ON THE INDEX OF FIXED POINT SUBGROUP

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

BY

ERKAN MURAT TÜRKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

AUGUST 2011

Approval of the thesis:

ON THE INDEX OF FIXED POINT SUBGROUP

submitted by **ERKAN MURAT TÜRKAN** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Canan Özgen
Dean, Graduate School of **Natural and Applied Sciences** ________________

Prof. Dr. Zafer Nurlu
Head of Department, **Mathematics** ________________

Assoc. Prof. Dr. Gülin Ercan
Supervisor, **Department of Mathematics, METU** ________________

Examining Committee Members:

Prof. Dr. İsmail Güloğlu
Department of Mathematics, Doğuş University ________________

Assoc. Prof. Dr. Gülin Ercan
Department of Mathematics, METU ________________

Prof. Dr. Mahmut Kuzucuoğlu
Department of Mathematics, METU ________________

Assoc. Prof. Dr. Ali Erdoğan
Department of Mathematics, Hacettepe University ________________

Assoc. Prof. Dr. Semra (Öztürk) Kaptanoğlu
Department of Mathematics, METU ________________

Date: ________________

I hereby 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 by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ERKAN MURAT TÜRKAN

Signature :

ABSTRACT

ON THE INDEX OF FIXED POINT SUBGROUP

Türkan, Erkan Murat
Ph.D., Department of Mathematics
Supervisor : Assoc. Prof. Dr. Gülin Ercan

August 2011, 84 pages

Let G be a finite group and A be a subgroup of Aut(G). In this work, we studied the influence of the index of fixed point subgroup of A in G on the structure of G.

When A is cyclic, we proved the following:

(1) [G,A] is solvable if this index is squarefree and the orders of G and A are coprime.

(2) G is solvable if the index of the centralizer of each x in H-G is squarefree where H denotes the semidirect product of G by A.

Moreover, for an arbitrary subgroup A of Aut(G) whose order is coprime to the order of G, we showed that when G is solvable, then the Fitting length f([G,A]) of [G,A] is bounded above by the number of primes (counted with multiplicities) dividing the index of fixed point subgroup of A in G and this bound is best possible.

Keywords: automorphism, solvable group, Fitting length, fixed point subgroup

ÖZ

SABİT NOKTA ALTGRUBUNUN İNDEKSİ ÜZERİNE

Türkan, Erkan Murat
Doktora, Matematik Bölümü
Tez Yöneticisi : Doç. Dr. Gülin Ercan

Ağustos 2011, 84 sayfa

G sonlu bir grup ve A, Aut(G)'nin bir altgrubu olsun. Bu çalışmada A'nın G içindeki sabit nokta altgrubunun indeksinin G grubunun yapısı üzerindeki etkisi çalışılmış olup, A grubu devirli olduğunda şu sonuçlar elde edilmiştir:

(1) Bu indeks hiçbir tamkareye bölünmüyor ve G ile A'nın mertebeleri aralarında asal ise [G,A] altgrubu çözülebilirdir.

(2) H, G'nin A ile yarıdolaylı çarpımını temsil etsin. H'nin G'de olmayan her x elemanının merkezleyeninin G içindeki indeksi hiçbir tamkareye bölünmüyor ise, G grubu çözülebilirdir.

Bunun ötesinde A, Aut(G)'nin herhangibir altgrubu, G çözülebilir bir grup ve G ile A'nın mertebesi aralarında asal ise [G,A] altgrubunun Fitting uzunluğunun, A'nın G içindeki sabit nokta altrubunun indeksinin asal çarpan ayrışımındaki üstlerin toplamı ile üstten sınırlı olduğu ve bu sınırın olabilecek en küçük sınır olduğu gösterilmiştir.

Anahtar Kelimeler: otomorfizma, çözülebilir altgrup, Fitting uzunluğu, sabit nokta altgrubu

To my family and my friends

ACKNOWLEDGMENTS

This thesis would not have been possible without help, support, guidance and patience of my thesis supervisor Gülin Ercan through all stages. I owe my deepest gratitude to her.

I would like to acknowledge TÜBİTAK for the financial support during my one year abroad research fellow.

I would like to show my gratitude to Professor Alexandre Turull for his comments, guidance, support and helps during my research in Gainesville.

I would like to thank to Professor İsmail Ş. Güloğlu for his support, help and guidance.

It is a pleasure to thank to the commitee members Professor Mahmut Kuzucuoğlu and Professor Ali Erdoğan who made this thesis possible with their thoughts, guidance and patience during this long and stressful period.

There are a huge number of people and institutions I would like to mention here, but I will simply thank the groups.

To my professors and lecturers, for learning so much from you;

To the staff in the department, for being ever helpful, for always smiling and motivating;

To my friends, within and without the mathematics circle, for being such a joyous crowd;

It is honor for me to thank to the staff in the Mathematics canteen for their moral support and especially to Nuray Özkan for everything.

I would like to express my special thanks to my close friends, they know who they are, for always supporting me and for their moral support and for being my friend.

Above all, I am deeply indepted to my parents for their love, care and unconditional support during my study.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

SYMBOLS

LIST OF SYMBOLS

$\pi(G)$	the set of prime divisors of the order of G
$C_G(H) = \{g \in G \mid aga^{-1} = g \text{ for all } a \in H\}$	the centralizer of H in G
$[G : H] = \lvert\{gH \mid g \in G\}\rvert$	the index of H in G
$\mathrm{Aut}(G)$	the set of all automorphisms of G
$[G, H] = \left\langle g^{-1}h^{-1}gh \mid g \in G, h \in H \right\rangle$	the commutator subgroup of G and H
$G' = [G, G]$	the commutator subgroup of G
$x^G = \{g^{-1}xg \mid g \in G\}$	the conjugacy class of G containing x
$\mathrm{Irr}(G)$	the set of all irreducible characters of G
$\mathrm{Con}(G) = \{x^G \mid x \in G\}$	the set of all conjugacy classes of G
$F(G)$	Fitting subgroup, the largest nilpotent normal subgroup, of G
$f(G)$	the Fitting length of G
$O_p(G)$	maximal normal p-subgroup of G
$O^p(G)$	maximal normal subgroup of G with p-power index
$dl(G)$	derived length of G
$cl(G)$	nilpotency class of G
$Syl_p(G)$	the set of all Sylow $p-$subgroups of G
$S(G)$	the maximal normal solvable subgroup of G
$(a, b) = gcd(a, b)$	the greatest common divisor of a and b

CHAPTER 1

INTRODUCTION

Let G be a finite group and A a group of automorphisms of G. The structure of the fixed point subgroup $C_G(A) = \{ g \in G \mid g^a = g \text{ for all } a \in A \}$ of the action of A on G and the way it is embedded in G becomes very restrictive and therefore explanatory about the structure of G. Hence a well-established area in the theory of finite groups is the study of how information on $C_G(A)$ may influence the properties such as solvability or non-simplicity of G. However, in the literature there are only a few works which handle the influence of the index $|G : C_G(A)|$ of $C_G(A)$ in G. It should be noted that if one adds a direct factor to G on which A acts trivially, this process does not change the index of the fixed point subgroup. Hence rather than asking about the structure of G one should ask about the structure of the subgroup $\langle g^{-1}g^a \mid g \in G, \ a \in A \rangle$ which is denoted by $[G, A]$, in terms of $|G : C_G(A)|$. In this framework, the first result is due to Kazarin [6]. In 1990, he stated that

If $|G : C_G(\alpha)|$ is a prime power for a finite group G and $\alpha \in Aut(G)$, then $[G, \alpha]$ is solvable.

Another result in this direction was obtained by Parker and Quick [27] in 2001. They proved that

If $A \leq Aut(G)$ with $(|G|, |A|) = 1$, then the order of $[G, A]$ is bounded above by $n^{\log_2(n+1)}$ where the index $|G : C_G(A)| \leq n$.

It should be noted that Kazarin's work has a distinction of providing a result without the assumption that $(|G|, |\alpha|) = 1$. In this kind of research, the assumption that the action of A on G is coprime is very important because there exist certain very useful relations between the groups G and A which make some inductive arguments very easy to apply under a coprime action. If the action is noncoprime it becomes rather difficult to use this type of arguments and the situation changes dramatically. Here is a list of some useful relations which are valid under a coprime action:

(1) $G = [G, A]C_G(A)$;

(2) $[G, A] = [G, A, A]$;

(3) $C_{G/N}(A) = G_G(A)N/N$ for each normal A-invariant subgroup N of G.

Kazarin's result stated above is a corollary of his main theorem in [25] which generalizes Burnside's well-known lemma asserting that a finite group is not simple if the number of elements in a conjugacy class is equal to a power of a prime number. In fact he proved that

If for some $x \in G$, $|G : C_G(x)|$ is a power of a prime, then $\langle x^G \rangle$ is solvable.

This is of course a contribution to the study of the influence on the structure of G of some arithmetical conditions imposed on the lengths of conjugacy classes of G. By giving this corollary, Kazarin pointed out that the methods of studying the structure of $[G, \alpha]$ for $\alpha \in Aut(G)$ in terms of the index of $C_G(\alpha)$ might be very closely related to the methods in the investigation of the influence of the lengths of conjugacy classes to the structure of G. Realizing this, the following important results due to Cossey and Wang stimulated our interest and led us to the main questions of this thesis.

(Cossey-Wang, 1999 [10]) Let G be a finite group and p be a prime divisor of $|G|$ such that if q is any prime divisor of $|G|$, not dividing $p - 1$. Suppose that no conjugacy class length of G is divisible by p^2. Then G is a solvable $p-$nilpotent group and $G/O_p(G)$ has a Sylow $p-$subgroup of order at most p. Further, if $P \in Syl_p(G)$, $|P'| \leq p$ and if $P \neq O_p(G)$, then $O_p(G)$ is abelian.

(Cossey-Wang, 1999 [10]) Let G be a finite group and suppose that $|C|$ is a squarefree number for each $C \in Con(G)$. Then G is supersolvable and both $G/F(G)$ and G' are cyclic groups with squarefree orders. The class of $F(G)$ is at most 2 and G is metabelian.

In addition, we would like to mention the works [1], [4], [5], [6], [8], [22], [23], [24] et. al., on the influence of the sizes of conjugacy classes on the structure of a finite group which brought us to the following:

Question 1. *Let G be a finite group and $\alpha \in Aut(G)$. Is $[G, \alpha]$ solvable, when $|G : C_G(\alpha)|$ is a squarefree number?*

We obtained a counter-example showing that the answer to this question may be affirmative only in the case $(|G|, |\alpha|) = 1$. Then we studied Question 1 first under this additional hypothesis and obtained the following:

Theorem 2: *Let $\alpha \in Aut(G)$ with $(|G|, |\alpha|) = 1$. If the index $|G : C_G(\alpha)|$ is squarefree, then G is solvable.*

Considering the question that how the information about $C_G(A)$ influence the structure of G for a noncoprime action, it has been observed by Ercan and Güloğlu in [11], [12], [13], [14], [15] that the properties of elements in $GA \setminus G$ may also influence the structure of G where GA stands for the semidirect product of G by A. They imposed some conditions on these elements in order to overcome some of the difficulties arising from a noncoprime action. We modified Question 1 by imposing similar restrictions on the elements of $G\langle\alpha\rangle \setminus G$.

Question 2. *Let G be a finite group and $\alpha \in Aut(G)$. Is G solvable if $|G : C_G(\alpha)|$ is squarefree for each $x \in H \setminus G$ where H denotes the semidirect product of G by $\langle\alpha\rangle$?*

Although we first attempted to impose restrictions only on $x \in H \setminus G$ of order equal to $|\alpha|$, the same counter-example served as a counter-example in this case as well. Consequently, we showed that the answer to Question 2 is affirmative by proving the following:

Theorem 3: *Let G be a finite group and $\alpha \in Aut(G)$. Assume that $|G : C_G(x)|$ is squarefree for each $x \in H \setminus G$ where $H = G\langle\alpha\rangle$. Then G is solvable.*

Apart from these, we considered a pair G, A with $A \leq Aut(G)$ and investigated the influence of $|G : C_G(A)|$ on the Fitting length of $[G, A]$ when G is a solvable group and $(|G|, |A|) = 1$. Namely, we obtained the following:

Theorem 1: *Let G be a finite solvable group and $A \leq Aut(G)$ with $(|G|, |A|) = 1$. Then $f([G, A])$ is bounded above by the number of primes dividing $|G : C_G(A)|$, counted with multiplicities. This bound is the best possible one.*

It should be noted that although this bound is best possible, it seems possible to improve it in some special cases.

The outline of the thesis is as follows:

Chapter 2 contains some useful theorems which will be referred throughout the presentation of the main results of this thesis.

In Chapter 3, we state and prove the main results we obtained. This chapter also contains examples and counterexamples supporting the arguments.

In Appendices A, B and C, we give some arithmetical information and tables on the automorphism groups of simple groups which will be referred throughout the proof of our Theorem 3.

CHAPTER 2

SOME USEFUL THEOREMS

In this chapter, we shall present some useful results pertaining to the proof of the main theorems of this thesis.

In 1904, Burnside proved the solvability of a group of order $p^{\alpha}q^{\beta}$. Since then many authors have investigated the relationship between the structure of a finite group and arithmetical condition on the sizes of its conjugacy classes. His proof depends on a very well-known result of him,Burnside's p^{α}-lemma, on nonsimplicity.

Theorem 2.0.1 (Burnside's p^{α}-lemma, [3]) *If the number of elements in a conjugacy class of a finite group G is equal to a power of a prime number then G is not simple.*

In 1990, Kazarin [25] generalized this lemma as follows:

Theorem 2.0.2 ([25], Theorem) *If for some $x \in G$, $|G : C_G(x)|$ is a power of a prime, then $\langle x^G \rangle$ is solvable.*

Proof. Let G be a minimal counter example to the theorem, that is, if K is a group with order less than the order of G and satisfying the assumptions of the theorem, then it satisfies the theorem. Let $x \in G$ such that $|G : C_G(x)| = p^{\alpha}$. Then $x \neq 1$ and also G is not simple by Burnside's p^{α}-lemma.

If M is a proper normal subgroup of G containing x, then it is obvious that $|M : C_M(x)| = p^{\beta}$ for some $\beta \leq \alpha$. It follows by induction that $\langle x^M \rangle$ is solvable, that is, $x \in S(M) \leq S(G)$. This contradiction shows that there is no proper normal subgroup of G containing x.

If $1 \neq M \lhd G$, then $C_G(x)M/M \subseteq C_{G/M}(xM)$ and hence $\left|G/M : C_{G/M}(xM)\right|$ is also a power of p. Thus, $xM \in S(G/M)$ by induction applied to G/M. If $S(G/M) = X/M \lhd G/M$, then $X \lhd G$ and hence $x \in X \lhd G$, a contradiction. Therefore, $S(G/M) = G/M$, that is, G/M is solvable for any $1 \neq M \lhd G$.

If $S(G) \neq 1$, then as $S(G) \neq G$ we get $G/S(G)$ is solvable. Since we also have $S(G)$ is solvable, we get G is solvable, a contradiction. Therefore, $S(G) = 1$.

Let N be a minimal normal subgroup of G. Then $1 \neq N \neq G$ as G is not simple and also we have $x \notin N$. Set $K = N\langle x\rangle$. It is obvious that $|N : C_N(x)| = |K : C_K(x)|$ is a power of p. If $K \neq G$, then by induction applied to K we get $x \in S(K)$. As $\langle x^N\rangle = [x, N]\langle x\rangle$, we have $[x, N] \subseteq S(K)$ and hence $[x, N] \subseteq S(K) \cap N \leq S(N) \leq S(G) = 1$. Thus, $x \in C_G(N) \lhd G$. It follows that $C_G(N) = G$, that is, $N \leq Z(G)$. Then N is solvable. We also have G/N is solvable. It follows that G is solvable, a contradiction.

Therefore, $G = N\langle x\rangle$, where N is a minimal normal subgroup of G.

Suppose that $|x| = rm$ for some prime r and integer $m > 1$. Set $y = x^m$. Then $|G : C_G(y)|$ is a power of p and hence $\langle y^N\rangle = [N, y]\langle y\rangle$ is solvable by induction applied to $N\langle y\rangle$. Note that $[N, y] \lhd N\langle x\rangle = G$. Then $[N, y] = N$ by the minimality of N and hence N is solvable. Therefore, G is solvable, a contradiction. So we may assume that $|x| = r$ where r is a prime number.

Suppose that M is another minimal normal subgroup of G. Then $M \cap N = 1$ and $MN = G$. Then $M \cong G/N \cong \langle x\rangle$ and hence M is solvable. Since $G/M \cong N$ is also solvable, we get G is solvable, a contradiction. Therefore, N is the unique minimal normal subgroup of G.

Suppose that either $r = p$ or $r \notin \pi(N)$. Then r is coprime to the number of Sylow p-subgroups of N. Hence there exists $P \in Syl_p(N)$ such that $P^x = P$ by Theorem 2.0.8 (c). It follows that $\langle x, P\rangle = P\langle x\rangle$ is a $\{p, r\}$-group and hence solvable. Since $|G : C_G(x)| = p^\alpha$ we have $G = PC_G(x)$ and then $x^G = x^P$. Now, $\langle x^G\rangle = \langle x^P\rangle \leq \langle x, P\rangle$ is a solvable group, a contradiction.

Therefore, $r \neq p$ and $r \in \pi(N)$.

Consider the principal r-block B_{r_0} of G. Let $\chi \in B_0(r)$. Then

$$|G : C_G(x)|\chi(x)\chi(1)^{-1} \equiv |G : C_G(x)| \pmod{\omega} \tag{2.1}$$

where ω is a maximal ideal in the ring of integer algebraic numbers containing r.

Also $|G : C_G(x)| = p^\alpha \not\equiv 0 \pmod{\omega}$. Thus,

$$\chi(x) \neq 0 \text{ for any } \chi \in B_0(r). \tag{2.2}$$

If p does not divide $\chi(1)$ then either $xKer\chi \in Z(G/Ker\chi)$ or $\chi(x) = 0$. In our case, G has a unique maximal normal subgroup. It follows that either $\chi(1) \equiv 0\ (modp)$, or $N \leq Ker\chi$ and χ is a linear character. Thus, $\chi(1) \not\equiv 0\ (modp)$ for any linear character $\chi \in B_0(r)$.

We observe that any linear character of the group G satisfies the relation $\lambda^r = 1_G$ where 1_G is a principal character and therefore it is easy to see that $\lambda \in B_0(r)$. Thus, there are exactly r linear characters in $B_0(r)$.

By the orthogonality formula (Theorem 2.0.16), for $B_0(r)$ and for an arbitrary r-element g we have

$$\sum_{\chi \in B_0(r)} \chi(1)\chi(g) = 0. \tag{2.3}$$

It was mentioned above that $r \in \pi(N)$. Thus, there is $y \in N$ of order r. Substituting y in the equation (2.3) and selecting terms corresponding to linear characters we obtain

$$0 = \sum_{\chi \in B_0(r),\ \chi(1)=1} \chi(y) + \sum_{\chi \in B_0(r),\ \chi(1)\neq 1} \chi(1)\chi(y) \tag{2.4}$$

Since $\chi(y) = 1$ for any linear character χ and $\chi(1) = pn_\chi$ for any nonlinear $\chi \in B_0(r)$, it follows that the equation (2.4) can be written in the form

$$r + p \sum_{\chi \in B_0(r),\ \chi(1)\neq 1} \chi(y)n_\chi = 0. \tag{2.5}$$

Hence it follows that r/p is an algebraic integer. This is a contradiction proving the theorem. ■

As a corollary of this theorem, Kazarin stated the following result. By doing this, he pointed out that the methods of studying the structure of $[G, \alpha]$ for $\alpha \in Aut(G)$ in terms of the index of $C_G(\alpha)$ might be very closely related to the methods in the investigation of the influence of the length of the conjugacy classes to the structure of G.

Corollary 2.0.3 ([25], Corollary 1) *Let G be a finite group and α one of its automorphisms. If $C_G(\alpha)$ contains a Sylow r-subgroup of the group G for all $r \in \pi(G)\backslash\{p\}$ then α induces the identity automorphism on $G/S(G)$.*

The following two theorems are due to A. Camina and R. Camina. We shall make use of them in proving the main results of this the thesis.

Theorem 2.0.4 ([7], Lemma 6) *If G is simple, then 4 divides the length of a conjugacy class of G.*

Theorem 2.0.5 ([4], Lemma 1, Corollary 1) *Let G be a finite group.*

1. *If for some prime number p, any p'-element has p'-index in G, then G has a unique Sylow p-subgroup which is a direct factor.*
2. *If for some prime number p, $p \nmid |C|$ for any $C \in Con(G)$ then G has a unique Sylow p-subgroup which is an abelian direct factor.*

We present next a result due to Gross which will be referred in the proof of Theorem 3.

Theorem 2.0.6 ([18]) *Let G be a finite simple non-abelian group and let p be an odd prime dividing the order of G. Let $A = Aut(G)$ and let S be a Sylow $p-$subgroup of A. Identifying G with $Inn(G)$, set $P = S \cap G$. Then $C_S(P) = Z(P)$.*

Finally, we shall state some well-known results which will be referred throughout the thesis.

Theorem 2.0.7 ([26], Theorem 8.2.2) *Let N be an A-invariant normal subgroup of G. Supppose that $(|A|, |N|) = 1$ and A or G is solvable. Then*

(a) $C_{G/N}(A) = C_G(A)N/N$,

(b) *If A acts trivially on N and G/N, then A acts trivially on G.*

Theorem 2.0.8 ([26], Theorem 8.2.7) *Suppose that the action of A on G is coprime. Let p be a prime divisor of $|G|$.*

(a) $G = [G, A]C_G(A)$,

(b) $[G, A] = [G, A, A]$.

(c) There exists an A-invariant Sylow p-subgroup of G.

Theorem 2.0.9 ([16], Theorem 2.2.3 (Three Subgroup Lemma)) *Let x, y, z be elements of G and H, K, L subgroups of G. Then we have*

(i) $[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$.

(ii) If $[H, K, L] = 1$ *and* $[K, L, H] = 1$*, then* $[L, H, K] = 1$.

Definition 2.0.10 ([16], Theorem 6.1.2) *Let G be a group. The subgroup of G generated by all its nilpotent normal subgroups is a nilpotent normal subgroup of G. This subgroup is called the Fitting subgroup of G and shall be denoted by $F(G)$.*

Theorem 2.0.11 ([16], Theorem 6.1.3) *If G is solvable, then $C_G(F(G)) \subseteq F(G)$.*

Definition 2.0.12 *Let G be a group. The Fitting series of G is the normal series defined by $F_0(G) = 1$ and $F_{i+1}(G)/F_i(G) = F\,(G/F_i(G))$ for all $i \geq 1$.*

If $G = F_n(G)$ for some $n \in \mathbb{N}$, then n is called the Fitting length of G and it is denoted by $f(G)$.

Theorem 2.0.13 ([30], Section 2.4) *If $n \geq 5$, then $Aut(A_n) \cong S_n$ whenever $n \neq 6$. $Aut(A_6)$ is isomorphic to the semidirect product of S_6 by the automorphism sending 3-cycles to product of two disjoint 3-cycles and sending product of two disjoint 3-cycles to 3-cycles.*

Theorem 2.0.14 *Let G be a group and x and y be two commuting elements of G such that* $(|x|, |y|) = 1$. *Then $C_G(xy) = C_G(x) \cap C_G(y)$.*

Proof. It is obvious that $C_G(x) \cap C_G(y) \leq C_G(xy)$.

Set $|x| = m$ and $|y| = n$. Since $(m, n) = 1$, there exist integers r, s such that $rm + sn = 1$. As $[x, y] = 1$, we have $(xy)^{rm} = x^{rm}y^{rm} = y^{1-sn} = y$ and $(xy)^{sn} = x^{sn}y^{sn} = x^{1-rm} = x$.

If $a \in C_G(xy)$, then $1 = [a, (xy)^{rm}] = [a, y]$ and $1 = [a, (xy)^{sn}] = [a, x]$. It follows that $a \in C_G(x)$ and $a \in C_G(y)$. Therefore, $C_G(xy) = C_G(x) \cap C_G(y)$, as desired. ■

Theorem 2.0.15 *If G is a nonabelian simple group, then 4 divides the order of G.*

Theorem 2.0.16 ([21], 15.23) *Let $x, y \in G$ with $p \nmid |x|$ and $p|\ |y|$. Let B be a p-block of G. Then*

$$\sum_{\chi \in B \cap Irr(G)} \chi(x)\overline{\chi(y)} = 0 \tag{2.6}$$

CHAPTER 3

MAIN THEOREMS

In this chapter, we shall state and prove the main results of this thesis.

Let G be a finite group and $A \leq Aut(G)$. We shall discuss the influence of $|G : C_G(A)|$ on the structure of the group G. In fact we should ask about the structure of $[G, A]$ rather than asking about that of G. Because by adding a direct factor K to G so that $[K, A] = 1$, we can obtain a group $H = G \times K$ such that $|H : C_H(A)| = |G : C_G(A)|$.

We shall present our results in two sections according to the action of A on G being coprime or noncoprime.

3.1 Results in the Coprime Case

In this section, we shall state and prove two results under the coprimeness condition first of which gives an upper bound for the Fitting length of $[G, A]$ in terms of $|G : C_G(A)|$ when G is solvable.

Theorem 1 *Let G be a finite solvable group, $A \leq Aut(G)$ such that $(|G|, |A|) = 1$ and $|G : C_G(A)| = m$. If $[G, A]$ is solvable, then $f([G, A]) \leq l(m)$ where $l(m)$ is the number of primes dividing m, counted with multiplicities.*

Proof. We shall proceed by induction on $|G|$.

If $[G, A]$ is properly contained in G, it follows by induction that

$$f([G, A, A]) \leq l(\left|[G, A] : C_{[G,A]}(A)\right|) = l(|[G, A]\, C_G(A) : C_G(A)|) \leq l(m) \qquad (3.1)$$

as $G = [G, A]C_G(A)$ by Theorem 2.0.8 (a) in Chapter 2.

In addition, we have $[G, A, A] = [G, A]$ since $(|G|, |A|) = 1$ by Theorem 2.0.8 (b). This leads to the contradiction $f([G, A]) \leq l(m)$ and hence $[G, A] = G$.

If G is nilpotent then $f(G) = 1 \leq l(m)$. Thus, we may assume that $F(G) \lneqq G$.

We observe next that $[F(G), A] \neq 1$:

Assume otherwise. Then $[F(G), G, A] = 1 = [A, F(G), G]$. It follows by the Three Subgroup Lemma (See Theorem 2.0.9) that $[G, A, F(G)] = [G, F(G)] = 1$. Since $C_G(F(G)) \subseteq F(G)$ by Theorem 2.0.11, we get $G = F(G)$, which is not the case. Hence $F(G) \nleq C_G(A)$ as claimed.

Now, $C_G(A)F(G) \neq C_G(A)$ and hence $l(|G : C_G(A)F(G)|) \lneqq l(m)$. By induction applied to $G/F(G)$, we see that $f(G) - 1 = f(G/F(G)) \leq l(|G/F(G) : C_{G/F(G)}(A)|)$. We also have $l(|G/F(G) : C_{G/F(G)}(A)|) \leq l(|G/F(G) : C_G(A)F(G)/F(G)|) = l(|G : F(G)C_G(A)|) \lneqq l(m)$. Consequently $f(G) - 1 \leq l(m) - 1$ and hence $f(G) \leq l(m)$, completing the proof. ■

Remark 3.1.1 *The bound given by Theorem 1 is best possible because of the following example:*

Let G be the group

$$\left\langle\, a, b, c, d \mid a^3 = b^7 = c^3 = d^7 = [a, c] = [a, d] = [b, c] = [b, d] = 1, a^{-1}ba = b^2, c^{-1}dc = d^2 \,\right\rangle$$

and let α be the automorphism of G given by $\alpha(a) = cd^5$, $\alpha(b) = d^2$, $\alpha(c) = ab$, $\alpha(d) = b^4$.

Then $|G| = 441$ and $|\alpha| = 2$ and hence the condition $(|G|, |\alpha|) = 1$ is satisfied.

We observe by means of GAP that

$$\begin{aligned} C_G(\alpha) = \{&1, cd^4, c^2d, c^3d^5, c^4d^2, c^5d^6, c^6d^3, abd, abcd^5, abc^2d^2, abc^3d^6, abc^4d^3, abc^5, abc^6d^4, \\ &a^2b^2d^3, a^2b^2c, a^2b^2c^2d^4, a^2b^2c^3d, a^2b^2c^4d^5, a^2b^2c^5d^2, a^2b^2c^6d^6\} = \left\langle cd^4, abd \right\rangle. \end{aligned}$$

Thus, $|G : C_G(\alpha)| = 21$ and hence $\ell(m) = 2$. We also observe by GAP that $[G, \alpha] = G$, $F([G, \alpha]) = \langle a, c \rangle$ and $F_2(G) = G$. Therefore, $f(G) = 2 = \ell(m)$.

As mentioned in the Introduction part, inspired by a result [10] due to Cossey and Wang, we handled the case where A is cyclic and $|G : C_G(A)|$ is squarefree. Under the coprimeness condition we obtained the following:

Theorem 2 *Let G be a finite group and α an automorphism of G such that* $(|G|, |\alpha|) = 1$. *If $|G : C_G(\alpha)|$ is squarefree. Then $[G, \alpha]$ is solvable.*

Proof. We proceed by induction on the order of H where H stands for the semidirect product of G by $\langle\alpha\rangle$, and deduce a contradiction over a series of steps.

1. *We may assume that α is of prime order.*

Let $|\alpha| = m$ and p be a prime divisor of m. Now, $|\alpha^k| = p$ where $k = \frac{m}{p}$. Since $|G : C_G(\alpha^k)|$ is squarefree as $C_G(\alpha) \subseteq C_G(\alpha^k)$, we see by induction that $[G, \alpha^k]$ is solvable.

Now, $[G, \alpha^k] \trianglelefteq G$ and $\overline{G} = G/[G, \alpha^k]$ is α-invariant. $|\overline{G} : C_{\overline{G}}(\alpha)|$ divides $|\overline{G} : \overline{C_G(\alpha)}|$ and hence divides $|G : C_G(\alpha)|$. It follows by induction that $[\overline{G}, \alpha] = \overline{[G, \alpha]} = [G, \alpha]/[G, \alpha^k]$ is solvable. Therefore $[G, \alpha]$ is solvable.

2. *α is not contained in a proper normal subgroup of $H = G\langle\alpha\rangle$.*

Let N be a proper normal subgroup of H containing α. Then $N = (N \cap G)\langle\alpha\rangle$.

It is obvious that $N_1 = N \cap G$ is α-invariant. Since $|N_1 : C_{N_1}(\alpha)|$ divides $|G : C_G(\alpha)|$, we have $[N_1, \alpha] = [N, \alpha]$ is solvable by induction applied to $N_1\langle\alpha\rangle$. This yields that
$\langle\alpha^N\rangle = [N, \alpha]\langle\alpha\rangle$ is solvable and hence $\alpha \in S(N) \leq S(H)$.

It follows that $\langle\alpha^H\rangle = \langle\alpha^G\rangle = [G, \alpha]\langle\alpha\rangle \leq S(H)$. Then $[G, \alpha]$ is solvable, a contradiction.

3. *For any nontrivial proper normal subgroup N of H, $\overline{H} = H/N$ is solvable.*

By Step 2, $\overline{\alpha} \neq 1$. Now, $\overline{H} = \overline{G}\langle\overline{\alpha}\rangle$ and $\left|\overline{G} : C_{\overline{G}}(\overline{\alpha})\right|$ divides $|G : C_G(\alpha)|$. Hence, by induction applied to $\overline{H}$, we have $[\overline{G}, \overline{\alpha}] = [\overline{H}, \alpha]$ is solvable. It follows that
$\langle\overline{\alpha}^{\overline{H}}\rangle = [\overline{H}, \overline{\alpha}]\langle\overline{\alpha}\rangle$ is solvable and hence $\overline{\alpha} \in S(\overline{H})$.

It is obvious that $S(\overline{H}) = X/N$ for some X containing α. In addition, $X \lhd H$. By Step 2, this is the case only when $X = H$.

Thus $S(\overline{H}) = \overline{H}$, that is, $\overline{H}$ is solvable.

4. $S(H) = 1$

If not, then both $S(H)$ and $H/S(H)$ are solvable, leading to the contradiction that H is solvable.

5. *G is the unique minimal normal subgroup of H and $H' = G$.*

Let N be a minimal normal subgroup of H. If $N \nleq G$, then $N \cap G = 1$ and $H = GN$ as $|H : G| = |\alpha|$ is prime. It follows that $|N|$ is prime and hence $N \leq S(H) = 1$, which is not the case. Thus $N \leq G$. Set $K = N\langle\alpha\rangle$. We shall observe that $H = K$:

Assume otherwise. Then by induction, $[N, \alpha]$ is solvable and hence $\langle\alpha^N\rangle = [N, \alpha]\langle\alpha\rangle$ is solvable. So $\alpha \in \langle\alpha^N\rangle = \langle\alpha^K\rangle \leq S(K)$.

Now, $[\alpha, N] \leq S(K) \cap N \leq S(N) \leq S(H) = 1$, implying that $\alpha \in C_H(N) \trianglelefteq H$. By Step 2, we get the equality $C_H(N) = H$. Thus $N \leq Z(H) \leq S(H) = 1$. This contradiction shows that $H = N\langle\alpha\rangle = K$. As a consequence $G = N$ is the unique minimal normal subgroup of H and $H' = G$.

6. *G is simple.*

Now, G is characteristically simple, and so it is a direct product of isomorphic copies of a simple group. More precisely, $G = E_1 \times \cdots \times E_k$ where each E_i is a simple group isomorphic to E_1, and E_1 is not abelian because otherwise H would be a $\{p, q\}$-group and hence solvable.

We consider the action of α on the set of subgroups of G. Let $\{ E_1, E_1^{\alpha}, \ldots, E_1^{\alpha^k} \}$ be the orbit of this action containing E_1. Then $C = E_1 \times E_1^{\alpha} \times \ldots \times E_1^{\alpha^k}$ is an α-invariant normal subgroup of G. That is, C is normal in H. Now, H/C is solvable by Step 3. It follows that G/C is solvable. This is the case only when $C = G = E_1 \times E_1^{\alpha} \times \ldots \times E_1^{\alpha^k}$.

Now, $k = 1$ or $k = p$. If the former holds, then $C_G(\alpha) = \{ xx^{\alpha}x^{\alpha^2} \ldots x^{\alpha^{p-1}} \mid x \in E_1 \}$ and hence $|C_G(\alpha)| = |E_1|$ implying that $|G : C_G(\alpha)| = |E_1|^{p-1}$ is squarefree. This is a contradiction since the simplicity of E_1 implies that $|E_1|$ is divisible by 4 by Theorem 2.0.15. Therefore, $k = 1$, that is, G is a nonabelian simple group, as claimed.

7. *Final Contradiction*

From Appendix A we observe that G is not a Sporadic simple group. By Theorem 2.0.13, we observe also that G is not an Alternating group. Thus, G is a simple group of Lie type. Then by Theorem B.0.14, α is of the form $idfg$. Any inner automorphism and any diagonal automorphism has order dividing order of G. Since order of graph automorphisms of simple groups of Lie type is either 2 or 3, we observe that α is a field automorphism.

By Theorem B.0.15, if $q = r^{2s}$ for some integer s and $G = L(q)$, then $C_G(\alpha) \cong L(r^s)$.

If $G = A_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) = A_m(r^s)$ or $C_G(\alpha) =^2 A_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{\frac{m(m+1)}{2}}}{(r^s)^{\frac{m(m+1)}{2}}} = r^{\frac{sm(m+1)}{2}}$

If $G = B_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) = B_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m^2}}{(r^s)^{m^2}} = r^{sm^2}$

If $G = C_m(q^{2s})$ for $m \geq 3$ then $C_G(\alpha) = C_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m^2}}{(r^s)^{m^2}} = r^{sm^2}$

If $G = D_m(q^{2s})$ for $m \geq 4$ then $C_G(\alpha) = D_m(r^s)$ or $C_G(\alpha) =^2 D_m(r^s)$ or $C_G(\alpha) =^3 D_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m(m-1)}}{(r^s)^{m(m-1)}} = r^{sm(m-1)}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{12}}{(r^s)^{12)}} = r^{12s}$

If $G = E_6(q^{2s})$ then $C_G(\alpha) = E_6(r^s)$ or $C_G(\alpha) =^2 E_6(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{36}}{(r^s)^{36}} = r^{36s}$

If $G = E_7(q^{2s})$ then $C_G(\alpha) = E_7(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{63}}{(r^s)^{63}} = r^{63s}$

If $G = E_8(q^{2s})$ then $C_G(\alpha) = E_8(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{120}}{(r^s)^{120}} = r^{120s}$

If $G = F_4(q^{2s})$ then $C_G(\alpha) = F_4(r^s)$ or $C_G(\alpha) =^2 F_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{24}}{(r^s)^{24}} = r^{24s}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{24}}{(r^s)^{12}} = r^{36s}$

If $G = G_2(q^{2s})$ then $C_G(\alpha) = G_2(r^s)$ or $C_G(\alpha) =^2 G_2(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{6}}{(r^s)^{6}} = r^{6s}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{6}}{(r^s)^{3}} = r^{9s}$

If $G =^2 A_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) =^2 A_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{\frac{m(m+1)}{2}}}{(r^s)^{\frac{m(m+1)}{2}}} = r^{\frac{sm(m+1)}{2}}$

If $G =^2 D_m(q^{2s})$ for $m \geq 4$ then $C_G(\alpha) =^2 D_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m(m-1)}}{(r^s)^{m(m-1)}} = r^{sm(m-1)}$

If $G =^2 E_6(q^{2s})$ then $C_G(\alpha) =^2 E_6(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{36}}{(r^s)^{36}} = r^{36s}$

If $G =^3 D_4(q^{2s})$ then $C_G(\alpha) =^3 D_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{12}}{(r^s)^{12}} = r^{12s}$.

In all cases, r^2 divides $|G : C_G(\alpha)|$. This contradiction completes the proof. ■

Remark 3.1.2 *One may ask if it is possible to replace the assumption that $|G : C_G(\alpha)|$ is squarefree by the assumption that $|G : C_G(\alpha)|$ is not divisible by 4. The following example shows that this is not possible:*

Let $G = PSL(3, \mathbb{F}_{3^5})$ and let σ be the field automorphism of order 5. Since $|G| = 2^4.3^{15}.11^4.13.61.4561$, we have $(|G|, |\sigma|) = 1$. We also know $C_G(\sigma) = PSL(3, \mathbb{F}_3)$, and hence $|C_G(\sigma)| = 2^4.3^3.13$. Then $|G : C_G(\sigma)| = 3^{12}.11^4.61.4561$ is odd.

3.2 Results in the Noncoprime Case

In this section we shall study without the coprimeness condition. The following example shows that it is not possible to obtain the conclusion of Theorem 2 if the action is noncoprime.

Example 3.2.1 *Let $G = A_5$ with $\alpha = \tau_{(1\ 2)} \in Aut(G) \setminus Inn(G)$. Then $|G : C_G(\alpha)| = 10$ but $[A_5, (1\ 2)] = A_5$ is simple.*

Considering the question that how the information about $C_G(A)$ influence the structure of G, it has been observed by Ercan and Güloğlu in [11], [12], [13], [14] that the properties of elements in $GA \setminus G$ may also influence the structure of G. They imposed some conditions on these elements in order to overcome some of the difficulties arising from a noncoprime action. This brought us to the following:

Question 2. *Let G be a finite group and $\alpha \in Aut(G)$. Is G solvable if $|G : C_G(x)|$ is squarefree for each $x \in H \setminus G$ where H denotes the semidirect product of G by $\langle\alpha\rangle$?*

We should note that we first attempted to use this hypothesis only for $x \in H \setminus G$ of order equal to $|\alpha|$. But the same counter-example mentioned above served as a counter-example in this case as well. Consequently, we showed that the answer to Question 2 is in affirmative. Namely, we proved the following:

Theorem 3 *Let G be a finite group and $\alpha \in Aut(G)$. Assume that $|G : C_G(x)|$ is squarefree for each $x \in H \setminus G$ where $H = G\langle\alpha\rangle$. Then G is solvable.*

3.2.1 Some Technical Lemmas

Before giving a proof of Theorem 3, we shall first observe that it is possible to eliminate $PSL(n, \mathbb{F}_q)$ under the weaker hypothesis that $|G : C_G(x)|$ is not divisible by 4 for each $x \in H \setminus G$.

This observation will be presented in a series of technical lemmas.

Remark 3.2.2 *Throughout this section, K denotes $SL(n, \mathbb{F}_q)$ for a prime power q and an integer $n \geq 2$ so that $n \neq 2$ when $q = 2$ or $q = 3$. In addition, G denotes $PSL(n, \mathbb{F}_q) = K/Z(K)$ and L denotes $GL(n, \mathbb{F}_q)$.*

Remark 3.2.3 *Since $Z(K)$ is characteristic in K, every automorphism of K induce an automorphism of G. Conversely, every automorphism of G determines a class of automorphisms of K. More precisely, we first define the relation $\sim$ on $A = Aut(K)$ as follows:*

For $\alpha, \beta \in A$, $\alpha \sim \beta$ if and only if $\alpha(g)\beta(g^{-1}) \in Z(K)$ for all $g \in K$.

This allows us to regard α as an automorphism of K rather than an automorphism of G.

Lemma 3.2.4 *Let α be a diagonal automorphism of G. Then there is an element $x \in G\langle\alpha\rangle \setminus G$ so that 4 divides $|G : C_G(x)|$.*

Proof. Let $V = \mathbb{F}_{q^n}$. We regard V as a vector space over $\mathbb{F}_q$. Let x be an element of V of order $q^n - 1$. Then $\mathbb{F}^*_{q^n} = \langle x\rangle$ and x can be thought as an element of L so that $x(v) = x.v$ on V. Then x has a matrix representation A in L and A is similar to the diagonal matrix $\mathbf{diag}(x, x^q, \ldots, x^{q^{n-1}})$ over F_{q^n}. It follows that the determinant of x is its norm, that is,
$\det(x) = Norm_{\mathbb{F}_{q^n} \to \mathbb{F}_q}(x) = xx^q \ldots x^{q^{n-1}} = x^{\frac{q^n-1}{q-1}}$. Since $\det(x) \in \mathbb{F}^*_q$ with $|\det(x)| = q - 1$, we have $\mathbb{F}*_{||} = \langle\det(x)\rangle$.

We observe first that $C_L(x) = \langle x\rangle$: Let $\gamma \in L$ such that $\gamma x = x\gamma$. Then for $1 = 1_V$, we have

$$\gamma(x) = \gamma(x.1) = \gamma(x(1)) = (\gamma x)(1) = (x\gamma)(1) = x.\gamma(1). \tag{3.2}$$

We observe next by induction that $\gamma(x^m) = x^m\gamma(1)$ for any positive integer m.

Assume that $\gamma(x^k) = x^k\gamma(1)$ for a fixed but arbitrary positive integer k. Now,

$$x^{k+1}\gamma(1) = xx^k\gamma(1) = x\gamma(x^k) = (x\gamma)(x^k) = (\gamma x)(x^k) = \gamma(x(x^k)) = \gamma(x^{k+1}). \tag{3.3}$$

Thus, by induction $\gamma(x^m) = x^m\gamma(1)$ for any positive integer m.

For each $v \in V \setminus \{0\}$, $v = x^m$ for some integer m and hence $\gamma(v) = \gamma(x^m) = x^m\gamma(1)$. Since $0 \neq \gamma(1) \in V$ we have $\gamma(1) = x^s$ for some integer s. Then $\gamma(v) = \gamma(x^m) = x^{m+s}$, that is $\gamma \in \langle x\rangle$ and hence $C_L(x) = \langle x\rangle$. To simplify the notation we set $T = \langle x\rangle$.

Let now $\mathbf{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle\sigma\rangle$. Then σ has order n and it can be viewed as an element of L. We now observe that

$$(\sigma x\sigma^{-1})(v) = \sigma(x(\sigma^{-1}(v))) = \sigma(x.\sigma^{-1}(v)) = \sigma(x).\sigma(\sigma^{-1}(v)) = \sigma(x).v = (\sigma(x))(v) \tag{3.4}$$

for any $v \in V$.

This gives that $\sigma x\sigma^{-1} = \sigma(x) \in T$ and hence $\sigma \in N_L(T)$.

If $\beta \in N_L(T)$ then $\beta x\beta^{-1} \in T$. The map $\theta : y \mapsto \beta y\beta^{-1}$ is a field automorphism of $\mathbb{F}_{q^n}$ fixing every element of $\mathbb{F}_q$ as $\langle\det(x)\rangle = \mathbb{F}_q^*$. So $\theta \in \langle\sigma\rangle$ such that $\beta^{-1}\theta \in C_L(T) = T$. Thus we obtain $N_L(T) = \langle\sigma, T\rangle$.

We shall claim that $C_{L/Z(L)}(T) = C_L(T)/Z(L)$:

To verify this claim, pick an element y from L such that $xy = zyx$ for some $z \in Z(L)$. Then $y^{-1}xy \in T$ as $z \in T$. This implies that $y \in N_L(T) = \langle\sigma, T\rangle$. If $y \notin T$ then $y = x^k\sigma^{-a}$ for some integer k and for some $a \in \{1, 2, \ldots, n-1\}$. It follows that

$$y^{-1}xy = \sigma^a x^{-k}xx^k\sigma^{-a} = \sigma^a x\sigma^{-a} = \sigma^a(x) = x^{q^a}. \tag{3.5}$$

Thus $x^{q^a} = zx$ which implies that $x^{q^a-1} = z$, a contradiction. Consequently, $y \in T = C_L(T)$ establishing the claim.

Therefore, $|C_{L/Z(L)}(x)| = \frac{|T|}{q-1} = \frac{q^n-1}{q-1}$.

We first handle the case $n > 2$. Note that

$$|G : C_G(x)| = \left|PGL(n, \mathbb{F}_q) : C_{PGL(n,\mathbb{F}_q)}(x)\right| = \frac{\frac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{q-1}}{\frac{q^n-1}{q-1}} = \prod_{i=1}^{n-1}(q^n - q^i). \tag{3.6}$$

Then $(q^n - q)(q^n - q^2)$ divides $|G : C_G(x)|$. So 4 divides $|G : C_G(x)|$, as desired.

We suppose next that $n = 2$. Then we have

$$|C_{L/Z(L)}(x)| = \frac{|T|}{q-1} = \frac{q^2 - 1}{q-1} = q + 1 \tag{3.7}$$

and

$$|G : C_G(x)| = \left|PGL(2, \mathbb{F}_q) : C_{PGL(2,\mathbb{F}_q)}(x)\right| = \frac{\frac{(q^2-1)(q^2-q)}{q-1}}{q+1} = q^2 - q. \tag{3.8}$$

Assume that **char** $\mathbb{F}_q = 2$:

Since $PSL(2, 2)$ is not simple we have $q > 2$ in this case and hence 4 divides q. It follows that 4 divides $|G : C_G(x)|$, as desired.

Thus **char** $\mathbb{F}_q \neq 2$ and $q \equiv \mp 1 (mod\ 4)$. We can also notice that $4 \nmid q - 1$, because otherwise 4 divides $|G : C_G(x)|$. Now, we may assume that 4 divides $q + 1$.

We consider next that the group $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid ab \neq 0;\ a, b \in \mathbb{F}_q \right\}$. Let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in H$ where a is a primitive $q-1^{st}$ root of unity and choose $B = \begin{bmatrix} c & 0 \\ 0 & c \end{bmatrix} \in H$ such that $\det(BA) = 1$. Then $BA = \begin{bmatrix} ac & 0 \\ 0 & c \end{bmatrix}$ and $1 = \det(BA) = ac^2$ and hence

$a = (c^{-1})^2$ which contradicts the primitivity of a as q is odd. So the coset of G in L containing A is not an element of G.

Let now $C = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in L$ such that $CA = \begin{bmatrix} xa & y \\ za & t \end{bmatrix} = \begin{bmatrix} ax & ay \\ z & t \end{bmatrix} = AC$. Then $y = ay$ and $z = az$ give $y = 0 = z$. This shows that $C_L(A) = H$.

We are now ready to observe that $C_{L/Z(L)}(A) = H/Z(L)$:

Let $E = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in L$ and $\lambda \in \mathbb{F}_q$ such that $EA = \begin{bmatrix} xa & y \\ za & t \end{bmatrix} = \begin{bmatrix} \lambda ax & \lambda ay \\ \lambda z & \lambda t \end{bmatrix} = \lambda AE$. This leads to the following equations:

$ax = \lambda ax$ (which means $x = \lambda x$ as $a \neq 0$) and $y = \lambda ay$ and $az = \lambda z$ and $t = \alpha t$.

If $x = 0$, then $y \neq 0 \neq z$. Then $\lambda a = 1$ and $\lambda = a$. Now, $a^2 = 1$ which gives $q - 1 = 2$, that is,

$q = 3$. But $PSL(2, \mathbb{F}_3)$ is not simple. Therefore, we have $x \neq 0$ and hence $\lambda = 1$.

It follows that, $C_{L/Z(L)}(A) = H/Z(L)$. Then $|C_{L/Z(L)}(A)| = \frac{(q-1)^2}{q-1} = q - 1$, implying that

$$|G : C_G(x)| = \left|PGL(2, \mathbb{F}_q) : C_{PGL(2,\mathbb{F}_q)}(x)\right| = \frac{(q+1)q(q-1)}{q-1} = q(q+1). \tag{3.9}$$

Since 4 divides $q + 1$, 4 divides $|G : C_G(x)|$, as desired. ■

Lemma 3.2.5 *Let char $\mathbb{F}_q = 2$ and let σ be a field automorphism of G. Then there is an element $x \in G\langle\sigma\rangle \setminus G$ so that 4 divides $|G : C_G(x)|$.*

Proof. Let σ be a field automorphism of K of order r for some prime number r. Let $\mathbb{F}_{q_0}$ be the fixed field of σ on $\mathbb{F}_q$ and set $L_0 = GL(n, \mathbb{F}_{q_0})$. Put $C_{K/Z(K)}(\sigma) = C/Z(K)$. Then for $x \in C$, $x^\sigma Z(K) = (xZ(K))^\sigma = xZ(K)$ implying that $x^\sigma = \sigma(x) = \lambda x$ for some $\lambda \in Z(K)$. It follows that

$$x = x^{\sigma^r} = (\lambda x)^{\sigma^{r-1}} = (\sigma(\lambda)\lambda x)^{\sigma^{r-2}} = \ldots = \sigma^{r-1}(\lambda)\sigma^{r-2}(\lambda)\ldots\sigma(\lambda)\lambda x. \tag{3.10}$$

So,

$$\mathbf{Norm}_{\mathbb{F}_q \longrightarrow \mathbb{F}_{q_0}}(\lambda) = \sigma^{r-1}(\lambda)\sigma^{r-2}(\lambda)\ldots\sigma(\lambda)\lambda = 1. \tag{3.11}$$

By Hilbert's Theorem 90 [20], there exists $\mu \in \mathbb{F}_q$ such that $\lambda = \frac{\sigma(\mu)}{\mu}$. Then

$$(\mu^{-1}x)^\sigma = \sigma(\mu^{-1})\lambda x = \frac{1}{\sigma(\mu)}\frac{\sigma(\mu)}{\mu}x = \mu^{-1}x \tag{3.12}$$

and hence $\mu^{-1}x \in L_0$.

This implies that $\mu\mu^{-1}x = x \in Z(L)L_0$. Therefore, we have $C \subseteq K \cap L_0Z(L)$.

Let now, $A \in K \cap L_0Z(L)$. Then $A = ZY$ for some $Z \in Z(L)$ and $Y \in L_0$ where
$1 = \det A = \det Z \det Y$. So $\det Y = (\det Z)^{-1} = \gamma^{-n}$ for some $\gamma \in \mathbb{F}_q^*$.

Now, $Y \in C_0 = \{\ X \in L_0 \mid \det X$ is an n-th power in $\mathbb{F}_q\ \}$. Thus, there exists $Y \in C_0$ so that $A = \frac{1}{(detY)^{1/n}}Y$.

Define $\varphi : C_0 \longrightarrow C/Z(K)$ by $X \mapsto \frac{1}{(\det X)^{1/n}}XZ(K)$. By the above argument, φ is surjective.

Furthermore, for any $X, Y \in C_0$,

$$\varphi(XY) = \frac{1}{(\det(XY))^{1/n}}XYZ(K) = \frac{1}{(\det X \det Y)^{1/n}}XYZ(K) = \varphi(X)\varphi(Y), \tag{3.13}$$

that is, φ is a homomorphism. We also observe that

$$\begin{aligned} Ker\varphi &= \left\{ X \in C_0 \mid \tfrac{1}{(\det X)^{1/n}} X \in Z(K) \right\} \\ &= \{ X \in C_0 \mid X \in Z(L) \} \\ &= C_0 \cap Z(L) \\ &= C_0 \cap Z(L_0) \end{aligned} \tag{3.14}$$

So, $\quad C/Z(K) \cong C_0/(C_0 \cap Z(L_0) \cong C_0 Z(L_0)/Z(L_0) \quad$ and as

$C_0 Z(L_0)/Z(L_0) \leq PGL(n, \mathbb{F}_{q_0})$, we see that $|C_G(\sigma)| = |C/Z(K)|$ divides $|PGL(n, \mathbb{F}_{q_0})|$. Then $|PGL(n, \mathbb{F}_{q_0})| = m|C_G(\sigma)|$ for some positive integer m, giving $\frac{|G|}{|C_G(\sigma)|} = m\frac{|G|}{m|C_G(\sigma)|} = m\frac{|G|}{|PGL(n,\mathbb{F}_{q_0})|}$. Hence, $\frac{|G|}{|PGL(n,\mathbb{F}_{q_0})|}$ divides $|G : C_G(\sigma)|$.

Notice that $\frac{|PSL(n,\mathbb{F}_q)|}{|PGL(n,\mathbb{F}_{q_0})|} = \frac{q^{n(n-1)/2}}{(n,q-1)q_0^{n(n-1)/2}} \prod_{i=2}^{n} \frac{q^i - 1}{q_0^i - 1} = q_0^{(r-1)n(n-1)/2} \frac{1}{(n, q-1)} \prod_{i=2}^{n} \frac{q^i - 1}{q_0^i - 1}$.

Since $char\, \mathbb{F}_q = 2$, $\frac{1}{(n,q-1)} \prod_{i=2}^{n} \frac{q^i - 1}{q_0^i - 1}$ is odd.

Hence we have $4 \nmid \frac{|PSL(n,\mathbb{F}_q)|}{|PGL(n,\mathbb{F}_{q_0})|} \Leftrightarrow 4 \nmid q_0^{(r-1)n(n-1)/2}$

$$\begin{aligned} &\Leftrightarrow q_0 = 2 \text{ and } \tfrac{(r-1)n(n-1)}{2} = 1 \\ &\Leftrightarrow q_0 = 2 \text{ and } (r-1)n(n-1) = 2 \\ &\Leftrightarrow q_0 = 2, r = 2 \text{ and } n = 2 \end{aligned}$$

It follows that $G = PSL(2, \mathbb{F}_4) \cong A_5$. Then there exists $x = (1\ 5)(2\ 4\ 3) \in G\langle\sigma\rangle \setminus G$ such that $C_G(x) = \{ (1), (2\ 3\ 4), (2\ 4\ 3) \}$ $|G : C_G(x)| = 20$ is divisible by 4, as desired. ∎

Lemma 3.2.6 *Let q be odd and let σ be a field automorphism of G. Then there is an element $x \in G\langle\sigma\rangle \setminus G$ so that 4 divides $|G : C_G(x)|$.*

Proof. Pick an element $A = \begin{bmatrix} 1 & x_1 & & & & \\ & 1 & x_2 & & \mathbf{0} & \\ & & \ddots & \ddots & & \\ & \mathbf{0} & & & 1 & x_{n-1} \\ & & & & & 1 \end{bmatrix}$ from K.

Let σ be a field automorphism of K of order r induced by a field automorphism of $\mathbb{F}_q$ with fixed field $\mathbb{F}_{q_0}$. We shall consider the element $\sigma A \in K\langle\sigma\rangle \setminus K$ and show by induction that $(\sigma A)^m = \sigma^m \sigma^{m-1}(A)\ldots\sigma(A)A$ for any $k \geq 1$. Now,

$$(\sigma A)^2 = \sigma A \sigma A = \sigma\sigma\sigma^{-1} A \sigma A = \sigma^2 \sigma(A)A. \tag{3.15}$$

Assume that $(\sigma A)^k = \sigma^k \sigma^{k-1}(A)\ldots\sigma(A)A$ for a fixed but arbitrary integer $k \geq 2$.

Then $(\sigma A)^{k+1} = \sigma A(\sigma A)^k$

$$= \sigma A \sigma^k \sigma^{k-1}(A)\ldots\sigma(A)A$$

$$= \sigma\sigma^k\sigma^{-k} A \sigma^k \sigma^{k-1}(A)\ldots\sigma(A)A$$

$$= \sigma^{k+1}\sigma^k(A)\sigma^{k-1}(A)\ldots\sigma(A)A.$$

Thus, $(\sigma A)^m = \sigma^m\sigma^{m-1}(A)\ldots\sigma(A)A$ for any $m \geq 1$, as desired. In particular, we have $(\sigma A)^r = \sigma^r\sigma^{r-1}(A)\ldots\sigma(A)A = \sigma^{r-1}(A)\ldots\sigma(A)A$. More precisely,

$$(\sigma A)^r = \begin{bmatrix} 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_1) & & & * \\ & 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_2) & & \\ & & \ddots & \ddots & \\ & \text{0} & & 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_{n-1}) \\ & & & & 1 \end{bmatrix}.$$

Since the trace function is surjective, we can find $x_1, x_2, \ldots, x_{n-1}$ so that $\sum_{j=0}^{r-1}\sigma^j(x_i) = tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_i) = 1$ for $i = 1, 2, \ldots, n-1$. This yields that

$$(\sigma A)^r = \begin{bmatrix} 1 & 1 & & & * \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & 1 \\ & & & & 1 \end{bmatrix}. \text{ Notice that } \quad J = \begin{bmatrix} 1 & 1 & & & 0 \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & 1 \\ & & & & 1 \end{bmatrix} \text{ is the}$$

Jordan form of $(\sigma A)^r$.

We shall observe next that $C_G(J) = C_K(J)/Z(K)$. To see this, pick $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in K$ such that $CJ = \lambda JC$ for some $1 \neq \lambda \in \mathbb{F}_q^*$. Then we obtain

$$CJ = \begin{bmatrix} a_{11} & a_{11} + a_{12} & a_{12} + a_{13} & \dots & a_{1(n-1)} + a_{1n} \\ a_{21} & a_{21} + a_{22} & a_{22} + a_{23} & \dots & a_{2(n-1)} + a_{2n} \\ a_{31} & a_{31} + a_{32} & a_{32} + a_{33} & \dots & a_{3(n-1)} + a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n1} + a_{n2} & a_{n2} + a_{n3} & \dots & a_{n(n-1)} + a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \lambda a_{11} + \lambda a_{21} & \lambda a_{12} + \lambda a_{22} & \lambda a_{13} + \lambda a_{23} & \dots & \lambda a_{1n} + \lambda a_{2n} \\ \lambda a_{21} + \lambda a_{31} & \lambda a_{22} + \lambda a_{32} & \lambda a_{23} + \lambda a_{33} & \dots & \lambda a_{2n} + \lambda a_{3n} \\ \lambda a_{31} + \lambda a_{41} & \lambda a_{32} + \lambda a_{42} & \lambda a_{33} + \lambda a_{43} & \dots & \lambda a_{3n} + \lambda a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda a_{(n-1)1} + \lambda a_{n1} & \lambda a_{(n-1)2} + \lambda a_{n2} & \lambda a_{(n-1)3} + \lambda a_{n3} & \dots & \lambda a_{(n-1)n} + \lambda a_{nn} \\ \lambda a_{n1} & \lambda a_{n2} & \lambda a_{n3} & \dots & \lambda a_{nn} \end{bmatrix}$$

$$= \lambda JC.$$

It follows that $a_{n1} = \lambda a_{n1}$ and $a_{n(i-1)} + a_{ni} = \lambda a_{ni}$ for $i = 2, \dots, n$.

$a_{n1} = \lambda a_{n1}$ gives $a_{n1} = 0$ as $1 \neq \lambda$. Then $a_{n2} = \lambda a_{n2}$ and hence $a_{n2} = 0$. We may see by an inductive argument that $a_{ni} = 0$ for $i = 3, \dots, n$:

Assume $a_{n(i-1)} = 0$, then $a_{n(i-1)} + a_{ni} = \lambda a_{ni}$ becomes $a_{ni} = \lambda a_{ni}$ and hence $a_{ni} = 0$.

Consequently, if $1 \neq \lambda$ then $a_{ni} = 0$ for $i = 1, \dots, n$ which is a contradiction as in this case $\det(C) = 0$.

Therefore, we get $C_G(J) = C_K(J)/Z(K)$.

Let now $D = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in C_K(J)$. Then we obtain

$$DJ = \begin{bmatrix} a_{11} & a_{11} + a_{12} & a_{12} + a_{13} & \dots & a_{1(n-1)} + a_{1n} \\ a_{21} & a_{21} + a_{22} & a_{22} + a_{23} & \dots & a_{2(n-1)} + a_{2n} \\ a_{31} & a_{31} + a_{32} & a_{32} + a_{33} & \dots & a_{3(n-1)} + a_{3n} \\ : & : & : & & : \\ a_{n1} & a_{n1} + a_{n2} & a_{n2} + a_{n3} & \dots & a_{n(n-1)} + a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11} + a_{21} & a_{12} + a_{22} & a_{13} + a_{23} & \dots & a_{1n} + a_{2n} \\ a_{21} + a_{31} & a_{22} + a_{32} & a_{23} + a_{33} & \dots & a_{2n} + a_{3n} \\ a_{31} + a_{41} & a_{32} + a_{42} & a_{33} + a_{43} & \dots & a_{3n} + a_{4n} \\ : & : & : & & : \\ a_{(n-1)1} + a_{n1} & a_{(n-1)2} + a_{n2} & a_{(n-1)3} + a_{n3} & \dots & a_{(n-1)n} + a_{nn} \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} = JD.$$

In the first row, we have

$a_{11} = a11 + a_{21}$ and $a_{1(i-1)} + a_{1i} = a_{1i} + a_{2i}$ for $i = 2, \dots, n$. Then we get

$a_{21} = 0$ and $a_{1(i-1)} = a_{2i}$ for $i = 2, \dots, n$.

In the second row, we have

$0 = a_{31}$, $a_{22} = a_{22} + a_{32}$ and $a_{2(i-1)} + a_{2i} = a_{2i} + a_{3i}$ for $i = 3, \dots, n$. Then we get

$a_{31} = 0$, $a_{32} = 0$ and $a_{2(i-1)} = a_{3i}$ for $i = 2, \dots, n$.

In the third row, we have

$0 = a_{41}$, $0 = a_{42}$, $a_{33} = a_{33} + a_{43}$ and $a_{3(i-1)} + a_{3i} = a_{3i} + a_{4i}$ for $i = 4, \dots, n$. Then we get

$a_{41} = 0$, $a_{42} = 0$, $a_{43} = 0$ and $a_{3(i-1)} = a_{4i}$ for $i = 4, \dots, n$.

Continuing these calculations we can describe the matrix D more explicitly as follows:

$$D = \begin{bmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ 0 & \ddots & \ddots & & a_{n-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & a_2 \\ 0 & \dots & \dots & 0 & a_1 \end{bmatrix}$$

Consequently, $|C_K((\sigma A)^r)| = |C_K(J)| = (n, q-1)q^{n-1}$ and hence

$|G : C_G((\sigma A)^r)| = \dfrac{q^{n(n-1)/2}\prod_{i=2}^{n}(q^i-1)}{q^{n-1}} = q^{(n^2-3n+2)/2}\prod_{i=2}^{n}(q^i-1)$ is divisible by 4. This completes the proof of Lemma 3.2.6. ■

Lemma 3.2.7 *Let σ be the graph automorphism of G. Then there is an element $x \in G\langle\sigma\rangle \setminus G$ so that* 4 *divides* $|G : C_G(x)|$.

Proof. Let $A = \begin{bmatrix} 0 & 1 & \\ -1 & 1 & 0 \\ 0 & & I_{n-2} \end{bmatrix} \in K$. Then $A^{-t} = \begin{bmatrix} 1 & 1 & \\ -1 & 0 & 0 \\ 0 & & I_{n-2} \end{bmatrix}$

and $B = AA^{-t} = \begin{bmatrix} -1 & 0 & \\ -2 & -1 & 0 \\ 0 & & I_{n-2} \end{bmatrix}$.

We shall observe that $C_G(B) = C_{K/Z(K)}(B) = C_K(B)/Z(K)$:

Let $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in K$ be such that $CB = \lambda BC$ for some $1 \neq \lambda \in \mathbb{F}_q^*$. Then we obtain

$$CB = \begin{bmatrix} -a_{11} & -a_{12} & -a_{13} & \dots & -a_{1n} \\ -2a_{11}-a_{21} & -2a_{12}-a_{22} & -2a_{13}-a_{23} & \dots & -2a_{1n}-a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} -\lambda a_{11} - 2\lambda a_{12} & -\lambda a_{12} & \lambda a_{13} & \dots & \lambda a_{1n} \\ -\lambda a_{21} - 2\lambda a_{22} & -\lambda a_{22} & \lambda a_{23} & \dots & \lambda a_{2n} \\ -\lambda a_{31} - 2\lambda a_{32} & -\lambda a_{32} & \lambda a_{33} & \dots & \lambda a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ -\lambda a_{n1} - 2\lambda a_{n2} & -\lambda a_{n2} & \lambda a_{n3} & \dots & \lambda a_{nn} \end{bmatrix} = \lambda BC.$$

As $\lambda \neq 1$ and $-a_{12} = -\lambda a_{12}$ we get $a_{12} = 0$ and hence $-a_{11} = -\lambda a_{11}$. It follows that $a_{11} = 0$.

If $\lambda \neq -1$ then $-a_{1i} = \lambda a_{1i}$ gives $a_{1i} = 0$ for each $i = 3, \dots, n$. It is now straightforward to verify that $\det C = 0$, a contradiction. Hence $\lambda = -1$.

As $-2a_{1i} - a_{2i} = \lambda a_{2i}$ for each $i = 3, \dots, n$, we get $a_{1i} = 0$ for each $i = 3, \dots, n$, and hence $\det C = 0$ again, which is a contradiction. Thus $C_G(B) = C_K(B)/Z(K)$, as claimed.

Let now $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in C_K(B)$. Then we have

$$CB = \begin{bmatrix} -a_{11} & -a_{12} & -a_{13} & \dots & -a_{1n} \\ -2a_{11} - a_{21} & -2a_{12} - a_{22} & -2a_{13} - a_{23} & \dots & -2a_{1n} - a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} -a_{11} - 2a_{12} & -a_{12} & a_{13} & \dots & a_{1n} \\ -a_{21} - 2a_{22} & -a_{22} & a_{23} & \dots & a_{2n} \\ -a_{31} - 2a_{32} & -a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ -a_{n1} - 2a_{n2} & -a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} = BC.$$

This leads to the equations, $-a_{1i} = a_{1i}$ and $a_{i2} = -a_{i2}$ for each $i = 3, \dots, n$. Hence $a_{1i} = 0$ and $a_{i2} = 0$ implying that $-a_{2i} = a_{2i}$ and $-a_{i1} = a_{i1}$ for each $i = 3, \dots, n$. Thus $a_{i1} = 0$ and $a_{2i} = 0$ for each $i = 3, \dots, n$.

Notice also that $-2a_{11} - a_{21} = -a_{21} - 2a_{22}$ gives $a_{11} = a_{22}$ and also that $-2a_{12} - a_{22} = -a_{22}$

gives $a_{12} = 0$.

This argument enables us to give a more precise description of $C_K(B)$, namely we have

$$C_K(B) = \left\{ \begin{bmatrix} a_{11} & 0 & & \mathbf{0} & \\ a_{21} & a_{11} & & & \\ & & a_{33} & \dots & a_{3n} \\ & \mathbf{0} & \vdots & & \vdots \\ & & a_{n3} & \dots & a_{nn} \end{bmatrix} \mid a_{ij} \in \mathbb{F}_q \right\}.$$

It follows that $|C_K(B)| = q(q-1)|SL(n-2, \mathbb{F}_q)|$

$$= q(q-1)q^{(n-2)(n-3)/2} \prod_{i=2}^{n-2} (q^i - 1)$$

$$= (q-1)q^{(n^2-5n+8)/2} \prod_{i=2}^{n-2} (q^i - 1)$$

and hence $|C_G(B)| = \frac{q-1}{(n,q-1)} q^{(n^2-5n+8)/2} \prod_{i=2}^{n-2} (q^i - 1)$.

Consequently, $|G : C_G(B)| = \dfrac{\frac{1}{(n,q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1)}{\frac{q-1}{(n,q-1)} q^{(n^2-5n+8)/2} \prod_{i=2}^{n-2} (q^i - 1)}$

$$= \tfrac{1}{q-1} q^{2n-4} (q^n - 1)(q^{n-1} - 1)$$

If $char \mathbb{F}_q = 2$, we see that $2^{2.3-4} = 4$ divides $|G : C_G(B)|$ as $n \geq 3$. Thus, we may assume that q is odd.

If $n = 2k$ for some integer $k \geq 2$, then $|G : C_G(B)| = \frac{1}{q-1} q^{2n-4} (q^k - 1)(q^k + 1)(q^{n-1} - 1)$ which is divisible by $(q^k + 1)(q^{n-1} - 1)$ as $q - 1$ divides $q^k - 1$. Since both $q^k + 1$ and $q^{n-1} - 1$ are even, $|G : C_G(B)|$ is divisible by 4.

If $n = 2k + 1$ for some integer $k \geq 1$, then $|G : C_G(B)| = \frac{1}{q-1} q^{2n-4} (q^n - 1)(q^k + 1)(q^k - 1)$ is divisible by $(q^k + 1)(q^n - 1)$ as $q - 1$ divides $q^k - 1$. Since both $q^k + 1$ and $q^n - 1$ are even, $|G : C_G(B)|$ is divisible by 4. This completes the proof. ■

Lemma 3.2.8 *Let q be odd. If α is a diagonal automorphism of G and σ is the graph automorphism of G, then there is an element $x \in G\langle\alpha\sigma\rangle \setminus G$ so that 4 divides $|G : C_G(x)|$.*

Proof. We observe that n is even as the order of a diagonal automorphism in $Out(G)$ divides $gcd(n, q-1)$. Let $A = \begin{bmatrix} \begin{matrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{matrix} & 0 \\ 0 & I_{n-3} \end{bmatrix}$. As $\det A = -1$, there is an inner automorphism τ_g of K such that $\tau_g\alpha = \tau_A$. Let σ be the graph automorphism of G and set $B = A\sigma A\sigma$. That is, $B = AA^{-t}$ where $B = \begin{bmatrix} \begin{matrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & -1 & 1 \end{matrix} & 0 \\ 0 & I_{n-3} \end{bmatrix}$ as $A^{-t} = \begin{bmatrix} \begin{matrix} -1 & -1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{matrix} & 0 \\ 0 & I_{n-3} \end{bmatrix}$.

We will observe next that $C_G(B) = C_K(B)/Z(K)$:

To see this, pick $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$ from K such that $BC = \lambda CB$ for some $1 \neq \lambda \in \mathbb{F}_q^*$.

Now, we have

$$BC = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \dots & a_{1n} \\ a_{11}+a_{21} & a_{12}+a_{22} & a_{13}+a_{23} & a_{14}+a_{24} & \dots & a_{1n}+a_{2n} \\ -a_{21}+a_{31} & -a_{22}+a_{32} & -a_{23}+a_{33} & -a_{24}+a_{34} & \dots & -a_{2n}+a_{3n} \\ a_{41} & a_{42} & a_{43} & a_{44} & \dots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \lambda a_{11} + \lambda a_{12} & \lambda a_{12} - \lambda a_{13} & \lambda a_{13} & \lambda a_{14} & \dots & \lambda a_{1n} \\ \lambda a_{21} + \lambda a_{22} & \lambda a_{22} - \lambda a_{23} & \lambda a_{23} & \lambda a_{24} & \dots & \lambda a_{2n} \\ \lambda a_{31} + \lambda a_{32} & \lambda a_{32} - \lambda a_{33} & \lambda a_{33} & \lambda a_{34} & \dots & \lambda a_{3n} \\ \lambda a_{41} + \lambda a_{42} & \lambda a_{42} - \lambda a_{43} & \lambda a_{43} & \lambda a_{44} & \dots & \lambda a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda a_{n1} + \lambda a_{n2} & \lambda a_{n2} - \lambda a_{n3} & \lambda a_{n3} & \lambda a_{n4} & \dots & \lambda a_{nn} \end{bmatrix} = \lambda CB.$$

Then $a_{ni} = \lambda a_{ni}$ and hence $a_{ni} = 0$ for each $i = 3, \dots, n$. This forces that $a_{n2} = \lambda a_{n2}$ implying $a_{n2} = 0$. Thus $a_{n1} = \lambda a_{n1}$ and so $a_{n1} = 0$. Consequently, we obtain $C_G(B) = C_K(B)/Z(K)$, as desired.

Let now $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in K$ be such that $BC = CB$.

Then $BC = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \dots & a_{1n} \\ a_{11} + a_{21} & a_{12} + a_{22} & a_{13} + a_{23} & a_{14} + a_{24} & \dots & a_{1n} + a_{2n} \\ -a_{21} + a_{31} & -a_{22} + a_{32} & -a_{23} + a_{33} & -a_{24} + a_{34} & \dots & -a_{2n} + a_{3n} \\ a_{41} & a_{42} & a_{43} & a_{44} & \dots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \dots & a_{nn} \end{bmatrix}$

$$= \begin{bmatrix} a_{11} + a_{12} & a_{12} - a_{13} & a_{13} & a_{14} & \dots & a_{1n} \\ a_{21} + a_{22} & a_{22} - a_{23} & a_{23} & a_{24} & \dots & a_{2n} \\ a_{31} + a_{32} & a_{32} - a_{33} & a_{33} & a_{34} & \dots & a_{3n} \\ a_{41} + a_{42} & a_{42} - a_{43} & a_{43} & a_{44} & \dots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} + a_{n2} & a_{n2} - a_{n3} & a_{n3} & a_{n4} & \dots & a_{nn} \end{bmatrix} = CB.$$

Notice that $a_{11} = a_{11} + a_{12}$ giving $a_{12} = 0$. It follows that $a_{13} = 0$. We also have

$a_{11} + a_{21} = a_{21} + a_{22}$ and hence $a_{11} = a_{22}$.

The equation $a_{12} + a_{22} = a_{22} - a_{23}$ implies $a_{12} = -a_{23}$ and hence $a_{23} = 0$.

Moreover, we have the equations $a_{1i} + a_{2i} = a_{2i}$ for $i = 3, \ldots, n$. It follows that $a_{1i} = 0$ for $i = 3, \ldots, n$.

We also have $-a_{21} + a_{31} = a_{31} + a_{32}$ which forces $-a_{21} = a_{32}$.

The equation $-a_{22} + a_{32} = a_{32} - a_{33}$ holds and so $a_{22} = a_{33}$.

Moreover we have $-a_{2i} + a_{3i} = a_{3i}$ for $i = \ldots, n$ giving $a_{2i} = 0$ for $i = 3, \ldots, n$.

Finally, we have $a_{i1} = a_{i1} + a_{i2}$ and $a_{i2} = a_{i2} - a_{i3}$ for $i = 4, \ldots, n$ implying $a_{i2} = 0$ and $a_{i3} = 0$ for $i = 4, \ldots, n$, respectively.

The above observation provides a more precise description of $C_K(B)$; namely

$$C_K(B) = \left\{ \begin{bmatrix} a_{11} & 0 & 0 & 0 & \ldots & 0 \\ a_{21} & a_{11} & 0 & 0 & \ldots & 0 \\ a_{31} & -a_{21} & a_{11} & a_{34} & \ldots & a_{3n} \\ a_{41} & 0 & 0 & a_{44} & \ldots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & 0 & 0 & a_{n4} & \ldots & a_{nn} \end{bmatrix} \in K \mid a_{ij} \in \mathbb{F}_q \right\}. \tag{3.16}$$

Then $|C_K(B)| = q^{n-1}.q^{n-3}.(q-1).|SL(n-3, \mathbb{F}_q)| = (q-1).q^{2n-4}.q^{(n-3)(n-4)/2}.\prod_{i=2}^{n-3}(q^i - 1)$

and hence

$$|G : C_G(B)| = |K : C_K(B)| = \frac{q^{n(n-1)/2}\prod_{i=2}^{n}(q^i - 1)}{(q-1)q^{2n-4}q^{(n-3)(n-4)/2}\prod_{i=2}^{n-3}(q^i - 1)} \tag{3.17}$$

$$= q^{n-2}\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)}{q-1}$$

which is divisible by 4. This completes the proof. ■

Lemma 3.2.9 *Let char*$(\mathbb{F}_q) = 2$. *If* α *is a diagonal automorphism of* G *and* σ *is the graph automorphism of* G, *then there is an element* $x \in G\langle\alpha\sigma\rangle \setminus G$ *so that* 4 *divides* $|G : C_G(x)|$.

Proof. We observe that n is odd as the order of a diagonal automorphism in $Out(G)$ divides

$gcd(n, q-1)$. Let $A = \left[\begin{array}{ccc|c} 0 & 0 & 1 & \\ 0 & c & 1 & \mathbf{0} \\ 1 & 0 & 1 & \\ & & & \\ & \mathbf{0} & & I_{n-3} \end{array}\right]$ where $c \in \mathbb{F}_q \setminus \{0, 1\}$.

As $\det A = c$, there is an element $g \in K$ which induces the inner automorphism τ_g of K such that $\tau_g \alpha = \tau_A$. Let σ be the graph automorphism of G and set $B = A\sigma A\sigma$. That is,

$$B = AA^{-t} \text{ where } B = \left[\begin{array}{ccc|c} 1 & 0 & 0 & \\ 1 & 1 & 0 & \mathbf{0} \\ 0 & c^{-1} & 1 & \\ & & & \\ & \mathbf{0} & & I_{n-3} \end{array}\right] \text{ as } A^{-t} = \left[\begin{array}{ccc|c} 1 & c^{-1} & 1 & \\ 0 & c^{-1} & 0 & \mathbf{0} \\ 1 & 0 & 0 & \\ & & & \\ & \mathbf{0} & & I_{n-3} \end{array}\right].$$

We will observe next that $C_G(B) = C_K(B)/Z(K)$. To see this, pick $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$ from K such that $BC = \lambda CB$ for some $1 \neq \lambda \in \mathbb{F}_q^*$. Now, we have

$$BC = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \dots & a_{1n} \\ a_{11} + a_{21} & a_{12} + a_{22} & a_{13} + a_{23} & a_{14} + a_{24} & \dots & a_{1n} + a_{2n} \\ c^{-1}a_{21} + a_{31} & c^{-1}a_{22} + a_{32} & c^{-1}a_{23} + a_{33} & c^{-1}a_{24} + a_{34} & \dots & c^{-1}a_{2n} + a_{3n} \\ a_{41} & a_{42} & a_{43} & a_{44} & \dots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \dots & a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \lambda a_{11} + \lambda a_{12} & \lambda a_{12} + c^{-1}\lambda a_{13} & \lambda a_{13} & \lambda a_{14} & \dots & \lambda a_{1n} \\ \lambda a_{21} + \lambda a_{22} & \lambda a_{22} + c^{-1}\lambda a_{23} & \lambda a_{23} & \lambda a_{24} & \dots & \lambda a_{2n} \\ \lambda a_{31} + \lambda a_{32} & \lambda a_{32} + c^{-1}\lambda a_{33} & \lambda a_{33} & \lambda a_{34} & \dots & \lambda a_{3n} \\ \lambda a_{41} + \lambda a_{42} & \lambda a_{42} + c^{-1}\lambda a_{43} & \lambda a_{43} & \lambda a_{44} & \dots & \lambda a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \lambda a_{n1} + \lambda a_{n2} & \lambda a_{n2} + c^{-1}\lambda a_{n3} & \lambda a_{n3} & \lambda a_{n4} & \dots & \lambda a_{nn} \end{bmatrix} = \lambda CB.$$

Then $a_{ni} = \lambda a_{ni}$ and hence $a_{ni} = 0$ for each $i = 3, \ldots, n$. This forces that $a_{n2} = \lambda a_{n2}$ implying $a_{n2} = 0$. Thus $a_{n1} = \lambda a_{n1}$ and so $a_{n1} = 0$.

Consequently, we obtain $C_G(B) = C_K(B)/Z(K)$, as desired.

Let now $C = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \in K$ be such that $BC = CB$.

Then $BC = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & \ldots & a_{1n} \\ a_{11}+a_{21} & a_{12}+a_{22} & a_{13}+a_{23} & a_{14}+a_{24} & \ldots & a_{1n}+a_{2n} \\ c^{-1}a_{21}+a_{31} & c^{-1}a_{22}+a_{32} & c^{-1}a_{23}+a_{33} & c^{-1}a_{24}+a_{34} & \ldots & c^{-1}a_{2n}+a_{3n} \\ a_{41} & a_{42} & a_{43} & a_{44} & \ldots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & a_{n3} & a_{n4} & \ldots & a_{nn} \end{bmatrix}$

$$= \begin{bmatrix} a_{11}+a_{12} & a_{12}+c^{-1}a_{13} & a_{13} & a_{14} & \ldots & a_{1n} \\ a_{21}+a_{22} & a_{22}+c^{-1}a_{23} & a_{23} & a_{24} & \ldots & a_{2n} \\ a_{31}+a_{32} & a_{32}+c^{-1}a_{33} & a_{33} & a_{34} & \ldots & a_{3n} \\ a_{41}+a_{42} & a_{42}+c^{-1}a_{43} & a_{43} & a_{44} & \ldots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1}+a_{n2} & a_{n2}+c^{-1}a_{n3} & a_{n3} & a_{n4} & \ldots & a_{nn} \end{bmatrix} = CB.$$

Notice that $a_{11} = a_{11} + a_{12}$ giving $a_{12} = 0$. It follows that $a_{13} = 0$. We also have

$a_{11} + a_{21} = a_{21} + a_{22}$ and hence $a_{11} = a_{22}$.

The equation $a_{12} + a_{22} = a_{22} + c^{-1}a_{23}$ implies $a_{12} = c^{-1}a_{23}$ and hence $a_{23} = 0$.

Moreover, we have the equations $a_{1i} + a_{2i} = a_{2i}$ for $i = 3, \ldots, n$. It follows that $a_{1i} = 0$ for $i = 3, \ldots, n$.

We also have $c^{-1}a_{21} + a_{31} = a_{31} + a_{32}$ which forces $c^{-1}a_{21} = a_{32}$.

The equation $c^{-1}a_{22} + a_{32} = a_{32} + c^{-1}a_{33}$ holds and so $a_{22} = a_{33}$.

Moreover we have $c^{-1}a_{2i} + a_{3i} = a_{3i}$ for $i = \ldots, n$ giving $a_{2i} = 0$ for $i = 3, \ldots, n$.

Finally, we have $a_{i1} = a_{i1} + a_{i2}$ and $a_{i2} = a_{i2} + c^{-1}a_{i3}$ for $i = 4, \ldots, n$ implying $a_{i2} = 0$ and $a_{i3} = 0$ for $i = 4, \ldots, n$, respectively.

The above observation provides a more precise description of $C_K(B)$, that is,

$$C_K(B) = \left\{ \begin{bmatrix} a_{11} & 0 & 0 & 0 & \ldots & 0 \\ a_{21} & a_{11} & 0 & 0 & \ldots & 0 \\ a_{31} & c^{-1}a_{21} & a_{11} & a_{34} & \ldots & a_{3n} \\ a_{41} & 0 & 0 & a_{44} & \ldots & a_{4n} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & 0 & 0 & a_{n4} & \ldots & a_{nn} \end{bmatrix} \in K \mid a_{ij} \in \mathbb{F}_q \right\}.$$

Then

$$|C_K(B)| = q^{n-1}.q^{n-3}.(q-1).|SL(n-3, \mathbb{F}_q)| = (q-1).q^{2n-4}.q^{(n-3)(n-4)/2}.\prod_{i=2}^{n-3}(q^i - 1) \quad (3.18)$$

and hence

$$|G : C_G(B)| \quad = \quad |K : C_K(B)| \quad = \quad \frac{q^{n(n-1)/2}\prod_{i=2}^{n}(q^i - 1)}{(q-1)q^{2n-4}q^{(n-3)(n-4)/2}\prod_{i=2}^{n-3}(q^i - 1)} \quad (3.19)$$

$$= \quad q^{n-2}\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)}{q-1}$$

which is divisible by 4. This completes the proof. ■

Lemma 3.2.10 *Let α be a field automorphism of G and let σ be the graph automorphism of G. Then there is an element $x \in G\langle\alpha\sigma\rangle \setminus G$ so that 4 divides $|G : C_G(x)|$.*

Proof. Assume first that $|\alpha|$ is odd. As the graph automorphism commutes with every field automorphism, σ is a power of $\alpha\sigma$ and the result follows by Lemma 3.2.7. Thus we may assume that $|\alpha|$ is even. If $|\alpha| \neq 2$, then $(\alpha\sigma)^2 = \alpha^2$ and the result follows by Lemma 3.2.5 and Lemma 3.2.6. Thus, $|\alpha| = 2$.

Let $A = \begin{bmatrix} \begin{matrix} 0 & 1 \\ -1 & 1 \end{matrix} & 0 \\ 0 & I_{n-2} \end{bmatrix} \in K$. Then $A^{-t} = \begin{bmatrix} \begin{matrix} 1 & 1 \\ -1 & 0 \end{matrix} & 0 \\ 0 & I_{n-2} \end{bmatrix}$.

Notice that $(A\alpha\sigma)^2 = A\alpha\sigma A\alpha\sigma = A\sigma\alpha A\alpha\sigma = A\sigma A\sigma = AA^{-t}$. To simplify the notation we set $B = AA^{-t}$. Then $B = \begin{bmatrix} -1 & 0 & & \\ -2 & -1 & & \mathbf{0} \\ & & & \\ & \mathbf{0} & & I_{n-2} \end{bmatrix}$.

Here, we have to note that from now on one can proceed as in the proof of Lemma 3.2.7 following the same notation and see that $|G : C_G(B)|$ is divisible by 4. ■

Lemma 3.2.11 *Let q be odd. If α is a diagonal automorphism and σ is a field automorphism of G, then there is an element $x \in G\langle\sigma\alpha\rangle \setminus G$ so that* 4 *divides* $|G : C_G(x)|$.

Proof. Set $\alpha A = \begin{bmatrix} 1 & x_1 & & & & \\ & 1 & x_2 & & & \mathbf{0} \\ & & \ddots & \ddots & & \\ & & & & 1 & x_{n-1} \\ & \mathbf{0} & & & & -1 \end{bmatrix}$. Let σ be the field automorphism of K of order r which is induced from the automorphism of $\mathbb{F}_q$ of order r with fixed field $\mathbb{F}_{q_0}$. We observe that

$$(\sigma\alpha A)^2 = (\sigma\alpha A)(\sigma\alpha A) = \sigma\sigma\sigma^{-1}\alpha A\sigma\alpha A = \sigma^2\sigma(\alpha A)\alpha A. \tag{3.20}$$

Assume next that

$$(\sigma\alpha A)^k = \sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \tag{3.21}$$

for a fixed but arbitrary integer $k \geq 2$.

Then $(\sigma\alpha A)^{k+1} = \sigma\alpha A(\sigma\alpha A)^k$

$$= \sigma\alpha A\sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A$$

$$= \sigma\sigma^k\sigma^{-k}\alpha A\sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A$$

$$= \sigma^{k+1}\sigma^k(\alpha A)\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A.$$

It follows by induction that

$$(\sigma\alpha A)^k = \sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \tag{3.22}$$

for any integer $k \geq 1$. In particular,

$$(\sigma\alpha A)^r = \sigma^r\sigma^{r-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A = \sigma^{r-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A. \tag{3.23}$$

Pick now $B = \begin{bmatrix} 1 & y_1 & & & * \\ & 1 & y_2 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & y_{n-1} \\ & & & & 1 \end{bmatrix}$ and $E = \begin{bmatrix} 1 & z_1 & & & * \\ & 1 & z_2 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & z_{n-1} \\ & & & & -1 \end{bmatrix}$

from K. Then $\alpha AB = \begin{bmatrix} 1 & x_1 + y_1 & & & * \\ & 1 & x_2 + y_2 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & x_{n-1} + y_{n-1} \\ & & & & -1 \end{bmatrix}$ and

$\alpha AE = \begin{bmatrix} 1 & x_1 + z_1 & & & * \\ & 1 & x_2 + z_2 & & \\ & & \ddots & \ddots & \\ & 0 & & 1 & x_{n-1} + z_{n-1} \\ & & & & 1 \end{bmatrix}$. It follows that

$$(\sigma\alpha A)^r = \begin{bmatrix} 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_1) & & & & * \\ & 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_2) & & & \\ & & & \ddots & \ddots & \\ & & & & 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(-x_{n-1}) \\ & \text{0} & & & & (-1)^r \end{bmatrix}.$$

Since the trace function is surjective, we can find $x_1, x_2, \ldots, x_{n-1}$ in $\mathbb{F}_q$ so that

$tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_i) = 1$ for each $i = 1, \ldots, n-1$. Then $(\sigma\alpha A)^r = \begin{bmatrix} 1 & 1 & & & & * \\ & 1 & 1 & & & \\ & & & \ddots & \ddots & \\ & & & & 1 & 1 \\ & 0 & & & & (-1)^r \end{bmatrix}$.

If r is even then the Jordan form of $(\sigma\alpha A)^r$ is $J = \begin{bmatrix} 1 & 1 & & & & 0 \\ & 1 & 1 & & & \\ & & & \ddots & \ddots & \\ & & & & 1 & \\ & 0 & & & 1 & 1 \\ & & & & & 1 \end{bmatrix}$. Then using the same notation and following the same steps as in Lemma 3.2.6, it is easy to show that 4 divides $|G : C_G((\sigma A)^r)| = |G : C_G(J)|$.

Next consider the case where r is odd. Then the Jordan form of $(\sigma\alpha A)^r$ is

$$J = \begin{bmatrix} 1 & 1 & & & & \text{\Large 0} & \\ & 1 & 1 & & & & \\ & & & \ddots & \ddots & & \\ & & & & & 1 & \\ & \text{\Large 0} & & & & 1 & 0 \\ & & & & & & -1 \end{bmatrix}.$$

We shall observe next that $C_G(J) = C_K(J)/Z(K)$. To see this pick $C = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in K$

such that $CJ = \lambda JC$ for some $1 \neq \lambda \in \mathbb{F}_q^*$. Then we obtain

$$CJ = \begin{bmatrix} a_{11} & a_{11} + a_{12} & \dots & a_{1(n-2)} + a_{1(n-1)} & -a_{1n} \\ a_{21} & a_{21} + a_{22} & \dots & a_{2(n-2)} + a_{2(n-1)} & -a_{2n} \\ a_{31} & a_{31} + a_{32} & \dots & a_{3(n-2)} + a_{3(n-1)} & -a_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{(n-1)1} & a_{(n-1)1} + a_{(n-1)2} & \dots & a_{(n-1)(n-2)} + a_{(n-1)(n-1)} & -a_{(n-1)n} \\ a_{n1} & a_{n1} + a_{n2} & \dots & a_{n(n-2)} + a_{n(n-1)} & -a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \lambda a_{11} + \lambda a_{21} & \lambda a_{12} + \lambda a_{22} & \lambda a_{13} + \lambda a_{23} & \dots & \lambda a_{1n} + \lambda a_{2n} \\ \lambda a_{21} + \lambda a_{31} & \lambda a_{22} + \lambda a_{32} & \lambda a_{23} + \lambda a_{33} & \dots & \lambda a_{2n} + \lambda a_{3n} \\ \lambda a_{31} + \lambda a_{41} & \lambda a_{32} + \lambda a_{42} & \lambda a_{33} + \lambda a_{43} & \dots & \lambda a_{3n} + \lambda a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda a_{(n-1)1} & \lambda a_{(n-1)2} & \lambda a_{(n-1)3} & \dots & \lambda a_{(n-1)n} \\ -\lambda a_{n1} & -\lambda a_{n2} & -\lambda a_{n3} & \dots & -\lambda a_{nn} \end{bmatrix} = \lambda JC.$$

Now, $a_{n1} = -\lambda a_{n1}$. If $\lambda \neq -1$, then $a_{n1} = 0$. It follows that $a_{n2} = -\lambda a_{n2}$, which gives $a_{n2} = 0$. Continuing in this manner we get $a_{ni} = 0$ for $i = 1, \dots, n-1$. We also have $-a_{nn} = -\lambda a_{nn}$ which gives $a_{nn} = 0$. Thus $\det(C) = 0$, a contradiction. Therefore, $\lambda = -1$.

Then we have the equality

$$CJ = \begin{bmatrix} a_{11} & a_{11}+a_{12} & \dots & a_{1(n-2)}+a_{1(n-1)} & -a_{1n} \\ a_{21} & a_{21}+a_{22} & \dots & a_{2(n-2)}+a_{2(n-1)} & -a_{2n} \\ a_{31} & a_{31}+a_{32} & \dots & a_{3(n-2)}+a_{3(n-1)} & -a_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{(n-1)1} & a_{(n-1)1}+a_{(n-1)2} & \dots & a_{(n-1)(n-2)}+a_{(n-1)(n-1)} & -a_{(n-1)n} \\ a_{n1} & a_{n1}+a_{n2} & \dots & a_{n(n-2)}+a_{n(n-1)} & -a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} -a_{11}-a_{21} & -a_{12}-a_{22} & -a_{13}-a_{23} & \dots & -a_{1n}-a_{2n} \\ -a_{21}-a_{31} & -a_{22}-a_{32} & -a_{23}-a_{33} & \dots & -a_{2n}-a_{3n} \\ -a_{31}-a_{41} & -a_{32}-a_{42} & -a_{33}-a_{43} & \dots & -a_{3n}-a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ -a_{(n-1)1} & -a_{(n-1)2} & -a_{(n-1)3} & \dots & -a_{(n-1)n} \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} = \lambda JC.$$

In the first column, we have

$a_{i1} = -a_{i1} - a_{(i+1)1}$ for $i = 1, \dots, n-2$ and $a_{(n-1)1} = -a_{(n-1)1}$. Then we get

$a_{i1} = 0$ for $i = 1, \dots, n-1$.

In the second column, we have

$a_{i2} = -a_{i2} - a_{(i+1)2}$ for $i = 1, \dots, n-2$, $a_{(n-1)2} = -a_{(n-1)2}$ and $a_{n1} + a_{n2} = a_{n2}$. Then we get

$a_{i2} = 0$ for $i = 1, \dots, n-1$ and either $a_{n1} = 0$ or $a_{n2} = 0$. This means that either first or second column is a zero column and so $\det(C) = 0$, a contradiction. Therefore, we get $C_G(J) = C_K(J)/Z(K)$.

Let now $D = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in C_K(J)$. Then we obtain

$$DJ = \begin{bmatrix} a_{11} & a_{11}+a_{12} & a_{12}+a_{13} & \dots & a_{1(n-2)}+a_{1(n-1)} & -a_{1n} \\ a_{21} & a_{21}+a_{22} & a_{22}+a_{23} & \dots & a_{2(n-2)}+a_{2(n-1)} & -a_{2n} \\ a_{31} & a_{31}+a_{32} & a_{32}+a_{33} & \dots & a_{3(n-2)}+a_{3(n-1)} & -a_{3n} \\ \vdots & \vdots & \vdots & & \vdots & \\ a_{n1} & a_{n1}+a_{n2} & a_{n2}+a_{n3} & \dots & a_{n(n-2)}+a_{n(n-1)} & -a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}+a_{21} & a_{12}+a_{22} & a_{13}+a_{23} & \dots & a_{1n}+a_{2n} \\ a_{21}+a_{31} & a_{22}+a_{32} & a_{23}+a_{33} & \dots & a_{2n}+a_{3n} \\ a_{31}+a_{41} & a_{32}+a_{42} & a_{33}+a_{43} & \dots & a_{3n}+a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)3} & \dots & a_{(n-1)n} \\ -a_{n1} & -a_{n2} & -a_{n3} & \dots & -a_{nn} \end{bmatrix} = JD.$$

In the first row, we have

$a_{11} = a11 + a_{21}$, $a_{1(i-1)} + a_{1i} = a_{1i} + a_{2i}$ for $i = 2, \dots, n-1$ and $-a_{1n} = a_{1n} + a_{2n}$. Then we get

$a_{21} = 0$, $a_{1(i-1)} = a_{2i}$ for $i = 2, \dots, n-1$ and $a_{2n} = -2a_{1n}$.

In the second row, we have

$0 = a_{31}$, $a_{22} = a_{22} + a_{32}$, $a_{2(i-1)} + a_{2i} = a_{2i} + a_{3i}$ for $i = 3, \dots, n-1$ and $-a_{2n} = a_{2n} + a_{3n}$. Then we get

$a_{31} = 0$, $a_{32} = 0$, $a_{2(i-1)} = a_{3i}$ for $i = 2, \dots, n-1$ and $a_{3n} = -2a_{2n}$.

In the third row, we have

$0 = a_{41}$, $0 = a_{42}$, $a_{33} = a_{33} + a_{43}$, $a_{3(i-1)} + a_{3i} = a_{3i} + a_{4i}$ for $i = 4, \dots, n-1$ and $-a_{3n} = a_{3n} + a_{4n}$. Then we get

$a_{41} = 0$, $a_{42} = 0$, $a_{43} = 0$, $a_{3(i-1)} = a_{4i}$ for $i = 4, \dots, n$ and $a_{3n} = -2a_{3n}$.

Continuing these calculations along first $n-1$ rows we get $a_{ij} = 0$ for $1 \le j < i \le n-1$ and $a_{in} = 0$ for $i = 1, \dots, n-1$.

In the last row, we have

$a_{n1} = -a_{n1}$, $a_{n(i-1)} + a_{ni} = -a_{ni}$ for $i = 2, \dots, n-1$. Then we get

$a_{ni} = 0$ for $i = 1, \dots, n-1$.

$$\text{Consequently, we obtained } D = \begin{bmatrix} a_1 & a_2 & & & a_{n-2} & a_{n-1} & 0 \\ & a_1 & & & & a_{n-2} & 0 \\ & & \ddots & \ddots & & & \\ & & & & & & \\ & & & & a_1 & a_2 & 0 \\ & \mathbf{0} & & & & a_1 & 0 \\ & & & & & & a_n \end{bmatrix}$$

It is easy now to observe that $|C_K((\sigma A)^r)| = (q-1)q^{n-2}$ and hence

$$|G : C_G((\sigma A)^r)| = \frac{q^{n(n-1)/2}\prod_{i=2}^{n}(q^i - 1)}{(q-1)q^{n-2}} = \frac{1}{q-1} q^{(n^2-3n+4)/2} \prod_{i=2}^{n}(q^i - 1) \text{ is divisible by 4, as desired.}$$

■

Lemma 3.2.12 *Let char* $(\mathbb{F}_q) = 2$*. If* α *is a diagonal automorphism and* σ *is a field automorphism of* G*, then there is an element* $x \in G\langle\sigma\alpha\rangle \setminus G$ *so that* 4 *divides* $|G : C_G(x)|$.

Proof. Let $q = 2^{ar}$ for some integer a and

$$\alpha A = \begin{bmatrix} 1 & x_1 & & & & \\ & 1 & x_2 & & \mathbf{0} & \\ & & \ddots & \ddots & & \\ & & & & x_{n-2} & 0 \\ & \mathbf{0} & & & 1 & 0 \\ & & & & & c \end{bmatrix}$$

, where $c \in \mathbb{F}_{||}$ and $c^{1+2^a+2^{2a}+\ldots+2^{a(r-1)}} \neq 1$. Let σ be the field automorphism of K of order r which is induced from the automorphism of $\mathbb{F}_q$ of order r with fixed field $\mathbb{F}_{q_0}$. We observe that

$$(\sigma\alpha A)^2 = (\sigma\alpha A)(\sigma\alpha A) = \sigma\sigma\sigma^{-1}\alpha A\sigma\alpha A = \sigma^2\sigma(\alpha A)\alpha A. \tag{3.24}$$

Assume next that

$$(\sigma\alpha A)^k = \sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \tag{3.25}$$

for a fixed but arbitrary integer $k \geq 2$.

$$\begin{aligned}\text{Then } (\sigma\alpha A)^{k+1} &= \sigma\alpha A(\sigma\alpha A)^k \\ &= \sigma\alpha A\sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \\ &= \sigma\sigma^k\sigma^{-k}\alpha A\sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \\ &= \sigma^{k+1}\sigma^k(\alpha A)\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A\end{aligned}$$

It follows by induction that

$$(\sigma\alpha A)^k = \sigma^k\sigma^{k-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A \tag{3.26}$$

for any integer $k \geq 1$. In particular,

$$(\sigma\alpha A)^r = \sigma^r\sigma^{r-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A = \sigma^{r-1}(\alpha A)\ldots\sigma(\alpha A)\alpha A. \tag{3.27}$$

Pick now $B = \begin{bmatrix} 1 & y_1 & & & & * \\ & 1 & y_2 & & & \\ & & \ddots & \ddots & & \\ & & & & y_{n-2} & 0 \\ & 0 & & & 1 & 0 \\ & & & & & d \end{bmatrix}$ from K. Then

$$\alpha AB = \begin{bmatrix} 1 & x_1 + y_1 & & & & * \\ & 1 & x_2 + y_2 & & & \\ & & \ddots & \ddots & & \\ & & & & x_{n-1} + y_{n-1} & 0 \\ & 0 & & & 1 & 0 \\ & & & & & cd \end{bmatrix}.$$

It follows that $(\sigma\alpha A)^r = \begin{bmatrix} 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_1) & & & & * \\ & 1 & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_2) & & & \\ & & & \ddots & \ddots & \\ & & & & tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_{n-2}) & 0 \\ & \mathbf{0} & & & 1 & 0 \\ & & & & & e \end{bmatrix}$

where $e = c^{1+2^a+2^{2a}+\ldots+2^{a(r-1)}} \neq 1$.

Since the trace function is surjective, we can find $x_1, x_2, \ldots, x_{n-1}$ in $\mathbb{F}q$ so that $tr_{\mathbb{F}_q\to\mathbb{F}_{q_0}}(x_i) = 1$

for each $i = 1, \ldots, n-1\}$. Then $(\sigma\alpha A)^r = \begin{bmatrix} 1 & 1 & & & & * \\ & 1 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & & 1 & 0 \\ & \mathbf{0} & & & 1 & 0 \\ & & & & & e \end{bmatrix}$.

Then the Jordan form of $(\sigma\alpha A)^r$ is $J = \begin{bmatrix} 1 & 1 & & & & \mathbf{0} \\ & 1 & 1 & & & \\ & & \ddots & \ddots & & \\ & & & & 1 & 0 \\ & \mathbf{0} & & & 1 & 0 \\ & & & & & e \end{bmatrix}$.

We will observe next that $C_G(J) = C_K(J)/Z(K)$. To see this pick $C = \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \in K$ be such that $CJ = \lambda JC$ for some $1 \neq \lambda \in \mathbb{F}_q^*$. Then we obtain

$$CJ = \begin{bmatrix} a_{11} & a_{11}+a_{12} & \dots & a_{1(n-2)}+a_{1(n-1)} & ea_{1n} \\ a_{21} & a_{21}+a_{22} & \dots & a_{2(n-2)}+a_{2(n-1)} & ea_{2n} \\ a_{31} & a_{31}+a_{32} & \dots & a_{3(n-2)}+a_{3(n-1)} & ea_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{(n-1)1} & a_{(n-1)1}+a_{(n-1)2} & \dots & a_{(n-1)(n-2)}+a_{(n-1)(n-1)} & ea_{(n-1)n} \\ a_{n1} & a_{n1}+a_{n2} & \dots & a_{n(n-2)}+a_{n(n-1)} & ea_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} \lambda a_{11}+\lambda a_{21} & \lambda a_{12}+\lambda a_{22} & \lambda a_{13}+\lambda a_{23} & \dots & \lambda a_{1n}+\lambda a_{2n} \\ \lambda a_{21}+\lambda a_{31} & \lambda a_{22}+\lambda a_{32} & \lambda a_{23}+\lambda a_{33} & \dots & \lambda a_{2n}+\lambda a_{3n} \\ \lambda a_{31}+\lambda a_{41} & \lambda a_{32}+\lambda a_{42} & \lambda a_{33}+\lambda a_{43} & \dots & \lambda a_{3n}+\lambda a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda a_{(n-1)1} & \lambda a_{(n-1)2} & \lambda a_{(n-1)3} & \dots & \lambda a_{(n-1)n} \\ \lambda ea_{n1} & \lambda ea_{n2} & \lambda ea_{n3} & \dots & \lambda ea_{nn} \end{bmatrix} = \lambda JC.$$

Then $a_{n1} = \lambda ea_{n1}$. If $\lambda \neq e^{-1}$, then $a_{n1} = 0$. It follows that $a_{n2} = \lambda ea_{n2}$, which gives $a_{n2} = 0$. Continuing in this manner we get $a_{ni} = 0$ for $i = 1, \dots, n-1$. We also have $ea_{nn} = \lambda ea_{nn}$ which gives $a_{nn} = 0$. Thus $\det(C) = 0$, a contradiction. Therefore, $\lambda = e^{-1}$.

Then we have the equality

$$CJ = \begin{bmatrix} a_{11} & a_{11}+a_{12} & \dots & a_{1(n-2)}+a_{1(n-1)} & e^{-1}a_{1n} \\ a_{21} & a_{21}+a_{22} & \dots & a_{2(n-2)}+a_{2(n-1)} & e^{-1}a_{2n} \\ a_{31} & a_{31}+a_{32} & \dots & a_{3(n-2)}+a_{3(n-1)} & e^{-1}a_{3n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{(n-1)1} & a_{(n-1)1}+a_{(n-1)2} & \dots & a_{(n-1)(n-2)}+a_{(n-1)(n-1)} & e^{-1}a_{(n-1)n} \\ a_{n1} & a_{n1}+a_{n2} & \dots & a_{n(n-2)}+a_{n(n-1)} & e^{-1}a_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} e^{-1}a_{11} + e^{-1}a_{21} & e^{-1}a_{12} + e^{-1}a_{22} & e^{-1}a_{13} + e^{-1}a_{23} & \dots & e^{-1}a_{1n} + e^{-1}a_{2n} \\ e^{-1}a_{21} + e^{-1}a_{31} & e^{-1}a_{22} + e^{-1}a_{32} & e^{-1}a_{23} + e^{-1}a_{33} & \dots & e^{-1}a_{2n} + e^{-1}a_{3n} \\ e^{-1}a_{31} + e^{-1}a_{41} & e^{-1}a_{32} + e^{-1}a_{42} & e^{-1}a_{33} + e^{-1}a_{43} & \dots & e^{-1}a_{3n} + e^{-1}a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ e^{-1}a_{(n-1)1} & e^{-1}a_{(n-1)2} & e^{-1}a_{(n-1)3} & \dots & e^{-1}a_{(n-1)n} \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$$

$$= \lambda JC.$$

In the first column, we have

$a_{i1} = e^{-1}a_{i1} + e^{-1}a_{(i+1)1}$ for $i = 1, \dots, n-2$ and $a_{(n-1)1} = e^{-1}a_{(n-1)1}$. Then we get

$a_{i1} = 0$ for $i = 1, \dots, n-1$.

In the second column, we have

$a_{i2} = e^{-1}a_{i2} + e^{-1}a_{(i+1)2}$ for $i = 1, \dots, n-2$, $a_{(n-1)2} = e^{-1}a_{(n-1)2}$ and $a_{n1} + a_{n2} = a_{n2}$. Then we get

$a_{i2} = 0$ for $i = 1, \dots, n-1$ and either $a_{n1} = 0$ or $a_{n2} = 0$. This means, either first or second column is a zero column and so $\det(C) = 0$, a contradiction. Therefore, we get $C_G(J) = C_K(J)/Z(K)$.

Let now $D = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} \in C_K(J)$. Then we obtain

$$DJ = \begin{bmatrix} a_{11} & a_{11} + a_{12} & a_{12} + a_{13} & \dots & a_{1(n-2)} + a_{1(n-1)} & ea_{1n} \\ a_{21} & a_{21} + a_{22} & a_{22} + a_{23} & \dots & a_{2(n-2)} + a_{2(n-1)} & ea_{2n} \\ a_{31} & a_{31} + a_{32} & a_{32} + a_{33} & \dots & a_{3(n-2)} + a_{3(n-1)} & ea_{3n} \\ \vdots & \vdots & \vdots & & \vdots & \\ a_{n1} & a_{n1} + a_{n2} & a_{n2} + a_{n3} & \dots & a_{n(n-2)} + a_{n(n-1)} & ea_{nn} \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}+a_{21} & a_{12}+a_{22} & a_{13}+a_{23} & \dots & a_{1n}+a_{2n} \\ a_{21}+a_{31} & a_{22}+a_{32} & a_{23}+a_{33} & \dots & a_{2n}+a_{3n} \\ a_{31}+a_{41} & a_{32}+a_{42} & a_{33}+a_{43} & \dots & a_{3n}+a_{4n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{(n-1)1} & a_{(n-1)2} & a_{(n-1)3} & \dots & a_{(n-1)n} \\ ea_{n1} & ea_{n2} & ea_{n3} & \dots & ea_{nn} \end{bmatrix} = JD.$$

In the first row, we have

$a_{11} = a11 + a_{21}$, $a_{1(i-1)} + a_{1i} = a_{1i} + a_{2i}$ for $i = 2, \dots, n-1$ and $ea_{1n} = a_{1n} + a_{2n}$. Then we get,

$a_{21} = 0$, $a_{1(i-1)} = a_{2i}$ for $i = 2, \dots, n-1$ and $a_{2n} = (e+1)a_{1n}$.

In the second row, we have

$0 = a_{31}$, $a_{22} = a_{22} + a_{32}$, $a_{2(i-1)} + a_{2i} = a_{2i} + a_{3i}$ for $i = 3, \dots, n-1$ and $ea_{2n} = a_{2n} + a_{3n}$. Then we get,

$a_{31} = 0$, $a_{32} = 0$, $a_{2(i-1)} = a_{3i}$ for $i = 2, \dots, n-1$ and $a_{3n} = (e-1)a_{2n}$.

In the third row, we have

$0 = a_{41}$, $0 = a_{42}$, $a_{33} = a_{33} + a_{43}$, $a_{3(i-1)} + a_{3i} = a_{3i} + a_{4i}$ for $i = 4, \dots, n-1$ and $ea_{3n} = a_{3n} + a_{4n}$. Then we get,

$a_{41} = 0$, $a_{42} = 0$, $a_{43} = 0$, $a_{3(i-1)} = a_{4i}$ for $i = 4, \dots, n$ and $a_{3n} = (e-1)a_{3n}$.

By means of these calculations we have from the first $n-1$ rows that

$a_{ij} = 0$ for $1 \leq j < i \leq n-1$ and $a_{in} = 0$ for $i = 1, \dots, n-1$.

In the last row, we have

$a_{n1} = ea_{n1}$, $a_{n(i-1)} + a_{ni} = ea_{ni}$ for $i = 2, \dots, n-1$. Then we get

$a_{ni} = 0$ for $i = 1, \dots, n-1$.

By means of these calculations we found that

$$D = \begin{bmatrix} a_1 & a_2 & & & a_{n-2} & a_{n-1} & 0 \\ & a_1 & & & & a_{n-2} & 0 \\ & & \ddots & \ddots & & & \\ & & & & & & \\ & & & & a_1 & a_2 & 0 \\ & 0 & & & & a_1 & 0 \\ & & & & & & a_n \end{bmatrix} \tag{3.28}$$

It is easy now to observe that $|C_K((\sigma A)^r)| = (q-1)q^{n-2}$ and hence

$|G : C_G((\sigma A)^r)| = \frac{q^{n(n-1)/2}\prod\limits_{i=2}^{n}(q^i-1)}{(q-1)q^{n-2}} = \frac{1}{q-1}q^{(n^2-3n+4)/2}\prod\limits_{i=2}^{n}(q^i-1)$ is divisible by 4, as desired. ■

3.2.2 Proof of Theorem 3

We are now ready to prove the last main result of this thesis.

Theorem 3 *Let G be a finite group and $\alpha \in Aut(G)$. Assume that $|G : C_G(x)|$ is squarefree for each $x \in H \setminus G$ where $H = G\langle\alpha\rangle$. Then G is solvable.*

Proof. We proceed by induction on the order of H and obtain a contradiction over a series of steps.

1. *We may assume that G has no nontrivial proper normal α−invariant subgroup. In particular, $G = [G, \alpha]$.*

Let N be a nontrivial α−invariant proper normal subgroup of G. Set $L = N\langle\alpha\rangle$ and let $x \in L \setminus N$. Then $x \in H \setminus G$ and $|N : C_N(x)| = |N : N \cap C_G(x)| = |C_G(x)N : C_G(x)|$ divides $|G : C_G(x)|$. It follows that $|N : C_N(x)|$ is squarefree. As $|L| \lneqq |H|$, N is solvable by induction.

Set $\overline{G} = G/N$ and $\overline{H} = \overline{G}\langle\alpha\rangle$. Let $y \in \overline{H} \setminus \overline{G}$. Then $y = (xN)\alpha^k$ for some $x \in G$ and for some integer k. It is obvious that $x\alpha^k \in H \setminus G$ and $\left|\overline{G} : C_{\overline{G}}(y)\right|$ divides

$\left|G/N : C_G(x\alpha^k)N/N\right| = \left|G : C_G(x\alpha^k)N\right|$. Since $\left|G : C_G(x\alpha^k)N\right|$ divides $\left|G : C_G(x\alpha^k)\right|$, we see that $\left|\overline{G} : C_{\overline{G}}(y)\right|$ is also squarefree. Now, by induction, $\overline{G}$ is solvable as $\left|\overline{H}\right| < |H|$. This forces that G is solvable, a contradiction.

In particular, we obtain $[G, \alpha] = G$.

2. *We may assume that* $|\alpha|$ *is a prime dividing* $|G|$.

Let α be of order m for some composite integer m and p be a prime divisor of m such that $m = kp$. Then $\left|\alpha^k\right| = p$. Set $K = G\left\langle\alpha^k\right\rangle$ and let $x \in K \setminus G$. It is obvious that $|G : C_G(x)|$ is squarefree as $x \in H \setminus G$. By induction applied to K, we see that G is solvable. This contradiction shows that α is of prime order p. Theorem 2 implies that p divides $|G|$.

3. *G is simple.*

G is characteristically simple by Step 1. That is, $G = E_1 \times \ldots \times E_s$ where each E_i, $i = 1, \ldots, s$, is a nonabelian simple group isomorphic to E_1. Let $\{\, E_1, E_1^{\alpha}, \ldots, E_1^{\alpha^k} \,\}$ be the orbit containing E_1 under the action of α on the subgroups of G. Then $C = E_1 \times E_1^{\alpha} \times \ldots \times E_1^{\alpha^k}$ is an $\alpha-$invariant normal subgroup of G and hence $G = C$ by Step 1. Now, if $s > 1$ then $|C_G(\alpha)| = |E_1|$ and we have $|G : C_G(\alpha)| = |E_1|^{s-1}$ is squarefree. This is impossible as 4 divides $|E_1|$ by Theorem 2.0.15. Therefore $s = 1$, that is, G is a nonabelian simple group.

4. α *is not an inner automorphism.*

Assume the contrary. Then α is an inner automorphism $\tau_g : G \longrightarrow G$ given by $x \mapsto g^{-1}xg$ for some $g \in G$. Now, $x^{\tau_g} = \tau_g^{-1} x \tau_g = g^{-1}xg$. For all $x \in G$,

$$x^{g^{-1}\tau_g} = \tau_g^{-1} g x g^{-1} \tau_g = g^{-1} g x g^{-1} g = x. \tag{3.29}$$

This yields that $C_G(g^{-1}\tau_g) = G$. Thus, $H = G\langle\tau_g\rangle = G \times \langle g^{-1}\tau_g\rangle$.

Let $a \in G$. Then $ag^{-1}\tau_g \in H \setminus G$. For $b \in G$, $b^a = b$ if and only if $b^{ag^{-1}\tau_g} = (b^a)^{g^{-1}\tau_g} = b^{g^{-1}\tau_g} = b$ if and only if $b \in C_G(ag^{-1}\tau_g)$. Then $C_G(a) = C_G(ag^{-1}\tau_g)$ and hence $|G : C_G(a)| = \left|G : C_G(ag^{-1}\tau_g)\right|$ is squarefree. Then 4 divides no conjugacy class length in G and we get a contradiction by Theorem 2.0.4.

5. *G is not an alternating group:*

Assume first that $G = A_n$ where $n \geq 5$, and $n \neq 6$. It is well known that $AutA_n \cong S_n$ for $n \neq 6$ and every automorphism of A_n is the restriction of an inner automorphism τ_ρ of S_n to A_n for some $\rho \in S_n$. Since α is a non-inner automorphism of prime order, it must be an automorphism of order 2 which is the restriction of τ_ρ to A_n for some involution $\rho \in S_n \setminus A_n$ (see Theorem 2.0.13).

Set $H = A_n \left\langle \tau_\rho \right\rangle$ and $K = S_n \left\langle \tau_\rho \right\rangle$. Now, as τ_ρ is an inner automorphism of S_n we have $K = S_n \times \left\langle \rho^{-1}\tau_\rho \right\rangle$. For any $x \in K \setminus S_n$, $x = g\rho^{-1}\tau_\rho$ for some $g \in S_n$. A similar argument as in Step 4 shows that $C_{A_n}(x) = C_{A_n}(g\rho^{-1}\tau_\rho) = C_{A_n}(g)$.

Next let $y \in H \setminus A_n$. Then $y = h\tau_\rho$ for some $h \in A_n$. Also $y \in K \setminus S_n$ implies that $y = g\rho^{-1}\tau_\rho$ for some $g \in S_n$. Hence $g = h\rho \in S_n \setminus A_n$. Then

$$\left|A_n : C_{A_n}(y)\right| = \left|A_n : C_{A_n}(h\tau_\rho)\right| = \left|S_n : C_{S_n}(g\rho^{-1}\tau_\rho)\right| = \left|S_n : C_{S_n}(g)\right|. \tag{3.30}$$

If n is odd, then we may choose $\rho = (1\ 2)$ and let h be an $(n-2)$-cycle fixing 1 and 2. Then $g = h\rho$ is a $\{2, n-2\}$-cycle and $\left|C_{S_n}(g)\right| = 2(n-2)$. It follows that
$\left|A_n : C_{A_n}(g)\right| = \left|S_n : C_{S_n}(g)\right| = \frac{n!}{2(n-2)}$ is divisible by 4, which is not the case.

If n is even, then we may choose $\rho = (1\ 2)$ and let h be an $(n-3)$-cycle fixing 1 and 2. Then $g = h\rho$ is a $\{2, n-2\}$-cycle and $\left|C_{S_n}(g)\right| = 2(n-3)$. It follows that
$\left|A_n : C_{A_n}(g)\right| = \left|S_n : C_{S_n}(g)\right| = \frac{n!}{2(n-3)}$ is divisible by 4, which is impossible.

Finally we let $G = A_6$. Then any non-inner automorphism α of G of prime order is of order 2 and it is either an inner automorphism of S_6 or an outer automorphism sending $3-$cycles to $\{3,3\}-$cycles and $\{3,3\}-$cycles to $3-$cycles (see Theorem2.0.13). Any $3-$element of G is either a $3-$cycle or a $\{3,3\}-$cycle. In the latter case, if 3 divides $|C_G(\alpha)|$, then there will be a 3-cyle or a $\{3,3\}$-cyle which is fixed by α which contradicts the definition of α. Thus, $|G : C_G(\alpha)|$ is divisible by 9, which is not the case. In the former for $g = h\rho$ where $\rho = (1\ 2)$ and $h = (3\ 4\ 5)$, $C_G(g\rho^{-1}\tau_\rho) = C_G(g)$ has order $2.3 = 6$. Hence $\left|A_n : C_{A_n}(g\rho^{-1}\tau_\rho)\right| = \left|S_n : C_{S_n}(g\rho^{-1}\tau_\rho)\right| = \frac{6!}{6} = 120$ is divisible by 4, establishing the claim.

6. *G is not a sporadic group. In fact, G is either solvable or a simple group of Lie type*

which is not isomorphic to $PSL(n, \mathbb{F}_q)$ *where* q *is a prime power and* $n \geq 2$ *with exceptions* $n = 2$*,* $q = 2$ *and* $n = 2$*,* $q = 3$.

By Theorem A.0.13, every Sporadic group having a noninner automorphism has a conjugacy class of noninner automorphisms whose length is divisible by 4. Thus, G is not a Sporadic simple group.

Technical lemmas proved in the previous section show that $G \ncong PSL(n, \mathbb{F}_q)$ where q is a prime power and $n \geq 2$ with exceptions $n = 2$, $q = 2$ and $n = 2$, $q = 3$.

Therefore, G is either solvable or a simple group of Lie type which is not isomorphic to $PSL(n, \mathbb{F}_q)$ for n, q with the properties given above.

7. $|G : C_G(\alpha)|$ *is divisible by* p *when* p *is odd.*

Assume that p is odd. If p does not divide $|G : C_G\,(\alpha)|$, then α centralizes a Sylow $p-$subgroup P of G. A result due to Gross (Theorem 2.0.6) implies that α is induced by an element of $Z(P)$ which is impossible by Step 4.

8. *We may assume that* $p = 2$.

Suppose that p is odd. Then p divides $|G : C_G(\alpha)|$ by Step 7. Let y be a p'-element of $C_G(\alpha)$. By Theorem 2.0.14 we have $C_{C_G(\alpha)}(y) = C_G(\alpha) \cap C_G(y) = C_G(y\alpha) \subseteq C_G(\alpha)$. Then $|G : C_G(y\alpha)| = |G : C_G(\alpha)| \left|C_G(\alpha) : C_{C_G(\alpha)}(y)\right|$ is squarefree and hence $p \nmid \left|C_G(\alpha) : C_{C_G(\alpha)}(y)\right|$.

It follows by Theorem 2.0.5 (1) that $C_G(\alpha)$ has a unique Sylow p-subgroup P which is a direct factor, that is, $C_G(\alpha) = P \times A$ where A is a p'-group. Let $a \in A$. Now, $C_{C_G(\alpha)}(a) = P \times C_A(a)$ and also $C_{C_G(\alpha)}(a) = C_G(\alpha) \cap C_G(a) = C_G(a\alpha) \subseteq C_G(\alpha)$ by Theorem 2.0.14. So $\left|C_G(\alpha) : C_{C_G(\alpha)}(a)\right| = |P \times A : P \times C_A(a)| = |A : C_A(a)|$ divides $|G : C_G(a\alpha)|$ and hence squarefree.

Let now $a \in A$ be an involution. Then $K = A\langle\tau_a\rangle = A \times \langle a^{-1}\tau_a\rangle$. For any $x \in K \setminus A$ there exists $c \in A$ such that $x = ca^{-1}\tau_a$ and hence $C_A(c) = C_A(x)$, that is, $|A : C_A(x)|$ is squarefree. As p is odd we have $|K| < |H|$. It follows by induction that A is solvable. This forces the solvability of $C_G(\alpha)$ if it contains a p'-element. In case $C_G(\alpha)$ is a p-group, it is already solvable.

By Theorem B.0.14, Table B.13, Theorem B.0.15 and Theorem B.0.16, $C_G(\alpha)$ has a simple subgroup. This contradicts to the solvability of $C_G(\alpha)$.

Therefore, we may assume that $p = 2$.

9. *Final Contradiction.*

By the classification of finite simple groups α is either an inner diagonal or a graph or a field or a graph-field automorphism. Set $q = r^f$.

We shall study in three cases:

Case 1. *α is an inner-diagonal or graph automorphism where q is odd.*

We shall eliminate all the families of simple groups of possible Lie type.

First of all we consider the family $A_m^{\varepsilon}(q)$ for $m \geq 2$, $\varepsilon = \pm 1$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$P_1 = A_{m-1}^{\varepsilon}(q)$. Then $|P_1|_r = q^{\frac{(m-1)m}{2}}$ and hence $|G : P_1|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{\frac{(m-1)m}{2}}} = q^m$.

$P_2 = A_{i-1}^{\varepsilon}(q)A_{m-i}^{\varepsilon}(q)$ and $2 \leq i \leq \frac{m}{2}$. Then $|P_2|_r = q^{\frac{(i-1)i}{2}}q^{\frac{(m-i)(m-i+1)}{2}}$ and hence $|G : P_2|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{\frac{(i-1)i}{2}}q^{\frac{(m-i)(m-i+1)}{2}}} = q^{mi-i^2}$.

$P_3 = A_{\frac{m-1}{2}}^{\varepsilon}(q)^2$ and m is odd. Then $|P_3|_r = q^{2\frac{\frac{m-1}{2}\frac{m+1}{2}}{2}}$ and hence $|G : P_3|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{2\frac{\frac{m-1}{2}\frac{m+1}{2}}{2}}} = q^{\frac{(m+1)^2}{4}}$.

$P_4 = A_{\frac{m-1}{2}}^{\varepsilon}(q^2)$ and m is odd. Then $|P_4|_r = q^{2\frac{\frac{m-1}{2}\frac{m+1}{2}}{2}}$ and hence $|G : P_4|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{2\frac{\frac{m-1}{2}\frac{m+1}{2}}{2}}} = q^{\frac{(m+1)^2}{4}}$.

$P_5 = C_{\frac{m+1}{2}}(q)$ and m is odd. Then $|P_5|_r = q^{(\frac{m+1}{2})^2}$ and hence $|G : P_5|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{(\frac{m+1}{2})^2}} = q^{\frac{m^2-1}{4}}$.

$P_6 = B_{\frac{m}{2}}(q)$ and m is even. Then $|P_6|_r = q^{(\frac{m}{2})^2}$ and hence $|G : P_6|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{(\frac{m}{2})^2}} = q^{\frac{m^2+2m}{4}}$.

$P_7 = D_{\frac{m+1}{2}}(q)$ and m is odd. Then $|P_7|_r = q^{\frac{m+1}{2}\frac{m-1}{2}}$ and hence $|G : P_7|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{\frac{m+1}{2}\frac{m-1}{2}}} = q^{\frac{(m+1)^2}{4}}$.

$P_8 =^2 D_{\frac{m+1}{2}}(q)$ and m is odd. Then $|P_8|_r = q^{\frac{m+1}{2}\frac{m-1}{2}}$ and hence $|G : P_8|_r = \frac{q^{\frac{m(m+1)}{2}}}{q^{\frac{m+1}{2}\frac{m-1}{2}}} = q^{\frac{(m+1)^2}{4}}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We consider next the family $B_m(q)$ for $m \geq 2$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$Q_1 = B_{m-1}(q)$. Then $|Q_1|_r = q^{(m-1)^2}$ and hence $|G : Q_1|_r = \frac{q^{m^2}}{q^{(m-1)^2}} = q^{2m-1}$.

$Q_2 = B_{m-1}(q)$. Then $|Q_2|_r = q^{(m-1)^2}$ and hence $|G : Q_2|_r = \frac{q^{m^2}}{q^{(m-1)^2}} = q^{2m-1}$.

$Q_3 = D_i(q)B_{m-i}(q)$ and $2 \leq i < m$. Then $|Q_3|_r = q^{i(i-1)}q^{(m-i)^2}$ and hence $|G : Q_3|_r = \frac{q^{m^2}}{q^{i(i-1)}q^{(m-i)^2}} = q^{2mi+i-2i^2}$.

$Q_4 =^2 D_i(q)B_{m-i}(q)$ and $2 \leq i < m$. Then $|Q_4|_r = q^{i(i-1)}q^{(m-i)^2}$ and hence $|G : Q_4|_r = \frac{q^{m^2}}{q^{i(i-1)}q^{(m-i)^2}} = q^{2mi+i-2i^2}$.

$Q_5 = D_m(q)$. Then $|Q_5|_r = q^{m(m-1)}$ and hence $|G : Q_5|_r = \frac{q^{m^2}}{q^{m(m-1)}} = q^m$.

$Q_6 =^2 D_m(q)$. Then $|Q_6|_r = q^{m(m-1)}$ and hence $|G : Q_6|_r = \frac{q^{m^2}}{q^{m(m-1)}} = q^m$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We consider now the family $C_m(q)$ for $m \geq 2$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$R_1 = C_i(q)C_{m-i}(q)$ and $1 \leq i < \frac{m}{2}$. Then $|R_1|_r = q^{i^2}q^{(m-i)^2}$ and hence $|G : R_1|_r = \frac{q^{m^2}}{q^{i^2}q^{(m-i)^2}} = q^{2mi-2i^2}$.

$R_2 = C_{\frac{m}{2}}(q)^2$ and m is even. Then $|R_2|_r = q^{2(\frac{m}{2})^2}$ and hence $|G : R_2|_r = \frac{q^{m^2}}{q^{2(\frac{m}{2})^2}} = q^{\frac{m^2}{2}}$.

$R_3 = C_{\frac{m}{2}}(q^2)$ and m is even. Then $|R_3|_r = q^{2(\frac{m}{2})^2}$ and hence $|G : R_3|_r = \frac{q^{m^2}}{q^{2(\frac{m}{2})^2}} = q^{\frac{m^2}{2}}$.

$R_4 = A_{m-1}(q)$. Then $|R_4|_r = q^{\frac{m(m-1)}{2}}$ and hence $|G : R_4|_r = \frac{q^{m^2}}{q^{\frac{m(m-1)}{2}}} = q^{\frac{m^2+m}{2}}$.

$R_5 =^2 A_{m-1}(q)$. Then $|R_5|_r = q^{\frac{m(m-1)}{2}}$ and hence $|G : R_5|_r = \frac{q^{m^2}}{q^{\frac{m(m-1)}{2}}} = q^{\frac{m^2+m}{2}}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We consider next the family $D^{\varepsilon}_m(q)$ for $m \geq 4$, $\varepsilon = \pm 1$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$S_1 = D^{\varepsilon}_{m-1}(q)$. Then $|S_1|_r = q^{(m-1)(m-2)}$ and hence $|G : S_1|_r = \frac{q^{m(m-1)}}{q^{(m-1)(m-2)}} = q^{2m-2}$.

$S_2 = D^{-\varepsilon}_{m-1}(q)$. Then $|S_2|_r = q^{(m-1)(m-2)}$ and hence $|G : S_2|_r = \frac{q^{m(m-1)}}{q^{(m-1)(m-2)}} = q^{2m-2}$.

$S_3 = D_i(q)D^{\varepsilon}_{m-i}(q)$ and $2 \leq i < \frac{m}{2}$. Then $|S_3|_r = q^{i(i-1)}q^{(m-i)(m-i-1)}$ and hence $|G : S_3|_r =$

$\frac{q^{m(m-1)}}{q^{i(i-1)}q^{(m-i)(m-i-1)}} = q^{2mi-2i^2}$.

$S_4 =^2 D_i(q)D^{-\varepsilon}_{m-i}(q)$ and $2 \leq i < \frac{m}{2}$. Then $|S_4|_r = q^{i(i-1)}q^{(m-i)(m-i-1)}$ and hence $|G : S_4|_r = \frac{q^{m(m-1)}}{q^{i(i-1)}q^{(m-i)(m-i-1)}} = q^{2mi-2i^2}$.

$S_5 = D_{\frac{m}{2}}(q)^2$ and $G = D^+_{2k}(q)$. Then $|S_5|_r = q^{2\frac{m}{2}\frac{m-2}{2}}$ and hence $|G : S_5|_r = \frac{q^{m(m-1)}}{q^{2\frac{m}{2}\frac{m-2}{2}}} = q^{\frac{m^2-2m+2}{2}}$.

$S_6 =^2 D_{\frac{m}{2}}(q)^2$ and
$G = D^+_{2k}(q)$. Then $|S_6|_r = q^{2\frac{m}{2}\frac{m-2}{2}}$ and hence $|G : S_6|_r = \frac{q^{m(m-1)}}{q^{2\frac{m}{2}\frac{m-2}{2}}} = q^{\frac{m^2-2m+2}{2}}$.

$S_7 = A_{m-1}(q)$ and $G = D^+_{2k}(q)$. Then $|S_7|_r = q^{\frac{m(m-1)}{2}}$ and hence $|G : S_7|_r = \frac{q^{m(m-1)}}{q^{\frac{m(m-1)}{2}}} = q^{\frac{m^2-m}{2}}$.

$S_8 =^2 A_{m-1}(q)$ and $G = D^+_{2k}(q)$. Then $|S_8|_r = q^{\frac{m(m-1)}{2}}$ and hence $|G : S_8|_r = \frac{q^{m(m-1)}}{q^{\frac{m(m-1)}{2}}} = q^{\frac{m^2-m}{2}}$.

$S_9 =^2 D_{\frac{m}{2}}(q)D_{\frac{m}{2}}(q)$ and $G = D^-_{2k}(q)$. Then $|S_9|_r = q^{2\frac{m}{2}\frac{m-2}{2}}$ and hence $|G : S_9|_r = \frac{q^{m(m-1)}}{q^{2\frac{m}{2}\frac{m-2}{2}}} = q^{\frac{m^2-2m+2}{2}}$.

$S_{10} =^2 D_{\frac{m}{2}}(q^2)$ and $G = D^-_{2k}(q)$. Then $|S_{10}|_r = q^{2\frac{m}{2}\frac{m-2}{2}}$ and hence $|G : S_{10}|_r = \frac{q^{m(m-1)}}{q^{2\frac{m}{2}\frac{m-2}{2}}} = q^{\frac{m^2-2m+2}{2}}$.

$S_{11} = A^{\varepsilon}_{m-1}(q)$ and $G = D^{\varepsilon}_{2k+1}(q)$. Then $|S_{11}|_r = q^{\frac{m(m-1)}{2}}$ and hence $|G : S_{11}|_r = \frac{q^{m(m-1)}}{q^{\frac{m(m-1)}{2}}} = q^{\frac{m^2-m}{2}}$.

$S_{12} = B_{m-1}(q)$. Then $|S_{12}|_r = q^{(m-1)^2}$ and hence $|G : S_{12}|_r = \frac{q^{m(m-1)}}{q^{(m-1)^2}} = q^{m-1}$.

$S_{13} = B_{i-1}(q)B_{m-i}(q)$ and $2 \leq i \leq \frac{m}{2}$. Then $|S_{13}|_r = q^{(i-1)^2}q^{(m-i)^2}$ and hence $|G : S_{13}|_r = \frac{q^{m(m-1)}}{q^{(i-1)^2}q^{(m-i)^2}} = q^{2mi-i^2+2i-m-1}$.

$S_{14} = B_{\frac{m-1}{2}}(q)^2$ and $G = D^{\varepsilon}_{2k+1}(q)$. Then $|S_{14}|_r = q^{2(\frac{m-1}{2})^2}$ and hence $|G : S_{14}|_r = \frac{q^{m(m-1)}}{q^{2(\frac{m-1}{2})^2}} = q^{\frac{m^2-1}{2}}$.

$S_{15} = B_{\frac{m-1}{2}}(q^2)$ and $G = D^{\varepsilon}_{2k+1}(q)$. Then $|S_{15}|_r = q^{2(\frac{m-1}{2})^2}$ and hence $|G : S_{15}|_r = \frac{q^{m(m-1)}}{q^{2(\frac{m-1}{2})^2}} = q^{\frac{m^2-1}{2}}$.

$S_{16} = B_3(q)$ and $G = D^+_4(q)$. Then $|S_{16}|_r = q^9$ and hence $|G : S_{16}|_r = \frac{q^{4.3}}{q^9} = q^3$.

$S_{17} = A_1(q)B_2(q)$ and $G = D^+_4(q)$. Then $|S_{17}|_r = q^{\frac{1.2}{2}}q^4 = q^5$ and hence $|G : S_{17}|_r = \frac{q^{4.3}}{q^5} = q^7$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We then consider the family $E_6^{\varepsilon}(q)$ for $\varepsilon = \pm 1$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$T_1 = D_5^{\varepsilon}(q)$. Then $|T_1|_r = q^{5.4} = q^{20}$ and hence $|G : T_1|_r = \frac{q^{36}}{q^{20}} = q^{16}$.

$T_2 = A_1(q)A_5^{\varepsilon}(q)$. Then $|T_2|_r = q^{\frac{1.2}{2}} q^{\frac{5.6}{2}} = q^{16}$ and hence $|G : T_2|_r = \frac{q^{36}}{q^{16}} = q^{20}$.

$T_3 = F_4(q)$. Then $|T_3|_r = q^{24}$ and hence $|G : T_3|_r = \frac{q^{36}}{q^{24}} = q^{12}$.

$T_4 = C_4(q)$. Then $|T_4|_r = q^{\frac{1.2}{2}} q^{\frac{5.6}{2}} = q^{16}$ and hence $|T : P_4|_r = \frac{q^{36}}{q^{16}} = q^{20}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We consider next the family $E_7(q)$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$U_1 = A_1(q)D_6(q)$. Then $|U_1|_r = q^{\frac{1.2}{2}} q^{6.5} = q^{31}$ and hence $|G : U_1|_r = \frac{q^{63}}{q^{31}} = q^{32}$.

$U_2 = A_7(q)$. Then $|U_2|_r = q^{\frac{7.8}{2}} = q^{28}$ and hence $|G : U_2|_r = \frac{q^{63}}{q^{28}} = q^{35}$.

$U_3 =^2 A_7(q)$. Then $|U_3|_r = q^{\frac{7.8}{2}} = q^{28}$ and hence $|T : U_3|_r = \frac{q^{63}}{q^{28}} = q^{35}$.

$U_4 = E_6(q)$. Then $|U_4|_r = q^{36}$ and hence $|G : U_4|_r = \frac{q^{63}}{q^{36}} = q^{27}$.

$U_5 =^2 E_6(q)$. Then $|U_5|_r = q^{36}$ and hence $|G : U_5|_r = \frac{q^{63}}{q^{36}} = q^{27}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

We consider next the family $3_4^D(q)$. Here is the only possibility for $O^{r'}(C_G(\alpha))$:

$V = A_1(q)A_1(q^3)$. Then $|V|_r = q^{\frac{1.2}{2}} (q^3)^{\frac{1.2}{2}} = q^4$ and hence $|G : V|_r = \frac{q^{12}}{q^4} = q^8$.

Notice that r^2 divides $|G : C_G(\alpha)|$, and hence it is not possible.

We consider next the family $G_2(q)$. Here is the only possibility for $O^{r'}(C_G(\alpha))$:

$W = A_1(q^2)$. Then $|W|_r = (q^2)^{\frac{1.2}{2}} = q^2$ and hence $|G : W|_r = \frac{q^6}{q^2} = q^4$.

Notice that r^2 divides $|G : C_G(\alpha)|$, and hence it is not possible.

We consider next the family ${}^2G_2(q)$ where $q = 3^{2n+1}$ for $n > 1$. Here is the only possibility for $O^{r'}(C_G(\alpha))$:

$Y = A_1(q^2)$. Then $|Y|_r = (q^2)^{\frac{1.2}{2}} = q^2$ and hence $|G : Y|_r = \frac{q^3}{q^2} = q = 3^{2n+1}$.

Notice that 9 divides $|G : C_G(\alpha)|$, and hence it is not possible.

We consider next the family $F_4(q)$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$Z_1 = A_1(q)C_3(q)$. Then $|Z_1|_r = q^{\frac{1.2}{2}} q^{3^2} = q^{10}$ and hence $|G : Z_1|_r = \frac{q^{24}}{q^{10}} = q^{14}$.

$Z_2 = B_4(q)$. Then $|Z_2|_r = q^{4^2} = q^{16}$ and hence $|G : Z_2|_r = \frac{q^{24}}{q^{16}} = q^{8}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

Finally, we consider the family $E_8(q)$. Here are all the possibilities for $O^{r'}(C_G(\alpha))$:

$H_1 = D_8(q)$. Then $|H_1|_r = q^{8.7} = q^{56}$ and hence $|G : H_1|_r = \frac{q^{120}}{q^{56}} = q^{64}$.

$H_2 = A_1(q)E_7(q)$. Then $|H_2|_r = q^{\frac{1.2}{2}} q^{63} = q^{64}$ and hence $|G : H_2|_r = \frac{q^{120}}{q^{63}} = q^{57}$.

Notice that in all the above cases r^2 divides $|G : C_G(\alpha)|$, and hence none of them is possible.

Case 2: *α is a field automorphism or a graph-field automorphism.*

By Theorem B.0.15, if $q = r^{2s}$ for some integer s and $G = L(q)$, then $C_G(\alpha) \cong L(r^s)$.

If $G = A_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) = A_m(r^s)$ or $C_G(\alpha) =^2 A_m(r^s)$. It follows that
$|G : C_G(\alpha)|_r = \frac{(r^{2s})^{\frac{m(m+1)}{2}}}{(r^s)^{\frac{m(m+1)}{2}}} = r^{\frac{sm(m+1)}{2}}$

If $G = B_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) = B_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m^2}}{(r^s)^{m^2}} = r^{sm^2}$

If $G = C_m(q^{2s})$ for $m \geq 3$ then $C_G(\alpha) = C_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m^2}}{(r^s)^{m^2}} = r^{sm^2}$

If $G = D_m(q^{2s})$ for $m \geq 4$ then $C_G(\alpha) = D_m(r^s)$ or $C_G(\alpha) =^2 D_m(r^s)$ or $C_G(\alpha) =^3 D_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m(m-1)}}{(r^s)^{m(m-1)}} = r^{sm(m-1)}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{12}}{(r^s)^{12)}} = r^{12s}$

If $G = E_6(q^{2s})$ then $C_G(\alpha) = E_6(r^s)$ or $C_G(\alpha) =^2 E_6(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{36}}{(r^s)^{36}} = r^{36s}$

If $G = E_7(q^{2s})$ then $C_G(\alpha) = E_7(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{63}}{(r^s)^{63}} = r^{63s}$

If $G = E_8(q^{2s})$ then $C_G(\alpha) = E_8(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{120}}{(r^s)^{120}} = r^{120s}$

If $G = F_4(q^{2s})$ then $C_G(\alpha) = F_4(r^s)$ or $C_G(\alpha) =^2 F_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{24}}{(r^s)^{24}} = r^{24s}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{24}}{(r^s)^{12}} = r^{36s}$

If $G = G_2(q^{2s})$ then $C_G(\alpha) = G_2(r^s)$ or $C_G(\alpha) =^2 G_2(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^6}{(r^s)^6} = r^{6s}$ or $|G : C_G(\alpha)|_r = \frac{(r^{2s})^6}{(r^s)^3} = r^{9s}$

If $G =^2 A_m(r^{2s})$ for $m \geq 2$ then $C_G(\alpha) =^2 A_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{\frac{m(m+1)}{2}}}{(r^s)^{\frac{m(m+1)}{2}}} = r^{\frac{sm(m+1)}{2}}$

If $G =^2 D_m(q^{2s})$ for $m \geq 4$ then $C_G(\alpha) =^2 D_m(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{m(m-1)}}{(r^s)^{m(m-1)}} = r^{sm(m-1)}$

If $G =^2 E_6(q^{2s})$ then $C_G(\alpha) =^2 E_6(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{36}}{(r^s)^{36}} = r^{36s}$

If $G =^3 D_4(q^{2s})$ then $C_G(\alpha) =^3 D_4(r^s)$. It follows that $|G : C_G(\alpha)|_r = \frac{(r^{2s})^{12}}{(r^s)^{12}} = r^{12s}$.

Notice that r^2 divides $|G : C_G(\alpha)|$ in all the above cases and hence none of them is possible.

Case 3: *α is a graph automorphism.*

If $G = A^{\pm}_{2m+1}(q)$ for $m \geq 1$ then $C_G(\alpha) = C_m(q)$. It follows that
$|G : C_G(\alpha)|_r = \frac{q^{\frac{(2m+1)2m}{2}}}{q^{m^2}} = q^{m^2+m}$

If $G = A^{\pm}_{2m}(q)$ for $m \geq 1$ then $C_G(\alpha) = C_m(q)$. It follows that $|G : C_G(\alpha)|_r = \frac{q^{\frac{2m(2m-1)}{2}}}{q^{m^2}} = q^{m^2-m}$

If $G = D^{\pm}_m(q)$ for $m \geq 4$ then $C_G(\alpha) = B_{m-1}(q)$. It follows that $|G : C_G(\alpha)|_r = \frac{q^{m(m-1)}}{q^{(m-1)^2}} = q^{m-1}$

If $G = E^{\pm}_6(q)$ then $C_G(\alpha) = F_4(q)$. It follows that $|G : C_G(\alpha)|_r = \frac{q^{36}}{q^{24}} = q^{12}$

Notice that q^2 divides $|G : C_G(\alpha)|$ in all the above cases and hence none of them is possible.

This completes the proof of Theorem 3. ■

REFERENCES

[1] R. Baer : Group elements of prime power index, *Trans. Amer. Math. Soc.*, **75**, (1953), 20-47

[2] N. Burgoyne and R. Griess and R. Lyons : Maximal Subgroups and Automorphisms of Chevalley Groups. *Pasific Journal of Mathematics*, Vol. **71**, no. 2, (1977), 365-403.

[3] W. Burnside : On the groups of order $p^\alpha q^\beta$, *Proc. London Math. Soc.*, **2**, (1904), 432-437

[4] A.R. Camina : Arithmetical conditions on the conjugacy class numbers of a finite group. *J. London Math. Soc. (2)*, **5**, (1972), 127-132

[5] A. R. Camina : Conjugacy classes of finite groups and some theorems of N. Itô, *J. London Math. Soc. (2)*, **6** (1973), 421-426

[6] A. R. Camina : Finite groups of conjugate rank 2, *Nagoya Math. J.*, **58**, (1974), 47-57

[7] A. R. Camina and R. D. Camina : Implications of the conjugacy class size. *J. Group Theory*, **1**, (1998), 257-269.

[8] D. Chillag and M. Herzog : On the length of the conjugacy classes of finite groups. *Journal of Algebra*, **131**, (1990), 110-125.

[9] J. H. Conway and R. T. Curtis and S. P. Norton and R. A. Parker and R. A. Wilson : *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985

[10] J. Cossey and Y. Wang : Remarks on the length of conjugacy classes of finite groups. *Comm. Algebra*, **27**, (1999), no.9, 4347-4353.

[11] G. Ercan : On finite groups admitting a special noncoprime action, *Proc. Amer. Math. Soc.*, **133**, (2005), no. 9, 2543-2547

[12] G. Ercan and İ.Ş. Güloğlu : On the Fitting length of $H_n(G)$, *Rend. Sem. Mat. Univ. Padova*, **89**, (1993), 171-175

[13] G. Ercan and İ.Ş. Güloğlu : On the Fitting length of $H_{pq}(G)$, *Arch. Math. (Basel)*, **56**, (1991), no. 3, 214-217

[14] G. Ercan and İ.Ş. Güloğlu : On the Fitting length of generalized Hughes subgroup, *Arch. Math. (Basel)*, **55**, (1990), no. 1, 5-9

[15] G. Ercan and İ.Ş. Güloğlu : On a generalization of Hughes problem, *Doğa Mat.*, **13**, (1989), no. 3, 107-109

[16] D. Gorenstein : *Finite Groups*, AMS Chelsea Publishing, New York, 1980

[17] D. Gorenstein and R. Lyons and R. Solomon : *The Classification of the Finite Simple Groups*, Number 3, American Mathematical Society, 1994

[18] Fletcher Gross : Automorphisms which centralize a Sylow $p-$subgroup. *J. of Algebra*, **77**, (1982), 202-233.

[19] John L. Hayden and David L. Winter : Finite groups admitting an automorphism trivial on a Sylow $2-$subgroup. *Can. J. Math.* Vol.**XXIX**, No. 4, (1977), 889-896.

[20] David Hilbert and I. T. Adamson and F. Lemmermeyer : *The Theory of Algebraic Number Fields: Zahlbericht*, Springer, 1998

[21] I. Martin Isaacs : *Character Theory of Finite Groups*, AMS Chelsea Publishing, Rhode Island, 2006

[22] N. Itô : On finite groups with given conjugate types. I, *Nagoya Math. J.*, **6**, (1953), 17-25

[23] N. Itô : On finite groups with given conjugate types. II, *Osaka J. Math.*, **7**, (1970), 231-251

[24] N. Itô : On finite groups with given conjugate types. III, *Math. Z.*, **117**, (1970), 267-271

[25] L.S. Kazarin : Burnside's $p^{\alpha}-$lemma. *(Russian) Mat. Zametki*, **48**, (1990), no.2, 45-48; *translation in Math. Notes*, **48**, (1990), no.1-2, 749-751 (1991).

[26] H. Kurzweil and B. Stellmacher : *The Theory of Finite Groups*, Springer, New York, 2004

[27] C. Parker and M. Quick : Coprime automorphisms and their commutators, *J. Algebra*, **244**, (2001), no. 1, 260-272

[28] M.Suzuki : *Group Theory I*, Springer-Verlag, Berlin; New York, 1982

[29] Alexandre Turull : The number of Hall $\pi-$subgroups of a $\pi-$separable group. *Proc. of the American Math. Soc.*, Vol. **132**, no. 9, (2004), 2563-2565.

[30] Robert A. Wilson : *The Finite Simple Groups*, Springer-Verlag, London, 2009

Appendix A

FIXED POINT SUBGROUPS OF AUTOMORPHISM GROUPS OF SPORADIC SIMPLE GROUPS

In this part we shall give some arithmetical information about the sporadic simple groups and some information about conjugacy classes of their noninner automorphisms that contains only lengths and names of the conjugacy classes and the order of their fixed point subgroups.

In the tables we give below, G denotes the name of the corresponding sporadic simple group, and x denotes a representative of a conjugacy class of noninner automorphisms.

First of all we shall describe these tables column-by-column.

In the first column, we give the name of the information given in the corresponding row. Each of the remaining columns gives the information about the conjugacy class of noninner automorphisms containing x.

Next, we shall describe the tables row-by-row. This is almost the same description as it is in Atlas of Finite Groups ([9], pages xxv-xxx).

In the first row, the numbers given are the orders of fixed point subgroups in the base group G.

For a conjugacy class, the set of the k^{th} power of the elements forms another conjugacy class. The resulting *power maps*, for a composite number l, between the classes can be obtained by repeated use of the *prime power maps*, the particular case when k is prime, for prime divisors of l.

The second row gives the tag letters of the name of the classes that contain respectively the powers $x^p, x^q, x^r, \ldots$ of x, where $p < q < r < \ldots$ are the prime divisors of the order of x. For example if we have an entry ABC for the power map of an element x of order 84, then we mean that x^2 is in class $42A$, x^3 in class $28B$, x^7 in class $12C$.

Let $x \in Aut(G)$ and π be a subset of $\pi(Aut(G))$, the set of prime divisors of order of $Aut(G)$. A certain power of x is called the π-part of x, denoted by $x(\pi)$, if the set of prime divisors of order of $x(\pi)$ is contained in π while none of those of order of $x(\pi)^{-1}x$. $x(\pi)^{-1}x$ is called the π'-part of x and it is denoted by $x(\pi')$. For each $x \in Aut(G)$, we can write $x = x(\pi)x(\pi') = x(\pi')x(\pi)$ uniquely. If π consists of a single prime p, then we denote them respectively by $x(p)$ and $x(p')$ and call them the p-part and p'-part of x. The π-parts for general sets π can be found by repeated use of the p'-parts.

The third row of the table gives the tag letters of the name of the classes that contain respectively the powers $x(p'), x(q'), x(r'), \ldots$, where $p < q < r < \ldots$ are the prime divisors of the order of x.

$nA, nB, nC, \ldots$ denote the conjugacy classes that contain elements of order n. The alphabet used here is potentially infinite, and reads

$$A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, A1, B1, \ldots, A2, B2, \ldots$$

The class name row contains the following information:

Entries of the form nX are called ‘Master’ class name entries. It just means that the column refers to a conjugacy class nX;

Entries of the form $Y * k$ (or $Y * *k, Y * *, Y*$) are called ‘Slave’ class name entries. It just means that the column refers to a conjugacy class nY, and one can obtain nY by applying the algebraic conjugacy operator $*k$ (or $* * k, **, *$) to the most recent ‘master’ class nX.

An algebraically conjugate family of classes consists of a ‘master’ class and the immediately subsequent ‘slave’ classes.

We define the algebraic conjugacy operators on classes as follows [9]:

$(nX)^{*k}$ contains the k^{th} powers of elements of nX;

$(nX)^{**k}$ contains the $(-k)^{th}$ powers of elements of nX;

$(nX)^{**}$ contains the inverses of elements of nX;

and

$(nX)^*$ is the class other than nX containing elements of order n that are powers of elements of nX, when this class is unique. It is to be understood that k is prime to n. The values of characters on these classes are the images of their values on nX under the appropriate algebraic conjugacies.

The last row gives the prime decomposition of the index of the corresponding fixed point subgroup in the base group G.

SPORADIC MATHIEU GROUP M_{11} ([9], page 18)

The order of M_{11} is $7,920 = 2^4.3^2.5.11$. The automorphism group of M_{11} is isomorphic to itself and hence there is no noninner automorphism of M_{11}.

SPORADIC MATHIEU GROUP M_{12} ([9], pages 31-33)

The order of M_{12} is $95,040 = 2^6.3^3.5.11$. The index of inner automorphism group of M_{12} in the automorphism group of M_{12} is 2.

Table A.1: Some of the Conjugacy Classes of Noninner Automorphisms of M_{12}

$\|C_G(x)\|$	120	24	12	6	10	10
p power	A	B	A	BC	AC	AC
p' part	A	A	A	BC	AC	AC
Class Name	2C	4C	4D	6C	10B	C*
$\|G : C_G(x)\|$	$2^3.3^2.11$	$2^3.3^2.5.11$	$2^4.3^2.5.11$	$2^5.3^2.5.11$	$2^5.3^3.11$	$2^5.3^3.11$

SPORADIC MATHIEU GROUP M_{22} ([9], pages 39-41)

The order of M_{22} is $443,520 = 2^7.3^2.5.7.11$. The index of inner automorphism group of M_{22} in the automorphism group of M_{22} is 2.

Table A.2: Some of the Conjugacy Classes of Noninner Automorphisms of M_{22}

$\lvert C_G(x)\rvert$	1344	320	48	32	6
p power	A	A	A	A	AB
p' part	A	A	A	A	AB
Class Name	2B	2C	4C	4D	6B
$\lvert G : C_G(x)\rvert$	$2.3.5.11$	$2.3^2.7.11$	$2^3.3.5.7.11$	$2^2.3^2.5.7.11$	$2^6.3.5.7.11$

SPORADIC MATHIEU GROUP M_{23} ([9], page 71)

The order of M_{23} is $10,200,960 = 2^7.3^2.5.7.11.23$. The automorphism group of M_{23} is isomorphic to itself and hence there is no noninner automorphism of M_{23}.

SPORADIC MATHIEU GROUP M_{24} ([9], pages 94-96)

The order of M_{24} is $244,823,040 = 2^{10}.3^3.5.7.11.23$. The automorphism group of M_{24} is isomorphic to itself and hence there is no noninner automorphism of M_{24}.

SPORADIC JANKO GROUP J_1 ([9], page 36)

The order of J_1 is $175,560 = 2^3.3.5.7.11.19$. The automorphism group of J_1 is isomorphic to itself and hence there is no noninner automorphism of J_1.

SPORADIC JANKO GROUP J_2 ([9], pages 42-43)

The order of J_2 is $604,800 = 2^7.3^3.5^2.7$. The index of inner automorphism group of J_2 in the automorphism group of J_2 is 2.

Table A.3: Some of the Conjugacy Classes of Noninner Automorphisms of J_2

$\lvert C_G(x)\rvert$	336	48	12	6	48	16
p power	A	A	B	BC	A	A
p' part	A	A	A	BC	A	A
Class Name	2C	4B	4C	6C	8B	8C
$\lvert G : C_G(x)\rvert$	$2^3.3^2.5^2$	$2^3.3^2.5^2.7$	$2^5.3^2.5^2.7$	$2^6.3^2.5^2.7$	$2^3.3^2.5^2.7$	$2^3.3^3.5^2.7$

SPORADIC JANKO GROUP J_3 ([9], pages 82-83)

The order of J_3 is $50,232,960 = 2^7.3^5.5.17.19$. The index of inner automorphism group of J_3 in the automorphism group of J_3 is 2.

Table A.4: Some of the Conjugacy Classes of Noninner Automorphisms of J_3

$\lvert C_G(x)\rvert$	2,448	48	9	48	16
p power	A	A	BB	A	A
p' part	A	A	BB	A	A
Class Name	2B	4B	6B	8B	8C
$\lvert G : C_G(x)\rvert$	$2^3.3^3.5.19$	$2^3.3^4.5.17.19$	$2^7.3^3.5.17.19$	$2^3.3^4.5.17.19$	$2^3.3^5.5.17.19$

SPORADIC JANKO GROUP J_4 ([9], pages 188-190)

The order of J_4 is $86,775,571,046,077,562,880 = 2^{21}.3^3.5.7.11^3.23.29.31.37.43$. The automorphism group of J_4 is isomorphic to itself and hence there is no noninner automorphism of J_4.

SPORADIC CONWAY GROUP Co_1 ([9], pages 180-187)

The order of Co_1 is $4,157,776,806,543,360,000 = 2^{21}.3^9.5^4.7^2.11.13.23$. The automorphism group of Co_1 is isomorphic to itself and hence there is no noninner automorphism of Co_1.

SPORADIC CONWAY GROUP Co_2 ([9], pages 154-155)

The order of Co_2 is $42,305,421,312,000 = 2^{18}.3^6.5^3.7.11.23$. The automorphism group of Co_2 is isomorphic to itself and hence there is no noninner automorphism of Co_2.

SPORADIC CONWAY GROUP Co_3 ([9], pages 134-135)

The order of Co_3 is $495,766,656,000 = 2^{10}.3^7.5^3.7.11.23$. The automorphism group of Co_3 is isomorphic to itself and hence there is no noninner automorphism of Co_3.

SPORADIC FISCHER GROUP Fi_{22} ([9], pages 156-163)

The order of Fi_{22} is $64,561,751,654,400 = 2^{17}.3^9.5^2.7.11.13$. The index of inner automorphism group of Fi_{22} in the automorphism group of Fi_{22} is 2.

Table A.5: Some of the Conjugacy Classes of Noninner Automorphisms of Fi_{22}

$\|C_G(x)\|$	1,045,094,400	3,317,760	663,552	122,880
p power	A	A	B	B
p' part	A	A	A	A
Class Name	2D	2E	4F	4G
$\|G : C_G(x)\|$	$2^4.3^3.11.13$	$2^4.3^5.5.7.11.13$	$2^4.3^5.5^2.7.11.13$	$2^4.3^8.5.7.11.13$

SPORADIC FISCHER GROUP Fi_{23} ([9], pages 177-179)

The order of Fi_{23} is $4,089,470,473,293,004,800 = 2^{18}.3^{13}.5^2.7.11.13.17.23$. The automorphism group of Fi_{23} is isomorphic to itself and hence there is no noninner automorphism of Fi_{23}.

SPORADIC FISCHER GROUP Fi_{24} ([9], pages 200-207)

The order of Fi_{24} is $1,255,205,709,190,661,721,292,800 = 2^{21}.3^{16}.5^2.7^3.11.13.17.23.29$. The index of inner automorphism group of Fi_{24} in the automorphism group of Fi_{24} is 2.

Table A.6: Some of the Conjugacy Classes of Noninner Automorphisms of Fi_{24}

$\|C_G(x)\|$	220,723,937,280	2,090,188,800
p power	A	A
p' part	A	A
Class Name	2D	4D
$\|G : C_G(x)\|$	$2^3.3^9.5.7^2.13.17.23.29$	$2^7.3^{10}.7^2.11.13.17.23.29$

SPORADIC HIGMAN-SIMS GROUP HS ([9], pages 80-81)

The order of HS is $44,352,000 = 2^9.3^2.5^3.7.11.$ The index of inner automorphism group of HS in the automorphism group of HS is 2.

Table A.7: Some of the Conjugacy Classes of Noninner Automorphisms of HS

$\vert C_G(x)\vert$	40,320	1,920	320	96	40
p power	A	A	A	A	B
p' part	A	A	A	A	A
Class Name	2C	2D	4D	4E	4F
$\vert G : C_G(x)\vert$	$2^2.5^2.11$	$2^2.3.5^2.7.11$	$2^3.3^2.5^2.7.11$	$2^4.3.5^3.7.11$	$2^6.3^2.5^2.7.11$

SPORADIC McLAUGHLIN GROUP M^cL ([9], pages 100-101)

The order of M^cL is $898,128,000 = 2^7.3^6.5^3.7.11.$ The index of inner automorphism group of M^cL in the automorphism group of M^cL is 2.

Table A.8: Some of the Conjugacy Classes of Noninner Automorphisms of M^cL

$\vert C_G(x)\vert$	7,920	720	18	48
p power	A	A	BB	A
p' part	A	A	BB	A
Class Name	2B	4B	6C	8B
$\vert G : C_G(x)\vert$	$2^3.3^4.5^2.7$	$2^3.3^4.5^2.7.11$	$2^6.3^4.5^3.7.11$	$2^3.3^5.5^3.7.11$

SPORADIC HELD GROUP *He* ([9], pages 104-105)

The order of He is $4,030,387,200 = 2^{10}.3^3.5^2.7^3.17$. The index of inner automorphism group of He in the automorphism group of He is 2.

Table A.9: Some of the Conjugacy Classes of Noninner Automorphisms of He

$\|C_G(x)\|$	15,120	240	7,560	72	18
p power	A	A	AC	AC	BC
p' part	A	A	AC	AC	BC
Class Name	2C	4C	6C	6D	6E
$\|G : C_G(x)\|$	$2^6.5.7^2.17$	$2^6.3^2.5.7^3.17$	$2^7.5.7^2.17$	$2^7.3.5^2.7^3.17$	$2^9.3.5^2.7^3.17$

SPORADIC RUDVALIS GROUP *Ru* ([9], pages 126-127)

The order of Ru is $145,926,144,000 = 2^{14}.3^3.5^3.7.13.29$. The automorphism group of Ru is isomorphic to itself and hence there is no noninner automorphism of Ru.

SPORADIC SUZUKI GROUP *Suz* ([9], pages 128-131)

The order of Suz is $448,345,497,600 = 2^{13}.3^7.5^2.7.11.13$. The index of inner automorphism group of Suz in the automorphism group of Suz is 2.

Table A.10: Some of the Conjugacy Classes of Noninner Automorphisms of Suz

index	1,209,600	190,080	2,304	672
p power	A	A	A	B
p' part	A	A	A	A
Class Name	2C	2D	4E	4F
$\|G : C_G(x)\|$	$2^5.3^4.11.13$	$2^6.3^4.5.7.13$	$2^5.3^5.5^2.7.11.13$	$2^8.3^6.5.7.11.13$

SPORADIC O’NAN GROUP $O'N$ ([9], pages 132-133)

The order of $O'N$ is $460,815,505,920 = 2^9.3^4.5.7^3.11.19.31$. The index of inner automorphism group of $O'N$ in the automorphism group of $O'N$ is 2.

Table A.11: Some of the Conjugacy Classes of Noninner Automorphisms of $O'N$

$\|C_G(x)\|$	175,560	30	672
p power	A	AB	A
p' part	A	AB	A
Class Name	2B	6B	8C
$\|G : C_G(x)\|$	$2^3.3^3.7^2.31$	$2^8.3^3.7^3.11.19.31$	$2^4.3^3.5.7^2.11.19.31$

SPORADIC HARADA-NORTON GROUP HN ([9], pages 164-166)

The order of HN is $273,030,912,000,000 = 2^{14}.3^6.5^6.7.11.19$. The index of inner automorphism group of HN in the automorphism group of HN is 2.

Table A.12: Some of the Conjugacy Classes of Noninner Automorphisms of HN

$\|C_G(x)\|$	3,628,800	88,704,000	15,360	1,280
p power	A	A	A	B
p' part	A	A	A	A
Class Name	2C	4D	4E	4F
$\|G : C_G(x)\|$	$2^6.3^2.5^4.11.19$	$2^4.3^4.5^3.19$	$2^4.3^5.5^5.7.11.19$	$2^6.3^6.5^5.7.11.19$

SPORADIC LYONS GROUP Ly ([9], pages 174-175)

The order of Ly is $51,765,179,004,000,000 = 2^8.3^7.5^6.7.11.31.37.67$. The automorphism group of Ly is isomorphic to itself and hence there is no noninner automorphism of Ly.

SPORADIC THOMPSON GROUP Th ([9], pages 176-177)

The order of Th is $90,745,943,887,872,000 = 2^{15}.3^{10}.5^3.7^2.13.19.31$. The automorphism group of Th is isomorphic to itself and hence there is no noninner automorphism of Th.

SPORADIC “BABY MONSTER” GROUP B ([9], pages 208-218)

The order of B is $2^{41}.3^{13}.5^6.7^2.11.13.17.19.23.31.47$. The automorphism group of B is isomorphic to itself and hence there is no noninner automorphism of B.

SPORADIC FISCHER-GRIESS “MONSTER” OR “FRIENDLY GIANT” GROUP M ([9], pages 220-234)

The order of M is $2^{46}.3^{20}.5^9.7^6.11^2.13^3.17.19.23.29.31.41.47.59.71$. The automorphism group of M is isomorphic to itself and hence there is no noninner automorphism of M.

Theorem A.0.13 *Let G be a sporadic simple group. If G has a noninner automorphism, then*

(a) G is one of the following groups

$$M_{12},\ M_{22},\ J_2,\ J_3,\ Fi_{22},\ Fi_{24},\ HS,\ M^cL,\ He,\ Suz,\ O'N,\ HN.$$

(b) G has a noninner automorphism x such that $|G : C_G(x)|$ *is divisible by* 4.

Proof. From the tables given above it is obvious that if G has a noninner automorphism then G is one of the following groups

$$M_{12},\ M_{22},\ J_2,\ J_3,\ Fi_{22},\ Fi_{24},\ HS,\ M^cL,\ He,\ Suz,\ O'N,\ HN.$$

If A is M_{11}, then any noninner automorphism in the conjugacy class $2C$ has index $2^3.3^2.11$ in G which is divisible by 4.

If A is M_{22}, then any noninner automorphism in the conjugacy class $4C$ has index $2^3.3.5.7.11$ in G which is divisible by 4.

If A is J_2, then any noninner automorphism in the conjugacy class $2C$ has index $2^3.3^2.5^2$ in G which is divisible by 4.

If A is J_3, then any noninner automorphism in the conjugacy class $2B$ has index $2^3.3^3.5.19$ in G which is divisible by 4.

If A is Fi_{22}, then any noninner automorphism in the conjugacy class $2D$ has index $2^4.3^3.11.13$ in G which is divisible by 4.

If A is Fi_{24}, then any noninner automorphism in the conjugacy class $2D$ has index $2^3.3^9.5.7^2.13.17.23.29$ in G which is divisible by 4.

If A is HS, then any noninner automorphism in the conjugacy class $2C$ has index $2^2.5^2.11$ in G which is divisible by 4.

If A is M^cL, then any noninner automorphism in the conjugacy class $2B$ has index $2^3.3^4.5^2.7$ in G which is divisible by 4.

If A is He, then any noninner automorphism in the conjugacy class $2C$ has index $2^6.5.7^2.17$ in G which is divisible by 4.

If A is Suz, then any noninner automorphism in the conjugacy class $2C$ has index $2^5.3^4.11.13$ in G which is divisible by 4.

If A is $O'N$, then any noninner automorphism in the conjugacy class $2B$ has index $2^3.3^3.7^2.31$ in G which is divisible by 4.

If A is HN, then any noninner automorphism in the conjugacy class $2C$ has index $2^6.3^2.5^4.11.19$ in G which is divisible by 4. ■

Appendix B

FIXED POINT SUBGROUP OF AUTOMORPHISMS OF SIMPLE GROUPS

In this part, we shall give some information about the fixed point subgroep of automorphisms of finite simple groups of Lie type.

Let K be a simple group of Lie type constructed on a field F of characteristic r and $(\overline{K}, \sigma)$ be a standard σ-setup defined in [17] with subgroups $\overline{B}, B, \overline{T}, H, \overline{U}, U, etc.$ and root system $\sum$ as in [17]. Let $x_{\hat{\alpha}}(.)$ and $h_{\hat{\alpha}}(.)$ be Chevalley generators of K as in [17].

Theorem B.0.14 ([17], Tables 2.5.1 and 2.5.2) *Every automorphism of K is a product $idfg$ such that*

(a) $i \in Inn(K)$

(b) d is a "diagonal" automorphism of K. d is induced by conjugation by an element $h \in N_{\overline{T}}(K)$, so that $x_\alpha(t)^d = x_\alpha(\alpha(h)t)$ for all $\alpha \in \sum$.

(c) f is a "field" automorphism of K, that is, it arises from an automorphism ϕ of $\overline{F}$, and carries the generators $x_{\hat{\alpha}}(t)$, $x_{\hat{\alpha}}(t, u)$, etc. and $h_{\hat{\alpha}}(t)$ to $x_{\hat{\alpha}}(t^\phi)$, $x_{\hat{\alpha}}(t^\phi, u^\phi)$, etc. and $h_{\hat{\alpha}}(t^\phi)$.

(d) g is a "graph" automorphism of K. $g = 1$ unless K is untwisted, and one of the following holds:

(1) $\sum$ has one root length, and for some isometry ρ of $\sum$ carrying $\prod$ to $\prod$, $x_\alpha(t)^g = x_{\alpha^\rho}(\varepsilon_\alpha t)$ for all $\alpha \in \sum$, $t \in \mathbb{F}_q$, where the ε_α are signs and $\varepsilon = 1$ if $\alpha \in \prod$ or $-\alpha \in \prod$; or

(2) $\sum = B_2, F_4$*, or* G_2*, with* $r = 2, 2,$ *or* 3*, respectively and g carries*

$$x_\alpha(t) \mapsto \begin{cases} x_{\alpha^p}(t) & \text{if } \alpha \text{ is long} \\ x_{\alpha^p}(t^r) & \text{if } \alpha \text{ is short} \end{cases}$$

Here ρ *is the unique angle-preserving and length-changing bijection from* $\sum$ *to* $\sum$ *carrying* $\prod$ *to* $\prod$*.*

We shall consider automorphisms of K of prime order. If α is an automorphism of K of prime order p, we shall consider such possible automorphisms in four cases:

(i) $p = 2$, r is odd and α is an inner-diagonal or graph automorphism;

(ii) $r \neq p$, p is odd and α is an inner-diagonal or graph automorphism;

(iii) α is a field automorphism or a graph-field automorphism;

(iv) $r = p$ and α is a graph automorphism.

Case 1 : $p = 2$*,* r *is odd and* α *is an inner-diagonal or graph automorphism*

As the first case we shall consider inner-diagonal involutions and graph involutions of finite simple groups of Lie type.

The tables given below for each family of finite simple groups of Lie type give information about the structure of $C_K(\alpha)$.

Each table has four columns each of which has a speciality.

The first column of each table gives information about the family.

The second column of each table gives special conditions for which such an automorphism exists.

The third column tells the name of the automorphism.

The last column gives the structure of $O^{r'}(C)$ where $C = C_K(\alpha)$.

We start with the families $A_m(q)$ for $m \geq 1$ and $^2A_m(q)$ for $m > 1$. In the table, $A^\varepsilon_m(q)$ denotes $A_m(q)$ for $\varepsilon = 1$, and $^2A_m(q)$ otherwise.

$|A_m(q)| = \frac{1}{(m+1,q-1)} q^{\frac{m(m+1)}{2}} \prod_{i=1}^{m}(q^{i+1} - 1)$ and $|^2A_m(q)| = \frac{1}{(m+1,q+1)} q^{\frac{m(m+1)}{2}} \prod_{i=1}^{m}(q^{i+1} - (-1)^{i+1})$.

We have the following table ([17], Table 4.5.2).

Table B.1: Inner-diagonal and graph involutions of $A_m(q)$ and $^2A_m(q)$

K	Conditions	t	$O^{r'}(C)$
$A_1(q)$		t_1	1
		t'_1	1
$A^\varepsilon_m(q)$ $m \geq 2$ $\varepsilon = \pm 1$		t_1	$A^\varepsilon_{m-1}(q)$
	$2 \leq i \leq \frac{m}{2}$	t_i	$A^\varepsilon_{i-1}(q)A^\varepsilon_{m-i}(q)$
	m odd	$t_{\frac{m+1}{2}}$	$A^\varepsilon_{\frac{m-1}{2}}(q)^2$
	m odd	$t'_{\frac{m+1}{2}}$	$A^\varepsilon_{\frac{m-1}{2}}(q^2)$
	m odd	γ_1	$C_{\frac{m+1}{2}}(q)$
	m even	γ_1	$B_{\frac{m}{2}}(q)$
	m odd	γ_2	$D_{\frac{m+1}{2}}(q)$
	m odd	γ'_2	$^2D_{\frac{m+1}{2}}(q)$

We consider next the family $B_m(q)$ for $m > 1$. We have $|B_m(q)| = \frac{1}{(2,q-1)} q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$

We have the following table ([17], Table 4.5.2).

Table B.2: Inner-diagonal and graph involutions of $B_m(q)$

K	Conditions	t	$O^{r'}(C)$
$B_m(q)$ $m \geq 2$		t_1	$B_{m-1}(q)$
		t'_1	$B_{m-1}(q)$
	$2 \leq i < m$	t_i	$D_i(q)B_{m-i}(q)$
	$2 \leq i < m$	t'_i	${}^2D_i(q)B_{m-i}(q)$
		t_m	$D_m(q)$
		t'_m	${}^2D_m(q)$

Then we consider the family $C_m(q)$ for $m > 2$. We have $|C_m(q)| = \frac{1}{(2,q-1)} q^{m^2} \prod_{i=1}^{m}(q^{2i} - 1)$

We have the following table ([17], Table 4.5.2).

Table B.3: Inner-diagonal and graph involutions of $C_m(q)$

K	Conditions	t	$O^{r'}(C)$
$C_m(q)$ $m \geq 2$	$1 \leq i < \frac{m}{2}$	t_i	$C_i(q)C_{m-i}(q)$
	m even	$t_{\frac{m}{2}}$	$C_{\frac{m}{2}}(q)^2$
	m even	$t'_{\frac{m}{2}}$	$C_{\frac{m}{2}}(q^2)$
		t_m	$A_{m-1}(q)$
		t'_m	${}^2A_{m-1}(q)$

We continue with the families $D_m(q)$ for $m > 3$ and ${}^2D_m(q)$ for $m > 3$. In the table, $D^{\varepsilon}_m(q)$ denotes $D_m(q)$ for $\varepsilon = 1$, and ${}^2D_m(q)$ otherwise.

$|D_m(q)| = \frac{1}{(4,q^m-1)} q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-1}(q^{2i} - 1)$ and

$|{}^2D_m(q)| = \frac{1}{(4,q^m+1)} q^{m(m-1)}(q^m + 1) \prod_{i=1}^{m-1}(q^{2i} - 1)$.

We have the following table ([17], Table 4.5.2 and 4.5.3).

Table B.4: Inner-diagonal and graph involutions of $D_m(q)$ and ${}^2D_m(q)$

K	Conditions	t	$O^{r'}(C)$
$D^{\varepsilon}_m(q)$ $m \geq 4$ $\varepsilon = \pm 1$		t_1	$D^{\varepsilon}_{m-1}(q)$
		t'_1	$D^{-\varepsilon}_{m-1}(q)$
	$2 \leq i < \frac{m}{2}$	t_i	$D_i(q)D^{\varepsilon}_{m-i}(q)$
	$2 \leq i < \frac{m}{2}$	t'_i	${}^2D_i(q)D^{\varepsilon}_{m-i}(q)$
	$K = D^+_{2k}(q)$	$t_{\frac{m}{2}}$	$D_{\frac{m}{2}}(q)^2$
	$K = D^+_{2k}(q)$	$t'_{\frac{m}{2}}$	$D_{\frac{m}{2}}(q^2)$
	$K = D^+_{2k}(q)$	$t''_{\frac{m}{2}}$	$D_{\frac{m}{2}}(q^2)$
	$K = D^+_{2k}(q)$	$t'''_{\frac{m}{2}}$	$D_{\frac{m}{2}}(q^2)$
	$K = D^+_{2k}(q)$	t_{m-1}	$A_{m-1}(q)$
	$K = D^+_{2k}(q)$	t'_{m-1}	${}^2A_{m-1}(q)$
	$K = D^+_{2k}(q)$	t_m	$A_{m-1}(q)$
	$K = D^+_{2k}(q)$	t'_m	${}^2A_{m-1}(q)$
	$K = D^-_{2k}(q)$	$t_{\frac{m}{2}}$	${}^2D_{\frac{m}{2}}(q)D_{\frac{m}{2}}(q)$
	$K = D^-_{2k}(q)$	$t'_{\frac{m}{2}}$	${}^2D_{\frac{m}{2}}(q^2)$

Table B.5: Inner-diagonal and graph involutions of $D_m(q)$ and ${}^2D_m(q)$ continued

K	Conditions	t	$O^{r'}(C)$
$D^{\varepsilon}_m(q)$ $m \geq 4$ $\varepsilon = \pm 1$	$K = D^{\varepsilon}_{2k+1}(q)$	t_m	$A^{\varepsilon}_{m-1}(q)$
		γ_1	$B_{m-1}(q)$
	$2 \leq i \leq \frac{m}{2}$	γ_i	$B_{i-1}(q)B_{m-i}(q)$
	$K = D^{\varepsilon}_{2k+1}(q)$	$\gamma_{\frac{m+1}{2}}$	$B_{\frac{m-1}{2}}(q)^2$
	$K = D^{\varepsilon}_{2k+1}(q)$	$\gamma'_{\frac{m+1}{2}}$	$B_{\frac{m-1}{2}}(q^2)$
	$K = D^{+}_{4}(q)$	γ^{*}_1	$B_3(q)$
	$K = D^{+}_{4}(q)$	γ^{**}_1	$B_3(q)$
	$K = D^{+}_{4}(q)$	γ^{*}_2	$A_1(q)B_2(q)$
	$K = D^{+}_{4}(q)$	γ^{**}_2	$A_1(q)B_2(q)$

We consider next the families $E_6(q)$ and ${}^2E_6(q)$. In the table, $E_6^\varepsilon(q)$ denotes $E_6(q)$ for $\varepsilon = 1$, and ${}^2E_6(q)$ otherwise.

$|E_6(q)| = \frac{1}{(3,q-1)}q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$ and

$|{}^2E_6(q)| = \frac{1}{(3,q+1)}q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$.

We have the following table ([17], Table 4.5.2).

Table B.6: Inner-diagonal and graph involutions of $E_6(q)$ and ${}^2E_6(q)$

K	Conditions	t	$O^{r'}(C)$
$E_6^\varepsilon(q)$ $\varepsilon = \pm 1$		t_1	$D_5^\varepsilon(q)$
		t_2	$A_1(q)A_5^\varepsilon(q)$
		γ_1	$F_4(q)$
		γ_1	$C_4(q)$

We consider next the family $E_7(q)$. We have

$|E_7(q)| = \frac{1}{(2,q-1)}q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1)$

We have the following table ([17], Table 4.5.2).

Table B.7: Inner-diagonal and graph involutions of $E_7(q)$

K	Conditions	t	$O^{r'}(C)$
$E_7(q)$		t_1	$A_1(q)D_6(q)$
		t_4	$A_7(q)$
		t'_4	${}^2A_7(q)$
		t_7	$E_6(q)$
		t'_7	${}^2E_6(q)$

We consider next the family ${}^3D_4(q)$. We have

$|{}^3D_4(q)| = q^{12}(q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1).$

We have the following table ([17], Table 4.5.1).

Table B.8: Inner-diagonal and graph involutions of ${}^3D_4(q)$

K	Conditions	t	$O^{r'}(C)$
${}^3D_4(q)$		t_2	$A_1(q)A_1(q^3)$

We consider next the family $G_2(q)$. We have

$|G_2(q)| = q^6(q^6 - 1)(q^2 - 1).$

We have the following table ([17], Table 4.5.1).

Table B.9: Inner-diagonal and graph involutions of $G_2(q)$

K	Conditions	t	$O^{r'}(C)$
$G_2(q)$		t_1	$A_1(q^2)$

We consider next the family ${}^2G_2(q)$. We have

$|{}^2G_2(q)| = q^3(q^3 + 1)(q - 1)$.

We have the following table ([17], Table 4.5.1).

Table B.10: Inner-diagonal and graph involutions of ${}^2G_2(q)$

K	Conditions	t	$O^{r'}(C)$
${}^2G_2(q)$	$q = 3^{a+\frac{1}{2}}$	t_1	$A_1(q^2)$

We consider next the family $F_4(q)$. We have

$|F_4(q)| = q^{24}(q^{12} - 1)(q^8 - 1)(q^6 - 1)(q^2 - 1)$.

We have the following table ([17], Table 4.5.1).

Table B.11: Inner-diagonal and graph involutions of $F_4(q)$

K	Conditions	t	$O^{r'}(C)$
$F_4(q)$		t_1 t_4	$A_1(q)C_3(q)$ $B_4(q)$

We consider next the family $E_8(q)$. We have

$|E_8(q)| = q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q2-1).$

We have the following table ([17], Table 4.5.1).

Table B.12: Inner-diagonal and graph involutions of $E_8(q)$

K	Conditions	t	$O^{r'}(C)$
$E_8(q)$		t_1	$D_8(q)$
		t_8	$A_1(q)E_7(q)$

Case 2: *$r \neq p$, p is odd and α is an inner-diagonal or graph automorphism*

In this case, G is either $A_m(q)$ or ${}^2A_m(q)$ or $E_6(q)$.

We have the following theorem for $A_m(q)$ and ${}^2A_m(q)$:

Theorem B.0.15 ([17], Theorem 4.8.4) *Let K be a classical group with underlying classical space V. Let p be an odd prime and let x be an inner-diagonal automorphism of K of order p which is not inducced by an element of $Isom(V)$ of order p. Then $Isom(V) = GL_n^\varepsilon(q)$ for some sign ε such that p divides both $m+1$ and $q-\varepsilon$. Let ω be a generator of a Sylow p-subgroup of the cyclic subgroup of $\overline{F}^\times$ of order $q-\varepsilon$. For a suitable choice of ω, x is induced by an element x_0 of $Isom(V)$ such that x_0^p is scalar multiplication by ω.*

Let $C = C_{GL^\varepsilon(V)}(x_0)$ and let C^* be the preimage in $GL^\varepsilon(V)$ of $C_{PGL^\varepsilon(V)}(x)$. Then $C \cong GL^\varepsilon_{n/p}(q^p)$ and $C^* = C\langle\phi\rangle$, where $\phi^p = 1$ and ϕ induces a field automorphism on C.

We next give a table about the structure of $C_{K^*}(t)$ where K^* denotes the extension group K by its diagonal automorphisms where K is either $E_6(q)$ or ${}^2E_6(q)$.

The second column of the table gives the name of automorphism and the last column gives the structure of $O^{r'}(C)$ where $C = C_{K^*}(t)$.

We have the following table ([17], Table 4.7.3A).

Table B.13: $C = C_{K^*}(t)$, $t \in Inndiag(K)\Gamma_K$ of order $p = 3$, $q \equiv \varepsilon$ (mod3)

K	t	$O^{r'}(C)$
$E_6^{\varepsilon}(q)$	$t_1^{\pm 1}$	$D_5^{\varepsilon}(q)$
	$t_2^{\pm 1}$	$A_1(q)A_4^{\varepsilon}(q)$
	t_3	$A_2^{\varepsilon}(q)^3$
	$t_3'^{\pm 1}$	$A_2^{\varepsilon}(q^3)$
	t_4	$A_5^{\varepsilon}(q)$
	$t_{1,6}$	$D_4(q)$
	$t_{1,6}'^{\pm 1}$	${}^3D_4(q)$
$E_6^{-\varepsilon}(q)$	t_3	$A_2^{\varepsilon}(q)A_2(q^2)$
	t_4	$A_5^{-\varepsilon}(q)$
	$t_{1,6}$	${}^2D_4(q)$

Case 3: *α is a field automorphism or a graph-field automorphism*

Next, we consider the case of field or graph-field automorphisms with no restriction on r. Then, we have an important theorem in the classification of finite simple groups:

Theorem B.0.16 ([17], Proposition 4.9.1) *Let $K =^d \sum(q)$ be a simple group of Lie type over a base field of characteristic r, let x be a field or graph-field automorphism of K of prime order p, and set $K_x = O^{r'}(C_K(x))$. Then*

If x is a field automorphism, then $K_x \cong^d \sum(q^{1/p})$, while if x is a graph-field automorphism, then $d = 1$, $p = 2$ or 3, and $K_x \cong^p \sum(q^{1/p})$.

Case 4: *$r = p$ and α is a graph automorphism*

Theorem B.0.17 ([17], Proposition 4.9.2) *If $K \in Lie(p)$ has a graph automorphism of order p then the following conditions hold:*

(a) Either K is untwisted and there is $\gamma \in \Gamma_K$ of order p, or K is a Steinberg group and there is $\gamma \in \Phi_K$ of order p.

(b) For γ as in (a), $C_K(\gamma) \in Lie(p)$ and one of the following holds:

(1) $p = 2$, $K \cong A^{\pm}_m(q)$, m odd, $m > 1$, and $C_K(\gamma) \cong C_{\frac{m+1}{2}}(q)$;

(2) $p = 2$, $K \cong A^{\pm}_m(q)$, m even, and $C_K(\gamma) \cong C_{\frac{m}{2}}(q)$;

(3) $p = 2$, $K \cong D^{\pm}_m(q)(\cong \Omega^{\pm}_{2m}(q), m > 3)$, $K\langle\gamma\rangle \cong O^{\pm}_{2m}(q)$ and $C_K(\gamma) \cong B_{m-1}(q)$;

(4) $p = 2$, $K \cong E^{\pm}_6(q)$ and $C_K(\gamma) \cong F_4(q)$; or

(5) $p = 3$, $K \cong D_4(q)$ or ${}^3D_4(q)$, and $C_K(\gamma) \cong G_2(q)$.

Appendix C

OUTER AUTOMORPHISMS OF $PSL(n, \mathbb{F}_q)$

In this chapter, we shall give some information on the outer automorphism groups of $PSL(n, \mathbb{F}_q)$ where $q = r^f$ for some prime number r and integer f. These information can also be found in [30], Section 3.3.4 in more detail.

From Appendix B we know that the outer automorphism groups of all the classical groups have a uniform description in terms of diagonal, field, and graph automorphisms.

As being induced by conjugation by diagonal matrices with respect to a suitable basis, we call the first type as diagonal automorphisms. As $SL(n, \mathbb{F}_q)$ is a normal subgroup of $GL(n, \mathbb{F}_q)$, $GL(n, \mathbb{F}_q)$ acts by conjugation on $SL(n, \mathbb{F}_q)$ as a group of automorphism. This action induces the action of $PGL(n, \mathbb{F}_q)$ on $PSL(n, \mathbb{F}_q)$ as a group of automorphisms of $PSL(n, \mathbb{F}_q)$. This group is called the group of diagonal outer automorphisms and corresponds to the quotient group $PGL(n, \mathbb{F}_q)/PSL(n, \mathbb{F}_q)$ which is a cyclic group of order $d = (n, q - 1)$.

The automorphism group of the underlying field $\mathbb{F}_q$, a cyclic group of order f, is the group generated by the Frobenius automorphism, $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ given by $\sigma(x) = x^r$. The field automorphisms of $GL(n, \mathbb{F}_q)$ are induced by automorphisms of the underlying field. The automorphism of $GL(n, \mathbb{F}_q)$ induced by σ is given by $A^\sigma = (A_{ij}^r)$ for each element $A = (A_{ij})$ of $GL(n, \mathbb{F}_q$. The group $G\langle\sigma\rangle$ which is the semidirect product of $GL(n, \mathbb{F}_q)$ with the group of field automorphisms is denoted by $\Gamma L(n, \mathbb{F}_q)$, and correspondingly the extension of $SL(n, \mathbb{F}_q)$, $PGL(n, \mathbb{F}_q)$ or $PSL(n, \mathbb{F}_q)$ by the induced group of field automorphisms is denoted by $\sum L(n, \mathbb{F}_q)$, $P\Gamma L(n, \mathbb{F}_q)$ or $P \sum L(n, \mathbb{F}_q)$.

The graph automorphisms are induced by an automorphism of the Dynkin diagram. The classical concept of duality is the best explanation of the graph automorphism in the case of the linear groups. For a vector space V and a basis $\{e_1, \dots, e_n\}$ of V, the basis $\{e_1^*, \dots, e_n^*\}$ of

V^* given by $e_i^*(e_i) = 1$ and $e_i^*(e_j) = 0$ if $i \neq j$ is a well-defined dual basis.

If the action of $g \in GL(V)$ on V and V^* are given respectively by

$$e_i \mapsto \sum_{i=1}^{n} g_{ij} e_j$$

and

$$e_i^* \mapsto \sum_{i=1}^{n} h_{ij} e_j^*$$

then as $a_i^*(a_j) = \delta_{ij}$ where δ_{ij} is the kronecker delta, we have

$$\delta_{ij} = \sum_{k=1}^{n} h_{ik} e_k^* \left(\sum_{l=1}^{n} g_{jl} e_l \right) = \sum_{k=1}^{n} h_{ik} \left(\sum_{l=1}^{n} g_{jl} e_k^*(e_l) \right) = \sum_{k=1}^{n} h_{ik} g_{jk}$$

Thus, if $h = (h_{ij})$ and $g = (g_{ij})$, then $hg^T = I_n$ and hence $h = (g^{-1})^T = (g^T)^{-1}$. The duality automorphism (with respect to these bases) of $GL(V)$ is the map which replaces each matrix by the transpose of its inverse. This is the so called graph automorphism of $GL(V)$.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name : Türkan, Erkan Murat

Nationality : Turkish (TC)

Date and Place of Birth : 30 November 1980, Akçaabat

Marital Status : Single

email : emturkan@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
BS	METU Department of Mathematics	2004
High School	Tülay Başaran Anatolian High School, Samsun	1998

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2011 March-June	Atılım University Department of Mathematics	Part Time Instructor
2005-2010	METU Department of Mathematics	Research Assistant

SCHOLARSHIP AND ACADEMIC VISITS

- May 2010-January 2011, Project Scholarship Granted by The Scientific and Technological Research Counsil of Turkey (TUBITAK) Project Number: 109T664
- August 2008-August 2009, Academic Visit, University of Florida, Gainesville, FL, USA, granted by TUBITAK