# On generalized fixed point free automorphisms of finite groups

Dissertation von
Alexander Stein

Halle(Saale), Juli 1999

Betreuer:
Prof. G.Stroth, Martin Luther Universität Halle-Wittenberg

Gutachter:
Prof. G.Stroth, Martin Luther Universität Halle-Wittenberg
Prof. K.Strambach, Universität Erlangen-Nürnberg
Prof. U.Dempwolff, Universität Kaiserslautern

# Contents

# 1 Introduction

The problem underlying this work may be seen from various standpoints. From the standpoint of quasigroups a paper of FISCHER, [7] gives some interesting questions. FISCHER proved in 1963 that a finite distributive quasigroup $Q$ has a solvable inner automorphism group $G$. As from this inner automorphism group $G$ the quasigroup $Q$ can be recovered, the structure of $G$ defines the structure of $Q$, so if we understand the group $G$, we understand the distributive quasigroup $Q$. Now the conditions for a group to be the inner automorphism group of a distributive quasigroup are very hard to check (in general this conditions cannot be verified, even to verify this condition for a given group is very hard). So one drops leftdistributivity to get an easy condition on the groups. The remaining structure is a rightdistributive quasigroup. The problem (1) is now to prove FISCHER's result for rightdistributive quasigroups.

A more group theoretical problem is the following: Let $G$ be a group and $C = x^G, x \in G$ be a conjugacy class. How can we describe the action of $C$ on $C$ by conjugation. For instance a famous theorem of GLAUBERMAN says, if $C$ is a class of involutions an element $x \in C$ has either two fixed points on $C$ or $< C >$ is solvable. Define a directed graph $\Gamma$ on $C$ by defining edges as ordered pairs $(a, b), a, b \in C$ where $b = a^c$ for some $c \in C$. A very special case is if $\Gamma$ is a complete graph. (In this case the operation $a \times b := a^b$ on $C$ defines a quasigroup.) The problem (2) is now, for which groups this holds.

Another standpoint is the following one: Let $G$ be a finite group and $\alpha$ be a fixed point free automorphism on $G$. By ROWLEY, [13] we know that $G$ is solvable in this case, though the proof uses the classification of finite simple groups. In this case every element $x \in G$ is a commutator with $\alpha$. Define now a new type of automorphism by the condition, that the set of commutators with $\alpha$ has to form a transversal for $C_G(\alpha)$. Obviously if $C_G(\alpha) = 1$ this condition holds. As this condition also holds for the trivial case $C_G(\alpha) = G$, we exclude this case by demanding that $G = [G, \alpha]$. The problem (3) now is to generalize ROWLEY's result. From this point of view we see, that the classification of finite simple groups will play a central role in solving this problem.

Another approach is to ask for finite groups in which a conjugacy class $C$ is a transversal for a subgroup $U$. This problem is very hard if there is no connection between $U$ and $C$. So we restrict us to a canonical subgroup $U$, namely $C_G(x)$ for some $x \in C$. As then $G =< C > U$ we can restrict this case further to $G =< C >$. The problem (4) is now to describe the structure

of $G$, mainly the question whether $G$ is solvable or not.
Now all these approaches give rise to more or less the same problem which is handled in this work.

A personal thank goes to the people supporting and encouraging me, especially my parents and Prof. Stroth.
The author acknowledges the support of the DFG.

## 2 Notations

Under a group we understand a finite group unless otherwise stated.
The notation is mixed from various sources:
- from [1] for general group theoretic notations,
- from [8] for classical groups with their modules,
- from [14], [2] and [3] for algebraic groups of lie type , weyl groups and maximal tori,
- from [5] for group structures and extensions of groups and
- from [7] for terms related to quasigroups.

A special notation is $\mathrm{Aut}_G(X) := N_G(< X >)/C_G(X)$ for a subset $X \subset G$. The notation of classical simple groups (and some natural extensions) should be clear. The lie groups $A_n, B_n, C_n$ etc. refer always to the simple groups (if these exists), otherwise we assume that these groups are center free and have no $p'$-factor group. By groups $G$ of **type** $A_n, B_n, C_n$ etc. we refer to an extension of the simple group, which may include a center of $F^*(G)$ of $p'$-order and $|G : F^*(G)|$ of $p'$-order too. This last notation is mostly used for describing the isomorphism type of a levi complement which allows the inaccuracy (as these groups are well defined).

## 3 Distributive quasigroups

(1) **Definition:** Let $Q$ be a set and $*$ be a binary operation on $Q$. Call $Q$ a **quasigroup** iff for all $a, b \in Q$ the equations $a * x = b$ and $y * a = b$ have a solution $x$ respectively $y \in Q$.
(2) **Lemma:** *Let $Q$ be a set with a binary operation $*$. Then $Q$ is a quasigroup iff the* **lefttranslation** $\lambda_a(b) = a * b, \lambda_a : Q \mapsto Q$ *and the* **righttranslation** $\rho_a(b) = b * a, \rho_a : Q \mapsto Q$ *are both bijections on $Q$ for all $a \in Q$.*
(3) **Definition:** Let $Q$ be a quasigroup. Define $G_r(Q) =< \rho_a | a \in Q >$ and $G_l(Q) =< \lambda_a | a \in Q >$
(4) **Definition:** Let $Q$ be a Quasigroup.
$Q$ is a **rightdistributive** quasigroup iff the equation $(a*b)*c = (a*c)*(b*c)$ holds for all $a, b, c \in Q$.
$Q$ is a **leftdistributive** quasigroup iff the equation $a*(b*c) = (a*b)*(a*c)$ holds for all $a, b, c \in Q$.
$Q$ is a **distributive** Quasigroup iff $Q$ is both a rightdistributive quasigroup and a leftdistributive quasigroup.
(5) **Lemma:** *Let $Q$ be a leftdistributive resp. rightdistributive quasigroup. Then $G_l(Q)$ resp. $G_r(Q)$ is a group of automorphisms of $Q$.*
**Proof:** This is obvious.
(6) **Theorem:** [7](Fischer '63) *Let $Q$ be a finite distributive quasigroup. Then $G_r(Q)$ is solvable.*
Aim of the paper is the following
(7) **Theorem:** (main theorem I)*Let $Q$ be a finite rightdistributive quasigroup. Then $G_r(Q)$ is solvable.*
(8) **Lemma:** *Let $Q$ be a rightdistributive quasigroup and $a \in Q$.
Then $G_r(Q) = C_{G_r(Q)}(\rho_a)\rho_a^{G_r(Q)}$.*
**Proof:** (i): Let $b \in Q$. Then $bb = b$. If $bc = b$ then $b = c$:
$(bb)b = (bb)(bb)$ by the rightdistributivity. As $Q$ is a quasigroup the lefttranslation $\lambda_{bb}$ is a permutation on $Q$. But now $b$ and $bb$ have the same image which forces $b = bb$. So $bb = b$ for each $b \in Q$. If now $bc = b$ then $bc = b = bb$ and as $\lambda_b$ is a permutaion of $Q$ we have $b = c$.
(ii): $x \in C_{\mathrm{Aut}(Q)}(\rho_a) =: C \Leftrightarrow x(a) = a$:
If $x(a) = a$ then $x(\rho_a(b)) = x(ba) = x(b)x(a) = x(b)a = \rho_a(x(b))$ for each $b \in Q$. So $x \in C$. If $x \in C$ then $x(a) = x(aa) = x(\rho_a(a)) = \rho_a(x(a)) = x(a)a$. By (i) this forces $x(a) = a$.
(iii): $\rho_a^{G_r(Q)} = \{\rho_b : b \in Q\}$:
By the rightdistributivity we have $(ab)c = (ac)(bc)$ for each $a, b, c \in Q$. But

this means that $\rho_c(\rho_b(a)) = \rho_{\rho_c(b)}(\rho_c(a))$. Setting $d = \rho_c(a)$ (so $a = \rho_c^{-1}(d)$) we see that $\rho_c(\rho_b(\rho_c^{-1}(d))) = \rho_{\rho_c(b)}(d)$. As $\rho_c^{-1}$ is an automorphism on $Q$ we see that $d$ runs over $Q$ if $a$ runs over $Q$. So $\rho_b^{\rho_c} = \rho_{\rho_c(b)}$. Let now $c$ and $d$ arbitrary elements of $Q$. As $Q$ is a quasigroup there is an $e \in Q$ with $c = de$. Then $\rho_d^{\rho_e} = \rho_c$ and so the righttranslations form a conjugacy class of $G_r(Q)$. Let $g \in G_r(Q)$ and $b = g(a)$. As $Q$ is a quasigroup there is a $c \in Q$ with $b = ac$. So $(\rho_c^{-1})(b) = a$ and $(\rho_c^{-1}g)(a) = a$ which means $h := \rho_c^{-1}g \in C_{G_r(Q)}(\rho_a)$ by (ii). Now $g = \rho_c h = h\rho_c^h$ and by (iii) we have that $\rho_c$ is conjugate to $\rho_a$, so the lemma is proven.

## 4 $C^3P$- and $C^2P-$ groups

(1) **Definition:** Let $G$ be a group. Call $G$ a $C^3P$**-group** or $CCCP$**-group (Centralizer Conjugacy Class Product)** iff $G = C_G(g)g^G$ for a $g \in G$
(2) **Lemma:** *Let $G$ be a $C^3P-$group for $g \in G$. Then the set $g^G$ is a right-distributive quasigroup with the operation $a * b = a^b$.*
**Proof:** If $G = C_G(g)g^G$ then also $G^h = (C_G(g))^h(g^G)^h$, that is $G = C_G(g^h)g^G$. So let $a, b \in g^G$. Then there is a $c \in G$ with $a^c = b$ and $c = hx$ with $x$ conjugate to $g$ and $h \in C_G(a)$. So for all $a, b \in g^G$ there is an $x \in g^G$ with $a^x = b$.
Set $y = b^{a^{-1}}$ then for all $a, b \in G$ there is a $y$ with $y^a = b$. So the set $g^G$ is a quasigroup with the operation $*$.
So let $a, b, c \in g^G$. As $(a * b) * c = (a^b)^c = a^{bc} = a^{cb^c} = (a * c) * (b * c)$ the operation is rightdistributive.
(3) **Definition:** Let $G$ be a group and $\alpha \in \mathrm{Aut}(G)$.
Call $G$ a $\alpha$**-CCP-group (Centralizer Commutator Product)** iff
$G = C_G(\alpha)\{[g, \alpha] | g \in G\}$.
Call $G$ a **strong** $\alpha$-CCP-group iff $G$ is an $\alpha$-CCP-group and $G = [G, \alpha]$.
(4) **Lemma:** *Let $G$ be a $C^3P$-group for $g \in G$. Then $G$ is an $\alpha$-CCP-group with $\alpha = i_g$, the inner automorphism induced by $g$.*
*Let $H$ be an $\alpha$-CCP-group and $g \in G$ with $\alpha(x) = x^g$ for all $x \in G$. Then $G$ is a $C^3P$-group for $g$.*
**Proof:** By definition $G = C_G(g)g^G$, so $G = g^G C_G(g)$. (If $x = hg^f$ then $x = hg^f h^{-1}h = g^{fh^{-1}}h$.) So for $x \in G$ we can write $(x^{-1})^{g^{-1}} = g^f h$ with $h \in C_G(g)$. Then $x^{g^{-1}} = h^{-1}(g^{-1})^f$ and $x = (g^{-1}h^{-1})((g^{-1})^f g) = (hg)^{-1}[f, g]$ with $(hg)^{-1} \in C_G(g)$, so $G$ is an $\alpha$-CCPgroup for $\alpha = i_g \in \mathrm{Inn}(G)$.
On the other side let $G = C_G(\alpha)\{[x, \alpha] | x \in G\}$. Then for $y \in G$ we can write $(y^{-1})^g = h[f, \alpha] = h[f, g] = h(g^{-1})^f g$ with $h \in C_G(\alpha) = C_G(g)$. Thus

$y^{-1} = gh(g^{-1})^f$ and $y = g^f h^{-1} g^{-1} = (gh)^{-1} g^{f(gh)^{-1}}$ with $(gh)^{-1} \in C_G(g)$.

(5) **Lemma:** *Let $G$ be an $\alpha$-CCP-group. If $[g,\alpha] \in C_G(\alpha)^h$ for some $g, h \in G$, then $[g,\alpha] = 1$.*

**Proof:** This follows immediately from the definition of an $\alpha$-CCP-group.

(6) **Lemma:** *Let $G$ be an $\alpha$-CCP-group and $U \leq G$ with $U^\alpha = U$. Then $U$ is an $\alpha$-CCP-group and $\{[u,\alpha] | u \in U\} = \{[g,\alpha] | g \in G\} \cap U$.*

**Proof:** The Definition of an $\alpha$-CCP-group means that each coset $C_G(\alpha)x$ for $x \in G$ contains exactly one element $y = [g,\alpha]$ for some $g \in G$ (As there are exactly as many different commutators $[g,\alpha]$ as cosets of $C_G(\alpha)$.) Now each coset of $C_U(\alpha)$ lies in a unique coset of $C_G(\alpha)$, thus contains at most one commutator $[g,\alpha]$ with $g \in G$. But in $U$ the number of commutators $[u,\alpha]$ for $u \in U$ is equal to the number of cosets of $C_U(\alpha)$. Thus each coset $C = C_U(\alpha)v$ of $U$ with $v \in U$ contains exactly one commutator $[g,\alpha]$ for some $g \in G$ and there is an $u \in U$ with $[g,\alpha] = [u,\alpha]$.

(7) **Corollary:***Let $G$ be an $\alpha$-CCP-group. Then $[G,\alpha]$ is a strong $\alpha$-CCP-group.*

**Proof:** As $[G,\alpha]$ is $\alpha$-invariant we can apply (5) and see, that in fact $[G,\alpha] = [G,\alpha,\alpha]$.

(8) **Lemma:** *Main Theorem I holds iff the following theorem holds.*

(9) **Theorem:** (Main Theorem II) *Let $G$ be a strong $\alpha$-CCP-group. Then $G$ is solvable.*

**Proof:** of Lemma (8): Let $Q$ be a rightdistributive quasigroup. By (3.8) the group $G_r(Q)$ is a $C^3P$-group for a righttranslation $\rho_a$. Then $G_r(Q)$ is an $\alpha$-CCP-group for $\alpha = i_{\rho_a}$.

As $G_r(Q) =< \rho_a^{G_r(Q)} >$ we can write $G_r(Q) = [G_r(Q),\alpha] < \alpha >$. By (7) $[G_r(Q),\alpha]$ is a strong $\alpha$-CCP-group. If now (9) holds we see that $G_r(Q)$ is solvable.

On the other hand let $G$ be a strong $\alpha$-CCP-group. Then set $H = G :< \alpha >$, the semidirect Product of $G$ with $< \alpha >$. As $G$ is a strong $\alpha$-CCP-group we get $H =< \alpha^G >=< \alpha^H >$.

By (4) we see that $H$ is a $C^3P$-group for $\alpha$. So by (2) we can construct a rightdistributive quasigroup $Q$ on the set of all conjugates of $\alpha$. If the main theorem holds, we see that $G_r(Q)$ is solvable. A righttranslation $\rho_\alpha$ is the map with $\rho_\alpha(\beta) = \beta^\alpha$. Thus $\rho_\alpha$ is the inner automorphism of $H$ induced by $\alpha$ and $G_r(Q) = \mathrm{Inn}(H) = H/Z(H)$. Thus $H$ is solvable and hence is $G$.

(10) **Lemma:** *Let $G$ be an $\alpha$-CCP-group and $N$ a normal subgroup with $N^\alpha = N$. Then $G/N$ is an $\alpha$-CCP-group with $C_{(G/N)}(\alpha) = C_G(\alpha)N/N$.*

**Proof:** For $Nx \in G/N$ we can write $Nx = NhN[g,\alpha] = NhNg^{-1}Ng^\alpha =$

$Nh(Ng)^{-1}(Ng)^\alpha$ if $x = h[g,\alpha]$ with $h \in C_G(\alpha)$. Thus $G/N$ is an $\alpha$-CCP-group. Assume $(Ng)^\alpha = Ng$ which means $Ng \in C_{G/N}(\alpha)$. Then $N[g,\alpha] = N$. By (6) there is an $n$ with $[n,\alpha] = [g,\alpha]$, but $[g,\alpha] = [(gn^{-1})n,\alpha] = [gn^{-1},\alpha]^n[n,\alpha]$, so $gn^{-1} \in C_G(\alpha)$. Thus $Ng = gN = (gn^{-1})N$ so $Ng \in C_G(\alpha)N/N$. Thus $C_{G/N}(\alpha) \le C_G(\alpha)N/N$. As the other inclusion is obvious the lemma holds.

(11) **Lemma:** *Let $G$ be a minimal counterexample to Theorem (9).*
*Then $G$ is a direct product of simple groups and $\alpha$ is transitive on the factors.*

**Proof:** Let $F = F(G)$ be the Fitting subgroup of $G$. As $G$ is nonsolvable and $F$ is solvable also $G/F$ is nonsolvable and by (10) a counterexample, thus by minimality we have $F = 1$.

So let $N = \mathrm{Soc}(G)$ the product of all minimal normal subgroups of $G$. $N$ is a direct product of simple groups (as $F = 1$), hence nonsolvable and $[N,\alpha] \ne 1$. (Otherwise $[G,N,\alpha] = 1 = [N,\alpha,G]$, so $[\alpha,G,N] = [G,N] = 1$) But $[N,\alpha]$ is nonsolvable as $N$ contains no solvable normal subgroups. But then $[N,\alpha]$ is a counterexample, thus by minimality we have $[N,\alpha] = G = N$ and $G$ is a direct product of simple groups. By minimality we see that $\alpha$ is transitive on the components as claimed.

(12) **Lemma:** *Let $G$ be a direct product of $n$ groups $L_i$ isomorphic to a group $L$ and $\alpha$ be transitive on the factors. If $G$ is an $\alpha$-CCP-group then each factor $L_i$ is an $\beta$-CCP-group for $\beta = \alpha^n$ and $(n, |C_{L_1}(\beta)|) = 1$.*

**Proof:** Define the indices such that $L_i^\alpha = L_{i+1}$ for $i < n$ and $L_n^\alpha = L_1$.
For $g \in G$ write $g = (g_1, g_2, \ldots, g_n)$ iff $g_i \in L_1$ and $g = g_1 g_2^\alpha \cdots g_n^{\alpha^{n-1}}$.
A group $G$ is not an $\alpha$-CCP-group iff there are $f, g \in G$ with $1 \ne [g,\alpha] \in C_G(\alpha)^f$: If $G$ is not an $\alpha$-CCP-group there are $a, b \in G$ with $[a,\alpha] \ne [b,\alpha]$ and $C_G(\alpha)[a,\alpha] = C_G(\alpha)[b,\alpha]$. As $[a,\alpha] = [(ab^{-1})b,\alpha] = [ab^{-1},\alpha]^b[b,\alpha]$ we see that $[ab^{-1},\alpha]^b \in C_G(\alpha)$, thus $[ab^{-1},\alpha] \in C_G(\alpha)^{b^{-1}}$, but as $[a,\alpha] \ne [b,\alpha]$ we have that $[ab^{-1},\alpha] \ne 1$. On the other side if $[g,\alpha] \in C_G(\alpha)^f$ then $[g,\alpha]^{f^{-1}} \in C_G(\alpha)$ and because $[gf^{-1},\alpha] = [g,\alpha]^{f^{-1}}[f^{-1},\alpha]$ we see that $C_G(\alpha)[gf^{-1},\alpha] = C_G(\alpha)[f^{-1},\alpha]$, but as $1 \ne [g,\alpha]$ we get $[gf^{-1},\alpha] \ne [f^{-1},\alpha]$ and so $G$ is not an $\alpha$-CCP-group.
We show now that if $L_1$ is not a $\beta$-CCP-group also $G$ is not an $\alpha$-CCP-group. Assume $[g,\beta] \in C_{L_1}(\beta)^f$. Set $g_1 = (g, g, g, \ldots, g)$.
Then $[g_1,\alpha] = ([g,\beta], 1, 1, \ldots, 1)$. Set $g_{k+1} = g_1^{\alpha^k}$ for $k < n$. Then $[g_k,\alpha] = [g_1,\alpha]^{\alpha^{k-1}} \in L_k$. Now set $h = g_1 g_2 \cdots g_n$. Let $\sim$ be the $G$-conjugate relation and for $J \subset \{1, 2, \ldots, n\} =: I$ set $L_J = \prod\limits_{j \in J} L_j$.
Claim: Let $E_k \subset I, k = 1, 2$ with $E_1 \cap E_2 = \emptyset$ and $g_1, g_2 \in G$ with

$[g_k,\alpha] \sim c_k \in L_{E_k}$. Then $[g_1g_2,\alpha] \sim c_1c_2 \in L_{E_1\cup E_2}$:
$[g_1g_2,\alpha] = [g_1,\alpha]^{g_2}[g_1,\alpha]$ , but $[g_1,\alpha] \in L_{E_1}$, so there is a $d \in L_{E_1}$ with $[g_1,\alpha]^{g_2} = [g_i,\alpha]^d$. But then $[g_1g_2,\alpha]$ =$[g_1,\alpha]^d[g_2,\alpha]^d$ as $E_1 \cap E_2 = \emptyset$. Now there are $d_k \in L_{E_k}$ with $[g_i,\alpha]^{dd_k}$ =$c_k$. Then $[g_1g_2,\alpha]^{dd_1d_2}$ =$c_1c_2$. Clearly $c_1c_2 \in L_{E_1\cup E_2}$ so the claim holds. Now we see that $[h,\alpha] \sim [g_1,\alpha][g_2,\alpha] \cdots [g_n,\alpha]$ and as $[g_1,\alpha] = [g,\beta] \sim [g,\beta]^{f^{-1}} =: c \in C_{L_1}(\beta)$ we have $[h,\alpha] \sim cc^\alpha \cdots c^{\alpha^{n-1}} = (c,c,\ldots,c) \in C_G(\alpha)$. Thus $G$ is not an $\alpha$-CCP-group. Assume now that $1 \neq d = (n, |C_{L_1}(\beta)|)$. Let $r$ be a prime dividing $d$. Then $C_{L_1}(\beta)$ contains an element $x$ of order $r$. Set $x_f = (x, x^2, x^3, \ldots x^n)$. We have $x_f^\alpha = x_f(x^{-1}, x^{-1}, x^{-1}, \ldots x^{-1})$ and so $[x_f,\alpha] \in C_G(\alpha)$, so $G$ is not an $\alpha$-CCP-group.

(13) **Lemma:** *Let $G$ be a minimal counterexample to Theorem (9). Then $G$ is simple.*

**Proof:** By (11) we have that $G$ is a direct product of say $n$ factors on which $\alpha$ acts transitively. Set $\beta = \alpha^n$. Applying (12) we get either $\beta = 1$ or $n = 1$. Otherwise our counterexample is not minimal.

So let $\beta = 1$. Using the notation of (12) we see that for each subgroup $U \leq L_1$ there is a subgroup $U^{<\alpha>} := UU^\alpha \cdots U^{\alpha^{n-1}}$ which is $\alpha$-invariant. As our counterexample is minimal we see that each proper subgroup of $L_1$ must be solvable. So $L_1$ is a minimal simple group which were classified by Thompson. So let $n$ be even. Then $L_1$ contains an involution $i$. Setting $g = (i,1,i,1,\ldots,i,1)$ we get $[g,\alpha] = (i,i,i,i,\ldots,i,i) \in C_G(\alpha)$, so $G$ is not an $\alpha$-CCP-group.

If $n$ is odd there are involutions $i, j \in L_1$ such that $i \sim j \sim ij$. Setting $g = (1,i,j,i,j,\ldots i,j)$ we get $[g,\alpha] = (j,i,ij,ij,ij,\ldots,ij,ij)$ which is conjugate to $(i,i,i,i,i,\ldots,i,i) \in C_G(\alpha)$ so again $G$ is not an $\alpha$-CCP-group.

(14) **Lemma:** *Let $G$ be a minimal counterexample to Theorem (9). Then $C_G(\alpha) \neq 1$.*

**Proof:** This is a theorem by Rowley [13] which also uses the classification of finite simple groups.

(15) **Lemma:** *Let $G$ be a group and $\phi : G \mapsto \mathrm{Inn}(G) \leq \mathrm{Aut}(G), \phi(g) = i_g$ with $i_g(x) = g^{-1}xg$ be the natural homomorphism from $G$ into $\mathrm{Aut}(G)$ and $\alpha \in \mathrm{Aut}(G)$. Then $\phi(g)^\alpha = \phi(g^\alpha)$ for each $g \in G$.*

**Proof:** Let $t \in G$. Then $\phi(g^\alpha)(t) = (g^\alpha)^{-1}tg^\alpha$: As $(\phi(g)^\alpha)(t) = (\alpha^{-1}\phi(g)\alpha)(t)$ $= \alpha(i_g(\alpha^{-1}(t))) = \alpha(g^{-1}t^{\alpha^{-1}}g) = \alpha(g^{-1})t\alpha(g) = (g^\alpha)^{-1}tg^\alpha$ the lemma is proven.

(16) **Corollary:***Let $g \in G$ and $\alpha \in \mathrm{Aut}(G)$. Then $i_{[g,\alpha]} = [i_g,\alpha]$. Especially $[g,\alpha] \in Z(G) \Leftrightarrow [i_g,\alpha] = 1$.*

**Proof:** By (15) we have $i_{[g,\alpha]} = \phi([g,\alpha]) = \phi(g^{-1}g^{\alpha}) = (\phi(g))^{-1}(\phi(g))^{\alpha} = [\phi(g),\alpha] = [i_g,\alpha]$. As $i_{[g,\alpha]} = 1$ iff $[g,\alpha] \in Z(G)$ the second statement holds.

(17) **Lemma:** *Let $G$ be an $\alpha$-CCP-group with automorphism $\alpha$.*
*Set $H =< \mathrm{Inn}(G), \alpha >\leq \mathrm{Aut}(G)$. Then $H$ is an $\alpha$-CCP-group.*

**Proof:** Let $h \in H$. Then $h = \alpha^k g$ for some $g \in \mathrm{Inn}(G)$ as $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$ and some integer $k$. Now $g = i_f$ for some $f \in G$ and $f = c[e,\alpha]$ with $e \in G$ and $c \in C_G(\alpha)$. But by (14) and (15) we have then $g = i_c i_{[e,\alpha]} = i_c[i_e,\alpha]$. So $h = (\alpha^i i_c)[i_e,\alpha]$. As $[c,\alpha] = 1$ we have $[i_c,\alpha] = 1$, so $\alpha^k i_c \in C_H(\alpha)$ and so $H$ is an $\alpha$-CCP-group as claimed.

(18) **Lemma:** *Let $G$ be a minimal counterexample to Theorem (9) and set $H =< \mathrm{Inn}(G), \alpha >$. If $\alpha$ is conjugate to $\alpha^k$ in $H$, then $\alpha = \alpha^k$. Furthermore $\alpha$ is not an involution.*

**Proof:** : Assume $\alpha^h = \alpha^k$ for some $h \in H$ and some integer $k$ with $\alpha \neq \alpha^k$. Then $1 \neq (\alpha^{-1})^h\alpha = [h,\alpha] = \alpha^{1-k} \in C_H(\alpha)$. But by (16) $H$ is an $\alpha$-CCP-group and so we get a contradiction. If now $\alpha$ is an involution we get by the $Z^*$-theorem of Glauberman that $C_G(\alpha)$ contains a conjugate $\beta = \alpha^g$ for some $g \in H$. As again $1 \neq (\alpha^{-1})^g\alpha = [g,\alpha] \in C_G(\alpha)$ we get a contradiction to (16) as before.

(19) **Lemma:** *Let $G$ be a $p$-group and $\alpha \in \mathrm{Aut}(G)$ of $p$-order. If $G$ is an $\alpha$-CCP-group then $\alpha = 1$.*

**Proof:** Set $C = C_G(\alpha)$ and assume $C \neq G$. Then $N := N_G(C) > C$ and $\alpha$ operates on $\bar{N} = N/C$. As $\alpha$ is of $p$-order, $C_{\bar{N}}(\alpha) \neq 1$. But $C_G(\alpha)$ has to cover this factor group by (10), a contradiction.

For completeness we state the following

(20) **Lemma:** *Let $G$ be a group. Then $G$ is a $C^3P$-group for $g \in G$ iff $N =< g^G >$ is a $C^3P$-group for $g \in N$ and $G = C_G(g)N$.*
*$G$ is an $\alpha$-CCP-group iff $M = [G,\alpha]$ is an $\alpha$-CCP-group and $G = MC_G(\alpha)$.*

**Proof:** Let $G$ be a $C^3P$-group for $g \in G$, So $G = C_G(g)g^G$ by definition. Therefore $G = C_G(g)N$. Let now $e = g^f$ for some $f \in G$. Then $f = f_1f_2$ with $f_1 \in C_G(g)$ and $f_2 \in N$, so $e = g^{f_2}$ and $g^G = g^N$. As now $g^G$ is a transversal, the cosets of $C_N(g)$ contain at most one element of $g^G$, but there are as many cosets of $C_N(g)$ in $N$ as elements in $g^G$, so each coset contains exactly one element, thus $N = C_N(g)g^N$ and $N$ is a $C^3P$-group for $g \in N$.

Let now $N = C_N(g)g^N$ and $G = C_G(g)N$. Then $g^N = g^G$ and therefore $G = C_G(g)C_N(g)g^N = C_G(g)g^G$ and so $G$ is $C^3P$-group for $g \in G$.

If now $G$ is an $\alpha$-CCP-group we have by (7) that $[G,\alpha]$ is a (strong) $\alpha$-CCP-group and by definition $G = C_G(\alpha)M$.

If $M$ is an $\alpha$-CCP-group and $G = C_G(\alpha)M$ then $\{[g,\alpha]|g \in G\} = \{[m,\alpha]|m \in M\}$ as for $g \in G$ we have $g = hm$ for some $h \in C_G(\alpha)$ and $m \in M$. Therefore $G = C_G(\alpha)M = C_G(\alpha)C_M(\alpha)\{[m,\alpha]|m \in M\} = C_G(\alpha)\{[g,\alpha]|g \in G\}$ and so $G$ is an $\alpha$-CCP-group.

# 5 Some tools

## 5.1 Further properties of $\alpha$-CCP-groups

(1) **Lemma:** *Let $G$ be an $\alpha$-CCP-group, $U \leq C_G(\alpha)$ and $N \leq G$ with $[U,N] = U$ and $N^\alpha = N$. Then there is a $D \leq C_G(\alpha)$ with $C_G(U)D = C_G(U)N$.*
*Especially if $C_G(U) \leq U$ then $[N,\alpha] = 1$.*
**Proof:** Applying the three subgroup lemma for $[U,\alpha,N] = 1 = [N,U,\alpha]$. we get $[\alpha,N,U] = 1$, so $[N,\alpha] \leq C_G(U)$ and $\alpha$ trivial on $NC_G(U)/C_G(U)$. Applying (1.7) on the group $M = C_G(U)N$ we get for $D = C_M(\alpha)$ that $C_G(U)D = C_G(U)N$.
(2) **Lemma:** *Let $G$ be an $\alpha$-CCP-group and $x \in C_G(\alpha)$ of prime order $r$. If $\mathrm{Aut}_G(x) \neq 1$ there is a prime $s$, such that* $s$divides$|C_G(\alpha)|$ *($s$ divides $|\mathrm{Aut}_G(x)|$).*
**Proof:** Set $U =< x >$, $N = N_G(U)$ and apply (1).
(3) **Lemma:** *Let $G$ be a dihedral group of order $2^n, n > 2$ or $\Sigma_4$. Assume $G$ is an $\alpha$-CCP-group. Then $[G,\alpha] = 1$.*
**Proof:** Let $G = D_{2^n}, n > 2$ and $T$ be the cyclical subgroup of index 2. Then $[G,\alpha] \leq T$. Set $C = C_T(\alpha)$ and assume $C \neq T$. Then there is a $t \in T - C$ with $t^2 \in C$. But then $t^{-1}t^\alpha \in C$ as $t^\alpha$ is an odd power of $t$ and $t^2 \in C$. Then $G$ is not an $\alpha$-CCP- group, so $T = C$ and $[T,\alpha] = 1$. But $[G,\alpha] \leq T \leq C_G(\alpha)$, so $[G,\alpha] = 1$ as claimed.
Now let $G = \Sigma_4$. As $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ we get $[G,\alpha] \leq G'$. But $G = [G,\alpha]C_G(\alpha)$, so $C_G(\alpha) \not\leq A_4$. But $\alpha$ cannot be a transposition or a cycle of length 4: Otherwise $\alpha$ would fix some involution $i$ in $V_4$ and interchange the both remaining involutions, making $i$ a commutator, which is a contradiction to $G$ an $\alpha$-CCP-group. If $\alpha$ is an involution of $V_4$ there is an element $x$ of order 3 such that $[x,\alpha] \in \mathrm{A}_4$ has order 2, thus commuting with $\alpha$ which is again a contradiction. If finally $\alpha$ is a three-cycle then $G \neq [G,\alpha]C_G(\alpha)$, a contradiction. So $\alpha = 1$.
(4) **Lemma:** *Let $G$ be a dihedral group of Order $n \neq 4$. Then there is an $S \in \mathrm{Syl}_2(G)$ with $S \leq C_G(\alpha)$.*
**Proof:** Assume $n > 4$. Let $T$ be the cyclical subgroup of index 2. Then

$[G, \alpha] \leq T$, so as $G = [G, \alpha]C_G(\alpha)$ we get an involution $i$ with $G =< T, i >$ and $[i, \alpha] = 1$. Let $S_0$ be a Sylow-2-subgroup of $T$. Then $S_0 \lhd G$ and $S :=< S_0, i >$ is a Sylow-2-subgroup of $G$. which is $\alpha$-invariant. By (3) we get $[S, \alpha] = 1$ except $|S_0| = 2$. But then $S_0 =< j >$, $j$ the central involution of $G$. So $[j, \alpha] = 1$ and thus $[S, \alpha] = [< i, j >, \alpha] = 1$.

## 5.2 Semisimple elements in algebraic groups

In the following paragraph we look at semisimple elements in a finite group $H$ of lie type from the standpoint of algebraic groups as discribed for instance in [2] or [14].

(1) **Notations:**Let $G$ be a simple simply connected algebraic group in characteristic $p$. Let $\sigma$ be an endomorphism of $G$ onto $G$ such that $G_\sigma$, the group of fixed points is finite (a so called frobenius map). From the theory of algebraic groups we know the following:

- $G_\sigma$ is a central extension of a finite group of lie type and conversely for each finite simple group of lie type $H$ exists a central extension $\hat{H}$ such that $\hat{H} \cong G_\sigma$ for some simple simply connected algebraic group $G$ and a Frobenius map $\sigma$ of $G$.
- $G$ contains a $\sigma$-stable Borel subgroup $B$ which contains a $\sigma$-stable (and therefore maximally split) maximal torus $T_0$.
- let $T$ be a $\sigma$-stable maximal torus of $G$. Then $T$ can be obtained by "twisting" $T_0$ with an element $w \in W = N_G(T_0)/T_0$ (the Weyl group) which means that $\sigma$ operates on $T$ as $w\sigma$ on $T_0$. The element $w$ is unique up to $\sigma$-conjugacy (define in [2],Prop. 3.3.2) and for each $\sigma$-conjugacy class there are $\sigma$-stable maximal tori obtained from $T_0$ by twisting with $w$.

Let $x \in G_\sigma$ be a semisimple element. Then the following holds:

- $C_G(x)$ is closed,connected,reductive and $\sigma$-stable by [14] II,3.9
- $C_G(x)$ contains a $\sigma$-stable maximal torus $T$ by [14] II,1.1.
- $C_{G_\sigma}(x) = (C_G(x))_\sigma$. Thus $C_{G_\sigma}(x)$ is either a central product of finite groups of lie type in characteristic $p$ or $T$ is the only maximal torus of $G$ containing $x$. Denote this last case as the "unique torus case". By [2],Prop. 3.6.1 and 3.6.5 we see in this case that $N_{G_\sigma}(T_\sigma)/T_\sigma \cong C_{W,\sigma}(w)$ where $w \in W$ is the element such that $T$ is obtained from $T_0$ by twisting with $w$. ($C_{w,\sigma} = \{u : u \in W | uw\sigma = w\sigma u\}$)

(2) **Lemma:** *Let $G$ as in (1) but assume that $W = W(G)$ contains a unique involution in its centre. (Thus $G$ is of type $A_1$, $B_n$, $C_n$, $D_{2n}$, $E_7$, $E_8$, $F_4$ or $G_2$). Let $\sigma$ be as in (1). Then each semisimple element of $G_\sigma$ is inverted by some element in $G_\sigma$.*

**Proof:** Let $x \in G_\sigma$ be a semisimple element. By (1) there is a $\sigma$-stable maximal torus $T$ containing $x$. Then $N_G(T)/T \cong W$. Let $Z$ be the preimage of $Z(W)$ (such that $T$ is of index 2 in $Z$). Each element of $Z - T$ acts as -1 on $T$, thus inverting the whole torus. We show now that $G_\sigma$ contains elements of this coset: Let $z_1 \in Z$. Then $\sigma(z_1) = z_1 t$ with $t \in T$. By the LANG-STEINBERG theorem and the connectedness of $T$ we get a $t_1 \in T$ with $t = t_1 \sigma(t_1)^{-1}$. Then $\sigma(z_1 t_1) = \sigma(z_1)\sigma(t_1) = z_1 t_1$ and $z_1 t_1$ is the element of $G_\sigma$ inverting $x$.

(3) **Lemma:** *Let $G = \mathrm{SL}_n(q), n > 1$, $\mathrm{SU}_n(q), n > 1$ odd or $\Omega^-_{2n}(q), n > 3$ odd and $x \in G$ an element of prime order $r$ acting irreducibly on the natural module $V$. Then $n$ divides $|\mathrm{Aut}_G(x)|$.*

**Proof:** Let $V$ be the natural $G$-module over the finite field $\mathrm{GF}(q_1)$. ($q_1 = q$ in the linear and orthogonal case and $q_1 = q^2$ in the unitary case.) As $x$ acts irreducibly on $V$ we see that $d_{q_1}(r) = n$. Thus the $r$ part of $\mathrm{GL}(V)$ is the $r$-part of $\Phi_n(q_1)$. Especially is this the $r$-part of $q^n - 1$ in the linear case and the $r$-part of $q^n + 1$ in the orthogonal and unitary case.

First let $G = \mathrm{SL}_n(q)$. Let $K = \mathrm{GF}(q^n)$ and $k = \mathrm{GF}(q)$. Then $K$ is an $n$-dimensional vectorspace over $k$ and w.l.o.g. we may assume that $V = K$. For $a \in K^*$ and $\phi \in \mathrm{Gal}(K : k)$ we define the following maps: $g_a : K \mapsto K, g_a(b) = b * a$ and $g_\phi : K \mapsto K, g_\phi(b) = b^\phi$. Then these maps are $k$-linear. Set $C =< g_a | a \in K^* >$ and $N =< C, g_\phi | \phi \in \mathrm{Gal}(K/k) >$. Then $C$ is a cyclical subgroup of $\mathrm{GL}_n(q)$ of order $q^n - 1$ and $N/C$ is a cyclical subgroup of $\mathrm{GL}_n(q)$ of order $n$. By Schur's lemma follows that $\det(g_a) = N^K_k(a)$ and as the norm map is surjective for finite fields we see that $|\det(C)| = q-1$. Thus $N_1 = \ker(\det|_N)$ is of type $\frac{q^n-1}{q-1} : n$. As $d_q(r) > 1$ we see that $N_1$ contains a Sylow-$r$-subgroup of $\mathrm{SL}_n(q)$ and therefore we may assume that $x \in N_1$. As $d_q(r) = n$, $x$ does not lie in a subfield of $K$, so the full galois group $\mathrm{Gal}(K : k)$ acts on $< x >$ nontrivially and therefore $n$ divides $|\mathrm{Aut}_G(x)|$.

Let now $G = \mathrm{SU}_n(q)$. Let $k = \mathrm{GF}(q) < K = \mathrm{GF}(q^2), k < l = \mathrm{GF}(q^n)$ and $K, l < L = \mathrm{GF}(q^{2n})$. For $a \in K$ denote with $\bar{a} := a^{q^n}$, such that $\bar{\cdot}$ is the automorphism of $L$ of order 2. Note that its restriction to $K$ is of order 2 too as $|L : K| = n$ is odd. Define the map $f : L \times L \mapsto K$ by $f(b, c) = \mathrm{Tr}^L_K(b\bar{c})$. It is easy to see that $f$ is a nondegenerated unitary form and as all such forms over the same vectorspace (and the same field extension) are isometric we may assume that $\mathrm{GU}_n(q) = \mathrm{Stab}(f)$. For $a \in L$ and $\phi \in \mathrm{Gal}(L : K)$ let $g_a$ and $g_\phi$ as defined above. We show now which of these elements are actually elements of $\mathrm{GU}_n(q)$: Assume $f(b, c) = f(b^{g_a}, c^{g_a}) = f(ba, ca)$. Then $\mathrm{Tr}(b\bar{c}(1 - a\bar{a})) = 0$ for all $b, c \in L$, which means that $L(1 - a\bar{a}) \leq \ker\mathrm{Tr}$. Now $\mathrm{Tr}$ is a nontrivial map and therefore $\ker\mathrm{Tr}$ a nontrivial subspace of $L$. But on the other hand $L$ is a field therefore the only ideal containing kerTr is the 0-ideal forcing $a\bar{a} = 1$. Now $a\bar{a} = N_l^L(a)$ and as $N_l^L$ is an epimorphism we have that $X = \{a \in L | a\bar{a} = 1\}$ is a subgroup of $L^*$ of order $q^n + 1$. Now we set $C =< g_a | a \in X >$. For $\phi \in \mathrm{Gal}(L : K)$ we have $f(b^\phi, c^\phi) = \mathrm{Tr}((b\bar{c})^\phi) = \mathrm{Tr}(b\bar{c})^\phi = \mathrm{Tr}(b\bar{c}) = f(b, c)$ and therefore these elements are always contained in $\mathrm{GU}_n(q)$. Setting $N =< C, g_\phi | \phi \in \mathrm{Gal}(L : K) >$ we get a subgroup of $\mathrm{GU}_n(q)$ of type $(q^n+1) : n$. Again for $g_a$ we have $\det(g_a) = N_K^L(a)$ and as $N_K^L$ is surjective we have that $|\det(C)| = (|C|, q^2-1) = q+1 = |\det(\mathrm{GU}_n(q))|$ and therefore $\mathrm{SU}_n(q)$ contains a subgroup $N_1$ of type $\frac{q^n+1}{q+1} : n$. As $N_1$ contains a Sylow-$r$-subgroup of $\mathrm{SU}_n(q)$ we may assume that $x \in N_1$ and as $d_{q^2}(r) = n$ (as $x$ acts irreducibly on $V$) we see that $\mathrm{Gal}(L : K)$ acts nontrivially on $< x >$, thus $n$ divides $\mathrm{Aut}_G(x)$.

Finally let $G = \Omega_{2n}^-(q)$ and $k, K, l, L$ as in the unitary case. For $a \in L$ define $Q : L \mapsto k$, $Q(a) = \mathrm{Tr}_k^l(a\bar{a})$. With some calculations one can see that $Q$ is a nondegenerated quadratic form of minus type over the $2n$-dimensional $k$-space $L$. As all such quadratic forms are isometric we may assume that $O_{2n}^-(q) = \mathrm{Stab}(Q)$. As $n$ is odd it follows that $Q(x) = f(x, x)$ for the unitary form $f$ already defined. Thus $\mathrm{GU}_n(q) \leq O_{2n}^-(q)$ in this case. By Sylow's theorem we may assume that $x$ is contained in a subgroup of type $\mathrm{GU}_n(q)$ and therefore $n$ divides $|\mathrm{Aut}_G(x)|$ in $O_{2n}^-(q)$. But $\Omega_{2n}^-(q) = O^2(O_{2n}^-(q))$ and $n$ is odd, therefore $n$ divides $|\mathrm{Aut}_G(x)|$ already in $\Omega_{2n}^-(q)$ as claimed.

**Remark:**The embedding of the subgroup $\frac{q^n-1}{q-1} : n$, $\frac{q^n+1}{q+1}$ resp. $\frac{q^n+1}{(4,q^n+1)} : n$ follows also from the existence of tori of type $A_n$ in all these cases.

### 5.3 Some arithmetics

(1) **Definition:** Let $p, r$ be primes and $q = p^f$. Define $d_q(r) = 0$ if $r = 2$ or $r = p$ and $d_q(r) := \min\{i | r \mathrm{divides} q^i - 1\}$ else.

(2) **Lemma:** *Let $(r, q) = 1, q = p^f, p$ and $r$ prime. Let $X$ be a group of order $r$. Then an irreducible* $\mathrm{GF}(q)X$*-module has dimension $d_q(r)$.*

**Proof:** This is a basic result of representation theory, see for instance [1]

(3) **Definition:** Let $q = p^f, p$ a prime. Define $\Phi_n(q) = (q^n-1)/\prod_{d|n, d\neq n} \Phi_d(q)$.

(4) **Lemma:** *Let $n, m > 0$ with $m \neq (n, m) \neq n$. Then $(\Phi_n(q), \Phi_m(q)) = 1$.*

**Proof:** Let $d = (n, m), n = da$ and $m = db$. Set $y = q^d$. For $k$ define $p(k) = \frac{y^k-1}{y-1}$. Then $\Phi_n(q) | p(a)$ and $\Phi_m(q) | p(b)$, so $(\Phi_n(q), \Phi_m(q))$ divides $(p(a), p(b)) =: t$. We show now that $t = 1$ by induction over $a + b$. W.l.o.g. we can assume that $a > b$. We can write $p(a) = p(b)y^{a-b} + p(a - b)$. So $t | (p(b), p(a - b))$. If $(b, a - b) = 1$ we get by induction that $t | 1$. Otherwise

$a = b = 1$ because $(a, b) = 1$. But then $p(a) = p(b) = 1$ so $t = 1$.
(5) **Lemma:** *Let $n, m > 0$ with $n = ma$. Then $(q^m - 1, \frac{q^n-1}{q^m-1})|a$.*

**Proof:** Set $y = q^m$ and define $p(k) = \frac{y^k-1}{y-1}$. Set $(y - 1, p(a)) =: t$. We show now that $t|a$. But this follows from the equation
$(y - 1) \sum\limits_{k=1}^{a-1} p(k) = \sum\limits_{k=1}^{a-1} (y^k - 1) = p(a) - a$.
(6) **Lemma:** *Let $m > 0$ and $k > 1$. Then $(\Phi_m(q), \Phi_{mk}(q)) = 1$ if $k$ is not a prime power and $(\Phi_m(q), \Phi_{mk}(q))$ divides $r$ if $k$ is a power of $r$.*
**Proof:** Let $d = (\Phi_m(q), \Phi_{mk}(q))$. First assume that $k$ is divisible by a prime $r$. Then $\Phi_m(q)$ divides $q^{mk/r} - 1$ and $\Phi_{mk}(q)$ divides $\frac{q^{mk}-1}{q^{mk/r}-1}$. With (5) now follows that $d$ divides $r$. If now $k$ is not a prime power we get primes $r, s, r \neq s$ dividing $k$. Thus $d$ divides $r$ and $s$ and so $d = 1$.
(7) **Lemma:** *Let $n, m > 0$ with $n < m$. If $(\Phi_n(q), \Phi_m(q)) \neq 1$ then $n$ divides $m$, $\frac{m}{n}$ is a power of a prime $r$ with $(\Phi_n(q), \Phi_m(q)) = r$. If $r$ is odd then $r^2$ does not divide $\Phi_m(q)$.*
**Proof:** : By (4) we have that $n$ divides $m$. By (6) we have that $\frac{m}{n}$ is a power of a prime $r$ and $(\Phi_n(q), \Phi_m(q)) = r$. Set now $t = q^{m/r}$. Then $\Phi_m(q)$ divides $\frac{t^r-1}{t-1}$ and $\Phi_n(q)$ divides $t - 1$. Let $t \equiv 1 + rb \pmod{r^2}$ (thus $t^i \equiv 1 + irb \pmod{r^2}$). Then $\frac{t^r-1}{t-1} \equiv \sum\limits_{i=0}^{r-1} t^i \equiv r + rb\frac{r(r-1)}{2} \pmod{r^2}$. If now $r$ is odd we have $\frac{t^r-1}{t-1} \equiv r \pmod{r^2}$ and the lemma holds.

## 5.4 Semisimple elements in finite groups of lie type

Aim of the following paragraph is
(1) **Lemma:** *Let $G$ be a finite simple group of lie type in characteristic $p$ and $x \in G$ an element of prime order $r$ with $2 \neq r \neq p$. The one of the following cases holds:*
*(i)* $\mathrm{Aut}_G(x) \neq 1$
*(ii) $O^{p'}(C_G(x))$ is a central product of groups of lie type in characteristic $p$.*
*(iii) $N_G(C)$ contains a characteristic subgroup of index 2, where $C$ is a characteristic subgroup of $C_G(x)$.(In most cases $C = C_G(x)$)*
(2) **Definition:** Let $q = p^f$ for a prime $p$ and $r$ prime with $d_q(r) > 1$ . Define $l(q, r)$ as the smallest prime dividing $d_q(r)$.
(3) **Lemma:** *Let $G = \mathrm{SL}_n(q), n > 1$ and $x \in G$ of prime order $r$ with $d_q(r) > 1$. Then $l(q, r)$ divides $|\mathrm{Aut}_G(x)|$. Especially case (i) in (1) holds.*
**Proof:** Let $x$ be a counterexample in minimal dimension (of the natural $G$-module $V$). (i): $C_V(x) = 0$. Otherwise $U := [V, x] < V$ is a proper sub-

module for $< x >$ and as $d_q(r) > 1$ we get $\dim(U) > 1$. So there is a $y \in \mathrm{SL}(U)$ with $x^y \neq x$ and $y^{l(q,r)} \in C_{\mathrm{SL}(U)}(x)$. But $y \in G$, so $l(q,r)$ divides $|\mathrm{Aut}_G(x)|$, a contradiction.
(ii) $x$ is irreducible on $V$. (note that $x$ is semisimple.) Otherwise let $V = V_1 \oplus V_2$ be a nontrivial invariant decomposition and $x_i$ the restriction of $x$ to $V_i$. So $x = x_1x_2$ and as $d_q(r) > 1$ and $C_V(x) = 0$ we get $\dim V_i > 1$. Let $G_i = \mathrm{SL}(V_i)$, so $x_i \in G_i$ as $d_q(r) > 1$. By minimality $l(q,r)$ divides $|N_{G_i}(< x_i >) : C_{G_i}(x_i)|$. So there are $y_i \in G_i$ with $y_i^{l(q,r)} \in C_{G_i}(x_i)$. Let $g = g_1g_2 \in G$. As $x^g = x_1^{g_1}x_2^{g_2}$, we see that $x$ is not a counterexample.
If finally $x$ is irreducible by (5.2.3) we have that $l(q,r)$ divides $|\mathrm{Aut}_G(x)|$, so $x$ is not a counterexample.
(4) **Lemma:** *Let $G = \mathrm{SU}_n(q), \Omega^+_{2m}(q) or\ \Omega^-_{2m}(q)$. Let $V$ be the natural module of $G$ and $x \in G$ as in (1). Then one of the following cases holds.*
*(i): $C_V(x) \neq 0$*
*(ii) $V = V_1 \perp V_2$ and the $V_i$ are nondegenerated nontrivial $x$-invariant subspaces of $V$*
*(iii) $V = U_1 \oplus U_2$, $U_i$ maximal singular subspaces of $V$, $V$ $x$-invariant.*
*(iv) $x$ acts irreducibly on $V$.*
**Proof:** Assume that not (i) or (ii) hold and let $U$ be a minimal $x$-invariant subspace of $V$. By minimality we have $U \cap U^\perp = U$ or $U \cap U^\perp = 0$. If $U \cap U^\perp = 0$ then $U$ and $U^\perp$ are nondegenerated $x$-invariant subspaces. But now $U = V$ and $U^\perp = 0$ as otherwise (ii) would hold. This means that $x$ acts irreducibly on $V$ and so case (iv) holds.
So $U \leq U^\perp$. As $x$ is semisimple we get a complement $W$ of $V$ to $U$ and a decomposition $W = W_1 \oplus W_2 \ldots W_k$ into a direct sum of irreducible $x$-invariant subspaces $W_i$. Now as $V$ is nondegenerated there is a $j$ such that $W_j \not\leq U^\perp$. Setting $X := U \oplus W$ we see that $X$ is nondegenerated: $\mathrm{Rad}(X)$ is $x$-invariant but both $U$ and $W$ are irreducible, so have trivial intersection. Assume $0 \neq v = u + w \in \mathrm{Rad}(X)$ with $u \in U$ and $w \in W$. As $U^\perp \cap W = 0$ we see that $w \neq 0$. But also $W^\perp \cap U = 0$ and so there is an $u' \in U$ with $(w, u') \neq 0$. But then also $(w + u, u') \neq 0$ contradicting $v \in X^\perp$. Now $X$ is nondegenerated, but by (i) and (ii) we have that $X = V$ and we are in case (iii).
(5) **Lemma:** *Let $G = \mathrm{SU}_n(q), n > 2$ and $x \in G$ of prime order $r$ with $d_{q^2}(r) > 1$. Then $l(q^2, r)$ divides $|\mathrm{Aut}_G(x)|$. Especially case (i) in (1) holds.*
**Proof:** Assume false and let $x$ be a counterexample with $n$ minimal and $V$ the natural module of $G$.
By (4) one of the four cases (i) to (iv) holds. By minimality of $n$ we see that

(i) does not hold.
If (ii) holds we can set $x = x_1x_2$ with $x_i = x|_{V_i}$ and by minimality there are $g_i \in N_{\mathrm{SU}(V_i)}(< x_i >)$ with $x_i^{g_i} \neq x_i$ and $g_i^{l(q^2,r)} \in C_{\mathrm{SU}(V_i)}(x_i)$. (Note that $d_{q^2}(r) > 1$ ensures that $x_i \in \mathrm{SU}(V_i)$). But then using $g = g_1g_2$ we can show that $x$ is not a counterexample.
If (iv) holds we have $d_{q^2}(r) = n$, but from the order formula one can see easily that $n$ has to be odd for $G$ containing such elements. Now by (5.2.3) we get that $n$ divides $|\mathrm{Aut}_G(x)|$ and so $l(q^2, r)$ divides $|\mathrm{Aut}_G(x)|$. If (iii) holds the stabilizer of $U_1$ induces a $\mathrm{SL}(U_i, \mathrm{GF}(q^2))$ on $U_i$ $(i = 1, 2)$. But now by (2) we see that $x$ was not a counterexample.
(6) **Lemma:** *Let $G = \mathrm{SL}_n(q)$ or $\mathrm{SU}_n(q)$ and $\epsilon = +1$ resp. $-1$ in each case. Let $r$ be an odd prime dividing $q-1$ resp. $q^2-1$ and $x \in G$ an element with $x^r \in Z(G)$. Set $H = G/Z(G)$. Then for $xZ(G) \in H$ one of the cases (i),(ii) or (iii) of (1) holds. Especially if $r$ divides $n$ then (i) or (ii) in (1) holds.*
**Proof:** : In the following let $V$ be always the natural module of $G$ over $K = \mathrm{GF}(q^{(3-\epsilon)/2})$. First let $G = \mathrm{SU}_n(q)$ and let $r$ divide $q - 1$. We may assume that $x^r = 1$ as $(|Z(G)|, r) = 1$. Now all eigenvalues of $x$ lie in $\mathrm{GF}(q)$. Let $v \in V$ be an eigenvector for an eigenvalue $a \neq 1$. Then $(v, v) = (v^x, v^x) = (av, av) = a^2(v, v)$. But $r$ is an odd prime which forces $(v, v) = 0$ which means $v$ is singular. Now $x$ is semisimple which means that $[V, x]$ and $C_V(x)$ are nondegenerated. So there is an $u \in V$ with $u^x = bu$ and $(v, u) \neq 0$. But then $(v, u) = (v^x, u^x) = (av, bu) = ab(v, u)$ which forces $ab = 1$. Now by (4) $V$ admitts an $x$-invariant decomposition $V = U \perp V_1 \perp V_2 \perp \ldots \perp V_k$ with $U = C_V(x)$ and $V_i$ nondegenerated subspaces of dimension 2 and $x|_{V_i} \in \mathrm{SU}(V_i) \cong \mathrm{SL}_2(q)$. But $x|_{V_i}$ is inverted in $\mathrm{SU}(V_i)$. So there is an $y \in G$ with $x^y = x^{-1}$ and we are in case (i) of (1).
Assume now that $r$ divides $q - \epsilon$. Remember that either $C_G(x)$ is a central product of groups of lie type by (5.2.1) and so we are in case (ii) of (1) or we are in the "unique torus case".
Assume that all irreducible $x$-invariant subspaces have dimension 1 which is the case if $o(x)$ divides $|K| - 1$ (The order of the multiplicative group of $K$). Let first be $G = \mathrm{SL}_n(q)$. If one (say $E(\lambda)$) of the eigenspaces for an eigenvalue $\lambda$ has dimension greater than one, $C_G(x)$ induces a $\mathrm{SL}(E(\lambda))$ on $E(\lambda)$, so we are not in the "unique torus case", thus (ii) of (1) holds. If all the eigenvalues are different we see that $x$ lies in a torus of order $(q - 1)^{n-1}$ which is therefore the centralizer of $x$ and is normalized by a $\Sigma_n$ (The full weyl group). In case $G = \mathrm{SU}_n(q)$ $V$ admitts by (4) a decomposition into the eigenspaces $V(a_i)$ of $x$ for the eigenvalues $a_i$. Let $v^x = av$,

$u^x = bu$ and $(v, u) \neq 1$. Then $(v, u) = (v, u)^x = a\bar{b}(v, u)$ where $\bar{b} = b^q$ is the image under the field automorphism of order 2. Thus either $(v, u) = 0$ or $1 = a\bar{b} = ab^{-1}b^{q+1} = ab^{-1}$ which forces $a = b$. Thus all the eigenspaces $E(a_i)$ for pairwise different $a_i$ are pairwise orthogonal. They are therefore nondegenerated. If one of these eigenspaces now has dimension greater than one, $C_G(x)$ induces a unitary group on this eigenspace and so $x$ is not in the "unique torus case", so (ii) of (1) holds. If all the different eigenspaces have dimension 1 , $x$ lies in a torus of order $(q+1)^{n-1}$ which is therefore the centralizer and is normalized by a $\Sigma_n$, so in both the linear and the unitary case we have that $|C_G(x)| = (q - \epsilon)^{n-1}$ and $N_G(C_G(x))/C_G(x) \cong \Sigma_n$.

Assume first that $(r, n) = 1$. Then $r$ is coprime to $|Z|$ so we may assume that $r$ is the order of $x$. But now by the arguments above we are either in case (ii) or (iii) of (1). (Note that $C_G(x)$ covers $C_H(xZ(G))$ and $N_G(C_G(x))$ covers $N_H(C_H(xZ(G)))$ as $r$ is coprime to $|Z(G)|$.) Assume now that $r$ divides $n$. We may assume now that $x^r = \lambda \mathrm{Id}_V$ with $\lambda \in K$ and $o(\lambda) = r^k$.

First assume $\lambda = 1$, so all the eigenvalues of $x$ lie in $K$. By the arguments above we may assume that the eigenvalues of $x$ are pairwise different as otherwise case (ii) of (1) would hold. Now $r$ divides $n$ and $r$ has at most $r$ different eigenvalues, so $r = n$ and the eigenvalues of $r$ are the $r$ different $r$-th roots of unity. But then $x^{-1}$ has the same eigenvalues and therefore $x$ is conjugate to $x^{-1}$ in $G$. As the same holds for $xZ(G) \in H$ we are in case (i) of (1).

So we may assume $\lambda \neq 1$. Assume first that $o(x)$ divides $|K| - 1$. So the polynomial $y^r - \lambda$ is fully reducible over $K$ and an irreducible $x$-invariant subspace has dimension 1. By the arguments above we may assume that all the eigenvalues of $x$ are pairwise different. But as $x^r \in Z(G)$ we have that all eigenvalues of $x$ are solutions of the equation $y^r = \lambda$ which has only $r$ different solutions. (Thus $n = r$.) But now $\det(x)$ is the product of all these solutions which is $\lambda \neq 1$, a contradiction.

So assume that $o(x)$ does not divide $|K| - 1$ and $K$ does not contain solutions of the equation $y^r = \lambda$. Now $y^r - \lambda$ splits totally over $L := \mathrm{GF}(|K|^r)$: $r$ divides $\frac{|K|^r - 1}{|K| - 1}$ as $|K| \equiv 1 \pmod{r}$ as $K$ contains the $r$-th roots of unity. Thus $L$ contains a solution of the equation $y^r = \lambda$ but then contains all these solutions. As now the degree $|L : K| = r$ is prime we see that $y^r - \lambda$ is irreducible over $K$. Let now $U$ be an $x$-irreducible subspace of $V$ and $0 \neq u \in U$. Then the vectors $u, u^x, u^{x^2}, \ldots, u^{r-1}$ form a basis of $U$: By the irreducibility they span $U$ and as $y^r - \lambda$ is irreducible over $K$ they are lineary independent. Note that $\det(x|_U) = \lambda \neq 1$.

Assume first that $G = \mathrm{SL}_n(q)$. Let $V = U_1 \oplus U_2 \dots U_k$ be an $x$-invariant decomposition of $V$ with $x$ irreducible on the $U_i$. If $k > 1$ $C_G(x)$ induces a $\mathrm{SL}_k(q)$ on $V$ as the action on the $U_i$ is all the same, so we are in (ii) of (1). If $k = 1$ we get a contradiction as $\det(x) \neq 1$. Assume now that $G = \mathrm{SU}_n(q)$. Assume an $x$-irreducible subspace $U$ is totally singular. (As $U$ is irreducible we have either $U \cap U^\perp = 0$ , so $U$ is nondegenerated or $U \cap U^\perp = U$ and so $U$ is totally singular) As $V$ is nondegenerated there is an $x$-irreducible subspace $W$ which does not lie in $U^\perp$. Now the action of $x$ on $W$ is dual to the action of $x$ on $U$, so $\det(x|_W) = \det(x|_U)^{-1}$. But the action of all $x$-irreducible subspaces is the same, so $\det(x|_W) = \det(x|_U)$. As now $\lambda \neq \lambda^{-1}$ we get a contradiction. So all the $x$-irreducible subspaces are nondegenerated. If now $k = n/r > 1$ $C_G(x)$ induces a $\mathrm{SU}_k(q)$ on $V$ and so we are in case (ii) of (1). If $k = 1$ we get a contradiction as $\det(x) \neq 1$.

(7) **Lemma:** *Let $G = \Omega^\pm_{2m}(q), n > 2$ and $x \in G$ of prime order $r$ with $d_q(r) > 2$. Then $l(q,r)$ divides $|\mathrm{Aut}_G(x)|$. Especially (i) in (1) holds.*

**Proof:** Let $V$ be the natural module of $G$ and assume false. Let $(G, x)$ be a counterexample with $n := \dim(V)$ minimal.

By (4) one of the four cases (i) to (iv) holds. By minimality of $n$ we see that (i) does not hold: (Note that $[V, x]$ and therefore $C_V(x)$ is of even dimension: By (4) we have a decomposition: $[V, x] = U_1 \perp U_2 \perp \dots \perp U_k$ with either $x$ on $U_i$ irreducible or $U_i = X_i \oplus Y_i$ where $X_i, Y_i$ are totally singular. Especially all the $U_i$ are nondegenerated. If $U_i = X_i \oplus Y_i$ then $U_i$ is of plus type and therefore of even dimension. If $x$ is irreducible on $U_i$ then by (3) we see that $o(x)$ divides $(q^{n_i} - 1, |O(U_i)|)$ where $n_i$ is the dimension of $U_i$. Further $d_q(o(x)) = n_i$ and now the order formulas show that $U_i$ is of minus type and therefore also even dimensional.)

If (ii) of (4) holds we can set $x = x_1x_2$ with $x_i = x|_{V_i}$ and by minimality there are $g_i \in N_{\Omega(V_i)}(< x >)$ with $x^{g_i} \neq x_i$ and $g_i^{l(q,r)} \in C_{\Omega(V_i)}(x_i)$. (Note that $d_q(r) > 2$ ensures that $\dim(V_i) > 2$ and the note above shows that the $V_i$ are of even dimension.) But then using $g = g_1g_2$ we can show that $x$ is not a counterexample.

If (iv) of (4) holds $o(x)$ divides $(q^n - 1, |G|)$, but $d_q(o(x)) = n$. So from the group order we see that $G = \Omega^-_n(q)$. If $n$ is even we have $l(q, r) = 2$ and by (5.2.2) we see that $x$ is inverted in $G$. If $n$ is odd (5.2.3) gives that $|\mathrm{Aut}_G(x)| = n$ and therefore $x$ is not a counterexample.

If (iii) of (4) holds we see that $G = \Omega^+_n(q)$ and the stabilizer of $U_1$ induces a $\mathrm{SL}(U_i)$ on $U_i$ $(i = 1, 2)$. Now by (3) we see that $x$ was not a counterexample.

(8) **Lemma:** *Let $G = \Omega^\pm_{2m}(q), m \geq 2$, $x \in G$ with $o(x) = r$ prime with*

$0 < d_q(r) < 2$. *Then one of the cases (i),(ii) or (iii) of (1) holds.*

**Proof:** We have $C_V(x) = 0$: Otherwise $C_V(x)$ contains an anisotropic subspace $U$ of dimension 1 and $x \in \mathrm{Stab}(U) \leq G$. Now $U$ induces on $U^\perp$ either a group $O^{2m-1}(q)$ or $\mathrm{Sp}_{2m-2}(q)$ depending on $q$ either odd or even. But by (5.2.2) we see then that $x$ is inverted in $\mathrm{Stab}(U)$, so we are in case (i) of (1). Also we may assume that $m$ is odd as otherwise we are again in case (i) by (5.2.2) .

Let now $d_q(r) = 1$ and $v \in V$ an eigenvector of $x$ such that $v^x = av$ with $a \neq 1$. Then $Q(v) = Q(v^x) = Q(av) = a^2Q(v)$. But $o(x)$ is odd and $a \neq 1$. Therefore $v$ is singular. Now $< v >^\perp$ is $x$-invariant and has codimension 1. As $r \neq p$ there is an $x$-invariant complement $< u >$ to $< v >^\perp$ and w.l.o.g. we may assume that $f(v, u) = 1$ where $f$ is the symmetric bilinear form associated with $Q$. Then again $u$ is singular but $< v, u >$ is a nondegenerated $O_2^+$-subspace of $V$. Continuing in this manner we get an $x$-invariant $O_2^+$ decomposition of $V$: $V = U_1 \perp U_2 \perp \ldots \perp U_k$ where $U_i =< v_i, u_i >$ with $v_i^x = a_iv_i, u_i^x = b_iu_i$ and $(v_i, u_i) = 1$. As $1 = (v_i, u_i) = (v_i^x, u_i^x) = a_ib_i(v_i, u_i)$ we see further that $a_ib_i = 1$.

Assume now that $x$ contains an eigenvalue $\lambda \neq 1$ more than once. Then the eigenspace $E(\lambda)$ to $\lambda$ is totally singular and has dimension $> 1$. But $C_G(x)$ induces the full linear group on $E(\lambda)$, so we cannot be in the "unique torus case" and so (ii) of (1) holds. Thus all nontrivial eigenvalues are pairwise different.

Let now $y \in C_G(x)$. Then $v_i^{yx} = v_i^{xy} = (a_iv_i)^y = a_iv_i^y$ and $u_i^{yx} = u_i^{xy} = b_iu_i^y$. But all the eigenvalues of $x$ are unique and so $y$ respects the base $\{v_i, u_i\}$ which forces $C_G(x)$ to be abelian of rank $m$. In fact now $C_G(x)$ is a Cartan subgroup and $N_G(C_G(x))/C_G(x)$ is the Weyl group of $G$ and so we are in case (iii) of (1).

Let now $d_q(r) = 2$. By (4) we get a decomposition of $V = U_1 \perp U_2 \perp \ldots U_k$ with $U_i$ either of type $O_2^-$ or $O_4^+$.

Assume a subspace $U_i$ is of type $O_4^+$ and $O_4^+ = U \oplus W$ with $U$ and $W$ totally singular and $x$-invariant. Let $U =< u_1, u_2 >$. Then $W$ contains a $w_1$ with $f(u_1, w_1) = 1$ and $f(u_2, w_1) = 0$. (Choose $x_1 \in W\cap < u_2 >^\perp$. Then $f(u_1, x_1) \neq 1$ as otherwise $x_1$ would lie in $\mathrm{Rad}(U_i)$. Set $w_1 = \lambda x_1$ to get $f(u_1, w_1) = 1$.) Using the same method we can find a $w_2$ with $f(u_1, w_2) = 0$ and $f(u_2, w_2) = 1$. Some easy arithmetic shows now that $x$ centralizes a $\mathrm{SL}_2(q)$ in $\Omega(U_i)$, so we are in case (ii) of (1). So all the $U_i$ are of type $O_2^-$. Now $C_G(x)$ contains the maximal torus of type $(q+1)^m$. So following (5.2.1) we are either in case (ii) of (1) or in the "unique torus case". In this last case we see that $N_G(C_G(x))/C_G(x) \cong 2^{m-1}\Sigma_m$. (For instance [8] Prop. 4.2.11) and we are in case (iii).

(9) **Lemma:** *Let $G = E_6(q)$ or ${}^2E_6(q)$ and $x \in G$ an element of prime order $r$ with $d_q(r) > 0$. Then one of the cases (i),(ii) or (iii) of (1) holds.*

**Proof:** The $r$-part of $|G|$ is contained in $n_i$ if $d_q(r) = i$, where $n_i$ is defined below. A Sylow-$r$-subgroup of $G$ is contained in a group of type $M_i$ and w.l.o.g we may assume $x \in M_i$. In case $E_6(q)$ this are the $n_i$s and $M_i$s:

| $i$ | $n_i$ | $M_i$ | cases |
|---|---|---|---|
| 1 | $\Phi_1^6$ | $A_1(q) \circ A_5(q)$ | $r \neq 3, 5$ |
| 1 | $\Phi_1^6 3^3$ | $\frac{(q-1)^6}{3} W(E_6)$ | $r = 3$ |
| 1 | $\Phi_1^6 5$ | $A_1(q) \circ A_5(q)$ | $r = 5$ |
| 2 | $\Phi_2^4$ | $F_4(q)$ | $r \neq 3$ |
| 2 | $\Phi_2^4 3^2$ | $F_4(q)$ | $r = 3$ |
| 3 | $\Phi_3^3$ | $A_2(q) \circ A_2(q) \circ A_2(q)$ | |
| 4 | $\Phi_4^2$ | $F_4(q)$ | |
| 5 | $\Phi_5$ | $D_5(q) \circ (q-1)$ | |
| 6 | $\Phi_6^2$ | $F_4(q)$ | |
| 8 | $\Phi_8$ | $F_4(q)$ | |
| 9 | $\Phi_9$ | $A_2(q^3)$ | |
| 12 | $\Phi_{12}$ | $F_4(q)$ | |

In case ${}^2E_6(q)$ this are the $n_i$s and $M_i$s:

| $i$ | $n_i$ | $M_i$ | cases |
|---|---|---|---|
| 1 | $\Phi_1^4$ | $F_4(q)$ | $r \neq 3$ |
| 1 | $\Phi_1^4 3^2$ | $F_4(q)$ | $r = 3$ |
| 2 | $\Phi_2^6$ | $A_1(q) \circ {}^2A_5(q)$ | $r \neq 3, 5$ |
| 2 | $\Phi_2^6 3^3$ | $\frac{(q+1)^6}{3} W(E_6)$ | $r = 3$ |
| 2 | $\Phi_2^6 5$ | $A_1(q) \circ {}^2A_5(q)$ | $r = 5$ |
| 3 | $\Phi_3^2$ | $F_4(q)$ | |
| 4 | $\Phi_4^2$ | $F_4(q)$ | |
| 5 | $\Phi_5$ | ${}^2D_5(q) \circ (q+1)$ | |
| 6 | $\Phi_6^3$ | ${}^2A_2(q) \circ {}^2A_2(q) \circ {}^2A_2(q)$ | |
| 8 | $\Phi_8$ | $F_4(q)$ | |
| 9 | $\Phi_9$ | ${}^2A_2(q^3)$ | |
| 12 | $\Phi_{12}$ | $F_4(q)$ | |

Proof of the $n_i$s: We analyze the semisimple part of the group order: if $d_q(r) = i$ then $r$ divides $\Phi_i(q)$. Now using (5.3.7) we can calculate the $r$-part of $G$. The existence of the subgroups of type $M_i$ follows from [12] for types $F_4$, $A_1(q) \circ A_5(q)$, $D_5^\epsilon(q) \circ q - \epsilon$ and from [4] for the other types.

Assume now that $M_i$ is of type $F_4$. By (5.2.2) we see now that $x$ is inverted in $M_i$, so we are in case (i). Let now $G$ be of type $E_6(q)$ and $d_q(r) > 1$. If $M_i$ is of type $A_2(q) \circ A_2(q) \circ A_2(q)$, $D_5(q) \circ (q-1)$ or $A_2(q^3)$ we are in case (i) by (3) and (6).

Let now $G$ of type ${}^2E_6(q)$ and $d_q(r) \neq 2$. First assume that $d_q(r) > 2$. Note that then $d_{q^2}(r) > 1$. So we can apply (5) and (6) to see that case (i) holds. Let now $G = E_6(q)$ and $d_q(r) = 1$ but $r \neq 3, 5$. Then the $r$-part of $G$ is the $r$-part of $(q-1)^6$. Set now $\bar{G}$ the central extension of $G$ with $d := (q-1, 3)$. Then $\bar{G}$ is a group of fixed points of some frobenius map of the simply connected simple algebraic group of type $E_6$. (See (5.2.1) .) Let $\bar{x}$ some element of the preimage of $x$. (Under the homomorphism from $\bar{G}$ to $G$) Then by (5.2.1) we have that $C_{\bar{G}}(\bar{x})$ is either a central product of groups of lie type in characteristic $p$ and we are in case (ii) as this holds also for $x$ in $G$ or we are in the "unique torus case". Now a Sylow-$r$-subgroup of $G$ is abelian of rank 6. Thus the torus has order $(q-1)^6$ in $\bar{G}$ and $(q-1)^6/d$ in $G$. (Note that $(d, r) = 1$, thus $C_G(x)$ covers $C_{\bar{G}}(\bar{x})$). Now $N_{\bar{G}}(C_{\bar{G}}(\bar{x}))/C_{\bar{G}}(\bar{x}) \cong W(E_6)$, the weyl group. and $r$ is coprime to $Z(\bar{G})$, so $N_G(C_G(x))/C_G(x) \cong W(E_6)$ and we are in case (iii) of (1).

Let now $r = 5$ and assume that $d_q(5) = 1$. $x$ is contained in a group $M$ of type $(A_1(q) \circ A_5(q)).(2, q-1)$. Set $M_0 = O^2(M)$, such that $M_0 = M_1M_2$ with $M_1 = A_1(q)$ and $M_2 = A_5(q)$. So $x = x_1x_2$ with $x_i \in M_i$. There is an epimorphism from $\mathrm{SL}_6(q)$ onto $M_2$. Let $\bar{x}$ be a preimage of $x_2$. We may choose $\bar{x}$ of order 5 as $|Z(\mathrm{SL}_6(q))|$ is coprime to 5. Then $\bar{x}$ has an eigenvalue of multiplicity greater than one (as $\bar{x}$ has only 5th roots of unity as eigenvalues, but $\bar{x}$ has 6 eigenvalues). So we are not in the unique torus case and hence in case (ii). If $G$ is of type ${}^2E_6(q)$ we can modify this proof by replacing the linear subgroups with unitary subgroups and $q-1$ with $q+1$, so the remaining cases are $r = 3$, $d_q(3) = 1$ for $E_6(q)$ and $d_q(3) = 2$ for ${}^2E_6(q)$. Let again be $\bar{G}$ be a central extension of $G$, such that $\bar{G}$ is a group of fixed points of a frobenius map of a simple simply connected algebraic group of type $E_6$. Let $\bar{x}$ be an element in the preimage of $x$. (Thus $\bar{x}$ has order 3 or order 9). By (5.2.1) then either $C_{\bar{G}}(\bar{x})$ is a central product of groups of lie type (and hence the same holds for $x$ and we are in case (ii) of (1)) or we are in the "unique torus case". Then 9 divides the order of the torus (as we have a nontrivial centre of order 3 which has to be contained in the unique torus containing $\bar{x}$). Using [3] we can calculate the orders of the maximal tori $T$ in groups of type $E_6$. By [14],II,1.10(c) we get the orders of the maximal tori in groups of type ${}^2E_6$ by replacing $q$ with $-q$. As the maximal tori are related to root-subsystems of the weyl group we can see, that all these maximal tori are contained in subgroups of type

$M = A_1(q) \circ A_5(q).(2, q-1)$ of $\bar{G}$ or $T$ is of one of the following types (in the notation of [3]): $D_4$, $D_4(a_1)$, $D_5$, $D_5(a_1)$, $A_2 \times A_2 \times A_2$ , $E_6$, $E_6(a_1)$ or $E_6(a_2)$ with orders $(q^3+1)(q+1)(q-1)^2$, $(q^2+1)(q^2+1)(q-1)^2$, $(q^4+1)(q+1)(q-1)$, $(q^3+1)(q^2+1)(q-1)$, $(q^2+q+1)^3$, $(q^4-q^2+1)(q^2+q+1)$, $q^6+q^3+1$ resp. $(q^2+q+1)(q^2-q+1)(q^2-q+1)$. (This are the orders in case of $E_6(q)$, for ${}^2E_6(q)$ we have to replace $q$ by $-q$). We can find the first four tori in a subgroup of type $D_5^\epsilon(q) \circ (q-\epsilon)$. From this we see, that for an element lying in such a torus case (ii) of (1) holds. (As $\bar{x}$ would centralize a subgroup of type $D_4(q)$ as the only terms divisible by 3 are the $q-\epsilon$-s.) In the last three cases we see by (5.3.7) that 9 does not divide the order of the torus, so $T$ is of type $(q^2+\epsilon q+1)^3$, embedded in a subgroup of type $3^2.(L_3^\epsilon(q) \times L_3^\epsilon(q) \times L_3^\epsilon(q)).3\Sigma_3$. By (5.3.7) we see that $(\Phi_1(q), \Phi_3(q)) = 3$, $(\Phi_2(q), \Phi_3(q)) = 1$ in case $E_6(q)$ and $(\Phi_1(q), \Phi_6(q)) = 1$, $(\Phi_2(q), \Phi_6(q)) = 3$, $(\Phi_3(q), \Phi_6(q)) = 2$, $(\Phi_4(q), \Phi_6(q)) = 1$, $(\Phi_5(q), \Phi_6(q)) = 1$. As $\Phi_3(q) \geq 7$ for $q \geq 2$ and $\Phi_6(q) \geq 7$ for $q \geq 3$ we get a prime $r$ dividing $\Phi_3(q)$ resp. $\Phi_6(q)$ with $d_q(r) = 3$ resp. 6. Set $S$ to be the Sylow-$r$-subgroup of the torus $T$. As $T$ is a Sylow-$r$- subgroup of $\bar{G}$ we have that $S \mathrm{char} \bar{T}$ and the image $S_0$ of $S$ in $G$ is a characteristic subgroup of $C_G(x)$. Then $N_G(S_0)/C_G(S_0) \cong 3^{1+2}2\Sigma_4$ (as $T$ is of type $A_2+A_2+A_2$) and so $N_G(S_0)$ contains a characteristic subgroup of index 2 and we are in case (iii) of (1). So the case ${}^2E_6(2)$ remains. Now by the character table in [5] we see that $G$ has 3 conjugacy classes of elements of order 3 with Centralizer $3 \times U_6(2)$, $(3 \times O_8^+(2) : 3)$ and $3^{1+6}2^{1+6}3^2$ and so we see that (i) and (ii) of (1) holds.

**Proof:** of (1): If $G$ is one of $A_1(q)$, $B_n(q)$, $n > 1$, ${}^2B_2(q)$, $C_n(q)$, $n > 2$, $D_{2n}(q)$,$n > 3$, ${}^2D_{2n}(q)$,$n > 3$, ${}^3D_4(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(q)$, $G_2(q)$ or ${}^2G_2(q)$ then by (5.2.2) we see that (i) holds. If $G$ is of type $A_n(q), n > 2$ or ${}^2A_n(q), n > 2$ we see that (i),(ii) or (iii) holds by (3),(5) and (6). The statement holds for groups of type $D_n(q)$ and ${}^2D_n(q)$ by (7) and (8) and for groups of type $E_6(q)$ resp. ${}^2E_6(q)$ by (9).

# 6 The minimal counterexample

Applying the classification of finite simple groups, a minimal counterexample to Theorem  (4.9) is an alternating group, a sporadic group or a group of lie type.

## 6.1 Alternating groups

(1) **Lemma:** *Let $G = \Sigma_n, n \geq 5$ and $x \in G$. Then there is an $y \in G$ with $x^g = y \neq x$ for a $g \in A_n$ and $[x, y] = 1$.*
**Proof:** Assume false and let $(G, x)$ be a counterexample with $n$ minimal. Assume $x$ has fixed points. As $G$ is a counterexample we have $n = 5$ and $x \in \Sigma_4$. W.l.o.g. we may assume that $x$ is one of $(1, 2)$, $(1, 2, 3)$, $(1, 2)(3, 4)$ or $(1, 2, 3, 4)$. Then set $g = (1, 3)(2, 4)$, $(1, 2)(4, 5)$, $(1, 2, 3)$, $(1, 2, 3)$ respectively $(1, 4)(2, 3)$ to see that $x$ is not a counterexample.
Assume $x$ admitts an invariant decomposition of $\{1, 2, \ldots, n\}$ into two sets $K_1, K_2$ with $|K_1| > 4$ or $|K_2| > 4$. Set $x = x_1x_2$ with $x_i \in \Sigma_{K_i}$. W.l.o.g. we may assume $|K_1| > 4$. By minimality we get a $g \in A_{K_1}$ with $[x_1^g, x_1] = 1$. So $x^g \neq x$ and $[x^g, x] = 1$ with $g \in A_n$. Assume now that $|K| \leq 4$ and $|L| \leq 4$. Now $x$ has no fixed points and so the $x_i$ have no fixed points. If $|X_i| = 4$ for some $i$, the $x_i$ is w.l.o.g. either $(1, 2)(3, 4)$ or $(1, 2, 3, 4)$ and we can set $g = (1, 2, 3)$ resp. $g = (1, 4)(2, 3)$. As $n \geq 5$ the remaining cases are w.l.o.g. $x = (1, 2, 3)(4, 5, 6)$ or $x = (1, 2, 3)(4, 5)$.Setting $g = (1, 2)(4, 5)$ (in both cases) we see that $x$ is not a counterexample.
Now $x$ is a cycle of length $n$. So there is a $g_1 \in \Sigma_n$ with $x^{g_1} = x^{-1}$. Assume $n$ is even. Then either $g_1 \in A_n$ or $xg_1 \in A_n$, so $x$ is not a counterexample. If $n$ is odd there is a $g_2$ with $x^{g_2} = x^2$. As $n > 3$ the elements $x, x^{-1}, x^2, x^{-2}$ are all (pairwise) different. So one of the elements $g_1, g_2, g_1g_2$ lies in $A_n$ which shows that $x$ is not a counterexample. So there is no counterexample and the lemma holds.
(2) **Lemma:** *A minimal counterexample to theorem  (4.9) is not an alternating group for $n > 6$.*
**Proof:** In case $n > 6$ we have $\mathrm{Aut}(G) = \Sigma_n$. So assume false and let $G$ be an $\alpha$-CCP-group for $\alpha \in \Sigma_n$. By (1) there is a $g \in A_n$ with $\alpha^g \neq \alpha$ and $[\alpha^g, \alpha] = 1$. But then $1 \neq [g, \alpha] = (\alpha^{-1})^g\alpha \in C_G(\alpha)$ and $G$ is not an $\alpha$-CCP-group.

## 6.2 Sporadic groups

(3) **Lemma:** *A minimal counterexample to theorem (4.9) is not a sporadic group.*
**Proof:** Set $H = <\text{Inn}(G), \alpha>$. By (4.17) now $H$ is an $\alpha$-CCP-group. Further by (4.18) we have that $\alpha$ is not an involution and all the generators of $<\alpha>$ fall into different $H$-conjugacy classes. If $\alpha \in \text{Inn}(G)$ then $H = G$ contains at least $\phi(o(\alpha))$ many conjugacy classes $C_i = x_i^G$ of the same size. If $\alpha \notin \text{Inn}(G)$ then the coset $H - \text{Inn}(G)$ contains at least $\phi(o(\alpha))$ conjugacy classes $C_i = x_i^G$ with the same size. By [5] this happens only in the following cases:

| case nr. | $G$ | $C_i$ | power map |
|---|---|---|---|
| 1 | $M_{12}$ | 4A,4B | A,A |
| 2 | $M_{24}$ | 6A,6B | AA,BB |
| 3 | $Suz$ | 6B,6C | BA,BA |
| 4 | $Suz$ | 6H,6I | CC,CD |
| 5 | $Co_2$ | 4E,4F | B,B |
| 6 | $Fi_{22}$ | 6F,6G | AC,BC |
| 7 | $Fi_{22}$ | 6S,6T | DD,DE |
| 8 | $Co_1$ | 6C,6D | BA,CA |
| 9 | $Co_1$ | 12HIJK | DC,EC,ED,FB |
| 10 | $J_4$ | 6B,6C | AA,AB |
| 11 | $Fi_{24}'$ | 6G,6H | DA,DB |

(Notation as in [5]). Now $\alpha$ has to be one of the $x_i$-s if $G$ is a counterexample. As seen in [5] all elements of order 3 in sporadic groups are conjugate to its inverses. (and otherwise this cases should occur in the table) So by the power map given in [5] we see that in the cases $\{2, 4, 6, 7, 8, 9, 10, 11\}$ not all subgroups of $< x_i >$ are conjugate, so the $x_i$ cannot be choosen as generators of a cyclical subgroup of $\text{Aut}(G)$. So the remaining cases are $G = M_{12}, Suz$ or $Co_2$ and $< \alpha >< C_H(\alpha)$ contains an involution of type $2A, 2A$ resp. $2B$. Let $i$ be this involution and $C = C_H(i)$. Then $C$ has structure $2^{1+4}\Sigma_3$,$2_-^{1+6}U_4(2)$ resp. $(2^{1+6} \times 2^4)A_8$. In case $M_{12}$ and $Co_2$ now $\alpha$ has order 4. By (4.19) we have now $[O_2(C), \alpha] = 1$. But then $[C, \alpha] = 1$ by (5.1.1) . By Glauberman $C$ contains an involution $j \neq i$ conjugate to $i$. By the maximality of $C$ now follows that $[G, \alpha] = 1$, a contradiction.

In case $Suz$ now $\alpha$ acts trivially on $S := C/O_2(C)$ as $S$ is simple. Now $S$ acts absolutly irreducibly on $O_2(C)$ and $\alpha$ centralizes $S$. Thus $\alpha$ has to act trivially on $C$ and by the maximality of $C$ and Glauberman-s $Z^*$-theorem now $[G, \alpha] = 1$, a final contradiction.

## 6.3 Lie groups of high rank

Note: In this paragraph let $G$ be a finite simple group of lie type in characteristic $p$. Set $H = C_G(\alpha)$.
(1) **Lemma:** *Let $G$ be a minimal counterexample to (4.9) and $A < G$ with $A^\alpha = A$. Let $B \lhd A$, such that $A/B$ is a central product of groups of lie type in characteristic $p$. Then the following holds:*
*(i) $C_{A/B}(\alpha)$ contains elements of order $p$.*
*(ii) $A/B$ contains an $\alpha$-invariant Sylow-$p$-subgroup.*
**Proof:** Let $C_1 = A/B$, $C_2 = O^{p'}(C_1)$, $D = C_2/Z(C_2)$. Then $D$ is a direct product of groups of lie type in characteristic $p$, generated by its elements of order $p$.
If $C_D(\alpha)$ contains elements of order $p$ then also $C_{A/B}(\alpha)$ contains elements of order $p$ by (4.10) . If $D$ contains an $\alpha$-invariant Sylow-$p$-subgroup $P$ then so does $A/B$ as the preimage of $P$ in $A/B$ contains a unique Sylow-$p$-subgroup.
Let $E_1 = E(D)$,$F = C_D(E_1)$, $E = C_D(F)$. Then $F$ is the direct product of all solvable groups of lie type and $Z(F) = 1$ by definition of $D$. So $E$ is the product of all nonsolvable factors and $E_1 = F^*(E)$. As now $G$ is a minimal counterexample we see that $\alpha$ is trivial on $E_1$. But now by (5.1.1) we see that $[E, \alpha] = 1$. So if $F = 1$ the lemma holds.
Assume $F \neq 1$ thus $p = 2$ or $p = 3$. First let $p = 2$, so each factor of $F$ is of one of the following types: $T_1 := A_1(2) = 3 : 2$, $T_2 :=^2 B_2(2) = 5 : 4$, $T_3 :=^2 A_2(2) = 3^2 : Q_8$, $T_: = D_2(2) = 3^2 : D_8$. We show now that $\alpha$ acts on the factors by permutation:
Let $i \in T_j$ be an involution and $x \in T_j$ an element of order 4 (if exists).
Then $|T_j : C_{T_j}(i)| = 3(j = 1)5(j = 2)9(j = 3)9$ or $6(j = 4)$ and
$|T_j : C_{T_j}(x)| =5(j = 2)18(j = 3)18(j = 4)$.
Let $F = L_1 L_2 \ldots L_k$ with each $L_j$ isomorphic to one of the above $T_j$'s.
Let $L_m$ be a factor of type $T_1$ and $i \in L_m$ with $|F : C_F(i)| = 3$. So the same holds for $\alpha(i)$ and so we see that $\alpha(i)$ is contained in an unique factor $L_n$ of type $T_1$. Now $L_m =< i^F >$ thus $L_n = \alpha(L_m)$.
Let now $L_m$ be of type $T_2$ and $x \in L_m$ of order 4 with $|F : C_F(x)| = 5$. As the same holds for $\alpha(x)$ we see again that $\alpha(x)$ is contained in an unique factor, say $L_n$ of type $T_2$. As now $L_m =< x^F >$ we see that $L_n = \alpha(L_m)$.
Let $L_m$ be a factor of type $T_3$ or $T_4$ and $x \in G$ of order 4 with $|F : C_F(x)| = 18$. Then also $|F : C_F(\alpha(x))| = 18$ and we see that $\alpha(x)$ lies in an unique factor $L_n$. Now $L_m =< x^F >$. So $< \alpha(x)^F >$ is isomorphic to $L_m$, hence $L_n =< \alpha(x)^F >$ and $L_n = \alpha(L_m)$.

Let now $F_i$ be the product of all factors $L_j$ of type $T_i$. As shown $\alpha$ permutes the factors of $F_i(i = 1, 2, 3, 4)$. By (4.12) we see now that each of the $F_i$'s contains an $\alpha$-invariant Sylow-2-subgroup and centralizes involutions. So $F$ and $D$ contain an $\alpha$-invariant Sylow-2-subgroup and $C_D(\alpha)$ contains involutions.

Finally let $p = 3$ so $F$ is a direct product of groups of type $A_4 = 2^2 : 3$. Now by (4.12) we see that $F$ and therefore $D$ contains an $\alpha$-invariant Sylow-3-subgroup and $C_F(\alpha)$ contains elements of order 3. By the remarks above the lemma holds now.

(2) **Lemma:** *Assume $G$ is a minimal counterexample to theorem (4.9) .*
*If $2$ divides $|H|$ then $p$ divides $|H|$ or the lie rank of $G$ is 1.*

**Proof:** We may assume $p \neq 2$. Let $i \in C_G(\alpha)$ be an involution. The isomorphism type of $C_G(i)$ is listed in [15] for all groups of lietype with $p$ odd. It turns out that $O^{p'}(C_G(i))$ is a central product of groups of lie type in characteristic $p$ if the lie rank is greater than one. By (1) now the lemma holds.

(3) **Lemma:** *Assume $G$ is a minimal counterexample to theorem (4.9) and $p$ divides $|H|$.*
*Then there is a $P \in \mathrm{Syl}_p(G), B = N_G(P)$ such that $B^\alpha = B$.*

**Proof:** Let $x_p \in H$ of order $p$. Set $N_0 = C_G(x_p)$ and $N_{i+1} = N_G(O_p(N_i))$. As $G$ is finite the chain $N_i$ ends in a stationary subgroup $P := N_k = N_{k+1}$. By a theorem of Borel and Tits the group $P$ is a parabolic subgroup of $G$. By construction is $P^\alpha = P$, so we can assume, that $O_p(P) \notin \mathrm{Syl}_p(G)$ as then the lemma holds.

Let $L := O^{p'}(P/O_p(P))$. $L$ is isomorphic to a levicomplement in $P$ to $O_p(P)$. We have to show now, that $L$ contains an invariant Sylow-$p$-subgroup but this follows from (1).

(4) **Lemma:** *Assume $G$ is a minimal counterexample to theorem (4.9) and $p \in \pi_H$.*
*Then either $U^\alpha = U$ for each $B \leq U \leq G$ or $G$ is one of $A_2(q)$,$B_2(q)$,$G_2(q)$ and the graph automorphism has order 2.*

**Proof:** Assume otherwise. Then $\alpha$ induces a graph automorphism on $G$ which means a symmetry on the dynkindiagram. So $G$ is one of $A_n(q), n > 1$, $B_2(q), q$even, $D_n(q), n > 3$, $E_6(q)$ or $G_2(q), q = 3^f$. Let $G$ be of type $A_n(q)$. If $n > 3$ let $P$ be the parabolic corresponding to all except the ending nodes of the dynkindiagram which is invariant under $\gamma$, so under $\alpha$. By minimality of $G$ we see that $\alpha$ is trivial on the quasisimple factor $O^{p'}(P/O_p(P))$ , so $\alpha$ cannot induce a symmetry on the dynkindiagram, a contradiction. If $n = 3$ set $P$ to correspond to the both ending nodes of the dynkindiagram. Then a levicomplement is isomorphic to $A_1(q) \times A_1(q)$ and hence nonsolvable for $q > 3$. In case $q > 3$ $\alpha$ is trivial by minimality. For $q = 2$ we get a contradiction by (5.1.5) and (4.12) . So let $q = 3$. Then $P$ has structure $3^4 : 2.(A_4 \times A_4).2$. Then $\alpha$ normalizes a section of type $H := (\mathrm{PSL}_2(3) \times \mathrm{PSL}_2(3)).2$ and elements in $H - O^2(H)$ induce a diagonal automorphism on $H$. As $\alpha$ is trivial on $H/O^2(H)$ we get an element $x \in C_H(\alpha)$ which covers this factor. Set $C := C_{O_2(H)}(x)$. we have $C^\alpha = C$ and $|C| = 4$. Now $C = (C \cap N_1)(C \cap N_2)$ where the $N_i$ are the normal subgroups of type $\mathrm{PSL}_2(q)$ which are interchanged by $\alpha$ as $\alpha$ induces a graph automorphism. But this contradicts (4.5) as then $\alpha$ fixes a commutator with $\alpha$ on $H$. So also in this case $\alpha$ is trivial on the overgroups of $B$.

So let $G$ be of type $D_4(q)$. If $\gamma$ has order 2 set $P$ to correspond to all nodes except the ending node fixed by $\gamma$. As the levicomplement is nonsolvable (of type $A_3(q)$) we see that $\alpha$ must be trivial on a levicomplement for this parabolic, a contradiction. If $\gamma$ has order 3 set $P$ to be the parabolic subgroup corresponding to all ending nodes. For $q > 3$ a levicomplement of $P$ is nonsolvable so must be centralized, a contradiction. For $q = 3$ we see by (5.1.6) and (4.12) that $\alpha$ cannot be transitive on the nodes. So let $q = 2$. Then $P$ has structure $2^{1+8}.(\Sigma_3 \times \Sigma_3 \times \Sigma_3)$. Set $\bar{P} = P/O_2(P)$. Assume $\alpha$ permutes the $\Sigma_3$-s transitively. By (4.12) we have then that $C_{\bar{P}}(\alpha)$ is not divisible by 3, but $C_{\bar{P}}(\alpha)$ contains involutions by (1) and a $\alpha$-invariant Sylow-2-subgroup $\bar{S}$. Let $S$ be the full preimage of $\bar{S}$. Set $Z = Z(S)$, $Z_2/Z = Z(S/Z)$, $D = S'$ and $O = O_2(P)$ Then $Z$ is of order 2, so $Z \leq C_G(\alpha)$, $|Z_2 : Z| = 2$, so $Z_2 \leq C_G(\alpha)$. Also $|O : D|$=2, so $C_S(\alpha)$ covers this factor. Finally $C_{\bar{P}}$ contains involutions, so $C_G(\alpha)$ contains a 2-group of order at least $2^4$. As $\alpha$ acts transitively on the factors of $\bar{P}$, $\alpha$ lies in a coset of a triality. Now by [5] we see that $\alpha = \beta\gamma = \gamma\beta$, where $\beta$ is of class $3F$ (a triality) and $o(\gamma)$ is not divisible by 3. Thus $C_G(\beta) \cong U_3(3) : 2$ is $\alpha$-invariant. By minimality of $G$ we have that $C_G(\beta) \leq C_G(\alpha)$ and so $\alpha = \beta$. But now $C_{\bar{P}}(\alpha)$ is divisible by 3, a contradiction.

Let $G$ be of type $D_n, n > 4$. Let $P$ be the parabolic of type $D_{n-1}$. So we get again a contradiction.

Finally let $G$ be of type $E_6(q)$ and $P$ the parabolic of type $A_5(q)$. Arguing as above we get a contradiction, so the lemma holds.

(5) **Lemma:** *Assume $G$ is a minimal counterexample to theorem (4.9) and $p \in \pi_H$. Assume further that $\alpha$ fixes all overgroups of the $\alpha$-invariant Borel subgroup $B$ given in (1) and that the lie rank is at least 2.*

*Then $C_G(\alpha)$ acts transitively on flags of the $p$-local geometry defined for $G$ or $G$ is one of ${}^2A_3(2)$,${}^2A_4(2)$ ,$B_2(2)'$, $B_2(3)$, ${}^3D_4(3)$, ${}^2F_4(2)'$ or $G_2(2)'$.*

**Proof:** For each lie group $G$ let $P_1$ and $P_2$ be the maximal parabolics containing $B$ of type given below:

| type of $G$ | type of $P_1$ | type of $P_2$ |
|---|---|---|
| $A_n(q), n > 1$ | $A_{n-1}(q)$ | $A_{n-1}(q)$ |
| ${}^2A_{2n}(q), n > 1$ | ${}^2A_{2n-2}(q)$ | $A_{n-1}(q^2)$ |
| ${}^2A_{2n+1}(q), n > 0$ | ${}^2A_{2n-1}(q)$ | $A_n(q)$ |
| $B_n(q), n > 1$ | $B_{n-1}(q)$ | $A_{n-1}(q)$ |
| $C_n(q), n > 2$ | $C_{n-1}(q)$ | $A_{n-1}(q)$ |
| $D_n(q), n > 3$ | $D_{n-1}(q)$ | $A_{n-1}(q)$ |
| ${}^2D_n(q), n > 3$ | ${}^2D_{n-1}(q)$ | $A_{n-2}(q)$ |
| ${}^3D_4(q)$ | $A_1(q)$ | $A_1(q^3)$ |
| $E_6(q)$ | $D_5(q)$ | $A_5(q)$ |
| ${}^2E_6(q)$ | ${}^2D_4(q)$ | ${}^2A_5(q)$ |
| $E_7(q)$ | $E_6(q)$ | $A_6(q)$ |
| $E_8(q)$ | $E_7(q)$ | $A_7(q)$ |
| $F_4(q)$ | $B_3(q)$ | $C_3(q)$ |
| ${}^2F_4(q)$ | ${}^2B_2(q)$ | $A_1(q)$ |
| $G_2(q)$ | $A_1(q)$ | $A_1(q)$ |

We claim the following: $C_{P_i}(\alpha)$ acts transitively on flags containing $E_i$. This follows if we can show that $P_i = BC_{P_i}(\alpha)$. Set $L_i := O^{p'}(P_i/O_p(P_i))$. If $E(L_i) \neq 1$ we have in fact $F^*(L_i) = E(L_i)$ and by minimality we have therefore $[F^*(L_i), \alpha] = 1$ from which follows $[L_i, \alpha] = 1$ by (5.1.1) . But now $C_{P_i}(\alpha)$ covers the factor group $L_i$ and so we have $P_i = BC_{P_i}(\alpha)$ . So let $E(P_i) = 1$ which means that the type of $P_i$ is one of the following groups: $A_1(2)$, $A_1(3)$, ${}^2A_2(2)$ or ${}^2B_2(2)$. But then $G$ is either an exception of the lemma or $G$ is one of the following groups: $A_2(2)$, $A_2(3)$, ${}^2A_3(3)$, ${}^3D_4(2)$ or $G_2(3)$. First let $G = {}^3D_4(2)$. By [5] the involved parabolic has structure $2^2.[2^9] : A_1(2)$ in ATLAS-notation. Note that the factor $A_1(2)$ acts faithfully on the normal subgroup $N$ of order 4. ( By [5] $P_1$ is $N(2A^2)$ which means that $Z(P_i)$ is trivial as $P_2 = N(2A)$). By assumption we have $P_1^\alpha = P_1$. So let $x \in C_{P_1}(\alpha)$ be an element which covers the factor $P_1/O^2(P_1)$. Now $|C_N(x)| = 2$ and so we see that $[N, \alpha] = 1$. But then we get by (5.1.1) that $[P, \alpha, N] = 1$ which means that $P_1 = BC_{P_1}(\alpha)$ in this case too. In the other cases we see by [5] that all the involved parabolics contain a characteristic subgroup $U$ with $P_i/U \cong \Sigma_4$ and $U < B$. Now by (5.1.4) we see that $[P_i/U, \alpha] = 1$ and therefore $P_i = BC_{P_i}(\alpha)$.

We can now prove flag transitivity:

Denote with $E_i$ the geometrical object fixed by $P_i$ and let $O_i = E_i^G$. We show first that $C_G(\alpha)$ acts transitively on $O_1$: Therefore we define the relation $\sim \subset (O_1 \cup O_2) \times (O_1 \cup O_2) : o_1 \sim o_2$ iff there is a flag containing both $o_1$ and $o_2$. From the theory of buildings and geometries we know that the graph $\sim$ is connected. So let $E \in O_1$ and proceed by induction over the distance of $E$ to $E_1$. If the distance is 0 we have $E = E_1$ and nothing is to show. Otherwise there are elements $F \in O_1, G \in O_2$ with $F \sim G \sim E$ and $d(E_1, F) < d(E_1, E)$. So there is an $x_1 \in C_G(\alpha)$ with $F^{x_1} = E_1$. Now $E_1 = F^{x_1} \sim G^{x_1} \sim E^{x_1}$ as $G$ respects the relation $\sim$. But $C_{P_1}(\alpha)$ acts transitively on flags containing $E_1$ so there is an $x_2 \in C_{P_1}(\alpha) < C_G(\alpha)$ with $(G^{x_1})^{x_2} = E_2$. But then there is an element $x_3 \in C_{P_2}(\alpha) < C_G(\alpha)$ with $(E^{x_1 x_2})^{x_3} = E_1$ and so $C_G(\alpha)$ acts transitively on $O_1$. But as $C_{P_1}(\alpha)$ acts transitively on the flags containing $E_1$ we have flag transitivity.

(6) **Lemma:** *Assume $G$ is a minimal counterexample to (4.9) . If $2 \in \pi_H$ or $p \in \pi_H$ then one of the following cases holds:*
*(i) The lie rank of $G$ is 1.*
*(ii) $G = A_2(q), B_2(q)$ or $G_2(q)$ and $\alpha$ induces a graph automorphism of order 2.*
*(iii) $G = {}^2A_3(2)$, ${}^2A_4(2)$, $B_2(2)'$, $B_2(3)$,${}^3D_4(3)$, ${}^2F_4(2)'$ or $G_2(2)'$.*

**Proof:** Assume that the lie rank of $G$ is greater than one and $2 \in \pi_H$ or $p \in \pi_H$. By (4) we may assume that $p \in \pi_H$. Now by (1) we get a Borel subgroup $B$ with $B^\alpha = B$. By (2) we see that either $G$ is one of the exceptions (ii) or $\alpha$ fixes all overgroups of $B$. So we can apply (3). Then $G$ is either one of the exceptions (iii) or $H$ acts flag transitively on $G$. We can now apply the main theorem of [11] to show that in fact $G = H$ as [11] gives all maximal factorizations of the finite simple groups.

From this we see that either $(G, M) = (A_2(q), A_0(q^3).3)$ , $(B_2(3), 2^4 : A_1(4))$ or $(A_3(2), A_7)$ where $M$ denotes the conjugacy class of maximal subgroups of $G$ which acts flag transitively. But $C_G(\alpha)$ is not contained in such a subgroup in the first case.The second case is excluded by (iii) and the third case contradicts (6.1.2) .

(7) **Lemma:** *Assume $G$ is a minimal counterexample to (4.9) . Then one of the following cases holds:*
*(i) The lie rank of $G$ is 1.*
*(ii) $G = A_2(q), B_2(q)$ or $G_2(q)$ and $\alpha$ induces a graph automorphism of order 2.*
*(iii) $G = {}^2A_3(2)$, ${}^2A_4(2)$, $B_2(2)'$, $B_2(3)$, ${}^3D_4(3)$, ${}^2F_4(2)'$ or $G_2(2)'$.*

**Proof:** By (4.14) we have $C_G(\alpha) \neq 1$. Let $x \in C_G(\alpha)$ be of prime order $r$. If $r = 2$ or $p$ the lemma holds by (6). So $x$ is semisimple. Now by (5.4.1) have that one of the cases (i),(ii) or (iii) holds. If case (ii) holds, $O^{p'}(C_G(x))$ is a central product of groups of lie type, which is $\alpha$-invariant. Thus by (1)

we have that $p$ divides $|C_G(x)|$ and now (6) proves the statement.
If (iii) holds, $\alpha$ acts trivially on a factor group of order 2, therefore 2 divides $|C_G(x)|$ and now (6) finishes the argumentation. If finally case (i) holds we get a prime $s$ diving $|\mathrm{Aut}_G(x)|$ and therefore $s$ divides $|C_G(x)|$ by (5.1.2) . So we can repeat this process with an element $y \in C_G(\alpha)$ of order $s$. As $s < r$ this process finally terminates and the lemma is proved.

## 6.4 Lie groups of low rank

In this section let $H = C_G(\alpha)$ and $\pi_U$ be the set of primes dividing $|U|$ for the subgroup $U \leq G$.
(1) **Lemma:** *Let* $G = A_1(q), q > 3$.
*Then G is not a minimal counterexample to theorem (4.9) .*
**Proof:** First let $q$ be even. Then $2 \in \pi_H$: Let $r \in \pi_H$ and $x_r \in H$. Then either $r = 2$ or $\mathrm{Aut}_G(x) = 2$ and so $2 \in \pi_H$ by (5.1.2) .
Let $i \in H$ be an involution and $S = C_G(i) \in \mathrm{Syl}_2(G)$. As all involutions of $S$ are conjugate in $G$, $\alpha$ is trivial on $S$. By (5.1.1) $\alpha$ is trivial on $N_G(S)$. Let $y \in N_G(S) - S$. By (5.1.2) there is an involution $j \in H$ inverting $y$ and $< N_G(S), j >= G$, so $H = G$ and $G$ is not a counterexample.
Assume now $q$ odd. Then $H$ contains either elements of order $p$, involutions or both. (Let $x \in H$ be a semisimple element. Then $x$ is inverted in $G$.)
First let $4|q+1$. Then all subgroups of order $p$ are conjugate in $G$: Let $P$ be a Sylow-$p$-subgroup. Then $|N_G(P) : P| = (|P| - 1)/2$ and $P$ consists of two classes of elements of order $p$. But no element of order $p$ is conjugate to its inverse (as $N_G(P)$ contains no involutions), which shows that all subgroups of order $p$ of $P$ are conjugate in $N_G(P)$.
Assume now that $p \in \pi_H$. Let $x \in H, o(x) = p$. Then $C_G(x) = P$ is a Sylow-$p$-subgroup and as all subgroups of order $p$ are conjugate we see that $[P, \alpha] = 1$. So by (5.1.1) we get $[N_G(P), \alpha] = 1$. Let $y \in N_G(P) - P$. Then $|\mathrm{Aut}_G(y)| = 2$ and by (5.1.2) we get an involution $i \in H$ and so $H \geq < N_G(P), i >= G$. So if $p \in \pi_H$, then $[G, \alpha] = 1$. Otherwise $2 \in \pi_H$.
Now let $4|q-1$. Then we have $2 \in \pi_H$: Let $r \in \pi_H, x \in H, o(x) = r$. If $r \neq p, 2$ we have $|\mathrm{Aut}_G(x)| = 2$ for $x \in H$, so $2 \in \pi_H$ by (5.1.2) . If $r = p$ then $C_G(x_r) = P \in \mathrm{Syl}_p(G)$ and $N_G(P)$ contains a unique subgroup of index 2 which forces $2 \in \pi_H$.
So in general $2 \in \pi_H$ for all odd $q$.
Let $i \in H, o(i) = 2$. Then $C_G(i)$ is a dihedral group and by (5.1.4) we get a Sylow-2-subgroup $S$ of $C_G(i)$ with $[S, \alpha] = 1$. But also $S \in \mathrm{Syl}_2(G)$. So for each involution $i \in H$ we get a Sylow-2-subgroup of $G$ with $i \in Z(S)$.

Assume now that $|S| = 4$. Then $N_G(S) \cong A_4$ as $G$ contains no $2'$-complement. By (5.1.6) we get a Sylow-3-subgroup $T$ of $N_G(S)$ with $T < H$ which shows $N_G(S) \leq H$. Assume $p = 3$. If 4 divides $q + 1$, then $H$ contains elements of order 3, so $H = G$ as seen above. If 4 divides $q - 1 = 3^f - 1$ we have $f = 2k$ for some $k$. But then $3^f - 1 = (3^k - 1)(3^k + 1)$ and so 8 divides $3^f - 1$. So $p \neq 3$ in this case and elements of order 3 are inverted in $G$. So each element of order 3 in $H$ is inverted by an element $j \in H$ of even order and for each involution $i \in H$ there is a subgroup $N \cong A_4$, $N \leq H$ with $i \in N$. By the list of maximal subgroups of $G$ we see that either $H$ a subgroup of type $L_2(q_0)$ for some $q_0$ with $q = q_0^e$ for some $e$ (allowing $e = 1$) or a subgroup of type $A_5$. If $p = 5$ a subgroup of type $A_5$ is of type $L_2(5) = L_2(q_0)$. If $p \neq 2, 3, 5$ we have the three subgroups $C_G(i)$,$N_G(C_G(y))$ and $N_G(C_G(z))$ for some $i, y, z \in H$ of order $2, 3, 5$ respectively which are $\alpha$-invariant. But then two of them must be conjugate say $N_i$ and $N_j$. But then $C_{N_i}(\alpha)$ is conjugate to $C_{N_j}(\alpha)$ as otherwise we get elements $x \in N_i$ and $y \in N_j$ with $x$ conjugate to $y$ and $x = [z, \alpha]$ for some $z \in N_i$ and $y \in H$ which contradicts the $\alpha$-CCP-property. But then $H$ contains elements of order $6, 10$ or $15$ and so $H$ is not of type $A_5$. So in this case ($|S| = 4$) $H$ is always of type $L_2(q_0)$. Now let $8||G|$. Then for each involution $i \in H$ there is an element $x \in H, o(x) = 4$ with $x^2 = i$. By the list of maximal subgroups we see now that $H$ has to be of type $L_2(q_0)$ for some $e$ and $q_0$ with $q_0^e = q$.

So in general $H$ is of type $L_2(q_0)$, But in case 4 divides $q+1$ we have elements of order $p$ in $H$, so $G = H$ as seen above. We show now that $q_0 = q$ as $H$ and $G$ contain the same Sylow-2-subgroup: First we see that $e$ is odd: otherwise $e = 2g$ and $q - 1 = q_0^{2g} - 1 = (q_0^2 - 1)m$ for some integer $m$ which shows that $|G : H| = q_0^{e-1} m(q + 1)$ is even. Let $P$ be an $\alpha$-invariant Sylow-$p$-subgroup of $G$. $P = [P, \alpha] \times C_P(\alpha)$ by the $\alpha$-CCP-property. Now the elements of order $p$ fall into two conjugacy classes. Let $\gamma \in \mathrm{Aut}(G)$ be a diagonal automorphism of order 2, fixing $P$ but interchanging the $p$-conjugacy classes of $P$. As $H \cong L_2(q_0)$ we have $C_P(\alpha)$ of GF($q_0$)-dimension 1 and $[P, \alpha]$ of GF($q_0$)-dimension $e - 1$. If now $e > 1$ we have $[P, \alpha] \cap [P, \alpha]^\gamma \neq 1$ as $e - 1 > e/2$. (Remember $e$ is odd). Thus $[P, \alpha]$ contains elements of order $p$ from both $G$-conjugacy classes and so some elements in $[P, \alpha]$ are $G$-conjugate to some elements in $C_P(\alpha)$, a contradiction to (4.5) . Thus $e = 1$ and $H = G$, a final contradiction.

(2) **Lemma:** *Let $G = {}^2A_2(q), q > 2$.*
*Then $G$ is not a minimal counterexample to theorem (4.9) .*

**Proof:** First assume $q$ odd. If $H$ contains an involution $i$ then $C := C_G(i)$ contains a subgroup $SL_2(q) : 2$. If $q > 3$ we have $E(C) \neq 1$, so $[E(C), \alpha] = 1$.

But $C$ contains a characteristic subgroup of index 2, so $C_C(\alpha)$ covers the factor group and $H$ contains a subgroup $\mathrm{SL}_2(q) : 2$ which contains other involutions than the central one. So we can do this for each involution $i \in H$ and get that $H = G$ as $C$ is a maximal subgroup. If $q = 3$ we have $C = SL_2(q) : 2 \cong 2\Sigma_4$ and by (5.1.3) we have $[C, \alpha] = 1$, so we get $G = H$ as before. So let $r \in \pi_H$. If $r|q$ we get an $\alpha$-invariant parabolic subgroup of $H$ which contains a unique subgroup of index 2 and therefore $2 \in \pi_H$. If $r|q-1$ then elements of order $r$ are inverted in $G$ as they are inverted in a subgroup $SL_2(q)$ and Sylow-$r$-subgroups are cyclical. If $r|\frac{q^2-q+1}{(q+1,3)}$ we have by (5.1.1) that $3 \in \pi_H$ and 3 divides either $q-1, q$ or $q+1$. If $r|q+1$ and $r \neq 2$ we have that either $C = F^*(C_G(x)) = (q+1)^2/(q+1,3)$ or $C = (q+1)/(q+1,3) * \mathrm{SL}_2(q)$ and in both cases $N_G(C)$ contains a unique subgroup of index 2, so $2 \in \pi_H$. So let $q$ be even and $r \in \pi_H$. If $r|q-1$ we have $2 \in \pi_H$ as elements of order $r$ are inverted in $G$. If $r|(q^2-q+1)/(q+1,3)$ we have that $C_G(x)$ is a cyclical group of order $(q^2-q+1)/(q+1,3)$ and $|\mathrm{Aut}_G(x)| = 3$ and hence $3 \in \pi_H$. If $r|q+1$ we have that $C := C_G(x) = \frac{(q+1)^2}{(q+1,3)}$ or $C = \frac{q+1}{(q+1,3)}\mathrm{PSL}_2(q)$ . In the first case we have $N_G(C)/C \cong \Sigma_3$ and so $N_G(C)$ contains a characteristic subgroup of index 2, so $2 \in \pi_H$. In the other case $C$ contains a subgroup $L_2(q)$ which is centralized by $\alpha$ by minimality of $G$ and so $2 \in \pi_H$. So let $i \in H$ be an involution. Then $C_G(i) = q^{1+2} : \frac{q+1}{(q+1,3)}$ where the subgroup $P := O_2(C_G(i)) = q^{1+2} \in \mathrm{Syl}_2(G)$ is a special group and $Z(P) = \Omega_1(P)$. All involutions in $G$ are conjugate as $|N_G(P) : P| = q^2 - 1/(3, q+1)$ and a cyclical subgroup of order $q-1$ acts transitive on the involutions of $P$. So $[Z(P), \alpha] = 1$ by (4.5) and by (5.1.1) we get a subgroup $K$ of order $q-1$ with $K \leq H$ (as $\alpha$ acts trivially on $N_G(Z(S))/C_G(Z(S))$.) and $[Z(P), K] = Z(P)$. Now $C_G(K)$ has order $q^2 - 1/(3, q+1)$ and contains a unique subgroup $L$ of order $\frac{q+1}{(q+1,3)}$. (Note that $q \neq 2$.) Now $C_G(L) = LM$ with $M \cong L_2(q)$. and $M$ is nonsolvable, hence $M \leq H$. Set $\bar{S} = S/Z(S)$ and $Q : \bar{S} \mapsto Z(S)$ defined by $Q(xZ(S)) = x^2$. $Q$ is well defined and it is known that $Q$ defines a nondegenerated quadratic form of minus type. Let now $\beta \in C_{\mathrm{Aut}(G)}(Z(S))$. $\beta$ acts on $\bar{S}$ as $S = O_2(N_G(Z(S)))$. Further $Q(x^\beta) = x^\beta x^\beta = \beta(x^2) = x^2 = Q(x)$, so $\beta$ induces an element of $O_2^-(q) \cong q+1 : 2$ on $\bar{S}$. Assume now that $\alpha$ acts on $L$ nontrivially. But $\alpha$ induces an element of $O_2^-(q)$ on $\bar{S}$ as the elements of $L$ do. So $\alpha$ has to induce an involution on $\bar{S}$, a contradiction to (4.19) . So $\alpha$ centralizes $L$ and $C_G(L)$. From the subgroup $\frac{(q+1)^2}{(3,q+1)}$ we see that $C_G(L)$ contains a subgroup $R$ conjugate to $L$, thus $C_G(R)$ is $\alpha$ invariant and acts

trivially on it. Now we see that $H = G$ as $C_G(L)$ is a maximal subgroup which is a final contradiction.
(3) **Lemma:** *Let $G =^2B_2(q), q > 2$.*
*Then $G$ is not a minimal counterexample to theorem (4.9) .*
**Proof:** Let $r \in \pi_H$. If $r$ is odd the elements of order $r$ are inverted in $G$, so $2 \in \pi_H$. So let $i \in H$ be an involution. Then $P = C_G(i) \in \mathrm{Syl}_2(G)$. As all involutions in $G$ are conjugate we have $[Z(P), \alpha] = 1$. So let $x \in P - Z(P)$. All elements of $P - Z(P)$ are of order 4. As all involutions are conjugate for each involution $i$ the number of elements $y$ of order 4 with $y^2 = i$ is constant. So this number is $q(q-1)/(q-1) = q$ and so for another $y_1$ with $y_1^2 = i$ we have $y_1 = yz$ with $z \in Z(P)$. Now $x^\alpha x^\alpha = \alpha(x^2) = x^2$ and so $x$ and $x^\alpha$ lie in the same $Z(P)$-coset of $P$ which means $[x, \alpha] \in Z(P)$. But then $[x, \alpha] = 1$ as involutions cannot be commutators by the $\alpha$-CCP-property. So we have $[P, \alpha] = 1$ and by (5.1.1) we get $[N_G(P), \alpha] = 1$. So there are elements of odd order in $H$. But then $H$ contains elements which invert these elements and so $H = G$ as $N_G(P)$ is a maximal subgroup.
(4) **Lemma:** *Let $G =^2G_2(q), q > 3$.*
*Then $G$ is not a minimal counterexample to theorem (4.9) .*
**Proof:** Here we use the list of maximal subgroups of $G$ given in [10]. Let $r \in \pi_H$: If $r = 3$ we get an $\alpha$-invariant maximal parabolic $P$ which contains a unique subgroup of index 2 (hence $2 \in \pi_H$) as can be seen from the list.
If $r \neq 3$, but $r$ odd we see that elements of order $r$ are inverted in $G$, so $2 \in \pi_H$.
If $i \in H$ is an involution then $C = C_G(i) = 2 \times L_2(q)$ is a maximal subgroup and as $q > 3$ we have $E(C) \neq 1$ and so by minimality we have $[C, \alpha] = 1$. But this holds for each involution $i \in H$ and $C$ contains involutions other than $i$. So $C < H$ and $H = G$ and $G$ is not a minimal counterexample.
(5) **Lemma:** *Let $G = A_2(q), q > 2$.*
*Then $G$ is not a minimal counterexample to theorem (4.9) .*
**Proof:** Set $d = (q-1, 3)$. First assume $q$ odd. Let $r \in \pi_H$ and $x \in H$ of order $r$. If $r | q^2 + q + 1/d$ we have $|\mathrm{Aut}_G(x)| = 3$ and so $3 \in \pi_H$. If $r | q + 1$ we have $|\mathrm{Aut}(x)| = 2$ and so $2 \in \pi_H$. If $r | q - 1$ we have either $C := C_G(x) = \frac{(q-1)}{d} * \mathrm{SL}_2(q)$ or $C = \frac{(q-1)^2}{d}$. In both cases $N_G(C)$ contains a characteristic subgroup of index 2. So $2 \in \pi_H$. If $p \in \pi_H$ we get an invariant Borel group $B$ of order $q^3(q-1)^2/d$.
Then $|B : C_G(P)| = q - 1$ and so $B$ contains a characteristic subgroup of index 2 and hence $2 \in \pi_H$. So finally we have $2 \in \pi_H$. Let $i \in H$ be an involution. Then $C_G(i)$ contains a characteristic subgroup $C_0$ of type $\mathrm{SL}_2(q) : 2$ .

If $q \neq 3$ we have $E(C_0) \neq 1$ and hence $[C_0, \alpha] = 1$. If $q = 3$ we have $C_0 \cong 2\Sigma_4$ and by (5.1.4) we get again $[C, \alpha] = 1$. But $C_0$ contains an involution other than $i$. We show now that $H = G$:

If $i, j \in G$ are involutions with $[i, j] = 1$ and $i \in H$, then $j \in H$. Let$\Gamma_G$ be the graph on the involutions of $G$ by defining edges as commuting pairs. We show $\Gamma_G$ is connected by showing $\Gamma_L$ is connected where $L = \mathrm{SL}_3(q)$. This works as involutions in $L$ correspond to involutions in $G$. For involutions $i, j \in L$ let $u, v \in V$ (the natural module of $L$) with $v^i = v$ and $u^j = u$. Then $G$ contains an involution $k$ with $v^k = -v$ and $u^k = -u$. So $ik$ and $kj$ have even orders and so $< i, k >$ and $< k, j >$ contain involutions $i_1$ and $j_1$ with $[i, i_1] = 1 = [i_1, k]$ and $[k, j_1] = 1 = [j_1, j]$.

So if $H$ contains an involution $i$, $H$ contains all involutions of $G$. As $G = i^G$ we have $H = G$.

Now let $q$ be even. Let $r \in \pi_H$ be a prime. By (5.4.1) and the usual arguments we may assume that $r = 2$. So we get an $\alpha$-invariant Sylow-2-subgroup $P$ of $G$. Note that all involutions in $G$ are conjugate, thus $[Z(P), \alpha] = 1$. Now $P$ contains exactly 2 elementary abelian groups $A$ and $B$ of order $q^2$. So either $A^\alpha = A$ or $A^\alpha = B$. In the first case $\alpha$ induces no graph automorphism and by (6.3.6) $G$ is not a counterexample.

So let $i \in A - Z(P)$. Then $1 \neq [i, \alpha]$ has order 4 as it cannot be an involution by (4.5) .

Then $[i, \alpha, \alpha] = (i^\alpha i)(ii^\alpha)^\alpha = (i^\alpha i)^2 (ii^{\alpha^2})$. Now $(i^\alpha i)^2 \in \mho^1(P) \leq Z(P)$ and $ii^{\alpha^2} \in A$ so $[i, \alpha, \alpha] \in A$. But this cannot be an involution as all involutions are conjugate in $G$. So $[i, \alpha] \in H$, a contradiction to (4.5) .

(6) **Lemma:** *Let $G = B_2(q), q > 3$.*

*Then $G$ is not a minimal counterexample to theorem (4.9) .*

**Proof:** Let $r \in \pi_H$. By (5.4.1) we may assume that $d_q(r) = 0$. So by (6.3.3) we get a Sylow-$p$-subgroup $P$ of $G$ with $P^\alpha = P$. Then there are exactly two subgroups $P_1$ and $P_2$ containing $N_G(P)$. If $P_i^\alpha = P_i$ we get a contradiction by (6.3.6) . So $q$ is even and $\alpha$ induces a graph automorphism on $G$. Set $Q_i = O_2(P_i)$ and $R_i = Z(O^{p'}(P_i))$. Then $Z(P) = R_1 \times R_2$ and $[Z(P), \alpha] \neq 1$ as $R_1^\alpha = R_2$. Let $i \in P$ be an involution with $[i, \alpha] = 1$. Each involution of $P$ lies in $Q_1 \cup Q_2$ but as $Q_1^\alpha = Q_2$ we have $i \in Z(P) = Q_1 \cap Q_2$. So $i \in Z(P) - (R_1 \cup R_2)$ and all such involutions are conjugate in $G$ as the Cartan group $(q-1)^2$ acts regularly on them. As $R_1^\alpha = R_2$ we get a contradiction: $1 \neq [Z(P), \alpha]$ and $[Z(P), \alpha] \not\leq R_1$ and $[Z(P), \alpha] \not\leq R_2$, so $[Z(P), \alpha]$ contains involutions conjugate to $i$, a contradiction to (4.5) .

(7) **Lemma:** *Let $G = G_2(q), q > 2$.*

*Then $G$ is not a minimal counterexample to theorem (4.9) .*

**Proof:** Let $r \in \pi_H$. By [10] and [6] (or (5.2.2) ) we may assume that $d_q(r) = 0$ as all semisimple elements of prime order are inverted in $G$, so either $2 \in \pi_H$ or $p \in \pi_H$. By (6.3.2) we have $p \in \pi_H$.
By (6.3.3) we get a Sylow-$p$-subgroup $P$ with $P^\alpha = P$. If now $\alpha$ does not induce a graph automorphism (which interchanges the maximal parabolics containing $N_G(P)$) we get a contradiction by (6.3.6) .
So $q$ is a power of 3. If now $2 \in \pi_H$ we get an involution $i \in H$. Now by [10] $G$ has a unique class of involutions and $F^*(C_G(i)) = E(C_G(i))$. So $[C_G(i), \alpha] = 1$ and $C_G(i)$ contains another involution $j \neq i$. Again $[C_G(j), \alpha] = 1$. By the maximality of $C_G(i)$ we have now that $H = G$, a contradiction.
So $\pi_H = \{3\}$ and we get a Sylow-3-subgroup $P$ of $G$ and $\alpha$ swaps the maximal parabolics containing $N_G(P)$. Let $P_i, i = 1, 2$ be the maximal parabolics containing $N_G(P)$. Set $Q_i = O_3(P_i)$ and $Z_i = Q_i'$. Let $D = Q_1 \cap Q_2$. Then $Z(P) = Z_1 Z_2$. As $P_i = Q : (q-1) * \mathrm{SL}_2(q) : 2$ we see that elements $1 \neq x \in Z_i$ are inverted in $P_i$. $N_G(P)$ contains a unique subgroup $T > P$ such that $T/P \cong V_4$. From the structure of the maximal parabolics we see that the elements of $T$ inverting $Z_1$ lie in exactly one $P$-coset of $T$ as do the elements inverting $Z_2$. So the coset related to the third involution in $T/P$ is fixed by $\alpha$ which means that $\alpha$ fixes an involution in $T/P$ and so $2 \in H$, a contradiction.
(8) **Lemma:** *Let $G ={}^2F_4(2)'$, ${}^3D_4(3)$, ${}^2A_3(2)$ or ${}^2A_4(2)$.
Then $G$ is not a minimal counterexample to theorem (4.9) .*
First let $G ={}^2A_3(2) = B_2(3)$. Let $x \in C_G(\alpha)$ be of prime order $r$. If $r = 5$ then $|\mathrm{Aut}_G(x)| = 4$ and therefore $C_G(\alpha)$ contains involutions. If $C_G(\alpha)$ contains elements of order 3 we get by (6.3.3) and the 3-local geometry an $\alpha$-invariant Sylow-3-subgroup $T$. Thus both maximal parabolics $P_1 \cong 3^{1+2}2A_4$ and $P_2 \cong 3^3\Sigma_4$ containing $T$ are $\alpha$-invariant. As $P_2/O_3(P_2) \cong \Sigma_4$ we get by (5.1.3) that $C_G(\alpha)$ covers this factor group and so $C_G(\alpha)$ contains involutions. If $C_G(\alpha)$ contains involutions we get by (6.3.3) and the 2-local geometry an $\alpha$-invariant Sylow-2-subgroup $S$ and the maximal parabolics $P_3 \cong 2^4A_5$ and $P_4 \cong 2^{1+4}(3^2 : 2)$ containing $S$. As $G$ is a minimal counterexample (if it is a counterexample) we see that $\alpha$ is trivial on $P_3$ $O_2(P_3)$. From the isomorphism $G \cong \Omega_5(3)$ we see that $O_2(P_3)$ is the permutation module of $A_5$ which is absolute irreducible. As now $\alpha$ centralizes $A_5$ we see that $\alpha$ centralizes $O_2(P_3)$, thus $\alpha$ centralizes $P_3$ and $S$. As $C$ contains a section isomorphic to $\Sigma_4$ we see that $[G, \alpha] = 1$, a contradiction.
Let now $G ={}^2A_3(2)$, so $\pi_G = \{2, 3, 5, 11\}$. Let $x \in C_G(\alpha) =: H$ be of prime order $r$. If $r = 11$ we have $|\mathrm{Aut}_G(x)| = 5$ and so $5 \in \pi_H$. If $r = 5$ then

$|\mathrm{Aut}_G(x)| = 4$ and so $2 \in C_G(\alpha)$. If $r = 3$ and $x$ is of class $3E$ or $3F$ in Atlas-notation, then $x$ is inverted in $G$ and so $2 \in \pi_H$. If $r$ is of class $3A$ or $3B$ then $C_G(x) =< x > U$ with $U \cong \mathrm{SU}_4(2)$. Thus $[U, \alpha] = 1$ by minimality of $G$ and so $2 \in \pi_H$. If now $2 \in \pi_H$ then by (6.3.3) we get an $\alpha$-invariant Sylow-2-subgroup $S$ and the $\alpha$-invariant maximal parabolics $P_1 \cong 2_-^{1+6}\mathrm{PGU}_3(2)$ and $P_2 \cong 2^{4+4}(3 \times A_5)$. As now $E(P_2/O_2(P_2)) \neq 1$ $\alpha$ acts trivially on this factor group and so $C_G(\alpha)$ contains an element $y$ of order 5. Now $C_G(y)$ is a cyclical subgroup of order 15. Let $z \in C_G(y)$ be of order 3. Then $z$ is in class $3A$ or $3B$ and so $C_G(< z >) =< z > U$ is $\alpha$-invariant with $U \cong \mathrm{SU}_4(2)$. Thus $U \leq H$. Now by [5] we see that $\alpha$ has to be of class $3A$ or $3B$ if it is nontrivially. From the subgroup $3^4\Sigma_5$ we see that $C_G(z)$ contains an element $z_1$ conjugate to $z$. Thus also $C_G(z_1)$ is $\alpha$-invariant and now $\alpha = z$ has to act trivially on $C_G(z_1)'$, a contradiction. Thus $H = G$ which is again a contradiction (as now $G$ is no counterexample).

Let now be $G =^3D_4(3)$. By (5.2.2) (or [9]) all semisimple elements of $G$ are inverted, thus $H$ contains involutions, if it contains semisimple elements. If $H$ contains elements of order 3 we get by (6.3.3) an $\alpha$-invariant Sylow-3-subgroup $S$. Let $P_1$ be the unique maximal parabolic containing $S$ with $O^{3'}(P_1)/O_3(P_1) \cong \mathrm{SL}_2(9)$. By minimality $\alpha$ centralizes this factor and thus $C_G(\alpha)$ contains involutions in this case too. Let $i$ be such an involution. Now $F^*(C_G(i)/ < i >)$ is simple by [9], thus by minimality is centralized from $\alpha$ which forces $[C_G(i), \alpha] = 1$. But $C_G(i)$ is maximal and contains another involution $j$ with $[C_G(j), \alpha] = 1$ too. Thus $[G, \alpha] = 1$, a contradiction.

Let finally be $G =^2F_4(2)'$, the Tits-group. Assume $G$ is a minimal counterexample and let $x \in C_G(\alpha)$ be of prime order $r$. By [5] we may assume that $x$ is an involution as all elements of prime order are inverted in $G$ by [5]. Thus by (6.3.3) we get an $\alpha$-invariant Sylow-2-subgroup $S$ and the two unique maximal parabolic subgroups $P_1 \cong 2.[2^8]5 : 4$ and $P_2 \cong 2^2.[2^8]\Sigma_3$ containing $S$. By [5] all involutions of $Z(O_2(P_i))$ are of type 2A for both parabolics. Thus by (4.5) $\alpha$ is trivial on $Z = Z(O_2(P_2))$. Now by (5.1.1) we see that $\alpha$ is trivial on $P_2/O_2(P_2) \cong \Sigma_3$, thus 24 divides $|H|$. Let $z \in H$ be an element of order 3. As all elements of order 3 are conjugate by [5] we see by (4.5) that $\alpha$ is trivial on $O_3(C_G(z))$ which is a Sylow-3-subgroup of $G$. Thus $216 = 8.27$ divides $|H|$, but now by [5] we see that $\alpha = 1$, a contradiction.

### 6.5 Proof of the main theorem

**Theorem:** *(Main theorem II): Let G be a strong $\alpha$-CCP-group. Then G is solvable.*
**Proof:** Let $G$ be a minimal counterexample to this theorem. $G$ is simple by (4.12) . By the classification of finite simple groups $G$ is either alternating, sporadic or of lie type. $G$ is not alternating with $n \geq 7$ by (6.1.2) . $G$ is not sporadic by (6.2.1) . Thus $G$ is of lie type. By (6.3.7) $G$ is of lie rank 1, of lie rank 2 and $\alpha$ permutes two maximal parabolics having a Borel subgroup in common or $G = {}^2A_3(2)$, ${}^2A_4(2)$, $B_2(2)'$, $B_2(3)$, ${}^2F_4(2)'$, or $G_2(2)'$. The lie rank one case was handled in (6.4.1) , (6.4.2) , (6.4.3) and (6.4.4) for groups of type $A_1(q)$, ${}^2A_2(q)$, ${}^2B_2(q)$ and ${}^2G_2(q)$ respectively. The lie rank two case was handled in (6.4.5) , (6.4.6) and (6.4.7) for groups of type $A_2(q)$, $B_2(q)$ and $G_2(q)$ respectively. The groups ${}^2A_3(2)$, ${}^2A_4(2)$ ,${}^3D_4(3)$ and ${}^2F_4(2)'$ were handled in (6.4.9) and the other exceptions are already handled by the following isomorphisms: $A_5 \cong A_1(4)$, $A_6 \cong B_2(2)' \cong A_1(9)$. $B_2(3) \cong^2 A_3(2)$, $G_2(2)' \cong^2 A_2(3)$. So finally none of these simple groups is a minimal counterexample to the theorem which now holds by the classification theorem of finite simple groups.

## 7 Summary

We have now proved the following:
**Theorem:** *Let $Q$ be a rightdistributive quasigroup. Then $G_r(Q)$ is a solvable group of automorphisms of $Q$.*
**Proof:** (4.8) and (4.9) .
**Theorem:** *Let G be a strong $\alpha$-CCP-group. Then G is solvable.*
**Proof:** This is (4.9) .
**Theorem:** *Let G be a group with an automorphism $\alpha$, such that $G = C_G(\alpha)$ $\{[g,\alpha] | g \in G\}$. Then $G = C_G(\alpha)N$ with $N = [G,\alpha]$, $N = C_N(\alpha)$ $\{[n,\alpha] | n \in N\}$ and N is solvable.*
**Proof:** This follows from (4.20) and (4.9) .
**Theorem:** *Let G be a group with $G = C_G(g)g^G$. Then $G = C_G(g)N$ with $N =< g^G >$, $N = C_N(g)g^N$ and N is solvable.*
**Proof:** This follows from (4.20) , (4.4) and (4.9) .
So we have answers of the problems from the introduction. To leave the end open we give a list of new problems arising from the different viewpoints:
- Classification problem of rightdistributive quasigroups,
- Generalizations of rightdistributive quasigroups,

- Generalization of Glauberman's theorem for odd primes,
- Generalization of the $\alpha$-CCP-automorphism type [1]
- Conjugacy classes as transversals for nonrelated subgroups

# References

[1] M.Aschbacher *Finite Group Theory*, Cambridge University Press,1986

[2] R.W.Carter *Finite Groups of Lie Type,conjugacy classes and complex characters*,Wiley-Interscience,1985

[3] R.W.Carter *Conjugacy classes in the Weyl group*, Compositio Math., 25(1972),1-59

[4] A.M. Cohen, M.W.Liebeck, J.Saxl, G.M.Seitz *The local maximal subgroups of the exceptional groups of lie type*, preprint

[5] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker and R.A.Wilson *An ATLAS of Finite Groups*, Oxford University Press

[6] B.N.Cooperstein *Maximal subgroups of* $G_2(2^n)$, J.Algebra 70 (1981), 23-36

[7] B.Fischer *Distributive Quasigruppen endlicher Ordnung* , Math.Zeitschr. 83, 267-303 (1964)

[8] P.Kleidman, M.Liebeck *The Subgroup Structure of the Finite Classical Groups* Cambridge University Press 1990

[9] P.Kleidman *The maximal subgroups of the Steinberg triality groups* ${}^3D_4(q)$ *and of their automorphism groups* ,J.Algebra 115(1988),182-199

[10] P.Kleidman *The maximal subgroups of the Chevalley groups* $G_2(q)$ *with q odd, of the Ree groups* ${}^2G_2(q)$*, and of their automorphism groups*, J.Algebra 117 (1988),30-71.

[1] $\alpha$ is said to be **inductive** if
(i) $\alpha|_U$ is inductive for each subgroup $U$ with $U^\alpha = U$ and
(ii) $\alpha$ is inductive on $G/N$ with $C_{G/N}(\alpha) = C_G(\alpha)N/N$ for all $N \triangleleft G$ with $N^\alpha = N$.
Note that fixed point free automorphisms, automorphisms of $\alpha$-CCP-groups and coprime automorphisms are of this type.

[11] M.Liebeck,C.E.Praeger,J.Saxl *The maximal factorizations of the finite simple groups and their automorphism groups* Memoirs of the AMS Vol.86,No.432

[12] M.Liebeck, J.Saxl *On the Orders of maximal Subgroups of the finite exceptional Groups of Lie type* Proc. London Math. Soc (3) 55 (1987) 299-330

[13] P.Rowley *Finite Groups admitting a fixed-point-free Automorphism Group.* J.Algebra 139 (1995), 724-727

[14] T.A.Springer, R.Steinberg *Conjugacy Classes* Seminar on algebraic groups and related finite groups (ed. A.Borel et al.), Lecture Notes in Mathematics 131 (Springer,Berlin, 1970),pp.168-266

[15] D.Gorenstein, R.Lyons, R.Solomon *The classification of finite simple groups III* Math. Surveys and Monographs Vol.40,no.3, Providence, Rhode Island

## Erklärung

Ich erkläre hiermit an Eides statt, daß ich die vorgelegte Dissertation selbstständig verfaßt, außer den angegeben Quellen und Hilfsmitteln keine weiteren benutzt und die den benutzten Werken wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

## Lebenslauf

| | |
|---|---|
| 1973 | geboren am 3.9. in Halle(Saale). |
| 1980-1990 | Besuch verschiedener Polytechnischer Oberschulen in Halle(Saale) |
| 1990 | Abschluß der 10. Klasse |
| 1990-1992 | Besuch der Spezialklassen für Mathematik und Informatik der Martin Luther Universität Halle-Wittenberg (MLU) |
| 1992 | Abitur |
| 1992 - 1997 | Studium der Mathematik an der MLU |
| 1997 | Mathematik Diplom an der MLU |
| seit 1997 | wiss. Mitarbeiter an der MLU, Beschäftigung an einem DFG-Projekt |