3\}$. i.e. each $PSL_2(7)$ in G is self-normalizing.*

6.7 – The conjugacy classes of A_5's in G

If $H\cong A_5$, then $H\in(2,3,4)$. Since $\beta_{2,3,5_1}=0$, $\beta_{2,3,5_i}=1$ for $i\in\{2,3,4\}$ and $gcd(\sigma_2,\sigma_3,\sigma_{5_i})=1$ for $i>1$ it follows that there are exactly 3 conjugacy classes of A_5's in G one for each 5_i, $i>1$. Consider $A_{5_i}=\langle x,y\rangle$, $(x,y)\in[K_2\times K_3\to K_{5_i}]$. $C(A_{5_i})=C(x)\cap C(y)\cap C(xy)=1$, implies that each A_5 is centralized by 1. $N(A_5)/C(A_5)\ \tilde{\leq}\ AutA_5\cong\mathcal{S}_5$. Therefore, $|N(A_5)|\mid 5!$, hence $N(A_5)\cong A_5$ or $\mathcal{S}_5$.

Consider $[K_2\times K_3\to K_{5_i}]$ for a fixed $i\in\{2,3,4\}$. Then, $|K_2\times K_3\to K_{5_i}|=a_{2,3,5_i}\cdot\frac{|G|}{25}=|G|$. Consider the mapping $\Phi:[K_2\times K_3\to K_{5_i}]\to\Lambda_i$, $i\in\{2,3,4\}$, where Λ_i is the conjugacy class of A_5's of type $(2,3,5_i)$, defined by $\Phi(x,y)=\langle x,y\rangle$. Then $H\in\Lambda_i\ \Rightarrow\ |\Phi^{-1}(H)|=|K_2\times K_3\to K_5|_{|A_5}$.
Hence, $|\Lambda_i|=\frac{2^4\cdot3^2\cdot5^3\cdot7}{3\cdot4\cdot2\cdot5}=2\cdot3\cdot5^2\cdot7$.

On the other hand

$$|\Lambda_i|=[G:N_G(H)],\ H\in\Lambda_i.$$

Hence, $\frac{2^4\cdot3^2\cdot5^3\cdot7}{2^2\cdot3\cdot5}\ \sum_{i=1}^{3}\frac{1}{n_i}=2\cdot3^2\cdot5^2\cdot7=|\Lambda_2|+|\Lambda_3|+|\Lambda_4|$.

Hence, $\sum_{i=1}^{3}\frac{1}{n_i}=\frac{3}{2}$, and consequently, each $n_i=2$. Thus, there is a unique up to conjugacy A_{5_i} for each $i\in\{2,3,4\}$ and each of these A_5's are contained in a corresponding $\mathcal{S}_5$. We will show later that none of the above $\mathcal{S}_5$'s is maximal in G.

6.8 – Groups containing $\mathbb{Z}_7^3$

It is well known that the full automorphism group of the Hoffman-Singleton graph on 50 verices is a split extension of our group $G=U_3(5)$ by a group of order 2 [17] [4]. In [17] the Higman-Sims graph of 100 vertices is viewed as the union of two Hoffman-Singleton graphs with appropriate interconnections between the two subgraphs on 50 vertices. In particular $U_3(5)$ acts intransitively on the 100 vertices of the Higman-Sims graph, and transitively, of rank 3, on each of the two Hoffman-Singleton subgraphs of the Higman-Sims graph. In what follows we consider the transitive, rank-3 action of G on the 50 vertices Ω of the Hoffman-Singleton graph. In view of the discussion in Section 5, the character of the action $G|\Omega$ must be of the form $\chi = [1] + [21] + [28]_i$ for some $i \in \{1, 2, 3\}$.

Suppose a subgroup H of G contains $\mathbb{Z}_7^3$ then

$$A_H \geq A_{\mathbb{Z}_7^3} = \begin{pmatrix} 0 & 7 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 3 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 1 & 0 & 3 & 0 & 3 \\ 0 & 1 & 2 & 1 & 1 & 2 \end{pmatrix}$$

Suppose $H \leq G$, $[G : H] = 50$, then $1_H \uparrow^G = [1] + [21] + [28]_j$, $j \in \{1, 2, 3\}$ $\Rightarrow$ $\#[\text{Orbits of } H \text{ on } \Omega] = (1_H \uparrow^G, \chi) = 3$ or 2.

Lemma 6.8. *If $H \cong A_7$, $H \leq G$, then $H \in [1, 7, 42] \cup [15, 35]$.*

Proof. $[G : H] = 50$. Via consideration of the possible compound characters of degree 50, we see as above that H has 2 or 3 orbits on the canonical set of 50 points. If there are 2 orbits then it easily follows that $A_7 \in [15, 35]$ by consideration of the possible transitive representations of A_7 on ≤ 50 points. Otherwise if A_7 has 3 orbits, the least orbit is of length $\leq [\frac{50}{3}] = 16$, hence of length $1, 7$ *or* 15. If the least orbit has length $= 1$ then $49 = k + \ell$, and A_7 acts transitively on k (as well as ℓ) points, therefore $k = 7$, $\ell = 42$. If the least orbit has length > 1 then by considering the possible transitive representations of A_7 we see that no assignment to k and ℓ is possible. Hence the least orbit must be of length 1. Clearly there is an $A_7 \in [1, 7, 42]$, since G_α in the canonical representation of G on 50 points is isomorphic to A_7. Since G is transitive on 50 points all A_7's with orbit structure $[1, 7, 42]$ are conjugate. □

Now we will show that there are two other conjugacy classes of A_7's in G, which in the standard representation $G|\Omega$ have orbit types $[15, 35]$.

Lemma 6.9. *If*

$$\begin{aligned} \sigma =& (1)(2\ 11\ 6\ 5\ 26\ 16\ 21)(3\ 39\ 31\ 30\ 36\ 50\ 41) \\ & (4\ 29\ 32\ 33\ 17\ 46\ 9)(7\ 14\ 43\ 25\ 34\ 19\ 47) \\ & (8\ 20\ 28\ 40\ 24\ 27\ 13)(10\ 49\ 42\ 23\ 22\ 35\ 48) \\ & (12\ 44\ 37\ 15\ 45\ 18\ 38) \in G \end{aligned}$$

and cycles of σ *are labelled* $PABCDEFK$, *then* $\mathbb{Z}_7^3 = N_G\langle\sigma\rangle \in [P, A, CFK, B, E, D] : [1, 7, 21, 7, 7, 7]$, *and any cover of* $\mathbb{Z}_7^3$ *with two orbits has orbit type* $[PED, ABCFK]$ *or* $[PBD, ACEFK]$.

Proof. This follows immediately by the discussion of section 3 and $A_{\mathbb{Z}_7^3}$. □

Corollary 6.5. *If* $H \cong A_7$, $H \leq G$ *and* H *has two orbits on* Ω, *then* $H \in [PED, ABCFK] \cup [PBD, ACEFK]$ *and consequently there can be at most* 3 *conjugacy classes of* A_7*'s in* G.

Definition 6.1. *Let* $\Delta_1 = PED \subseteq \Omega$ *and* $\Delta_2 = PBD \subseteq \Omega$, *then we call a subset* $\Gamma \subseteq \Omega$ *a decapentad of type* 1 *if and only if* $\Gamma^g = \Delta_1$ *for some* $g \in G$, *or a decapentad of type* 2 *if and only if* $\Gamma^g = \Delta_2$ *for some* $g \in G$. *Computation shows there are precisely* 50 *decapentads of each type.*

Let $\Lambda_i = \Delta_i^G$. Then G acts transitively on Λ_1, Λ_2 and $|G_{(\Delta_i)}| = \frac{|G|}{50} = \frac{7!}{2}$. Hence each $G_{(\Delta_1)}$, $G_{(\Delta_2)}$ are subgroups of G of order $\frac{7!}{2}$ and $G_{(\Delta_1)}$ is not G-conjugate to $G_{(\Delta_2)}$ since $\Delta_2 \notin \Lambda_i$.

Proposition 6.6. $G_{(\Delta_1)} \cong G_{(\Delta_2)} \cong A_7$.

Proof. $G_{(\Delta_1)}$ has a representation on the 15 points of Δ_1. Since $G_{(\Delta_1)}$ has at most 3 orbits on Ω and since by consideration of $A_{\mathbb{Z}_7^3}$, $P\underline{ED}$ or PED are the only possible orbit structures, $G_{(\Delta_1)}$ is transitive on Δ_1. $H = G_{(\Delta_1)}$ acts primitively on Δ_1, for if $H_\alpha \lneqq K \leq H$, then K would have orbit type $[8, 7]$ or $[15]$ on Δ_1. But $K \supseteq \mathbb{Z}_7^3$, since $H_\alpha \supseteq \mathbb{Z}_7^3$, hence $[8, 7]$ is not possible. Therefore, K would be transitive on Δ_1, and consequently $|K| = |K_\alpha| \cdot 15$. But clearly $K_\alpha = H_\alpha$ and therefore $K = H$.

It is known however [5] that the only primitive group on 15 points of order $\frac{7!}{2}$ is a group isomorphic to A_7. Therefore, $G_{(\Delta_1)} \cong A_7$. Similarly $G_{(\Delta_2)} \cong A_7$. □

Corollary 6.6. *There are at least three conjugacy classes of* A_7*'s namely* $A_{7_1} \cong G_\alpha$, $A_{7_2} \cong G_{(\Delta_1)}$, $A_{7_3} \cong G_{(\Delta_2)}$. *Hence there are exactly* 3 *conjugacy classes of* A_7*'s in* G.

The standard representation is $G|\{\text{right cosets of } A_{7_1}\}$. Since $\chi = [1]+[21]+[28]_i$ for some i, and since $\#[orb] = 3$, without loss of generality we take:

$$\chi = \chi_1 = 1_{A_{7_1}} \uparrow^G = 1 + [21] + [28]_1.$$

Since A_{7_2}, A_{7_3} have 2 orbits on Ω, without loss of generality

$$1_{A_{7_2}} \uparrow^G = 1 + [21] + [28]_2$$
and
$$1_{A_{7_3}} \uparrow^G = 1 + [21] + [28]_3.$$

Therefore, the elements of order 5 in A_{7_2} or A_{7_3} come from $5_3 \cup 5_2$. Clearly, there is a 3 way symmetry of the above argument relating the representation of G on the cosets of A_7's to the 3 types of A_7's. Therefore each induced character involves each $[28]_i$ exclusively. Hence, $5_2 \in A_{7_1}$, $5_3 \in A_{7_2}$, $5_4 \in A_{7_3}$.

Now we investigate the normalizer $N_G(A_{5_i}) \cong \mathcal{S}_5$. Since each A_{5_i} is contained in an appropriate A_{7_i} and the normalizer in A_{7_i} of A_{5_i} is isomorphic to $\mathcal{S}_5$, $N_G(A_{5_i}) \leq A_{7_i}$, and therefore $N_G(A_{5_i})$ are not maximal in G. Of course $N_G(A_7) = A_{7_i}$ are maximal since there are no permutation characters for G of degree less than 50.

6.9 – The A_6's and their normalizers

Suppose $H \leq G$, $H \cong PGL_2(9)$, then $[G : H] = 175$. Therefore, $\chi = 1_H \uparrow^G = 1 + [125] + [21] + [28]_i \;\; i \in \{1, 2, 3\} \Rightarrow \; \chi(2) = 1 + 5 + 5 + 4 + 15$. But $\chi(2)$ should be $\sigma_G(2)(\frac{1}{\sigma_H(2_1)} + \frac{1}{\sigma_H(2_2)}) = 240(\frac{1}{16} + \frac{1}{20}) = 27$, a contradiction. Hence no subgroup of G is isomorphic to $PGL_2(9)$.

Suppose next that there exists $H \leq G$, $H \cong \mathcal{S}_6$. Then $\chi(2) = 240(\frac{1}{48} + \frac{1}{16} + \frac{1}{48}) = 25$, a contradiction; therefore $\mathcal{S}_6 \not\leq G$.

Hence if $A_6 \lhd H \lneq G$, then $H \cong M_{10}$. Consider $\Omega = [K_2 \times K_4 \to K_{5_i}]$ $i \in \{2, 3, 4\}$ fixed. $|\Omega| = 75 \cdot |K_{5_i}| = 2^4 \cdot 3^3 \cdot 5^3 \cdot 7$ (Since $a_{2,4,5_i} = 75$). Let $S \subseteq \Omega$ be defined by:

$$(x, y) \in S \text{if and only if } \langle x, y\rangle \cong \mathcal{S}_5$$

$$S \neq \emptyset, \text{ since there exists } H \leq G, \; H \cong \mathcal{S}_5 \in (2, 4, 5_i).$$

There exists a mapping Φ from S into the collection of all subgroups of G, namely

$$\Phi : (x, y) \to \langle x, y\rangle.$$

We have

$$|\Phi(S)| = \#[of\ S_5\ with\ a\ 5_i] = [G : \mathcal{S}_5] = 2 \cdot 3 \cdot 5^2 \cdot 7$$

any $H \in \Phi(S)$ is generated in 120 ways as $\langle x, y\rangle \quad |x| = 2,\ |y| = 4,\ |xy| = 5,$ $x, y \in H$.

Therefore, $|S| = 120 \cdot |\Phi(S)| = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$.

Therefore, $T = \Omega \setminus S$ has $2^5 \cdot 3^2 \cdot 5^3 \cdot 7$ elements.

Now consider an A_6 with a 5_i in it. (Such exists since $A_6 \leq A_7$) If $N(A_6) = A_6$, then

$$\#[A_6's\ conjugate\ to\ this\ A_6] = [G : A_6] = 350.$$

But each A_6 is generated as a $(2, 4, 5_i)$ in $2^5 \cdot 3^2 \cdot 5$ ways. Therefore, there would be $350 \cdot 2^5 \cdot 3^2 \cdot 5$ ordered pairs in Ω yielding A_6's. But $350 \cdot 2^5 \cdot 3^2 \cdot 5 > |T| = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7$ a contradiction. Hence, $N(A_6) \cong M_{10}$ and then

$$|T| = 175 \cdot 2^5 \cdot 3^2 \cdot 5.$$

Corollary 6.7. *There are exactly* 3 *conjugacy classes of* A_6*'s one for each* $5_2, 5_3, 5_4$*, each normalized by an* M_{10}*.*

– Appendix

Generators of $PSU_3(5^2)$:

x :
$(3,17,7)(4,46,38)(5,11,21)(6,26,16)(8,36,32)(9,28,19)$
$(10,13,33)(14,47,15)(18,43,49)(20,44,23)(24,25,39)$
$(29,50,37)(30,35,41)(31,45,40)(34,42,48)$
y :
$(1,3,5,2,4)(6,28,20,12,24)(7,29,16,13,25)(8,30,17,14,21)$
$(9,26,18,15,22)(10,27,19,11,23)(36,37,38,39,40)$
$(41,45,44,43,42)(46,49,47,50,48)$

Character Table of $PSU_3(5^2)$:

x	1	2	4	8_1	8_2	3	6	5_1	5_2	5_3	5_4	10	7_1	7_2
σ_x	$\|G\|$	240	8	8	8	36	12	250	25	25	25	10	7	7
κ_x	1	525	15750	15750	15750	3500	10500	504	5040	5040	5040	12600	18000	18000
χ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_2	20	-4	0	0	0	2	2	-5	0	0	0	1	-1	-1
χ_3	28	4	0	0	0	1	1	3	3	-2	-2	-1	0	0
χ_4	28	4	0	0	0	1	1	3	-2	-2	3	-1	0	0
χ_5	28	4	0	0	0	1	1	3	-2	3	-2	-1	0	0
χ_6	21	5	1	-1	-1	3	-1	-4	1	1	1	0	0	0
χ_7	84	-4	0	0	0	3	-1	9	-1	-1	-1	1	0	0
χ_8	126	6	-2	0	0	0	0	1	1	1	1	1	0	0
χ_9	105	1	1	-1	-1	-3	1	5	0	0	0	1	0	0
χ_{10}	144	0	0	0	0	0	0	-6	-1	-1	-1	0	γ	δ
χ_{11}	144	0	0	0	0	0	0	-6	-1	-1	-1	0	δ	γ
χ_{12}	125	5	1	1	1	-1	-1	0	0	0	0	0	-1	-1
χ_{13}	126	-6	0	α	β	0	0	1	1	1	1	-1	0	0
χ_{14}	126	-6	0	β	α	0	0	1	1	1	1	-1	0	0

Hoffman-Singleton Graph

1/	2	5	6	11	16	21	26	26/	1	28	29	34	36	45	49
2/	1	3	7	12	17	22	27	27/	2	29	30	35	37	41	50
3/	2	4	8	13	18	23	28	28/	3	26	30	31	38	42	46
4/	3	5	9	14	19	24	29	29	4	26	27	32	39	43	47
5/	1	4	10	15	20	25	30	30/	5	27	28	33	40	44	48
6/	1	8	9	31	37	43	48	31/	6	12	20	24	28	32	35
7/	2	9	10	32	38	44	49	32/	7	13	16	25	29	31	33
8/	3	6	10	33	39	45	50	33/	8	14	17	21	30	32	34
9/	4	6	7	34	40	41	46	34/	9	15	18	22	26	33	35
10/	5	7	8	35	36	42	47	35/	10	11	19	23	27	31	34
11/	1	13	14	35	39	44	46	36/	10	13	17	24	26	37	40
12/	2	14	15	31	40	45	47	37/	6	14	18	25	27	36	38
13/	3	11	15	32	36	41	48	38/	7	15	19	21	28	37	39
14/	4	11	12	33	37	42	49	39/	8	11	20	22	29	38	40
15/	5	12	13	34	38	43	50	40/	9	12	16	23	30	36	39
16/	1	18	19	32	40	42	50	41/	9	13	20	21	27	42	45
17/	2	19	20	33	36	43	46	42/	10	14	16	22	28	41	43
18/	3	16	20	34	37	44	47	43/	6	17	23	29	15	42	44
19/	4	16	17	35	38	45	48	44/	7	11	18	24	30	43	45
20/	5	17	18	31	39	41	49	45/	8	12	19	25	26	41	44
21/	1	23	24	33	38	41	47	46/	9	11	17	25	28	47	50
22/	2	24	25	34	39	42	48	47/	10	12	18	21	29	46	48
23/	3	25	21	35	40	43	49	48/	6	13	19	30	47	49	22
24/	4	21	22	31	36	44	50	49/	7	14	20	23	26	48	50
25/	5	22	23	32	37	45	46	50/	8	15	16	24	27	46	49

Λ_1

1	1	7	8	13	14	19	20	24	25	27	28	34	40	43	47
2	2	8	9	14	15	20	16	25	21	28	29	35	36	44	48
3	3	9	10	15	11	16	17	21	22	29	30	31	37	45	49
4	4	10	6	11	12	17	18	22	23	30	26	32	38	41	50
5	5	6	7	12	13	18	19	23	24	26	27	33	39	42	46
6	11	20	4	43	45	28	21	34	2	40	32	48	50	37	10
7	6	28	29	25	18	40	2	19	11	24	33	10	41	15	49
8	5	40	32	34	38	24	11	47	6	27	17	49	3	45	42
9	16	27	17	47	44	13	5	14	26	8	9	23	31	38	22
10	21	13	46	7	37	8	26	43	16	20	4	22	30	12	35
11	39	4	49	45	6	21	46	2	35	32	36	30	15	18	42
12	31	29	42	18	5	2	9	11	48	33	50	36	45	38	23
13	36	33	22	12	16	6	29	5	49	46	3	41	38	44	35
14	50	17	35	44	21	5	32	26	42	9	39	3	12	37	48
15	41	46	48	37	2	26	33	16	23	4	31	39	44	15	10
16	17	22	21	16	45	29	37	49	10	3	11	9	15	30	31
17	46	35	2	21	18	32	15	42	49	39	6	4	45	36	30
18	13	17	1	45	42	30	23	31	4	37	34	50	47	39	7
19	14	18	2	41	43	26	24	32	5	38	35	46	48	40	8
20	15	19	3	42	44	27	25	33	1	39	31	47	49	36	9
21	7	29	30	21	19	36	3	20	12	25	34	6	42	11	50
22	10	27	28	24	17	39	1	18	15	23	32	9	45	14	48
23	1	36	33	35	39	25	12	48	7	28	18	50	4	41	43
24	2	37	34	31	40	21	13	49	8	29	19	46	5	42	44
25	3	38	35	32	36	22	14	50	9	30	20	47	1	43	45
26	7	33	29	19	36	12	22	18	6	41	28	23	16	50	5
27	8	34	30	20	37	13	23	19	7	42	29	24	17	46	1
28	9	35	26	16	38	14	24	20	8	43	30	25	18	47	2
29	10	31	27	17	39	15	25	16	9	44	26	21	19	48	3
30	27	18	25	13	28	1	12	10	43	39	9	49	19	48	3
31	28	19	21	14	29	2	13	6	44	40	10	50	20	25	34
32	29	20	22	15	30	3	14	7	45	36	6	46	16	21	35
33	30	16	23	11	26	4	15	8	41	37	7	47	17	22	31
34	17	47	28	45	14	27	7	5	24	13	16	6	39	23	34
35	18	48	29	41	15	28	8	1	25	14	17	7	40	20	35
36	19	49	30	42	11	29	9	2	21	15	18	8	36	25	31
37	24	7	11	40	6	19	3	27	25	42	26	47	15	33	20
38	25	8	12	36	7	20	4	28	21	43	27	48	11	34	16
39	33	18	26	2	4	50	10	48	38	41	43	31	40	25	11
40	34	19	27	3	5	46	6	49	39	42	44	32	36	21	12
41	35	20	28	4	1	47	7	50	40	43	45	33	37	22	13
42	39	5	31	19	9	47	26	2	44	13	37	50	42	33	23
43	40	1	32	20	10	48	27	3	45	14	38	46	43	34	24
44	30	2	50	45	47	23	36	20	34	32	11	38	4	42	6
45	26	3	46	41	48	24	37	16	35	33	12	39	5	43	7
46	27	4	47	42	49	25	38	17	31	34	13	40	1	44	8
47	28	5	48	43	50	21	39	18	32	35	14	36	2	45	9
48	34	2	24	11	5	49	28	8	47	37	19	41	32	40	43
49	31	4	21	13	2	46	30	10	49	39	16	43	34	37	45
50	32	5	22	14	3	47	26	6	50	40	17	44	35	38	41

Λ_2

1	1	3	7	14	19	25	30	31	34	36	39	41	43	47	50
2	2	4	8	15	20	21	26	32	35	37	40	42	44	48	46
3	3	5	9	11	16	22	27	33	31	38	36	43	45	49	47
4	4	1	10	12	17	23	28	34	32	39	37	44	41	50	48
5	5	2	6	13	18	24	29	35	33	40	38	45	42	46	49
6	11	29	20	45	28	2	16	33	48	15	24	23	37	10	9
7	6	32	28	18	40	11	21	17	10	45	27	22	15	49	4
8	26	17	24	12	27	5	11	9	42	38	8	48	18	23	32
9	16	46	27	44	13	26	6	4	23	12	20	10	38	22	33
10	21	9	13	37	8	16	5	29	22	44	28	49	12	35	17
11	39	26	4	6	21	35	13	17	30	12	50	25	18	42	7
12	31	16	29	5	2	48	8	46	36	44	41	34	38	23	14
13	30	21	32	26	11	10	20	9	50	37	3	19	12	22	43
14	36	2	33	16	6	49	28	4	41	15	39	47	44	35	25
15	50	11	17	21	5	42	40	29	3	45	31	7	37	48	34
16	41	6	46	2	26	23	24	32	39	18	30	14	15	10	19
17	29	1	49	44	46	22	40	19	33	31	15	37	3	41	10
18	32	1	42	37	9	35	24	47	17	30	45	15	39	3	49
19	33	1	23	15	4	48	27	7	46	36	18	45	31	39	42
20	17	1	22	45	29	10	13	14	9	50	38	18	30	31	23
21	46	1	35	18	32	49	8	43	4	41	12	38	36	30	22
22	9	1	48	38	33	42	20	25	29	3	44	12	50	36	35
23	12	30	16	41	29	3	17	34	49	11	25	24	38	6	10
24	14	27	18	43	26	5	19	31	46	13	22	21	40	8	7
25	15	28	19	44	27	1	20	32	47	14	23	22	36	9	8
26	40	5	50	41	7	22	47	3	31	33	37	26	11	19	43
27	36	1	46	42	8	23	48	4	32	34	38	27	12	20	44
28	37	2	47	43	9	24	49	5	33	35	39	28	13	16	45
29	38	3	48	44	10	25	50	1	34	31	40	29	14	17	41
30	32	30	43	19	1	3	10	12	49	34	46	37	41	39	24
31	33	26	44	20	2	4	6	13	50	35	47	38	42	40	25
32	34	27	45	16	3	5	7	14	46	31	48	39	43	36	21
33	35	28	41	17	4	1	8	15	47	32	49	40	44	37	22
34	40	32	21	11	20	10	28	4	48	50	2	45	37	43	34
35	46	18	31	45	22	1	33	27	43	10	40	4	13	38	49
36	47	19	32	41	23	2	34	28	44	6	36	5	14	39	50
37	48	20	33	42	24	3	35	29	45	7	37	1	15	40	46
38	49	16	34	43	25	4	31	30	41	8	38	2	11	36	47
39	8	46	1	18	23	36	22	30	29	15	19	41	7	31	14
40	43	38	11	3	25	16	27	33	26	12	48	9	10	24	20
41	25	12	6	39	34	21	13	17	16	44	10	4	49	27	28
42	19	37	26	30	47	11	20	9	2	15	42	32	23	8	24
43	47	15	16	36	7	6	28	4	11	45	23	33	22	20	27
44	7	45	21	50	14	5	40	29	6	18	22	17	35	28	13
45	43	33	50	11	7	41	31	40	37	19	47	26	22	5	3
46	25	17	41	6	14	3	30	24	15	47	7	16	35	26	39
47	19	9	39	26	25	31	50	13	18	14	43	2	10	21	30
48	42	8	24	13	9	30	1	12	18	35	17	29	38	25	49
49	22	28	13	20	29	50	1	37	12	10	9	33	44	19	23
50	1	50	17	48	31	34	44	10	14	40	38	41	29	3	25

Acknowledgement

The second author wishes to express his thanks to the Institute for Experimental Mathematics, University of Essen, Germany, and to the Centre for Applied Cryptographic Research, University of Waterloo, Canada, whose hospitality he enjoyed while carrying out parts of this work. Thanks also to L. Babai and E. Luks for many helpful comments.
Research supported in part by National Science Foundation grant CCR- 9610138.

REFERENCES

[1] A. A. Albert – J. Thompson: *Two-element generation of the projective unimodular group*, Illinois J. Math., **3** (1959) pp. 421–439.

[2] E. Bannai – T. Ito: *Algebraic Combinatorics I - Association schemes*, Benjamin/Cummings Publishing Co., London, 1984.

[3] N. Biggs: *Algebraic graph theory*, Cambridge University Press, Cambridge, 1974.

[4] A. E. Brower – J. H. van Lint: *Strongly regular graphs and partial geometries, in: Enumeration and Design*, Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982, D.M. Jackson & S.A. Vanstone (eds.) Academic Press, Toronto (1984) pp. 85–122.

[5] C. J. Colbourn – J. H. Dinitz: *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, Boca Raton, 2007.

[6] C. W. Curtis – I. Reiner: *Methods of Representation Theory with Applications to Finite Groups and Orders*, John Wiley & Sons, New York, 1981.

[7] W. Feit: *Characters of Finite groups*, W. A. Benjamin, Inc., New York, 1967.

[8] D. Gorenstein: *Finite groups*, Harper & Row, New York, 1968.

[9] M. D. Hestenes – D. G. Higman: *Rank* 3 *Groups and Strongly Regular Graphs*, Computers in Algebra and Number Theory, SIAM-AMS Proceeding, **4** (1971) pp. 141–159.

[10] D. G. Higman: *Intersection Matrices for Finite Permutation Groups*, J. Algebra, **6** (1967) pp. 22–42.

[11] D. G. Higman: *Coherent Configurations*, Oxford University Lecture Notes, **4** (1971) pp. 141-159.

[12] B. Huppert: *Endliche Gruppen*, Springer, 1967.

[13] I. M. Isaacs: *Character Theory of Finite Groups*, Academic Press, 1976.

[14] E. S. Kramer – D. M. Mesner: *t-designs on hypergraphs*, Discrete Math., **15** (1976) pp. 263–296.

[15] E. S. Kramer – S. S. Magliveras – D. M. Mesner: *t-designs from the large Mathieu groups*, Discrete Math., **36** (1981) pp. 171–189.

[16] D. E. Littlewood: *The Theory of group characters*, 2nd edition, Clarendon Press, Oxford, 1958.

[17] S. S. Magliveras: *The Subgroup Structure of the Higman-Sims Simple Group*, Ph.D. Dissertation, University of Birmingahm, England (1970), pp. 1–141.

[18] S. S. Magliveras: *The Subgroup Structure of the Higman-Sims Simple Group*, Bulletin of the AMS 77, **4** (1971) pp. 535–539.

[19] M. Hall Jr.: *The theory of groups*, Macmillan, New York, 1959.

[20] D. S. Passman: *Permutation Groups*, W.A. Benjamin, Inc., New York, 1968.

[21] C. C. Sims: *Graphs and Finite Permutation Groups*, Math. Z., **95** (1967) pp. 76–86.

[22] H. Wielandt: *Finite Permutation Groups*, Academic Press, 1964.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo degli Autori:

Cafer Caliskan – Department of Mathematical Sciences – Florida Atlantic University
E-mail: ccaliska@fau.edu

Spyros S. Magliveras – Department of Mathematical Sciences – Florida Atlantic University
Email: spyros@fau.edu

Lucille C. Yu – Sabre Holdings
E-mail: flo_lucille@yahoo.com