MINIMAL NON-FC-GROUPS AND COPRIME AUTOMORPHISMS OF QUASI-SIMPLE GROUPS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

KIVANÇ ERSOY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
MATHEMATICS

SEPTEMBER 2004

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Şafak ALPAY
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asist. Prof. Dr. Ayşe A. BERKMAN	Prof. Dr. Mahmut KUZUCUOĞLU
Co-advisor	Supervisor

Examining Committee Members

Prof. Dr. Adnan TERCAN	(Hacettepe University)	
Assist. Prof. Dr. Ayşe BERKMAN	(METU, MATH)	
Assoc. Prof. Dr. Ferruh ÖZBUDAK	(METU, MATH)	
Assoc. Prof. Dr. Gülin ERCAN	(METU, MATH)	
Prof. Dr. Mahmut KUZUCUOĞLU	(METU, MATH)	

I hearby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required, I have fully cited and referenced all material and results that are not original to this work.

Name Lastname : Kıvanç ERSOY

Signature :

ABSTRACT

MINIMAL NON-FC-GROUPS AND COPRIME AUTOMORPHISMS OF QUASI-SIMPLE GROUPS

Ersoy, Kıvanç
M.Sc., Department of Mathematics
Supervisor: Prof. Dr. Mahmut Kuzucuoğlu
Co-Advisor: Assist. Prof. Dr. Ayşe A. Berkman

September 2004, 62 pages

A group G is called an FC-group if the conjugacy class of every element is finite. G is called a minimal non-FC-group if G is not an FC-group, but every proper subgroup of G is an FC-group. The first part of this thesis is on minimal non-FC-groups and their finitary permutational representations. Belyaev proved in 1998 that, every perfect locally finite minimal non-FC-group has non-trivial finitary permutational representation. In Chapter 3, we write the proof of Belyaev in detail.

Recall that a group G is called quasi-simple if G is perfect and $G/Z(G)$ is simple. The second part of this thesis is on finite quasi-simple groups and their coprime automorphisms. In Chapter 4, the result of Parker and Quick is written in detail: Namely; if Q is a quasi-simple group and A is a non-trivial group of coprime automorphisms of Q satisfying $|Q : C_Q(A)| \leq n$ then $|Q| \leq n^3$, that is $|Q|$ is bounded by a function of n.

Keywords: Minimal non-FC-group, finitary permutational representation, quasi-simple group, coprime automorphism.

ÖZ

MİNİMAL FC OLMAYAN GRUPLAR VE YARI BASİT GRUPLARIN GÖRECELİ ASAL OTOMORFİZMALARI

Ersoy, Kıvanç
Yüksek Lisans, Matematik Bölümü
Tez Yöneticisi: Prof. Dr. Mahmut Kuzucuoğlu
Yardımcı Danışman: Yrd. Doç. Dr. Ayşe A. Berkman

Eylül 2004, 62 sayfa

Eğer G grubunun her elemanının eşlenik sınıfı sonlu ise G'ye FC grup denir. Eğer G bir FC grup değil, ancak G'nin her öz altgrubu bir FC grup ise G'ye minimal FC olmayan grup adı verilir. Bu tezin ilk bölümü minimal FC olmayan gruplar ve onların sonlumsu permutasyon gösterimleri üzerinedir. Belyaev 1998'de her yerel sonlu, minimal FC olmayan ve $G = G'$ eşitliğini sağlayan grubun sonlumsu permutasyon gösterimi olduğunu kanıtladı. Bölüm 3'te, Belyaev'in kanıtı ayrıntılarıyla yazılmıştır.

Eğer $G = G'$ ve $G/Z(G)$ basit ise G grubuna yarı basit denir. Tezin ikinci bölümü yarı basit gruplar ve onların göreceli asal otomorfizmaları üzerinedir. Bölüm 4'te, Parker ve Quick'in kanıtı ayrıntılarıyla yazılmıştır. Buna göre, eğer Q bir yarı basit grup ve A, Q'nun birimden farklı bir göreceli asal otomorfizma grubu ise ve $|Q : C_Q(A)| \leq n$ sağlanıyorsa bu durumda $|Q| \leq n^3$ olur, yani Q grubunun mertebesi n'nin bir fonksiyonuyla sınırlanır.

Anahtar sözcükler: Minimal FC olmayan grup, sonlumsu permutasyonal gösterim, yarı basit grup, göreceli asal otomorfizma.

ACKNOWLEDGMENTS

I gratefully acknowledge the valuable guidance, enlightening advices, constant support and encouragement of my supervisor, Prof. Dr. Mahmut Kuzucuoğlu. I would like to express my appreciation to Assist. Prof. Dr. Ayşe Berkman for her encouragement and continuous helps.

I wish to thank my friends Ufuk Genç, who provided me the opportunity to use the Bilkent Library, and Mustafa Topkara, who answered all of my questions about LaTeX.

My sincere thanks are due my family for their full support and motivation. Finally, I would like to express my gratitude to Esra Çiğdem Kurt for her endless support, patience and encouragement.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

Introduction

A group G is called an FC-group if conjugacy class of every element in G is finite. A minimal non-FC-group is a group G which is not an FC-group, where all proper subgroups of G are FC-groups. In [2], Belyaev described all minimal non-FC-groups which are different from their commutator subgroups and showed that non-perfect minimal non-FC-groups are exactly the Miller-Moreno groups described in [5]. Recall that a group G is called a group of Miller-Moreno type if G' is infinite and for every proper subgroup H in G, we have H' is finite. In [2], Belyaev also showed that a perfect locally finite minimal non-FC-group is either a quasi-simple group or a p-group. Recall that a group G is called quasi-simple if G is perfect and $G/Z(G)$ is simple. In [22], Kuzucuoğlu and Phillips proved that there exists no simple locally finite minimal non-FC-group. This result says quasi-simple case is impossible in the case of locally finite groups. Therefore, a perfect locally finite minimal non-FC-group must be a p-group. Leinen and Puglisi showed in [23] that every perfect locally finite minimal non-FC-group has a non-trivial finitary linear representation. Moreover they proved that if a perfect locally finite minimal non-FC group exists, then it will be a subgroup of a McLain group $M(\mathbb{Q}, GF(p))$. In [4] Belyaev strenghtened the result of [23] by proving that every perfect locally finite minimal non-FC-group has non-trivial finitary permutational representation. The aim of the first part of this thesis is to explain this work in detail. The same theorem is also proved by Leinen in [24].

In Chapter 4 we study the fixed points of automorphisms of quasi-simple groups. The inner automorphisms of order 2 are first studied by Brauer. Namely, in [6], Brauer has indicated that the information on the structure of the centralizers of involutions may give structural results about a finite simple group. Then he proved that if a simple group G contains an involution j such that $C_G(j)$ is isomorphic to the centralizer of an involution in $L_2(q)$ or $L_3(q)$ with some restriction on q, then G is isomorphic to the corresponding group $L_2(q)$ or $L_3(q)$ except for a few isolated cases. This played an important role and gave direction to group theorists for the classification of finite simple groups. The general problem is: If some information is given about the fixed points of automorphisms of a group, then what kind of information can we obtain about the structure of the group? On these lines the case $A \leq Aut(G)$ and $(|A|, |G|) = 1$ obtain a special attention. In the case if $|A| = p$ and A acts fixed point freely on G, then Thompson proved in [31] that G is nilpotent. There are results showing that the structure of $C_G(A)$ imposes some restriction on G. For example, Turull proved in [34] that if G is a finite soluble group and A a group of automorphisms such that $(|A|, |G|) = 1$, then when $C_G(A) = 1$ and A acts with regular orbits on G, we have $h(G) \leq l(A)$ where $h(G)$ denotes the Fitting height of G and $l(A)$ denotes the length of the longest chain of subgroups of A. Moreover, in this case, if A is soluble then $h(G) \leq 2l(A) + h(C_G(A))$.

The second part of this thesis is about finite quasi-simple groups and coprime automorphisms. Parker and Quick worked on the following problem which is dual to above problems: Let G be a finite group and A be a group of coprime automorphisms of G such that $|G : C_G(A)|$ is bounded by n. They proved that in this case we can bound $|[G, A]|$ with a suitable function of n. In this proof they used the following result:

If Q is a quasi-simple group and A a group of automorphisms such that orders of Q and A are coprime and $|Q : C_Q(A)| \leq n$, then $|Q| \leq n^3$. In the second part of this thesis, the proof of this result is written in detail.

CHAPTER 2

Preliminaries

In this chapter we give the basic definitions and primary results that we will use in other chapters.

2.1 Minimal non-FC-groups

Definition 2.1.1. *An element $g \in G$ is called an **FC-element** if it has a finite number of conjugates in G.*

Theorem 2.1.2. *In any group FC-elements form a characteristic subgroup.*

Proof. Let g and h be any two FC-elements in G. Then $C_G(g)$ and $C_G(h)$ have finite index in G, which implies $C_G(g) \cap C_G(h)$ has finite index in G. $C_G(gh^{-1}) \geq C_G(g) \cap C_G(h)$ so $C_G(gh^{-1})$ has finite index in G, i.e. gh^{-1} is an FC-element. Therefore, the set of FC-elements form a subgroup of G. Let α be an element of $Aut(G)$. Since $C_G(g^{\alpha}) = (C_G(g))^{\alpha}$, g^{α} is an FC-element.

Therefore the set of FC-elements of any group forms a characteristic subgroup. □

Definition 2.1.3. *The subgroup consisting of the FC-elements is called the **FC-center**.*

Definition 2.1.4. *A group G is called an **FC-group** if it is equal to its FC-center, that is, every conjugacy class of G is finite.*

Example 2.1.5. Every finite group and every abelian group are FC-groups.

Definition 2.1.6. *A group G is called quasi-abelian if G' is finite.*

Theorem 2.1.7. *Every quasi-abelian group is an FC-group.*

Proof. Let $|G'| = n$ and $a \in G$. We claim that a has at most n conjugates. Suppose to the contrary that a has $n+1$ distinct conjugates $b_1, b_2 \dots b_{n+1}$. For $1 \leq i \leq n+1$ there exists $g_i \in G$ such that

$$b_i = g_i^{-1} a g_i$$

So $b_i a^{-1} = g_i^{-1} a g_i a^{-1} \in G'$ for all $i = 1, 2, \dots n+1$. Therefore $S = \{[g_i, a^{-1}] : 1 \leq i \leq n+1\}$ is a subset of G'. Since the map $a^{g_i} \longrightarrow a^{g_i}.a^{-1}$ is a one-to-one function, the set S has $n+1$ elements.

That is, $n+1 = |S| \leq |G'| = n$ which is a contradiction. Hence a has at most n conjugates for all $a \in G$, i.e. G is an FC-group. $\square$

Definition 2.1.8. *A group G is called a* ***minimal non-FC-group*** *if it is not an FC-group and every proper subgroup of G is an FC-group.*

Example 2.1.9. Recall that the quasi-cyclic p-group $\mathbb{C}_{p^\infty}$ is defined as $\{x \in \mathbb{C} : x^{p^n} = 1, n \in \mathbb{N}\}$ with the usual multiplication in $\mathbb{C}$.

Let $G = \langle \psi \rangle \ltimes \mathbb{C}_{p^\infty}$ where ψ is the automorphism of $\mathbb{C}_{p^\infty}$ which takes x to x^{-1}. (ψ is an automorphism since $\mathbb{C}_{p^\infty}$ is abelian.) Now, (for the case where p is odd), $C_G(\psi) = \{1, \psi\}$ has order 2. Therefore, $|G : C_G(\psi)|$ is infinite, so G is not an FC-group. However, every proper subgroup of G is either finite, or isomorphic to $\mathbb{C}_{p^\infty}$, hence abelian. Therefore all proper subgroups of G are FC-groups. So, G is a minimal non-FC-group.

Definition 2.1.10. *A group G is called a group of Miller-Moreno type (or a minimal non-quasi-abelian group) if G' is infinite and for every $H < G$ we have H' is finite.*

By Theorem 2.1.7, all proper subgroups of a group of Miller-Moreno type are FC-groups. We will prove Theorem 2.1.12 to conclude that every group of Miller-Moreno type is a minimal non-FC-group. First we will state the following result which will be necessary to prove Theorem 2.1.12.

Lemma 2.1.11. ***(Schur)*** *Let G be a group with $|G/Z(G)|$ finite. Then G' is finite.*

Proof. Let $|G/Z(G)| = n$. Then every element $g \in G$ can be written in the form $g = x_i z_i$ where $x_i \in \{x_1, x_2 \dots x_n\}$ are the coset representatives of $Z(G)$ in G. Now, since for all $z \in Z(G)$ and $g, h \in G$ we have $[g, h] = [gz, h] = [g, hz]$, every commutator $[g, h] \in G'$ can be written as $[x_i, x_j]$ where $g = x_i z_i$ and $h = x_j z_j$ for some $z_i, z_j \in Z(G)$. Therefore, there are at most $n^2 - n$ non-identity commutators in G, since $[x_i, x_i] = 1$ for all $i \in \{1, 2, \dots n\}$. The commutator subgroup G' is generated by the commutators, so it is an $n^2 - n$ generated group.

Claim: Every element $g \in G'$ can be written as a product of at most n^3 commutators.

Let $\Omega = \{[x_i, x_j] : i, j = 1, 2 \dots n\}$ be the set of all commutators. If the claim holds, then

$$G' \subseteq \prod_{i=1}^{n^3} \Omega_i, \quad \text{where each } \Omega_i = \Omega \text{ has } n^2 - n + 1 \text{ elements.}$$

This implies G' is finite. Now assume there exists an element $g \in G'$ such that g can be expressed as a product of at least k commutators $d_{i_1}, d_{i_2} \dots d_{i_k}$ where $k > n^3$, that is $g = d_{i_1} d_{i_2} \dots d_{i_k}$. Since the total number of commutators is $n^2 - n + 1$, one of the commutators must repeat at least $n + 2$ times. For a commutator $[x, y]$, we have $[x, y]^g = [x^g, y^g]$. Hence, a conjugate of a commutator is also a commutator. Consider $d_{i_1}.d_{i_2}.d_{i_1}.d_{i_3} = d_{i_1}^2.d_{i_1}^{-1}.d_{i_2}.d_{i_1}.d_{i_3} = d_{i_1}^2 d_{i_2}^{d_{i_1}} d_{i_3}$. By this way, we can switch the repeating commutator to the beginning of the writing of g as a product of commutators. Therefore, if $d = [a, b]$ is the $n + 2$ times repeating commutator, g can be written as $g = d^{n+2}.d_{j_1}.d_{j_2} \dots d_{j_m}$ for some commutator d_{j_l}

where the total product is of lenght $k > n^3$. Since $G/Z(G)$ has order n, $d^n \in Z(G)$. Then $(d^n)^a = d^n$. Now, $d^n.d^2 = [a,b]^n.[a,b]^2 = ([a,b]^n)^a.[a,b]^2 = ([a,b]^{n-1})^a.[a,b]^a.[a,b]^2 = ([a,b]^{n-1})^a.[a^2,b][a,b]$ since $[a^2,b] = a^{-2}b^{-1}a^2b = a^{-2}b^{-1}aab = a^{-2}b^{-1}abaa^{-1}b^{-1}ab = a^{-2}b^{-1}aba[a,b] = [a,b]^a.[a,b]$. Therefore, the number of commutators in the product reduced 1 which contradicts with k being the least. Hence given an element $g \in G'$ can be written as a product of at most n^3 commutators, which proves the claim. □

Theorem 2.1.12. *A group of Miller-Moreno type can not be an FC-group.*

Proof. Let G be group of Miller-Moreno type. Assume that G is an FC-group. Since G' is infinite, clearly G is non-abelian. Choose $g \in G \backslash Z(G)$. Since G is an FC-group, $|G : C_G(g)| < \infty$.

Let $H = \bigcap_{x \in G}(C_G(g))^x$. Since $C_G(g)$ is proper, H is proper. Then since G is of Miller-Moreno type, H' is finite. Also $|G : H|$ is finite. So $G = FH$ where F is a finitely generated subgroup of G. Let $\bar{G} = G/H' = \bar{F}\bar{H}$. Then $|\bar{G} : C_{\bar{G}}(\bar{F})| < \infty$ since $\bar{G}$ is an FC-group. Since $|\bar{G} : \bar{H}| < \infty$, the index $|\bar{G} : C_{\bar{G}}(\bar{F}) \cap \bar{H}| = |\bar{G} : \bar{H}||\bar{H} : C_{\bar{G}}(\bar{F}) \cap \bar{H}| < \infty$. Clearly $C_{\bar{G}}(\bar{F}) \cap \bar{H}$ is contained in $Z(\bar{G})$. Hence $|\bar{G} : Z(\bar{G})|$ is finite. Now, by Lemma 2.1.11, $\bar{G}'$ is finite. But then $\bar{G}' = (G/H')' = G'H'/H' = G'/H'$ is finite. Since H' is finite by assumption, we conclude that G' is finite, which is a contradiction since G is of Miller-Moreno type.

□

Now we give a lemma which we use later.

Lemma 2.1.13. ***(Grün's Lemma)*** *If G is perfect, then $Z(G/Z(G)) = 1$.*

Proof. Let $aZ(G) \in Z(G/Z(G))$. Then $aZ(G)$ commutes with $xZ(G)$ for every $x \in G$, that is, for every $x \in G$, $[a,x] \in Z(G)$. Now, define

$$\begin{aligned} \phi_a : &G \longrightarrow Z(G) \\ &x \longmapsto [x,a]. \end{aligned}$$

$$\phi_a(xy) = [xy, a] = y^{-1}x^{-1}a^{-1}xya = y^{-1}x^{-1}a^{-1}xaa^{-1}ya$$
$$= y^{-1}[x, a]a^{-1}ya = [x, a][y, a] = \phi_a(x)\phi_a(y)$$

since $[x, a] \in Z(G)$. So ϕ_a is a homomorphism.

$$Ker(\phi_a) = \{x \in G : [x, a] = 1\} = C_G(a)$$

Then $G/C_G(a) = Im(\phi_a) \leq Z(G)$, so $G/C_G(a)$ is abelian. Therefore, $G' \leq C_G(a)$. Since G is perfect, $G = C_G(a)$. Therefore $a \in Z(G)$. Hence $Z(G/Z(G)) = 1$.

□

2.2 Permutational representations

Definition 2.2.1. *Let G be a transitive permutation group on X. A proper subset $Y \subset X$ with at least two elements is called a* ***block of imprimitivity*** *of G if for each permutation $\sigma \in G$, either $Y = Y\sigma$ or $Y \cap Y\sigma = \emptyset$. A group is called* ***imprimitive*** *if it has at least one block of imprimitivity, otherwise it is called* ***primitive****.*

Theorem 2.2.2. *Let G be a group acting on a set X transitively and N be a normal subgroup of G. Then orbits of N form a set of blocks of imprimitivity in X and G acts on the set N-orbits of X transitively. .*

Proof. Let X_i be an N-orbit in X, i.e. $X_i = \{x_i.n : n \in N\}$ for some $x_i \in X$. For some $g \in G$ assume $X_i \cap X_i.g \neq \emptyset$. Then there exist $x_i, y_i \in X_i$ such that $x_i = y_i.g$. Now for all $z_i \in X_i$, since $z_i = x_i.n$ for some $n \in N$,

$$z_i = x_i.n = (y_i.g).n = y_i.(gn) = y_i.((gng^{-1})g)$$

Now since $N \lhd G$, $gng^{-1} \in N$, we have $y_i.((gng^{-1})g) = y_i.(n^{g^{-1}}g) = (y_in^{g^{-1}}).g \in X_i.g$. So $X_i \subseteq X_i.g$. Conversely if $a \in X_i.g$, then $a = t_i.g$

for some $t_i \in X_i$. Now, since y_i, t_i belong to the same orbit X_i, $t_i = y_i.n_1$ for some $n_1 \in N$. Then

$$a = t_i.g = (y_i.n_1).g = y_i.(n_1 g) = y_i.(g(g^{-1}n_1 g)) = x_i.(g^{-1}n_1 g) \in X_i$$

since $N \lhd G$ and X_i is an N-orbit. So $a \in X_i$, ie $X_i.g \subseteq X_i$. Since we have already showed that $X_i \subseteq X_i.g$, $X_i = X_i.g$

Therefore X_i is a block of imprimitivity in X.

Let X_i, X_j be two N-orbits in G and $x_i \in X_i, x_j \in X_j$ be any two elements of X. Since G acts on X transitively, there exists $g \in G$ such that $x_i = x_j.g$. Then $x_i \in X_i \cap X_j.g$, by imprimitivity $X_i = X_j.g$ i.e. for any N-orbit X_i, X_j of X, there exists $g \in G$ that takes X_i to X_j. Therefore G acts transitively on the blocks of imprimitivity of X.

□

Definition 2.2.3. *A homomorphism from a group G into $Sym(X)$ of some set X is called a* ***permutational representation*** *of G on X.*

The following result is known as Cayley's Theorem, says that every group has a permutational representation.

Theorem 2.2.4. *(**Cayley's Theorem**) Every group is isomorphic to a group of permutations.*

Proof. See Corollary 4.6 in [19] □

Definition 2.2.5. *Let Ω be an infinite set. The set of all* ***finitary*** *permutations on Ω denoted by $S(\Omega)$ is the set of all permutations of Ω which fix all but finitely many elements of Ω.*

Definition 2.2.6. *Let V be a vector space over the field $\mathbf{F}$ and α is a linear transformation of V. α is called* ***finitary*** *if $[V, a]$=$\{v(\alpha - 1) : v \in V\}$ is a finite dimensional subspace of V.*

Definition 2.2.7. *The set of all invertible finitary transformations on a vector space V is denoted by $FGL(V, F) \subseteq End_F V$. Subgroups of $FGL(V, F)$ are called finitary linear groups.*

Theorem 2.2.8. *Every group of finitary permutations is finitary linear.*

Proof. Let G be a group of finitary permutations. Then there exists a set Ω such that G acts on Ω faithfully with $x.g = x$ for all but finitely many elements x in Ω. Precisely, let $\Omega = \{a_i : i \in I\}$ where I is an index set and let V be the vector space with basis $\{v_{a_i} : i \in I\}$ over a field $\mathbb{F}$.

Let $\Gamma = \{a_{j_1}, a_{j_2}, \ldots a_{j_n}\}$ be the set of the elements which are not fixed by G.

Define

$$\begin{aligned} - :&G \longrightarrow GL(\mathrm{V}) \\ &g \longrightarrow \bar{g} \end{aligned}$$

where $\bar{g}$ is the linear transformation of V given by the following:

$$\begin{aligned} \bar{g} : \mathrm{V} &\longrightarrow \mathrm{V} \\ v_{a_i} &\longrightarrow v_{a_i.g}. \end{aligned}$$

Then $-$ is a homomorphism from G into $GL(\mathrm{V})$, that is G can be embedded in $GL(\mathrm{V})$. Moreover $[\mathrm{V}, g]$ is a finite dimensional vector space as $[\mathrm{V}, g]$ is contained in $W = \langle v_{a_{j_i}} : i \in \{1, 2, \ldots n\}\rangle$. Therefore G is a finitary linear group. $\square$

By Theorem 2.2.8 we can conclude that for a group G, having a finitary permutational represantation is a stronger property than having a finitary linear representation.

Definition 2.2.9. *Let X and Y be subgroups of G. X and Y are called* ***commensurable*** *if $X \cap Y$ has finite index in X and Y.*

Definition 2.2.10. *A group G is called an infinite Schmidt group (or a quasifinite group) if every proper subgroup of G is finite.*

Example 2.2.11. $\mathbb{C}_{p^\infty}$ is an infinite Schmidt group for every prime p.

Definition 2.2.12. *A group G is called **locally graded** if any non-trivial finitely generated subgroup H of G has a proper subgroup of finite index.*

2.3 The minimum condition and Chernikov groups

Definition 2.3.1. *A group G is said to have minimum condition on subgroups, or simply, **min**, if each non-empty set of subgroups of G has a minimal element; that is, if $S = \{H_i : i \in I\}$ is a set of non-empty subgroups of G, then there exists $K \in S$ such that if $L \in S$ and $L \leq K$, then $L = K$.*

Example 2.3.2. All finite groups satisfy **min**.

Example 2.3.3. Schmidt groups satisfy **min** since their all proper subgroups are finite.

The following lemma gives a useful characterization for the groups satisfying **min**.

Lemma 2.3.4. *A group G has the minimum condition if and only if every descending chain of subgroups terminates in finitely many steps.*

Proof. Suppose G satisfies **min** but it has an infinite proper descending chain

$$G_0 > G_1 > G_2 > \dots$$

Then $\Omega = \{G_k : k \in \mathbb{N}\}$ is a set of subgroups which does not have a minimal element, so we get a contradiction.

Conversely suppose G does not satisfy **min**, but every descending chain of subgroups terminates after finitely many steps. Since G does not satisfy **min**, there exists a non-empty set Σ consisting of subgroups of G such that Σ has no minimal element. Then for any $H_i \in \Sigma$, we can choose an element $H_{i+1} \in \Sigma$ such that $H_{i+1} < H_i$. With this construction,

$$H_1 > H_2 > \dots$$

forms an infinite descending chain which contradicts with the assumption. □

Here we will give a famous theorem of Shunkov and Kegel-Wehrfritz which we will use later, without giving the proof. For the proof, see [21] or [27].

Theorem 2.3.5. *Every locally finite group satisfying* ***min*** *is Chernikov.*

2.4 McLain's Group

Let $\mathbb{Q}$ be the set of rational numbers. If $(\lambda, \mu), (\lambda_1, \mu_1) \in \mathbb{Q} \times \mathbb{Q}$ satisfying

$$\mu - \lambda > 0$$

$$\mu_1 - \lambda_1 > 0$$

then there exists an order preserving permutation α of $\mathbb{Q}$ such that $\lambda\alpha = \lambda_1$, $\mu\alpha = \mu_1$. To be precise;

$$x\alpha = \frac{x - \lambda}{\lambda - \mu}(\lambda_1 - \mu_1) + \lambda_1, \quad \forall x \in \mathbb{Q}.$$

Let $\mathbb{F}$ be a field, V countably infinite dimensional vector space with basis $\mathcal{B}$=$\{v_\lambda : \lambda \in \mathbb{Q}\}$. Define $e_{\lambda\mu}$ for all $\lambda \leq \mu$, $\lambda, \mu \in \mathbb{Q}$ such that

$$v_\gamma e_{\lambda\mu} = \begin{cases} v_\mu & \text{if } \gamma = \lambda \\ 0 & \text{if } \gamma \neq \lambda. \end{cases}$$

The standard multiplication rules hold for these $e_{\lambda\mu}$:

$$e_{\lambda\mu}e_{\nu\theta} = \begin{cases} e_{\lambda\theta} & \text{if } \mu = \nu \\ 0 & \text{otherwise.} \end{cases}$$

In particular $e_{\lambda\mu}^2 = 0$. It follows that $(1+ae_{\lambda\mu})^{-1} = 1-ae_{\lambda\mu}$ for all $a \in \mathbb{F}$. It is easy to verify the following:

$$[1+ae_{\lambda\mu}, 1+be_{\nu\theta}] = \begin{cases} 1+abe_{\lambda\theta} & \text{if } \mu = \nu \\ 1 & \text{if } \mu \neq \nu \text{ and } \lambda \neq \theta. \end{cases}$$

McLain's group is the group of linear transformations of V generated by all $1+ae_{\lambda\mu}$ where $a \in \mathbb{F}$ and $\lambda < \mu \in \mathbb{Q}$. In other words, McLain's group $M(\mathbb{Q},\mathbb{F}) = \langle 1+ae_{\lambda\mu} : a \in \mathbb{F},\ \lambda,\mu \in \mathbb{Q},\ \lambda < \mu \rangle$. Every element x of $M(\mathbb{Q},\mathbb{F})$ can be written uniquely in the form

$$x = 1 + \sum_{\lambda<\mu} a_{\lambda\mu}e_{\lambda\mu}, \qquad \text{where almost all of } a_{\lambda\mu} \text{ are zero.}$$

Conversely, every element of this form belongs to $M(\mathbb{Q},\mathbb{F})$. To prove this assume that $x \neq 1$ is an element of this form and let $\mu_0 \in \mathbb{Q}$ be the largest element in $\mathbb{Q}$ satisfying $a_{\lambda_0\mu_0} \neq 0$ for some $\lambda_0 \in \mathbb{Q}$. Denote $u = a_{\lambda_0\mu_0}e_{\lambda_0\mu_0}$ and $v = x - u - 1$. Now, uv is the sum of elements of the form $b_{\lambda_0\mu_1}e_{\lambda_0\mu_1}$ where $\lambda_0 < \mu_1$ and $\mu_0 < \mu_1$. Since μ_0 is chosen to be maximal among the indices of nonzero coefficients, we obtain $b_{\lambda_0\mu_1}e_{\lambda_0\mu_1} = 0$, so $uv = 0$. Therefore, $x = 1+u+v = (1+u)(1+v)$. By induction on the number of non-zero terms in x, we have $1+v \in M(\mathbb{Q},\mathbb{F})$, $1+u \in M(\mathbb{Q},\mathbb{F})$ then $x = (1+u)(1+v) \in M(\mathbb{Q},\mathbb{F})$.

Definition 2.4.1. *A group G is called locally nilpotent if every finitely generated subgroup of G is nilpotent.*

Now we will state a property of locally nilpotent groups which we will use later.

Theorem 2.4.2. *Minimal normal subgroup of a locally nilpotent group G is central.*

Proof. Let N be a minimal normal subgroup of G which is not central. Then since $N \nleq Z(G)$, there exist $a \in N$, $g \in G$ such that $b = [g, a] \neq 1$. Since N is normal in G, we have $b = [g, a] = g^{-1}a^{-1}ga \in N$. Since N is minimal, $b^G = N$. So $a \in \langle b^{g_1} \dots b^{g_n} \rangle$ for some certain $g_i \in G$. Denote $H = \langle a, g, g_1 \dots g_n \rangle$. Since G is locally nilpotent, H is nilpotent. Set $A = a^H = \langle a^h : h \in H \rangle$. Then $b = [a, g] = a^{-1}g^{-1}ag \in [A, H]$ since $a \in A$ and $g \in H$. Since $[A, H]^H = [A, H]$ and $g_i \in H$, we have $b^{g_i} \in [A, H]^H = [A, H]$, therefore $a \in [A, H]$. Now, since A is normal in H, we have $[A, H] \leq A$. Now, since $[A, H]$ is normalized by H, and A is the minimal normal subgroup of H containing a, we have $A = [A, H]$. But then $[[A, H], H] = [A, H] = A$, so inductively $[A,_r H] = A$ for all $r \in \mathbb{N}$. But $[A,_r H] \leq \gamma_r(H)$ which is equal to 1 after some r since H is nilpotent. Then $A = 1$. So $a = 1$ and $b = [a, g] = 1$ which gives a contradiction. □

The following result which we will state without proof is a generalization of the Fitting's Theorem which states that in any group G, product of normal nilpotent subgroups H and K is nilpotent of at most class equal to sum of nilpotency classes of H and K.

Theorem 2.4.3. *Let H and K be normal locally nilpotent subgroups of G. Then the product $J = HK$ is locally nilpotent.*

Proof. See [26], Theorem 12.2. □

Theorem 2.4.4. *In every group G, there is a unique maximal normal locally nilpotent subgroup (called the Hirsch-Plotkin radical of G) containing all normal locally nilpotent subgroups of G.*

Proof. Let Ω be the set of normal locally nilpotent subgroups of G. Since $1 \in \Omega$, we have $\Omega \neq \emptyset$. Now, let $N_1 \leq N_2 \leq \dots N_\alpha \dots$ be a chain in Ω.

Since the union $\bigcup_{\alpha \in I} N_\alpha$ is normal and locally nilpotent, every chain in Ω has an upper bound. By Zorn's Lemma, Ω has a maximal element, that is G has a maximal normal locally nilpotent subgroup. Now, if H and K be two maximal normal locally nilpotent subgroups of G, then by Theorem 2.4.3, HK is a normal locally nilpotent subgroup of G which contains both H and K. Since H and K are maximal, we have $H = HK = K$. So, for every group the maximal normal locally nilpotent group containing all normal locally nilpotent groups is unique. □

The following theorem, which is known as McLain's Theorem, lists the essential properties of the McLain's group.

Theorem 2.4.5. *Let $M = M(\mathbb{Q}, \mathbb{F})$.*

1. *M is a product of its normal abelian subgroups, so M is locally nilpotent.*
2. *If $char(\mathbb{F}) = p$, then M is a locally finite p-group. If $char(\mathbb{F}) = 0$ then M is torsion-free.*
3. *M is characteristically simple, hence M is perfect and $Z(M) = 1$.*

Proof. 1. Let $1 + ae_{\lambda\mu}$ be an element of M where $a \neq 0$. Consider the normal closure $(1 + ae_{\lambda\mu})^M$ of $1 + ae_{\lambda\mu}$. Clearly we have

$$(1 + ae_{\lambda\mu})^M = \langle (1 + ae_{\lambda\mu})^g : g \in M \rangle.$$

Now, for $\alpha < \beta$, we have

$$\begin{aligned}(1 + be_{\alpha\beta})^{-1}(1 + ae_{\lambda\mu})(1 + be_{\alpha\beta}) &= (1 + ae_{\lambda\mu})[1 + ae_{\lambda\mu}, 1 + be_{\alpha\beta}] \\ &= \begin{cases} (1 + ae_{\lambda\mu}) & \text{if } \alpha \neq \mu. \\ (1 + ae_{\lambda\mu})(1 + abe_{\lambda\beta}) & \text{if } \alpha = \mu. \end{cases} \\ &= \begin{cases} (1 + ae_{\lambda\mu}) & \text{if } \alpha \neq \mu. \\ (1 + ae_{\lambda\mu} + abe_{\lambda\beta}) & \text{if } \alpha = \mu, \end{cases}\end{aligned}$$

since $e_{\lambda\mu}e_{\lambda\beta} = 0$. Therefore, every conjugate of $1 + ae_{\lambda\mu}$ belong to the subgroup generated by $1 + ue_{\gamma\delta}$ where $\gamma \leq \lambda \leq \mu \leq \delta$. Now, since

$$(1 + u_{\gamma\delta})(1 + ve_{\xi\zeta}) = (1 + ve_{\xi\zeta})(1 + u_{\gamma\delta})$$

holds for $\gamma < \lambda < \mu < \delta$ and $\xi < \lambda < \mu < \zeta$, and $(1 + ae_{\lambda\mu})^M$ is abelian. Since M is generated by elements of the form $1 + ae_{\lambda\mu}$, M is the product of its normal abelian subgroups. By Theorem 2.4.4, we know that the Hirsch-Plotkin radical J of M contains all normal locally nilpotent subgroups, then J must contain all the normal abelian subgroups. Then $J = M$, therefore M is locally nilpotent.

2. Let x be an element of M. Then there exists $\lambda_1 < \lambda_2 < \ldots < \lambda_n \in \mathbb{Q}$ such that

$$x = 1 + \sum_{i=1}^{n} a_{\lambda_i\lambda_{i+1}} e_{\lambda_i\lambda_{i+1}}.$$

Then x belongs to the subgroup $H = \langle 1 + ae_{\lambda_i\lambda_{i+1}} : i = 1, 2 \ldots n-1, a \in \mathbb{F}\rangle$. Now, the map $\psi : H \longrightarrow UT(n, \mathbb{F})$ given by $1 + ae_{\lambda_i\lambda_{i+1}} \longmapsto I + aE_{i\,i+1}$ where I denotes the $n \times n$ identity matrice and E_{ij} is the $n \times n$ matrice whose ij-th entry is 1 and other entries are zero, gives an isomorphism between H and $UT(n, \mathbb{F})$.

We know that if $char(\mathbb{F}) = 0$ we have $UT(n, \mathbb{F})$ is torsion-free and if $char(\mathbb{F}) = p$ then $UT(n, \mathbb{F})$ is a p-group. Since every element of M is contained in a subgroup which is isomorphic to $UT(n, \mathbb{F})$ for some n, we conclude that if $char(\mathbb{F}) = 0$ then M is torsion-free and if $char(\mathbb{F}) = p$ then M is a p-group.

Now, when $char(\mathbb{F}) = p$, let K be a finitely generated subgroup of M, that is $K = \langle 1 + a_{k_i}e_{\lambda_{k_i}\lambda_{k_{i+1}}} : i = 1, 2 \ldots n-1, k = 1, 2 \ldots m$ for some m and $a_{k_i} \in \mathbb{F}\rangle$. Then, by the same way we can embed K into a unitriangular group $UT(r, \mathbb{F})$ for some suitable r. Since $char(\mathbb{F}) = p$, the unitriangular group $UT(r, \mathbb{F})$ is a p-group. Hence, K is finite, that is, M is locally finite.

3. Let E be a non-trivial characteristic subgroup of M. First we need to show that E contains a generator of M. Let $x \in E$, clearly $x = 1 + a_{\lambda_1\mu_1}e_{\lambda_1\mu_1} \dots a_{\lambda_m\mu_m}e_{\lambda_m\mu_m}$. Then x belongs to a subgroup H generated by $1 + e_{\lambda_i\mu_i}$. By above arguement $H \cong UT(n, \mathbb{F})$, so H is nilpotent.

   Now, since $x \in H \cap E$, the intersection $H \cap E \neq \emptyset$. Since $E \trianglelefteq M$, we have $H \cap E \trianglelefteq H$. Since H is nilpotent, $Z(H)$ intersects with every non-trivial normal subgroup of H non-trivially. Therefore, $1 \neq Z(H) \cap H \cap E = Z(H) \cap E$. Now, since $H \cong UT(n, \mathbb{F})$, we have $Z(H) \cong Z(UT(n, \mathbb{F})) = \langle I + aE_{1n} : a \in \mathbb{F}\rangle$. Therefore, $Z(H)$ is generated by elements of the form $1 + ae_{\lambda_1\lambda_n}$, that is E contains a generator of M.

   Given $\mu_1, \mu_2 \in \mathbb{Q}$ with $\mu_1 < \mu_2$ we know that there exists an order-preserving permutation such that $\mu_1\alpha = \lambda_1$ and $\mu_2\alpha = \lambda_n$. Now, $(1 + ae_{\lambda\mu})\alpha = 1 + ae_{\lambda\alpha\,\mu\alpha}$, so α is an automorphism of M. Since E is a characteristic subgroup, E contains $1 + ae_{\lambda\mu}$ for all $(\lambda, \mu) \in \mathbb{Q} \times \mathbb{Q}$ with $\lambda < \mu$. Moreover, if $b \in \mathbb{F}$ then $[1 + a_{\lambda\mu}, 1 + a^{-1}be\mu nu] = 1 + be_{\lambda\nu} \in E$ for all $\alpha < \nu$. Therefore, E contains all the generators of M, that is $E = M$. So M has no proper non-trivial characteristic subgroups. Now, since $Z(M)$ and M' are characteristic subgroups of M, since M is non-abelian we have $Z(M) = 1$ and $M' = M$.

□

Lemma 2.4.6. *Let $\mathbb{F}$ be a finite field with characteristic char$(\mathbb{F}) = p$. The McLain's group $M = M(\mathbb{Q}, \mathbb{F})$ has no proper subgroup of finite index.*

Proof. Let K be a subgroup of M of finite index. By the right action of M on the cosets of K, there exists a normal subgroup N of M such that $N \triangleleft K$ with

$|M/N| = n$. Then $(xN)^n = N$ for all x in M. Now, $N \geq M^n = \langle x^n : x \in M \rangle$ and M^n is a characteristic subgroup of M. But by Theorem 2.4.5, M is characteristically simple, so $M^n = 1$ which is not true since M has elements of order p^k for all $k \in \mathbb{N}$, that is, M is not of bounded exponent. So M has no subgroups of finite index. □

Corollary 2.4.7. *If $char(\mathbb{F}) = p$, McLain's group has no finitely generated normal subgroup.*

Proof. Let $G = M(\mathbb{Q}, \mathbb{F})$.Clearly where $char(\mathbb{F}) = p$, $M(\mathbb{Q}, \mathbb{F})$ is locally finite by Theorem 2.4.5. Assume that it has a finitely generated normal subgroup N. Then N must be finite. Since G acts on N, there exists a homomorphism $\phi : G \longrightarrow Aut(N)$. Then $G/ker(\phi) \leq Aut(N)$ where $Aut(N)$ is finite. So $ker(\phi)$ is a subgroup of G with finite index, but this contradicts Lemma 2.4.6. □

2.5 Central extensions

Definition 2.5.1. *A **central extension** of a group G is a pair (H, π) where H is a group and $\pi : H \longrightarrow G$ is a surjective homomorphism with $ker(\pi) \leq Z(H)$. H is also said to be a central extension of G.*

Example 2.5.2. $PSL(n, F)$ is defined as $SL(n, F)/Z(SL(n, F))$. Consider the canonical homomorphism π from $SL(n, F)$ to $PSL(n, F)$. Clearly $ker(\pi) = Z(SL(n, F))$. So $(SL(n, F), \pi)$ is a central extension of $PSL(n, F)$.

Example 2.5.3. Consider the quaternion group

$$Q_8 = \langle x, y : x^4 = x^2y^{-2} = y^{-1}xyx = 1 \rangle.$$

Consider $Z(Q_8) = \langle x^2 \rangle$. Now, $Q_8/Z(Q_8)$ is isomorphic to the Klein-4-group V since $Q_8/Z(Q_8)$ has order 4 and $xZ(Q_8)$, $yZ(Q_8)$, $xyZ(Q_8)$ are three distict elements of order 2 in $Q_8/Z(Q_8)$. Therefore, Q_8 is a central extension of V.

Recall that the dihedral group D_8 of order 8 is given by $D_8 = \langle r, \rho : r^4 = \rho^2 = (\rho r)^2 = 1\rangle$. Now, $Z(D_8) = \langle r^2\rangle$ and $D_8/Z(D_8) \cong V$ since $D_8/Z(D_8)$ has order 4 and $\rho Z(D_8)$, $rZ(D_8)$ and $(\rho r)Z(D_8)$ are three distinct elements of order 2 in $D_8/Z(D_8)$. So both Q_8 and D_8 are central extensions of the same group V. Therefore central extensions of groups are not unique.

Definition 2.5.4. *A **morphism** $\alpha : (G_1, \pi_1) \longrightarrow (G_2, \pi_2)$ of central extensions of G is a group homomorphism $\alpha : G_1 \longrightarrow G_2$ with $\pi_1 = \alpha\pi_2$,. That is, if α is a morphism of central extensions, then the following diagram commutes:*

$$\begin{array}{ccc} G_1 & \xrightarrow{\alpha} & G_2 \\ \pi_1 \searrow & & \downarrow \pi_2 \\ & & G \end{array}$$

Definition 2.5.5. *A central extension $(\tilde{G}, \pi)$ of G is said to be **universal** if for each central extension (H, σ) of G there is a unique morphism $\alpha : (\tilde{G}, \pi) \longrightarrow (H, \sigma)$.*

Theorem 2.5.6. *Up to isomorphism there is at most one universal central extension of G.*

Proof. Let $(G_1, \pi_1), (G_2, \pi_2)$ be two distinct universal central extensions of G. By definition of a universal central extension, there are morphisms of central extensions $\alpha_1 : (G_1, \pi_1) \longrightarrow (G_2, \pi_2)$ and $\alpha_2 : (G_2, \pi_2) \longrightarrow (G_1, \pi_1)$. Then $\alpha_1 : G_1 \longrightarrow G_2$ is a group homomorphism and $\pi_1 = \alpha_1\pi_2$. Similarly $\alpha_2 : G_2 \longrightarrow G_1$ is a group homomorphism with $\pi_2 = \alpha_2\pi_1$.

Now, for $i = 1, 2$, the map $\alpha_i\alpha_{3-i} : G_i \longrightarrow G_i$ is a group homomorphism with $(\alpha_i\alpha_{3-i})\pi_i = \alpha_i(\alpha_{3-i}\pi i) = \alpha_i\pi_{3-i} = \pi_i$. Therefore, $\alpha_i\alpha_{3-i}$:

$(G_i, \pi_i) \longrightarrow (G_i, \pi_i)$ is a morphism of central extensions for $i = 1, 2$. Since $1_{G_i} : (G_i, \pi_i) \longrightarrow (G_i, \pi_i)$ is also a morphism of central extensions for $i = 1, 2$, by uniqueness of such a morphism, we have $1_{G_i} = \alpha_i \alpha_{3-i}$. That is, $\alpha_1 \alpha_2 = 1_{G_1}$ and $\alpha_2 \alpha_1 = 1_{G_2}$.

Now, if $g \in ker(\alpha_1)$ then $g = (g)1_{G_1} = (g)\alpha_1\alpha_2 = (g\alpha_1)\alpha_2 = 1$, so $ker(\alpha_1) = 1$, that is α_1 is a monomorphism. Moreover, since for all $x \in G_2$ there exists $x\alpha_2 \in G_1$ such that $(x\alpha_2)\alpha_1 = x$, the map $\alpha_1 : G_1 \longrightarrow G_2$ is onto. Therefore α_1 is an isomorphism. (Similarly α_2 is an isomorphism too). Therefore, $G_1 \cong G_2$, that is, up to isomorphism there is at most one universal central extension of G. □

Lemma 2.5.7. *Let G, H be two groups and $\alpha : G \longrightarrow H$ be a surjective group homomorphism. Then $G'\alpha = H'$.*

Proof. $G' = \langle [g_i, g_j] : g_i, g_j \in G \rangle$. Then an arbitrary element $x \in G'$ can be written as

$$x = [g_1, g_2][g_3, g_4] \dots [g_{k-1}, g_k] \text{for some } g_i \in G.$$

Then

$$\begin{aligned} x\alpha &= ([g_1, g_2][g_3, g_4] \dots [g_{k-1}, g_k])\alpha \\ &= [g_1, g_2]\alpha \, [g_3, g_4]\alpha \, \dots [g_{k-1}, g_k]\alpha \\ &= [g_1\alpha, g_2\alpha][g_3\alpha, g_4\alpha] \dots [g_{k-1}\alpha, g_k\alpha] \in (G\alpha)' = H'. \end{aligned}$$

Therefore, $G'\alpha \subseteq H'$.

Conversely, let $[h_1, h_2]$ be a commutator in H'. Since α is surjective, there exists $g_i \in G$ such that $h_i = g_i\alpha$ for $i = 1, 2$. Then $[h_1, h_2] = [g_1\alpha, g_2\alpha] = [g_1, g_2]\alpha \in G'\alpha$. Since every generator of H' lies in $G'\alpha$, $H' \subseteq G'\alpha$. Hence $H' = G'\alpha$. □

Theorem 2.5.8. *If $(\tilde{G}, \pi)$ is a universal central extension of G, then both G and $\tilde{G}$ are perfect.*

Proof. Let $H = \tilde{G} \times (\tilde{G}/\tilde{G}')$ and define $\alpha : H \longrightarrow G$ by $(x, y)\alpha = x\pi$. Since $(\tilde{G}, \pi)$ is a central extension of G, $\pi : \tilde{G} \longrightarrow G$ is a homomorphism with $ker(\pi) \leq Z(\tilde{G})$. Now since $Z(H) = Z(\tilde{G}) \times \tilde{G}/\tilde{G}'$, we have

$$\begin{aligned} ker(\alpha) &= \{(x, y) : (x)\pi = 1\} \\ &= ker(\pi) \times \tilde{G}/\tilde{G}' \\ &\leq Z(\tilde{G}) \times \tilde{G}/\tilde{G}' \\ &= Z(H). \end{aligned}$$

Then (H, α) is a central extension of G and $\alpha_i : (\tilde{G}, \pi) \longrightarrow (H, \alpha)$ are morphisms, where $x\alpha_1 = (x, 1)$ and $x\alpha_2 = (x, x\tilde{G}')$. Since $(\tilde{G}, \pi)$ is the universal central extension of G, the morphism from $(\tilde{G}, \pi)$ to (H, α) must be unique, therefore $\alpha_1 = \alpha_2$. Now

$$(x, \tilde{G}') = (x)\alpha_1 = (x)\alpha_2 = (x, x\tilde{G}').$$

That is $x \in \tilde{G}'$ for all $x \in G$, therefore $\tilde{G} = \tilde{G}'$. Thus, $\tilde{G}$ is perfect. G is a homomorphic image of a perfect group, so G is also perfect by Lemma 2.5.7. □

Theorem 2.5.9. *Let G be perfect and (H, π) a central extension of G. Then $H = ker(\pi)H'$ with H' perfect.*

Proof. By Lemma 2.5.7, $H'\pi = (H\pi)' = G'$. Since G is perfect, $H'\pi = G$. Hence $H = H'ker(\pi)$. Since (H, π) is a central extension, $ker(\pi) \leq Z(H)$. Now

$$\begin{aligned} H' &= [H, H] = [H'ker(\pi), H'ker(\pi)] \\ &= [H', H'], \text{since } ker(\pi) \leq Z(H) \\ &= H^{(2)}. \end{aligned}$$

Therefore H' is perfect. □

For the proof of Theorem 2.5.11 we need the following result which is known as Van Dyck's Theorem.

Lemma 2.5.10. *Let $\alpha : Y \longrightarrow Y\alpha$ be a function of Y onto a set $Y\alpha$, H a group generated by $Y\alpha$ and W a set of words $w = y_1^{\delta_1} \dots y_n^{\delta_n}$ in $Y \cup Y^{-1}$ with $w\alpha = (y_1\alpha)^{\delta_1} \dots (y_n\alpha)^{\delta_n} = 1$ in H for each $w \in W$. (That is H is generated by $Y\alpha$ and satisfies the relations $w = 1$ for all $w \in W$.) Then α extends uniquely to a surjective homomorphism of $\langle Y, W\rangle$ onto H.*

Proof. See [1], Theorem 28.6. $\square$

The following theorem gives an important characterization of perfect groups.

Theorem 2.5.11. *G has a universal central extension if and only if G is perfect.*

Proof. If G has a universal central extension, by Theorem 2.5.8, G is perfect. We need to show the converse. Assume G is perfect. Let

$$- : G \longrightarrow \overline{G}$$
$$g \longrightarrow \overline{g}$$

be a bijection between G and a set $\overline{G}$. Let F be the free group on $\bar{G}$. Define $\Gamma = \{\overline{x}\,\overline{y}(\overline{xy})^{-1} : x, y \in G\} \subseteq F$. Let M be the normal subgroup of F generated by Γ. Now for every $x, y \in G$ we have

$$\overline{x}\,\overline{y}(\overline{xy})^{-1}M = M$$
$$\text{Therefore, } \overline{x}\,\overline{y}M = (\overline{xy})M.$$

Next define $\Delta = \{[w, \overline{z}] : w \in \Gamma, z \in G\}$. Let N be the normal subgroup of F generated by Δ. Now $N = [M, F]$, so $N \lhd M$. Consider $M/N \leq F/N$. Now $\big[F/N, M/N\big] = [F, M]N/N = N/N$, so $M/N \leq Z(F/N)$. By Lemma

2.5.10, there is a unique homomorphism $\pi : F/N \longrightarrow G$ with $(\bar{x}N)\pi = x$ for all $x \in G$. Then $M/N = ker(\pi) \leq Z(F/N)$, that is $(F/N, \pi)$ is a central extension of G.

Let (H, σ) be a central extension of G. Then $\sigma : H \longrightarrow G$ is an epimorphism with $ker(\sigma) \leq Z(H)$. Since σ is an epimorphism, for all $x \in G$ there exists $h(x) \in H$ such that $h(x)\sigma = x$. Now for every $x, y, z \in G$, consider $w = h(x)h(y)h(xy)$ satisfies $(w)\sigma = (h(x)h(y)h(xy))\sigma = (h(x))\sigma(h(y))\sigma(h(xy))\sigma = xy(xy^{-1}) = 1$. Therefore, $w \in ker(\sigma) \leq Z(H)$. Then necessarily $[w, h(z)] = 1$. Then since $M/N < Z(F/N)$, the same relations hold in F/N and H, that is, by Lemma 2.5.10, there is a unique epimorphism α with $(\bar{x}N)\alpha = h(x)$ for each x in G. Now, since $(\bar{x}N)\alpha = h(x)$ and $(h(x))\sigma = x = (\bar{x}N)\pi$ for all $\bar{x}N \in F/N$, we have $\alpha\sigma = \pi$ that is α is a morphism between the central extensions $(F/N, \pi)$ and (H, σ) of G.

Now define $\tilde{G} = (F/N)'$. Since G is perfect and $(F/N, \pi)$ is a central extension of G, by Theorem 2.5.9, we have $F/N = ker(\pi)\tilde{G}$ and $\tilde{G}$ is perfect. Since $ker(\pi) \leq Z(F/N)$, $ker(\pi) \leq Z(\tilde{G})$ that is $(\tilde{G}, \pi)$ is also a central extension of G.

Let $\beta : (\tilde{G}, \pi) \longrightarrow (H, \sigma)$ be a morphism. Define $\gamma : \tilde{G} \longrightarrow H$ by $u\gamma = (u\alpha)(u\beta)^{-1}$ for all $u \in \tilde{G}$. Since $\pi = \alpha\sigma = \beta\sigma$, for any $u \in \tilde{G}$, $(u\gamma)\sigma = ((u\alpha)(u\beta)^{-1})\sigma = u\pi(u\beta\sigma)^{-1} = (u\pi)(u\pi)^{-1} = 1$. Then $\tilde{G}\gamma \leq ker(\sigma) \leq Z(H)$. So $\tilde{G}\gamma$ is abelian.

Consider for all $u, v \in \tilde{G}$,

$$\begin{aligned}
(uv)\gamma &= ((uv)\alpha)((uv)\beta)^{-1} \\
&= (u\alpha)(v\alpha)((u\beta)(v\beta))^{-1} \\
&= (u\alpha)(v\alpha)(v\beta)^{-1}(u\beta)^{-1} \\
&= (u\alpha)(v\gamma)(u\beta)^{-1} \\
&= (u\alpha)(u\beta)^{-1}(v\gamma), \text{ since } v\gamma \in Z(H) \\
&= (u\gamma)(v\gamma).
\end{aligned}$$

Therefore, γ is a homomorphism. $\tilde{G}$ is perfect. By Lemma 2.5.7, $\tilde{G}\gamma$ is perfect. But since it is abelian, we have $\tilde{G}\gamma = 1$, which means $u\gamma = (u\alpha)(u\beta)^{-1} = 1$ for all $u \in \tilde{G}$. Hence, $\alpha = \beta$. This proves that $(\tilde{G}, \pi)$ is the universal central extension of G. $\square$

Definition 2.5.12. *If G is a perfect group and $(\tilde{G}, \pi)$ its universal central extension, then $\tilde{G}$ is called the* ***universal covering group*** *of G and $ker(\pi)$ is called* ***the Schur multiplier*** *of G.*

A **perfect central extension** or a **covering** of a group G is a central extension (H, α) of G with H perfect. In this case, the map α is also known as **covering**.

By Theorem 2.5.8, for a perfect group G, the universal covering group $\tilde{G}$ is also perfect. Since $ker(\pi) \leq Z(\tilde{G})$, we can conclude that the Schur multiplier is always an abelian group.

Lemma 2.5.13. *Let (H, α) be a central extension of a group G and (K, β) be a perfect central extension of H. Then $(K, \beta\alpha)$ is a perfect central extension of G.*

Proof. Since $\beta : K \longrightarrow H$ and $\alpha : H \longrightarrow G$ are epimorphisms, $\beta\alpha : K \longrightarrow G$ is an epimorphism. Since K is perfect, all our need to show is $ker(\beta\alpha) \leq Z(K)$. Let x be an element of $ker(\beta\alpha)$. Then $(x)\beta\alpha = 1$, which means $(x)\beta \in ker(\alpha)$. Since (H, α) is a central extension of G, we have $ker(\alpha) \leq Z(H)$. Therefore, for all $y\beta \in H$, the commutator $[x\beta, y\beta] = 1$ that is, $[x, y]\beta = 1$ for all $y \in K$. Then $[x, y] \in ker(\beta) \leq Z(K)$ since (K, β) is a central extension of H. Now, $[x, y, t] = 1$ for every $y, t \in K$. Therefore $[ker(\beta\alpha), K, K] = 1$ and $[K, ker(\beta\alpha), K] = 1$. By Three Subgroup Lemma, $[K, K, ker(\beta\alpha)] = 1$. Since K is perfect $1 = [K, K, ker(\beta\alpha)] = [K, ker(\beta\alpha)]$, therefore $ker(\beta\alpha) \leq Z(K)$, and this is what we need to show. $\square$

Lemma 2.5.14. *Let (H, α) and (K, β) be central extensions of a group G with K perfect, and $\gamma : (H, \alpha) \longrightarrow (K, \beta)$ be a morphism of central extensions. Then (H, γ) is a central extension of K.*

Proof. We need to prove that $\gamma : H \longrightarrow K$ is an epimorphism with $ker(\pi) \leq Z(H)$. Since γ is a morphism of central extensions, γ is a homomorphism from H to K and $\gamma\beta = \alpha$. Then $ker(\gamma) \leq ker(\alpha)$. Since (H, α) is a central extension of G, $\alpha : H \longrightarrow G$ is an epimorphism with $ker(\alpha) \leq Z(H)$. So, $ker(\gamma) \leq Z(H)$. Then $\gamma\beta$ is an epimorphism from H to G. Now, $K = (H\gamma)(ker(\beta))$. Then

$$\begin{aligned} K &= K' \\ &= [(H\gamma)(ker(\beta), (H\gamma)(ker(\beta)] \\ &= [H\gamma, H\gamma], \text{ since } ker(\beta) \leq Z(K), \end{aligned}$$

since K is perfect. Therefore, $H\gamma = K$, that is, γ is an epimorphism. $\square$

Lemma 2.5.15. *Let $\tilde{G}$ be the universal covering group of a perfect group G and let (H, α) be a perfect central extension of $\tilde{G}$. Then α is an isomorphism.*

Proof. Let $\pi : \tilde{G} \longrightarrow G$ be the universal covering. By Lemma 2.5.13, $(H, \alpha\pi)$ is a perfect central extension of G. Since $(\tilde{G}, \pi)$ is the universal central extension of G, there is a morphism $\beta : (\tilde{G}, \pi) \longrightarrow (H, \alpha\pi)$. Since β is a morphism of central extensions, $\beta\alpha\pi = \pi$. Then, from $(\tilde{G}, \pi)$ to $(\tilde{G}, \pi)$, we have both the identity morphism 1 and $\beta\alpha$. Since $(\tilde{G}, \pi)$ is universal, we have $\beta\alpha = 1$.

Now, let $x \in ker(\beta)$, that is, $x\beta = 1$. Then $x\beta\alpha = 1\alpha = 1$. But since $\beta\alpha$ is identity, $x = 1$. So β is a monomorphism.

Since $(\tilde{G}, \pi)$ and $(H, \alpha\pi)$ are central extensions of G with H perfect and $\beta : (\tilde{G}, \pi) \longrightarrow (H, \alpha\pi)$ is a morphism of central extensions, by Lemma 2.5.14 $(\tilde{G}, \beta)$ is a central extension of H, that is, β is an epimorphism. Then β is an isomorphism. Since $\beta^{-1} = \alpha$, α is an isomorphism. $\square$

Theorem 2.5.16. *Let G be a perfect group, $(\tilde{G}, \pi)$ be the universal central extension of G, and (H, σ) be a perfect central extension of G. Then;*

1. *There exists a covering $\alpha : \tilde{G} \longrightarrow H$ with $\pi = \alpha\sigma$.*

2. *$(\tilde{G}, \alpha)$ is the universal central extension of H.*

3. *The Schur multiplier of H is a subgroup of the Schur multiplier of G.*

4. *If $Z(G) = 1$, then $Z(\tilde{G}) = ker(\pi)$ is the Schur multiplier of G, and $Z(H) = ker(\sigma) = ker(\pi)/ker(\alpha)$ is the quotient of the Schur multiplier of G with the Schur multiplier of H.*

Proof. 1. Since $(\tilde{G}, \pi)$ is the universal central extension and (H, σ) is another central extension of G, there exists a unique morphism $\alpha : (\tilde{G}, \pi) \longrightarrow (H, \sigma)$. Then α is a homomorphism from $\tilde{G}$ to H with $\pi = \alpha\sigma$. Now, $ker(\alpha) \leq ker(\pi) \leq Z(\tilde{G})$, therefore, $(\tilde{G}, \alpha)$ is a perfect central extension (or covering) of H.

2. Since H is perfect, by Theorem 2.5.11, H has a universal central extension. Denote it $(\tilde{H}, \beta)$. Since $\alpha : (\tilde{G}, \pi) \longrightarrow (H, \sigma)$ is a morphism of central extensions and H is perfect, then by Lemma 2.5.14, $(\tilde{G}, \alpha)$ is a (perfect) central extension of H. By universal property of $(\tilde{H}, \beta)$, there exists a unique morphism $\gamma : (\tilde{H}, \beta) \longrightarrow (\tilde{G}, \alpha)$. Then γ is a group homomorphism from $\tilde{H}$ to $\tilde{G}$ with $\gamma\alpha = \beta$.

   Now, by Lemma 2.5.14, $(\tilde{H}, \gamma)$ is a (perfect) central extension of $\tilde{G}$, which is the universal covering group of a perfect group. Then by Lemma 2.5.15, γ is an isomorphism. So, $(\tilde{G}, \alpha)$ is a universal central extension of H.

3. Since $(\tilde{G}, \alpha)$ is the universal central extension of H and $(\tilde{G}, \pi)$ is the universal central extension of G, it is enough to show that $ker(\alpha) \leq$

$ker(\pi)$. Let $x \in ker(\alpha)$. Since $\pi = \alpha\sigma$, we have

$$\begin{aligned}(x)\pi =& (x)\alpha\sigma \\ =& (x\alpha)\sigma \\ =& (1)\sigma = 1.\end{aligned}$$

So, $x \in ker(\pi)$, that is $ker(\alpha) \leq ker(\pi)$.

4. Since $(\tilde{G}, \pi)$ is the universal central extension of G, the Schur multiplier of G is $ker(\pi)$. Clearly, $ker(\pi) \leq Z(\tilde{G})$. Now let $g \in Z(\tilde{G}) \backslash ker(\pi)$. Then $g.ker(\pi) \neq ker(\pi)$. So, $g.ker(\pi)$ is a non-trivial element of $\tilde{G}/ker(\pi)$.

   Since $\tilde{G}/ker(\pi)$ is isomorphic to G, there exists an isomorphism

   $$\begin{aligned}\bar{\pi} : \tilde{G}/ker(\pi) &\longrightarrow G \\ x.ker(\pi) &\longrightarrow (x)\pi.\end{aligned}$$

   Then, if $g \in Z(\tilde{G})$, $(g.ker(\pi))\bar{\pi}$ is a central element of G. But, since $Z(G) = 1$, we get a contradiction. Therefore $ker(\pi) = Z(\tilde{G})$.

   Similarly we have $ker(\sigma) = Z(H)$. Now $\alpha : \tilde{G} \longrightarrow H$ and $\sigma : H \longrightarrow G$ epimorphisms with $\alpha\sigma = \pi$. Clearly, $ker(\alpha) \leq ker(\pi)$. Define $\bar{\alpha} : ker(\pi) \longrightarrow \mathrm{ker}(\sigma)$ such that $(x)\bar{\alpha} = (x)\sigma$ for all $x \in ker(pi)$. Since α is onto, $\bar{\alpha}$ is an epimorphism. Since $ker(\alpha) \leq ker(\pi)$, $ker(\bar{\alpha}) = ker(\alpha)$. Therefore $ker(\pi)/ker(\alpha) = Im(\bar{\alpha}) = ker(\sigma)$.

□

Since all non-abelian simple groups are necessarily perfect, then up to isomorphism there is a unique universal central extension. Therefore the Schur multiplier exists for every non-abelian simple group. The following result is an easy consequence of Theorem 2.5.16.

Corollary 2.5.17. *For a non-abelian finite simple group G, the Schur multiplier is the center of the universal central extension.*

Proof. For a non-abelian simple group, center is trivial. Then by Theorem 2.5.16 Part 4, we can conclude that the Schur multiplier of a non-abelian finite simple group G is exactly the center of the universal central extension of G. □

Theorem 2.5.18. *Let G be a perfect finite group. Then the universal covering group of G is finite, hence the Schur multiplier of G is finite.*

Proof. Since G is perfect, G has a universal central extension $(\tilde{G}, \pi)$ by Theorem 2.5.11. Now, $\tilde{G}$ is the universal covering of G, and $ker(\pi)$ is the Schur multiplier of G. Since $ker(\pi) \leq Z(\tilde{G})$, we have $|\tilde{G}/Z(\tilde{G})| \leq |\tilde{G}/ker(\pi)|$. But since $\tilde{G}/ker(\pi)$ is isomorphic to G, it is finite, therefore, $\tilde{G}/Z(\tilde{G})$ is finite. Then, by Lemma 2.1.11, we have $\tilde{G}'$ is finite. Since $\tilde{G}$ is perfect, the universal covering group $\tilde{G}$ of G is finite. □

2.6 Schur multipliers of finite simple groups

In this section the tables of Schur multipliers of finite simple groups are presented. By The Classification of Finite Simple Groups, ([12, 13, 14, 15]), we know that a non-abelian finite simple group is either an alternating group or a simple group of Lie type or one of the 26 sporadic groups.

In Table 2.2, the Schur multiplier of a simple group of Lie type has order $d.e$, the outer automorphism group has order $d.f.g$, where the order of the base field is $q = p^f$ and the numbers d, f, g denote the diagonal, field and the graph automorphisms. The Schur multiplier is the direct product of groups of orders d (diagonal or canonical part of the Schur multiplier) and e (exceptional multiplier). The diagonal multiplier extends the adjoint group to the corresponding universal Chevalley group. The exceptional multiplier

Table 2.1: Schur multipliers of alternating groups

$\mathbf{n}$	$\mathbf{M(A_n)}$
$n = 4, 5$	Z_2
$n = 6, 7$	Z_6
$n > 7$	Z_2

is always a p-group, and is trivial except in finitely many cases. (For the details see [9, page xv].)

In Table 2.3, $\mathcal{N}$ denotes the order of the universal Chevalley group and $\mathcal{N}/d$ is the order of the adjoint Chevalley group.

In Table 2.4, $M(G)$ denotes the Schur multiplier and $Out(G)$ is the outer automorphism group of G. For a sporadic group the Schur multiplier and the outer automorphism group are both cyclic of order given in Table 2.4.

Table 2.2: Automorphisms and Schur multipliers of Chevalley groups

Condition	**Group**	**d**	**f**	**g**	**Cases when e $\neq$ 1**
	$A_1(q)$	$(2, q-1)$	$q = p^f$	1	$A_1(4) \to 2,\ A_1(9) \to 3$
$n \geq 2$	$A_n(q)$	$(n+1, q-1)$	$q = p^f$	2	$A_2(2) \to 2,\ A_2(4) \to 4^2,$ $A_3(2) \to 2$
$n \geq 2$	${}^2A_n(q)$	$(n+1, q+1)$	$q^2 = p^f$	1	${}^2A_3(2) \to 2,\ {}^2A_3(3) \to 3^2$ ${}^2A_5(2) \to 2^2$
	$B_2(q)$	$(2, q-1)$	$q = p^f$	1	$B_2(2) \to 2$
f odd	${}^2B_2(q)$	1	$q = 2^f$	1	${}^2B_2(8) \to 2^2$
$n \geq 3$	$B_n(q)$	$(2, q-1)$	$q = p^f$	1	$B_3(2) \to 2,\ B_3(3) \to 3$
$n \geq 3$	$C_n(q)$	$(2, q-1)$	$q = p^f$	1	$C_3(2) \to 2$
	$D_4(q)$	$(2, q-1)^2$	$q = p^f$	3!	$D_4(2) \to 2^2$
	${}^3D_n(q)$	1	$q = p^f$	1	none
$n \geq 4$	${}^2D_n(q)$	$(4, q^n+1)$	$q^2 = p^f$	1	none
$n \geq 4$, even	$D_n(q)$	$(2, q-1)^2$	$q = p^f$	2	none
$n \geq 4$, odd	$D_n(q)$	$(4, q^n-1)$	$q = p^f$	2	none
	$G_2(q)$	1	$q = p^f$	2 if $p = 3$	$G_2(3) \to 3,\ G_2(4) \to 2$
f odd	${}^2G_2(q)$	1	$q = 3^f$	1	none
	$F_4(q)$	1	$q = p^f$	2 if $p = 2$	$F_4(2) \to 2$
f odd	${}^2F_4(q)$	1	$q = 2^f$	1	none
	$E_6(q)$	$(3, q-1)$	$q = p^f$	2	none
	${}^2E_6(q)$	$(3, q+1)$	$q^2 = p^f$	1	${}^2E_6(2) \to 2^2$
	$E_7(q)$	$(2, q-1)$	$q = p^f$	1	none
	$E_8(q)$	1	$q = p^f$	1	none

Table 2.3: Orders of Chevalley groups

G	$\mathcal{N}$	**d**
$A_n(q)$, $n \geq 1$	$q^{n(n+1)/2} \prod_{i=1}^{n}(q^{i+1}-1)$	$(n+1, q-1)$
$B_n(q)$, $n \geq 2$	$q^{n^2} \prod_{i=1}^{n}(q^{2i}-1)$	$(2, q-1)$
$C_n(q)$, $n \geq 3$	$q^{n^2} \prod_{i=1}^{n}(q^{2i}-1)$	$(2, q-1)$
$D_n(q)$, $n \geq 4$	$q^{n(n-1)}(q^n-1) \prod_{i=1}^{n-1}(q^{2i}-1)$	$(4, q^n-1)$
$G_2(q)$	$q^6(q^6-1)(q^2-1)$	1
$F_4(q)$	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)$	1
$E_6(q)$	$q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$	$(3, q-1)$
$E_7(q)$	$q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$	$(2, q-1)$
$E_8(q)$	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1)$	1
${}^2A_n(q)$, $n \geq 2$	$q^{n(n+1)/2} \prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$	$(n+1, q+1)$
${}^2B_2(q)$, $q = 2^{2m+1}$	$q^2(q^2+1)(q-1)$	1
${}^2D_n(q)$, $n \geq 4$	$q^{n(n-1)}(q^n+1) \prod_{i=1}^{n-1}(q^{2i}-1)$	$(4, q^n+1)$
${}^3D_4(q)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$	1
${}^2G_2(q)$, $q = 3^{2m+1}$	$q^3(q^3+1)(q-1)$	1
${}^2F_4(q)$, $q = 3^{2m+1}$	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1)$	1
${}^2E_6(q)$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$	$(3, q+1)$

Table 2.4: Orders and the Schur multipliers of the 26 sporadic groups

G	**Order**	**|M(G)|**	**|Out(G)|**
M_{11}	$2^4.3^2.5.11$	1	1
M_{12}	$2^6.3^3.5.11$	2	2
M_{22}	$2^7.3^2.5.7.11$	12	2
M_{23}	$2^7.3^2.5.7.11.23$	1	1
M_{24}	$2^{10}.3^3.5.7.11.23$	1	1
J_2	$2^7.3^3.5^2.7$	2	2
Suz	$2^{13}.3^7.5^2.7.11.13$	6	2
HS	$2^9.3^2.5^3.7.11$	2	2
McL	$2^7.3^6.5^3.7.11$	3	2
Co_3	$2^{10}.3^7.5^3.7.11.23$	1	1
Co_2	$2^{18}.3^6.5^3.7.11.23$	1	1
Co_1	$2^{21}.3^9.5^4.7^2.11.13.23$	2	1
He	$2^{10}.3^3.5^2.7^3.17$	1	2
Fi_{22}	$2^{17}.3^9.5^2.7.11.13$	1	2
Fi_{23}	$2^{18}.3^{13}.5^2.7.11.13.17.23$	1	1
Fi_{24}'	$2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$	3	2
HN	$2^{14}.3^6.5^6.7.11.19$	1	2
Th	$2^{15}.3^{10}.5^3.7^2.13.19.31$	1	1
B	$2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$	2	1
M	$2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$	1	1
J_1	$2^3.3.5.7.11.19$	1	1
$O'N$	$2^9.3^4.5.7^3.11.19.31$	3	2
J_3	$2^7.3^5.5.17.19$	3	2
Ly	$2^8.3^7.5^6.7.11.31.37.67$	1	1
Ru	$2^{14}.3^3.5^3.7.13.29$	2	1
J_4	$2^{21}.3^3.5.7.11^3.23.29.31.37.43$	1	1

CHAPTER 3

On the Existence of Minimal Non-FC-Groups

3.1 Perfect locally finite minimal non-FC-groups

In [2], Belyaev described all minimal non-FC-groups which are different from their commutator subgroups and showed that non-perfect minimal non-FC-groups are exactly the Miller-Moreno groups described in [5]. In [2], Belyaev also showed that a perfect locally finite minimal non-FC-group is either a quasi-simple group or a locally finite p-group.

Let G be a locally finite simple group. A Kegel cover $\mathcal{K} = (G_i, N_i)_{i \in I}$ is a pair of subgroups of G such that $G_i \leq G_{i+1}$, the union $\bigcup_{i \in I} G_i$ is equal to G, each N_i is maximal normal in G_i, i.e. G_i/N_i simple and there exists $j \in I$ such that $G_i \cap N_j = 1$.

Belyaev proved that a perfect locally finite minimal non-FC-group is countable. Hence, for a locally finite simple minimal non-FC-group, we can choose the index set $\mathbb{N}$. In [22], Kuzucuoğlu and Phillips has shown that if there exists a simple locally finite minimal non-FC-group then it has a Kegel cover $\mathcal{K} = (G_i, N_i)_{i \in \mathbb{N}}$ where $N_i \leq Z(G)$. First, it is easy to show that if such a group exist then it can not be a linear simple group as these groups are generated by (B, N) pairs but (by [2] Lemma 6) we know that every two proper subgroup of a perfect minimal non-FC-groups generates a proper subgroup.

Then by using the above Kegel cover, it is shown in [22] that centralizer of an element involves an infinite simple group but this is impossible. Hence a simple locally finite minimal non-FC-group does not exist.

Since quasi-simple groups are perfect central extensions of simple groups, this investigation have demonstrated that quasi-simple case is impossible in the class of locally finite groups. This result implies if a perfect locally finite minimal non-FC-group exists, then it will belong to the class of p-groups.

Leinen and Puglisi showed in [23] that every perfect locally finite minimal non-FC-group has a non-trivial finitary linear representation. Moreover they proved that if a perfect locally finite minimal non-FC group exists, then it will be a subgroup of a McLain group $M(\mathbb{Q}, GF(p))$.

In [4] Belyaev strenghtened the result of [23] by proving that every perfect locally finite minimal non-FC-group has non-trivial finitary permutational representation. The aim of the following section is to explain this work. This result is also shown in [24] by Leinen.

The question whether or not there exists a perfect locally finite minimal non-FC-group exists is still open.

3.2 Belyaev's theorem

Our aim is to show that every perfect locally finite minimal non-FC group has nontrivial finitary permutational representation. The proof needs the following lemma. Recall that the subgroups X and Y are called **commensurable** if $X \cap Y$ has finite index in X and Y.

Lemma 3.2.1. *Let G be an arbitrary group and let a and b be elements of G satistying the following conditions:*

1. $|B : C_B(a)|$ *is finite where* $B = \langle b^G \rangle$.
2. $|\{[b, a^x] : x \in G\}|$ *is finite.*

3. $|C_G([g,a]) : C_G([g,a]) \cap C_G(a)| < \infty$ *for every* $g \in B \setminus C_B(a)$

4. the cenralizers of all elements conjugate with a *in* G *are commensurable.*

Then the number of elements conjugate with $a \in G$ *and not commuting with* b *is finite.*

Proof. Define $\Omega = a^G$. Consider the action of G on Ω by conjugation.

Let $\{\Omega_i : i \in I\}$ be the set of all B-orbits of elements in Ω. Then $\Omega = \bigcup_{i \in I} \Omega_i$. Since G acts on Ω transitively and $B \lhd G$, by Theorem 2.2.2 orbits of B form the blocks of imprimitivity in Ω. For all $\alpha_i \in \Omega_i, \alpha_j \in \Omega_j$ there exists $g \in G$ such that $\alpha_i^g = \alpha_j$. Then $\Omega_i^g \cap \Omega_j \neq \emptyset$. Since Ω_i is a block of imprimitivity, we have $\Omega_i^g = \Omega_j$. So G acts transitively on the set of blocks of imprimitivity of Ω.

By the first condition we have $|B : C_B(a)| < \infty$, so number of B-conjugates of a in B are finite. Therefore, for each $i \in I$, Ω_i is finite. Since G acts transitively on the set $\{\Omega_i : i \in I\}$, for any $i, j \in I$, Ω_i is conjugate to Ω_j. So each Ω_i have the same cardinality.

For all $i \in I$ define $\Delta_i = \Omega_i^{-1}.\Omega_i = \{x^{-1}y : x, y \in \Omega_i\}$. Since each Ω_i is finite, each Δ_i is finite.

Now, assume that the set of elements conjugate with a and not commuting with b is infinite, that is, the set $S = \{a^{x_i} : i \in I, [a^{x_i}, b] \neq 1\}$ is infinite.

Since S is a subset of Ω, $S = S \cap \Omega = S \cap (\bigcup_{i \in I} \Omega_i) = \bigcup_{i \in I}(S \cap \Omega_i)$. Since for all $i \in I$ we have $|\Omega_i| < \infty$, we have $|S \cap \Omega_i| < \infty$ for all $i \in I$. Therefore there exists infinitely many $i \in I$ satisfying

$$\Omega_i \cap S \neq \emptyset.$$

Consider the set $\{\Omega_i : \Omega_i \cap S \neq \emptyset\}$.

Denote the set of such $i \in I$ as I_1. Clearly I_1 is infinite. Let

$$K = \{[b, a^x] : x \in G\}$$

Assume $\Delta_i \cap K \neq 1$. Then $[b, a^x] \neq 1$ for some $x \in G$ and $a^x \in \Omega_i$ for some $i \in I$. Then $(a^x)^b \in \Omega_i$. Then $S \cap \Omega_i \neq 1$, i.e. $i \in I_1$. Conversely let $i \in I_1$, that is, there exists a non-trivial element $a^x \in \Omega_i \cap S$. Then $[b, a^x] \neq 1$ and $[b, a^x] \in \Delta_i \cap K$. Hence, we can write

$$I_1 = \{i \in I : K \cap \Delta_i \neq 1\}.$$

$|K| = |\{[b, a^x] : x \in G\}| < \infty$ by (2). Let

$$K = \{k_1, k_2, \dots k_n\}.$$

Define

$$J_i = \{j \in I_1 : k_i \in \Delta_j \cap K\}.$$

Clearly $\bigcup_{i=1}^{n} J_i = I_1$. Since I_1 is infinite there exists $k_m \in K$ such that J_m is infinite. Denote this infinite set J_m by I_2 and denote $k_m = t$. Then

$$t \in \Delta_i \cap K$$

for every $i \in I_2$. Now fix some index $n \in I_2$. Since G acts on the set of Ω_i's transitively, there exists $x_i \in G$ such that

$$\Omega_n^{x_i} = \Omega_i.$$

Now, $\Delta_n^{x_i} = x_i^{-1}\Omega_n^{-1}\Omega_n x_i = x_i^{-1}\Omega_n^{-1}x_i x_i^{-1}\Omega_n x_i = (x_i^{-1}\Omega_n^{-1}x_i)^{-1}(x_i^{-1}\Omega_n x_i) = \Omega_i^{-1}\Omega_i = \Delta_i$. Since $t \in \Delta_i$ for all $i \in I_2$, $t \in \Delta_n^{x_i}$, hence, we have $t^{x_i^{-1}} \in \Delta_n$ for all $i \in I_2$.

Recall Δ_n is finite, i.e. say $\Delta_n = \{n_1, n_2, \dots n_k\}$. Define

$$U_j = \{i \in I_2 : t^{x_i^{-1}} = n_j\}.$$

Clearly $\bigcup_{j=1}^{n} U_j = I_2$. Since I_2 is infinite, one of the U_j's must be infinite. Denote this set by I_3. So there is an infinite subset I_3 of I_2 such that $t^{x_i^{-1}} = t^{x_j^{-1}}$ for every $i, j \in I_3$. Then for all $i, j \in I_3$, $t^{x_i^{-1}x_j} = t$. Hence

$$x_i^{-1}x_j \in C_G(t)$$

for every $i, j \in I_3$. So the elements $x_i^{-1}, i \in I_3$ lie in one right coset of $C_G(t)$.

Now, since $t \in \Delta_n$, $t \in \Omega_n^{-1}\Omega_n$. So, there exists $g \in G$, $h \in B$ such that

$$t = a^{-gh}a^g = h^{-1}g^{-1}a^{-1}ghg^{-1}ag$$

$$= g^{-1}(gh^{-1}g^{-1})a^{-1}(ghg^{-1})ag = g^{-1}(h^{-1})^{g^{-1}}a^{-1}h^{g^{-1}}ag$$

$$= g^{-1}[h^{g^{-1}}, a]g$$

In any group G, for every $x \in G$,

$$C_G(x^g) = (C_G(x))^g$$

holds for all $g \in G$. Therefore, we have,

$$C_G(t) = C_G(g^{-1}[h^{g^{-1}}, a]g)$$

$$= C_G([h^{g^{-1}}, a]^g) = (C_G([h^{g^{-1}}, a]))^g.$$

Since $B \lhd G$ and $h \in B$, we have $h^{g^{-1}} \in B$. Assume $h^{g^{-1}} \in C_B(a)$. Then $[h^{g^{-1}}, a] = 1 \Rightarrow t = g^{-1}[h^{g^{-1}}, a]g = 1$ which contradicts with the choice of t.

$\therefore h^{g^{-1}} \in B \setminus C_B(a)$. So, by (3) we have

$$|C_G([h^{g^{-1}}, a]) : C_G([h^{g^{-1}}, a]) \cap C_G(a)| < \infty$$

$$\Rightarrow |(C_G([h^{g^{-1}}, a]))^g : (C_G([h^{g^{-1}}, a]) \cap C_G(a))^g| < \infty$$

$$\Rightarrow |C_G(t) : C_G(t) \cap C_G(a^g)| < \infty.$$

Then $C_G(t) = \bigcup_{i=1}^{m}(C_G(t) \cap C_G(a^g))v_i \Rightarrow C_G(t) \subseteq \bigcup_{i=1}^{m} C_G(a^g)v_i$. So every right coset of $C_G(t)$ can be covered with finitely many right cosets of $C_G(a^g)$. Recall that for every $i, j \in I_3$ we have $x_i^{-1}x_j \in C_G(t)$. Then for some fixed $\alpha \in I_3$ we have $x_i^{-1}x_\alpha \in C_G(t) \Rightarrow x_i^{-1} \in C_G(t)x_\alpha$ for every i$\in I_3$. Denote $x_\alpha = u$. So

$$x_i^{-1} \in C_G(t)u$$

for every $i \in I_3$. Then

$$x_i^{-1} \in C_G(t)u \subseteq \bigcup_{j=1}^{m} C_G(a^g)v_j u$$

for every i$\in I_3$. Since $\{x_i^{-1} : i \in I_3\}$ is infinite, for some $j \in \{1, 2, \ldots m\}$ there is an infinite subset I_4 of I_3 such that $x_i^{-1} \in C_G(a^g)v_j u$ for all $i \in I_4$. Then $x_i \in u^{-1}v_j^{-1}C_G(a^g)$ for all $i \in I_4$. Denote $u^{-1}v_j^{-1} = w$ i.e. $x_i \in wC_G(a^g)$ for all $i \in I_4$.

By (4), $C_G(a^g)$ and $(C_G(a^g))^{w^{-1}}$ are commensurable. Then;

$$|C_G(a^g) : C_G(a^g) \cap C_G(a^{gw^{-1}})| < \infty.$$

$$|C_G(a^{gw^{-1}}) : C_G(a^g) \cap C_G(a^{gw^{-1}})| < \infty.$$

Therefore $wC_G(a^g) = wC_G(a^g)w^{-1}w = C_G(a^{gw^{-1}})w \subseteq \bigcup_{k=1}^{n} C_G(a^g)z_k$ for some n$\in \mathbb{N}$ for some $z_k \in G$. Therefore every left coset of $C_G(a^g)$ can be covered with finitely many right cosets of $C_G(a)$. Therefore in the set $\{x_i : i \in I_4\}$ we may choose an infinite subset $\{x_i : i \in I_5\}$ that lies in one right coset of $C_G(a)$. Then

$$C_G(a^g)x_i = C_G(a^g)x_j$$

for all $i, j \in I_5$. This implies $C_G(a^g)x_i x_j^{-1} = C_G(a^g)$, so $(a^g)^{x_i} = (a^g)^{x_j}$ for all $i, j \in I_5$. Since $a^g \in \Omega_n$, $(a^g)^{x_i} \in \Omega_i$ and $a^g)^{x_j} \in \Omega_j$. But since $(a^g)^{x_i} = (a^g)^{x_j}$ for all $i, j \in I_5$, $\Omega_i \cap \Omega_j \neq \emptyset$ for any $i, j \in I_5$. Since the set $\{\Omega_i : i \in I\}$ forms the blocks of imprimitivity, we have $\Omega_i = \Omega_j$ for any $i, j \in I_5$. This contradicts with the choice of x_i's.

Therefore, the set of elements conjugate with a and not commuting with b is finite. □

Theorem 3.2.2. *Let G be an arbitrary group in which*

1. *The centralizers of all non-trivial elements are commensurable.*

2. Each element belongs to a normal FC-subgroup.

Then for every pair of elements a and b of G, the element b does not commute only with finitely many elements conjugate with a.

Proof. Let G be a group satisfying (1) and (2) of the Theorem and a and b be nontrivial elements in G. Let $B = \langle b^G \rangle$. Now for all $g \in B \setminus C_B(a)$, we have $[g, a] \neq 1$. Since $a \neq 1$, $C_G(a)$ and $C_G([g, a])$ are commensurable. So condition (3) of Lemma 3.2.1 is satisfied. Clearly condition (4) of Lemma 3.2.1 is a direct consequence of the first condition of the Theorem.

Since each element in G belongs to a normal FC-subgroup, B is the smallest normal subgroup of G containing b, and subgroup of an FC-group is an FC-group, we have B is an FC-group. Then $|B : C_B(x)| < \infty$ for every $x \in B$. In particular, $|B : C_B(b)| < \infty$. Since by the first condition of the Theorem we know that $C_B(b)$ and $C_B(a)$ are commensurable, we have;

$$|C_B(a) : C_B(a) \cap C_B(b)| < \infty$$
$$|C_B(b) : C_B(a) \cap C_B(b)| < \infty.$$

Then $|B : C_B(a) \cap C_B(b)| = |B : C_B(b)||C_B(b) : C_B(a) \cap C_B(b)| < \infty$. But $|B : C_B(a) \cap C_B(b)| = |B : C_B(a)||C_B(a) : C_B(a) \cap C_B(b)|$. Therefore $|B : C_B(a)| < \infty$. So, condition (1) of Lemma 3.2.1 is satisfied for all $a, b \in G$. Let $A = \langle a^G \rangle$. Then for all $b \in G$ the index $|A : C_A(b)|$ is finite by condition (1) of Lemma 3.2.1. So the number of $A-$conjugates of b in G is finite. Then

$$|\{b^{a^x} : x \in G\}| = |\{a^{-x} b a^x : x \in G\}| < \infty.$$

Now

$$\{[b, a^x] : x \in G\} = \{b^{-1} a^{-x} b a^x : x \in G\}.$$

But we have

$$|\{b^{-1} a^{-x} b a^x : x \in G\}| = |\{a^{-x} b a^x : x \in G\}|.$$

Therefore $|\{[b, a^x] : x \in G\}| < \infty$.

Hence, the first condition of Lemma 3.2.1 implies the second one.

Now, all conditions of Lemma 3.2.1 is satisfied for arbitrary elements $a, b \in G$. Then for any pair of elements $a, b \in G$, b does not commute with only finitely many elements conjugate with a. $\square$

Theorem 3.2.3. *Let G be a perfect locally finite minimal non-FC-group and let $Z(G) = 1$. Then for every pair of element $a, b \in G$, b does not commute only finitely many conjugates of a.*

Proof. Let G be a perfect locally finite minimal non-FC-group. In [3] Belyaev proved that if G is a perfect minimal non-FC-group then G is one of the following:

1. G is a two generated quasi-simple group.
2. G is an infinite non-abelian Schmidt group.
3. G is a locally finite group with centralizers of all non-central elements are commensurable.

In our case, G is locally finite. If G is a two-generated quasi-simple group, since G is locally finite, it must be finite. Since every finite group is an FC-group, a perfect locally finite minimal non-FC-group can not be two-generated. If G is an infinite non-abelian Schmidt group, i.e. every proper subgroup of G is finite, then G satisfies minimal condition. Since G is a locally finite group satisfying **min**, by Theorem 2.3.5, G is a Chernikov group. Therefore G has a divisible abelian hence infinite subgroup, so it can not be a Schmidt group. Hence G has to be an element of the third class above, that is, G must be a locally finite group with centralizers of all non-central elements are commensurable. So, the first condition of Theorem 3.2.2 holds.

Now, we need to show that every element in a perfect locally finite p-group belong to a proper normal subgroup. Firstly, we need the following result.

Lemma 3.2.4. *A simple locally nilpotent group is finite, so, isomorphic to* $\mathbb{Z}_p$ *for some prime* p.

Proof. Let H be a simple locally nilpotent group. Then H itself is the minimal normal subgroup of H. By Lemma 2.4.2, H must be central, that is H is abelian. But an abelian simple group must be isomorphic to Z_p for some prime p. Hence there exists no infinite locally nilpotent simple group. □

Now let's return to the proof of Theorem 3.2.3. Since G is a locally finite p-group, it is locally nilpotent. Since G is not an FC-group, G is necessarily infinite . Then, by Lemma 3.2.4, G can not be simple. Let N be a proper normal subgroup of G. If $x \in N$, then there is nothing to prove. If x is not in N, consider G/N, which is again a locally finite p-group, so can not be simple. Continuing in this way, we can write G as a union of its proper normal subgroups. Therefore, every element $x \in G$ belong to a proper normal subgroup.

In particular, every element in a perfect locally finite p-group belong to a proper normal subgroup. Hence conditions of Theorem 3.2.2 are satisfied, therefore for every pair of element $a, b \in G$, b does not commute only with finitely many elements conjugate with a. □

Theorem 3.2.5. *Every perfect locally finite minimal non-FC-group has non-trivial finitary permutational representation.*

Proof. Let G be a perfect locally finite minimal non-FC-group. Let $H = G/Z(G)$. First, since $H' = G'Z(G)/Z(G) = G/Z(G) = H$, we have H is perfect. Since G is perfect, by Theorem 2.1.13, $Z(H)$ is trivial, that is, H is a perfect locally finite minimal non-FC-group with trivial center. So, by

Theorem 3.2.3, for every $x, y \in H$ the number of elements conjugate with x and not commuting with y is finite. Now, fix an element $a \in H$ and let $X = a^H = \{a^h : h \in H\}$ be the conjugacy class of a in H. Clearly the map

$$\begin{aligned} \tau_h :& X \longrightarrow X \\ & a^{h_0} \longrightarrow a^{h_0 h} \end{aligned}$$

is a permutation of X. Define the map ρ as

$$\begin{aligned} \rho :& H \longrightarrow Sym(X) \\ & h \longrightarrow \tau_h. \end{aligned}$$

Now for every $h_1, h_2 \in H, (h_1h_2)\rho = \tau_{h_1h_2}$. For all a^x in a^H, $a^x(h_1h_2)\rho = a^x\tau_{h_1h_2} = a^{xh_1h_2}$. On the other hand, $(h_1)\rho(h_2)\rho = \tau_{h_1}\tau_{h_2}$. Therefore, for all $a^x \in a^H$, $(a^x)(h_1)\rho(h_2)\rho = a^{xh_1}(h_2)\rho = a^{xh_1h_2}$. Therefore $\rho(h_1h_2) = \rho(h_1)\rho(h_2)$. Hence, ρ is a homomorphism from H to $Sym(X)$, i.e. it is a permutational representation. We need to show that ρ is finitary. Since by Theorem 3.2.3, number of elements conjugate with a and not commuting with h is finite for all $h \in H$, $(a^x)\tau_h = a^{xh} = a^h$ for all but finitely many $a^x \in X$, so, we have $(h)\rho = \tau_h$ is equal to identity permutation for all but finitely many $h \in H$, that is ρ is a finitary permutational representation of H.

Now, consider the canonical homomorphism $\pi : G \longrightarrow G/Z(G) = H$ given by $\pi(g) = gZ(G)$ for all $g \in G$. Then $\rho\pi$ is a homomorphism from G to $Sym(X)$. Since ρ is finitary, so is $\pi\rho$. Hence $\pi\rho$ will be the needed finitary permutational representation of G.

□

CHAPTER 4

Coprime Automorphisms of Quasi-simple Groups

4.1 Coprime automorphisms of finite groups

Let G be a finite group and A a group of automorphisms of G such that orders of G and A are coprime. This situation, in particular the case where the action is fixed-point-free, i.e. $C_G(A)=1$, or when there is an other restriction on $C_G(A)$ has been studied by many authors. In [25], a dual situation where the index $|G : C_G(A)|$ is bounded is investigated by Parker and Quick. They obtained the following two results:

Theorem 4.1.1. *Let G be a finite group and A be a group of automorphisms of G such that orders of G and A are coprime. If $|G : C_G(A)| \leq n$, then $|[G, A]| \leq n^{\log_2(n+1)}$.*

Theorem 4.1.2. *Let G be a finite p-group for some prime p and A be a group of automorphisms of G such that p does not divide the order of A. If $|G : C_G(A)| \leq p^m$, then $|[G, A]| \leq p^{(m^2+m)/2}$.*

For the proofs of these results, see [25]. Theorem 4.1.2 is used for the proof of Theorem 4.1.1. But in fact, we are interested in finite quasi-simple groups and their coprime automorphisms. Because of this, we write in sequel only the quasi-simple groups part of this article. Recall that a group G is called quasi-simple if G is perfect and $G/Z(G)$ is simple. In this chapter, we give some basics results on quasi-simple groups and prove that if Q is a quasi-simple group and A a group of automorphisms of Q such that orders of Q and A are coprime satisfying $|Q : C_Q(A)| \leq n$, then $|Q| \leq n^3$. This result is used to prove Theorem 4.1.1 in [25].

4.2 Basic results on quasi-simple groups

Theorem 4.2.1. *Let Q be a finite quasi-simple group. Then $|Z(Q)|^3 \leq |Q|$.*

Proof. Recall that a group Q is quasi-simple if $Q = Q'$ and $Q/Z(Q)$ is simple. Clearly finite quasi-simple groups are exactly the perfect covering groups of finite simple groups.

Now let Q be a quasi-simple group and let $X = Q/Z(Q)$. Being simple, X has to be perfect, so the universal central extension (G, π) of X exists by Theorem 2.5.11. Since $Z(X)$ is necessarily trivial, by Theorem 2.5.16 (4), the Schur multiplier $M(X) = ker(\pi)$ is equal to $Z(G)$ and $Z(Q)$ is a quotient of $Z(G) = M(X)$. Then $|Z(Q)| \leq |M(X)|$.

We know that if X is a non-abelian finite simple group then X belongs to the families of alternating groups or simple groups of Lie type or the 26 sporadic group.

We need to verify that if X is a finite simple group, the Schur multiplier $M(X)$ of X satisfies

$$|M(X)|^2 \leq |X|.$$

If this inequality holds, then since $|Z(Q)|^2 \leq |M(X)|^2 \leq |X| = |Q/Z(Q)|$, we have $|Z(Q)|^3 \leq |Q|$.

Let's start with the case where X is an alternating group A_n for some $n > 4$. By Table 2.1, the order of the Schur multiplier of an alternating group can not exceed 6. We know that the smallest non-abelian simple alternating group is A_5 which has order 60. Clearly $6^2 < 60$, so $|M(X)|^2 \leq |X|$ for every alternating group X.

For simple groups of Lie type we use Table 2.2. If X is a simple group of Lie type, then $|X|$ can be calculated using the information given in Table 2.3 i.e. $|X| = \mathcal{N}/d$ where $\mathcal{N}$ is the order of the universal Chevalley group and d denotes the number of diagonal automorphisms of X. Table 2.2 consists of not only the simple groups of Lie type, but other Chevalley groups which are not simple also. We will prove the inequality for all groups in Table 2.2.

We need to verify that $|X| > |M(X)|^2$, but since $|X| = \mathcal{N}/d$ and $|M(X)| = d.e$, so, we need to verify that $\mathcal{N}/d > d^2e^2$ i.e. $\mathcal{N} > d^3e^2$. Except finitely many cases given in Table 2.2, $e = 1$. Now, we will consider the cases seperately:

- For $X = A_1(q)$, if $e = 1$ and $q = 2$, $d = (2, q-1) = 1$. Then, clearly, $\mathcal{N} > d^3e^2 = 1$. If $e = 1$ and q is odd, then $d = (2, q-1) = 2$. So, $d^3e^2 = 8$, but $\mathcal{N}$ is at least $3^{1(1+1)/2}(3^2-1) = 27$ which is greater than 8. For $A_1(4)$, $d = 1$, $e = 2$, so $d^3e^2 = 4$ where $\mathcal{N} = 60 \geq 4$. For $A_1(9)$, $d = 2$, $e = 3$, so $d^3e^2 = 72$ where $\mathcal{N} = 720 \geq 72$.

- For $X = A_n(q)$ where $n \geq 2$, if d divides $q-1$ and $e = 1$ except for $X = A_2(2), A_2(4)$ and $A_3(2)$. Now if $e = 1$, then $d^3e^2 = d^3 \leq (q-1)^3$. Now since $n \geq 2$, $(q^2-1)(q^3-1)$ divides $\mathcal{N}$, but clearly $(q-1)^3 \leq (q^2-1)(q^3-1)$, so the inequality holds.
  For $X = A_2(2)$, $\mathcal{N} = 360$, $d = 1$, $e = 2$, so $d^3e^2 = 4 < \mathcal{N}$.
  For $X = A_2(4)$,$\mathcal{N} = 244800$,$d = 3$,$e = 16$ so $d^3e^2 = 6912 < \mathcal{N}$.
  For $X = A_3(2)$, $\mathcal{N} = 181440$, $d = 1$, $e = 2$ so $d^3e^2 = 4 < \mathcal{N}$.
  Therefore the inequality holds for $X = A_n(q)$.

- For $X = {}^2A_n(q)$, $n \geq 2$, we need to investigate the cases where $n = 2$ and $n > 2$ seperately. If $n = 2$, then d divides 3. In this case, we know that $e = 1$, $d^3e^2 \leq 27$. But the smallest value for $\mathcal{N}$ is $2^3.(2^2-1)(2^4-1) = 360$, that is, the inequality holds.

Now, if $n > 2$, then d divides $q+1$. If $e = 1$, then $d^3e^2 \leq (q+1)^3$. But by Table 2.3, $\mathcal{N}$ is divisible by $q^6(q^2-1)(q^3+1)(q^4-1)$, and clearly $(q+1)^3$ divides this product. Therefore, $\mathcal{N} \geq d^3e^2$ holds. The cases where $e \neq 1$ are $X = {}^2A_3(2)$, ${}^2A_3(3)$ and ${}^2A_5(2)$.
For $X = {}^2A_3(2)$, $d = (4,3) = 1$, $e = 2$, so $d^3e^2 = 4$, which is strictly less than $\mathcal{N}$ which is divisible by 2^6.
For $X = {}^2A_3(3)$, $d = (4,4) = 4$, $e = 3^2$, so $d^3e^2 = 5184$. In this case $\mathcal{N} = 3^6.(3^2-1).(3^3+1).(3^4-1) = 13063680 > d^3e^2 = 5184$.
For $X = {}^2A_5(2)$, $d = (6,3) = 3$, $e = 2^2$, so $d^3e^2 = 432$, so, it is strictly less than $\mathcal{N}$ which is divisible by 2^{15}.

- For $X = B_2(q)$, d divides 2, and e is at most 2. Then $d^3e^2 \leq 32$. But $\mathcal{N} = q^2.(q^2-1).(q^4-1)$, so $\mathcal{N}$ is at least $4.3.15 = 120$, therefore $\mathcal{N} > d^3e^2$.

- For $X = {}^2B_n(q)$ where $q = 2^f$ and f odd, d divides 2, and e is trivial except $X =^2 B_n(q)$. Now, if $X \neq^2 B_n(q)$, then $d = e = 1$, so the result is trivial. If $X =^2 B_n(q)$ then $\mathcal{N} = 29120$ and $d^3e^2 = 16$ so the inequality holds.

- For $X = B_n(q)$ where $n \geq 3$, d divides 2, and e is at most 3. Then $d^3e^2 \leq 108$. But q^{n^2} divides $\mathcal{N}$, but since $n \geq 3$ and q is at least 2, this implies $\mathcal{N} \geq 2^9 = 512 > 108$.

- For $X = C_n(q)$ where $n \geq 3$, d divides 2, and e is at most 2. Then $d^3e^2 \leq 32$. But q^{n^2} divides $\mathcal{N}$, but since $n \geq 3$ and q is at least 2, this implies $\mathcal{N} \geq 2^9 > 32$.

- For $X = D_4(q)$, d divides 4, and $e = 4$. Then $d^3e^2 \leq 2^{10}$. But q^{12} divides $\mathcal{N}$, but since q is at least 2, this implies $\mathcal{N} \geq 2^{12} > 2^{10}$.

- For $X = {}^2D_n(q)$ where $n \geq 4$, d divides 4, and e is trivial. Then $d^3e^2 \leq 64$. But $q^{n(n-1)}$ divides $\mathcal{N}$, but since $n > 4$ and q is at least 2, this implies $\mathcal{N} \geq 2^{4.3} = 2^{12} > 64$.

- For $X = D_n(q)$ where $n \geq 4$ and odd, d divides 4, and e is trivial. Then $d^3e^2 \leq 64$. But $q^{n(n-1)}$ divides $\mathcal{N}$, but since $n > 4$ and q is at least 2, this implies $\mathcal{N} \geq 2^{5.4} = 2^{20} > 64$.

- For $X = D_n(q)$ where $n \geq 4$ and even, d divides 4, and e is trivial. Then $d^3e^2 \leq 64$. But $q^{n(n-1)}$ divides $\mathcal{N}$, but since $n > 4$ and q is at least 2, this implies $\mathcal{N} \geq 2^{4.3} = 2^{12} > 64$.

- For $X = G_2(q)$, d is always 1, and e is at most 3. Then $d^3e^2 \leq 9$. But q^6 divides $\mathcal{N}$, which clearly implies $\mathcal{N} \geq 4$ for all $q > 1$.

- For $X = F_4(q)$, d is always 1, and e is at most 2. Then $d^3e^2 \leq 4$. But q^{24} divides $\mathcal{N}$, which clearly implies $\mathcal{N} \geq 4$ for all $q > 1$.

- For $X = E_6(q)$, d is at most 3, and e is always trivial. Then $d^3e^2 \leq 9$. However q^{36} divides $\mathcal{N}$, which clearly implies $\mathcal{N} \geq 9$ for all $q > 1$.

- For $X =^2 E_6(q)$, d is at most 3, and e is at most 4. Then $d^3e^2 \leq 108$. However q^{36} divides $\mathcal{N}$, which clearly implies $\mathcal{N} \geq 108$ for all $q > 1$.

- For $X = E_7(q)$, d is at most 2, and e is always trivial. Then $d^3e^2 = 8$ where q^{63} divides $\mathcal{N}$, which clearly implies $\mathcal{N} \geq 8$ for all $q > 1$.

- For $X = {}^3D_n(q), {}^2G_2(q), {}^2F_4(q), E_8(q)$, d and e are equal to 1, so the Schur multiplier is 1, that is $|M(X)|^2 \leq |X|$ is trivially satisfied.

We use Table 2.4 to verify $|M(X)|^2 \leq |X|$ for every sporadic group X. In this case we see that among all sporadic groups, the one with largest Schur multiplier is the Mathieu group M_{22}. We have $|M(M_{22})| = 12$. We can see from Table 2.4 that order of all sporadic groups are divisible by

$2^3.3.5.7 = 840$ or $2^3.3.5.11 = 1080$. Since $|M(M_{22})|^2 = 144$ is smaller than even these numbers, we can conclude that our inequality $|M(X)|^2 \leq |X|$ holds for all sporadic groups.

Now, since for every non-abelian finite simple group we have $|M(X)|^2 \leq |X|$, we have

$$|Z(Q)|^2 \leq |M(X)|^2 \leq |X| = \frac{|Q|}{|Z(Q)|}.$$

Then the inequality $|Q| \geq |Z(Q)|^3$ holds.

□

Theorem 4.2.2. *Let $\mathbb{F}$ be a finite field of characteristic p, say $GF(p^n)$. Then $Aut(\mathbb{F}) \cong \mathbb{Z}_n$.*

Proof. Let $\theta \in Aut(\mathbb{F})$. Then $\theta(0) = 0, \theta(1) = 1, \ldots, \theta(k) = k\theta(1) = k$ when $k \in GF(p)$. Therefore, every element in $GF(p)$ is fixed by θ. Since $x^p = x$ has at most p disinct roots, the fixed field of $Aut(\mathbb{F})$ is exactly $GF(p)$, that is $Aut(\mathbb{F}) = Aut_{GF(p)}(\mathbb{F})$. Consider

$$\begin{aligned} \alpha : GF(p^n) &\longrightarrow GF(p^n) \\ x &\longmapsto x^p. \end{aligned}$$

Now, $\alpha(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p = \alpha(x) + \alpha(y)$ since $char(\mathbb{F}) = p$ and $\alpha(xy) = (xy)^p = x^p y^p = \alpha(x)\alpha(y)$. Therefore, α is a ring homomorphism. Now, $ker(\alpha) = \{x \in \mathbb{F} : x^p = 0\} = \{0\}$. So, α is one-to-one. Then $|Im(\alpha)| \geq |GF(p^n)| = p^n$, that is α is onto. Hence α is an automorphism of $\mathbb{F}$. Now, $\alpha^k \in Aut(GF(p^n))$ for all k and since $\alpha^n(x) = x^{p^n} = x$ for all $x \in \mathbb{F}$, α^n is identity. Since $\mathbb{F} = GF(p^n)$ is a Galois extension of $GF(p)$ of degree n, we have $|Aut_{GF(p)}(\mathbb{F})| = [\mathbb{F} : GF(p)] = n$. But $Aut_{GF(p)}(\mathbb{F})$ has an element α of order n, hence $Aut(\mathbb{F}) = Aut_{GF(p)}(\mathbb{F})$ is generated by α (which is called the Fröbenius automorphism) and isomorphic to the cyclic group of order n. □

The following lemma is a consequence of (a) and (c) of Proposition 4.9.1 in [14]. Let $K = {}^d\Sigma(q)$ be a universal Lie type group defined on a finite field $\mathbb{F}$ of order $q = p^n$ for some prime p with the root system Σ. Let x be a field automorphism of K. Since x is an element of $Aut(\mathbb{F})$ which is isomorphic to $\mathbb{Z}_n$ by Theorem 4.2.2, $|x|$ divides n. Therefore, if $|x| = r$, then $q^{1/r} = p^{n/r} \in \mathbb{N}$, which will make the notation in Lemma 4.2.3 meaningful.

Lemma 4.2.3. *Let $K =^d \Sigma(q)$ be a universal Lie type group and x be a field automorphism of prime order r. Set $K_x = O^{r'}(C_K(x))$. Then the following hold:*

1. *K_x is isomorphic to ${}^d\Sigma(q^{1/r})$.*

2. *$C_K(x) = K_x$ and K_x is universal.*

Proof. See [14], Proposition 4.9.1. □

Theorem 4.2.4. *If $\delta : L \longrightarrow K$ is a universal covering of the quasi-simple group K with kernel Z. Then any automorphism α of K lifts via δ to a unique automorphism β of L and β stabilizes Z.*

Proof. See Corollary 5.1.4 in [14]. □

The following result of number theory will be useful in the proof of Theorem 4.2.12.

Lemma 4.2.5. *If q is not divisible by 3, then $q^2 - 1$ is divisible by 3.*

Proof. If q is not divisible by 3, then $q \equiv 1 \ (mod\, 3)$ or $q \equiv 2 \ (mod\, 3)$. Then, for both of these cases, $q^2 \equiv 1 \ (mod\, 3)$, hence $q^2 - 1 \equiv 0 \ (mod\, 3)$, which we needed to show. □

The following observation is an application of Lemma 4.2.5.

Remark 4.2.6. By Table 2.2, we can see that for every universal Lie type group G except ${}^2B_2(q^3)$ where $q = 2^{2m+1}$, order of G which is denoted by $\mathcal{N}$ is either divisible by $q^2 - 1$ or q is a multiple of 3. So, in these cases, $\mathcal{N}$ is divisible by 3 by Lemma 4.2.5.

Now, ${}^2B_2(q^3)$ has order $q^2(q^2+1)(q-1)$. Since $q = 2^{2m+1}$, it is easy to show that $q \equiv 2 \ (mod\, 3)$. Therefore, $\mathcal{N} = q^2(q^2+1)(q-1)$ is not divisible by 3.

Hence, we can conclude that the only Chevalley group whose order is not divisible by 3 is ${}^2B_2(q^3)$ where $q = 2^{2m+1}$.

By Lemma 4.2.3 we know that when G is a universal Lie type group and α is a coprime automorphism of G of prime order, both G and $C_G(\alpha)$ are finite groups of Lie type of the same type. We will use Table 2.3 to compare the orders of G and $C_G(\alpha)$. Now we will define the **cyclotomic polynomials** which will be a useful tool in this comparison.

Definition 4.2.7. *If ξ is an n-th root of unity such that n is the smallest positive integer for which $\xi^n = 1$, we say that ξ is a* ***primitive* n*-th root of unity*.**

Example 4.2.8. The complex number $i = \sqrt{-1}$ is an 8-th root of unity but it is not a primitive 8-th root of unity since $i^4 = 1$. However, i is a primitive 4-th root of unity.

Definition 4.2.9. *If d is a positive integer, then the* **d*-th cyclotomic polynomial*** *Φ_d is defined by*

$$\Phi_d = \prod_{i=1}^{r}(x - \xi_i)$$

where $\xi_1, \xi_2, \ldots \xi_r$ are all the distinct primitive d-th roots of unity.

By the following result, we will have an easy way to compute the cyclotomic polynomials.

Lemma 4.2.10. *For every integer $n \geq 1$*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Proof. See [19], Proposition 8.2. $\square$

Example 4.2.11. Since the only primitive first root of of unity is 1, we have $\Phi_1(x) = x - 1$.
$\Phi_2(x) = x - (-1) = x + 1$ since the only primitive second root of unity is -1.

Let p be any prime. By Lemma 4.2.10 we know that

$$x^p - 1 = \prod_{d|p} \Phi_d(x).$$

Now, since p is prime, the only divisors of p are itself and 1, so we have $x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x)$. Therefore,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = 1 + x + \ldots + x^{p-1}$$

for every prime p.

Theorem 4.2.12. *Let G be a universal Lie type group and α be an automorphism of G of prime order r where r does not divide the order of G. Then $|G : C_G(\alpha)| > |C_G(\alpha)|^2$.*

Proof. Let G be a universal Lie type group ${}^d\Sigma(q^r)$ for some root system Σ and for some prime power q. Since r does not divide order of G, by Table 2.2, α is a field automorphism. By Lemma 4.2.3, $G_\alpha = O^{r'}(C_G(\alpha)) = C_G(\alpha)$ since r does not divide the order of G and $C_G(\alpha)$ is isomorphic to ${}^d\Sigma(q)$. Therefore, both G and $C_G(\alpha)$ are finite groups of Lie type of the same type.

Now, by Table 2.3 and Table 4.1, we can see that if G is a universal Lie type group with root system Σ and N is the number of positive roots in Σ,

Table 4.1: The number of positive roots of the simple Chevalley groups

G	N- the number of positive roots in Σ
$A_n(q), n \geq 1$	$n(n+1)/2$
$B_n(q), n \geq 2$	n^2
$C_n(q), n \geq 3$	n^2
$D_n(q), n \geq 4$	$n(n-1)$
$G_2(q)$	6
$F_4(q)$	24
$E_6(q)$	36
$E_7(q)$	63
$E_8(q)$	120

then $\mathcal{N} = q^N . \prod_{i=1}^m f_i(q)$ where $f_i(q)$ are polynomials of the form $q^{k_i}-1, q^{k_i}+1$ or $q^{2k_i} + q^{k_i} + 1$ for some positive integer k_i. The same result is obtained for the twisted Chevalley groups in Theorem 14.3.1 in [7] with $f_i(q) = q^{k_i} - 1$ or $q^{k_i} + 1$. Since we can write $q^k - 1 = \Phi_1(q^k)$, $q^k + 1 = \Phi_2(q^k)$ and $q^{2k}+q^k+1 = \Phi_3(q^k)$, it is enough to use the first three cyclotomic polynomials to write the orders of universal Chevalley groups as a product of cyclotomic polynomials and powers of q.

Therefore, we have

$$|G : C_G(\alpha)| = \frac{q^{rN} \prod_{i=1}^m \Phi_{l_i}(q^{rd_i})}{q^N \prod_{i=1}^m \Phi_{l_i}(q^{d_i})}$$

where N is the number of positive roots in Σ, $l_i \in \{1, 2, 3\}$, Φ_{l_i} is the l_i-th cyclotomic polynomial and d_i are positive integers.

First, we need a simple inequality:

Claim: $t^{13/8} > t + 1$ if $t \geq 2$.

Consider $f(t) = t^{13/8} - t - 1$. Now $f(2) > 0$. Since $f'(t) = \frac{13}{8}t^{\frac{5}{8}} - 1 > 0$,

f is increasing, so the inequality holds for all $t \geq 2$.

Now, if $t \geq 2$, then the following holds:

$$\Phi_1(t^r) = t^r - 1 > (t-1)^{r-1} = (\Phi_1(t))^{r-1}$$
$$\Phi_2(t^r) = t^r + 1 > t^r = (t^{13/8})^{8r/13} > (t+1)^{8r/13} = (\Phi_2(t))^{8r/13}.$$
$$\Phi_3(t^r) = t^{2r} + t^r + 1 > t^{2r} = (t^3)^{\frac{2r}{3}} > (t^2+t+1)^{\frac{2r}{3}} = (\Phi_3(t))^{2r/3}.$$

Now, since r is coprime with $|G|$ which is even, r is necessarily an odd prime, hence $r \geq 3$. For $l \in \{1,2,3\}$, for all $t \geq 2$ and $r \geq 3$, we proved that $\Phi_l(t^r) > (\Phi_l(t))^{\frac{8r}{13}}$. Then, whenever $r \geq 5$ we have;

$$\begin{aligned}
|G : C_G(\alpha)| &= \frac{q^{rN} \prod_{i=1}^m \Phi_{l_i}(q^{rd_i})}{q^N \prod_{i=1}^m \Phi_{l_i}(q^{d_i})} \\
&> q^{(r-1)N} \prod_{i=1}^m (\Phi_{l_i}(q^{d_i}))^{(\frac{8r}{13})-1} \text{ since } \Phi_l(t^r) > (\Phi_l(t))^{\frac{8r}{13}} \text{ holds,} \\
&> q^{(r-1)N} \prod_{i=1}^m (\Phi_{l_i}(q^{d_i}))^{(\frac{8.5}{13})-1} \text{ since } r \geq 5, \\
&> q^{(r-1)N} \prod_{i=1}^m (\Phi_{l_i}(q^{d_i}))^{(\frac{27}{13})} \\
&> q^{2N} \prod_{i=1}^m (\Phi_{l_i}(q^{d_i}))^2 = |C_G(\alpha)|^2,
\end{aligned}$$

since we have $r-1 > 2$ and $\frac{27}{13} > 2$. Hence, the inequality holds when $r \geq 5$. Since r is necessarily greater than 2, we have only to show that the inequality holds when $r = 3$. But since r must be coprime with $|G|$, we need to consider the cases where G is a universal Lie type group whose order is not divisible by 3. By Remark 4.2.6, we know ${}^2B_2(q^3)$ is the only universal Chevalley group whose order is not divisible by 3. Therefore, when $r = 3$, G is necessarily isomorphic to ${}^2B_2(q^3)$. In this case, $C_G(\alpha) \cong {}^2B_2(q)$ by Lemma 4.2.3, so

$$\begin{aligned}
|G : C_G(\alpha)| =& \frac{q^6(q^6+1)(q^3-1)}{q^2(q^2+1)(q-1)} \\
=& q^4(q^4 - q^2 + 1)(q^2 + q + 1).
\end{aligned}$$

Now, since $|C_G(\alpha)|^2 = q^4(q^2+1)^2(q-1)^2$, to show the inequality we need to verify that

$$q^4(q^4 - q^2 + 1)(q^2 + q + 1) > q^4(q^2 + 1)^2(q - 1)^2.$$

Since $q^4 > 0$, it is enough to show that $(q^4-q^2+1)(q^2+q+1) > (q^2+1)^2(q-1)^2$. Define $h(x) = (x^4 - x^2 + 1)(x^2 + x + 1) - (x^2 + 1)^2(x - 1)^2$. Now $h(x) = 3x^5 - 3x^4 + 3x^3 - 3x^2 + 3x = 3x^4(x-1) + 3x^2(x-1) + 3x$. So, $h(x) > 0$ for all $x > 1$. Therefore, since $h(q) > 0$ the inequality $(q^4-q^2+1)(q^2+q+1) > (q^2+1)^2(q-1)^2$ holds for all $q \geq 2$. Hence, it is shown that $|G : C_G(\alpha)| > |C_G(\alpha)|^2$ holds when α has order 3, which completes the proof.

□

4.3 Main theorem

Theorem 4.3.1. *Let Q be a quasi-simple group and let A be a non-trivial group of automorphisms of Q such that the orders of Q and A are coprime. If $|Q : C_Q(A)| = n$, then $|Q| < n^3$.*

Proof. We need to show that A acts on $Q/Z(Q)$ non-trivially. Assume the action is trivial. Then

$$\begin{aligned} &[Q, A] \leq Z(Q) \\ \Rightarrow &[Q, A, Q] = 1 \text{ and} [A, Q, Q] = 1 \\ \Rightarrow &[Q, Q, A] = 1 \text{ by Three Subgroup Lemma} \\ \Rightarrow &[Q, A] = 1 \text{ since } Q' = Q \end{aligned}$$

which is not the case.

Hence A acts on $Q/Z(Q)$ non-trivially. Now, since $|A|$ and $|Q|$ are coprime, A necessarily consists of outer automorphisms. By Table 2.4 we know that the outer automorphism group of a sporadic group has order

1 or 2. Consider the alternating groups A_n where $n \geq 5$. By (3.2.17) in [28], we know that $Aut(A_n) = S_n$ except for $n \neq 6$. Since $Z(A_n) = 1$, and $Inn(A_n) = A_n/Z(A_n) = A_n$, $Out(A_n) = Aut(A_n)/Inn(A_n)$ is isomorphic to Z_2 for $n \neq 6$. If $n = 6$, by (3.2.19) of [28], $|Aut(A_6)/Inn(A_6)| = 2^2$. Therefore the outer automorphism group of an alternating or a sporadic group is a 2-group. But since order of every non-abelian simple group is necessarily even and $(|A|, |Q|)$ holds, we have $A = 1$, which is not the case. Therefore $Q/Z(Q)$ is a simple group of Lie type.

Let α be a non-trivial element of A of prime order r. Recall that the Schur multiplier of a simple group of Lie type is the direct product of groups of orders d (diagonal or canonical part of the Schur multiplier) and e (exceptional multiplier). The diagonal multiplier extends the adjoint group to the corresponding universal Chevalley group. The exceptional multiplier is always a p-group, and is trivial except in finitely many cases. We have to consider the cases where the exceptional part of the Schur multiplier of Q is trivial and non-trivial seperately.

First consider the cases where the exceptional part of the Schur multiplier of $Q/Z(Q)$ is non-trivial. There are 18 cases which are shown in Table 2.2. Since order of every non-abelian simple group is necessarily even, and $(|A|, |Q|) = 1$, we can omit the cases where $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $A_1(4)$, then according to Table 2.2 $e = 2$, $p = 2$, $f = 2$, $q = 4$, $d = (2, q-1) = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 2$, hence $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $A_1(9)$, then $e = 3$, $p = 3$, $f = 2$, $q = 9$, $d = (2, q-1) = (2, 8) = 2$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 4$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $A_2(2)$, then $e = 2$, $p = 2$, $q = 2$, $f = 1$, $n =$

2 $d = (n+1, q-1) = (2,1) = 1$, and $g = 2$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 2$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $A_2(4)$, then $e = 4^2$, $p = 2$, $q = 4$, $f = 2$, $n = 2$ $d = (n+1, q-1) = (2,3) = 1$, and $g = 2$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 4$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $A_3(2)$, then $e = 2$, $p = 2$, $f = 1$, $q = 2$, $n = 2$ $d = (n+1, q-1) = (2,1) = 1$, and $g = 2$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 4$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to ${}^2A_3(2)$, then $e = 2$, $p = 2$, $q = 2$, $p^f = q^2 = 4$, so $f = 2$, $n = 3$, $d = (n+1, q+1) = (4,3) = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 4$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to ${}^2A_3(3)$, then $e = 3^2$, $q = 3$, $p = 2$, $p^f = q^2 = 9$, so $f = 2$, $n = 3$, $d = (n+1, q+1) = (4,4) = 4$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 8$, that is, $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to ${}^2A_5(2)$, then $e = 2^2$, $p = 2$, $q = 2$, $p^f = q^2 = 4$, so $f = 2$, $n = 5$, $d = (n+1, q+1) = (6,3) = 3$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 6$. Therefore, A divides 6. By Table 2.3, we know that $|{}^2A_5(2)|$ is divisible by both 2 and 3, so $(|A|, |{}^2A_5(2)|) = 1$ implies $A = 1$ which is not the case.

- If $Q/Z(Q)$ is isomorphic to $B_2(2)$, then $e = 2$, $p = 2$, $q = 2$, $q = p^f$, so $f = 1$, $n = 2$, $d = (2, q-1) = (2,1) = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 1$. That means A is trivial, which is impossible.

- If $Q/Z(Q)$ is isomorphic to $B_3(2)$, then $e = 2$, $p = 2$, $q = 2$, $q = p^f$, so $f = 1$, $n = 3$, $d = (2, q-1) = (2,1) = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 1$, that is, A is necessarily trivial which is not the case.

- If $Q/Z(Q)$ is isomorphic to $B_3(3)$, then $e = 3$, $p = 3$, $q = 3$, $q = p^f$, so $f = 1$, $n = 3$, $d = (2, q-1) = (2,2) = 2$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 2$, so $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $C_3(2)$, then $e = 2$, $p = 2$, $q = 2$, $q = p^f$, so $f = 1$, $n = 3$, $d = (2, q-1) = (2,1) = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 1$, so A is necessarily trivial which is not the case.

- If $Q/Z(Q)$ is isomorphic to $D_4(2)$, then $e = 2^2$, $p = 2$, $q = 2$, $q = p^f$, so $f = 1$, $n = 4$, $d = (4, q^n + 1) = (4, 17) = 1$, and $g = 6$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 6$. Then $|A|$ divides 6. Now, since $|D_4(2)| = 2^{12}.15.3.15.63$ is divisible by 6, if $(|A|, |Q/Z(Q)|) = 1$ then A must be trivial which is not the case.

- If $Q/Z(Q)$ is isomorphic to $G_2(3)$, then $e = 3$, $p = 3$, $q = 3$, $q = p^f$, so $f = 1$, $n = 2$, $d = 1$, and $g = 2$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 2$, so $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $G_2(4)$, then $e = 2$, $p = 2$, $q = 4$, $q = p^f$, so $f = 2$, $n = 2$, $d = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 2$, so $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to $F_2(4)$, then $e = 2$, $p = 2$, $q = 4$, $q = p^f$, so $f = 2$, $n = 2$, $d = 1$, and $g = 2$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 4$, so $Out(Q/Z(Q))$ is a 2-group.

- If $Q/Z(Q)$ is isomorphic to ${}^2E_6(2)$, then $e = 2^2$, $p = 2$, $q = 2$, $q = p^f$, so $f = 1$, $n = 6$, $d = (3,3) = 3$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 3$. Then A divides 3. Since $|{}^2E_6(2)| = 2^{36}.(2^{12}-1)(2^9+1)(2^8-1)(2^6-1)(2^5+1)(2^2-1)$ is divisible by 3, if $(|A|, |Q/Z(Q)|) = 1$, A is necessarily trivial which is not the case.

- If $Q/Z(Q)$ is isomorphic to ${}^2B_2(8)$, then $e = 2^2$, $p = 2$, $q = 8$, $q = 2^f$, so $f = 3$, $n = 2$, $d = 1$, and $g = 1$. So the outer automorphism group of $Q/Z(Q)$ has order $dfg = 3$. Since $|{}^2B_2(8)| = 64.65.7$ is not divisible by 3, for any subgroup A of the outer automorphism group, $(|A|, |Q/Z(Q)|) = 1$. Therefore, $Q/Z(Q)$ is necessarily isomorphic to ${}^2B_2(8)$.

This analysis demonstrates that if the exceptional part of the Schur multiplier of $Q/Z(Q)$ is non-trivial, then necessarily $Q/Z(Q)$ is isomorphic to ${}^2B_2(8)$. By Table 2.2, observe that $|{}^2B_2(8)|$ has order $64.65.7 = 29120$ and Schur multiplier of ${}^2B_2(8)$ has order 4. Since $Q/Z(Q)$ is isomorphic to ${}^2B_2(8)$, (Q, π) is a central extension of ${}^2B_2(8)$ where $\pi : Q \longrightarrow Q/Z(Q)$, the canonical homomorphism . By Theorem 14.4.1 in [7], ${}^2B_2(8)$ is simple. Hence, it is necessarily perfect, so by Theorem 2.5.11, the universal central extension $(\tilde{G}, \sigma)$ of ${}^2B_2(8)$ exists. Then there exists a unique morphism of central extensions $\lambda : (\tilde{G}, \sigma) \longrightarrow (Q, \pi)$. Therefore, $\lambda : \tilde{G} \longrightarrow Q$ is an epimorphism with $\sigma = \lambda\pi$. Since $ker(\pi) = Z(Q) \leq ker(\sigma)$ which has order 4, we conclude $|Z(Q)| \leq 4$. By Lemma 4.2.3, $C_{Q/Z(Q)}(\alpha)$ is isomorphic to ${}^2B_2(2)$ which has order 20. Now, since $|Q/Z(Q) : C_{Q/Z}(\alpha)| \leq |Q/Z(Q) : C_{Q/Z}(A)|$, if $|Q/Z(Q) : C_{Q/Z}(A)| \leq n$, then $n > 29120/20 = 1456$. Since $n^3 > 3086626816$, and $|Q| = 116480$, the required inequality holds.

Now we may assume that the exceptional part of the Schur multiplier of Q is trivial. By [9, page xv], the diagonal multiplier extends the adjoint type group to the corresponding universal type group. So Q is a quotient of the universal Lie type group of the same type. Let G be the universal Lie type group such that Q is the quotient of G by a central subgroup Z, that is $Q \cong G/Z$. By Lemma 4.2.4, α extends to an automorphism of G which has coprime order to G and stabilizes Z. Since $(|\alpha|, |G|) = 1$ and Z is an α-invariant normal subgroup of G, by Lemma 1.7.7 in [10], we have $C_Q(\alpha) = C_{G/Z}(\alpha) \cong C_G(\alpha)Z/Z$. Since $C_Q(A) \leq C_Q(\alpha)$, we have $|Q : C_Q(\alpha)| \leq |Q : C_Q(A)| \leq n$. Now,

$$\begin{aligned} n \geq |Q : C_Q(\alpha)| =& |G/Z : C_{G/Z}(\alpha)| \\ =& |G/Z : C_G(\alpha)Z/Z| \\ =& |G : C_G(\alpha)Z| \end{aligned}$$

We have $|C_G(\alpha)Z : C_G(\alpha)| \leq |Z|$. Since Z is a central subgroup of G, $|Z| \leq |Z(G)|$. Since G is a universal Lie type group, it is the universal covering group of a simple group of Lie type, that is, G is quasi-simple. So, by Theorem 4.2.1, $|Z|^3 \leq |Z(G)|^3 \leq |G|$. Then $|C_G(\alpha)Z : C_G(\alpha)| \leq |Z| \leq |G|^{1/3}$. Since G is a universal Lie type group and α is a coprime automorphism, by Theorem 4.2.12, we have $|C_G(\alpha)|^2 \leq |G : C_G(\alpha)|$. Now,

$$|C_G(\alpha)|^2 \leq |G : C_G(\alpha)| = |G : C_G(\alpha)Z||C_G(\alpha)Z : C_G(\alpha)| \leq n|Z| \leq n|G|^{1/3}.$$

So, we have

$$|C_G(\alpha)| \leq n^{1/2}|G|^{1/6}.$$

Therefore $|G| = |G : C_G(\alpha)||C_G(\alpha)| \leq n^{3/2}|G|^{1/2}$, which implies $|G| \leq n^3$. Since Q is a quotient of G, $|Q| \leq n^3$.

□

REFERENCES

[1] Aschbacher, M. *Finite Group Theory* Cambridge Studies in Advanced Mathematics Vol.10 Cambridge University Press, Cambridge, UK, 1986.

[2] Belyaev, V.V. *"Minimal non-FC-groups"* in Abstracts: Sixth All Union Symposium on Group Theory (Cherkassy,1978).

[3] Belyaev, V.V. *"Groups of the Miller-Moreno type"* Sibirsk Math. Zh.,**19** No.3, 509-514 (1978).

[4] Belyaev, V.V. *"On the question of existence of minimal non-FC-groups"* Sibirsk Math. Zh. **39**, No.6,1093-1095 (1998).

[5] Belyaev, V.V., Sesekin, M.F. *"On infinite groups of Miller-Moreno type"* Acta. Math. Acad. Sci. Hung (1975) **26** 3-4 369-376

[6] Brauer, R., *"On the structure of groups of finite order"* Proc. Internat. Congr. Math, vol:1, North-Holland, Amsterdam, 1954, 209-217.

[7] Carter, R.W, *Simple Groups of Lie Type* John Wiley & Sons 1972

[8] Carter, R.W, *Finite Groups of Lie Type-Conjugacy Classes and Complex Characters* John Wiley & Sons 1993

[9] Conway, J.H., Curtis, T., Parker, R.A., Wilson *Atlas of Finite Groups*, Oxford University Press, Oxford 1985.

[10] Dixon, M.R., *Sylow Theory, Formations and Fitting Classes in Locally Finite Groups* World Scientific Publishing Co. Pte. Ltd. 1994.

[11] Giovanni, F.D., Newell, M.L., *"Infinite Groups 1994"*, Proceedings of the Ravello Conference, Italy, 1994.

[12] Gorenstein, D., Lyons, R., Solomon, R., *Classification of finite simple groups* Volume I, AMS Volume 40. 1994.

[13] Gorenstein, D., Lyons, R., Solomon, R., *Classification of finite simple groups* Volume II, AMS Volume 40. 1995.

[14] Gorenstein, D., Lyons, R., Solomon, R., *Classification of finite simple groups* Volume III, AMS Volume 40. 1998.

[15] Gorenstein, D., Lyons, R., Solomon, R., *Classification of finite simple groups* Volume IV, AMS Volume 40. 1999.

[16] Hartley, B., Isaacs, I.M., *"On characters and fixed points of coprime operator groups"*, J. Algebra **131**, 342-358 (1990).

[17] Hartley, B., Otal, J., Pena, J.M. *"Locally graded minimal non-CC-groups"* Arch. Math., **57** No.3. 209-211 (1991)

[18] Higman, G., *Groups and rings having automorphisms without non-trivial fixed elements*, J. London Math. Soc. **32** (1957), 321-334.

[19] Hungerford, T., *Algebra*, Holt,Rinehart and Winston Inc., 1974.

[20] Isaacs, I.M., Navarro, G. *"Coprime actions, fixed-point subgroups and irreducible induced characters"*, Journal of Algebra, **185** (1996), 125-143.

[21] Kegel, O.H., Wehrfritz, B. *Locally finite groups*, North-Holland Publishing Company, 1973.

[22] Kuzucuoğlu, M. and Phillips, R.E. *"Locally finite minimal non-FC-groups"*Math. Proc. Camb. Philos. Soc.,**105**, No.3, 417-420 (1989).

[23] Leinen, F. and Puglisi, O. *"Unipotent finitary linear groups"* J.London Math. Soc.,**48**, No.1,59-76(1993).

[24] Leinen, Felix *"A reduction theorem for perfect locally finite minimal non-FC-groups"*, Glasgow Math. J., **41** 1999, No: 1. 81-83.

[25] Parker, C., Quick, M. *"Coprime Automorphisms and their commutators"*, J. Algebra, **244**, 260-272 (2001)

[26] Robinson, D. *A course in theory of groups* Springer (1991) Second edition.

[27] Shunkov V.P. *"On the minimality problem for locally finite groups"*, Algebra i Lojika., **9** (1970), 220-248

[28] Suzuki, M.,*Group Theory I*, Springer-Verlag, 1986.

[29] Suzuki, M.,*Group Theory II*, Springer-Verlag, 1986.

[30] Tomkinson, M.J., *FC-groups* Pitman Publishing Limited, London, 1984

[31] Thompson,J., *"Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat/ Acad/ Sci. USA **45** (1959) 578-581.

[32] Turull, A., *"Examples of centralizers of automorphism groups"*, Proc. Amer. Math. Soc, **91**, No:4 537-539, (1984).

[33] Turull, A., *"Groups of automorphisms and centralizers"*, Math. Proc. Camb. Phil. Soc, **107**, 227-238, (1990).

[34] Turull, A., *"Fitting heihts of groups and fixed points"*, J. Algebra, **86**, 555-566, (1986)