This is to certify that the
dissertation entitled

CENTRALIZERS OF ELEMENTS OF PRIME ORDER IN LOCALLY FINITE SIMPLE GROUPS

presented by

Elif Seçkin

has been accepted towards fulfillment
of the requirements for the

Ph.D. degree in Mathematics

Major Professor's Signature

12/13/2007

Date

CENTRALIZERS OF ELEMENTS OF PRIME ORDER IN LOCALLY FINITE SIMPLE GROUPS

By

Elif Seçkin

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

2008

ABSTRACT

CENTRALIZERS OF ELEMENTS OF PRIME ORDER IN LOCALLY FINITE SIMPLE GROUPS

By

Elif Seçkin

This thesis is mainly focused on the centralizer of elements of prime order. We prove a result which gives all the cases where $C_G(g_1) = C_G(g_2)$ holds for $G = \mathrm{PGL}_{\mathbb{K}}(V)$ or $G = \mathrm{PSL}_{\mathbb{K}}(V)$ if V is a finite dimensional $\mathbb{K}$-space and $g_1, g_2 \in G$ of prime order r such that $r \neq \mathrm{char}\,\mathbb{K}$. A similar result is obtained for finite alternating groups. We prove that a simple locally finite group containing an element of prime order p whose centralizer is abelian is either linear or a group of p-type. Another result presented is that any non-linear simple locally finite group contains a p-subgroup which is not Černikov. This in turn proves that such a group contains an infinite abelian p-subgroup.

To the memory of Dr. Richard E. Phillips

ACKNOWLEDGMENTS

I would like to express my deepest and sincerest gratitude to my advisor, Ulrich Meierfrankenfeld, for his exceptional support and constant encouragement, without which this thesis would not have been possible. I am very thankful to him for his understanding, boundless patience with me, and not giving up on me. It has been an honor to work with him and the time I have spent as his apprentice will forever be appreciated.

I would also like to express my gratitude to Jonathan I. Hall, Jeanne Wald, Ronald Fintushel, and Abdul Sami for agreeing to be on my committee, for their kindness, and support. I am thankful to Dr. Fintushel for introducing me to Beamer and for his joyful chats. I would like to thank to Abdul Sami for his friendship and for valuable conversations.

I would like to thank to my dear friend Jui-Ling Yu for supporting me when I needed help most and for encouraging me to continue. Her friendship have helped me immensely. I am also very grateful to my friend Onur Ağırseven for his continual help. Finally, I want to thank my brothers H. Murat Seçkin and Şahin Seçkin for their love and support.

I would like to once again dedicate this work to the memory of Dr. Richard E. Phillips, my thesis advisor at the beginning of my doctoral studies.

TABLE OF CONTENTS

Introduction

Centralizers have long played a very important role in the theory of finite as well as locally finite groups. These subgroups are one of the key tools that can be used to obtain detailed information about the structure of the group itself.

In this dissertation, we focus on the centralizer of elements of prime order. The thesis is organized as follows. In Chapter 2 and 3, we investigate the cases when two such centralizers are equal in certain groups. In other words, the following question is considered in these chapters:

Question 1. Let G be a group and $a, b \in G$ be elements of prime order r such that $C_G(a) = C_G(b)$. Then what can be said about (G, a, b) ?

In Chapter 2, we deal with the case when G is a projective linear or a special linear group. More precisely, in Section 2.1 we prove a result (Theorem 2.1.1) that characterizes exactly when $C_G(g_1) = C_G(g_2)$ holds for $G = \mathrm{PGL}_{\mathbb{K}}(V)$ if V is a finite dimensional $\mathbb{K}$-space and $g_1, g_2 \in G$ of prime order r such that $r \neq \operatorname{char}\mathbb{K}$. A similar result is obtained for the group $\mathrm{PSL}_{\mathbb{K}}(V)$ in Section 2.2 (Theorem 2.2.3). The key lemmas giving the structure and properties of $C_G(g_i)$ that are needed for the proofs of theorems in Chapter 2 are provided in the first two sections of Chapter 1. Some small cases (i.e., when $\dim V \leq 3$ and $|\mathbb{K}| \leq 5$) appearing in these results are investigated in Section 1.3.

In Chapter 3, we consider the finite alternating group $\mathrm{Alt}(n)$ and determine all possibilities for (n, x, y) such that $x, y \in \mathrm{Alt}(n)$ of prime order, $\langle x \rangle \neq \langle y \rangle$ and $C_{\mathrm{Alt}(n)}(x) = C_{\mathrm{Alt}(n)}(y)$.

Chapter 4 is, roughly speaking, about the centralizers of elements of prime order in a simple locally finite group. In order to give a more precise description of each section we shall need some definitions as well as the classification theorems that are used in our proofs.

- Let G be a group. G is called *locally finite* if every finite subset of G generates a finite subgroup of G. G is a *LFS-group* if G is a simple, locally finite group.
- A set of pairs $\{(H_i, M_i) \mid i \in I\}$ is called a *Kegel cover* for G if, for all $i \in I$, H_i is a finite subgroup of G, M_i is a maximal normal subgroup of H_i and for each finite subgroup $F \leq G$ there exists $i \in I$ with $F \leq H_i$ and $F \cap M_i = 1$. The groups H_i/M_i, $i \in I$, are called the factors of the Kegel cover.

It has been shown in [13, p.113] that every LFS-group has a Kegel cover. Kegel covers are one of the important tools in the study of locally finite groups because using Kegel covers many question about LFS-groups can be transferred to questions about finite simple groups, which in turn may be answered using the classification of finite simple groups.

- A group G is called *finitary* if there exists a field $\mathbb{K}$ and a faithful $\mathbb{K}G$-module V such that $\dim_{\mathbb{K}}[V, g] < \infty$ for all $g \in G$ where $[V, g] := \{v(g-1) | \, v \in V\}$.

The classification of infinite finitary LFS-groups has been completed:

(a) those that are linear have been classified independently by several authors:

Theorem 1 ([1, 2, 10, 17]) *Each LFS-group which is not finite but has a faithful representation as a linear group in finite dimension over a field is isomorphic to a group of Lie type over an infinite locally finite field.*

(b) those that are non-linear have been classified by J. I. Hall:

Theorem 2 ([8]) *Each LFS-group which is not linear in finite dimension but has a faithful representation as a finitary linear group over a field is isomorphic to one the following holds*:

(1) *an alternating group* $\mathrm{Alt}(\Omega)$ *with* Ω *infinite*;

(2) *a finitary classical group*: $FSp_K(V,s)$, $FSU_K(V,u)$, $F\Omega_K(V,q)$;

(3) *a special transvection group* $T_K(W,V)$.

Here K *is a (possibly finite) subfield of* $\overline{\mathbb{F}}_p$, *for some prime* p; *the forms* s, u, *and* q *are non-degenerate on the infinite dimensional* K*-space* V; *and* W *is a subspace of the dual* $V^\star$ *whose annihilator in* V *is trivial*: $0 = \{v \in V \mid vW = 0\}$.

Let G be a non-finitary LFS-group. Then

- G is of *alternating type* if G has a Kegel cover all of whose factors are alternating groups.
- G is of p*-type* for some prime p if every Kegel cover for G contains at least one factor which is isomorphic to a classical group defined over a field in characteristic p.

In [14, Theorem A], U. Meierfrankenfeld proved an important result on the structure of an arbitrary LFS-group showing that any LFS-group can be sorted into one of the following classes:

Theorem 3 ([14]) *Let G be a LFS-group. Then one of the following holds*:

(a) *G is finitary.*

(b) *G is of alternating type.*

(c) *There exists a prime p and a Kegel cover $\{(H_i, M_i) \mid i \in I\}$ for G such that G is of p-type and for all $i \in I$, $H_i/O_p(H_i)$ is the central product of perfectcentral extension of classical groups defined over a field in characteristic p and H_i/M_i is a projective special linear group.*

It is possible to split the groups of alternating type into two categories. First, let us give more notation and terminology. Let G be an infinite LFS-group, H a finite subgroup of G and Ω an H-set such that $|\Omega| \geq 7$ and $H/C_H(\Omega) \cong \mathrm{Alt}(\Omega)$. Let $\mathcal{A}$ be the class of such pairs (H, Ω). Note that G is of alternating type if and only if for each finite subgroup F of G there exists $(H, \Omega) \in \mathcal{A}$ such that $F \leq H$ and F acts faithfully on Ω. Let G be of alternating type, $F \leq G$ be finite, and define

$$\mathcal{A}_{reg}(F) := \{(H, \Omega) \in \mathcal{A} \mid F \leq H \text{ and } F \text{ has a regular orbit on } \Omega\}.$$

Then

- F is called *regular* if $\mathcal{A}_{reg}(F)$ is a Kegel cover for G.
- G is of *regular alternating type* if G is locally regular, that is, every finite subgroup of G is regular.
- F is called *non-regular* if there exists a finite subgroup F^* of G with $F \leq F^*$ such that for all $(H, \Omega) \in \mathcal{A}$ with $F^* \leq H$, F has no regular orbit on Ω.
- G is called *non-regular alternating type* if G is of alternating type and G has a non-regular finite subgroup.

There is another characterization of regular and non-regular alternating type groups given in [4, Theorem 1.4], for which the following definitions are needed.

- G is of 1-*type* if every Kegel cover has a factor which is an alternating group.
- We say that G is of ∞-*type* if the following property holds:
  Let $\mathcal{S}$ be any class of finite simple groups such that every finite group can be embedded into a member of $\mathcal{S}$. Then there exists a Kegel cover for G all of whose factors are isomorphic to a member of $\mathcal{S}$.

Theorem 4 ([4]) *Let G be a LFS-group of alternating type.*

(a) *G is of non-regular type if and only if G is of 1-type.*

(b) *G is of regular alternating type if and only if G is of ∞-type.*

In [6], it is proven that if G is a locally finite simple group of alternating type, p is a prime, and $Z \leq G$ is an elementary abelian subgroup of order p^2, then there exists $1 \neq z \in Z$ with $C_G(z) \neq C_G(Z)$. One might ask whether a stronger result is true; namely,

Question 2. Let G be a locally finite simple group of alternating type and p be a prime. Does $C_G(a) \neq C_G(b)$ hold for all $a, b \in G$ with $|a| = |b| = p$ and $\langle a \rangle \neq \langle b \rangle$.

Note that this is a special case of Question 1. In Section 4.1, we observe that Question 2 is true when G is a regular alternating group (see Theorem 4.1.2), and we also prove that if G is a non-regular alternating group, $C_G(x)$ is non-abelian for $x \in G$ with $|x| = p$, p a prime. One of the corollaries we derive from these results is the following: If G is a LFS-group of alternating type, then $C_G(x)$ is non-abelian for any $x \in G$ with $|x| = p$ (see Theorem 4.2.5). In addition to this, Section 4.2 answers the following question.

Question 3. What can be said about the structure of a simple locally finite group containing an element of prime order p whose centralizer is abelian.

This question is stated by Hartley in [9, page 39] and it is mentioned that "We have not been able to say anything about the structure of such a group even with the assumption that the centralizer is elementary abelian." We shall show that the group under consideration must be either linear or a group of p-type. For the proof of this result, we shall be using the classifications mentioned above in Theorems 2 and 3.

Finally, in the last chapter, we prove that a non-linear LFS-group contains a p-subgroup which is not Černikov where p is a prime. This enables us to show that such a group contains an infinite abelian p-subgroup.

Chapter 1

Preliminaries

This chapter provides the definitions, notation and lemmas that will be used in Chapter 2. Some well-known material is included in order to make the presentation self-contained. Throughout this chapter we assume the following:

> $\mathbb{K}$ *is a field of characteristic* p, p *is a prime or zero,* V *is a finite dimensional* $\mathbb{K}$*-space,* $G = \mathrm{GL}_{\mathbb{K}}(V)$, $\overline{G} = G/Z(G) = \mathrm{PGL}_{\mathbb{K}}(V)$, $S = \mathrm{SL}_{\mathbb{K}}(V)$, $\overline{S} = \mathrm{PSL}_{\mathbb{K}}(V)$ *and* r *is a prime.*

Also, we regard $\mathbb{K}$ as a subring of $\mathrm{End}_{\mathbb{K}}(V)$, that is, we identify k with $k\,\mathrm{id}_V$ for $k \in \mathbb{K}$.

1.1 Structure of Centralizer in $\mathrm{GL}_{\mathbb{K}}(V)$

Lemma 1.1.1 *Assume that* $r \neq p$. *Let* $x^r - 1 = \prod_{i=0}^{m} t_i(x)$ *where* $t_i(x) \in \mathbb{K}[x]$ *is irreducible and* $t_0 = x - 1$. *Let* $\mathbb{E}$ *be a splitting field for* $x^r - 1$ *over* $\mathbb{K}$. *Let* ξ_i *be a root of* t_i *in* $\mathbb{E}$. *Then*

(a) $x^r - 1$ *has* r *distinct roots in* $\mathbb{E}$.

(b) $t_i(x) \neq t_j(x)$ *for all* $0 \leq i < j \leq m$.

(c) $\mathbb{E} = \mathbb{K}[\xi_i]$ *for all* $1 \leq i \leq m$.

(d) *Let* $d = \dim_{\mathbb{K}} \mathbb{E}$. *Then* $\deg t_i = d$ *for all* $1 \leq i \leq m$.

Proof: (a) $rx^{r-1} \neq 0$ since $\operatorname{char} \mathbb{K} \neq r$. So $\gcd(x^r - 1, rx^{r-1}) = 1$ and hence $x^r - 1$ has no multiple roots in $\mathbb{E}$.

(b) This is immediate from part (a).

(c) Any root of $t_i(x)$, $1 \leq i \leq m$, is a primitive r-th root of unity and ξ_i is algebraic over $\mathbb{K}[x]$. Therefore $\mathbb{K}[\xi_i] = \mathbb{K}(\xi_i)$ and it contains all the roots of $x^r - 1$, that is, it contains $\mathbb{E}$. The other inclusion, $\mathbb{K}(\xi_i) \subseteq \mathbb{E}$, is obvious. Thus $\mathbb{K}(\xi_i) = \mathbb{E} = \mathbb{K}[\xi_i]$.

(d) For all $1 \leq i \leq m$, we have $d = \dim_{\mathbb{K}} \mathbb{E} = [\mathbb{E} : \mathbb{K}] = [\mathbb{K}(\xi_i) : \mathbb{K}] =$ degree of the minimal polynomial of ξ_i over $\mathbb{K}[x] = \deg t_i$.

Definition 1.1.2 *Let* $\mathbb{K}$ *be a subfield of a field* $\mathbb{F}$ *and* V *be an* $\mathbb{F}$*-space. Then* $\Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$ *is the set of all* $\mathbb{F}$*-semilinear isomorphisms of* V *which are* $\mathbb{K}$*-linear. So if* $h \in \mathrm{GL}_{\mathbb{K}}(V)$, *then* $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$ *if and only if there exists* $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ *with* $h(fv) = \sigma(f)(hv)$ *for all* $v \in V$ *and* $f \in \mathbb{F}$.

Lemma 1.1.3 *Let* $\mathbb{F}$ *be a subfield of* $\mathrm{End}_{\mathbb{K}}(V)$ *containing* $\mathbb{K}$. *If* $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$ *acts* σ*-semilinearly, then* $hfh^{-1} = \sigma(f)$ *for all* $f \in \mathbb{F}$. *Moreover,* $\Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V) = N_{\mathrm{GL}_{\mathbb{K}}(V)}(\mathbb{F})$.

Proof: Let $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$ be σ-semilinear. Then $h(fv) = \sigma(f)(hv)$ for all $v \in V$ and $f \in \mathbb{F}$ by definition. Thus $hf = \sigma(f)h$ and hence $hfh^{-1} = \sigma(f)$ for all $f \in \mathbb{F}$, proving the first statement.

For the proof of the second statement, let $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$ with $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ as the corresponding automorphism. Then $hfh^{-1} = \sigma(f) \in \mathbb{F}$ for all $f \in \mathbb{F}$ by the

first part. Hence h normalizes $\mathbb{F}$, giving us $\Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V) \subseteq N_{\mathrm{GL}_{\mathbb{K}}(V)}(\mathbb{F})$. For the converse inclusion, take $h \in N_{\mathrm{GL}_{\mathbb{K}}(V)}(\mathbb{F})$. Then $hfh^{-1} \in \mathbb{F}$ for all $f \in \mathbb{F}$. Defining $\sigma(f) := hfh^{-1}$, we see that $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ and $h(fv) = \sigma(f)(hv)$ for $v \in V$, $f \in \mathbb{F}$. Hence $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{F}}(V)$.

Lemma 1.1.4 *Let $g \in G$ and $\overline{g} = gZ(G) \in \overline{G}$. Assume that $\mathbb{E} := \mathbb{K}[g] \leq \mathrm{End}_{\mathbb{K}}(V)$ is a field. Then*

$$\mathrm{GL}_{\mathbb{E}}(V) = C_G(g) \subseteq C_G(\overline{g}) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}}(V). \tag{1.1}$$

Proof: Let us first prove $\mathrm{GL}_{\mathbb{E}}(V) = C_G(g)$:
If $x \in C_G(g)$, then $xg^n = g^n x$ for all $n \in \mathbb{Z}^+$. Therefore, $xp(g) = p(g)x$ for any $p(x) \in \mathbb{K}[x]$ and hence $xe = ex$ for $e \in \mathbb{E}$, that is, $x \in \mathrm{GL}_{\mathbb{E}}(V)$ which gives $C_G(g) \subseteq \mathrm{GL}_{\mathbb{E}}(V)$. For the converse inclusion, observe that any element in $\mathrm{GL}_{\mathbb{E}}(V)$ commutes with g since $\mathbb{E} = \mathbb{K}[g]$. Hence $\mathrm{GL}_{\mathbb{E}}(V) \subseteq C_G(g)$, giving the first equality in (1.1).
Now we shall show the last inclusion as the other one is obvious. Let $h \in C_G(\overline{g})$. Then $g^h = \eta g \in \mathbb{E}$ for some $\eta \in \mathbb{K}$. Hence $hg^n h^{-1} \in \mathbb{E}$ for all $n \in \mathbb{Z}^+$ and so $heh^{-1} \in \mathbb{E}$ for all $e \in \mathbb{E}$. That is, $h \in N_G(\mathbb{E})$ and hence $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}}(V)$ by Lemma 1.1.3.

Lemma 1.1.5 *Assume that $r \neq p$ and let $g \in G$ with $g^r = 1$. Let $f(x)$ be the minimal polynomial of g. Then the following holds*:

(a) *$f(x)$ divides $x^r - 1$ in $\mathbb{K}[x]$.*

(b) *$f(x) = \prod_{i=1}^{s} f_i(x)$ where f_i's are pairwise distinct and $f_i = t_{i'}$ for some $0 \leq i' \leq m$.*

(c) *For* $1 \leq i \leq s$, *let* $V_i = \mathrm{Ann}(f_i(g)) := \{v \in V \mid f_i(g)v = 0\}$. *Then* $V_i \neq 0$ *for all* i *and*

$$V = \bigoplus_{i=1}^{s} V_i.$$

(d) *Let* g_i *be the restriction of* g *to* V_i. *Then* $f_i(g_i) = 0$.

(e) *Let* $\mathbb{E}_i = \mathbb{K}[g_i]$ *be the* $\mathbb{K}$*-subalgebra of* $\mathrm{End}_{\mathbb{K}}(V_i)$ *generated by* g_i. *Then* $\mathbb{E}_i \cong \mathbb{K}[x]/f_i(x)\mathbb{K}[x]$.

(f) $\mathbb{E}_i = \mathbb{K}$ *if* $f_i(x) = x - 1$ *and* $\mathbb{E}_i \cong \mathbb{E}$ *if* $f_i(x) \neq x - 1$ *where* $\mathbb{E}$ *is a splitting field for* $x^r - 1$ *over* $\mathbb{K}$.

(g) V_i *is a vector space over* $\mathbb{E}_i$ *and*

$$\bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i) = C_G(g)$$

where we identify $\bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i)$ *with its image in* $\mathrm{GL}_{\mathbb{K}}(V)$.

Proof: (a) This is obvious as g satisfies the polynomial $x^r - 1 \in \mathbb{K}[x]$.

(b) Follows from Lemma 1.1.1 since $f(x) \mid x^r - 1$.

(c) Each V_i is a g-invariant subspace and V is a direct sum of these subspaces are from a theorem about decomposition of a vector space via a linear transformation (see [11, Theorem 12, p.220]). Also note that, for each $1 \leq i \leq s$, $V_i \neq 0$ because otherwise $f(x)/f_i(x)$ would be the minimal polynomial of g, contradiction.

(d) By definition of V_i, we have $f_i(g)v_i = 0$ for all $v_i \in V_i$. Hence $f_i(g_i) = 0$.

(e) Let $m(x)$ be a polynomial in $\mathbb{K}[x]$ such that $m(g_i) = 0$. Then $m(g)q_i(g) = 0$ where $q_i(x) = f(x)/f_i(x)$. Since f is the minimal polynomial of g, f divides mq_i and hence f_i divides m. This shows that $f_i(x)$ is the minimal polynomial of g_i. Consider now the map $\vartheta : \mathbb{K}[x] \longrightarrow \mathrm{End}_{\mathbb{K}}(V_i)$ given by $\vartheta(m(x)) = m(g_i)$. We

observe that the kernel of ϑ is $f_i(x)\mathbb{K}[x]$ and the image is $\mathbb{K}[g_i]$, giving the required isomorphism of part (e).

(f) If $f_i(x) = x - 1$, then $f_i(g_i) = 0$ implies that $g_i = 1$ and hence $\mathbb{E}_i = \mathbb{K}[g_i] = \mathbb{K}$. If $f_i(x) \neq x - 1$ then $g_i \neq 1$. Part (e) and Lemma 1.1.1 easily imply that $\mathbb{E}_i = \mathbb{K}[x]/f_i(x)\mathbb{K}[x] \cong \mathbb{K}[\xi_i'] = \mathbb{E}$ where ξ_i' is a root of the irreducible polynomial $f_i(x)$.

(g) For any $v \in V_i$ and $e \in \mathbb{E}_i \leq \mathrm{End}_{\mathbb{K}}(V_i)$, let us define $e \cdot v := e(v)$. It is straight forward to check that this multiplication gives an $\mathbb{E}_i$-module structure on V_i. Note also that $\mathbb{E}_i$ is a field because it is isomorphic to either $\mathbb{K}$ or $\mathbb{E}$ by part (f), giving us the first part.

For the second part, let $1 \leq i \leq s$. If $h \in C_G(g)$, then $hg^n = g^n h$ for all $n \in \mathbb{Z}^+$ and hence $hp(g) = p(g)h$ for any polynomial $p(x) \in \mathbb{K}[x]$. In particular, $hf_i(g) = f_i(g)h$. Applying $v_i \in V_i$ to both sides of this equation and using part (d), we get $0 = f_i(g)h(v_i)$. So $h(v_i) \in V_i$ by definition of V_i. Define h_i as the restriction of h on V_i. Then h_i is a $\mathbb{K}$-linear map on V_i. In fact it is $\mathbb{E}_i$-linear since $h_i g_i = g_i h_i$ and $\mathbb{E}_i = \mathbb{K}[g_i]$. Hence, $h_i \in \mathrm{GL}_{\mathbb{E}_i}(V_i)$ implies that $C_G(g) \leq \bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i)$ with the correspondence $h \mapsto (h_1, h_2, \cdots, h_s)$. For the converse inclusion, note that since $\mathbb{E}_i$ is a field for each $1 \leq i \leq s$, we can apply Lemma 1.1.4 and conclude that $\mathrm{GL}_{\mathbb{E}_i}(V_i) = C_{\mathrm{GL}_{\mathbb{K}}(V_i)}(g_i) \subseteq C_{\mathrm{GL}_{\mathbb{K}}(V)}(g)$. Thus $\bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i) \leq C_G(g)$.

Remark 1.1.6 *Let H be a group and assume that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$ where V_i's are simple $\mathbb{K}H$-submodules of V for $1 \leq i \leq s$. Then $\{V_i \mid 1 \leq i \leq s\}$ is the set of all simple $\mathbb{K}H$-submodules of V if and only if the V_i's are pairwise non-isomorphic.*

Proof: ($\Longrightarrow$) Without loss of generality, assume that $V_1 \cong V_2$ as $\mathbb{K}H$-modules. Then there exists a $\mathbb{K}$-linear map $f : V_1 \longrightarrow V_2$ such that $f(hv_1) = hf(v_1)$ for all $h \in H$ and $v_1 \in V_1$. Let us denote the image of v_1 under f by $\overline{v}_1$. Then

$W := \{(v_1, \bar{v}_1, 0, \ldots, 0) \mid v_1 \in V_1\}$ is a nonzero simple $\mathbb{K}H$-submodule of V and $W \neq V_i$ for any i, a contradiction. Hence V_i's are pairwise non-isomorphic.

($\Longleftarrow$) Let W be a nonzero simple $\mathbb{K}H$-submodule of V. Then the projection $\pi_i : W \to V_i$ is nontrivial for some $1 \leq i \leq s$. Since both W and V_i are simple submodules, $W \cong V_i$ by Schur's Lemma. So $W \ncong V_j$ and thus $\pi_j = 0$ for all $j \neq i$. Therefore $W = V_i$ for some i, as desired.

Lemma 1.1.7 *Let $\mathbb{E}_i$ be a field containing $\mathbb{K}$ for $1 \leq i \leq s$. Assume that $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$ where V_i is an $\mathbb{E}_i$-space and $\dim_{\mathbb{E}_i} V_i \neq 1$ for all i. Let $H = \bigtimes_{i=1}^{s} \mathrm{SL}_{\mathbb{E}_i}(V_i)$. Then*

(a) *V_i's are pairwise non-isomorphic.*

(b) *$\{V_i \mid 1 \leq i \leq s\}$ is the set of all simple $\mathbb{K}H$-submodules of V.*

Proof: (a) Since for any $j \in \{1, 2, \ldots, s\}$

$$C_H(V_j) = \bigtimes_{i \neq j}^{s} \mathrm{SL}_{\mathbb{E}_i}(V_i),$$

we observe that V_j and V_i have different centralizer if $i \neq j$. Hence $V_i \ncong V_j$.
(b) The assumption $\dim_{\mathbb{E}_i} V_i > 1$ implies that V_i is a simple $\mathrm{SL}_{\mathbb{E}_i}(V_i)$-submodule and in particular a simple $\mathbb{K}H$-submodule. Remark 1.1.6 finishes the proof.

Notation: We will denote the set of nonzero elements of a set S by $S^\sharp$.

Lemma 1.1.8 *Assume that $r \neq p$. Let $g \in G$ with $|g| = r$ and $f, s, f_i, \mathbb{E}_i, V_i$ be defined as in Lemma 1.1.5. Then the following holds:*

(a) *V_i's are pairwise non-isomorphic.*

(b) $\{V_i \mid 1 \leq i \leq s\}$ *is the set of all simple* $\mathbb{K}C_G(g)$*-submodules of* V.

(c) $\mathbb{E}_i = C_{\mathrm{End}_{\mathbb{K}}(V_i)}(\mathrm{GL}_{\mathbb{E}_i}(V_i)) = C_{\mathrm{End}_{\mathbb{K}}(V_i)}(C_G(g))$ *for* $1 \leq i \leq s$.

Proof: (a) Observe that

$$C_{C_G(g)}(V_i) = \bigtimes_{k \neq i}^{s} \mathrm{GL}_{\mathbb{E}_k}(V_k).$$

Suppose to the contrary that $C_{C_G(g)}(V_i) = C_{C_G(g)}(V_j)$ for some distinct i and j. Then $\mathrm{GL}_{\mathbb{E}_i}(V_i) = \mathrm{GL}_{\mathbb{E}_j}(V_j) = \{1\}$ and this implies $\dim_{\mathbb{E}_k} V_k = 1$ and $\mathbb{E}_k = \mathbb{K} = \mathbb{F}_2$ for $k = i, j$. By Lemma 1.1.5(f), $\mathbb{E}_k = \mathbb{K} = \mathbb{E}$ where $\mathbb{E}$ is a splitting field of $x^r - 1$ over $\mathbb{K}$ and hence $\mathbb{K}$ contains a primitive r-th root of unity, a contradiction to $|\mathbb{K}| = 2$. Thus $C_{C_G(g)}(V_i) \neq C_{C_G(g)}(V_j)$ for any i, j. Since isomorphic $\mathbb{K}C_G(g)$-submodules must have the same centralizer in $C_G(g)$, we conclude that V_i's are pairwise non-isomorphic.

(b) By Lemma 1.1.5 (g),

$$C_G(g) = \bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i).$$

Since $\mathrm{GL}_{\mathbb{E}_i}(V_i)$ acts transitively on $V_i^\sharp$, so does $C_G(g)$. Thus, V_i's are simple $\mathbb{K}C_G(g)$-modules. Now, Remark 1.1.6 completes the proof of part (b).

(c) Note that the second equality is trivial and we only need to verify the first one:
($\subseteq$) Denote $C := C_{\mathrm{End}_{\mathbb{K}}(V_i)}(\mathrm{GL}_{\mathbb{E}_i}(V_i))$ and let $e \in \mathbb{E}_i \leq \mathrm{End}_{\mathbb{K}}(V_i)$. Then for any $h \in \mathrm{GL}_{\mathbb{E}_i}(V_i)$ we have $h(ev_i) = eh(v_i)$ for $v_i \in V_i$, that is, $e \in C$.
($\supseteq$) Let $0 \neq h \in C$. Then h commutes with every element in $\mathrm{GL}_{\mathbb{E}_i}(V_i)$ and, in particular, it commutes with every element in $\mathbb{E}_i$ since $\mathbb{E}_i^\sharp \subseteq \mathrm{GL}_{\mathbb{E}_i}(V_i)$. Thus $h \in Z(\mathrm{GL}_{\mathbb{E}_i}(V_i))$ which implies that $h = \xi\,\mathrm{id}_{V_i}$ for some $\xi \in \mathbb{E}_i$. So $h \in \mathbb{E}_i$.

Lemma 1.1.9 *Assume that $r \neq p$ and for $j = 1, 2$, let $g_j \in G$ with $|g_j| = r$. Let f_j, s_j, f_{ij}, $\mathbb{E}_{ij}$ and V_{ij} be defined as in Lemma 1.1.5. Then the following are equivalent*:

(a) $C_G(g_1) = C_G(g_2)$.

(b) $s := s_1 = s_2$ *and* (*possibly after permuting* $f_{12}, f_{22}, \ldots, f_{s2}$) $V_{i1} = V_{i2}$ *and* $\mathbb{E}_{i1} = \mathbb{E}_{i2}$ *for all* $1 \leq i \leq s$.

Proof: (b)$\Rightarrow$ (a): Trivial by Lemma 1.1.5(g).

(a)$\Rightarrow$ (b): Assume that $C_G(g_1) = C_G(g_2)$. By Lemma 1.1.8(b), $\{V_{ij} \mid 1 \leq i \leq s_j\}$ is the set of all simple $\mathbb{K}C_G(g_j)$-submodules of V for $j = 1, 2$. Then the assumption $C_G(g_1) = C_G(g_2)$ implies that $s := s_1 = s_2$ and possibly after permuting the f_{ij}'s $V_{i1} = V_{i2}$ for all $1 \leq i \leq s$. By Lemma 1.1.8(c), we have

$$\mathbb{E}_{i1} = C_{\mathrm{End}_{\mathbb{K}}(V_{i1})}(C_G(g_1)) = C_{\mathrm{End}_{\mathbb{K}}(V_{i2})}(C_G(g_2)) = \mathbb{E}_{i2}.$$

Lemma 1.1.10 *Assume that $r \neq p$ and let $g \in G$ with $|g| = r$. Let the notation be as in Lemma 1.1.5. Then exactly one of the following holds*:

1. $C_{\overline{G}}(\overline{g}) = \overline{C_G(g)}$.
2. (a) $\mathbb{E} = \mathbb{K}$.
   (b) $f(x) = x^r - 1$.
   (c) $s = r$ *and there exists* $1 \neq \xi \in \mathbb{K}^\sharp$ *with* $\xi^r = 1$ *such that for all* $1 \leq i \leq r$ $f_i(x) = x - \xi^{i-1}$ (*possibly after reordering the* f_i*'s*).
   (d) $\dim_{\mathbb{K}} V_i = \dim_{\mathbb{K}} V_j$ *for all* $1 \leq i < j \leq r$.
   (e) $C_{\overline{G}}(\overline{g}) = \overline{C_G(g)\langle h\rangle}$ *where* $h \in G$ *with* $h^r = 1$, $hV_i = V_{i+1}$ *for all* $1 \leq i < r$ *and* $hV_r = V_1$.

Proof: Assume that (1) does not hold. Then $C_{\overline{G}}(\overline{g}) \gneqq \overline{C_G(g)}$ and hence there exists $\overline{y} \in C_{\overline{G}}(\overline{g})$ such that $y \notin C_G(g)$. So $1 \neq [g,y] \in Z(G)$. Let $1 \neq [g,y] = \xi$ for some $\xi \in \mathbb{K}^\sharp$. As $y^{-1}gy = \xi g$ and $|y^{-1}gy| = |g| = r$, we have $|\xi| = r$. That is, ξ is a primitive r-th root of unity in $\mathbb{K}^\sharp$ and hence $\mathbb{E} = \mathbb{K}$. This proves 2(a).

We shall now prove the parts 2(b)-(d) together: Since $f(x) = \prod_{i=1}^{s} f_i(x)$ divides $x^r - 1$ and $x^r - 1$ splits in $\mathbb{K}[x]$, we may let $f_i(x) = x - \xi_i$, $1 \leq i \leq s$, where ξ_i is an r-th root of unity in $\mathbb{K}$. Note that, for each $1 \leq i \leq s$,

$$V_i = \mathrm{Ann}(f_i(g)) = \{v \in V \mid gv = \xi_i v\} = \mathrm{Ker}(g - \xi_i).$$

That is to say, V_i is the eigenspace of g corresponding to the eigenvalue ξ_i. For any $\lambda \in \mathbb{K}^\sharp$ and $v \in V$, we have

$$g^y v = \xi\lambda v \Leftrightarrow \xi g v = \xi\lambda v \Leftrightarrow gv = \lambda v,$$

which means that

$$\mathrm{Ker}(g - \lambda) = \mathrm{Ker}(g^y - \xi\lambda). \tag{1.2}$$

Using (1.2) with $\lambda = \xi_i$, it follows that $V_i = \mathrm{Ker}(g - \xi_i) = \mathrm{Ker}(g^y - \xi\xi_i)$. Let us now consider $\mathrm{Ker}(g^y - \xi_i)$ and observe that

$$\mathrm{Ker}(g^y - \xi_i) = \{v \in V \mid g^y v = \xi_i v\} = \{v \in V \mid \xi g v = \xi_i v\} = \{v \in V \mid gv = \xi^{-1}\xi_i v\}$$

is the eigenspace of g corresponding to the eigenvalue $\xi^{-1}\xi_i$. Thus, $\mathrm{Ker}(g^y - \xi_i)$ gives another eigenspace V_j, where $j \neq i$. Also, note here that

$$\begin{aligned}\dim_{\mathbb{K}} V_i &= \dim_{\mathbb{K}} \mathrm{Ker}(g - \xi_i) = \dim_{\mathbb{K}} h^{-1}(\mathrm{Ker}(g^y - \xi_i)) \\ &= \dim_{\mathbb{K}} \mathrm{Ker}(g^y - \xi_i) = \dim_{\mathbb{K}} V_j,\end{aligned}$$

which yields 2(d). By (1.2), we have $\mathrm{Ker}(g^y - \xi^j\xi_i) = \mathrm{Ker}(g - \xi^{j-1}\xi_i)$. Since $|\xi| = r$, for each $j \in \{1, 2, \ldots, r\}$, $\mathrm{Ker}(g^y - \xi^j\xi_i)$ gives a different eigenspace of g. Therefore, $s = r$ as claimed in part 2(c) and hence $f(x) = x^r - 1$. Without loss of generality, let $f_i(x) = x - \xi^{i-1}$ for $1 \leq i \leq r$.

2(e) First we shall show that an arbitrary $h \in G$ with the conditions $h^r = 1$, $hV_i = V_{i+1}$ and $hV_r = V_1$, for all $1 \leq i < r$, must satisfy $C_{\overline{G}}(\overline{g}) = \overline{C_G(g)\langle h\rangle}$. Note that, for any i, we have

$$g^h v_i = (h^{-1}gh)(v_i) = h^{-1}g(h(v_i)) = h^{-1}(\xi^i h v_i) = \xi^i v_i \text{ for all } v_i \in V_i. \qquad (1.3)$$

On the other hand, $\xi g v_i = \xi\xi^{i-1}v_i$ for all $v_i \in V_i$. Combining this with (1.3), we conclude that $g^h = \xi g$ on each V_i and hence on V. Now $g^h = \xi g$ implies $h \in C_G(\overline{g})$ and hence $C_G(\overline{g}) \supseteq C_G(g)\langle h\rangle$. Conversely, take an element $\overline{d} \in C_{\overline{G}}(\overline{g})$. We need to show that $dh^{-k} \in C_G(g)$ for some $k \in \mathbb{Z}$. Let $[g, d] = \lambda \in Z(G)$ for some $\lambda \in \mathbb{K}^\sharp$. Since $\lambda^r = 1$, we have $\lambda = \xi^k$ for some k. Then $dh^{-k} \in C_G(g)$ easily follows.

Next we shall show the existence of such an h. For this, we let $h_i : V_i \longrightarrow V_{i+1}$ be arbitrary $\mathbb{K}$-linear maps for all $1 \leq i < r$ and define $h_r : V_r \longrightarrow V_1$ as $h_r = (h_{r-1}h_{r-2}\cdots h_1)^{-1}$. Now let $h \in G$ with $h|_{V_i} := h_i$. Then obviously $h^r = 1$ and above observation implies that $C_G(\overline{g}) = C_G(g)\langle h\rangle$.

Let us mention some further observations that will be needed later.

Remark 1.1.11 *Assume that $r \neq p$ and let $g \in G$ with $|g| = r$ be as in Lemma 1.1.10(2). If $y \in C_G(\overline{g})$ with $yV_1 = V_2$, then $yV_i = V_{i+1}$ for all $1 \leq i < r$ and $yV_r = V_1$.*

Proof: $y \in C_G(\overline{g})$ implies $y^{-1}gy = \lambda g$ for some $\lambda \in \mathbb{K}$. Then, for any $v_1 \in V_1$, $y^{-1}gyv_1 = \lambda g v_1$. As $yv_1 \in V_2$ and $gv_1 = v_1$, we get $y^{-1}\xi y v_1 = \lambda v_1$ and hence $\xi = \lambda$. Now take $v_i \in V_i$ and observe that

$$yv_i \in V_{i+1} \Leftrightarrow g(yv_i) = \xi^i yv_i \Leftrightarrow y^{-1}gyv_i = \xi^i v_i \Leftrightarrow \xi g v_i = \xi^i v_i.$$

The last equality above does hold by the definition of V_i. Hence $yv_i \in V_{i+1}$. Also we know that V_i's have the same dimension.

Proposition 1.1.12 *Assume that $r \neq p$ and let $g \in G$ with $|g| = r$ be as in Lemma 1.1.10(2). Further assume that $\dim_{\mathbb{K}} V_i = 1$ for $1 \leq i \leq r$. Then either $C_G(g)$ is the unique abelian subgroup of index r in $C_G(\overline{g})$ or $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$.*

Proof: Let $A = C_G(g)$ and $B = C_G(\overline{g})$. Note that A is an abelian normal subgroup of B and $|B/A| = r$. Suppose that there is a subgroup D of B such that D is abelian, $|B/D| = r$ and $D \neq A$. Then $AD = B$. Now

$$A \cap D \underset{D \text{ abelian}}{\leq} C_A(D) \underset{A \text{ abelian}}{=} C_A(AD) = C_A(B) = C_A(A\langle h \rangle) = C_A(h)$$

and $|A/A \cap D| = |AD/D| = |B/D| = r$ imply that $|A/C_A(h)| \leq r$. Since $\dim_{\mathbb{K}} V_i = 1$, $A \cong \bigtimes_{i=1}^{r} \mathbb{K}^\sharp$. Let $y = (k_1, k_2, \ldots, k_r) \in A$ where $k_i \in \mathbb{K}^\sharp$ for all i. Since h permutes the k_i's, $y \in C_A(h)$ if and only if y is of the form $y = (k, k, \ldots, k)$ for some $k \in \mathbb{K}^\sharp$. Therefore $C_A(h) \cong \mathbb{K}^\sharp$ and hence $|A/C_A(h)| = |\mathbb{K}^\sharp|^{r-1} \leq r$. Since $\mathbb{K}$ contains an r-th root of unity, $|\mathbb{K}^\sharp| \geq r$. Thus $r^{r-1} \leq r = r^1$ which gives $r = 2$. Now $r \leq |\mathbb{K}^\sharp| \leq r$ implies that $|\mathbb{K}| = 3$. Furthermore, $\dim_{\mathbb{K}} V = 2$ follows from $r = 2$ and $\dim_{\mathbb{K}} V_i = 1$ for $1 \leq i \leq r$.

Now we will state a similar result where $\mathrm{GL}_{\mathbb{K}}(V)$ is replaced by $\mathrm{SL}_{\mathbb{K}}(V)$.

Proposition 1.1.13 *Assume that $r \neq p$. Let $g \in G$ with $|g| = r$ be as in Lemma 1.1.10(2). Assume that $\dim_{\mathbb{K}} V_i = 1$ for $1 \leq i \leq r$. Then either $C_S(g)$ is the unique abelian subgroup of index r in $C_S(\overline{g})$ or we have one of the following cases:*

(1) $r = 3$, $|\mathbb{K}| = 4$, *and* $\dim_{\mathbb{K}} V = 3$.

(2) $r = 2$, $|\mathbb{K}| = 3$, *and* $\dim_{\mathbb{K}} V = 2$.

(3) $r = 2$, $|\mathbb{K}| = 5$, *and* $\dim_{\mathbb{K}} V = 2$.

Proof: Let $h \in C_G(\overline{g}) \setminus C_G(g)$ and $d := \det(h)$. Consider the element $x \in G$ which acts as d^{-1} on V_1 and as identity on the remaining V_i's. Trivially $x \in C_G(g)$ and $hx \in C_G(\overline{g})$ has determinant 1, that is, $hx \in C_S(\overline{g})$. It is also obvious that $hx \notin C_S(g)$. Thus, we have $C_S(\overline{g}) \neq C_S(g)$.
Since $C_G(g) \leq C_G(g)C_S(\overline{g}) \leq C_G(\overline{g})$ and $|C_G(\overline{g})/C_G(g)| = r$, we have $C_G(g) = C_G(g)C_S(\overline{g})$ or $C_G(g)C_S(\overline{g}) = C_G(\overline{g})$. The first case implies that $C_S(\overline{g}) = C_S(g)$ which is not possible. Therefore, by the latter case $r = |C_G(\overline{g})/C_G(g)| = |C_G(g)C_S(\overline{g})/C_G(g)| = |C_S(\overline{g})/C_S(g)|$.

The rest of the proof is essentially the same as the proof of Proposition 1.1.12: Let $A = C_S(g)$ and $B = C_S(\overline{g})$ and suppose that there exists an abelian subgroup D of index r in B and $D \neq A$. Then $AD = B$ and $|B/D| = r$ implies $|A/A \cap D| = r$. Since $B = S \cap (C_G(g)\langle h \rangle)$, we have $B \supseteq A(S \cap \langle h \rangle)$ and

$$A \cap D \underset{D \text{ abelian}}{\leq} C_A(D) \underset{A \text{ abelian}}{=} C_A(AD) = C_A(B) \leq C_A(S \cap \langle h \rangle).$$

Thus $|A/C_A(S \cap \langle h \rangle)| \leq r$. We also have $A = S \cap \bigtimes_{i=1}^{r} \mathbb{K}^\sharp$ and $|A| = |\mathbb{K}^\sharp|^{r-1}$. The elements in $C_A(S \cap \langle h \rangle)$ are of the form $(k, k, \ldots, k)$ with $k^r = 1$ where $k \in \mathbb{K}^\sharp$. Since $\mathbb{K}$ contains an r-th root of unity, $|C_A(S \cap \langle h \rangle)| = r$ and hence

$|A/C_A(S \cap \langle h \rangle)| = |\mathbb{K}^\sharp|^{r-1}/r \leq r$. Therefore

$$|\mathbb{K}^\sharp|^{r-1} \leq r^2 \text{ and } |\mathbb{K}^\sharp| \geq r.$$

From these inequalities we get $r^{r-1} \leq r^2$. Thus $r = 2$ or $r = 3$. The first case yields $|\mathbb{K}| = 3$ or 5 ($|\mathbb{K}| \neq 4$ since $r \neq p$) while the second case gives $|\mathbb{K}| = 4$.

Remark 1.1.14 *Assume that $r \neq p$. Let $\overline{g} \in \overline{G}$ with $|\overline{g}| = r$. Put $\xi = g^r \in \mathbb{K}^\sharp$. Then the following are equivalent.*

(a) *$|gk| \neq r$ for any $k \in \mathbb{K}^\sharp$.*

(b) *$\xi \notin \mathbb{K}^r$.*

(c) *$x^r - \xi$ is irreducible over $\mathbb{K}$.*

Proof: (a) $\Leftrightarrow$ (b):
$|gk| = r$ for some $k \in \mathbb{K}^\sharp \iff (gk)^r = 1$ for some $k \in \mathbb{K}^\sharp \iff g^r = k^{-r}$ for some $k \in \mathbb{K}^\sharp \iff \xi = k^{-r}$ for some $k \in \mathbb{K}^\sharp \iff \xi \in \mathbb{K}^r$ for some $k \in \mathbb{K}^\sharp$.
(b) $\Leftrightarrow$ (c): See [12, Lemma 16.3].

Lemma 1.1.15 *Assume that $r \neq p$ and let $g \in G$ with $|\overline{g}| = r$. Suppose $|gk| \neq r$ for any $k \in \mathbb{K}^\sharp$ and let $\xi \in \mathbb{K}^\sharp$ be such that $g^r = \xi$. Put $\mathbb{E} := \mathbb{K}[g] \leq \mathrm{End}_{\mathbb{K}}(V)$. Then the following holds.*

(a) *$f(x) := x^r - \xi$ is irreducible.*

(b) *$\mathbb{E} \cong \mathbb{K}[x]/f(x)\mathbb{K}[x]$ is a field with $\dim_{\mathbb{K}} \mathbb{E} = r$.*

(c) *V is a vector space over $\mathbb{E}$ and $C_G(\overline{g}) = \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}}(V)$.*

(d) *$|\mathbb{K}| > 2$.*

Proof: (a) This is from Remark 1.1.14.

(b) Obvious since $f(x)$ is the minimal polynomial of g and $\dim_{\mathbb{K}} \mathbb{E} = \deg f(x) = r$.

(c) Define $e \cdot v = e(v)$ for all $e \in \mathbb{E}$ and $v \in V$. This defines an $\mathbb{E}$-module structure on V. Note that by Lemma 1.1.4 we have $C_G(\overline{g}) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}}(V)$. Thus, it remains to show the converse inclusion. Let $h \in \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}}(V)$ with $\sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E})$ being the corresponding automorphism. We need to prove that $h \in C_G(\overline{g})$, which is equivalent to $hgh^{-1}g^{-1} \in \mathbb{K}$. By Lemma 1.1.3, $heh^{-1} = \sigma(e)$ for all $e \in \mathbb{E}$. Letting $e = g \in \mathbb{E}$, we get $hgh^{-1} = \sigma(g)$ and hence $hgh^{-1}g^{-1} = \sigma(g)g^{-1}$. Therefore, we are done if we show that $\sigma(g)g^{-1} \in \mathbb{K}$.

Since $g^r = \xi = \sigma(g)^r$, we have $(\sigma(g)g^{-1})^r = 1$. Hence $\sigma(g)g^{-1}$ is a root of $x^r - 1$. The degree of the minimal polynomial of $\sigma(g)g^{-1}$ is strictly less than r because $x^r - 1$ is reducible. Then $[\mathbb{E} : \mathbb{K}] = r$ and $[\mathbb{K}(\sigma(g)g^{-1}) : \mathbb{K}]$ divides $[\mathbb{E} : \mathbb{K}]$ imply that $\sigma(g)g^{-1} \in \mathbb{K}$.

(d) If $|\mathbb{K}| = 2$, then $g^r = 0$ or 1, contradiction.

Remark 1.1.16 *Let $\overline{y} \in \overline{S}$ with $|\overline{y}| = r$ where $r \neq p$. Then $C_{\overline{S}}(\overline{y})$ is not solvable if $n > 2r(r-1)$ where $n = \dim_{\mathbb{K}} V$.*

Proof: Assume first that $|yk| \neq r$ for any $k \in \mathbb{K}$. Put $y^r = \xi \in \mathbb{K}$. Then, by Lemma 1.1.15, $\dim_{\mathbb{K}} \mathbb{E} = r$ where $\mathbb{E} = \mathbb{K}[y]$ and moreover $C_{\overline{G}}(\overline{y}) = \Gamma_{\mathbb{K}} \mathrm{GL}(V)$. Hence $C_{\overline{S}}(\overline{y}) = \overline{S} \cap \overline{\Gamma_{\mathbb{K}} \mathrm{GL}(V)} \supseteq \mathrm{SL}_{\mathbb{E}}(V)Z(G)/Z(G)$. Choosing $n > 2r$ implies that $\dim_{\mathbb{E}} V > 2$. Then $\mathrm{SL}_{\mathbb{E}}(V)Z(G)/Z(G)$ and hence $C_{\overline{S}}(\overline{y})$ is non-solvable, giving the desired result in this case.

Now suppose that $|yk| = r$ for some $k \in \mathbb{K}$. Without loss of generality, we may assume $|y| = r$ and then use Lemma 1.1.10. In Case 1.1.10(1), we have $C_{\overline{S}}(\overline{y}) \supseteq [\bigtimes_{i=1}^{s} \mathrm{SL}_{\mathbb{E}_i}(V_i)]Z(G)/Z(G)$, where $\mathbb{E}_i = \mathbb{E}$ or $\mathbb{K}$ and $[\mathbb{E} : \mathbb{K}] \leq r-1$. Thus choosing

$n > 2r(r-1)$ implies that $\dim_{\mathbb{E}_i} V_i > 2$ for some i and hence $C_{\overline{S}}(\overline{y})$ is not solvable. In Case 1.1.10(2), we observe that $C_{\overline{S}}(\overline{y}) \supseteq [\bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_i)]Z(G)/Z(G)$. Similarly, if $n > 2r$ then $\dim_{\mathbb{K}} V_i > 2$ for some i, which leads to desired result.

1.2 Field Extensions

Lemma 1.2.1 *Assume that $r \neq p$ and $\mathbb{K}$ contains a primitive r-th root of unity. Suppose a is an element of an extension field of $\mathbb{K}$ such that $a^r \in \mathbb{K}$. If $b \in \mathbb{K}(a)$ with $b^r \in \mathbb{K}$, then $b = a^j k$ for some $j \in \mathbb{Z}$ and some $k \in \mathbb{K}$.*

Proof: It is trivial if $a \in \mathbb{K}$, so we assume $a \notin \mathbb{K}$. Since $\mathbb{K}$ has a primitive r-th root of unity, we have $a^r \notin \mathbb{K}^r$. Put $c := a^r \in \mathbb{K}$ and $g(x) := x^r - c \in \mathbb{K}[x]$. By Remark 1.1.14, $g(x)$ is irreducible and it is also separable since $\gcd(g(x), g'(x)) = 1$. Thus $\mathbb{K}(a)$ is a splitting field of $g(x)$ and $\mathbb{K}(a)/\mathbb{K}$ is a Galois extension with $[\mathbb{K}(a) : \mathbb{K}] = r$. Let $1 \neq \sigma \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{K}(a))$. Then $\sigma(a) = \xi a$ where ξ is a primitive r-th root of unity. Hence $\sigma(a^i) = \xi^i a^i$ for all $0 \leq i < r$, which means ξ^i is an eigenvalue of σ with the corresponding eigenvector a^i for $0 \leq i < r$. Obviously $\mathbb{K}a^i \subseteq \mathrm{Ann}(\sigma - \xi^i)$. Since $K(a)$ is a vector space of dimension r over $\mathbb{K}$, each eigenspace of σ has dimension 1 and thus $\mathbb{K}a^i = \mathrm{Ann}(\sigma - \xi^i)$. By assumption $d := b^r \in \mathbb{K}$. So both b and $\sigma(b)$ are the roots of the polynomial $x^r - d \in \mathbb{K}[x]$. Hence $\sigma(b) = b\xi^j$ for some j. Therefore, b is in the eigenspace of σ corresponding to the eigenvalue ξ^j and thus $b \in \mathbb{K}a^j$.

Lemma 1.2.2 *Assume that $r \neq p$ and let a be an element of an extension field of $\mathbb{K}$ such that $a^r \in \mathbb{K} \setminus \mathbb{K}^r$. If $b \in \mathbb{K}(a)$ with $b^r \in \mathbb{K}$, then $b = a^j k$ for some $j \in \mathbb{Z}$ and $k \in \mathbb{K}$.*

Proof: Let ξ denote a primitive r-th root of unity in an extension field of $\mathbb{K}(a)$. Then $[\mathbb{K}(\xi) : \mathbb{K}] \leq r - 1$. Since $a^r \notin \mathbb{K}^r$, we have $[\mathbb{K}(a) : \mathbb{K}] = r$. Hence $[\mathbb{K}(a) : \mathbb{K}]$ and $[\mathbb{K}(\xi) : \mathbb{K}]$ are relatively prime and so $\mathbb{K}(a) \cap \mathbb{K}(\xi) = \mathbb{K}$. We

are now in a position to apply Lemma 1.2.1 to the field extension $\mathbb{K}(\xi)(a)/\mathbb{K}(\xi)$ and conclude that $b = ka^j$ for some $j \in \mathbb{Z}$ and $k \in \mathbb{K}(\xi)$. On the other hand, $k = ba^{-j} \in \mathbb{K}(\xi) \cap \mathbb{K}(a) = \mathbb{K}$.

The previous lemma will in fact be needed and used in Chapter 2 only in the following set up and, for convenience, we would like to mention it here.

Lemma 1.2.3 *Let $g_j \in G$ be such that $|\overline{g}_j| = r$ where $r \neq p$. Assume that $\mathbb{E}_j := \mathbb{K}[g_j]$ is a field for $j = 1, 2$. Assume further that for at least one of g_j we have $|kg_j| \neq r$ for any $k \in \mathbb{K}^\sharp$. If $\mathbb{E}_1 = \mathbb{E}_2$ then $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$.*

Proof: For $j = 1, 2$ we have $g_j^r \in \mathbb{K}$ and, say, $g_2^r \notin \mathbb{K}^r$. Using Lemma 1.2.2, we get $g_2 = g_1^j k$ for some $j \in \mathbb{Z}$ and $k \in \mathbb{K}$. Then $\overline{g}_2 \in \langle \overline{g}_1 \rangle$ and the lemma follows.

Lemma 1.2.4 *Let $\mathbb{E}$ be an extension field of $\mathbb{F}$. Then*

$$|\mathbb{E}^\sharp : \mathbb{F}^\sharp| = \text{ number of 1-dimensional } \mathbb{F}\text{-subspaces of } \mathbb{E}.$$
$$> \dim_{\mathbb{F}} \mathbb{E} \quad \text{unless} \quad \mathbb{F} = \mathbb{E}.$$

Proof: Let $\mathbb{F}e$ be a 1-dimensional $\mathbb{F}$-subspace of $\mathbb{E}$, where $e \in \mathbb{E}^\sharp$. It is easily seen that $\mathrm{Stab}_{\mathbb{E}}(\mathbb{F}e) = \mathbb{F}$. Let Ω be the set of all 1-dimensional $\mathbb{F}$-subspaces of $\mathbb{E}$. Since $\mathbb{E}^\sharp$ acts transitively on $\mathbb{E}^\sharp$, and hence on Ω, we have $|\mathbb{E}^\sharp : \mathrm{Stab}_{\mathbb{E}^\sharp}(\mathbb{F}e)| = |\mathbb{E}^\sharp : \mathbb{F}^\sharp| = |\Omega|$. The last part is from the fact that each element in an $\mathbb{F}$-basis of $\mathbb{E}$ gives a 1-dimensional $\mathbb{F}$-subspace. But there are 1-dimensional subspaces other than this type.

Lemma 1.2.5 *Let V be an $\mathbb{E}$-space and $\mathbb{K}$ be a subfield of $\mathbb{E}$. If $\dim_{\mathbb{E}} V \neq 1$, then $C_{\mathrm{End}_{\mathbb{K}}(V)}(\mathrm{SL}_{\mathbb{E}}(V)) = \mathbb{E}$.*

Proof: Let us denote $C_{\mathrm{End}_{\mathbb{K}}(V)}(\mathrm{SL}_{\mathbb{E}}(V))$ by D. Note that $D = \mathrm{End}_{\mathbb{K}\,\mathrm{SL}_{\mathbb{E}}(V)}(V)$ and V is a simple $\mathbb{K}\,\mathrm{SL}_{\mathbb{E}}(V)$-module, so D is a division ring by Schur's Lemma. If $e \in \mathbb{E}$ and $h \in \mathrm{SL}_{\mathbb{E}}(V)$, then e commutes with h since h is $\mathbb{E}$-linear. Hence $e \in D$, giving the inclusion $\mathbb{E} \subseteq D$. Now, let $t \in \mathrm{SL}_{\mathbb{E}}(V)$ be a transvection. Then $[V,t]$ is a 1-dimensional space over $\mathbb{E}$. Let $d \in D$ and $0 \neq v \in [V,t]$. Since D centralizes t, $[V,t]$ is invariant under D. Hence $dv \in [V,t]$, and $dv = ev$ for some $e \in \mathbb{E}$. Then $d = e$ since D is a division ring. Therefore $D \subseteq \mathbb{E}$, completing the proof.

Lemma 1.2.6 *Let* $\mathbb{E}_1$, $\mathbb{E}_2$ *be subfields of* $\mathrm{End}_{\mathbb{K}}(V)$ *containing* $\mathbb{K}$ *with* $\mathrm{SL}_{\mathbb{E}_2}(V) \leq \Gamma_{\mathbb{K}}\,\mathrm{GL}_{\mathbb{E}_1}(V)$. *Then one of the following holds*:

(1) $\dim_{\mathbb{E}_2} V = 1$.

(2) $\mathbb{E}_1 \subseteq \mathbb{E}_2$.

(3) $\mathbb{K} = \mathbb{E}_2 \cong \mathbb{F}_2$, $\mathbb{E}_1 \cong \mathbb{F}_4$, *and* $\dim_{\mathbb{K}} V = 2$.

Proof: Note that since V is finite dimensional, $\dim_{\mathbb{K}} \mathbb{E}_j < \infty$ for $j = 1, 2$. We may assume that $\dim_{\mathbb{E}_2} V > 1$. Let $S_2 = \mathrm{SL}_{\mathbb{E}_2}(V)$.

Case (a) Assume that $(\dim_{\mathbb{E}_2} V, |\mathbb{E}_2|) \neq (2,2), (2,3)$.
Then S_2 is quasisimple. Since $S_2 \leq N_G(\mathbb{E}_1)$, $C_{S_2}(\mathbb{E}_1^\sharp) \trianglelefteq S_2$. Suppose for a contradiction that $[S_2, \mathbb{E}_1^\sharp] \neq 1$. Then $S_2/C_{S_2}(\mathbb{E}_1^\sharp) \neq 1$. Furthermore, S_2 being quasisimple implies that $C_{S_2}(\mathbb{E}_1^\sharp) \leq Z(S_2)$. Since $S_2/C_{S_2}(\mathbb{E}_1^\sharp)$ is isomorphic to a subgroup of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$, $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$ has a section isomorphic to $S_2/Z(S_2) = \mathrm{PSL}_{\mathbb{E}_2}(V)$. Also since $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$ is finite, $\mathrm{PSL}_{\mathbb{E}_2}(V)$ is finite. Thus $\mathbb{E}_2$, and so $\mathbb{K}$ and $\mathbb{E}_1$, are finite. Hence $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$ is cyclic, but $S_2/Z(S_2)$ is not, a contradiction. Therefore, $[S_2, \mathbb{E}_1^\sharp] = 1$ and hence $\mathbb{E}_1^\sharp \subseteq \mathbb{E}_2$ by Lemma 1.2.5. Thus (2) holds in this case.

Case (b) Assume that $(\dim_{\mathbb{E}_2} V, |\mathbb{E}_2|) = (2,2)$ or $(2,3)$.

Since $\mathbb{K} \subseteq \mathbb{E}_2$, $\mathbb{K} = \mathbb{E}_2$. If $\mathbb{E}_1 = \mathbb{E}_2$, then (2) holds. So we may assume that $\mathbb{E}_2 = \mathbb{K} \subsetneq \mathbb{E}_1$. Since $2 = \dim_{\mathbb{E}_2} V = \dim_{\mathbb{E}_2} \mathbb{E}_1 \cdot \dim_{\mathbb{E}_1} V$, it follows that $\dim_{\mathbb{E}_2} \mathbb{E}_1 = 2$ and $\dim_{\mathbb{E}_1} V = 1$. Therefore,

$$\mathbb{K} = \mathbb{E}_2 = \mathbb{F}_p \quad \text{and} \quad \mathbb{E}_1 = \mathbb{F}_{p^2} = V \tag{1.4}$$

where $p = 2$ or 3. Since $\mathrm{SL}_{\mathbb{E}_2}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_1}(V)$, we have

$$|\mathrm{SL}_{\mathbb{E}_2}(V)| = \frac{(p^2-1)(p^2-p)}{p-1} \leq |\Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_1}(V)| \leq 2(p^2-1).$$

This implies $p = 2$ and hence (3) holds by (1.4).

Proposition 1.2.7 *Assume that $r \neq p$ and let $\mathbb{E}_1$ and $\mathbb{E}_2$ be subfields of $\mathrm{End}_{\mathbb{K}}(V)$ containing $\mathbb{K}$.*

(a) *If $\mathbb{E}_1^\sharp \leq N_G(\mathbb{E}_2)$ and $\mathbb{E}_2^\sharp \leq N_G(\mathbb{E}_1)$, then $[\mathbb{E}_1^\sharp, \mathbb{E}_2^\sharp] = 1$.*

(b) *Assume that $\mathrm{GL}_{\mathbb{E}_1}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V)$ and $\mathrm{GL}_{\mathbb{E}_2}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_1}(V)$. Then $\mathbb{E}_1 = \mathbb{E}_2$ or the following holds: $\mathbb{K} = \mathbb{F}_2$, $\{\mathbb{E}_1, \mathbb{E}_2\} = \{\mathbb{F}_2, \mathbb{F}_4\}$, and $V = \mathbb{F}_4$.*

Proof: (a) For $i = 1, 2$, let us define $\mathbb{L}_i$ by $\mathbb{L}_i := C_{\mathbb{E}_i}(\mathbb{E}_{3-i}^\sharp)$. Obviously, $\mathbb{L}_i$ is a subfield of $\mathbb{E}_i$. Since $\mathrm{End}_{\mathbb{K}}(V)$ is finite dimensional over $\mathbb{K}$, we have $[\mathbb{E}_i : \mathbb{K}] < \infty$ and hence $[\mathbb{E}_i : \mathbb{L}_i] < \infty$.

Now consider the map $\theta_1 : \mathbb{E}_1^\sharp \longrightarrow \mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)$ defined as $\theta(e_1)(e_2) = e_1^{-1} e_2 e_1$ for all $e_1 \in \mathbb{E}_1^\sharp$ and $e_2 \in \mathbb{E}_2$. The first isomorphism theorem implies that $\mathbb{E}_1^\sharp / \mathbb{L}_1^\sharp$ is isomorphic to a subgroup of $\mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)$ and thus $|\mathbb{E}_1^\sharp / \mathbb{L}_1^\sharp| \leq |\mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)|$. Let $a \in \mathbb{E}_2$ be in the fixed field of $\mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)$. Then, in particular, a is fixed by the

automorphisms $\theta_1(e_1)$ for each $e_1 \in \mathbb{E}_1^\sharp$. So a commutes with every element in $\mathbb{E}_1^\sharp$, hence $a \in \mathbb{L}_2$. This shows that the fixed field of $\mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)$ is equal to $\mathbb{L}_2$, that is, $\mathbb{E}_2/\mathbb{L}_2$ is a Galois extension and $|\mathrm{Aut}_{\mathbb{L}_2}(\mathbb{E}_2)| = \dim_{\mathbb{L}_2}\mathbb{E}_2$. Therefore,

$$|\mathbb{E}_1^\sharp/\mathbb{L}_1^\sharp| \leq \dim_{\mathbb{L}_2}\mathbb{E}_2. \tag{1.5}$$

We define the map $\theta_2 : \mathbb{E}_2^\sharp \longrightarrow \mathrm{Aut}_{\mathbb{L}_1}(\mathbb{E}_1)$ in a similar manner and obtain

$$|\mathbb{E}_2^\sharp/\mathbb{L}_2^\sharp| \leq \dim_{\mathbb{L}_1}\mathbb{E}_1. \tag{1.6}$$

Combining (1.5) and (1.6), along with Lemma 1.2.4, gives

$$|\mathbb{E}_1^\sharp/\mathbb{L}_1^\sharp| \leq \dim_{\mathbb{L}_2}\mathbb{E}_2 \leq |\mathbb{E}_2^\sharp/\mathbb{L}_2^\sharp| \leq \dim_{\mathbb{L}_1}\mathbb{E}_1 \leq |\mathbb{E}_1^\sharp/\mathbb{L}_1^\sharp| \leq \dim_{\mathbb{L}_2}\mathbb{E}_2.$$

Thus $|\mathbb{E}_i^\sharp/\mathbb{L}_i^\sharp| = \dim_{\mathbb{L}_i}\mathbb{E}_i$ and hence $\mathbb{E}_i = \mathbb{L}_i$ by Lemma 1.2.4 for $i = 1, 2$. In other words, $\mathbb{E}_1$ and $\mathbb{E}_2$ do commute, proving part (a).

(b) Observe that the assumption $\mathrm{GL}_{\mathbb{E}_j}(V) \leq \Gamma_{\mathbb{K}}\,\mathrm{GL}_{\mathbb{E}_{3-j}}(V)$ implies that $\mathbb{E}_j^\sharp \leq N_G(\mathbb{E}_{3-j})$ for $j = 1, 2$. Then by the previous part $e_1(e_2 v) = e_2(e_1 v)$ for all $e_i \in \mathbb{E}_i$ and $v \in V$. That is, $\mathbb{E}_1^\sharp \leq \mathrm{GL}_{\mathbb{E}_2}(V)$ and $\mathbb{E}_2^\sharp \leq \mathrm{GL}_{\mathbb{E}_1}(V)$. Without loss, assume

$$\dim_{\mathbb{E}_1} V \leq \dim_{\mathbb{E}_2} V. \tag{1.7}$$

If $\dim_{\mathbb{E}_2} V = 1$, then $\mathbb{E}_1^\sharp \leq \mathrm{GL}_{\mathbb{E}_2}(V) = \mathbb{E}_2^\sharp$. Moreover, since $\dim_{\mathbb{E}_1} V = 1$ we have $\mathbb{E}_2^\sharp \leq \mathrm{GL}_{\mathbb{E}_1}(V) = \mathbb{E}_1^\sharp$. Hence $\mathbb{E}_1^\sharp = \mathbb{E}_2^\sharp$. We are done in this case, so assume that $\dim_{\mathbb{E}_2} V > 1$. By Lemma 1.2.6, either $\mathbb{E}_1 \subseteq \mathbb{E}_2$ or $\mathbb{K} = \mathbb{E}_2 \cong \mathbb{F}_2$, $\mathbb{E}_1 \cong \mathbb{F}_4$, and $\dim_{\mathbb{K}} V = 2$. In the latter case we are done and in the former case $\mathbb{E}_1 = \mathbb{E}_2$ by (1.7).

Definition 1.2.8 *Let $\mathbb{K}$ be a subfield of $\mathbb{E}$ with $[\mathbb{E} : \mathbb{K}] < \infty$. Let $e \in \mathbb{E}$. Then the norm on $\mathbb{E}$ over $\mathbb{K}$ is defined by*

$$N_{\mathbb{E}}^{\mathbb{K}}(e) := \det_{\mathbb{E}}^{\mathbb{K}}(r_e)$$

where r_e is the left multiplication by e; namely, $r_e : \mathbb{E} \longrightarrow \mathbb{E}$ such that $r_e(a) = ea$ for all $a \in \mathbb{E}$. Note that r_e is a $\mathbb{K}$-linear map. Also, we define $\widetilde{\mathbb{E}}$ by

$$\widetilde{\mathbb{E}} := \{e \in \mathbb{E} \mid N_{\mathbb{E}}^{\mathbb{K}}(e) = 1\}.$$

Remark 1.2.9 (a) *$N_{\mathbb{E}}^{\mathbb{K}} : \mathbb{E}^\sharp \longrightarrow \mathbb{K}^\sharp$ is multiplicative.*

(b) *$N_{\mathbb{E}}^{\mathbb{K}}(k) = k^n$ for all $k \in \mathbb{K}$ where $[\mathbb{E} : \mathbb{K}] = n$.*

(c) *If V is a 1-dimensional vector space over $\mathbb{E}$ and $g \in \mathrm{GL}_{\mathbb{E}}(V)$, then g is multiplication by an element of $\mathbb{E}$. So $g = eI = r_e$ for some $e \in \mathbb{E}^\sharp$. It easily follows that $\det_V^{\mathbb{K}}(g) = \det_{\mathbb{E}}^{\mathbb{K}}(r_e) = N_{\mathbb{E}}^{\mathbb{K}}(e)$.*

(d) *If $\mathbb{E}/\mathbb{K}$ is a finite Galois extension with Galois group A, then*

$$N_{\mathbb{E}}^{\mathbb{K}}(e) = \prod_{\sigma \in A} \sigma(e)$$

for all $e \in \mathbb{E}$. See [15, Corollary 8.13].

Lemma 1.2.10 *Let V be an $\mathbb{E}$-space and $\mathbb{K}$ a subfield of $\mathbb{E}$ with $[\mathbb{E} : \mathbb{K}] < \infty$. Let $g \in \mathrm{GL}_{\mathbb{E}}(V)$. Then*

(a) $\mathrm{SL}_{\mathbb{E}}(V) \leq \mathrm{SL}_{\mathbb{K}}(V)$.

(b) $\det_V^{\mathbb{K}}(g) = N_{\mathbb{E}}^{\mathbb{K}}(\det_V^{\mathbb{E}}(g))$.

Proof: (a) Note that $\mathrm{SL}_{\mathbb{E}}(V)$ is generated by transvections. Let $t = I + aE_{ij}$ be a transvection in $\mathrm{SL}_{\mathbb{E}}(V)$, where $0 \neq a \in \mathbb{E}$ and $i \neq j$. Clearly, $\det_V^{\mathbb{K}}(t) = 1$, that is, $t \in \mathrm{SL}_{\mathbb{K}}(V)$.

(b) Let $g \in \mathrm{GL}_{\mathbb{E}}(V)$ and $d := \det_V^{\mathbb{E}}(g)$. We can write g in the form $g = kh$ where $k = \mathrm{diag}(d, 1, 1, \ldots, 1)$ and h is a product of transvections in $\mathrm{SL}_{\mathbb{E}}(V)$. By part (a), $\det_V^{\mathbb{K}}(h) = 1$. Note that we can view k as a linear transformation on a 1-dimensional vector space, and hence Remark 1.2.9(c) gives $\det_V^{\mathbb{K}}(k) = N_{\mathbb{E}}^{\mathbb{K}}(d)$. Thus

$$\det_V^{\mathbb{K}}(g) = \det_V^{\mathbb{K}}(k) \det_V^{\mathbb{K}}(h) = \det_V^{\mathbb{K}}(k) = N_{\mathbb{E}}^{\mathbb{K}}(d) = N_{\mathbb{E}}^{\mathbb{K}}(\det_V^{\mathbb{E}}(g)).$$

Lemma 1.2.11 *Let $\mathbb{K} \leq \mathbb{F} \leq \mathbb{E}$ be a chain of fields with $[\mathbb{E} : \mathbb{K}] < \infty$. Then*

$$N_{\mathbb{E}}^{\mathbb{K}}(e) = N_{\mathbb{F}}^{\mathbb{K}}(N_{\mathbb{E}}^{\mathbb{F}}(e)) \quad \textit{for all} \quad e \in \mathbb{E}^\sharp.$$

Proof: Let $V = \mathbb{E}$. We can view V as a vector space over both $\mathbb{K}$ and $\mathbb{F}$. Let $e \in \mathbb{E}^\sharp$. Using Lemma 1.2.10(b) for the field extensions $\mathbb{F}/\mathbb{K}$ and $\mathbb{E}/\mathbb{F}$, we get

$$\det_V^{\mathbb{K}}(e) = N_{\mathbb{F}}^{\mathbb{K}}(\det_V^{\mathbb{F}}(e)) \quad \text{and} \tag{1.8a}$$

$$\det_V^{\mathbb{F}}(e) = N_{\mathbb{E}}^{\mathbb{F}}(\det_V^{\mathbb{E}}(e)) \tag{1.8b}$$

respectively. Combining these equations and using $\det_V^{\mathbb{E}}(e) = e$, we obtain

$$N_{\mathbb{E}}^{\mathbb{K}}(e) = N_{\mathbb{E}}^{\mathbb{K}}(\det_V^{\mathbb{E}}(e)) \underset{1.2.10(b)}{=} \det_V^{\mathbb{K}}(e) \underset{(1.8a)}{=} N_{\mathbb{F}}^{\mathbb{K}}(\det_V^{\mathbb{F}}(e))$$

$$\underset{(1.8b)}{=} N_{\mathbb{F}}^{\mathbb{K}}(N_{\mathbb{E}}^{\mathbb{F}}(\det_V^{\mathbb{E}}(e))) = N_{\mathbb{F}}^{\mathbb{K}}(N_{\mathbb{E}}^{\mathbb{F}}(e)).$$

Lemma 1.2.12 *Let $\mathbb{E}$ be a separable extension field of $\mathbb{K}$ of degree $n > 1$. Assume that $\mathbb{K}$ is maximal in $\mathbb{E}$ and let $N = N_{\mathbb{E}}^{\mathbb{K}}$. Then $e^n/N(e) \notin \mathbb{K}$ for some $e \in \mathbb{E} \setminus \mathbb{K}$. In particular, there are elements in $\mathbb{E} \setminus \mathbb{K}$ whose norm is 1.*

Proof: First observe that $e^n/N(e)$ has norm 1 by Remark 1.2.9(a)-(b). Suppose for a contradiction that for any $e \in \mathbb{E} \setminus \mathbb{K}$ we have $e^n/N(e) \in \mathbb{K}$. Then $e^n \in \mathbb{K}$. Let q be a prime dividing n. We shall show that $n = q$ and $\operatorname{char} \mathbb{K} \neq q$.

Since $e^n = (e^q)^{n/q} \in \mathbb{K}$, we have $[\mathbb{K}(e^q) : \mathbb{K}] \leq n/q < n$. Moreover, $[\mathbb{E} : \mathbb{K}] = n$ implies that $\mathbb{K}(e^q) \neq \mathbb{E}$. Therefore $e^q \in \mathbb{K}$ by maximality of $\mathbb{K}$. Now since $e \in \mathbb{E} \setminus \mathbb{K}$, $\mathbb{E} = \mathbb{K}(e)$ again by maximality of $\mathbb{K}$. Hence $n = [\mathbb{K}(e) : \mathbb{K}] \leq q$ and so $n = q$. Now $x^q - e^q \in \mathbb{K}[x]$ is the minimal polynomial of e and so it is irreducible. Then $\mathbb{E}/\mathbb{K}$ is a separable extension implies that $\operatorname{char} \mathbb{K} \neq q$.

Since $x^q - e^q$ is irreducible, $e^q \notin \mathbb{K}^q$ by Remark 1.1.14. By our assumption $b^q/N(b) \in \mathbb{K}$, and so $b^q \in \mathbb{K}$ for any $b \in \mathbb{E} \setminus \mathbb{K}$. Now we observe that the hypothesis of Lemma 1.2.2 are satisfied. Therefore, for any $b \in \mathbb{E}$, $b \in \langle e \rangle \mathbb{K}^\sharp$ and hence $\mathbb{E}^\sharp = \langle e \rangle \mathbb{K}^\sharp$. As $\mathbb{E}^\sharp/\mathbb{K}^\sharp = \langle e\mathbb{K}^\sharp \rangle$ and $e^q \in \mathbb{K}$, we have $|\mathbb{E}^\sharp/\mathbb{K}^\sharp| = q$. On the other hand, $|\mathbb{E}^\sharp/\mathbb{K}^\sharp| > \dim_{\mathbb{K}} \mathbb{E} = q$ by Lemma 1.2.4. This contradiction completes the proof.

Corollary 1.2.13 *Let $\mathbb{E}$ be a finite separable extension field of $\mathbb{K}$. Then*

$$\mathbb{E} = \mathbb{K}(e \in \mathbb{E} \mid N_{\mathbb{E}}^{\mathbb{K}}(e) = 1\,).$$

Proof: Suppose that $\mathbb{E} \neq \mathbb{K}(e \in \mathbb{E} \mid N_{\mathbb{E}}^{\mathbb{K}}(e) = 1\,)$. Let $\mathbb{F}$ be a maximal field in $\mathbb{E}$ containing $\mathbb{K}(e \in \mathbb{E} \mid N_{\mathbb{E}}^{\mathbb{K}}(e) = 1\,)$ and note that $\mathbb{E}/\mathbb{F}$ is separable. By Lemma 1.2.12, there exists an $x \in \mathbb{E} \setminus \mathbb{F}$ with $N_{\mathbb{E}}^{\mathbb{F}}(x) = 1$. Then $N_{\mathbb{E}}^{\mathbb{K}}(x) = N_{\mathbb{F}}^{\mathbb{K}}(N_{\mathbb{E}}^{\mathbb{F}}(x)) = N_{\mathbb{F}}^{\mathbb{K}}(1) = 1$ by Lemma 1.2.11. Hence $x \in \mathbb{F}$ by definition of $\mathbb{F}$, contradiction.

Lemma 1.2.14 *Assume that $r \neq p$ and let $\mathbb{E}$ be an extension field of $\mathbb{K}$ of degree r. Then there exists $e \in \mathbb{E}$ such that $e^r \notin \mathbb{K}$.*

Proof: Assume that $e^r \in \mathbb{K}$ for all $e \in \mathbb{E}$. Let $e \in \mathbb{E} \setminus \mathbb{K}$. By assumption both $(1+e)^r$ and e^r are in $\mathbb{K}$, so is their difference. That is, $(1+e)^r - e^r = [\sum_{j=0}^{r} \binom{r}{j} e^j] - e^r = k$ for some $k \in \mathbb{K}$. Put $f(x) = rx^{r-1} + \cdots + 1 - k$. Then $f(x)$ is a polynomial of degree $r-1$ in $\mathbb{K}[x]$ with the root $e \in \mathbb{E} \setminus \mathbb{K}$ which implies that $[\mathbb{K}(e) : \mathbb{K}] \leq r-1$, a contradiction since $\mathbb{K}(e) = \mathbb{E}$ and $[\mathbb{E} : \mathbb{K}] = r$.

Lemma 1.2.15 *Let $\mathbb{E}/\mathbb{K}$ be a Galois extension of degree r where $r \neq p$. Assume that $\mathbb{K}$ contains a primitive r-th root of unity. If $(r, |\mathbb{K}|) \neq (2,3)$ then there exists an element $e \in \mathbb{E}$ such that $N_{\mathbb{E}}^{\mathbb{K}}(e) = 1$ and $e^r \notin \mathbb{K}$.*

Proof: Assume to the contrary that whenever $e \in \mathbb{E}$ with $N(e) = 1$ we have $e^r \in \mathbb{K}^\sharp$. By Corollary 1.2.13, there are elements in $\mathbb{E} \setminus \mathbb{K}$ whose norm is 1. Let β be such an element. By assumption $\beta^r \in \mathbb{K}$, so let $\beta^r = d \in \mathbb{K}$. Since $[\mathbb{E} : \mathbb{K}] = r$, we have $\mathbb{E} = \mathbb{K}(\beta)$. Let $1 \neq \sigma \in \mathrm{Aut}_{\mathbb{K}} \mathbb{E}$. Note that $\sigma(\beta) = \xi\beta$ where ξ is a primitive r-th root of unity. We observe that $a\sigma(a)^{-1}$ has norm 1 for $a \in \mathbb{E}$. Thus $a^r = k\sigma(a)^r$ for some $k \in \mathbb{K}$. Choosing $a = 1+\beta$ gives $(1+\beta)^r = k(1+\xi\beta)^r$. Note that $\{1, \beta, \beta^2, \ldots, \beta^{r-1}\}$ is a basis for $\mathbb{E}/\mathbb{K}$. We expand both sides to get

$$(1+d) + r\beta + \binom{r}{2}\beta^2 + \cdots + r\beta^{r-1} = k(1+d) + k\xi r\beta + \cdots + kr\xi^{r-1}\beta^{r-1}.$$

If $d \neq -1$, then $k = 1 = \xi$, a contradiction Thus, $d = -1$. Comparing the coefficients of β and of β^{r-1}, we get $k\xi = 1$ and $k\xi^{r-1} = 1$ correspondingly. Hence $\xi^{r-2} = 1$, which implies $r = 2$. Replacing a by $1 + c\beta$ where $c \in \mathbb{K}^\sharp$ gives $1 + dc^2 = 0$. Thus $c^2 = 1$ for all $c \in \mathbb{K}^\sharp$ and hence $|\mathbb{K}| = 3$.

Proposition 1.2.16 *Assume that* $r \neq p$. *For* $j = 1, 2$, *let* $\mathbb{E}_j$ *be a subfield of* $\mathrm{End}_{\mathbb{K}}(V)$ *containing* $\mathbb{K}$ *with* $\dim_{\mathbb{K}} \mathbb{E}_j = r$.

(a) *Suppose that* $\widetilde{\mathbb{E}}_1 \leq N_G(\mathbb{E}_2)$ *and* $\widetilde{\mathbb{E}}_2 \leq N_G(\mathbb{E}_1)$. *Then* $[\mathbb{E}_1^\sharp, \mathbb{E}_2^\sharp] = 1$ *or* $r = 2$, $|\mathbb{K}| = 3$, $|\mathbb{E}_j| = 9$.

(b) *If* $\mathrm{GL}_{\mathbb{E}_1}(V) \cap \mathrm{SL}_{\mathbb{K}}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V)$ *and* $\mathrm{GL}_{\mathbb{E}_2}(V) \cap \mathrm{SL}_{\mathbb{K}}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_1}(V)$, *then one of the following holds:*

(i) $\mathbb{E}_1 = \mathbb{E}_2$.

(ii) $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$, *and* $|\mathbb{E}_j| = 9$ *for* $j = 1, 2$.

Proof: (a) Certainly $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)| \leq \dim_{\mathbb{K}} \mathbb{E}_2 = r$. But in fact $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)| = 1$ or r. To see this, let $\mathbb{E}_0 = \mathrm{Fix}(\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2))$, the fixed field of $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)$. Then $\mathbb{E}_2/\mathbb{E}_0$ is a Galois extension. If $\mathbb{E}_0 = \mathbb{K}$, then $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)| = \dim_{\mathbb{K}} \mathbb{E}_2 = r$. If $\mathbb{E}_0 = \mathbb{E}_2$, then $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2) = \{\mathrm{id}\}$ by definition of $\mathbb{E}_0$. These arguments remain true if $\mathbb{E}_2$ is replaced by $\mathbb{E}_1$. Hence, we have $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)| = 1$ or r.
Obviously, $\widetilde{\mathbb{E}}_j$ is a multiplicative group for $j = 1, 2$. Now we consider the map $\vartheta : \widetilde{\mathbb{E}}_1 \longrightarrow \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)$ defined by $\vartheta(e_1)(e_2) = e_1^{-1} e_2 e_1$ for $e_1 \in \widetilde{\mathbb{E}}_1, e_2 \in \mathbb{E}_2$. The assumption $\widetilde{\mathbb{E}}_1 \leq N_G(\mathbb{E}_2)$ implies that $e_1^{-1} e_2 e_1 \in \mathbb{E}_2$. It is easy to check that ϑ is well-defined and $\mathrm{Ker}(\vartheta) = C_{\widetilde{\mathbb{E}}_1}(\mathbb{E}_2)$. Therefore, $|\widetilde{\mathbb{E}}_1 / C_{\widetilde{\mathbb{E}}_1}(\mathbb{E}_2)|$ divides $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)|$. By symmetry, $|\widetilde{\mathbb{E}}_2 / C_{\widetilde{\mathbb{E}}_2}(\mathbb{E}_1)|$ divides $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)|$.

Case(1) Suppose that $|\widetilde{\mathbb{E}}_j / C_{\widetilde{\mathbb{E}}_j}(\mathbb{E}_{3-j})| = 1$ for $j = 1$ or $j = 2$.

Without loss, assume that $j = 1$. Then $\widetilde{\mathbb{E}}_1 = C_{\widetilde{\mathbb{E}}_1}(\mathbb{E}_2)$ and hence $[\widetilde{\mathbb{E}}_1, \mathbb{E}_2] = 1$. Since $r \neq p$, $\mathbb{E}_1/\mathbb{K}$ is separable, thus there exists an element $a \in \widetilde{\mathbb{E}}_1 \setminus \mathbb{K}$ such that $\mathbb{E}_1 = \mathbb{K}(a)$ by Corollary 1.2.13. So $[\mathbb{E}_1, \mathbb{E}_2] = 1$, and we are done in this case.

Case(2) Suppose that

$$|\widetilde{\mathbb{E}}_j/C_{\widetilde{\mathbb{E}}_j}(\mathbb{E}_{3-j})| = r \quad \text{for} \quad j = 1, 2. \tag{1.9}$$

Then $C_{\widetilde{\mathbb{E}}_j}(\mathbb{E}_{3-j}) \lneqq \widetilde{\mathbb{E}}_j$ and hence $C_{\mathbb{E}_j}(\mathbb{E}_{3-j}) \lneqq \mathbb{E}_j$. Note that certainly $\mathbb{K} \leq C_{\mathbb{E}_j}(\mathbb{E}_{3-j})$. Therefore, $\mathbb{K} = C_{\mathbb{E}_j}(\mathbb{E}_{3-j}) \lneqq \mathbb{E}_j$ by $\dim_{\mathbb{K}} \mathbb{E}_j = r$. We now have

$$[\widetilde{\mathbb{E}}_1, \widetilde{\mathbb{E}}_2] \subseteq \widetilde{\mathbb{E}}_1 \cap \widetilde{\mathbb{E}}_2 \subseteq C_{\mathbb{E}_j}(\mathbb{E}_{3-j}) = \mathbb{K}. \tag{1.10}$$

Using (1.9), together with

$$\mathbb{K}^\sharp = C_{\mathbb{E}_j^\sharp}(\mathbb{E}_{3-j}) \quad \text{and} \quad \frac{\widetilde{\mathbb{E}}_j\mathbb{K}^\sharp}{\mathbb{K}^\sharp} \cong \frac{\widetilde{\mathbb{E}}_j}{\widetilde{\mathbb{E}}_j \cap \mathbb{K}^\sharp} \cong \frac{\widetilde{\mathbb{E}}_j}{C_{\widetilde{\mathbb{E}}_j}(\mathbb{E}_{3-j})},$$

it follows that $|\widetilde{\mathbb{E}}_j\mathbb{K}^\sharp/\mathbb{K}^\sharp| = r$. Thus there exist elements $e_j \in \widetilde{\mathbb{E}}_j \setminus \mathbb{K}$ for $j = 1, 2$. Then by (1.10) we have $[e_1, e_2] \in [\widetilde{\mathbb{E}}_1, \widetilde{\mathbb{E}}_2] \subseteq \mathbb{K}$, which implies $e_2^{-1}e_1e_2 = e_1k$ for some $k \in \mathbb{K}^\sharp$. Note that since $C_{\mathbb{E}_1}(\mathbb{E}_2) = \mathbb{K}$ and $\mathbb{E}_2 = \mathbb{K}(e_2)$, we have $[e_1, e_2] \neq 1$ and hence $k \neq 1$.

Denote $N_{\mathbb{E}_j}^{\mathbb{K}}$ by N_j. Since $e_2 \in \widetilde{\mathbb{E}}_2 \leq N_G(\mathbb{E}_1)$, we define $\theta : \mathbb{E}_1 \longrightarrow \mathbb{E}_1$ by $\theta(e) = e_2^{-1}ee_2$ where $e \in \mathbb{E}_1$. Then $\theta \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)$. Note that $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1)| = r$ by (1.9) and thus $\mathbb{E}_1/\mathbb{K}$ is a Galois extension. Since θ is a nontrivial automorphism of $\mathbb{E}_1$, $\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_1) = \langle\theta\rangle$. Using $e_2^{-1}e_1e_2 = e_1k$, we obtain $\theta^n(e_1) = k^ne_1$ for all n. Then $n = r$ gives $k^r = 1$. Hence k is an r-th root of unity. By Remark 1.2.9(d),

$$1 = N_1(e_1) = e_1 \cdot ke_1 \cdots k^{r-1}e_1 = e_1^r k^{r(r-1)/2} = e_1^r k^{\binom{r}{2}} \tag{1.11}$$

If $r \neq 2$, then $\binom{r}{2}$ is divisible by r. Since k is an r-th root of unity, we have $k^{\binom{r}{2}} = 1$. Hence, (1.11) simplifies to $e_1^r = 1$. Since $\mathbb{K}$ contains a primitive r-th

root of unity, namely k, we have $e_1 \in \mathbb{K}$, which contradicts to the choice of e_1. Therefore $r = 2$.

It remains to show $|\mathbb{K}| = 3$ and $|\mathbb{E}_j| = 9$. By (1.11), $e_1^2 = k^{-1} = -1$ as $k^2 = 1$ and $k \neq 1$. Then $e_1 = \pm i$ where $i^2 = -1$. If $k \in \mathbb{K}$ with $N_1(k) = 1$, then $k^2 = 1$ and hence $k = \pm 1$. We thus conclude that $\widetilde{\mathbb{E}}_1 = \{\pm 1, \pm i\}$. For any $a \in \mathbb{E}_1$, the N_1-norm of $a^r/N_1(a)$ is equal to 1, that is to say, $a^r/N_1(a) \in \widetilde{E}_1$. Therefore $a^2 = f$ or $a^2 = fi$ for some $f \in \mathbb{K}$. Also $\mathbb{E}_1 = \mathbb{K}(i)$. Let $k \in \mathbb{K}^\sharp$ and consider the element $k + i \in \mathbb{E}_1$. If $(k+i)^2 = k^2 - 1 + 2ki = f \in \mathbb{K}$ then $k = 0$, contradiction. Hence we may assume $(k+i)^2 = fi$. It implies that $k^2 - 1 = 0$. Thus $k = \pm 1$ and $|\mathbb{K}| = 3$ since $k \in \mathbb{K}^\sharp$ is arbitrary. Finally, $|\mathbb{E}_j| = 9$ follows from $\dim_{\mathbb{K}} \mathbb{E}_j = 2$, completing the proof of part (a).

(b) The assumption $\mathrm{GL}_{\mathbb{E}_1}(V) \cap \mathrm{SL}_{\mathbb{K}}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V)$ implies that $\widetilde{\mathbb{E}}_1 \leq N_G(\mathbb{E}_2)$. Similarly, $\widetilde{\mathbb{E}}_2 \leq N_G(\mathbb{E}_1)$. Hence $[\mathbb{E}_1^\sharp, \mathbb{E}_2^\sharp] = 1$ or we have $r = 2$, $|\mathbb{K}| = 3$, and $|\mathbb{E}_j| = 9$ by part (a).

Assume first that $[\mathbb{E}_1^\sharp, \mathbb{E}_2^\sharp] = 1$. Then $\mathbb{E}_j^\sharp \leq \mathrm{GL}_{\mathbb{E}_{3-j}}(V)$ for $j = 1, 2$. Without loss of generality, suppose

$$\dim_{\mathbb{E}_1} V \leq \dim_{\mathbb{E}_2} V. \tag{1.12}$$

If $\dim_{\mathbb{E}_2} V = 1$, then $\mathbb{E}_1^\sharp \leq \mathrm{GL}_{\mathbb{E}_2}(V) = \mathbb{E}_2^\sharp$. Moreover since $\dim_{\mathbb{E}_1} V = 1$ we have $\mathbb{E}_2^\sharp \leq \mathrm{GL}_{\mathbb{E}_1}(V) = \mathbb{E}_1^\sharp$. Thus $\mathbb{E}_1^\sharp = \mathbb{E}_2^\sharp$ and part (i) holds. So assume that $\dim_{\mathbb{E}_2} V > 1$. Since $\mathrm{SL}_{\mathbb{E}_j}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_{3-j}}(V)$, by Lemma 1.2.6 either $\mathbb{E}_1 \subseteq \mathbb{E}_2$ or $\mathbb{K} = \mathbb{E}_2 \cong \mathbb{F}_2$, $\mathbb{E}_1 \cong \mathbb{F}_4$ and $\dim_{\mathbb{K}} V = 2$. The latter case is a contradiction to the assumption $\dim_{\mathbb{K}} \mathbb{E}_j = r$. Thus $\mathbb{E}_1 \subseteq \mathbb{E}_2$. Now it clearly follows from (1.12) that $\mathbb{E}_1 = \mathbb{E}_2$.

Next assume that $r = 2$, $|\mathbb{K}| = 3$, $|\mathbb{E}_j| = 9$. If $\mathbb{E}_1 = \mathbb{E}_2$, then again part (i) holds. So assume $\mathbb{E}_1 \neq \mathbb{E}_2$, and without loss, say $\mathbb{E}_1 \not\subseteq \mathbb{E}_2$. Then $\dim_{\mathbb{E}_2} V = 1$ by Lemma 1.2.6. Hence $\dim_{\mathbb{K}} \mathbb{E}_2 = 2$ implies that $\dim_{\mathbb{K}} V = 2$ and so (ii) holds in this case.

1.3 Exceptional Cases of Theorems 2.1.1 and 2.2.3

In this section we investigate the existence of the exceptional cases that will show up in the results of the next Chapter. As in the previous sections, we let $G = \mathrm{GL}_{\mathbb{K}}(V)$, $\overline{G} = G/Z(G)$, $S = \mathrm{SL}_{\mathbb{K}}(V)$ and $\overline{S} = SZ(G)/Z(G) \cong \mathrm{PSL}_{\mathbb{K}}(V)$.

Lemma 1.3.1 *Let $G = \mathrm{GL}_2(3)$ and $g_j \in G$ such that $|\overline{g}_j| = |g_j| = 2$ for $j = 1, 2$. If $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$ and $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$, then the following holds:*

(a) $\det g_j = -1$ *and* $C_{\overline{G}}(\overline{g}_j) = \langle \overline{g}_1, \overline{g}_2 \rangle$ *is an elementary abelian group of order* 4.

(b) $C_G(g_1) \neq C_G(g_2)$.

(c) g_j *satisfies Lemma 1.1.10(2), $j = 1, 2$. In particular,* $C_G(\overline{g}_j) \neq C_G(g_j)$.

Moreover, with respect to some suitable basis, $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ *and* $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Proof: We shall prove (a)-(c) together. Since $g_1 \neq \pm 1$ and it has order 2, its minimal polynomial is $x^2 - 1$ and we may assume that $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ with respect to a basis $\{v_1, v_2\}$. Then

$$C_G(g_1) = \{\pm I, \pm g_1\} \text{ and } C_G(\overline{g}_1) = \left\{\pm I, \pm g_1, \pm \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\right\}.$$

The assumptions $C_G(\overline{g}_1) = C_G(\overline{g}_2)$ and $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$ with g_2 has order 2 imply that $\pm\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ are the only options for g_2. If necessary we may change the basis to $\{-v_1, v_2\}$ so that $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Note that the matrix of g_1 remains unchanged. Then $C_G(g_2) = \{\pm I, \pm g_2\}$ and the lemma follows easily.

Lemma 1.3.2 *Let $G = GL_2(3)$ and $g_j \in G$ such that $|\overline{g}_j| = |g_j| = 2$ for $j = 1, 2$ and $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$. If $C_{\overline{S}}(\overline{g}_1) = C_{\overline{S}}(\overline{g}_2)$, then*

(a) $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$.

(b) *g_j satisfies Lemma 1.1.10(2), $j = 1, 2$. In particular, $C_G(\overline{g}_j) \neq C_G(g_j)$.*

(c) $C_S(g_j) = \pm I$ *and* $C_G(g_1) \neq C_G(g_2)$.

Moreover, $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *and* $g_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ *for some suitable basis.*

Proof: As in the previous lemmas, we may assume that $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then

$$C_G(\overline{g}_1) = \left\{ \pm I, \pm g_1, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\} \text{ and } C_S(\overline{g}_1) = \left\{ \pm I, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Let $h := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $h \in C_S(\overline{g}_1)$ and hence $[g_2, h] \in Z(G)$. Let $g_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Using $g_2^2 = 1$, if $g_2 h = h g_2$, we get $g_2 = \pm 1$, a contradiction. Thus $g_2 h = -h g_2$ and so $g_2 = \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. As in Lemma 1.3.1 by changing the basis we may assume $g_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $C_G(g_2) = \{\pm I, \pm g_2\}$ and all parts of the lemma follow.

Lemma 1.3.3 *Let $G = GL_2(5)$ and $g_j \in G$ such that $|\overline{g}_j| = |g_j| = 2$ for $j = 1, 2$. Assume that $C_{\overline{S}}(\overline{g}_1) = C_{\overline{S}}(\overline{g}_2)$ and $C_{\overline{G}}(\overline{g}_1) \neq C_{\overline{G}}(\overline{g}_2)$. Then the following holds:*

(a) *$C_{\overline{S}}(\overline{g}_j) = \langle \overline{g}_1, \overline{g}_2 \rangle$ is an elementary abelian group of order 4.*

(b) *Lemma 1.1.10(2) holds for g_j, $j = 1, 2$. In particular $C_G(\overline{g}_j) \neq C_G(g_j)$.*

(c) $C_S(g_1) \neq C_S(g_2)$.

Furthermore, there is a basis so that $g_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ *and* $g_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Proof: Let $\mathbb{K} = \{0, \pm 1, \pm i\}$. Since $g_1 \neq \pm 1$, we may assume $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, say with respect to the basis $\{v_1, v_2\}$. Then

$$C_S(\overline{g}_1) = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ -a^{-1} & 0 \end{smallmatrix}\right) \mid a \in \mathbb{K}^\sharp \right\} \cong Q_8.$$

Also $C_{\overline{S}}(\overline{g}_1)$ is elementary abelian of order 4. Now $ig_1 \in S$ and $\overline{g}_1 \in C_{\overline{S}}(\overline{g}_1)$ imply that $g_1 g_2 = g_2 g_1 z$, where $z \in Z(S)$. Let $g_2 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Having $z = I$ would imply g_2 equals $\pm g_1$ or $\pm I$, either of which is not possible. Hence $z = -I$ and $g_2 = \pm \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ or $g_2 = \pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The second case does not hold as $|g_2| = 2$. Thus $g_2 = \pm \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. If necessary changing the basis to $\{-v_1, v_2\}$ gives $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $C_S(g_2) = \{\pm I, \pm \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)\}$ and

$$C_S(\overline{g}_2) = \left\{ \pm I, \pm \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \right\}.$$

Now observe that $\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) \in C_S(g_2) \backslash C_S(g_1)$, giving part (c). Also $\left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right) \in C_{\overline{G}}(\overline{g}_2) \backslash C_{\overline{G}}(\overline{g}_1)$. Now the lemma follows.

Lemma 1.3.4 *Let $G = GL_3(4)$ and $g_j \in G$ with $|\overline{g}_j| = |g_j| = 3$ for $j = 1, 2$. Assume that g_j has three different eigenvalues. If $C_{\overline{S}}(\overline{g}_1) = C_{\overline{S}}(\overline{g}_2)$ and $C_{\overline{G}}(\overline{g}_1) \neq C_{\overline{G}}(\overline{g}_2)$, then the following holds:*

(a) *$C_{\overline{S}}(\overline{g}_j) = \langle \overline{g}_1, \overline{g}_2 \rangle$ is an elementary abelian group of order 9.*

(b) *Lemma 1.1.10(2) holds for g_j, $j = 1, 2$. In particular $C_G(\overline{g}_j) \neq C_G(g_j)$.*

(c) *$C_S(g_1) \neq C_S(g_2)$.*

Moreover, there exists a suitable basis and $\xi \in \mathbb{K}^\sharp$ with $|\xi| = 3$ so that

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix} \text{ and } \quad g_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Also the pair (g_1, g_2) *is unique up to conjugation by an element of* $\Gamma\mathrm{GL}_3(4)$.

Proof: Let $\mathbb{K} = \{0, 1, \xi, \xi^2\}$ where $\xi^3 = 1$. Since g_1 has three distinct eigenvalues, we may assume

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix}$$

with respect to some basis $\{v_1, v_2, v_3\}$. Hence

$$C_G(\overline{g}_1) = \left\{ \begin{pmatrix} * & 0 & 0 \\ 0 & * & 0 \\ 0 & 0 & * \end{pmatrix}, \begin{pmatrix} 0 & 0 & * \\ * & 0 & 0 \\ 0 & * & 0 \end{pmatrix}, \begin{pmatrix} 0 & * & 0 \\ 0 & 0 & * \\ * & 0 & 0 \end{pmatrix} \mid * \in \mathbb{K}^\sharp \right\},$$

$|C_S(\overline{g}_1)| = 27$, and $C_{\overline{S}}(\overline{g}_1)$ is elementary abelian of order 9. Since $g_1 \in C_S(\overline{g}_1)$ we have $g_2 g_1 = g_1 g_2 z$ for some $z \in Z(S)$. Let $g_2 = (a_{ij})$ and use $|g_2| = 3$. Then if $z = 1$, we get $g_2 \in Z(S)$ or $g_2 = k g_1^{\pm 1}$ for some $k \in \mathbb{K}$, a contradiction. Hence $z \neq 1$ and so $z \in \mathbb{K}^\sharp$ with $|z| = 3$. Without loss of generality (by changing v_2 and v_3 if necessary), we assume that $z = \xi$. Then $g_2 = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}$ where $abc = 1$. In this case changing the basis to $\{v_1, av_2, abv_3\}$, we get $g_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. Note that the matrix of g_1 is unchanged with respect to this basis.

Now a trivial calculation gives parts (a) and (b). We also note that

$$g_2 \in C_S(g_2) \setminus C_S(g_1) \text{ and } \begin{pmatrix} 0 & 0 & 1 \\ \xi & 0 & 0 \\ 0 & \xi & 0 \end{pmatrix} \in C_G(\overline{g}_1) \setminus C_G(\overline{g}_2).$$

Lemma 1.3.5 *Let* $G = GL_2(3)$, $g_j \in G$ *with* $|\overline{g}_j| = 2$, $|g_j| \neq 2$ *for* $j = 1, 2$ *and* $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$. *Assume that* $C_{\overline{G}}(\overline{g}_1) \neq C_{\overline{G}}(\overline{g}_2)$ *and* $C_{\overline{S}}(\overline{g}_1) = C_{\overline{S}}(\overline{g}_2)$. *Then* $|g_j| = 4$ *and* $C_{\overline{S}}(\overline{g}_j) = \langle \overline{g}_1, \overline{g}_2 \rangle$ *is an elementary abelian group of order* 4. *Moreover, with respect to some basis,*

$$g_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Proof: Note that $|g_j| = 4$, since $g_j^2 = -1$. Furthermore, $vg_1 \neq \pm v$, for any $0 \neq v \in V$. Hence, with respect to the basis $\{v, vg_1\}$, we have $g_1 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Also, with respect to the same basis, the only elements of G of order 4 other than $\pm g_1$ are the followings:

$$\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right).$$

If we have the first case above, then we are done. If not, we can change the basis to $\{v + vg_1, -v + vg_1\}$, $\{v - vg_1, v + vg_1\}$, and $\{-vg_1, v\}$, respectively, to get $g_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ while the matrix representation of g_1 remains unchanged. Elementary calculations give $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in C_G(\overline{g}_2) \setminus C_G(\overline{g}_1)$ and $C_{\overline{S}}(\overline{g}_j) = \langle \overline{g}_1, \overline{g}_2 \rangle$.

Chapter 2

Centralizers in $\mathrm{PGL}_{\mathbb{K}}(V)$ and $\mathrm{PSL}_{\mathbb{K}}(V)$

In this chapter, we prove two main results (Theorems 2.1.1 and 2.2.3) which describe when two distinct elements of prime order in the finite dimensional projective and special linear group shall have the same centralizer. We adopt the notation and set up of Chapter 1. *Furthermore, throughout this chapter we will assume that* $r \neq p$.

2.1 The $\mathrm{PGL}_{\mathbb{K}}(V)$ Case

Theorem 2.1.1 *For* $j = 1, 2$, *let* $\overline{g}_j \in \overline{G}$ *with* $|\overline{g}_j| = r$ *and choose* g_j *so that* $|kg_j| \geq |g_j|$ *for all* $k \in \mathbb{K}^\sharp$. *Then* $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$ *if and only if one of the following holds.*

(a) $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$.

(b) $C_G(g_1) = C_G(g_2)$, $|g_j| = r$, *and* $\overline{C_G(g_j)} = C_{\overline{G}}(\overline{g}_j)$ *for* $j = 1, 2$.

(c) $r = 2$, $|\mathbb{K}| = 3$, *and* $\dim_{\mathbb{K}} V = 2$. *Moreover, there exists a basis of* V *with respect to which* $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ *and* $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Proof: ($\Longleftarrow$) See the proof of Lemma 1.3.1.

($\Longrightarrow$) Assume that $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$ and hence

$$C_G(\overline{g}_1) = C_G(\overline{g}_2). \tag{2.1}$$

Due to lemmas 1.1.10 and 1.1.15, it is reasonable to split the proof into the following five cases:

Case 1. $|g_j| = r$ and $C_G(\overline{g}_j) = C_G(g_j)$ for $j = 1, 2$.

Case 2. $|g_j| = r$ for $j = 1, 2$, and $C_G(\overline{g}_1) = C_G(g_1)$, $C_G(\overline{g}_2) \neq C_G(g_2)$.

Case 3. $|g_j| = r$ and $C_G(\overline{g}_j) \neq C_G(g_j)$ for $j = 1, 2$.

Case 4. $|g_j| \neq r$ for $j = 1, 2$.

Case 5. $|g_1| = r$, $|g_2| \neq r$.

Case 1. By the hypothesis of this case and (2.1), clearly Theorem 2.1.1(b) is attained.

Case 2. Note that the assumptions of this case imply that g_1 and g_2 satisfy parts (1) and (2) of Lemma 1.1.10, respectively. Then, using Lemma 1.1.5, we have

$$C_G(\overline{g}_1) = C_G(g_1) = \bigtimes_{i=1}^{s_1} \mathrm{GL}_{\mathbb{E}_{i1}}(V_{i1}), \tag{2.2}$$

$$C_G(\overline{g}_2) = C_G(g_2)\langle h_2 \rangle = \Big[\bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i2})\Big]\langle h_2 \rangle. \tag{2.3}$$

We observe that V is a simple $C_G(\overline{g}_2)$-module. Then (2.1), together with (2.2), gives $s_1 = 1$, and hence $V_{11} = V$. Moreover, by Lemma 1.1.10 (2a), $\mathbb{E} = \mathbb{K}$. Recall that $\mathbb{E}$ was the splitting field of $x^r - 1$ over $\mathbb{K}$ and $\mathbb{E}_{i1} = \mathbb{K}$ or $\mathbb{E}$ by

Lemma 1.1.5(f). Hence $\mathbb{E}_{11} = \mathbb{K}$. Therefore (2.2) turns into $C_G(g_1) = \mathrm{GL}_{\mathbb{K}}(V)$, that is, $g_1 \in Z(G)$, a contradiction to $|\overline{g}_1| = r$. Hence, this case does not occur.

Case 3. Note that we are in the situation of Lemma 1.1.10(2) for both g_1 and g_2. In particular, we have (2.3) and

$$C_G(\overline{g}_1) = C_G(g_1)\langle h_1 \rangle = \Big[\bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i1})\Big]\langle h_1 \rangle. \tag{2.4}$$

Furthermore, the V_{ij}'s have the same dimension over $\mathbb{K}$ for all i and j, namely $\dim_{\mathbb{K}} V_{ij} = \dim_{\mathbb{K}} V/r$.

Step 1. *If $C_G(g_1) = C_G(g_2)$, then $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$ (and hence Theorem 2.1.1(a) holds)*:

We use the notation and results of Lemma 1.1.5 and Lemma 1.1.10(2) and write $V = V_{1j} \oplus V_{2j} \oplus \cdots \oplus V_{rj}$ where $V_{ij} = \mathrm{Ann}(f_{ij}(g_j)) = \{v \in V \mid g_j v = \xi_j^{i-1} v\}$ for all $1 \leq i \leq r$ and $j = 1, 2$ where $\xi_j \in \mathbb{K}^\sharp$ is a primitive r-th root of unity. Now, g_j acts as $(1, \xi_j, \xi_j^2, \ldots, \xi_j^{r-1})$ on $(V_{1j}, V_{2j}, \cdots, V_{rj})$. Put $\xi = \xi_1$. By Lemma 1.1.9,

$$\{V_{i1} \mid 1 \leq i \leq r\} = \{V_{i2} \mid 1 \leq i \leq r\}.$$

Hence g_2 is of the form $(\xi^{i_1}, \xi^{i_2}, \ldots, \xi^{i_r})$ on V where the exponents i_k are in $\mathbb{Z}$. Note that $\overline{g}_2 = \overline{\xi^{-i_1} g_2}$. Replacing g_2 by $\xi^{-i_1} g_2$, we may assume that g_2 acts as an identity on V_{11} and hence $g_2 = (1, \xi^{i_2}, \ldots, \xi^{i_r})$. On V_{21}, we have $g_2^n v = \xi^{n i_2} v$ for any integer n. Choose an n so that $\xi^{n i_2} = \xi$. Note that $\langle \overline{g}_2 \rangle = \langle \overline{g_2^n} \rangle$. Then replacing g_2 by g_2^n gives $g_2 = (1, \xi, \xi^{i_2}, \ldots, \xi^{i_r})$. Thus,

$$V_{11} = V_{12} \quad \text{and} \quad V_{21} = V_{22}. \tag{2.5}$$

Take $y \in C_G(\overline{g}_1)$ with $yV_{11} = V_{21}$. Then, by Remark 1.1.11, $yV_{i1} = V_{i+1,1}$ for all i. Now (2.1), together with (2.5), implies that $y \in C_G(\overline{g}_2)$ and $yV_{12} = V_{22}$. Hence $yV_{i2} = V_{i+1,2}$ for all i. It follows that $V_{i1} = V_{i2}$ for all i and thus $g_1 = g_2$ and $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$.

Step 2. *If* $\dim_{\mathbb{K}} V_{ij} > 1$, *then* $C_G(g_1) = C_G(g_2)$ *and part*(a) *holds*:

First assume $|\mathbb{K}| > 3$. Since $C_G(\overline{g}_j)/C_G(g_j) \cong \langle h_j \rangle$ is abelian, we have $C_G(\overline{g}_j)'' \leq C_G(g_j)' = \bigtimes_{i=1}^{r} (\mathrm{GL}_{\mathbb{K}}(V_{ij}))' = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{ij})$. Conversely, we have $\mathrm{SL}_{\mathbb{K}}(V_{ij}) = (\mathrm{SL}_{\mathbb{K}}(V_{ij}))'' \leq C_G(\overline{g}_j)''$ for each i. Thus $C_G(\overline{g}_j)'' = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{ij})$. If $|\mathbb{K}| \leq 3$, let us consider the group $O^{p'}(C_G(\overline{g}_j))$. Since the quotient $C_G(\overline{g}_j)/C_G(g_j)$ is a p'-group, $O^{p'}(C_G(\overline{g}_j)) = O^{p'}(C_G(g_j))$. Besides

$$O^{p'}(C_G(g_j)) = \bigtimes_{i=1}^{r} O^{p'}(\mathrm{GL}_{\mathbb{K}}(V_{ij})) = \bigtimes_{i=1}^{r} O^{p'}(\mathrm{SL}_{\mathbb{K}}(V_{ij})) = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{ij}).$$

For the last equality we used the fact that $\mathrm{SL}_{\mathbb{K}}(V_{ij})$ is generated by transvections and if $t \in \mathrm{SL}_{\mathbb{K}}(V_{ij})$ is a transvection then it has order p, which implies that $t \in O^{p'}(\mathrm{SL}_{\mathbb{K}}(V_{ij}))$. Thus, the assumption (2.1) yields

$$\bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{i1}) = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{i2}).$$

regardless of the order of $\mathbb{K}$. Therefore, $\{V_{i1} \mid 1 \leq i \leq r\} = \{V_{i2} \mid 1 \leq i \leq r\}$ by Lemma 1.1.7. Since $\mathbb{E}_{ij} = \mathbb{K}$, we deduce from Lemma 1.1.9 that $C_G(g_1) = C_G(g_2)$. By step (1), we conclude that whenever $\dim_{\mathbb{K}} V_{ij} > 1$ part (a) of the theorem holds. It remains to treat the case $\dim_{\mathbb{K}} V_{ij} = 1$.

Step 3. *If* $\dim_{\mathbb{K}} V_{ij} = 1$ *for all* i, *then* $C_G(g_1) = C_G(g_2)$ *or* $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$:

This statement follows from Proposition 1.1.12 and by mentioning that both $C_G(g_1)$ and $C_G(g_2)$ are contained in $C_G(\overline{g}_j)$.

The case $C_G(g_1) = C_G(g_2)$ implies that part (a) holds again by step (1). Therefore, we may assume $r = 2$, $|\mathbb{K}| = 3$ and $\dim_{\mathbb{K}} V = 2$. Lemma 1.3.1 shows that this exceptional case does really occur and the properties stated in part (c) are satisfied. Moreover, since $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$ and $C_G(g_1) \neq C_G(g_2)$, we get a new case as claimed in the theorem.

Case 4. Note that in this case we have $|kg_j| \neq r$ for all $k \in \mathbb{K}^\sharp$, $j = 1, 2$. Put $\mathbb{E}_j := \mathbb{K}[g_j] \leq \mathrm{End}_{\mathbb{K}}(V)$. Then Lemma 1.1.15 implies that $\mathbb{E}_j$ is a field and $|\mathbb{K}| > 2$. By Lemma 1.1.4, $C_G(g_j) = \mathrm{GL}_{\mathbb{E}_j}(V) \subseteq C_G(\overline{g}_j) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_j}(V)$ which implies, together with the assumption (2.1), that $\mathrm{GL}_{\mathbb{E}_1}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V)$ and $\mathrm{GL}_{\mathbb{E}_2}(V) \leq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_1}(V)$. Therefore, $\mathbb{E}_1 = \mathbb{E}_2$ or $\mathbb{K} = \mathbb{F}_2$ by Proposition 1.2.7. The latter case does not hold. Thus $\mathbb{E}_1 = \mathbb{E}_2$ and by Lemma 1.2.3, we get $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$, giving part (a).

Case 5. Recall that by the hypothesis of this case, g_1 satisfies Lemma 1.1.10 and hence one of the following holds:

$$C_G(\overline{g}_1) = C_G(g_1) = \bigtimes_{i=1}^{s_1} \mathrm{GL}_{\mathbb{E}_{i1}}(V_{i1}) \quad \text{or} \tag{2.6a}$$

$$C_G(\overline{g}_1) = C_G(g_1)\langle h_1 \rangle = \left[\bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i1})\right] \langle h_1 \rangle. \tag{2.6b}$$

By the assumption of this case g_2 satisfies Lemma 1.1.15 and in particular, $\mathbb{E}_2 := \mathbb{K}[g_2]$ is a field with $\dim_{\mathbb{K}} \mathbb{E}_2 = r$. Thus Lemma 1.1.4 implies

$$C_G(g_2) = \mathrm{GL}_{\mathbb{E}_2}(V) \subseteq C_G(\overline{g}_2) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V).$$

We observe that $C_G(\overline{g}_2)$ acts transitively on V and so is primitive. Thus, $C_G(\overline{g}_1)$ is primitive. Hence (2.6b) does not hold and $s_1 = 1$, which means that the minimal polynomial of g_1 is irreducible. Then $V_{11} = V$ and $\mathbb{E}_{11} = \mathbb{K}[g_1]$. By Lemma 1.1.5(f), $\mathbb{E}_{11} = \mathbb{K}$ or $\mathbb{E}$. If $\mathbb{E}_{11} = \mathbb{K}$, then (2.6a) gives $g_1 \in Z(G)$, a contradiction to $|\overline{g}_1| = r$. Thus $\mathbb{E}_{11} = \mathbb{E}$. Note that since $\mathbb{E}$ is the splitting field of $x^r - 1$ over $\mathbb{K}$, $\dim_{\mathbb{K}} \mathbb{E}_{11} < r$. By Lemma 1.1.4, $C_G(g_1) = \mathrm{GL}_{\mathbb{E}_{11}}(V) \subseteq C_G(\overline{g}_1) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_{11}}(V)$. We now can imitate the proof given in Case (4) and apply Proposition 1.2.7 where $\mathbb{E}_1$ is replaced by $\mathbb{E}_{11}$ and conclude that $\mathbb{E}_{11} = \mathbb{E}_2$. But, this is a contraction because these fields have different dimensions over $\mathbb{K}$. Thus, Case (5) does not hold.

2.2 The $\mathrm{PSL}_{\mathbb{K}}(V)$ Case

In the $\mathrm{PSL}_{\mathbb{K}}(V)$ case, we have an analogue to Theorem 2.1.1. For its proof, we will use the following lemmas.

Lemma 2.2.1 *Let $g \in G$ with $|g| = r$. Let the notation be as in Lemma 1.1.5. Then the following holds:*

(a) *V_i is a simple $\mathbb{K}C_S(g)$-submodule of V for all i.*

(b) *Assume that $g \neq -I$. Then $\{V_i \mid 1 \leq i \leq s\}$ is the set of all simple $\mathbb{K}C_S(g)$-submodules of V if and only if the following does not hold:*

$$r = 2,\ |\mathbb{K}| = 3,\ \textit{and}\ \ \dim_{\mathbb{K}} V = 2. \qquad (\dagger)$$

(c) $\mathbb{E}_i = \mathrm{End}_{\mathbb{K}C_S(g)}(V_i)$ *for all* $1 \leq i \leq s$.

Proof: Note that we have

$$C_S(g) = \mathrm{SL}_{\mathbb{K}}(V) \cap \bigtimes_{i=1}^{s} \mathrm{GL}_{\mathbb{E}_i}(V_i) \geq \bigtimes_{i=1}^{s} \mathrm{SL}_{\mathbb{E}_i}(V_i). \tag{2.7}$$

(a) Fix an $i \in \{1, 2 \ldots, s\}$.

If $\dim_{\mathbb{E}_i} V_i > 1$, then V_i is a simple $\mathrm{SL}_{\mathbb{E}_i}(V_i)$-submodule and, in particular, it is a simple $\mathbb{K}C_S(g)$-submodule of V. Now assume $\dim_{\mathbb{E}_i} V_i = 1$. If $\mathbb{K} = \mathbb{E}_i$, then V_i is a 1-dimensional $\mathbb{K}$-space and hence it is simple. Therefore, we may suppose that $\mathbb{K} \neq \mathbb{E}_i$. Note that for all $e \in \mathbb{E}_i^\sharp$, we have $\det_{\mathbb{E}_i}^{\mathbb{K}}(e) = N_{\mathbb{E}_i}^{\mathbb{K}}(e)$ by definition. Moreover, by (2.7) and by the assumption $\dim_{\mathbb{E}_i} V_i = 1$, we have $C_S(g) \supseteq \{e \in \mathbb{E}_i^\sharp \mid \det_{\mathbb{E}_i}^{\mathbb{K}}(e) = 1\} = \{e \in \mathbb{E}_i^\sharp \mid N_{\mathbb{E}_i}^{\mathbb{K}}(e) = 1\} = \widetilde{\mathbb{E}}_i$. By Lemma 1.1.5(f), $\mathbb{E}_i = \mathbb{E}$ (recall that $\mathbb{E}$ is the splitting field of $x^r - 1$ ove $\mathbb{K}$). Hence, $\mathbb{E}_i$ is a Galois extension over $\mathbb{K}$ and, in particular, it is separable. Observe that V_i is simple if $\mathbb{E}_i = \mathbb{K}(e \in \mathbb{E}_i^\sharp \mid N_{\mathbb{E}_i}^{\mathbb{K}}(e) = 1)$. But, this is immediate by Corollary 1.2.13, proving part (a).

(b) We observe, by Remark 1.1.6 and part (a), that the V_i's are the set of all simple submodules if and only if they are pairwise non-isomorphic. Thus, it is enough to show that V_i's are non-isomorphic if and only if (†) does not hold.

($\Longleftarrow$) Suppose that there exist j and k such that $1 \leq j \neq k \leq s$ and $V_j \cong V_k$ as $\mathbb{K}C_S(g)$-submodules. We shall show that (†) holds.

Step 1. $\dim_{\mathbb{E}_j} V_j = \dim_{\mathbb{E}_k} V_k = 1$. *In particular,* $|\mathbb{E}_j| = |V_j| = |V_k| = |\mathbb{E}_k|$:
Suppose false and without loss of generality let $\dim_{\mathbb{E}_j} V_j \neq 1$. Then $1 \neq \mathrm{SL}_{\mathbb{E}_j}(V_j)$ acts nontrivially on V_j and trivially on V_k, contradiction.

Step 2. $\mathbb{K} = \mathbb{E}_j = \mathbb{E}_k$ *and* $|\mathbb{K}| \leq 3$:

Since $V_j \cong V_k$, there exists a $\mathbb{K}C_S(g)$-linear isomorphism $\alpha : V_j \longrightarrow V_k$. Define the map $\widetilde{\alpha} : \mathrm{End}_{\mathbb{K}\langle g\rangle}(V_j) \longrightarrow \mathrm{End}_{\mathbb{K}\langle g\rangle}(V_k)$ by $\widetilde{\alpha}(\sigma)(v_k) = \alpha(\sigma(\alpha^{-1}(v_k)))$ where $\sigma \in \mathrm{End}_{\mathbb{K}\langle g\rangle}(V_j)$ and $v_k \in V_k$. It is straight forward to check that $\widetilde{\alpha}$ is an isomorphism of $\mathbb{K}$-algebras. Since $\dim_{\mathbb{E}_j} V_j = 1$, we have $\mathrm{End}_{\mathbb{E}_j}(V_j) = \mathbb{E}_j$, that is, $\mathrm{End}_{\mathbb{K}\langle g\rangle}(V_j) = \mathbb{E}_j$ and, by symmetry, we also have $\mathrm{End}_{\mathbb{K}\langle g\rangle}(V_k) = \mathbb{E}_k$. Therefore $\widetilde{\alpha} : \mathbb{E}_j \longrightarrow \mathbb{E}_k$. Take an element $e \in \mathbb{E}_j^\sharp$ and define $\overline{e} \in G$ by

$$\overline{e}v = \begin{cases} ev & \text{if } v \in V_j \\ \widetilde{\alpha}(e)^{-1}v & \text{if } v \in V_k \\ v & \text{if } v \in V_l,\ l \neq j,k \end{cases}$$

Since by definition $\mathbb{E}_j = \mathbb{K}[g_j]$ where $g_j = g|_{V_j}$, and similarly for k, we see that $\overline{e}$ commutes with g. Also $\widetilde{\alpha}(e) = \alpha e \alpha^{-1}$ by definition. Taking the determinant of both sides gives $\det(\widetilde{\alpha}(e)) = \det(\alpha e \alpha^{-1}) = \det(e)$. Thus, $\det(\overline{e}) = 1$ and hence $\overline{e} \in C_S(g)$. By $\mathbb{K}C_S(g)$-linearity of α, we have $\alpha(\overline{e}v_j) = \overline{e}\alpha(v_j)$ for all $v_j \in V_j$. Expanding this equality gives $\alpha(ev_j) = \alpha(\overline{e}v_j) = \overline{e}\alpha(v_j) = \widetilde{\alpha}(e)^{-1}\alpha(v_j) = \widetilde{\alpha}(e^{-1})\alpha(v_j) = \alpha(e^{-1}\alpha^{-1}(\alpha v_j)) = \alpha(e^{-1}v_j)$, that is, $\alpha(ev_j) = \alpha(e^{-1}v_j)$ for all $v_j \in V_j$ and $e \in \mathbb{E}_j^\sharp$. Now by injectivity of α, $ev_j = e^{-1}v_j$. Hence $e = e^{-1}$, i.e., $e^2 = 1$. As e is an arbitrary element of $E_j^\sharp$, we conclude that $|\mathbb{E}_j| \leq 3$. Hence $\mathbb{E}_j = \mathbb{K}$ as $\mathbb{K} \subseteq \mathbb{E}_j$. Then $\mathbb{E}_j = \mathbb{K} = \mathbb{E}_k$ because $|\mathbb{E}_j| = |\mathbb{E}_k|$ and $\mathbb{K} \subseteq \mathbb{E}_k$. Also $|\mathbb{K}| \leq 3$.

Step 3. $|\mathbb{K}| = 3$, $r = 2$, *and* $\dim_{\mathbb{K}} V = 2$:

By Lemma 1.1.5(f), $\mathbb{E}_i \neq \mathbb{E}$ for at most one i, $1 \leq i \leq s$. So $\mathbb{E}_j = \mathbb{K} = \mathbb{E}_k = \mathbb{E}$ and since $|\mathbb{K}| \leq 3$, $r \neq p$, and $\mathbb{E}$ contains a primitive r-th root of unity, we conclude that $|\mathbb{K}| = 3$ and $r = 2$. Since $s \leq r = 2$, we also have $\dim_{\mathbb{K}} V = 2$, completing

the proof of this direction.

($\Longrightarrow$) Suppose that (†) holds. Since $g \neq -I$ and g has order 2, its minimal polynomial is $x^2 - 1$, and $V = V_1 \oplus V_2$. Without loss of generality, we may assume $g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then V_1 and V_2 are isomorphic as $\mathbb{K}C_S(g)$-modules because $C_S(g) = \pm I$.

(c) The proof splits into two cases depending on the dimension of $\dim_{\mathbb{E}_i} V_i$.

First assume that $\dim_{\mathbb{E}_i} V_i = 1$. Then $\widetilde{\mathbb{E}}_i \subseteq C_S(g)$. Since $\mathbb{E}_i = \mathbb{K}$ or $\mathbb{E}_i/\mathbb{K}$ is Galois, we have $\mathbb{E}_i = \mathbb{K}(\widetilde{\mathbb{E}}_i) \subseteq \phi(\mathbb{K}C_S(g))$ by Corollary 1.2.13 where ϕ is the canonical homomorphism $\phi : \mathbb{K}C_S(g) \to \mathrm{End}_{\mathbb{K}}(V)$. Therefore, $\mathbb{E}_i \subseteq \mathrm{End}_{\mathbb{K}C_S(g)}(V_i) \subseteq \mathrm{End}_{\mathbb{E}_i}(V_i) = \mathrm{End}_{\mathbb{E}_i}(\mathbb{E}_i) = \mathbb{E}_i$ which gives $\mathbb{E}_i = \mathrm{End}_{\mathbb{K}C_S(g)}(V_i)$, as claimed.

If $\dim_{\mathbb{E}_i} V_i \neq 1$, then we have $\mathbb{E}_i = C_{\mathrm{End}_{\mathbb{K}}(V_i)}(\mathrm{SL}_{\mathbb{E}_i}(V_i))$ by Lemma 1.2.5. Now let $\varphi \in \mathrm{End}_{\mathbb{K}C_S(g)}(V_i)$. Then φ commutes with every element in $C_S(g)$. Because of (2.7), in particular, φ commutes with every element in $\mathrm{SL}_{\mathbb{E}_i}(V_i)$ which gives $C_{\mathrm{End}_{\mathbb{K}}(V_i)}(\mathrm{SL}_{\mathbb{E}_i}(V_i)) \supseteq \mathrm{End}_{\mathbb{K}C_S(g)}(V_i)$. Combining these two, we obtain

$$\mathbb{E}_i = C_{\mathrm{End}_{\mathbb{K}}(V_i)}(\mathrm{SL}_{\mathbb{E}_i}(V_i)) \supseteq \mathrm{End}_{\mathbb{K}C_S(g)}(V_i) \supseteq \mathbb{E}_i,$$

which completes the proof of part (c).

Proposition 2.2.2 *Let $g_j \in G$ with $|g_j| = r$ and $g_j \neq -I$ for $j = 1, 2$. Then $C_S(g_1) = C_S(g_2)$ if and only if one of the following holds:*

(a) $C_G(g_1) = C_G(g_2)$.

(b) $|g_j| = 2$, $\det g_j = -1$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$, *and* $C_S(g_j) = \pm I$.

Proof: ($\Longleftarrow$) Obvious.

($\Longrightarrow$) Suppose that $C_S(g_1) = C_S(g_2)$.

Assume first that (b) does not hold. Then for $j = 1, 2$, $\{V_{ij} \mid 1 \leq i \leq s_j\}$ is the set

of all simple $\mathbb{K}C_S(g_j)$-submodules of V by Lemma 2.2.1. Since $C_S(g_1) = C_S(g_2)$, we conclude that $s := s_1 = s_2$ and $V_{i1} = V_{i2}$ for all $1 \leq i \leq s$. Furthermore, $\mathbb{E}_{i1} = \mathrm{End}_{\mathbb{K}C_S(g_1)}(V_{i1}) = \mathrm{End}_{\mathbb{K}C_S(g_2)}(V_{i2}) = \mathbb{E}_{i2}$ by part (c) of previous lemma. Hence $C_G(g_1) = C_G(g_2)$ by Lemma 1.1.9.

It remains to treat the case $r = 2$, $|\mathbb{K}| = 3$ and $\dim_{\mathbb{K}} V = 2$. The following claim implies that part (b) does occur.

Claim: Let $G = GL_2(3)$ and $g \in G$ be such that $|g| = 2$ and $g \neq -1$. Then $\det g = -1$ and $C_S(g_j) = \pm I$. In particular, if $g_1, g_2 \in G$ with $|g_j| = 2$ and $g_j \neq \pm 1$, then $C_S(g_1) = C_S(g_2)$.

Proof of claim: The minimal polynomial of g is $x^2 - 1$ and, without loss, we put $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Take $x \in C_S(g)$ and let $x = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $[x, g] = 1$ and $x \in S$ imply that $x = \pm I$, and so $C_S(g) = \{\pm I\}$.

Theorem 2.2.3 *Let $\overline{g}_j \in \overline{G}$ with $|\overline{g}_j| = r$ for $j = 1, 2$. Choose g_j so that $|kg_j| \geq |g_j|$ for all $k \in \mathbb{K}^\sharp$. Then $C_{\overline{S}}(\overline{g}_1) = C_{\overline{S}}(\overline{g}_2)$ if and only if one of the following holds:*

(a) $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$.

(b) $|g_j| = r$, $r = 3$, $|\mathbb{K}| = 4$, $\dim_{\mathbb{K}} V = 3$, *and there exists a basis of V and some $\xi \in \mathbb{K}^\sharp$ with $|\xi| = 3$ such that*

$$g_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^2 \end{pmatrix} \text{ and } \quad g_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

(c) $|g_j| = r$, $r = 2$, $|\mathbb{K}| = 5$, $\dim_{\mathbb{K}} V = 2$, *and there exists a basis of V such that $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

(d) $|g_j| = 4$, $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$ *and $g_1 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ for some suitable basis of V.*

Proof: ($\Longleftarrow$) See the proof of Lemmas 1.3.3, 1.3.4, and 1.3.5.

($\Longrightarrow$) Assume that

$$C_S(\overline{g}_1) = C_S(\overline{g}_2). \tag{2.8}$$

As before, the proof splits into five cases and those are exactly the same cases as in the proof of Theorem 2.1.1 (see page 39).

Case 1. If $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$, then (a) holds. So assume $\langle \overline{g}_1 \rangle \neq \langle \overline{g}_2 \rangle$. By the hypothesis of this case, we have $C_G(\overline{g}_j) = C_G(g_j)$ and hence $C_S(\overline{g}_j) = C_S(g_j)$. Then by (2.8), we obtain $C_S(g_1) = C_S(g_2)$. By Proposition 2.2.2, we have either the case $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$ or $C_G(g_1) = C_G(g_2)$. But, the first case does not satisfy the assumption $C_G(\overline{g}_j) = C_G(g_j)$ by Lemma 1.3.2. Thus $C_G(g_1) = C_G(g_2)$. By the assumptions of Case (1), we get $C_{\overline{G}}(\overline{g}_1) = C_{\overline{G}}(\overline{g}_2)$.

Case 2. In this case, g_1 and g_2 satisfy part (1) and (2) of Lemma 1.1.10, respectively. Then, using Lemma 1.1.5, we have

$$C_G(\overline{g}_1) = C_G(g_1) = \bigtimes_{i=1}^{s_1} \mathrm{GL}_{\mathbb{E}_{i1}}(V_{i1}), \tag{2.9}$$

$$C_S(\overline{g}_2) = S \cap C_G(g_2)\langle h_2 \rangle = S \cap \left(\left[\bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i2}) \right] \langle h_2 \rangle \right) \tag{2.10}$$

and, by Lemma 1.1.10 (2a) we have $\mathbb{E} = \mathbb{K}$. Furthermore, $\mathbb{E}_{i1} = \mathbb{K} = \mathbb{E}$ by Lemma 1.1.5(f).

Claim: V is a simple $\mathbb{K}C_S(\overline{g}_2)$-module.

Observe that $g_2 \neq -I$. Assume first that $r = 2, |\mathbb{K}| = 3$, and $\dim_{\mathbb{K}} V = 2$. Without loss of generality, we put $g_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Then

$$C_S(\overline{g}_2) = \left\{ \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \right\} = \langle x := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \rangle.$$

Note that x has order 4 and its eigenvalues are 4-th roots of unity. Suppose that $W := \mathbb{K}w = \langle w \rangle$ is a 1-dimensional $\mathbb{K}C_S(\overline{g}_2)$-invariant subspace of V. Then for an arbitrary $h \in C_S(\overline{g}_2)$, we have $hw = kw$ for some $k \in \mathbb{K}^\sharp$. Thus the only eigenvalues of h are ± 1, a contradiction. Hence such a W does not exist and V is a simple module.

Now assume that we are not in the above case, let $0 \neq W \leq V$ be a $\mathbb{K}C_S(\overline{g}_2)$-submodule and $0 \neq U$ be a simple $\mathbb{K}C_S(g_2)$-submodule of W. By Lemma 2.2.1, $U = V_{k2}$ for some $1 \leq k \leq r$. Let $x := (t, 1, 1, \ldots, 1) \in \bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i2})$ be chosen such that $\det(t) = \det(h_2)^{-1}$. Then $xh_2 \in C_S(\overline{g}_2)$ and $\langle xh_2 \rangle$ permutes the subspaces V_{i2} for all i. So $V \leq V_{k2}^{\langle xh_2 \rangle} = U^{\langle xh_2 \rangle} \subseteq W$, that is $V = W$, proving the claim.

The above claim, along with (2.8), implies that V is a simple $C_S(\overline{g}_1)$-module. This implies $s_1 = 1$ and $V = V_{11}$. Consequently, (2.9) simplifies to $C_G(g_1) = \mathrm{GL}_{\mathbb{K}}(V)$, that is, $g_1 \in Z(G)$, a contradiction to $|\overline{g}_1| = r$. Hence Case (2) does not hold.

Case 3. In this case, Lemma 1.1.10(2) holds for both g_1 and g_2. In particular we have (2.10) and a similar formula for g_1 holds. The proof of this case is essentially the same as the proof of Case (3) of Theorem 2.1.1:

Suppose first that $\dim_{\mathbb{K}} V_{ij} > 1$ *for all* i, j.

If $|\mathbb{K}| > 3$, then $C_S(\overline{g}_j)'' = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{ij})$ and if $|\mathbb{K}| \leq 3$, then $O^{p'}(C_S(\overline{g}_j)) =$

$\bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{ij})$. Hence in both cases we get

$$\bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{i1}) = \bigtimes_{i=1}^{r} \mathrm{SL}_{\mathbb{K}}(V_{i2}).$$

Therefore, by Lemma 1.1.7, $\{V_{i1} \mid 1 \leq i \leq r\} = \{V_{i2} \mid 1 \leq i \leq r\}$. By Lemma 1.1.9, $C_G(g_1) = C_G(g_2)$. Hence, by Step(1) of Case (3) in the proof of Theorem 2.1.1 (see page 40), we conclude that $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$ and so $C_G(\overline{g}_1) = C_G(\overline{g}_2)$.

Suppose next that $\dim_{\mathbb{K}} V_{ij} = 1$ *for all* i, j.

Then Proposition 1.1.13 implies that one of the following holds:

(a) $C_S(g_1) = C_S(g_2)$ or (b) $(r, |\mathbb{K}|, \dim_{\mathbb{K}} V) = (2,3,2), (2,5,2)$ or $(3,4,3)$.

Suppose first that Case (a) holds. Then by Proposition 2.2.2, we get either $C_G(g_1) = C_G(g_2)$ which as above implies $C_G(\overline{g}_1) = C_G(\overline{g}_2)$, or we have $r = 2, |\mathbb{K}| = 3, \dim_{\mathbb{K}} V = 2$ which again implies that $C_G(\overline{g}_1) = C_G(\overline{g}_2)$ by Lemma 1.3.2.

Now suppose that $C_S(g_1) \neq C_S(g_2)$ and let us look at the cases listed in (b). By Lemma 1.3.2 $r = 2, |\mathbb{K}| = 3$ is not possible. By Lemma 1.3.3, $r = 2$, $|\mathbb{K}| = 5$ gives (c). Finally note that g_j's have three different eigenvalues in the case $r = 3$, $|\mathbb{K}| = 4$, $\dim_{\mathbb{K}} V = 3$ and Lemma 1.3.4 gives (d).

Case 4. For $j = 1, 2$, put $\mathbb{E}_j = \mathbb{K}[g_j] \subseteq \mathrm{End}_{\mathbb{K}}(V)$. Since $|kg_j| \neq r$ for all $k \in \mathbb{K}$, $\mathbb{E}_j$ is a field, V is a vector space over $\mathbb{E}_j$, and $\dim_{\mathbb{K}} \mathbb{E}_j = r$ by Lemma 1.1.15. Note that

$$C_S(g_j) = S \cap \mathrm{GL}_{\mathbb{E}_j}(V) \subseteq C_S(\overline{g}_j) \subseteq S \cap \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_j}(V). \tag{2.11}$$

Write $V = \bigoplus_{i=1}^{d_j} \mathbb{E}_j$ where $d_j := \dim_{\mathbb{E}_j} V$. Use the notation $N_j := N_{\mathbb{E}_j}^{\mathbb{K}}$ and let $e_j \in \mathbb{E}_j$. Then by Lemma 1.2.10(b) we have

$$\det_V^{\mathbb{K}}(e_j) = \left[\det_{\mathbb{E}_j}^{\mathbb{K}}(e_j)\right]^{\dim_{\mathbb{E}_j} V} = \left[N_j(\det_{\mathbb{E}_j}^{\mathbb{E}_j}(e_j))\right]^{\dim_{\mathbb{E}_j} V} = [N_j(e_j)]^{\dim_{\mathbb{E}_j} V}. \tag{2.12}$$

Thus whenever $N_j(e_j) = 1$, $e_j \in \mathrm{SL}_{\mathbb{K}}(V)$ by (2.12). Also note that e_j commutes with g_j by definition of $\mathbb{E}_j$, hence $\widetilde{\mathbb{E}}_j \subseteq C_S(g_j)$ where $\widetilde{\mathbb{E}}_j := \{e_j \in \mathbb{E}_j \mid N_j(e_j) = 1\}$. Moreover, we have $\mathrm{GL}_{\mathbb{E}_j}(V) \cap \mathrm{SL}_{\mathbb{K}}(V) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_{3-j}}(V)$ for $j = 1, 2$. So by Proposition 1.2.16 one of the following two situations holds:

(1) $\mathbb{E}_1 = \mathbb{E}_2$. This gives $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$ by Lemma 1.2.3 and thus (a) holds.

(2) $r = 2$, $|\mathbb{K}| = 3$, $\dim_{\mathbb{K}} V = 2$. In this case part (d) holds, see Lemma 1.3.5.

Case 5. In this case, $|g_1| = r$ and $|g_2| \neq r$. Then $\mathbb{E}_2 = \mathbb{K}[g_2]$ is a field and $\dim_{\mathbb{K}} \mathbb{E}_2 = r$ by Lemma 1.1.15. Moreover, we have

$$\mathrm{SL}_{\mathbb{E}_2}(V) \subseteq C_S(g_2) = \mathrm{GL}_{\mathbb{E}_2}(V) \cap \mathrm{SL}_{\mathbb{K}}(V) \subseteq C_S(\overline{g}_2) \subseteq \Gamma_{\mathbb{K}} \mathrm{GL}_{\mathbb{E}_2}(V).$$

As for g_1, we have either

$$C_S(\overline{g}_1) = \mathrm{SL}_{\mathbb{K}}(V) \cap \bigtimes_{i=1}^{s_1} \mathrm{GL}_{\mathbb{E}_{i1}}(V_{i1}) \quad \text{or} \tag{2.13a}$$

$$C_S(\overline{g}_1) = \mathrm{SL}_{\mathbb{K}}(V) \cap \left(\left[\bigtimes_{i=1}^{r} \mathrm{GL}_{\mathbb{K}}(V_{i1})\right]\langle h_1 \rangle\right). \tag{2.13b}$$

by Lemma 1.1.10.

Claim(1) V is an irreducible $\mathbb{K}C_S(g_2)$-module:

If $\dim_{\mathbb{E}_2} V \neq 1$, then V is a simple $\mathbb{K}\,\mathrm{SL}_{\mathbb{E}_2}(V)$-module, and the claim follows easily. If $\dim_{\mathbb{E}_2} V = 1$, then $C_S(g_2) = \{e \in \mathbb{E}_2 \mid N(e) = 1\}$ where $N := N_{\mathbb{E}_2}^{\mathbb{K}}$. Let $\mathbb{F} := \mathbb{K}[e \in \mathbb{E}_2 \mid N(e) = 1]$. In order to prove the claim it suffices to show that $\mathbb{F} = \mathbb{E}_2$. By Lemma 1.2.14, there is $e \in \mathbb{E}_2$ such that $e^r \notin \mathbb{K}$. Let $\alpha := e^r/N(e)$. Since $[\mathbb{E}_2 : \mathbb{K}] = r$, we have $\mathbb{E}_2 = \mathbb{K}(\alpha)$. On the other hand, $\alpha \in \mathbb{F}$, thus $\mathbb{K}(\alpha) \leq \mathbb{F}$, and $\mathbb{F} = \mathbb{E}_2$, as required.

We now deduce, using both (2.8) and the above claim, that V is an irreducible $\mathbb{K}C_S(\overline{g}_1)$-module. Hence $s_1 = 1$ or (2.13b) must hold.

Claim(2) $s_1 \neq 1$ and hence (2.13b) holds:

Suppose to the contrary that $s_1 = 1$. Then $V = V_{11}$ and $\mathbb{E}_{11} = \mathbb{K}[g_1]$ is a field. Therefore $\mathrm{SL}_{\mathbb{E}_{11}}(V) \subseteq C_S(\overline{g}_1) \subseteq \Gamma_{\mathbb{K}}\,\mathrm{GL}_{\mathbb{E}_{11}}(V)$ by Lemma 1.1.4 and so the hypothesis of Proposition 1.2.16 are satisfied. Hence one of the following holds:

(1) $\mathbb{E}_{11} = \mathbb{E}_2$. Then $\langle \overline{g}_1 \rangle = \langle \overline{g}_2 \rangle$ by Lemma 1.2.3. However, this implies $g_2 k$ has order r for some $k \in \mathbb{K}^\sharp$, a contradiction to the choice of g_2.

(2) $r = 2$, $|\mathbb{K}| = 3$. Then $|g_1| = 2$ implies $g_1 = -1 \in \mathbb{K}^\sharp$, contradiction.

Claim(3) We have $\dim_{\mathbb{E}_2} V = 1$ and $\dim_{\mathbb{K}} V_{i1} = 1$ for all $1 \leq i \leq r$:

If $\dim_{\mathbb{E}_2} V \neq 1$, then $1 \neq \mathrm{SL}_{\mathbb{E}_2}(V) \subseteq C_S(\overline{g}_2)$. So $C_S(\overline{g}_2)$ is transitive (and primitive) on V. But $C_S(\overline{g}_1)$ is not primitive, a contradiction. Thus $\dim_{\mathbb{E}_2} V = 1$. Now $\dim_{\mathbb{K}} \mathbb{E}_2 = r$ implies that $\dim_{\mathbb{K}} V = r$ and hence $\dim_{\mathbb{K}} V_{i1} = 1$ for all i. Therefore,

$$C_S(\overline{g}_1) = \mathrm{SL}_{\mathbb{K}}(V) \cap [\bigtimes_{i=1}^{r} \mathbb{K}^\sharp\,]\langle h_1 \rangle \quad \text{and} \quad C_S(\overline{g}_2) = \mathrm{SL}_{\mathbb{K}}(V) \cap \mathbb{E}_2^\sharp\,\mathrm{Aut}_{\mathbb{K}}\,\mathbb{E}_2.$$

Claim(4) $\mathbb{K}$ *is finite*:

Let us take $y = (\lambda, \lambda^{-1}, 1, \ldots, 1) \in C_S(\overline{g}_1) = C_S(\overline{g}_2)$ where λ is any nonzero element in $\mathbb{K}$. Since $|C_S(\overline{g}_2)/\widetilde{\mathbb{E}}_2|$ divides $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)|$ and $|\mathrm{Aut}_{\mathbb{K}}(\mathbb{E}_2)| = 1$ or r, we see that $|C_S(\overline{g}_2)/\widetilde{\mathbb{E}}_2||r$ and hence $y^r \in \widetilde{\mathbb{E}}_2$. Note that if $a \in \widetilde{\mathbb{E}}_2$ has an eigenvalue in $\mathbb{K}$, then $av = kv$ for some $0 \neq v \in V = \mathbb{E}_2$ and $k \in \mathbb{K}$, giving us $a = k$. Therefore, since y^r has an eigenvalue in $\mathbb{K}$, we get $y^r = (\lambda^r, \lambda^r, \ldots, \lambda^r)$. That is, if $r = 2$ then $\lambda^r = \lambda^{-r}$ and if $r > 2$ then $\lambda^r = 1$. In any case, $\mathbb{K}$ is finite.

As our final step let $q := |\mathbb{K}|$. The determinant map $\det : C_G(\overline{g}_1) \longrightarrow \mathbb{K}^\sharp$ is onto with $\mathrm{Ker}(\det) = C_S(\overline{g}_1)$. Also $|C_G(\overline{g}_1)| = r|\mathbb{K}^\sharp|^r = r(q-1)^r$. Hence $|C_S(\overline{g}_1)| = r(q-1)^r/q-1$. On the other hand, $|\mathbb{E}_2| = q^r$ and $|C_G(\overline{g}_2)| = |\mathbb{E}_2^\sharp|r$. Furthermore, the norm map $N : \mathbb{E}_2^\sharp \longrightarrow \mathbb{K}^\sharp$ is onto since both fields are finite and image of N is a cyclic group of order $q-1$. Thus $|C_S(\overline{g}_2)| = (q^r-1)r/q-1$. But $(q-1)^r < q^r - 1$ implies that $C_S(\overline{g}_1) \neq C_S(\overline{g}_2)$, a contradiction. Hence Case (5) does not occur.

Chapter 3

Centralizers in $\mathrm{Alt}(\Omega)$

3.1 Centralizers in $\mathrm{Alt}(n)$

Throughout this section assume the following: $G = \mathrm{Alt}(\Omega)$ where Ω is a finite set of size n and x and y are elements of G of prime order p such that $\langle x \rangle \neq \langle y \rangle$. Our aim is to prove a theorem which lists all possibilities for x, y, and n so that x and y have the same centralizer in G.

Let

$$x = x_1 x_2 \cdots x_r \quad \text{and} \quad y = y_1 y_2 \cdots y_s$$

be the decompositions of x and y into the product of disjoint p-cycles where

$$x_i = (a_{i1}, a_{i2}, \ldots, a_{ip}) \quad \text{and} \quad y_j = (b_{j1}, b_{j2}, \ldots, b_{jp})$$

for all $1 \leq i \leq r$ and $1 \leq j \leq s$.

Theorem 3.1.1 *Let x, y, and G be as above. Then the cases where $C_G(x) = C_G(y)$ are exactly the following:*

(a) *p is odd, $n = 2p$ or $2p+1$, and $x = x_1 x_2$, $y = x_1^k x_2^l$ with k, $l \in \mathbb{Z}$, $1 \leq k \neq l < p$.*

(b) $p = 3,\ n = 6$ *and* $x = x_1 x_2,\ y = x_1^k$ *or vice versa where* $1 \leq k < p$.

(c) $p = 3,\ n = 6$ *and* $x = x_1,\ y = y_1$ *with* $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \emptyset$.

(d) $p = 2,\ n = 4$ *or* 5 *and* $\mathrm{supp}(x) = \mathrm{supp}(y)$ *has size* 4.

For the proof of this theorem, the following two lemmas will be needed.

Lemma 3.1.2 $C_G(x)$ *does not act transitively on* $\mathrm{supp}(x)$ *if and only if* p *is odd,* $|\mathrm{supp}(x)| = 2p$, *and* $n = 2p$ *or* $2p + 1$.

Proof: Note that $C_G(x)$ acts on $\mathrm{supp}(x)$.

Case 1. *Suppose* $r = 1$.

Then $x = x_1$ and p is necessarily odd since $x \in \mathrm{Alt}(n)$. Clearly, $C_G(x)$ contains the subgroup $\langle x_1 \rangle$ and hence acts transitively on $\mathrm{supp}(x)$.

We may now assume that $r \geq 2$. Let α and β be in $\mathrm{supp}(x)$. If they belong to the same orbit of x, then there exists an element $\sigma \in \langle x \rangle$ which moves α to β. Hence it is enough to consider only the case where α and β are in two different orbits of x. Without loss of generality, assume that $\alpha = a_{11}$ and $\beta = a_{21}$.

Case 2. *Suppose* $r \geq 3$.

Let $\sigma = (a_{11}, a_{21}, a_{31})(a_{12}, a_{22}, a_{32}) \ldots (a_{1p}, a_{2p}, a_{3p})$. It is evident that σ is an even permutation, commutes with x, and $\sigma(a_{11}) = a_{21}$. This proves that $C_G(x)$ acts transitively on $\mathrm{supp}(x)$ when $r \geq 3$.

Case 3. *Suppose* $r = 2$.

Let $\mu := (a_{11}, a_{21})(a_{12}, a_{22}) \cdots (a_{1p}, a_{2p})$. If $n \neq 2p, 2p + 1$, then define σ by

$$\sigma = \begin{cases} \mu & \text{if } p \text{ is even} \\ \mu\pi & \text{if } p \text{ is odd} \end{cases}$$

where π is a transposition whose support is contained in $\Omega \setminus \mathrm{supp}(x)$. Such a transposition exists since $n > 2p+1$. Then $\sigma \in C_G(x)$ and σ sends a_{11} to a_{21}, which proves the transitivity of $C_G(x)$ on $\mathrm{supp}(x)$ in this case.

Finally, if $n = 2p$ or $2p+1$, then we have $C_{\mathrm{Sym}(n)}(x) = \langle x_1, x_2, \tau \rangle$ where $\tau := (a_{11}, a_{21}) \cdots (a_{1p}, a_{2p})$. If p is even (so $n = 4$ or 5), then $\tau \in \mathrm{Alt}(n)$ and thus $C_G(x)$ is transitive on $\mathrm{supp}(x)$. On the other hand, if p is odd then $C_G(x) = \langle x_1, x_2 \rangle$. Hence $C_G(x)$ does not act transitively on $\mathrm{supp}(x)$.

Lemma 3.1.3 *Let $1 \leq i \leq r$ and $1 \leq j \leq s$ and let p be an odd prime. Put $x = x_1 x_2 \cdots x_r$ and $y = y_1 y_2 \cdots y_s$ be as above with $C_G(x) = C_G(y)$. Then either $\mathrm{supp}(x_i) = \mathrm{supp}(y_j)$ or $\mathrm{supp}(x_i) \cap \mathrm{supp}(y_j) = \emptyset$. Furthermore, if $\mathrm{supp}(x_i) = \mathrm{supp}(y_j)$ then $y_j = x_i^k$ for some $0 < k < p$.*

Proof: Since p is odd, x_i is an even permutation and $x_i \in C_G(x) = C_G(y)$. Thus $\mathrm{supp}(x_i)$ is y-invariant and so it is a union of orbits of y. Now the first part of the lemma follows from the facts that $|\mathrm{supp}(x_i)| = p$ and orbits of y have length 1 or p. For the second part, note that $[y_j, y] = 1$ and hence $y_j \in C_G(y) = C_G(x)$. Then $[y_j, x_i] = 1$ as $\mathrm{supp}(x_i) = \mathrm{supp}(y_j)$. Since $y_j \in C_{\mathrm{Sym}(\mathrm{supp}(x_i))}(x_i) = \langle x_i \rangle$, we get $y_j = x_i^k$ for some $0 < k < p$.

Proof of Theorem 3.1.1. We split the proof into two cases:

Case 1. $C_G(z)$ does not act transitively on $\mathrm{supp}(z)$ for $z = x$ or $z = y$.

Without loss of generality, assume that $C_G(x)$ does not act transitively on $\mathrm{supp}(x)$. Then by Lemma 3.1.2, $|\mathrm{supp}(x)| = 2p$ where p is odd and $n = 2p$ or $2p+1$. Thus, $\mathrm{supp}(x) \cap \mathrm{supp}(y) \neq \emptyset$. By Lemma 3.1.3, $y = x_1^{k_1} x_2^{k_2}$ for some $0 \leq k_i < p$, $i = 1, 2$. First assume that both k_1 and k_2 are nonzero. If $k := k_1 = k_2$, then $y = x^k$, a contradiction to $\langle x \rangle \neq \langle y \rangle$. Thus $k_1 \neq k_2$ which gives part (a) of the theorem. If

one of the k_i is zero, say k_2, then $y = x_1^{k_1}$ where $1 \leq k_1 < p$. Note that $p \geq 5$ is not possible since otherwise we can construct an element $1 \neq \sigma \in \mathrm{Alt}(n)$ such that $\mathrm{supp}(\sigma) \subsetneq \mathrm{supp}(x_2)$. Then $\sigma \in C_G(y) \setminus C_G(x)$, a contradiction. Therefore $p = 3$ and hence $n = 6$ or 7. When $n = 7$, we can define $\sigma := (a_{21}, a_{22})(a_{23}, b)$ where $b \in \Omega \setminus \mathrm{supp}(x)$. Then σ commutes with y but not with x, a contradiction. Hence $n = 6$ and (b) is attained.

Case 2. $C_G(z)$ acts transitively on $\mathrm{supp}(z)$ where $z \in \{x, y\}$.

Since $\mathrm{supp}(x)$ is an orbit of $C_G(x)$, $\mathrm{supp}(y)$ is an orbit of $C_G(y)$, and $C_G(x) = C_G(y)$, we have $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \emptyset$ or $\mathrm{supp}(x) = \mathrm{supp}(y)$.

Case 2a. $\mathrm{supp}(x) \cap \mathrm{supp}(y) = \emptyset$:

In this case, $x \in \mathrm{Alt}(\Omega \setminus \mathrm{supp}(y))$. Moreover, $\mathrm{Alt}(\Omega \setminus \mathrm{supp}(y)) \subseteq C_G(y) = C_G(x)$. So $1 \neq x \in Z(\mathrm{Alt}(\Omega \setminus \mathrm{supp}(y)))$ and hence $|\Omega \setminus \mathrm{supp}(y)| = 3$. This implies $|\mathrm{supp}(x)| = 3$. We use the same argument for y instead of x and get $|\mathrm{supp}(y)| = 3$, giving us (c).

Case 2b. $\mathrm{supp}(x) = \mathrm{supp}(y)$:

Suppose to the contrary that p is odd. We write y as $y = x_1^{k_1} x_2^{k_2} \ldots x_r^{k_r}$ for some $0 < k_i < p$ by Lemma 3.1.3. If all the k_j's are equal then $y = x^k$, a contradiction. Thus, if necessary by replacing y with some power of y and re-ordering x_i's we choose the notation as $y = x_1 x_2^{k_2} \ldots x_r^{k_r}$ with $k_2 \neq 1$. If $r \geq 3$, the permutation $(a_{11}, a_{21}, a_{31})(a_{12}, a_{22}, a_{32}) \ldots (a_{1p}, a_{2p}, a_{3p})$ is in $C_G(x) \setminus C_G(y)$, a contradiction. Therefore $r = 2$. By Lemma 3.1.2, $n > 2p + 1$. Now the element $\sigma := (a_{11}, a_{21})(a_{12}, a_{22}) \cdots (a_{1p}, a_{2p})\pi$, where π is a transposition whose support is in $\Omega \setminus \mathrm{supp}(x)$ satisfies $[\sigma, x] = 1$ and $[\sigma, y] \neq 1$, a final contradiction. So $p = 2$.

Next we will show that $r = 2$. Assume for a contradiction that $r \geq 3$. Let $1 \leq i \leq r$ be arbitrary and pick j and k such that $|\{i, j, k\}| = 3$ where $1 \leq j, k \leq r$. Since $x_i\, x_j \in C_G(x) = C_G(y)$, $\mathrm{supp}(x_i\, x_j)$ is y-invariant. Similarly, $\mathrm{supp}(x_i\, x_k)$ is y-invariant. Then their intersection, $\mathrm{supp}(x_i\, x_j) \cap \mathrm{supp}(x_i\, x_k) = \mathrm{supp}(x_i)$, is y-invariant as well. That is, $\mathrm{supp}(x_i)$ is an orbit of y. As i is arbitrary, we get $x = y$ which is a contradiction. Thus $r = 2$.

Now $p = 2$ and $r = 2$ imply that $\mathrm{supp}(x) = \mathrm{supp}(y)$ has size 4. Finally, the assumption $C_G(x) = C_G(y)$ forces $n \leq 5$. To see this, without loss of generality let $x = (a, b)(c, d)$ and $y = (a, c)(b, d)$. If $n \geq 6$, take $e, f \in \Omega \setminus \mathrm{supp}(x)$ and consider $\sigma = (b, d)(e, f)$. Clearly, σ commutes with y but not with x, a contradiction. This gives (d) and completes the proof of the Theorem.

Chapter 4

On Abelian Centralizer in Locally Finite Simple Groups

In this chapter, we show that the centralizer of an element of prime order in a group of alternating type as well as in a nonlinear finitary group is non-abelian.

4.1 The Non-regular Alternating Case

Recall the definition of regular and non-regular alternating groups from the Introduction.

Lemma 4.1.1 *Let G be a LFS-group of alternating type and $C_p \times C_p \cong Z \leq G$ a regular subgroup of G. Then $C_G(z) \neq C_G(Z)$ for all $1 \neq z \in Z$.*

Proof: Since Z is regular, there is an element $(H, \Omega) \in \mathcal{K}$ such that Z has at least t regular orbits on Ω for all Kegel covers $\mathcal{K}$ and for all non-negative integers t by [4, Theorem 1.2]. Choosing $t \geq 5^3 p^3$ implies $C_H(z) \neq C_H(Z)$ for some $1 \neq z \in Z$ by [6, Theorem 6.1]. In fact, the proof of [6, Theorem 6.1] gives a stronger result; namely, $C_H(z) \neq C_H(Z)$ *for all* $1 \neq z \in Z$. In that proof the assumption "for all $1 \neq z \in Z$" is used only in one place, the forth line before the end of the proof.

Instead, one could have said "for some $1 \neq z \in Z$" because the lemma referred to only requires the existence of some such element. Thus $C_G(z) \neq C_G(Z)$ for all $1 \neq z \in Z$.

Proposition 4.1.2 *Let G be a regular alternating group. Then $C_G(a) \neq C_G(b)$ for all $a, b \in G$ with $|a| = |b| = p$ and $\langle a \rangle \neq \langle b \rangle$ where p is a prime.*

Proof: Assume it is false. Let $a, b \in G$ be of order p such that $\langle a \rangle \neq \langle b \rangle$ and $C_G(a) = C_G(b)$. Put $Z := \langle a, b \rangle$. Since G is regular, $Z \cong C_p \times C_p$ is regular and $C_G(Z) = C_G(a) \cap C_G(b) = C_G(a) = C_G(b)$, a contradiction to the above lemma.

For the remaining of the section more definitions and terminology will be needed. Let $(H, \Omega) \in \mathcal{A}$. Then, by [14, Lemma 2.8], there exists a unique minimal (sub)normal supplement R to $C_H(\Omega)$ in H. That is, R is a normal subgroup of H and minimal with respect to $H = RC_H(\Omega)$. For $\omega \in \Omega$, we denote the minimal normal supplement to $C_H(\Omega)$ in $C_H(\omega)$ by R_ω.

Definition 4.1.3 *Let Λ be an H-set and Σ be an orbit for H on Λ. Then*

(a) *Σ is called Ω-essential if $C_H(\Sigma) \leq C_H(\Omega)$.*

(b) *Σ is called Ω-natural if Σ and Ω are isomorphic as H-sets.*

(c) *Σ is called Ω-block-natural if for some H-invariant partition Δ of Σ, Δ is Ω-natural and $N_H(D) = C_H(D)C_H(\Omega)$ for all $D \in \Delta$.*

(d) *If all the Ω-essential orbits on Λ are Ω-block-natural, then Λ is said to be Ω-block-diagonal.*

Remark: (a) The condition $N_H(D) = C_H(D)C_H(\Omega)$ in the above definition is equivalent to $C_H(D) \not\leq C_H(\Omega)$.

(b) Σ is an Ω-essential orbit for H on $\Lambda \Leftrightarrow R$ acts non-trivially on Σ.

Proof: (a) Obvious since $N_H(D)/C_H(\Omega) \cong \mathrm{Alt}(|\Omega| - 1)$ is simple.

(b) Assume that R acts non-trivially on Σ. Then $R \not\leq C_H(\Sigma)$ and hence $C_H(\Sigma)C_H(\Omega) \neq H$. Since $H/C_H(\Omega)$ is simple, $C_H(\Sigma) \leq C_H(\Omega)$. For the converse, assume that Σ is an Ω-essential orbit. If $R \leq C_H(\Sigma) \leq C_H(\Omega)$, then $H = C_H(\Omega)$, a contradiction. So $R \not\leq C_H(\Sigma)$.

Let G be a group of alternating type. For $A \in \mathcal{A}$, we define H_A and Ω_A by $A = (H_A, \Omega_A)$. Let $\mathcal{D}$ be a subset of $\mathcal{A}$. Then $\mathcal{D}$ is called a Kegel cover for G if $\{(H, C_H(\Omega)) \mid (H, \Omega) \in \mathcal{D}\}$ is a Kegel cover for G. For any finite subgroup F of G, we define $\mathcal{D}(F) := \{(H, \Omega) \in \mathcal{D} \mid F \leq H \text{ and } C_F(\Omega) = 1\}$.

Remark: Let A and E be finite groups with E perfect and acting transitively on a finite set Ω. Denote the base group of $A \wr_\Omega E$ by A^Ω and put $(A^\Omega)_\circ := A^\Omega \cap (A \wr_\Omega E)'$. Then $(A \wr_\Omega E)' = [A^\Omega E, A^\Omega E] = (A^\Omega)'[A^\Omega, E]\, E$. Furthermore,

$$(A^\Omega)_\circ = (A^\Omega)'\,[A^\Omega, E] = \Big\{(a_\omega)_{\omega\in\Omega} \in A^\Omega \;\Big|\; \prod_{\omega\in\Omega} a_\omega \in A'\Big\}. \tag{4.1}$$

The first equality in (4.1) is clear. For the second equality, we will first assume that A is abelian and show that $[A^\Omega, E] = \{(a_\omega)_{\omega\in\Omega} \in A^\Omega \mid \prod_{\omega\in\Omega} a_\omega = 1\}$:

$(\subseteq)$ is obvious since E permutes the coordinates of the elements of the base group and A is abelian. For the converse inclusion, without loss of generality, we put $\Omega = \{1, 2, \ldots, n\}$ and let $a = (a_i)_{i\in\Omega} \in A^\Omega$ such that $\prod_{i=1}^n a_i = 1$. We need show that $a \in [A^\Omega, E]$. Since E is transitive, there exists $e_i \in E$ such that $1^{e_i} = i$ for $i \in \Omega$. For each $1 \neq k \in \Omega$ define $h(k) \in A^\Omega$ by $h(k) = (a_k, 1, 1, \ldots, 1)$. Then $[h(k), e_k] = (a_k^{-1}, 1, \ldots, 1, a_k, 1, \ldots, 1)$ where a_k is in the k^{th} position.

Hence

$$\prod_{k=2}^{n}[h(k), e_k] = (\prod_{k=2}^{n} a_k^{-1}, a_2, \ldots, a_n)$$

which is equal to a since $\prod_{i=1}^{n} a_i = 1$. Thus, $a \in [A^\Omega, E]$.

For the general case, since $A^\Omega/(A^\Omega)' = (A/A')^\Omega$ is abelian, we get

$$(A')^\Omega[A^\Omega, E]/(A')^\Omega = [(A/A')^\Omega, E] = \Big\{(a_i A')_{i\in\Omega} \mid \prod_{i=1}^{n} a_i A' = A'\Big\}.$$

This implies $(A')^\Omega[A^\Omega, E] = \{(a_i)_{i\in\Omega} \mid \prod_{i\in\Omega} a_i \in A'\}$, as claimed.

We now quote a theorem proven in [4, Theorem 4.3].

Theorem 4.1.4 ([4]) *Let $(H, \Omega) \in \mathcal{A}$ and suppose that H is faithful and Ω-block-diagonal on some set. Let R be the minimal normal supplement to $C_H(\Omega)$ in H. Let $\omega \in \Omega$ and put $K = C_R(\omega)/R_\omega$. Then $R \cong (K \wr_\Omega \mathrm{Alt}(\Omega))'$.*

Let us denote the isomorphism defined in the proof of the above theorem by $\phi : R \xrightarrow{\cong} (K \wr_\Omega \mathrm{Alt}(\Omega))'$. We will show that it can be extended to H as follows:

Lemma 4.1.5 *Let $H, R, \omega, R_\omega, \Omega$ and K be as above. Put $L := L_\omega = C_H(\omega)/R_\omega$ and $D := \{(d_\omega)_{\omega\in\Omega} \in L^\Omega \mid d_\omega K = d_{\omega'} K$ for all $\omega, \omega' \in \Omega\}$. Then there exists a monomorphism $\theta : H \longrightarrow L \wr_\Omega \mathrm{Alt}(\Omega)$ such that $\theta_{|R} = \phi$. Moreover,*

$$(K^\Omega)_\circ \leq K^\Omega \cap \theta(H) \leq K^\Omega \trianglelefteq \theta(C_H(\Omega))K^\Omega = D \trianglelefteq \theta(H)K^\Omega = D\,\mathrm{Alt}(\Omega)$$

with $K^\Omega/(K^\Omega)_\circ \cong K/K'$ and $D/K^\Omega \cong L/K$.

Proof: Let us first show that $R_\omega^h = R_{\omega^h}$ for all $h \in H$ and $\omega \in \Omega$. By definition of R_ω, $C_H(\omega) = R_\omega C_H(\Omega)$ and conjugating it by h gives $C_H(\omega^h) = R_\omega^h C_H(\Omega^h) = R_\omega^h C_H(\Omega)$. Thus $R_{\omega^h} \leq R_\omega^h$ by definition of R_{ω^h}. In

a similar way, we have $R_\omega \leq R_{\omega^h}^{h^{-1}}$ and so $R_\omega^h = R_{\omega^h}$. Next we will show that $L_\omega \cong L_{\omega'}$ for any $\omega, \omega' \in \Omega$. Since $H/C_H(\Omega) \cong \mathrm{Alt}(\Omega)$ and $H = RC_H(\Omega)$, H and hence R acts transitively on Ω. So choose $r \in R$ such that $\omega^r = \omega'$ and define $\vartheta : C_H(\omega) \to C_H(\omega')/R_{\omega'}$ by $\vartheta(h) = r^{-1}hrR_{\omega'}$. One can easily check that it is an epimorphism with kernel R_ω, giving the isomorphism $L_\omega \cong L_{\omega'}$.

Definition of θ and the proof that it is a monomorphism will be similar to that of the one given in [4]. But they are included below as well because the explicit definition of θ and some further observations will be needed later on.

Without loss of generality, assume $\Omega = \{1, 2, \ldots, n\}$ and $w = 1$. For $i \in \Omega$, pick $r_i \in R$ such that $1^{r_i} = i$. Since $r_i h r_{ih}^{-1} \in C_H(1)$ for all $h \in H$ and $i \in \Omega$, we obtain a map

$$\theta : H \to L \wr_\Omega \mathrm{Alt}(\Omega) : h \to ((r_i h r_{ih}^{-1} R_1)_{i\in\Omega}, \pi(h))$$

where $\pi : H \to \mathrm{Alt}(\Omega)$ is the onto homomorphism arising from the action of H on Ω. θ is a homomorphism since for any $h, t \in H$ we have

$$\begin{aligned}
\theta(h)\theta(t) &= ((r_i h r_{ih}^{-1} R_1)_{i\in\Omega}, \pi(h))((r_i t r_{it}^{-1} R_1)_{i\in\Omega}, \pi(t)) \\
&= ((r_i h r_{ih}^{-1} r_{ih} t r_{iht}^{-1} R_1)_{i\in\Omega}, \pi(h)\pi(t)) \\
&= ((r_i h t r_{iht}^{-1} R_1)_{i\in\Omega}, \pi(ht)) \\
&= \theta(ht).
\end{aligned}$$

Now let $h \in H$ such that $\theta(h) = 1$. Then $\pi(h) = 1$, that is, $\pi(h)$ acts trivially on Ω. Hence $\theta(h) = ((r_i h r_i^{-1} R_1)_{i\in\Omega}, 1)$ and so $r_i h r_i^{-1} \in R_1$ and $h \in R_1^{r_i} = R_i$ for all i. By assumption H acts faithfully and Ω-block-diagonally on some set, say Λ, and $\cap_{i\in\Omega} R_i$ acts trivially on Λ by [4, 4.1(b)]. Thus $h = 1$ and θ is one-to-one.

Note that $(K^\Omega)_\circ = K^\Omega \cap \theta(R) \leq K^\Omega \cap \theta(H)$. To show that $K^\Omega/(K^\Omega)_\circ \cong K/K'$, define $\psi : K^\Omega \to K/K'$ by $\psi : (k_j)_{j\in\Omega} \to (\prod_{j\in\Omega} k_j)K'$ and observe that it is an epimorphism and the kernel consists of elements $(k_j)_{j\in\Omega}$ such that $\prod_{j\in\Omega} k_j \in K'$. Then $\mathrm{Ker}(\psi) = (K^\Omega)_\circ$ by (4.1).

Since $r_j, r_k \in R$ and $R \trianglelefteq H$, we have $(r_j h r_{jh}^{-1})^{-1}(r_k h r_{kh}^{-1}) \in C_R(1)$ for any $j,k \in \Omega$. This implies $r_j h r_{jh}^{-1} K = r_k h r_{kh}^{-1} K$ for $j,k \in \Omega$ and from this it is immediate that $\theta(C_H(\Omega)) \subseteq D$. Obviously, $K^\Omega \leq D$ and hence $\theta(C_H(\Omega))K^\Omega \subseteq D$. In fact, we will show that $\theta(C_H(\Omega))K^\Omega = D$. For this, let $d = (d_i R_1)_{i\in\Omega} \in D$. So $d_i \in C_H(1)$ and $d_i C_R(1) = d_j C_R(1)$ for all $i,j \in \Omega$. Since $C_H(1) = R_1 C_H(\Omega)$, there exist $t \in R_1$ and $h \in C_H(\Omega)$ such that $d_1 = th$. Recall that $\theta(h) = (r_i h r_i^{-1} R_1)_{i\in\Omega}$ by definition. Putting $s = (s_i R_1) = d\theta(h)^{-1}$, we have $s_i = d_i(r_i h^{-1} r_i^{-1}) = d_i r_i (d_1^{-1} t) r_i^{-1} = (d_i r_i d_i^{-1})(d_i d_1^{-1})(t r_i^{-1})$. Note that $d_i^{-1} d_1 \in C_R(1)$ and since $R \trianglelefteq H$ and $d_i \in H$, we also have $d_i r_i d_i^{-1} \in R$, thus $s_i \in R$. In fact, $s_i \in C_R(1)$ because $s_i = d_i(r_i h^{-1} r_i^{-1})$ and both d_i and $r_i h^{-1} r_i^{-1}$ fixes 1. Therefore, $s \in K^\Omega$ and hence $d = s\theta(h) \in K^\Omega \theta(C_H(\Omega))$ which gives $D \subseteq \theta(C_H(\Omega))K^\Omega$.

Next let us consider the map $\psi : D \to L/K$ defined by $\psi : (d_j)_{j\in\Omega} \to d_1 K$. It can be easily checked that ψ is an onto homomorphism and if $(d_j) \in \mathrm{Ker}(\psi)$, then $d_1 K = K$, that is, $d_1 \in K$. Thus $d_j \in K$ for all $j \in \Omega$, giving $\mathrm{Ker}(\psi) = K^\Omega$ and $D/K^\Omega \cong L/K$. Finally, $\theta(R) = (K \wr_\Omega \mathrm{Alt}(\Omega))' = (K^\Omega)_\circ \mathrm{Alt}(\Omega)$ and $H = C_H(\Omega)R$ imply that $\theta(H) = \theta(C_H(\Omega)\theta(R)) = \theta(C_H(\Omega))(K^\Omega)_\circ \mathrm{Alt}(\Omega)$. Multiplying this by K^Ω and using $(K^\Omega)_\circ \leq K^\Omega$, we obtain $\theta(H)K^\Omega = D\,\mathrm{Alt}(\Omega)$, completing the proof.

Put $B := \phi^{-1}((K^{\Omega})_{\circ})$ and note that $g \in C_R(\Omega)$ if and only if $\pi(g) = 1$ if and only if $\phi(g) = ((r_i g r_{ig}^{-1} R_1)_{i\in\Omega}, 1) \in (K^{\Omega})_{\circ}$. In other words, $B = C_R(\Omega)$ and hence $B = R \cap C_H(\Omega) \trianglelefteq H$. Without loss of generality, we let $\Omega = \{1, 2, \ldots, n\}$ for the remaining of the section. Moreover, whenever convenient, we shall identity the group with its image under the isomorphism ϕ. In particular, for the next lemma we identify R with $(K \wr_{\Omega} \mathrm{Alt}(\Omega))'$ and B with $(K^{\Omega})_{\circ}$.

Lemma 4.1.6 *Let* $R^* := \{(g_i)\pi \in R \mid g_1 = 1$ *and* $1^{\pi} = 1\}$. *Then* $R_1 = R^*$.

Proof: It is straight forward to check that R^* is a group.

Step 1. $R_1 \leq R^*$:

It is enough to show $R^* \trianglelefteq C_H(1)$ and $C_H(1) = R^* C_H(\Omega)$, since then $R_1 \leq R^*$ follows from the minimality of R_1. For $R^* \trianglelefteq C_H(1)$; let $u \in C_H(1)$ and $y = (y_i)\pi \in R^*$. Since $y_1 = 1$, $1^{\pi} = 1$, and $\phi(u) = (u_i)\sigma$ where $u_i = r_i u r_{iu}^{-1} R_1$ with $1^{\sigma} = 1$, we get $((y_i)\pi)^{\phi(u)} = \sigma^{-1}(u_i)^{-1}(y_i)\pi(u_i)\sigma = [(u_i)^{-1}(y_i)(u_i)^{\pi^{-1}}]^{\sigma}\sigma^{-1}\pi\sigma$. The first coordinate of this element is $(r_1 u r_1^{-1})^{-1} \cdot 1 \cdot r_1 u r_1^{-1} R_1 = 1_K$ and $\sigma^{-1}\pi\sigma$ fixes 1. Thus, $((y_i)\pi)^{\phi(u)} \in R^*$ and hence $R^* \trianglelefteq C_H(1)$. For the second part, notice that $\mathrm{Alt}(\Omega \setminus \{1\}) \subseteq R^*$ and hence $C_H(1) = C_H(\Omega)\,\mathrm{Alt}(\Omega \setminus \{1\}) \subseteq C_H(\Omega) R^* \subseteq C_H(1)$.

Step 2. $(K')^{\Omega^*} \leq R_1$ where $\Omega^* = \Omega \setminus \{1\}$:

Let $k \in K$ and $r = (r_i)\pi \in R_1$ be such that $2^{\pi} = 3$. Let $a := (k, k^{-1}, 1, \ldots, 1) \in B$. Then $a^r = (k, 1, k^{-r2}, 1, \ldots, 1)$ and $a^{-1}a^r = (1, k, k^{-r2}, 1 \ldots, 1)$. Since $R_1 \trianglelefteq C_R(1)$ and $B = C_R(\Omega) \leq C_R(1)$, B normalizes R_1 and hence $a^{-1}a^r = [a, r] \in R_1 \cap B$. Let $s = (s_i)\sigma \in R_1$ such that $2^{\sigma} = 4$ and consider $c := (l, l^{-1}, 1, \ldots, 1) \in B$ where $l \in K$. Similarly, $c^{-1}c^s = (1, l, 1, l^{-s2}, 1, \ldots, 1) \in R_1 \cap B$ and the commutator $[a^{-1}a^r, c^{-1}c^s]$ gives $(1, [k, l], 1, 1, \ldots, 1) \in R_1 \cap B$. In fact, for $2 \leq j \leq n$, if we put k^{-1} and l^{-1} into the j^{th} position in the definition of a and b respectively, and choose r and s so that $j^r \neq 1, j$ and $j^s \neq 1, j, j^r$ we get the commutator $[k, l]$ in

the j^{th} position. This proves Step 2 as $[k,l]$'s generate K'.

Step 3. $R_1 \cap B = R^* \cap B$:

Obviously, $R_1 \cap B \leq R^* \cap B$ by Step 1. For the converse, let $g \in R^* \cap B$. Then $g = (g_i)_{i\in\Omega}$ where $g_1 = 1$ and $\prod_{i=1}^{n} g_i \in K'$. Observe that g can be written as $g = (1, g_2, g_2^{-1}, 1, \ldots, 1)(1, 1, g_2g_3, (g_2g_3)^{-1}, 1, \ldots, 1)\cdots(1, \ldots, 1, y, y^{-1})(1, \ldots, 1, x)$ where $y = \prod_{i=2}^{n-1} g_i$ and $x = \prod_{i=2}^{n} g_i$. Since $x \in K'$, the last factor of g is in R_1 by Step 2. In order to conclude $g \in R_1$, we shall show that the other factors are in R_1 as well. Without loss, take $(1, k, k^{-1}, 1, \ldots, 1)$ for some $k \in K$. Recall that $d := (1, k, k^{-r}2, 1, \ldots, 1) \in R_1$ from the previous step. Moreover, since $a^{-1}a^r \in B$, $kk^{-r}2 \in K'$ and so does its inverse and hence $e := (1, 1, k^{-1}k^r2, 1, \ldots, 1) \in R_1$. Thus $de = (1, k, k^{-1}, 1, \ldots, 1) \in R_1$.

Step 4. $R_1 = R^*$:

Since $R_1 \trianglelefteq C_R(1)$ and $R^* \leq C_R(1)$, we have $R_1 \trianglelefteq R^*$. Also $R^*/R^* \cap B \cong \mathrm{Alt}(\Omega\backslash\{1\})$ is simple. Then $R_1 \not\leq B$, together with Step (3), implies that $R^* \cap B \lneq R_1 \trianglelefteq R^*$ and hence $R_1 = R^*$, completing the proof of the lemma.

Let $(H, \Omega), (H_A, \Omega_A) \in \mathcal{A}$ such that $H \leq H_A$, $C_H(\Omega_A) = 1$ and H is Ω-block-diagonal on Ω_A. Since $R \neq 1$, $R \not\leq C_H(\Omega_A)$ and hence there exists an orbit Σ for H on Ω_A such that $R \not\leq C_H(\Sigma)$. Thus, Σ is an Ω-essential orbit. Let Λ^* be the union of all Ω-essential orbits for H on Ω_A. Then there exists an H-invariant partition Λ of Λ^* such that $\Lambda \cong \Omega$ as H-sets. Thus, set $\Lambda = \{\Lambda_i \mid i \in \Omega\}$. Define $B_1 = \{(g_i)_{i\in\Omega} \in B \mid g_1 = 1\}$. Then:

Lemma 4.1.7 $C_B(\Lambda_1) \leq B_1$.

Proof: Put $J_1 := \{g_1 \mid g = (g_i)_{i\in\Omega} \in C_B(\Lambda_1)\}$. In other words, J_1 is the projection of $C_B(\Lambda_1)$ onto the first coordinate and hence $J_1 \leq K$. We define $J := \{g \in B \mid g_i \in J_1 \text{ for all } i \in \Omega\}$ and observe that it is a group. Since $B = \{(g_i)_{i\in\Omega} \in K^\Omega \mid \prod_{i\in\Omega} g_i \in K'\}$, we can choose any element of K as g_1 and choose rest of the coordinates so that the product of these coordinates is in K'. This shows that if we take the projection of the groups $C_B(\Lambda_1)$ and B onto the first coordinate and use $C_B(\Lambda_1) \trianglelefteq B$, we get $J_1 \trianglelefteq K$. We now claim that $J \trianglelefteq R$. To see this, take $g \in J$ and $r \in R$. Since $R = B\,\mathrm{Alt}(\Omega)$, we put $r = (r_i)\pi$ where $(r_i) \in B$. Then $g^r = (r_i^{-1} g_i r_i)^\pi_{i\in\Omega}$ and each of these coordinates is in J_1 since $g_i \in J_1$ and $r_i \in K$. Hence $J \trianglelefteq R$, as claimed.

Next we shall show that $R_1 \leq C_R(\Lambda_1)$. Let Ψ be an Ω-essential orbit for H on Ω_A. Then $C_H(\Psi \cap \Lambda_1) \not\leq C_H(\Omega)$ by Remark (a) on page 60. Put $H_1 := C_H(1)$. Then $C_{H_1}(\Psi \cap \Lambda_1) \trianglelefteq H_1$ and so $C_{H_1}(\Psi \cap \Lambda_1)C_H(\Omega) \trianglelefteq H_1$. Since $H_1/C_{H_1}(\Omega)$ is simple, we obtain $H_1 = C_{H_1}(\Psi \cap \Lambda_1)C_H(\Omega)$. Minimality of R_1 implies that $R_1 \leq C_{H_1}(\Psi \cap \Lambda_1)$ and since Ψ is arbitrary, we get $R_1 \leq C_H(\Lambda_1)$. Then $R_1 \leq R$ gives $R_1 \leq C_R(\Lambda_1)$.

Now we claim that $C_B(\Lambda_1) = \{g \in B \mid g_1 \in J_1\}$. Observe that $(\subseteq)$ is trivial. For the converse, let $g \in B$ with $g_1 \in J_1$. Then $g_1 = h_1$ for some $h \in C_B(\Lambda_1)$ and hence $h^{-1}g \in B \cap R^* = B \cap R_1 \leq B \cap C_R(\Lambda_1)$. Now $h^{-1}g \in C_B(\Lambda_1)$ implies that $g \in C_B(\Lambda_1)$, proving the converse. As our final step, we shall show that $J = 1$. Note that trivially $J \subseteq \{g \in B \mid g_1 \in J_1\} = C_B(\Lambda_1)$. Let $\omega \in \Omega$. Then $\omega = 1^g$ for some $g \in R$ and since $J \trianglelefteq R$, $J = J^g \subseteq C_B(\Lambda_1)^g = C_B(\Lambda_\omega)$. Since ω is arbitrary, we get $J \leq C_B(\Lambda^*)$. On the other hand, R and in particular B acts trivially on $\Omega_A \setminus \Lambda^*$. Hence $C_B(\Lambda^*) \leq C_H((\Omega_A \setminus \Lambda^*) \cup \Lambda^*) = C_H(\Omega_A) = 1$. Thus $J = 1$ which implies that $J_1 = 1$ and thus $C_B(\Lambda_1) \leq B_1$, completing the proof.

Proposition 4.1.8 *Let G be a non-regular alternating group and $x \in G$ be of prime order p. Then there exists $g \in G$ such that $Z := \langle x, x^g \rangle \cong C_p \times C_p$ and Z is a regular subgroup of G.*

Proof: By [4, Theorem 3.4], there exists an alternating Kegel cover $\mathcal{D}$ for G such that, for any $A, B \in \mathcal{D}$ with $H_A \leq H_B$, H_A is Ω_A-block-diagonal on Ω_B. Without loss of generality, $x \in H_A$ for all $A \in \mathcal{D}$. Since the set $\{\deg_{\Omega_A}(x) \mid A \in \mathcal{D}\}$ is unbounded by [8, Corollary 3.13], we pick an element $(H, \Omega) \in \mathcal{D}$ such that $\deg_\Omega(x) \geq 2p^2$, that is, x has at least $2p$ non-trivial orbits on Ω. Thus, we write

$$\pi = [\prod_{i=1}^{p}(a_{i1}, a_{i2}, \ldots, a_{ip})][\prod_{i=1}^{p}(b_{i1}, b_{i2}, \ldots, b_{ip})]\sigma \tag{4.2}$$

where π is the image of x in $\mathrm{Alt}(\Omega)$, $\{a_{ij}, b_{ij}\} \subseteq \Omega$, and σ denotes the action of x on the remaining elements of Ω.

Without loss of generality, we may assume that $\mathcal{D} = \mathcal{D}(H)$ and hence H acts faithfully on Ω_A for all $A \in \mathcal{D}$ by definition of $\mathcal{D}(H)$. We continue the notation used above and recall the definition of $\phi : R \xrightarrow{\cong} (K \wr_\Omega \mathrm{Alt}(\Omega))'$. In particular, recall that $B = C_R(\Omega) = \phi^{-1}((K^\Omega)_\circ) \trianglelefteq H$ and $(K^\Omega)_\circ = \{(g_i)_{i\in\Omega} \in K^\Omega \mid \prod_{i\in\Omega} g_i \in K'\}$. We now consider the cases $p \nmid |K|$ and $p \mid |K|$ separately.

Case (a) Assume that $p \nmid |K|$.

Let $\overline{H} = H/C_H(\Omega)$ and note that $\mathrm{Alt}(\Omega) \cong \overline{H} = RC_H(\Omega)/C_H(\Omega) = \overline{R}$ and $(K^\Omega)_\circ$ is a p'-group. Observe that there exists an element $g \in R$ so that

$$\overline{x}^{\overline{g}} = [\prod_{i=1}^{p}(a_{1i}, a_{2i}, \ldots, a_{pi})][\prod_{i=1}^{p}(b_{1i}, b_{2i}, \ldots, b_{pi})]\sigma. \tag{4.3}$$

Indeed, we can let

$$g := [\prod_{1\le i<j\le p}(a_{ij}, a_{ji})][\prod_{1\le i<j\le p}(b_{ij}, b_{ji})].$$

Note that g is a product of even number of transpositions and hence $g \in \mathrm{Alt}(\Omega)$. Clearly $\langle \overline{x} \rangle \neq \langle \overline{x}^{\overline{g}} \rangle$, $[\overline{x}, \overline{x}^{\overline{g}}] = 1$, and $|\overline{x}| = |\overline{x}^{\overline{g}}| = p$. Thus $\langle \overline{x}, \overline{x}^{\overline{g}} \rangle \cong C_p \times C_p$. Note that $\{a_{ij} \mid 1 \le i, j \le p\}$ (or $\{b_{ij} \mid 1 \le i, j \le p\}$) is a regular orbit for $\langle \overline{x}, \overline{x}^{\overline{g}} \rangle$ on Ω. Since $\langle \overline{x}, \overline{x}^{\overline{g}} \rangle$ is abelian, $[x, x^g] \in C_H(\Omega)$. Moreover, since $g \in R$ and $R \trianglelefteq H$, we have $xR = x^g R$. Thus $[x, x^g] \in C_R(\Omega) = B$ and so $xB = x^g B$. On the other hand, observe that $\langle x \rangle B = \langle x^g \rangle B$ would imply that $\langle x \rangle C_H(\Omega) = \langle x \rangle B C_H(\Omega) = \langle x^g \rangle C_H(\Omega)$, a contradiction. Therefore $\langle x \rangle B \neq \langle x^g \rangle B$ and hence $\langle x, x^g \rangle B/B \cong C_p \times C_p$. Let T be a Sylow p-subgroup of $\langle x, x^g \rangle B$ containing x. Since B is a p'-group, $T \cap B = 1$. Then $\langle x, x^g \rangle B = TB$ and $C_p \times C_p \cong TB/B \cong T$. Let y be such that $T \cap x^g B = \{y\}$. Since $\langle y \rangle$ and $\langle x^g \rangle$ are Sylow p-subgroups of $\langle x^g \rangle B$, there exists an element $h = (x^g)^i b \in \langle x^g \rangle B$ with $\langle x^g \rangle^h = \langle y \rangle$. Hence $\langle x^{gb} \rangle = \langle y \rangle$, which implies $y^{-1} x^{gb} \in \langle y \rangle$. Moreover, $x^{gb} B = x^g B = yB$ since $g \in R$ and $B \trianglelefteq H$. Thus, $y^{-1} x^{gb} \in \langle y \rangle \cap B = 1$ and $y = x^{gb}$. By the definition of g, $y = x^{gb} \notin \langle x \rangle$ and hence $T = \langle x, y \rangle = \langle x, x^{gb} \rangle \cong C_p \times C_p$. Since $b \in B$ acts trivially on Ω, T has a regular orbit on Ω as well. So let $\omega \in \Omega$ such that $C_T(\omega) = 1$.

Let $A \in \mathcal{D}$ be arbitrary and let Σ be an Ω-essential orbit for H on Ω_A. Let Δ be an H-invariant partition of Σ such that $\Omega \cong \Delta$ as H-sets and let D be the element in Δ corresponding to w. Then $C_T(\{D\}) = C_T(\omega) = 1$, that is, $D^t \neq D$ for any $1 \neq t \in T$. Hence $d^t \neq d$ for any $1 \neq t \in T$ and $d \in D$. So $C_T(d) = 1$, in other words, T has a regular orbit on Ω_A. Therefore, we have shown that

$$\mathcal{D}_{reg}(T) := \{(H_A, \Omega_A) \in \mathcal{D} \mid T \le H_A \text{ and } T \text{ has a regular orbit on } \Omega_A\} = \mathcal{D}.$$

Since $\mathcal{D}_{reg}(T) \subseteq \mathcal{A}_{reg}(T)$, we conclude that $\mathcal{A}_{reg}(T)$ is a Kegel cover for G and hence T is a regular subgroup of G. This proves Case (a) with 'Z'='T' and 'g'='gb'.

Case (b) Assume that $p \mid |K|$.

Since $x \in H \leq L \wr_\Omega \mathrm{Alt}(\Omega)$, write $x = (x_i)_{i\in\Omega}\pi$ where $(x_i)_{i\in\Omega} \in L^\Omega$. Recall that by (4.2) we already defined the action of x on Ω. However, for the rest of the proof we shall change this notation and put $\pi = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p)\sigma$ where σ denotes the remaining orbits of x on Ω. This is done to simplify the notation. Besides the proof of Case (b) requires only that x has at least two non-trivial orbits. Let $k \in K$ be of order p and define $h \in K^\Omega$ by $h := (k, 1, \ldots, 1, k^{-1}, 1, \ldots, 1)$ where k^{-1} is on the $(p+1)^{\text{st}}$ coordinate. Put

$$g := \prod_{i=1}^{p} h^{ix^{i-1}} = h \cdot h^{2x} \cdot h^{3x^2} \cdots h^{(p-1)x^{p-2}} \cdot 1 \tag{4.4}$$

and observe that since $h \in B$ and $B \trianglelefteq H$, we have $g \in B$. For any $1 \leq n \leq p$, $h^{nx} = (1, k^{nx_1}, 1, \ldots, 1, k^{-nx_{p+1}}, 1, \ldots, 1)$ where $k^{-nx_{p+1}}$ appearing in the $(p+2)^{\text{nd}}$ coordinate. In a similar way, $h^{nx^j} = (1, \ldots, 1, *, 1, \ldots, 1, *, 1, \ldots, 1)$ where the non-trivial elements $*$ are on the $(j+1)^{\text{st}}$ and $(p+j+1)^{\text{st}}$ coordinate for any $1 \leq j < p$. This shows that $[h^{nx^i}, h^{mx^j}] = 1$ for all n, m and for all $1 \leq i, j \leq p$.

Let us now consider the product $\prod_{i=1}^{p} h^{(i+1)x^i} = h^{2x} \cdot h^{3x^2} \cdots (h^p)^{x^{p-1}} \cdot (h^{p+1})^{x^p}$. Since $h^p = x^p = 1$, the last two factors of this product are equal to 1 and h, respectively. Since the factors do commute, we get $g = \prod_{i=1}^{p} h^{(i+1)x^i}$.

Then $g^{-1} = \prod_{i=1}^{p} h^{-(i+1)x^i}$ and

$$g^{-1}g^x = \prod_{i=1}^{p} h^{-(i+1)x^i} \cdot h^{ix^i} = \prod_{i=1}^{p} h^{-x^i}. \tag{4.5}$$

Since the first coordinate of $g^{-1}g^x$ is $k^{-1} \neq 1$, $g^{-1}g^x \notin B_1$ by definition of B_1. In particular, $g^{-1}g^x \neq 1$ which means $x \neq x^g$. Next assume to the contrary that $\langle x \rangle = \langle x^g \rangle$. Then $x^{-1}x^g \in \langle x \rangle$. Since $g \in B$ and $B \trianglelefteq H$, $xB = x^gB$ and hence $x^{-1}x^g \in B$ and $x^{-1}x^g \in B \cap \langle x \rangle$. Note that $B \cap \langle x \rangle$ is a group of order 1 or p and since x does not act trivially on Ω, $x \notin B$. Thus $B \cap \langle x \rangle = 1$ which implies $x^{-1}x^g = 1$, a contradiction. Hence $\langle x \rangle \neq \langle x^g \rangle$. Notice that $(g^{-1}g^x)^x = g^{-1}g^x$ by (4.5) and so x^g and x do commute and $\langle x, x^g \rangle \cong C_p \times C_p$. Put $Z := \langle x, z \rangle \cong C_p \times C_p$ where $z := [g, x]$. Note that $Z = \langle x, x^g \rangle$.

Let $A \in \mathcal{D}$. We shall show that Z has a regular obit on Ω_A. Since $z = g^{-1}g^x \notin B_1$, $z \notin C_B(\Lambda_1)$ by Lemma 4.1.7. Therefore, there exists $\lambda \in \Lambda_1$ such that $\lambda^z \neq \lambda$. We claim that λ^Z is a regular orbit for Z. Since $z \in B = C_R(\Omega)$ acts trivially on Λ, we have $z \in N_Z(\Lambda_1)$. On the other hand, $x \notin N_Z(\Lambda_1)$. Thus, $\langle z \rangle \leq N_Z(\Lambda_1) \lneq Z$ and since $|z| = |Z| = p^2$ we get $N_Z(\Lambda_1) = \langle z \rangle$. For any $y \in C_Z(\lambda)$, we have $\lambda^y = \lambda \in \Lambda_1$. Since Λ is an H-invariant partition, $\Lambda_1^y = \Lambda_1$, that is, $y \in N_Z(\Lambda_1)$. Thus, $C_Z(\lambda) \leq N_Z(\Lambda_1) = \langle z \rangle$. This implies $C_Z(\lambda) = C_{\langle z \rangle}(\lambda) = 1$ and hence Z has a regular orbit on Λ_1 and so on Ω_A. By an argument similar to the one in the previous case, we deduce that Z is a regular subgroup of G, completing the proof.

Theorem 4.1.9 *Let G be a non-regular alternating group and $x \in G$ with $|x| = p$ where p is a prime. Then $C_G(x)$ is non-abelian.*

Proof: Let $x \in G$ be of order p. There exists an element $g \in G$ such that $Z := \langle x, x^g \rangle \cong C_p \times C_p$ and Z is a regular subgroup of G by Proposition 4.1.8. Then by Lemma 4.1.1 $C_G(z) \neq C_G(Z)$ for all $1 \neq z \in Z$ and, in particular, $C_G(x) \neq C_G(x^g)$. Suppose to the contrary that $C_G(x)$ is abelian. Then $x^g \in C_G(x)$ implies that $C_G(x) \leq C_G(x^g)$ and similarly $C_G(x^g) \leq C_G(x)$. Thus $C_G(x) = C_G(x^g)$, a contradiction. Therefore, $C_G(x)$ is non-abelian.

4.2 The Finitary Case

Lemma 4.2.1 *Let P be a finite p-group, p a prime, and $x \in P$ with $|x| = p$. If $X = \langle x \rangle \not\trianglelefteq Z(P)$, then there is an element $g \in P$ with $\langle x \rangle \neq \langle x^g \rangle$ and $[x, x^g] = 1$.*

Proof: $X \not\trianglelefteq Z(P)$ implies that $C_P(X)$ is a proper subgroup of P. By the normalizer condition, $C_P(X) \lneq N_P(C_P(X))$. Since the quotient $N_P(X)/C_P(X)$ is isomorphic to a subgroup of $\mathrm{Aut}(X)$ whose order is $p-1$, we also have $C_P(X) = N_P(X)$. Let g be an element in $N_P(C_P(X)) \setminus N_P(X)$. Then $g \notin N_P(X)$ implies $\langle x^g \rangle \neq \langle x \rangle$ and $g \in N_P(C_P(X))$ gives us $x^g \in C_P(X)$ and hence $[x, x^g] = 1$.

Lemma 4.2.2 *Let G be a locally finite group and $x \in G$ such that $|x| = p$, p a prime. If $[x, x^g] \neq 1$ for any $g \in G$ with $\langle x \rangle \neq \langle x^g \rangle$, then every finite p-subgroup is conjugate to a subgroup of $C_G(x)$.*

Proof: Let P be a finite p-subgroup of G. Since G is locally finite, $\langle P, x \rangle$ is a finite subgroup. Choose a Sylow p-subgroup S of $\langle P, x \rangle$ with $x \in S$. Then $P^g \leq S$ for some $g \in \langle P, x \rangle$. If $x \notin Z(S)$, we get a contradiction by Lemma 4.2.1. Thus $x \in Z(S)$ and hence $P^g \leq S \leq C_G(x)$.

Theorem 4.2.3 *Let G be a non-linear LFS-group and $n \in \mathbb{Z}^+$. Then there exist $A \trianglelefteq B \leq G$ with B finite and $B/A \cong \mathrm{Sym}(n)$.*

Proof: It is a well known result. See, for instance, [9, Theorem 2.6].

Corollary 4.2.4 *Let G be a LFS-group and p a prime. If every finite p-subgroup of G is abelian, then G is linear.*

Proof: Suppose that G is non-linear. Then, by Theorem 4.2.3, for any $n \in \mathbb{Z}^+$ there exist $A \trianglelefteq B \leq G$ such that $B/A \cong \mathrm{Sym}(n)$. We can choose n large enough so that $\mathrm{Sym}(n)$ has non-abelian Sylow p-subgroups. So let PA/A be a non-abelian

Sylow p-subgroup of B/A where $P \in \mathrm{Syl}_p(B)$. As $PA/A \cong P/P \cap A$, P is non-abelian. Hence G contains a non-abelian p-subgroup, a contradiction.

Theorem 4.2.5 *Let G be a LFS-group of alternating type. Then $C_G(x)$ is not abelian for any $x \in G$ with $|x| = p$ where p is a prime.*

Proof: Assume that $C_G(x)$ is abelian for some $x \in G$ with $|x| = p$. Suppose for a contradiction that $[x, x^g] \neq 1$ for all $g \in G$ with $\langle x \rangle \neq \langle x^g \rangle$. Then, by Lemma 4.2.2, every finite p-subgroup is conjugate to a subgroup of $C_G(x)$. So every finite p-subgroup is abelian. Then G is linear by Corollary 4.2.4, a contradiction. Hence there exists $t \in G$ such that $\langle x \rangle \neq \langle x^t \rangle$ and $[x, x^t] = 1$. Since $C_G(x)$ is abelian and $x^t \in C_G(x)$, we have $C_G(x) \leq C_G(x^t)$. By a similar argument we obtain $C_G(x^t) \leq C_G(x)$ and thus $C_G(x^t) = C_G(x)$. By Proposition 4.1.2, G is non-regular. Now by Theorem 4.1.9, we get a final contradiction.

Lemma 4.2.6 *Let $\mathbb{K}$ be a field, V a vector space over $\mathbb{K}$, X a finite dimensional subspace of V and s a nondegenerate bilinear form on V. Then there exists a finite dimensional subspace U of V containing X such that $s|_{U \times U}$ is nondegenerate.*

Proof: Write $V = (X + X^\perp) \oplus Y$ for some $\mathbb{K}$-space Y. Note that $\dim Y = \dim V/X + X^\perp \leq \dim V/X^\perp = \dim X < \infty$. Let $U := X + Y$. We need to show that $U \cap U^\perp = 0$. Since $U \cap U^\perp \subseteq U \cap X^\perp \subseteq (X+Y) \cap (X+X^\perp) = X + (Y \cap (X+X^\perp)) = X$, we have $U \cap U^\perp \subseteq X$. Moreover, $X \cap U^\perp = X \cap X^\perp \cap Y^\perp \subseteq (X+X^\perp)^\perp \cap Y^\perp = V^\perp = 0$. Thus $U \cap U^\perp \subseteq X \cap U^\perp = 0$.

Lemma 4.2.7 *Let $s : V \times W \longrightarrow \mathbb{K}$ be a nondegenerate bilinear map and X_1 and Y_1 be finite dimensional subspaces of V and W, respectively. Then there are finite dimensional subspaces X and Y satisfying the following: $X_1 \leq X \leq V$, $Y_1 \leq Y \leq W$, $V = X \oplus Y^\perp$ and $W = X^\perp \oplus Y$.*

Proof: See [8, Lemma 3.5].

Lemma 4.2.8 *Let G be a group, $\mathbb{K}$ a field, and A and B be $\mathbb{K}G$-modules. Let $s : A \times B \longrightarrow \mathbb{K}$ be a G-invariant bilinear map, that is, $s(a^g, b^g) = s(a, b)$ for all $a \in A$, $b \in B$ and $g \in G$. If $A^\perp = 0$, then $[A, g]^\perp = C_B(g)$ for all $g \in G$.*

Proof:

$$\begin{aligned} b \in [A,g]^\perp &\Leftrightarrow s([a,g],b) = 0 \quad \text{for all } a \in A. \\ &\Leftrightarrow s(a^g - a, b) = 0 \quad \text{for all } a \in A. \\ &\Leftrightarrow s(a^g, b) - s(a,b) = 0 \quad \text{for all } a \in A. \\ &\Leftrightarrow s(a, b^{g^{-1}}) - s(a,b) = 0 \quad \text{since } s \text{ is } G\text{-invariant.} \\ &\Leftrightarrow s(a, b^{g^{-1}} - b) = 0 \quad \text{for all } a \in A. \\ &\Leftrightarrow b^{g^{-1}} - b \in A^\perp \Leftrightarrow b^{g^{-1}} = b. \\ &\Leftrightarrow b \in C_B(g). \end{aligned}$$

Corollary 4.2.9 *Let G be a LFS-group and $x \in G$ such that $|x| = r$ where r is a prime. If $C_G(x)$ is abelian, then G is either a group of r-type or linear. In particular, if there are two elements in G with distinct prime orders and with abelian centralizers, then G is linear.*

Proof: Let $x \in G$ with $|x| = r$ and $C_G(x)$ abelian. By Theorem 4.2.5, G can not be of alternating type. Hence, using Theorem 3 (page 4), we will assume that G is either a group of p-type for some prime $p \neq r$ or a non-linear finitary group and obtain a contradiction in both cases.

Case 1. Assume that G is a group of p-type where $p \neq r$.

Then there exists a Kegel cover $\mathcal{K}$ for G such that if $(H, N) \in \mathcal{K}$ then $H/O_p(H)$ is

the central product of perfect central extensions of classical groups defined over a field in characteristic p and H/N is a projective special linear group, again by Theorem 3. So $H/N \cong \mathrm{PSL}_n(p^k)$ for some n and k and, without loss of generality, we may assume $n \gg r$. Note that H/N is simple, so $O_p(H/N) = 1$ and $O_p(H) \leq N$ for any $(H, N) \in \mathcal{K}$. Now choose $(H, N) \in \mathcal{K}$ such that $x \in H \setminus N$ and write $\overline{H} := H/O_p(H) = G_1 \cdot G_2 \cdots G_l$ where $[G_i, G_j] = 1$ for all $i \neq j$, G_i's are perfect, and $G_i/Z(G_i)$ is isomorphic to a classical group. Put $\overline{x} = x_1 x_2 \cdots x_l$ where $x_i \in G_i$. Since $\overline{N}$ is a maximal normal subgroup of $\overline{H}$, there exists $1 \leq i \leq l$, say $i = 1$, such that $G_1 \nleq \overline{N}$. Then $\overline{H} = G_1\overline{N}$. Also $[G_j, G_1] = 1$ implies that $G_j\overline{N}/\overline{N} \leq Z(\overline{H}/\overline{N})$. Then since $\overline{H}/\overline{N}$ is simple, $G_j \subseteq \overline{N}$ for $j = 2, 3 \ldots, l$. Thus $x_1 \notin \overline{N}$ and, in particular, $x_1 \neq 1$. Note that $|x| = r$ implies $x_1^r \in G_1 \cap \prod_{j=2}^{l} G_j = Z(\overline{H})$, that is, $x_1 Z(G_1)$ has order r in $G_1/Z(G_1)$. Moreover,

$$\mathrm{PSL}_n(p^k) \cong H/N \cong \overline{H}/\overline{N} = G_1\overline{N}/\overline{N} = G_1/G_1 \cap \overline{N} \cong G_1/Z(G_1).$$

Denote $D/Z(G_1) := C_{G_1/Z(G_1)}(x_1)$. Then $D/Z(G_1)$ and hence $D'Z(G_1)/Z(G_1)$ is not solvable by Remark 1.1.16. So D' is non-abelian. Since $[D, x_1] \leq Z(G_1)$, by Three Subgroup Lemma we have $D' \leq C_{G_1}(x_1)$. Therefore $C_{G_1}(x) = C_{G_1}(x_1)$ is non-abelian. Moreover $C_{\overline{H}}(x) = \overline{C_H(x)}$ by [16, Theorem 8.13, p.238]. Since $C_{G_1}(x) \leq C_{\overline{H}}(x)$, we conclude that $C_H(x)$ and hence $C_G(x)$ is not abelian. This contradiction completes the proof of this case.

Case 2. Assume that G is a non-linear finitary group.

Then by Theorem 2 (p. 3), G is isomorphic to one of the following:

(a) an alternating group $\mathrm{Alt}(\Omega)$ where Ω is infinite,

(b) a finitary classical group, or

(c) a finitary special transvection group.

(a) This is not possible: Clearly, $\mathrm{Alt}(\Omega \setminus \mathrm{supp}(x)) \subseteq C_{\mathrm{Alt}(\Omega)}(x)$ implies that $C_{\mathrm{Alt}(\Omega)}(x)$ is not abelian, a contradiction to the assumption.

(b) Assume G is a finitary classical group and let $G \leq \mathrm{FGL}_{\mathbb{K}}(V)$ and s be the corresponding bilinear form on V. Since G is finitary, $X := [V, x]$ is finite dimensional. By Lemma 4.2.6, there exists a finite dimensional subspace U of V containing X and $V = U \oplus \widetilde{U}$ where $\widetilde{U} := U^{\perp}$. Now we get $[\widetilde{U}, x] \leq U \cap \widetilde{U} = 0$ and note that $\widetilde{U}$ is infinite dimensional and induces a full classical group $K := Cl_{\mathbb{K}}(\widetilde{U}, s)$. Hence $[x, K]$ centralizes both U and $\widetilde{U}$, which implies that $[x, K] = 1$. Thus $K \subseteq C_G(x)$. Hence $C_G(x)$ is not abelian, contradiction.

(c) Suppose now that G is a finitary special transvection group, that is,

$$G = T_{\mathbb{K}}(W, V) := \langle\, t(\varphi, v) \mid \varphi \in W, v \in V, v\varphi = 0 \,\rangle \leq \mathrm{GL}_{\mathbb{K}}(V)$$

where W is a subspace of the dual $V^{\star}$ and $\mathrm{Ann}_V W = 0$. Observe that $\mathrm{Ann}_W V = 0$. We note here that $t(\varphi, v)$ is defined by $u.t(\varphi, v) := u + (u\varphi)v$ for all $u \in V$. Observe that W is a G-submodule of $V^{\star}$ with the action given by $u.\lambda g := (ug^{-1})\lambda$ where $u \in V$, $\lambda \in W$ and $g \in G$.

Let $x \in G$. Since G is finitary, $\dim[V, x] < \infty$. Define $s : V \times W \longrightarrow \mathbb{K}$ by $s(v, \lambda) = v.\lambda$. Obviously, s is a G-invariant, non-degenerate bilinear map. Since $V^{\perp} = 0$ and $W^{\perp} = 0$, we have $[W, x]^{\perp} = C_V(x)$ and $[V, x]^{\perp} = C_W(x)$ by Lemma 4.2.8. Then $\dim[W, x] = \mathrm{codim}\, C_W(x) = \mathrm{codim}[V, x]^{\perp} = \dim[V, x] < \infty$. Therefore, there are finite dimensional subspaces X and Y such that $[V, x] \leq X \leq V$ and $[W, x] \leq Y \leq W$ with $V = X \oplus Y^{\perp}$ and $W = X^{\perp} \oplus Y$ by Lemma 4.2.7.

We now claim that $H := T(X^{\perp}, Y^{\perp}) \leq C_G(x)$. Clearly, $[V, x, H] \leq [X, H] = 0$. Let $u \in V$ and $t(\varphi, v) \in H$ where $\varphi \in X^{\perp}$ and $v \in Y^{\perp}$ such that $v\varphi = 0$. Then $[u, t(\varphi, v)] = (u\varphi)v \in \mathbb{K}v \leq Y^{\perp}$ implies that $[V, H] \leq Y^{\perp}$. Since $[W, x] \leq Y$, we have $Y^{\perp} \leq [W, x]^{\perp} = C_V(x)$. Thus $[V, H, x] \leq [Y^{\perp}, x] = 0$. Using Three Subgroup Lemma, we conclude that $[V, [x, H]] = 0$. Hence $[x, H] = 1$, that is, $H \leq C_G(x)$. Therefore $C_G(x)$ is not abelian, a contradiction. This completes the proof of the first statement of the theorem.

The second statement follows from the fact that a LFS-group cannot be a p-type group for two different primes.

Chapter 5

On Infinite Abelian Subgroups in Locally Finite Simple Groups

Recall that a group is said to have the minimum condition, or min, if every descending chain of subgroups terminates in finitely many steps and G is called a Černikov group if it is abelian-by-finite and satisfies min.

Notation: $(C_{p\infty})^k := \underbrace{C_{p\infty} \times C_{p\infty} \times \cdots \times C_{p\infty}}_{k-times}$ where $C_{p\infty}$ stands for Prüfer groups.

Lemma 5.1.1 *Let $Y \trianglelefteq X \leq R$ where X/Y is a finite elementary abelian p-group and $R \cong (C_{p\infty})^k$. Then $|X/Y| \leq p^k$.*

Proof: First consider the special case when X is finite. Then $X \cong C_{p^{r_1}} \times C_{p^{r_2}} \times \cdots \times C_{p^{r_k}}$ for some $r_i \in \mathbb{Z}^+$ where $1 \leq i \leq k$ and the Frattini subgroup of X is $\Phi(X) \cong C_{p^{r_1-1}} \times C_{p^{r_2-1}} \times \cdots \times C_{p^{r_k-1}}$. Since X/Y is elementary abelian, $\Phi(X/Y) = 1$. Then $\Phi(X)Y/Y \leq \Phi(X/Y)$ gives $\Phi(X) \leq Y$ and hence $|X/Y| \leq |X/\Phi(X)| = p^k$.

For the general case, write $X = \cup_{i \in I} X_i$ where X_i is of finite order with $X_i < X_{i+1}$ for all $i \in I$. Note here that X is a locally finite group. By letting $Y_i := Y \cap X_i$, we get $Y = \cup Y_i$ and $X_i Y \leq X_{i+1} Y$ for all $i \in I$. Assume to the contrary that $|X/Y| > p^k$. Then we can choose $i \in I$ such that $|X_i Y/Y| > p^k$. But

$$X_i/Y_i \cong X_i/Y \cap X_i \cong X_i Y/Y$$

implies that $|X_i/Y_i| > p^k$ for some i and X_i/Y_i is elementary abelian since X_i/Y_i is isomorphic to a subgroup of X/Y. As X_i is finite, we get a contradiction to the special case. Thus $|X/Y| < p^k$.

Lemma 5.1.2 *Let G be a Černikov p-group. Then there exists an integer n such that $|A/B| \leq p^n$ for all $B \trianglelefteq A \leq G$ with A/B elementary abelian.*

Proof: Let A/B be an arbitrary elementary abelian section of G. Since A/B satisfies min, the order of A/B is finite. Recall that G is a Černikov p-group implies that there exists an abelian normal subgroup R of G such that G/R is finite and $R \cong (C_{p^\infty})^k$ for some $k \in \mathbb{Z}^+$, see [5, Theorem 1.5.5]. Let $|G/R| = p^l$ and $A/B \cong (C_p)^t$. We shall show that $t \leq n := k + l$.

$R \leq RB \leq RA \leq G$ implies that RA/RB, which is isomorphic to $A/A \cap RB$, has order divisible by p^l. Hence

$$|A/A \cap RB| \leq p^l. \tag{5.1}$$

We also have $A \cap BR/B \cong (A \cap R)B/B \cong A \cap R/A \cap B \cap R := X/Y$. Since X/Y is isomorphic to a subgroup of A/B, it is elementary abelian. Note that $X \leq R$. By Lemma 5.1.1, we get

$$|A \cap BR/B| = |X/Y| \leq p^k. \tag{5.2}$$

Combining (5.1) and (5.2), we obtain $|A/B| \leq p^{k+l}$.

Theorem 5.1.3 *Let G be a non-linear LFS-group and p a prime. Then there exists a p-subgroup of G which is not Černikov.*

Proof: For any integer n, there exist $A_n \trianglelefteq B_n \leq G$ with B_n finite and $B_n/A_n \cong \mathrm{Sym}(n)$ by Theorem 4.2.3. Let $s_n := \lfloor n/p \rfloor$. $\mathrm{Sym}(n)$, and thus B_n/A_n, has elementary abelian p-subgroups of order p^{sn}. Let C_n/A_n be such a group and let $P_n \in \mathrm{Syl}_p(C_n)$. Then $C_n = P_n A_n$ and

$$\frac{C_n}{A_n} = \frac{P_n A_n}{A_n} \cong \frac{P_n}{A_n \cap P_n} \text{ is an elementary abelian group of order } p^{sn}.$$

This means P_n has arbitrarily large elementary abelian sections as n gets arbitrarily large. Let $Q_1 = P_1$. Let Q_2 be a Sylow p-subgroup of $\langle P_1, P_2 \rangle$ containing the p-subgroup P_1. Continuing like this, we choose Q_{n+1} as $Q_{n+1} \in \mathrm{Syl}_p(\langle Q_n, P_{n+1} \rangle)$ containing Q_n. Then we get a chain $Q_1 \leq Q_2 \leq \cdots Q_n \leq Q_{n+1} \leq \cdots$. Define $Q := \cup Q_n$ and note that Q is a p-group. Since P_n is a p-subgroup and Q_n is a Sylow p-subgroup of $\langle Q_{n-1}, P_n \rangle$, we have $Q_n \supseteq P_n^g$ for some $g \in G$. As P_n has elementary abelian sections of order p^{sn}, so does P_n^g. So Q has elementary abelian sections of unbounded order as n gets arbitrarily large. Therefore, Lemma 5.1.2 implies that Q can not be Černikov.

Corollary 5.1.4 *Let G be a non-linear LFS-group and p a prime. Then there exists an infinite elementary abelian p-subgroup of G.*

Proof: By Theorem 5.1.3, there exists a p-subgroup Q of G which is not Černikov. Then, by [13, 1.G.6], Q contains an infinite elementary abelian p-subgroup and so does G.

Corollary 5.1.5 *Let G be a LFS-group. Then the following are equivalent.*

(a) *G is non-linear.*

(b) *For all prime p, there exists an infinite elementary abelian p-subgroup of G.*

(c) *There exist distinct primes p_1 and p_2 such that G has an infinite elementary abelian p_i-subgroup for $i = 1, 2$.*

Proof: (a) $\Rightarrow$ (b) This is Corollary 5.1.4.

(b) $\Rightarrow$ (c) Trivial.

(c) $\Rightarrow$ (a) Suppose for a contradiction that G is linear and let $G \leq \mathrm{GL}_{\mathbb{F}}(V)$ where V is a finite dimensional vector space over a field $\mathbb{F}$. Let $p \in \{p_1, p_2\}$ with $p \neq \mathrm{char}\,\mathbb{F}$ and let H be an infinite elementary abelian p-subgroup of G. Clearly, $H \cong C_p \times C_p \times \cdots$ and does not satisfy min. On the other hand, this gives a contradiction to the fact that a linear p-group over a field of characteristic different than p satisfies min condition, see [13, 1.L.3].

Corollary 5.1.6 *Let G be a LFS-group. Then G is infinite if and only if G has an infinite elementary abelian p-subgroup for some prime p.*

Proof: ($\Longleftarrow$) Obvious.

($\Longrightarrow$) If G is not linear then we are done by Corollary 5.1.5.

If G is linear, then by Theorem 1 (page 3) G is a group of Lie type defined over an infinite locally finite field $\mathbb{F}$. Let A be a long root subgroup in G. Then $A \cong (\mathbb{F}, +)$ and so A is an infinite elementary abelian p-subgroup of G.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] V. V. Belyaev, *Locally finite Chevalley groups,* in Studies in Group Theory, Urals Scientific Center of Academy of Sciences of USSR, Sverdlovsk (1984), pp. 39-50.

[2] A. V. Borovik, *Periodic linear groups of odd characteristic,* Dokl. Akad. Nauk. SSSR 266 (1982), pp. 1289-1291.

[3] R. W. Carter, *Simple Groups of Lie Type,* Wiley-Interscience, 1972.

[4] S. Delcroix and U. Meierfrankenfeld, *Locally Finite Simple Groups of 1-type,* J. Algebra 247 (2002) pp. 728-746.

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

[6] N. Flowers and U. Meierfrankenfeld, *On the center of maximal subgroups in locally finite simple groups of alternating type,* J. Group Theory 5 (2002), pp. 429-439.

[7] J. I. Hall, *Locally Finite Simple Finitary Groups,* in: Finite and Locally Finite Groups (Istanbul, 1994), eds. B. Hartley, G. M. Seitz, A. V. Borovik, R. M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 471 (1995), pp. 147-188.

[8] J. I. Hall, *Periodic simple groups of finitary linear transformations,* Ann. of Math. (2) 163 (2006), no. 2, pp. 445–498.

[9] B. Hartley, *Simple Locally Finite Groups,* in: Finite and Locally Finite Groups (Istanbul, 1994), eds. B. Hartley, G. M. Seitz, A. V. Borovik, R. M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 471 (1995), pp. 1-44.

[10] B. Hartley and G. Shute, *Monomorphisms and direct limits of finite groups of Lie type,* Quart. J. Math. (2) 35 (1984), pp. 49-71.

[11] K. Hoffman and R. Kunze, *Linear Algebra,* 2nd. Edition, Prentice-Hall Inc., 1971.

[12] G. Karpilovsky, *Field Theory: Classical Foundations and Multiplicative Groups,* Marcel Dekker, 1988.

[13] O. H. Kegel and B. A. F. Wehrfritz, *Locally Finite Groups,* North-Holland, Amsterdam, 1973.

[14] U. Meierfrankenfeld, *Non-finitary simple locally finite groups,* in: Finite and Locally Finite Groups (Istanbul, 1994), eds. B. Hartley, G. M. Seitz, A. V. Borovik, R. M. Bryant, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 471 (1995), pp. 189-212.

[15] P. Morandi, *Field and Galois Theory,* Springer-Verlag, New York, 1996.

[16] M. Suzuki, *Group Theory I,* Springer-Verlag, 1982.

[17] S. Thomas, *The classification of the simple periodic linear groups,* Arch. Math. 41 (1983), pp. 103-116.