DISSERTATION

AUTOMORPHISM TOWERS OF GENERAL LINEAR GROUPS

Submitted by

Margrét Sóley Jónsdóttir

Department of Mathematics

In partial fulfillment of the requirements

for the degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Fall 2008

COLORADO STATE UNIVERSITY

August 26, 2008

WE HEREBY RECOMMEND THAT THE DISSERTATION PREPARED UNDER OUR SUPERVISION BY MARGRÉT SÓLEY JÓNSDÓTTIR ENTITLED "AUTOMORPHISM TOWERS OF GENERAL LINEAR GROUPS" BE ACCEPTED AS FULFILLING IN PART REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY.

Committee on Graduate Work

Professor Anton Betten

Professor Robert A. Liebler

Professor Ross McConnell

Adviser: Professor Alexander Hulpke

Department Head: Professor Gerhard Dangelmayr

ABSTRACT OF DISSERTATION

AUTOMORPHISM TOWERS OF GENERAL LINEAR GROUPS

Let G_0 be a group, G_1 be the automorphism group of G_0, G_2 the automorphism group of G_1 etc. The sequence of these groups together with the natural homomorphisms $\pi_{i,i+1} : G_i \to G_{i+1}$, which take each element to the inner automorphism it induces, is called the automorphism tower of G_0. If $\pi_{i,i+1}$ is an isomorphism for some i then the automorphism tower of G is said to terminate.

For a given group it is in general not easy to say whether its automorphism tower terminates. Wielandt showed in 1939 that if G is finite with a trivial center then the automorphism tower of G will terminate in a finite number of steps. Since then, some sporadic examples of automorphism towers of finite groups have been described but no general results have been proven.

In this thesis we study automorphism towers of finite groups with a non-trivial center. We look at the two extremes:

- Groups which are center-rich.
- Groups which have a small but non-trivial center.

We show that when looking for an infinite family of groups with terminating automorphism towers the first case is unfeasible. We then turn our attention to the

latter case, specifically general linear groups of dimension at least two. In odd characteristic $\mathrm{GL}(2,q)$ is not a split extension of the center. The first thing we do is to calculate the automorphism group of $\mathrm{GL}(2,q)$ for odd prime powers q. We provide explicit generators and describe the structure of $\mathrm{Aut}(\mathrm{GL}(2,q))$ in terms of well-known groups. In this case, the first automorphism group in the tower is a subdirect product of two characteristic factors. This structure is propagated through the tower and we use it to reduce the problem to studying subgroups of automorphism groups of smaller groups. We then use this structure to compute examples of automorphism towers of $\mathrm{GL}(2,q)$.

Margrét Sóley Jónsdóttir
Department of Mathematics
Colorado State University
Fort Collins, Colorado 80523
Fall 2008

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

1.1 History of the automorphism tower problem

The automorphism tower of a group G is defined to be the sequence of groups G_n together with maps $\pi_{n,n+1}\colon G_n \to G_{n+1}$, defined by

- $G_0 = G$
- $G_{n+1} = \mathrm{Aut}(G_n)$, for all $n \geq 0$.

The map $\pi_{n,n+1}$ is the natural map induced by conjugation and its image is the group of inner automorphisms of G_n. The tower is said to terminate if the map $\pi_{n,n+1}$ is an isomorphism for some n. A natural question to ask is:

Does this process terminate for a given group G?

This is the question Wielandt[Wie39] asked in 1939. He answered the question positively in the case when G is a finite group with a trivial center.

There are two ways to state the general tower problem: either remove the restriction that G must have a trivial center, or remove the restriction that G must be finite. Simon Thomas[Tho85] and Joel Hamkins[Ham98] have concentrated on the latter and found bounds on the cardinal number that is the height of the tower

if the starting group is infinite with a trivial center. No new results have been published for finite groups since Wielandt first asked the question. On his website Thomas has a preliminary version of a book[Tho] on the tower problem and in a book[Isa08] by Isaacs on finite group theory, which was published this year, there is a chapter on automorphism towers but neither gives any new results when G is a finite group with a non-trivial center.

1.2 Wielandt's result

Suppose G is a group. For any element $g \in G$, the homomorphism

$$h \mapsto h^g = g^{-1}hg, \text{ for any } h \in G$$

is an automorphism of G. An automorphism of this type is called an inner automorphism and the collection of all the inner automorphisms form a group which is denoted by $\mathrm{Inn}(G)$. The group of inner automorphisms is normal in the full automorphism group of G.

The inner automorphisms of groups with a trivial center have a useful property:

Lemma 1.2.1. *Suppose G is a group with a trivial center. Then $G \cong \mathrm{Inn}(G)$.*

Proof. It is clear that

$$\alpha : G \to \mathrm{Inn}(G) : g \mapsto (h \mapsto h^g = g^{-1}hg)$$

is a homomorphism, so we just need to prove that the kernel of the map is trivial. Suppose $g \in \ker(\alpha)$. Then $g^{-1}hg = h$ for all $h \in G$. This implies that g is in the center of G but the center is trivial and g is therefore the identity element of G. This shows that $G \cong \mathrm{Inn}(G)$. □

If we continue computing automorphism groups, then each group in the tower has a trivial center by the following lemma:

Lemma 1.2.2. *Suppose G is a group with a trivial center. Then* $\mathrm{Aut}(G)$ *also has a trivial center.*

Proof. Suppose ϕ is an automorphism of G which lies in the center of $\mathrm{Aut}(G)$. Then ϕ commutes with all elements of $\mathrm{Aut}(G)$; in particular it commutes with the inner automorphisms of G. Thus we have for all $g, h \in G$

$$h^{\phi^{-1}g\phi} = h^{g^{\phi}} = h^{g}.$$

Because G has a trivial center, this gives that $g = g^{\phi}$ for any $g \in G$. Thus ϕ is the identity element of $\mathrm{Aut}(G)$ and the center of $\mathrm{Aut}(G)$ is trivial. □

Now suppose G is a group with a trivial center. In this case we identify G with the group of inner automorphisms of G and lemmata 1.2.1 and 1.2.2 give:

$$G \lhd \mathrm{Aut}(G) \lhd \mathrm{Aut}(\mathrm{Aut}(G)) \lhd \mathrm{Aut}(\mathrm{Aut}(\mathrm{Aut}(G))) \lhd \ldots$$

Definition 1.2.3. *If there exist groups $G_1, G_2, \ldots, G_n$ such that*

$$G \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n \lhd A,$$

then G is said to be a subnormal subgroup of A.

Note that if G is a group with a trivial center, then G is a subnormal subgroup of any group in the automorphism tower of G. Furthermore, if G is a finite group we can use results on subnormal groups[Pet83, Sch55, Sch68] to see that the order of any group in the automorphism tower of G is bounded by a single constant

involving the order of G. Thus the orders of the groups in the automorphism tower of G form a non-decreasing sequence which is bounded above and therefore the group order must become stationary after a finite number of steps. Since each group in the tower is contained in the next group in the tower we see that after a finite number of steps each step in the tower is an isomorphism.

It is not possible to apply methods similar to Wielandt's method if the group has a non-trivial center. If the group has a non-trivial center, then the starting group is in general not a subnormal subgroup of the other groups in the tower. Also, the bound on the order of groups in the subnormal series depends on the groups in the series having a trivial center. Thus we cannot extend Wielandt's methods to groups with a non-trivial center.

1.3 Thesis outline

In this dissertation we study automorphism towers of finite groups with a non-trivial center. There are two extremes in the open cases for automorphism towers of finite groups with a non-trivial center:

- Groups that are far from having a trivial center.
- Groups that are close to having a trivial center.

We look at the first case in chapter 3 and the second in chapter 5. In the first case, which we call center-rich groups, we look at abelian groups and p-groups. In both of these cases the problem proves to be too difficult and in chapter 3 we will show why that is. The automorphism tower can only terminate if some group in the automorphism tower has no center. All $p-$groups have a non-trivial center and the automorphism group of a $p-$group is likely to again be a $p-$group[HM06]. Thus

the towers are likely to be too tall to be described in the level of detail required to compute the center. This is shown in section 3.1. In the case of abelian groups, the study of the automorphism towers is related to the study of which primes p divide $q-1$, where q is also a prime. The divisibility criteria can be analyzed using number theory and asymptotic graph theory. The behavior of the automorphism tower of an abelian group has random aspects and it cannot be said in which cases the automorphism tower is likely to terminate. This is shown in section 3.1.1.

The other extreme in the case of groups with a non-trivial center are groups which have a relatively small center compared to the size of the group. An example of these are general linear groups over a finite field and we study them in chapters 4 and 5. In chapter 4 we describe in detail the automorphism group of $\mathrm{GL}(2,q)$ for an odd prime q. We do this by giving explicit generators for the automorphism group as well as giving the abstract structure both as a direct product of two well understood groups and as a subdirect product of two characteristic factors of the group. In chapter 5 we go on to generalize this abstract structure to all groups in the automorphism tower of $\mathrm{GL}(2,q)$. It turns out that under special conditions on the groups in the tower, that seem to hold for all odd prime powers, any group in the tower is a subdirect product of two characteristic factors of the group, one of which does not change. The factor that does change can be computed without reference to the other factor or the to full group and therefore the computation of the automorphism tower can be reduced to calculating this smaller tower. This is both useful in practical situations, as computers can can be used to compute higher towers of larger groups because the groups involved will be smaller, and also to describe the theory of the tower as the groups in the reduced towers are smaller and have structure that is easier to describe. This process is described for

general linear groups of dimension 2 but could be done for higher dimensions and other related classes of groups. Finally, in section 5.2, we give conditions on certain prime powers that give rise to a sub-family of $\mathrm{GL}(2, q)$ where the groups in the family have related automorphism towers. These prime powers give automorphism towers which are in some cases easy to construct by hand and examples are given in 5.3.1.

Chapter 2

CONSTRUCTIONS AND ALGORITHMS

As stated earlier, there are two extremes in the open cases for automorphism towers of finite groups, namely the groups that are far from having a trivial center and the groups that are close to having a trivial center. General linear groups of dimension at least two are an example of groups with a relatively small center. To discuss this case we need to understand this class of matrix groups. In this chapter we give the definitions we will need and state the well-known results we will use. Unless the proof of a result gives some special insight into the theorem, it is omitted. We will also use some standard objects from group theory without defining them. Definitions of these objects can be found in [DF99].

2.1 Matrix groups

Definition 2.1.1. *The group of all $n \times n$ matrices with entries from a field $\mathbb{F}_q$ is called the general linear group of dimension n over $\mathbb{F}_q$ and is written* $\mathrm{GL}(n, q)$.

Definition 2.1.2. *The group of all the matrices of* $\mathrm{GL}(n, q)$ *with determinant 1 is the special linear group of dimension n over $\mathbb{F}_q$ and is written* $\mathrm{SL}(n, q)$.

Note that $\mathrm{SL}(n, q)$ is the derived subgroup of $\mathrm{GL}(n, q)$ and is therefore a characteristic subgroup of $\mathrm{GL}(n, q)$.

Lemma 2.1.3. *The center of* $\mathrm{GL}(n,q)$ *consists exactly of the diagonal matrices in* $\mathrm{GL}(n,q)$ *which have the same non-zero entry on the main diagonal. The center of* $\mathrm{GL}(n,q)$ *is a cyclic group. We call these matrices scalar matrices and write the center of* $\mathrm{GL}(n,q)$ *as* $Z(\mathrm{GL}(n,q))$ *or* Z

Definition 2.1.4. *The group* $\mathrm{GL}(n,q)/Z(\mathrm{GL}(n,q))$ *is called the projective general linear group of dimension* n *over* $\mathbb{F}_q$ *and is written* $\mathrm{PGL}(n,q)$.

Definition 2.1.5. *The group* $\mathrm{SL}(n,q)/Z(\mathrm{SL}(n,q))$ *is called the projective special linear group of dimension* n *over* $\mathbb{F}_q$ *and is written* $\mathrm{PSL}(n,q)$.

Lemma 2.1.6. $\mathrm{PSL}(n,q)$ *is a simple group for* $n \geq 2$ *except for* $\mathrm{PSL}(2,2)$ *and* $\mathrm{PSL}(2,3)$.

Proposition 2.1.7. *Suppose* q *is an odd prime power. Then*

$$H = \langle Z(\mathrm{GL}(2,q)), \mathrm{SL}(2,q) \rangle$$

is subgroup of $\mathrm{GL}(2,q)$ *of index* 2 *and* $S = Z \cap \mathrm{SL}(2,q)$ *is a subgroup of* $\mathrm{GL}(2,q)$ *of order 2.*

The structure of $\mathrm{GL}(2,q)$ described in proposition 2.1.7 can be seen in figure 2.1 on page 10.

For even prime powers q, $\mathrm{GL}(2,q)$ is a direct product of two characteristic subgroups $\mathrm{SL}(2,q)$ and $Z(\mathrm{GL}(2,q))$. The automorphism group in this case is the direct product of the automorphism groups of the two factors. To get to the description of the automorphism group of $\mathrm{GL}(2,q)$, q odd, we will need one more group. This is the group U shown in Figure 2.1.

Lemma 2.1.8. *Let* p *be an odd prime and* $q = p^n$. *Then* $\mathrm{GL}(2,q)$ *contains a subgroup* U *with* $U \cap H = Z$ *and such that* U *contains* Z *as a subgroup of index 2.*

Proof. First note that if U exists, it is generated by the generator of Z together with one matrix K with $K^2 \in Z$. If $K \notin \mathrm{SL}(2,q)$, then $U \cap H = Z$. It is therefore sufficient to show that $\mathrm{GL}(2,q)$ always contains a matrix which is not a product of a scalar matrix with a matrix with determinant 1 and whose square is in Z. The determinant of a 2×2 scalar matrix is a square, so we need to find a matrix K whose square is a scalar and whose determinant is a non-square. We now consider two cases depending of the congruence of $q \mod 4$.

First we consider the case $q \equiv 3 \mod 4$. In this case -1 is not a square, so $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \notin \langle Z, \mathrm{SL}(2,q) \rangle$ and we can choose K to be $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

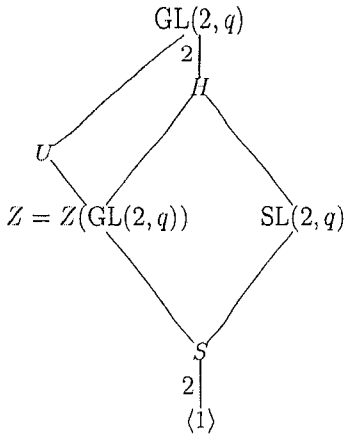
If $q \equiv 1 \mod 4$ we consider a matrix of the form $K = \begin{pmatrix} 1 & 1 \\ -c & -1 \end{pmatrix}$, where $c \in \mathbb{F}_q$. This matrix has determinant $d = c - 1$ and its square is the scalar matrix $K^2 = \begin{pmatrix} 1-c & 0 \\ 0 & 1-c \end{pmatrix}$. If we choose $c = 1 - \alpha$, where α is a primitive element of $\mathbb{F}_q$, then K is invertible. Note that if $d = -\alpha$ is a square in $\mathbb{F}_q$ then $\alpha = b^2(-1) = (b\sqrt{-1})^2$ is a square as well because -1 is a square in $\mathbb{F}_q$. The order of $\mathbb{F}_q^*$ is divisible by 2, so we know that α cannot be a square and therefore we have $K \notin \langle Z, \mathrm{SL}(2,q) \rangle$.

The two cases cover all odd primes, so U always exists. □

Corollary 2.1.9. *If $q \equiv 1 \mod 4$, then U is cyclic.*

Proof. Follows directly from the proof of lemma 2.1.8. □

Definition 2.1.10. *Suppose G is a group and M is a normal subgroup of G. If there exists a subgroup U of G such that $G = M \rtimes U$, then G is said to split over M and U is called a complement of M.*



- $\mathrm{SL}(2,q) = \langle s_1, s_2 \rangle$
- $Z = \left\langle \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \right\rangle$, $\mathbb{F}_q = \langle \alpha \rangle$.
- $U = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z \right\rangle$, $q \equiv 3 \mod 4$.
- $U = \left\langle \begin{pmatrix} 1 & 1 \\ \alpha - 1 & -1 \end{pmatrix} \right\rangle$, $q \equiv 1 \mod 4$.

Figure 2.1: The structure of $\mathrm{GL}(2,q)$ with q an odd prime power.

Note that we have that $\mathrm{GL}(2,q)/S$ splits over $\mathrm{SL}(2,q)/S$ and that the complement to $\mathrm{SL}(2,q)/S$ is U/S.

2.1.1 Affine general linear groups

Definition 2.1.11. *The group $(C_2)^n \rtimes \mathrm{SL}(n,2)$ is called the affine general linear group of dimension n over $\mathbb{F}_2$ and is written $\mathrm{AGL}(n,2)$. The multiplication in the group is $(\mathbf{v}, A)(\mathbf{w}, B) = (\mathbf{v}B + \mathbf{w}, AB)$ where $\mathbf{v}, \mathbf{w} \in (C_2)^n$ and $A, B \in \mathrm{SL}(n,2)$.*

Lemma 2.1.12. *Let $\mathbf{v}$ be a row vector of length n with entries from $\mathbb{F}_q$ and $\langle \mathbf{v} \rangle$ be the additive group generated by $\mathbf{v}$. The stabilizer $\mathrm{Stab}_{\mathrm{GL}(n,q)}(\langle \mathbf{v} \rangle)$, where the action is by right multiplication, is isomorphic to $\mathrm{AGL}(n-1,2)$.*

Lemma 2.1.13. *The group consisting of all matrices of the form*

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & \mathrm{GL}(n,2) & \\ * & & & \end{array}\right)$$

is isomorphic to $\mathrm{AGL}(n,2)$.

Lemma 2.1.14. $\mathrm{AGL}(1,2) \cong C_2$ *and* $\mathrm{AGL}(2,2) \cong S_4$, *where* S_4 *is the symmetric group acting on four points.*

Lemma 2.1.15. *The center of* $\mathrm{AGL}(n,2)$ *is trivial for* $n \geq 2$.

Proof. Recall that $\mathrm{AGL}(n,2) = (C_2)^n \rtimes \mathrm{GL}(n,2)$. Let C be the center of $\mathrm{AGL}(n,2)$ with $n \geq 2$ and ϕ the natural homomorphism from $\mathrm{AGL}(n,2)$ to $\mathrm{AGL}(n,2)/(C_2)^n$. The image of C under ϕ is contained in the center of $\mathrm{GL}(n,2)$ and therefore is trivial. This shows that $C \leq (C_2)^n$, i.e. the elements of C have form $(\mathbf{v}, I)$ where $\mathbf{v} \in (C_2)^n$ and I is the identity element of $\mathrm{GL}(n,2)$. The group C is the center of $\mathrm{AGL}(n,2)$, so $(-\mathbf{v}, I)(\mathbf{w}, A)(\mathbf{v}, I) = (\mathbf{w} - \mathbf{v}A + \mathbf{v}, A) = (\mathbf{w}, A)$. This implies $A\mathbf{v} = \mathbf{v}$ for all $A \in \mathrm{GL}(n,2)$. Therefore we have that $\mathbf{v}$ is the identity element of $(C_2)^n$ and C is trivial. □

When we build automorphism towers in chapter 5, we will need to understand the automorphism groups of affine general linear groups and therefore give a lemma with the structure of the relevant groups.

Lemma 2.1.16.

- $\mathrm{Aut}(\mathrm{AGL}(1,2)) \cong \langle 1 \rangle$
- $\mathrm{Aut}(\mathrm{AGL}(2,2)) \cong \mathrm{AGL}(2,2) \cong S_4$
- $\mathrm{Aut}(\mathrm{AGL}(3,2)) \cong \mathrm{AGL}(3,2) \rtimes C_2$
- $\mathrm{Aut}(\mathrm{AGL}(4,2)) \cong \mathrm{AGL}(4,2)$
- $\mathrm{Aut}(\mathrm{AGL}(5,2)) \cong \mathrm{AGL}(5,2)$

2.2 Description of the algorithm

To find automorphism groups we use an algorithm by Cannon and Holt[CH03]. This is a general algorithm that can be used for any finite group but we will only describe the aspects we explicitly use here. For detail and a full description of the algorithm, see [CH03].

Let G be a finite group. First we choose a characteristic series for G:

$$G = G_0 > G_1 > G_2 > \cdots > G_n = \langle 1 \rangle$$

where each group in the series is a characteristic subgroup of G. We also impose the extra condition that the quotient of two consecutive groups in the series is a cyclic group.

The idea is to use the automorphism group of G/G_k to help in the calculation of G/G_{k+1} until we have the automorphism group of $G/G_n \cong G$. To describe the algorithm we need to describe how to get from one quotient group to the next and to do that we can assume without loss of generality that the characteristic series is $G > M > \langle 1 \rangle$, where M is cyclic and $\mathrm{Aut}(G/M)$ is known.

We get from $\mathrm{Aut}(G/M)$ to $\mathrm{Aut}(G)$ with the help of three groups:

- C: the automorphisms which act trivially on M and induce the trivial action on G/M.
- B: the automorphisms which induce trivial action on G/M.
- A: the full automorphism group of G.

Lemma 2.2.1. *For the groups A, B and C described above, we have $C \lhd B \lhd A$.*

Proof. M is a characteristic subgroup of G and therefore any automorphism of G induces an automorphism of G/M. Let ϕ be the natural homomorphism from $\mathrm{Aut}(G)$ to $\mathrm{Aut}(G/M)$ which takes any automorphism of G to the induced automorphism on G/M. Then $B = \ker\phi$ and therefore normal in $A = \mathrm{Aut}(G)$. Now let ψ be the natural homomorphism which takes any automorphism of G to the induced automorphism on M. Then $C = \ker\psi \cap \ker\phi$ and is therefore a normal subgroup of B. □

2.2.1 Automorphisms centralizing both M and G/M

As above, C is the group of automorphisms of G which induce the identity on both M and G/M. Let $\phi \in C$. Then, for any $x \in G$, $x^\phi = x \cdot m$, where m is an element of M. Note that because M is abelian and ϕ acts trivially on M, we have

$$(xn)^\phi = x^\phi n^\phi = x^\phi n = xmn = (xn)m,$$

for any $n \in M$, so the image of $x \in G$ only depends on the coset in which x is. Thus we define a map τ from G/M to M by $(xM)^\tau = m$ where $m = x^{-1}x^\phi$.

Because ϕ is a homomorphism we get for all $x, y \in G$ the following condition for τ:

$$\begin{aligned} x \cdot y \cdot (xyM)^\tau &= (x \cdot y)^\phi \\ &= x^\phi \cdot y^\phi \\ &= x \cdot (xM)^\tau \cdot y \cdot (yM)^\tau \\ &= x \cdot y\,((xM)^\tau)^y\,(yM)^\tau \end{aligned}$$

Canceling $x \cdot y$ gives

$$(xyM)^\tau = ((xM)^\tau)^y\,(yM)^\tau$$

Setting $u = xM$ and $v = yM$, we get

$$(uv)^\tau = (u^\tau)^v \cdot v^\tau. \tag{2.1}$$

This is exactly the condition for τ being in the group of 1-cocycles, $Z^1(G/M, M)$[CNW90].

Conversely, if τ is a map in $Z^1(G/M, M)$, it satisfies (2.1) and if we set $\phi : G \to G : x \mapsto x(xM)^\tau$, then $\phi \in C$. Thus C corresponds to maps in $Z^1(G/M, M)$ and the only thing needed is a way to calculate $Z^1(G/M, M)$.

In our case $M \leq Z(G)$ and therefore G/M acts trivially on M and τ is a homomorphism. Finding $Z^1(G/M, M)$ when $M \not\leq Z(G)$ is similar to the case when $M \leq Z(G)$ but the latter case is easier to describe.

To find $Z^1(G/M, M)$ we need G/M written as a finitely presented group on a set of generators S with relators $\mathcal{R}$. We consider a map $\nu : G \to G$ which takes each element of G to a fixed $M-$coset representative. The images of elements of G under ν must satisfy the relators $\mathcal{R}$. Any automorphism $\phi \in C$ takes $x \in G$ to an element of the form $x \cdot m$ with $m \in M$ and the images $(x \cdot m)^\nu$ must satisfy the relators $\mathcal{R}$. Writing the relators in these images gives a linear system that we solve for the entries from M. Note that this is a homogeneous system and therefore is guaranteed to have at least one solution, namely the trivial one. The group M is abelian and therefore a direct product of elementary abelian subgroups. Therefore the elements of M can be written as vectors with the entries grouped by the different characteristics.

In practice we only need to store generators of $Z^1(G/M, M)$ and give the maps in $Z^1(G/M, M)$ as a vector of images for the generating set S of G/M.

2.2.2 Automorphisms centralizing G/M but not on M

Recall that B is the subgroup of automorphisms of G which induce the identity on G/M, but not necessarily on M and that M is a cyclic group. We add the further restriction that G splits over M.

Suppose $\phi \in B$. If m is an element of M and g an element of G, then we have $(m^g)^\phi = (m^\phi)^{g^\phi} = (m^\phi)^g$ because M is abelian and ϕ maps g to an element in the same M-coset. In the general setting, when M is an abelian characteristic subgroup of G, the restriction of ϕ to M is a module automorphism of M but in our case M is contained in the center of G and the equation above holds trivially. We therefore have the following lemma:

Lemma 2.2.2. *Suppose ϕ is an automorphism of G which centralizes G/M where M is a characteristic subgroup of G contained in the center of G. Then the restriction of ϕ to M is a group automorphism of M.*

Because G splits over M, each element g of G can be written uniquely in the form $m \cdot u$, where $m \in M$ and u is an element of the complement of M. We now claim that each automorphism ϕ of M gives rise to an automorphism $\hat{\phi}$ of G which induces ϕ on M and the identity on G/M. This automorphism is $g^{\hat{\phi}} = m^\phi \cdot u$, for any $g \in G$, written as a product of an element of M and an element from the complement of M. The map $\hat{\phi}$ is clearly bijective, so the only thing that needs to be shown is that $\hat{\phi}$ is a homomorphism.

Lemma 2.2.3. *Let U be the complement of M in G. Then the map*

$$\hat{\phi} : G \to G : \ m \cdot u \to m^\phi \cdot u,$$

where $u \in U$ and $m \in M$, is a group automorphism of G.

Proof. Suppose $m \cdot u$ and $n \cdot v$ are elements of G where $m, n \in M$ and $u, v \in U$. Because $(m \cdot u)(n \cdot v) = (mn^u) \cdot uv$ we have

$$((m \cdot u)(n \cdot v))^{\hat{\phi}} = ((mn^u) \cdot uv)^{\hat{\phi}}$$

and because ϕ is a homomorphism this equals $m^{\phi}(n^u)^{\phi} \cdot uv$. Because M is an abelian group and ϕ maps an element from one $M-$coset to the same coset, this again equals

$$m^{\phi}\left(n^{\phi}\right)^{u} \cdot uv = (m^{\phi} \cdot u)(n^{\phi} \cdot v) = (m \cdot u)^{\hat{\phi}}(n \cdot v)^{\hat{\phi}}.$$

This shows that $\hat{\phi}$ is a homomorphism. □

We now know that if G splits over M, the automorphisms from B/C correspond to automorphisms of M and we can generate B by the generators of C together with automorphisms of the type $m \cdot u \mapsto m^{\phi} \cdot u$ where $m \in M$, $u \in U$ and ϕ is an automorphism of M. The group M is cyclic so we can easily find the full automorphism group of M and we have all of B.

2.2.3 Automorphisms centralizing neither G/M nor M

Recall that A is the full automorphism group of G. Since we already have all the automorphisms which induce the identity on G/M we now only need to consider the automorphisms which induce non-trivial automorphisms on G/M. If ϕ is an automorphism of G which induces $\overline{\phi}$ we say that ϕ is a lift of $\overline{\phi}$ or that $\overline{\phi}$ lifts to ϕ.

Lemma 2.2.4. *Suppose ϕ_1 and ϕ_2 are two lifts of $\overline{\phi} \in \mathrm{Aut}(G/M)$. Then $\phi_2\phi_1^{-1} \in B$, i.e. $\phi_2\phi_1^{-1}$ induces the identity on G/M.*

Note that by lemma 2.2.4 we only need to determine whether a given automorphism $\overline{\phi} \in \mathrm{Aut}(G/M)$ lifts and, if it lifts, find a single automorphism ϕ of G which induces it because we already have the automorphisms of G which induce the identity on G/M.

In our context it will be clear how automorphisms lift but for a general description see [CH03].

2.3 Subdirect products

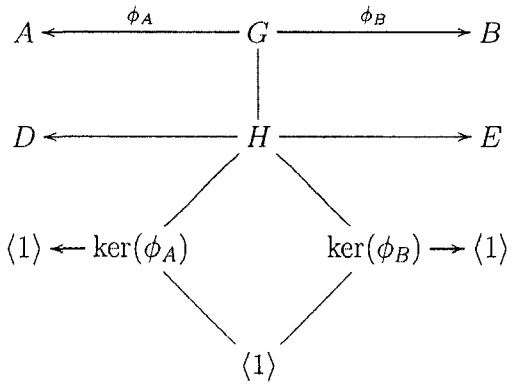


Figure 2.2: G is a subdirect product of $G/\ker(\phi_A)$ and $G/\ker(\phi_B)$.

Lemma 2.3.1. *Suppose G, A and B are groups and*

$$\phi_A : G \to A \text{ and } \phi_B : G \to B$$

are surjective homomorphisms with non-intersecting kernels. Let π_A and π_B be the natural maps

$$\pi_A : A \to A/\left(\ker(\phi_B)\right)^{\phi_A} \text{ and } \pi_B : B \to B/\left(\ker(\phi_A)\right)^{\phi_B}.$$

Furthermore, let $\psi : A/\left(\ker(\phi_B)\right)^{\phi_A} \to B/\left(\ker(\phi_A)\right)^{\phi_B}$, *defined by* $\left(\left(g_A^{\phi}\right)^{\pi_A}\right)^{\psi} = \left(g_B^{\phi}\right)^{\pi_B}$. *Then the set* $K = \{(a,b) \in A \times B | \left(\left(a^{\phi_A}\right)^{\pi_A}\right)^{\psi} = \left(b^{\phi_B}\right)^{\pi_B}\}$ *is a subgroup of* $A \times B$ *isomorphic to* G.

Proof. K is a subset of $A \times B$ so we just need to show that K is closed under the group operation. Suppose $(a_1, b_1), (a_2, b_2) \in K$. Then we have $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$ and $\left((a_1 a_2)^{\pi_A}\right)^{\psi} = \left(a_1^{\pi_A}\right)^{\psi} \left(a_2^{\pi_A}\right)^{\psi} = b_1^{\pi_B} b_2^{\pi_B} = (b_1 b_2)^{\pi_B}$, so $(a_1, b_1)(a_2, b_2) \in K$ and K is a group.

Let $\tau : G \to K; g \mapsto \left(g^{\phi_A}, g^{\phi_B}\right)$. Note that by choice of ψ, we have $\left(\left(g^{\phi_A}\right)^{\pi_A}\right)^{\psi} = \left(g^{\phi_B}\right)^{\pi_B}$ and τ is clearly a homomorphism.

If $g^{\tau} = (1,1)$ then $g \in \ker(\phi_A) \cap \ker(\phi_B) = \langle 1 \rangle$, so τ is injective.

Suppose $(a,b) \in K$. The map ϕ_A is surjective, so there exists a $g \in G$ with $g^{\tau} = (a, \widetilde{b})$. Then $g^{\tau}(a,b)^{-1} = (1, \widetilde{b}b^{-1})$. The element $(1, \widetilde{b}b^{-1})$ is in K, so $\widetilde{b}b^{-1} \in \ker(\phi_A)^{\phi_B}$. Let $f \in G$ such that $f^{\phi_B} = \widetilde{b}b^{-1}$. Then $(f^{-1}g)^{\tau} = \left(1, \left(f^{\phi_B}\right)^{-1}\right) \cdot \left(a, \widetilde{b}\right) = (a,b)$, so τ is surjective. This shows that $\tau : G \to K$ is an isomorphism. □

Definition 2.3.2. *If* G, A *and* B *are as in lemma 2.3.1 then* G *is said to be a subdirect product of* A *and* B *and is written* $G \cong A \perp B$.

Note:

The notation $A \perp B$ does not define a unique group up to isomorphism and must be read in context.

Theorem 2.3.3. *Suppose* G *is a group,* S *and* T *are two non-intersecting characteristic subgroups of* G *and* $H = \langle S, T \rangle$. *Suppose furthermore that* G/S *only*

has inner automorphisms. Let $A_S = \mathrm{Aut}(G/S)$ *and* A_T *be the subgroup of* $\mathrm{Aut}(G/T)$ *which induces inner automorphisms on* G/H *via the natural isomorphism* $(G/T)/(H/T) \cong G/H$. *Let*

$$\pi_S : A_S \to \mathrm{Aut}(G/H)$$

$$\pi_T : A_T \to \mathrm{Aut}(G/H)$$

via the natural isomorphisms $G/H \cong (G/S)/(H/S) \cong (G/T)/(H/T)$. *Then* $\mathrm{Aut}(G) \cong A_S \curlywedge A_T = \{(\sigma, \tau) \in A_S \times A_T | \sigma^{\pi_S} = \tau^{\pi_T}\}$.

Proof. By lemma 2.3.1 G is a subdirect product of G/S and G/T. Let ϕ_S : $\mathrm{Aut}(G) \to A_S$ be the homomorphism which takes an automorphism of G to the induced automorphism on G/S. The group S is a characteristic subgroup of G so ϕ_S is well defined. Any element in A_S is an inner automorphism by an element $Sg \in G/S$ and is induced by the automorphism of G, namely conjugation by g. This implies that ϕ_S is surjective. Let $\eta : \mathrm{Aut}(G) \to \mathrm{Aut}(G/T)$ be the homomorphism which takes an automorphism of G to the induced automorphism on G/T. Any automorphism of G induces an inner automorphism on G/S and therefore on G/H, so the image of η is contained in A_T. Let $\phi_T : \mathrm{Aut}(G) \to A_T : \psi \mapsto \psi^\eta$. Any automorphism τ of A_T induces an inner automorphism on G/H. This same inner automorphism of G/H can be induced by an automorphism σ of G/S via π_S. Let $\psi : G/S \curlywedge G/T \to G/S \curlywedge G/T : (s,t) \mapsto (s^\sigma, t^\tau)$. Since σ and τ agree on G/H and σ and τ are both automorphisms, this is a well defined automorphism. The automorphism ψ induces τ on G/T, so ϕ_T is surjective.

Now suppose $\psi \in \ker(\phi_S) \cap \ker(\phi_T)$. Then ψ acts trivially on G/S and on G/T and therefore also acts trivially on $G \leq G/S \times G/T$.

We therefore have $\mathrm{Aut}(G) \cong A_S \curlywedge A_T = \{(\sigma, \tau) \in A_S \times A_T | \sigma^{\pi_S} = \tau^{\pi_T}\}$. □

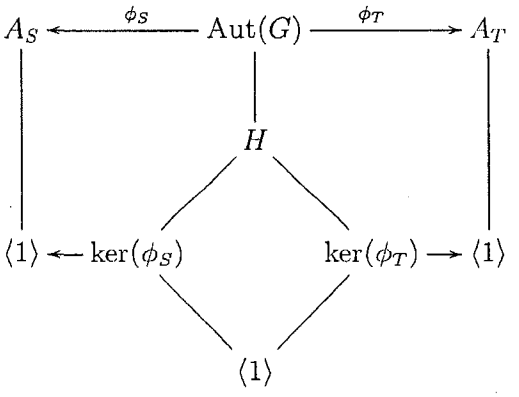


Figure 2.3: $\mathrm{Aut}(G)$ is a subdirect product of $\mathrm{Aut}(G)/\ker(\phi_S)$ and $\mathrm{Aut}(G)/\ker(\phi_T)$.

Subdirect products are a generalization of direct products and this work is related to work currently being done to describe automorphism groups in terms of subgroups and quotient groups[Die07, MP03].

Corollary 2.3.4. *Suppose G is a group, S and T are two non-intersecting characteristic subgroups of G and $H = \langle S, T \rangle$. Suppose furthermore that G/S has only inner automorphisms and that G/H is abelian. Let $A_S = \mathrm{Aut}(G/S)$ and A_T be the subgroup of $\mathrm{Aut}(G/T)$ which induces trivial automorphisms on G/H via the natural isomorphism $(G/T)/(H/T) \cong G/H$. Then $\mathrm{Aut}(G) \cong A_S \times A_T$.*

Chapter 3

THE EXTREME CASES

3.1 $p-$groups

In the extreme case of a group being center-rich, one of the classes of groups to look at is the class of $p-$groups. Though $p-$groups do not always have a large center they somehow have "as much center as possible" as corollary 3.1.3 will show.

Definition 3.1.1. *Suppose G is a group. If G has order p^n, where p is a prime then G is said to be a $p-group$.*

Lemma 3.1.2. *Suppose G is a $p-$group. Then G has a non-trivial center.*

Corollary 3.1.3. *Any non-trivial subgroup and any non-trivial quotient group of a $p-$group is again a $p-$group.*

Corollary 3.1.3 shows that $p-$groups and groups which derive from them have a non-trivial center and thus they are an obvious candidates to look at when studying groups with a non-trivial center. Recently new results[HM07] have been proven about the automorphism groups of p-group which are useful when trying to determine whether automorphism towers of $p-$groups are likely to terminate. Before we can state that result we need to define two new ways of measuring the size of a group.

Definition 3.1.4. *A group G is minimally generated by d elements if there exist elements $g_1, g_2, \ldots, g_d \in G$ such that $G = \langle g_1, g_2, \ldots g_d \rangle$ but $\langle f_1, f_2, \ldots f_{d-1} \rangle \neq G$ for all $f_1, f_2, \ldots f_{d-1} \in G$.*

Definition 3.1.5. *Fix a prime p. For any group H the lower $p-$series*

$$H = H_1 \geq H_2 \geq \ldots$$

of H is defined by $H_{i+1} = H_i{}^p[H_i, H]$ for $i \geq 1$ where

$$[H_i, H] = \left\langle h_i^{-1} h^{-1} h_i h | h_i \in H_i, h \in H \right\rangle.$$

The group H is said to have lower $p-$length n, if H_n is the last non-identity element of the lower $p-$series.

Proposition 3.1.6. *Suppose H is s finite group. Then H is a $p-$group if and only if H has a finite p-length.*

Now we have three ways of describing the size of a p-groups: the $p-$length, the number of generators and the size of the prime p. This allows us to state a theorem describing the proportion of p-groups that have a $p-$group as their automorphism group by letting one of the three parameters go to infinity at a time.

Theorem 3.1.7. *[HM07] Fix a prime p and positive integers d and n. Let $r_{d,n}$ be the proportion of $p-$groups minimally generated by d elements and with lower $p-$length at most n whose automorphism group is a $p-$group. If $n \geq 2$, then*

$$\lim_{d \to \infty} r_{d,n} = 1.$$

If $d \geq 5$, then

$$\lim_{n \to \infty} r_{d,n} = 1.$$

If $n = 2$ *and* $d \geq 10$, *or* $n \geq 3$ *and* $d \geq 6$ *or* $n \geq 10$ *and* $d \geq 5$ *then*

$$\lim_{p \to \infty} r_{d,n} = 1.$$

Theorem 3.1.7 says that for almost all $p-$groups the automorphism groups is again a $p-$group though it is not in the sense that we consider all groups of order p^n and let n got to infinity. Recall that by lemma 3.1.3 any $p-$group has a non-trivial center and that if the tower terminates the last group in the tower must be have a trivial center. This implies that while the groups in the automorphism tower of a group are $p-$groups the tower cannot terminate. Theorem 3.1.7 implies that $p-$groups are not good candidates if we are looking for groups with automorphism towers which terminate after few steps. They might be a good candidate if we wanted to find groups with non-terminating towers but that would be another study and here we must abandon $p-$groups as they are too difficult.

3.1.1 Abelian groups

Abelian groups are another example of groups that are far from having a trivial center. For these the center is the whole group. Each finite abelian group can be written as a direct product of cyclic groups so it is useful to understand the automorphism groups of cyclic groups.

Lemma 3.1.8. *[Hup] Suppose* G *is a finite cyclic group of order* G^m. *Then*

$$\mathrm{Aut}(G) \cong \begin{cases} C_2 \times C_{2(m-2)} & \text{if } p = 2 \\ C_{p-1} \times {C_p}^{m-1} & \text{if } p \text{ is odd} \end{cases}$$

Suppose G is a direct product of cyclic groups of prime power order, where any two factors are coprime and let A be the automorphism group of G. In this

case A is the direct product of the automorphism groups of the factors of G. If the factors of A have coprime orders, it is easy to describe the automorphism group of A. The problem here is that the factors usually do not have coprime orders. If, for example, p and q are two odd primes, then $q-1$ and $p-1$ always have a prime divisor in common, namely 2. This means that the factors in the next step will not be coprime. One problem that needs to be considered is how to describe the potential prime divisors of orders of groups in the tower and give a general description of what kind of primes can come up as divisors of $q-1$. This is not necessarily an easy problem and a study of asymptotic behavior can be used to get an insight into the difficulties.

Before we can describe the relationship between the automorphism towers of abelian groups and graph theory we need to describe the process of building a random graph. First we fix a set of vertices V. For any un-ordered pair of vertices in V, the two vertices are connected by an edge with independent probability $\frac{1}{2}$. The resulting graph is called a random graph on V.

Theorem 3.1.9. *[Cam99] There exists a graph on countably many vertices such that any random graph on a countable number of vertices is isomorphic to this graph. This graph is called the countable random graph.*

There is a way to describe the random countable graph that does not involve probability and this description is more convenient in our case.

Theorem 3.1.10. *[Cam99] Suppose R is a graph on a countable number of vertices such that for any pair of finite disjoint set of vertices U and V there is a vertex of R adjacent to every vertex in U and to none in V. Then R is isomorphic to the countable random graph.*

To see how this is related to our situation we need the following lemma:

Lemma 3.1.11 (Dirichlet's theorem). *[Neu92] If integers a and b are relatively prime, then the sequence*

$$s_n = an + b,\ n = 1, 2, \ldots$$

contains an infinite number of primes.

Theorem 3.1.12. *[Jon] Let Π be the graph whose vertices are all odd primes and there is an edge between p and q exactly if $q|p-1$. Then Π is isomorphic to the random graph.*

Proof. Suppose U and V are disjoint finite subsets of Π. By the Chinese remainder theorem the simultaneous congruences

$$p \equiv \begin{cases} 1 \mod q & \forall q \in U \\ -1 \mod q & \forall q \in V \end{cases}$$

are equivalent to a single congruence

$$p \equiv c \mod n,$$

where $n = \prod_{q \in U \cup V} q$ and c is coprime to n.

By Dirichlet's theorem, there is at least one $p \in \Pi$ satisfying this congruence, so p is adjacent to every $q \in U$ and to no $q \in V$. Hence Π is isomorphic to the random graph. □

Note:

We want to describe the behavior of the automorphism tower of cyclic groups and have just seen that is very related to describing patterns in the random countable graph. Because any behavior occurs in the random graph it is impossible to give

general rules or algorithms for determining all primes that might come up when computing automorphism towers of cyclic groups and therefore infeasible to describe the general behavior of automorphism towers of cyclic groups.

3.2 Direct products of non-abelian simple groups

For any finite group with a trivial center, the automorphism tower of the group terminates in a finite number of steps[Wie39]. An extreme in the case of groups with a trivial center is the case non-abelian simple groups. Not only do they not have a non-trivial center but the also have no non-trivial normal subgroups at all. A slightly more general situation is to consider direct products of non-abelian simple groups. In this section we will show that for groups that are a direct product of non-abelian simple group, the tower terminates in at most two steps.

Lemma 3.2.1. *Let G be a group and H a normal subgroup of G. If S is a characteristic subgroup of H, then S is a normal subgroup of G.*

Proof. Suppose $s \in S$ and $g \in G$. Since H is a normal subgroup of G, the conjugation of an element $g \in G$ induces an automorphism of H. The group S is a characteristic subgroup of H and any automorphism of H leaves S invariant. Therefore we have $g^{-1}sg \in S$ for any $s \in S$, so S is a normal subgroup of G. □

Lemma 3.2.2. *Let $G = R \times S$. Then any element of G can be written uniquely in the form rs, where $r \in R$ and $s \in S$.*

Corollary 3.2.3. *Let $G = R \times S$. Then the conjugation action of R on S is trivial.*

Proof. Any element of G can be written uniquely in the form rs with $r \in R$ and $s \in S$. Let $r_1, r_2 \in R$ and s_1, s_2 in S. Then $(r_1 s_1)(r_2 s_2) = (r_1 r_2)(s_1^{r_1} s_2)$ with $r_1 r_2 \in R$ and $s_1^{r_1} s_2 \in S$. We also have $(r_1 s_1)(r_2 s_2) = (r_1 r_2^{s_1^{-1}})(s_1 s_2)$ with $r_1 r_2^{s_1^{-1}} \in R$ and $s_1 s_2 \in S$. Since any element factories uniquely into rs with $r \in R$ and $s \in S$ we have $s_1^{r_1} = s_1$ for any $r_1 \in R$ and s_1 in S, so the conjugation action of R on S is trivial. □

Definition 3.2.4. *The socle of G is the group generated by all the minimal normal subgroups of G. We denote this group by* $\mathrm{Soc}(G)$.

Lemma 3.2.5. *Suppose G is the direct product of non-abelian simple groups, $G = S_1 \times S_2 \times \cdots \times S_n$. Then $G \cong \mathrm{Soc}(\mathrm{Aut}(G))$.*

Proof. G has a trivial center and thus we can identify G with its groups of inner automorphisms. We write the group of inner automorphisms of G as G.

Suppose that $S_1, \ldots, S_k$ are isomorphic and S_1 is not isomorphic to S_l for any $l > k$. Then $S = S_1 \times S_2 \times \cdots \times S_k$ is a characteristic subgroup of G. Because $G \lhd \mathrm{Aut}(G)$, S is normal in $\mathrm{Aut}(G)$ by lemma 3.2.1. For any $i, j \in \{1..k\}$ there is an element in $\mathrm{Aut}(G)$ which switches S_i and S_j and none of the S_i have non-trivial normal subgroups. Therefore S is a minimal normal subgroup of $\mathrm{Aut}(G)$. This shows that G is contained in the socle of $\mathrm{Aut}(G)$.

Suppose $r \in \mathrm{Soc}(\mathrm{Aut}(G))$. Then $\mathrm{Aut}(G)$ contains a minimal normal subgroup R_i, with $r \in R_i$. This holds for any $r \in \mathrm{Aut}(G)$. The groups R_i and G are normal subgroups of $\mathrm{Aut}(G)$ so we know that the socle has the form $G \times R_1 \times R_2 \times \cdots \times R_l$. Let $R = R_1 \times R_2 \times \cdots \times R_l$. Then $\mathrm{Soc}(\mathrm{Aut}(G)) = G \times R$ and any $\phi \in R$ must act trivially on G by lemma 3.2.3 and therefore acts trivially on G. This shows that ϕ is the identity element of $\mathrm{Aut}(G)$ and therefore R is trivial and $G \cong \mathrm{Soc}(\mathrm{Aut}(G))$. □

Corollary 3.2.6. *If G is the direct product of non-abelian simple groups, then* $\mathrm{Aut}(G)$ *contains a characteristic subgroup isomorphic to* G.

Proof. $\mathrm{Soc}(\mathrm{Aut}(G)) \cong G$ is a characteristic subgroup of $\mathrm{Aut}(G)$. □

Corollary 3.2.7. *If G is the direct product of non-abelian simple groups, then* $\mathrm{Aut}(G)$ *only has inner automorphisms.*

Proof. Suppose ϕ is an automorphism of $\mathrm{Aut}(G)$. We identify G and the socle of $\mathrm{Aut}(G)$. The socle is a characteristic subgroup of $\mathrm{Aut}(G)$ so we can restrict ϕ to G. All automorphisms of G are inner automorphisms of $\mathrm{Aut}(G)$, so there exists an inner automorphism ψ of $\mathrm{Aut}(G)$ which has the same action as ϕ on G. Let $\tau = \psi\phi^{-1}$. Then τ is an automorphism of $\mathrm{Aut}(G)$ which acts trivially on G.

We study the action of τ on an element γ of $\mathrm{Aut}(G)$. For any element $g \in G$ we have

$$\begin{aligned} g^{\gamma^\tau} &= g^{\tau^{-1}\gamma\tau} \\ &= \left((\tau|_G)g(\tau^{-1}|_G)\right)^{\gamma\tau} \\ &= g^{\gamma\tau} \\ &= \left((\tau^{-1}|_G)g^\gamma(\tau|_G)\right) \\ &= g^\gamma. \end{aligned}$$

The last equality holds because τ acts trivially on G. Therefore $\gamma = \gamma^\tau$ so τ must be the identity. This shows that all automorphisms of $\mathrm{Aut}(G)$ are inner automorphisms. □

Chapter 4

AUTOMORPHISM GROUPS OF GENERAL LINEAR GROUPS OF DIMENSION 2

4.1 Set-up for automorphism group algorithm

To find the automorphism group of $\mathrm{GL}(2,q)$ we use the algorithm described in section 2.2.

The first step in the algorithm is to choose a characteristic series of subgroups of $\mathrm{GL}(2,q)$, where the largest group other than $\mathrm{GL}(2,q)$ is the center of $\mathrm{GL}(2,q)$.

We already have such a series from proposition 2.1.7:

$$\mathrm{GL}(2,q) \triangleright Z \triangleright S \triangleright \langle 1 \rangle,$$

where Z is the center of $\mathrm{GL}(2,q)$ and $S = Z \cap \mathrm{SL}(2,q)$. We assume that $\mathrm{Aut}(\mathrm{GL}(2,q)/Z)$ is known and use that to find $\mathrm{Aut}(\mathrm{GL}(2,q)/S)$ and then use $\mathrm{Aut}(\mathrm{GL}(2,q)/S)$ to finally get the full automorphism group $\mathrm{Aut}(\mathrm{GL}(2,q))$.

In the case of $\mathrm{GL}(2,q)$, q odd, we have two lifting steps:

- From G/Z to G/S,
- From G/S to G itself.

To do the lifting we need a description of $\mathrm{PSL}(2,q)$.

Proposition 4.1.1 (Steinberg presentation for $\mathrm{PSL}(2,q)$). *[Car89] Let G be the finitely presented group given on the generators $\{x_1(t), x_{-1}(t) | t \in \mathbb{F}_q\}$ subject to the relations R_1, R_2 and R_3.*

For $r \in \{\pm 1\}$:

- $R_1 = \{x_r(t_1)x_r(t_2) = x_r(t_1 + t_2)\}$
- $R_2 = \{n_r(t)x_r(u)n_r(t)^{-1} = x_{-r}(-t^{-2}u),\ t, u \in K,\ t \neq 0\}$
- $R_3 = \{h_r(t_1)h_r(t_2) = h_r(t_1t_2),\ t_1t_2 \neq 0\}$

where

$$h_r(t) = n_r(t)n_r(-1)$$

and

$$n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t).$$

The group $G/Z(G)$ is isomorphic to $\mathrm{PSL}(2,q)$, and an isomorphism is given by the surjective homomorphism

$$\phi : \mathrm{SL}(2,q) \to G/Z(G) : \begin{cases} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \mapsto x_1(t)Z(G) \\ \\ \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \mapsto x_{-1}(t)Z(G) \end{cases}$$

which has as its kernel the center of $\mathrm{SL}(2,q)$.

When computing the automorphism group of $\mathrm{GL}(2,q)$ factor groups isomorphic to $\mathrm{PSL}(2,q)$ come up and we use the description of $\mathrm{PSL}(2,q)$ to restrict the behavior of automorphisms of $\mathrm{GL}(2,q)$ on those by using the following corollary.

Corollary 4.1.2. *Suppose q is an odd prime power and that M is an abelian group which centralizes* $\mathrm{PSL}(2,q)$. *Suppose furthermore that M has order dividing $q-1$. If ϕ is a homomorphism such that for any $g \in \mathrm{PSL}(2,q)$ there exists $m \in M$ with $g^\phi = mg$, then ϕ is the trivial map.*

Proof. By Proposition 4.1.1, $\mathrm{PSL}(2,q)$ is a homomorphic image of a group G satisfying the relators on 4.1.1. The elements

$$\{x_r(\alpha^n), \text{ where } \alpha \text{ is a generator of } \mathbb{F}_q^*,\ r \in \{1,-1\}\}$$

generate $\mathrm{PSL}(2,p^n)$ and must therefore satisfy the relators in Proposition 4.1.1.

Let $m_i, n_j \in M$ be such that

- $x_1(\alpha^t)^\phi = m_t x_1(\alpha^t)$
- $x_{-1}(\alpha^t)^\phi = n_t x_{-1}(\alpha^t)$.

The map ϕ is a homomorphism, so the images must also satisfy the relators. Since m_i and n_j centralize $\mathrm{PSL}(2,q)$, we use R_1 and R_2 to get

$$m_i = (n_{i-2j})^{-1} \text{ for all } i \text{ and } j.$$

By setting $i = 0$ we get that $m_0 = (n_{2j})^{-1}$ for all j. This shows that

$$m_{2i} = (n_{2i})^{-1} = e$$

for all i where e is a fixed element of M. Similarly, we get

$$m_{2i+1} = (n_{2i+1})^{-1} = o \in M.$$

We study the odd and even indices separately. Setting $u = 4$ and $t = 2$ in R_2 gives $m_0^4 = n_0^{-1}$. Since $m_0 = n_0^{-1} = e$ this gives that $e^3 = 1$.

If the characteristic of $\mathbb{F}_q$ is 3, then 3 does not divide $(q-1)$. In this case M has no elements of order 3 and therefore e must be trivial. We therefore assume 3 does not divide q. In this case we set $u = 9$ and $t = 3$ in R_2 and get $e^9 = e$, so the order of e is even and a divisor of 3 and e must be trivial. We treat the odd indices in a similar manner. First set $t = 2\alpha$ and $u = 4\alpha^3$ in R_2 to get $o^3 = 1$. Now, M either does not have any elements of order 3 or the characteristic of the field is not 3 and we can set $t = 3\alpha$ and $u = 9\alpha^3$ in R_2 to get that o^8 is trivial. In either case o must be the identity element of M.

We have that the elements m_i and n_i are trivial, so ϕ is trivial.

□

4.2 First lifting

When calculating the automorphism group of $\mathrm{GL}(2,q)$, q odd, we need to determine the subgroups described section 2.2. To do this, we can use the presentation of $\mathrm{PSL}(2,q)$ given in proposition 4.1.1. In this section C is the group of automorphisms of G/S which centralize both Z/S and $(G/S)/(Z/S)$, B is the group containing automorphisms which centralize $(G/S)/(Z/S)$ and A is the full automorphism group of G/S.

Proposition 4.2.1.

$$C \cong \begin{cases} \langle 1 \rangle, & \text{if } q \equiv 3 \mod 4 \\ C_2, & \text{if } q \equiv 1 \mod 4 \end{cases}$$

Proof. G/S is a product of U/S and $\mathrm{SL}(2,q)/S \cong \mathrm{PSL}(2,q)$. Let ϕ be an automorphism in C. The automorphism ϕ takes any element g from G/S to gm where $m \in Z/S$. We can describe the action of ϕ on G/S by its action on U/S, its

action $\mathrm{PSL}(2,q)$ and the interaction between the two groups. For each element in $\mathrm{PSL}(2,q)$, ϕ acts as multiplication by an element in the centralizer of $\mathrm{PSL}(2,q)$. Therefore ϕ acts trivially on $\mathrm{PSL}(2,q)$ by Corollary 4.1.2.

Now we need to study the action of ϕ on U/S. The group U/S is generated by two elements z and u with z a generator of the cyclic group Z/S and $u \notin Z/S$ with $u^2 = z^k$ for some integer k. The automorphism ϕ acts trivially on Z/S, so we only need to study the action on u. Let $m \in Z/S$ be such that $u^\phi = um$. The element u^2 is in Z/S so $(u^2)^\phi = u^2m^2 = u^2$ so $m^2 = 1$. Therefore the element m has order 1 or 2. If $q \equiv 3 \mod 4$, then Z/S contains no element of order 2, so $|C| = 1$. If $q \equiv 1 \mod 4$, then Z/S contains exactly one element of order 2 and $|C| \leq 2$. This element m does give an automorphism, so $|C| = 2$. □

Proposition 4.2.2. *$B/C \cong \mathrm{Aut}(C_{\frac{q-1}{2}})$ and has order $\phi(\frac{q-1}{2})$.*

Proof. The size of B/C is the size of $\mathrm{Aut}(Z/S)$. The group Z/S is cyclic of order $\frac{q-1}{2}$. A generator z of Z/S can be taken to any element $z^k \in Z/S$ with k coprime to $\frac{q-1}{2}$. There are $\phi(\frac{q-1}{2})$ such numbers k and any such map is an automorphism, so $B/C \cong \mathrm{Aut}(C_{\frac{q-1}{2}})$ and has order $\phi(\frac{q-1}{2})$. □

To determine A we need to understand the automorphisms of $\mathrm{PSL}(2,q)$ and, to do that, we use the following lemma:

Lemma 4.2.3. *[CCN+85] Let p be an odd prime and $n \in \mathbb{N}$. Then the group of outer automorphisms of $\mathrm{PSL}(2,p^n)$ is a direct product of the group of diagonal automorphisms, which has order 2, and the group of field automorphisms of $\mathbb{F}_{p^n}$.*

Lemma 4.2.4. *Let p be an odd prime and $n \in \mathbb{N}$. Then the only outer automorphisms of $\mathrm{PGL}(2,p^n)$ are the field automorphisms of $\mathbb{F}_{p^n}$.*

Lemma 4.2.5. *Let q be a prime power. Then* $\mathrm{Aut}(\mathrm{PSL}(2,q)) \cong \mathrm{Aut}(\mathrm{PGL}(2,q))$.

Proof. $\mathrm{PSL}(2,q)$ is the socle of $\mathrm{PGL}(2,q)$ so any automorphism of $\mathrm{PGL}(2,q)$ restricts to an automorphism of $\mathrm{PSL}(2,q)$. Let ϕ be a map in the kernel of the natural homomorphism $\mathrm{Aut}(\mathrm{PGL}(2,q)) \to \mathrm{Aut}(\mathrm{PSL}(2,q))$. The kernel consists of those automorphisms of $\mathrm{PGL}(2,q)$ which act trivially on $\mathrm{PSL}(2,q)$. Let $a \in \mathrm{PSL}(2,q)$, $b \in \mathrm{PSL}(2,q)$ and $c = b^a$. Then $c = c^\phi = (b^\phi)^{a^\phi} = b^{a^\phi}$. That is, a and a^ϕ have the same action on $\mathrm{PSL}(2,q)$, so $a^{-1}a^\phi$ is in the centralizer of $\mathrm{PSL}(2,q)$. Because the centralizer of $\mathrm{PSL}(2,q)$ in $\mathrm{PGL}(2,q)$ is trivial the automorphism ϕ must be trivial. By lemmata 4.2.3 and 4.2.4 we know that $|\mathrm{Aut}(\mathrm{PSL}(2,q))| = |\mathrm{Aut}(\mathrm{PGL}(2,q))|$, so the two groups must be isomorphic. □

Proposition 4.2.6. *$A/B = \mathrm{Aut}(\mathrm{PSL}(2,q))$, where $q = p^n$ with p an odd prime.*

Proof. We are lifting from $G/Z \cong \mathrm{PGL}(2,q)$ to G/S. By lemma 4.2.4 we have that $\mathrm{Aut}(\mathrm{PGL}(2,q))$ consists of inner automorphisms and field automorphisms which clearly lift to automorphisms of $G = \mathrm{GL}(2,q)$ and therefore to automorphisms of G/S. The field automorphisms of $\mathrm{PGL}(2,q)$ lift to field automorphisms of G/S of the same order. Because Z is the center of $\mathrm{GL}(2,q)$, the inner automorphisms also lift to a group of automorphisms of the same order as the group of inner automorphisms of $\mathrm{PGL}(2,q)$. We have by lemma 4.2.5 that $\mathrm{Aut}(\mathrm{PGL}(2,q)) \cong \mathrm{Aut}(\mathrm{PSL}(2,q))$ so $A/B \cong \mathrm{Aut}(\mathrm{PSL}(2,q))$. □

Corollary 4.2.7. *The group A contains a characteristic subgroup isomorphic to* $\mathrm{PSL}(2,q)$.

4.3 Second lifting

Here we consider the lifting from G/S to G, where $G = \mathrm{GL}(2,q)$, q an odd prime power. Here C consists of the automorphisms which act trivially on G/S and S, B is the group of automorphisms which act trivially on G/S and A is the automorphism group of G.

Proposition 4.3.1. *When lifting from G/S to G*

- *B/C is trivial,*
- *$C \cong C_2$.*

Proof. Because S is elementary abelian and G does not split over S, the group B/C is trivial[CH03]. C corresponds to the group of 1-cocycles $Z^1(G/S, S)$. Since G/S is a a product of $\mathrm{PSL}(2,q)$ and U/S, we can write the conditions for Z^1 as a system of equations consisting of three parts:

- Equations for $\mathrm{PSL}(2,q)$,
- Equations for U/S,
- Equations for the interaction of $\mathrm{PSL}(2,q)$ and U/S.

The last system can only give restrictions but not new automorphisms. Lemma 4.1.2 gives that C is trivial on $\mathrm{PSL}(2,q)$. Suppose $\phi \in C$ and $s \in S$. Then, for any element $v \in U$, we have $v^\phi = vs^i$ for some power i. The group S has order 2, so ϕ is trivial on S. We consider two cases based on congruence of q mod 4.

If $q \equiv 3 \mod 4$, then U/S is generated by an element $u \in U/S$ of order 2 and a generator z of the cyclic group Z/S. All the elements of Z/S have odd order, so

z must be taken to itself. The element u has even order so mapping u to us, while keeping Z fixed, gives an automorphism and $|C| = 2$.

If $q \equiv 1 \mod 4$, then U/S is cyclic of order $q-1$. If u is a generator of U, then $u \mapsto su$ is a homomorphism so $|C| = 2$. □

4.4 The structure of $\mathrm{Aut}(G)$

In general, not all automorphisms of factor groups lift to automorphisms of the full group but, as we have seen, in the case of $\mathrm{GL}(2,q)$ every automorphisms of the factor does lift. Here we put together the automorphisms from Section 4.2 and the automorphisms from Section 4.3. We first look at the automorphisms from the two groups called C.

Proposition 4.4.1. *Let D be the subgroup of $\mathrm{Aut}(G)$ containing the automorphisms of G which either induce the automorphisms in the group C from section 4.2 or are in C in section 4.3. Then*

$$D \cong \begin{cases} C_2 & \text{if } q \equiv 3 \mod 4 \\ C_2 \times C_2 & \text{if } q \equiv 5 \mod 8 \\ C_4 & \text{if } q \equiv 1 \mod 8. \end{cases}$$

Proof. If $q \equiv 3 \mod 4$, then the first C is trivial and thus the only contribution is from the second C which has order 2.

Now suppose that $q \equiv 1 \mod 4$. The only non-trivial automorphism in the first C takes $\overline{u}$ to $\overline{uz}$ where $\overline{u}$ is a generator of U/S and $\overline{z}$ is the unique element of order 2 in Z/S.

If $\phi \in \mathrm{Aut}(G)$ induces this automorphism on G/S, then $u^\phi = uz$ where u is a generator of U and $z = u^{\frac{q-1}{2}}$ or $z = u^{\frac{3(q-1)}{2}}$. The two maps with different

choices of z differ by multiplication by the element s, so it is enough to consider the case when $z = u^{\frac{q-1}{2}}$. A map ϕ with this action, $u^\phi = u^{\frac{q+1}{2}}$, on U and the trivial action on $\mathrm{PSL}(2,q)$ is an automorphism of G if it keeps the intersection $U \cap \mathrm{PSL} = \langle s \rangle$ fixed. Since $\frac{q+1}{2}$ is odd, s, which has order 2, is kept fixed by ϕ and ϕ is an automorphism of G.

Now we calculate the order of ϕ.

$$\left(u^\phi\right)^\phi = \left(u^{\frac{q+1}{2}}\right)^{\frac{q+1}{2}} = s^{1+\frac{q-1}{4}}u = \begin{cases} u & \text{if } \frac{q-1}{4} \text{ is odd} \\ su & \text{if } \frac{q-1}{4} \text{ is even.} \end{cases}$$

If $q \equiv 5 \mod 8$, then ϕ has order two and $D \cong C_2 \times C_2$. If $q \equiv 1 \mod 8$ then ϕ has order four and contains the C from section 4.3 so $D \cong C_4$. □

Next we consider the automorphism described in Proposition 4.2.2.

Proposition 4.4.2. *Let E be the group of all the automorphisms which induce the identity automorphism on $(G/S)/(Z/S)$ or on G/S. Then*

$$E = \begin{cases} C_2 \times \mathrm{Aut}(C_{q-1}), & \text{if } q \equiv 3 \mod 4 \\ \mathrm{Aut}(C_{2(q-1)}), & \text{if } q \equiv 1 \mod 4 \end{cases}$$

Proof. The elements from E are the elements from C in section 4.3 and the elements which induce B and C in section 4.2. We have already considered the automorphism corresponding to the C's, so we need to study the automorphisms in B.

First consider the case when $q \equiv 3 \mod 4$, z is a generator of Z and $u \in U$ the element of order 2 which generates U/Z. Let ϕ be the map which acts as a homomorphism taking z to z^l with $\gcd(l, q-1) = 1$ and acts trivially on $\mathrm{PSL}(2,q)$ and $\langle u \rangle$. The integer l is odd so it fixes $Z \cap \mathrm{PSL}(2,q)$ and ϕ is an automorphism of G. If $\gcd(q-1, l) = 1$, then $\gcd(\frac{q-1}{2}, l) = 1$ and ϕ induces an automorphism from

B/C on G/S. Any automorphism in B/C is induced by such an automorphism ϕ. The subgroup D of $\mathrm{Aut}(G)$ moves u and therefore is not accounted for by any of these automorphisms. The group D and the automorphism group of Z act on separate domains so $E \cong C_2 \times \mathrm{Aut}(C_{q-1})$.

Now consider the case when $q \equiv 1 \mod 4$. In this case U is cyclic. Let ϕ be the automorphism which takes a generator u of U to u^l, with $\gcd(2(q-1), l) = 1$, and acts trivially on $\mathrm{PSL}(2, q)$. Since l is odd, we have that $s^l = s$ and therefore ϕ is well defined. Since $\gcd(2(q-1), l) = 1$ we have $\gcd(\frac{q-1}{2}, l) = 1$ and ϕ induces an automorphism from B/C on G/S. In 2.2.2, we showed that any automorphism from B/C is induced by such an automorphism. The automorphisms of this type account for all automorphisms acting trivially on $\mathrm{PSL}(2, q)$ and taking generators of U to other generators of U, so the automorphisms of D are among them. Therefore $E \cong \mathrm{Aut}(C_{2(q-1)})$. □

We now have described all the automorphisms of $\mathrm{GL}(2, q)$ which induce the identity on $\mathrm{GL}(2, q)/S$. It therefore only remains to find representatives for the automorphisms for the factor A/B.

Theorem 4.4.3. *Suppose q is an odd prime power. Then*

$$\mathrm{Aut}(\mathrm{GL}(2, q)) \cong E \times \mathrm{Aut}(\mathrm{PSL}(2, q)),$$

where

$$E = \begin{cases} C_2 \times \mathrm{Aut}(C_{q-1}), & \text{if } q \equiv 3 \mod 4 \\ \mathrm{Aut}(C_{2(q-1)}), & \text{if } q \equiv 1 \mod 4. \end{cases}$$

Proof. The automorphisms in Proposition 4.2.6 are inner automorphisms and field automorphisms and therefore must lift to automorphisms of G. The group S is contained in the center of $\mathrm{GL}(2, q)$, so the subgroup of the lifted inner automorphism has the same order as on the factor. The field automorphisms also lift to

automorphisms of the same order, so $\mathrm{Aut}(\mathrm{GL}(2,q))$ has a subgroup isomorphic to $\mathrm{Aut}(\mathrm{PSL}(2,q))$. These automorphisms all induce non-trivial action on both G/S and $(G/S)/(Z/S) \cong \mathrm{PGL}(2,q)$, so $E \cap \mathrm{Aut}(\mathrm{PSL}(2,q)) = \langle 1 \rangle$, where E is the group from lemma 4.4.2. We have all the automorphisms of $\mathrm{GL}(2,q)$ and the only thing that remains to be shown is that $\mathrm{Aut}(\mathrm{PSL}(2,q))$ and E are both normal subgroups of $\mathrm{Aut}(\mathrm{GL}(2,q))$.

We now have generators for $\mathrm{Aut}(\mathrm{GL}(2,q))$ and can use this to show that $\mathrm{Aut}(\mathrm{PSL}(2,q))$ and E are normal subgroups. The generators are shown in table 4.1. To show that $\mathrm{Aut}(\mathrm{PSL}(2,q))$ is normal in $\mathrm{Aut}(\mathrm{GL}(2,q))$, first note that the group of inner automorphisms of $\mathrm{GL}(2,q)$ is normal in $\mathrm{Aut}(\mathrm{GL}(2,q))$. Clearly the field automorphisms are centralized by automorphisms of the from $u \mapsto u^l$ where l is an integer. Therefore it is sufficient to show that in the case when $q \equiv 3 \mod 4$ the automorphism ϕ which has $u \mapsto us$ and keeps the other generators of $\mathrm{GL}(2,q)$ fixed centralizes field automorphisms. Recall that in the case when $q \equiv 3 \mod 4$ the matrix $u = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has entries from the base field only and thus is fixed by field automorphisms. Also recall that S has order 2 and is a characteristic subgroup of $\mathrm{GL}(2,q)$ and therefore is fixed by any automorphism of $\mathrm{GL}(2,q)$. Thus ϕ centralizes field automorphisms. Both the field automorphisms and the inner automorphisms form normal subgroups so their span, $\mathrm{Aut}(\mathrm{PSL}(2,q))$, is a normal subgroup of $\mathrm{Aut}(\mathrm{GL}(2,q))$.

To see that E is normal in $\mathrm{Aut}(\mathrm{GL}(2,q))$, note that $\mathrm{Aut}(\mathrm{PSL}(2,q))$ contains a characteristic subgroup isomorphic to $\mathrm{PSL}(2,q)$. This group is a normal subgroup of $\mathrm{GL}(2,q)$ by lemma 3.2.1. It is the only normal subgroup of $\mathrm{Aut}(\mathrm{GL}(2,q))$ isomorphic to $\mathrm{PSL}(2,q)$ and is therefore a characteristic subgroup of $\mathrm{Aut}(\mathrm{GL}(2,q))$. Any element of E centralizes $\mathrm{SL}(2,q)$ and therefore centralizes $\mathrm{PSL}(2,q)$. The centralizer of $\mathrm{PSL}(2,q)$ in $\mathrm{Aut}(\mathrm{PSL}(2,q))$ is trivial, so E is the centralizer of $\mathrm{PSL}(2,q)$

in $\mathrm{Aut}(\mathrm{PSL}(2,q))$ and is therefore a characteristic subgroup of $\mathrm{Aut}(2,q)$. This implies that E is a normal subgroup of $\mathrm{Aut}(\mathrm{GL}(2,q))$. Both E and $\mathrm{Aut}(\mathrm{PSL}(2,q))$ are normal subgroups of $\mathrm{Aut}(\mathrm{GL}(2,q))$, they span the group and intersect trivially and thus $\mathrm{Aut}(G)$ is a direct product of the two. □

We have some immediate corollaries from the proof of theorem 4.4.3:

Corollary 4.4.4. *Let q be an odd prime power. Then*

$$\mathrm{Aut}(\mathrm{GL}(2,q)) \cong C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q)) \times \mathrm{Aut}(\mathrm{PSL}(2,q)).$$

Corollary 4.4.5. *Let q be an odd prime power. Then $C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q))$ is a characteristic subgroup of* $\mathrm{Aut}(\mathrm{GL}(2,q))$.

Corollary 4.4.6. $\mathrm{Aut}(\mathrm{GL}(2,q))$ *contains a characteristic subgroup isomorphic to* $\mathrm{PSL}(2,q)$.

We have calculated the full automorphism group of $\mathrm{GL}(2,q)$ for any odd prime power q. Besides knowing the abstract structure of the automorphism group of $\mathrm{GL}(2,q)$, we also have generators of the automorphism group. These are shown in table 4.1.

Note that we know two characteristic subgroups of $\mathrm{Aut}(\mathrm{GL}(2,q))$, namely $\mathrm{PSL}(2,q)$ and $C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q))$. The intersection $C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q)) \cap \mathrm{PSL}(2,q)$ is the center of $\mathrm{PSL}(2,q)$. The group $\mathrm{PSL}(2,q)$ has a trivial center and thus the two groups must intersect trivially. We therefore have one more

	$q \equiv 3 \mod 4$	$q \equiv 1 \mod 4$
	Inner automorphisms	
	Field automorphisms	
From first C	No non-trivial	$u \mapsto u^{\frac{q+1}{2}}$, $s_1 \mapsto s_1,\ s_2 \mapsto s_2$
From first B	For l with $\gcd(q-1,l) = 1$: $z \mapsto z^l,\ u \mapsto u$ $s_1 \mapsto s_1, \quad s_2 \mapsto s_2$	For l with $\gcd(2(q-1),l) = 1$: $u \mapsto u^l$ $s_1 \mapsto s_1, \quad s_2 \mapsto s_2$
From second C	$u \mapsto us = uz^{\frac{q-1}{2}},\ z \mapsto z$ $s_1 \mapsto s_1, \quad s_2 \mapsto s_2$	$u \mapsto us = u^q$ $s_1 \mapsto s_1, \quad s_2 \mapsto s_2$

Table 4.1: The generators for the automorphism groups of $\mathrm{GL}(2,q)$

way to describe the structure of $\mathrm{Aut}(\mathrm{GL}(2,q))$ and this time in terms of characteristic subgroups. By lemma 2.3.1 $\mathrm{Aut}(\mathrm{GL}(2,q))$ is a subdirect product of $S = \mathrm{Aut}(\mathrm{GL}(2,q))/\mathrm{PSL}(2,q)$ and

$$\mathrm{Aut}(\mathrm{GL}(2,q))/C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q)).$$

We know that the characteristic copy of $\mathrm{PSL}(2,q)$ in $\mathrm{GL}(2,q)$ is contained in $\mathrm{Aut}(\mathrm{PSL}(2,q))$. This configuration is shown in figure 4.4. We now have:

Corollary 4.4.7. *Let q be an odd prime power, P the characteristic copy of $\mathrm{PSL}(2,q)$ in $\mathrm{Aut}(\mathrm{GL}(2,q))$ and C the centralizer of $\mathrm{Aut}(\mathrm{PSL}(2,q))$ in $\mathrm{Aut}(\mathrm{GL}(2,q))$. Then*

(a) $\mathrm{Aut}(\mathrm{GL}(2,q))/\mathrm{PSL}(2,q) \cong C \times (\mathrm{Aut}(\mathrm{PSL}(2,q))/\mathrm{PSL}(2,q))$

(b) $\mathrm{Aut}(\mathrm{GL}(2,q))/C \cong \mathrm{Aut}(\mathrm{PSL}(2,q))$

(c) $G = (C \times (\mathrm{Aut}(\mathrm{PSL}(2,q))/\mathrm{PSL}(2,q))) \leftthreetimes \mathrm{Aut}(\mathrm{PSL}(2,q))$.

We have described $\mathrm{Aut}(\mathrm{GL}(n,q))$ in the case when $n = 2$ and q is an odd prime power. If q is an even prime power then $\mathrm{GL}(2,q) = \mathrm{SL}(2,q) \times Z(\mathrm{GL}(2,q))$. Both of the direct factors are characteristic subgroups of $\mathrm{GL}(2,q)$ and thus we have $\mathrm{Aut}(\mathrm{GL}(2,q)) \cong \mathrm{Aut}(\mathrm{SL}(2,q)) \times \mathrm{Aut}(Z(\mathrm{GL}(2,q))$ which is analogous to the

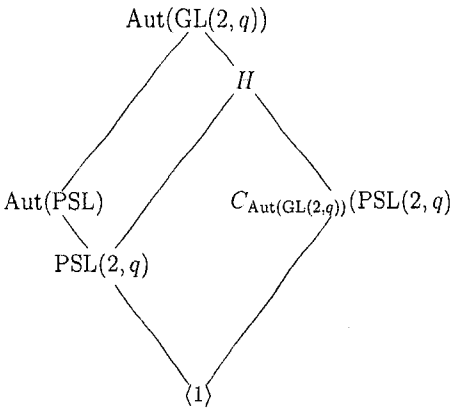


Figure 4.1: Characteristic factors of $\mathrm{Aut}(\mathrm{GL}(2,q))$

result for odd prime powers. If $n \geq 3$, then $\mathrm{SL}(n,q)$ and $Z(\mathrm{GL}(2,q))$ generate a subgroup of index $\gcd(n, q-1)$[CCN+85]. Here n might have non-trivial divisors, so more than two cases need to be considered. A Steinberg presentation similar to the one in 4.1.1 also exists for dimension $n \geq 3$. Thus an approach similar to the one taken here can be used to describe $\mathrm{Aut}(n,q)$ for any $n > 2$.

Chapter 5

AUTOMORPHISM TOWERS OF GENERAL LINEAR GROUPS OF DIMENSION 2

5.1 Properties of the groups in the automorphism tower of $\mathrm{GL}(2,q)$

From chapter 4 we know the structure of the automorphism group of $\mathrm{GL}(2,q)$ for odd prime powers q and we now use this structure to describe the automorphism towers of $\mathrm{GL}(2,q)$. One of the results from chapter 4 is corollary 4.4.6 which says that $\mathrm{Aut}(\mathrm{GL}(2,q))$ contains a characteristic subgroup isomorphic to $\mathrm{PSL}(2,q)$. For ease of notation we fix a prime power q and give names to the groups in the automorphism tower of $\mathrm{GL}(2,q)$.

Definition 5.1.1. *Let* A_1 *be the automorphism group of* $\mathrm{GL}(2,q)$ *and* $A_n = \mathrm{Aut}(A_{n-1})$ *for* $n > 1$.

Let P_1 be the characteristic subgroup of A_1 isomorphic to $\mathrm{PSL}(2,q)$. Note that P_1 is a characteristic subgroup of A_1 and P_1 has a trivial center, so A_2 must necessarily contain a normal subgroup isomorphic to $\mathrm{PSL}(2,q)$. We call this subgroup P_2. We also have that P_2 is the group of inner automorphisms of A_1 corresponding to the subgroup P_1. We can therefore identify P_1 and P_2. If P_2 is the only normal subgroup of A_2 isomorphic to $\mathrm{PSL}(2,q)$, then it is a characteristic subgroup of A_2 and we repeat this process for A_3.

This suggests a property that we will demand of the groups in our automorphism towers:

Condition 5.1.2. *Suppose that for all n, A_n contains a characteristic subgroup P_n isomorphic to $\mathrm{PSL}(2,q)$. As $P_n \leq A_n$ is the subgroup of the inner automorphisms of A_{n-1} coming from P_{n-1}, we can identify P_{n-1} and P_n. We will therefore refer to P_n by P for all $n \in \mathbb{N}$.*

We demand that condition 5.1.2 is satisfied for all the choices of q considered in this chapter. Though we cannot prove that this condition holds for arbitrary odd prime powers q, we have not found any choice of q for which it does not hold.

Theorem 5.1.3. *Let E_n be the centralizer of P in A_n and $K = \mathrm{Aut}(\mathrm{PSL}(2,q))$. Then for $n \in \mathbb{N}$*

(a) $A_n \cong \mathrm{Aut}(\mathrm{PSL}(2,q)) \times E_n$

(b) $A_n = A_n/P \leftthreetimes A_n/E_n \cong \mathrm{Aut}(\mathrm{PSL}(2,q)) \leftthreetimes (K \times E_n)$

Proof. (by induction)

(a) and (b) hold for A_1 by corollaries 4.4.4 and 4.4.7.

Suppose (a) and (b) hold for A_n. Let $S = E_n$, $T = P$, $H = \langle S, T \rangle$. Note that $A_n/S \cong \mathrm{Aut}(\mathrm{PSL}(2,q))$, so A_n/S only has inner automorphisms by corollary 3.2.7. We also have from corollary 4.2.3 that $A_n/H \cong \mathrm{Aut}(\mathrm{PSL}(2,q))/\mathrm{PSL}(2,q)$ is abelian. Let F be the subgroup of G/P which induces the identity on G/H. We have from corollary 2.3.4 that $A_{n+1} \cong F \times \mathrm{Aut}(\mathrm{PSL}(2,q))$. Because $\mathrm{Aut}(\mathrm{PSL}(2,q))$ has a trivial center, the centralizer of P is fully contained in F and by corollary 3.2.3 we have $F = C_{A_{n+1}}(P) = E_{n+1}$ and thus (a) holds for $n+1$.

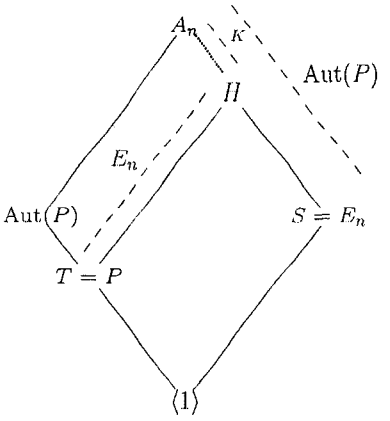


Figure 5.1: Set-up in theorem 5.1.3

We have assumed that A_n contains a characteristic subgroup P isomorphic to $\mathrm{PSL}(2,q)$. The group $\mathrm{Aut}(\mathrm{PSL}(2,q))$ contains this characteristic subgroup. We have $A_{n+1} \cong A_{n+1}/\mathrm{Aut}(\mathrm{PSL}(2,q)) \times A_{n+1}/H$, so $A_{n+1}/P \cong E_{n+1} \times K$ and we have $A_{n+1}/E_{n+1} \cong \mathrm{Aut}(\mathrm{PSL}(2,q))$. The group A_{n+1} is a subdirect product of the two quotient groups, so we have $A_{n+1} \cong \mathrm{Aut}(\mathrm{PSL}(2,q)) \curlywedge (E_{n+1} \times K)$ which is property (b) for $n+1$. □

In theorem 5.1.3 we described the groups in the automorphism tower of $\mathrm{GL}(2,q)$ both as a direct product and as a subdirect product. The direct product description in convenient when studying the center of A_n but $\mathrm{Aut}(\mathrm{PSL}(2,q))$ is not a characteristic subgroup of A_n. The direct product can therefore not be used directly to build automorphism tower. This is the reason we also need that any group in the automorphism tower of $\mathrm{GL}(2,q)$ for an odd prime power q is a subdirect product of two characteristic factors. In the proof of the theorem we showed how this structure is propagated through the tower. A property to notice in the proof is that though E_n is the centralizer of P, it is calculated as a stabilizer

in a group without an explicit reference to either A_{n-1} or P. This leads to the following corollary:

Corollary 5.1.4. *Let E_n be the centralizer of P in A_n and $K = \mathrm{Aut}(\mathrm{PSL}(2,q))$. Suppose q is an odd prime. For $n \in \mathbb{N}$*

(a) $A_n \cong \mathrm{Aut}(\mathrm{PSL}(2,q)) \times E_n$

(b) $A_n = A_n/P \curlywedge A_n/E_n \cong \mathrm{Aut}(\mathrm{PSL}(2,q)) \curlywedge (C_2 \times E_n)$,

where $\begin{cases} E_1 = C_{A_1}(P) \\ E_{n+1} = \mathrm{Stab}_{\mathrm{Aut}(C_2 \times E_n)}(E_n) \end{cases}$

Proof. Because q is a prime, then $\mathrm{Aut}(\mathrm{PSL}(2,q))/\mathrm{PSL}(2,q) \cong C_2$. By the proof of theorem 5.1.3 we know that E_{n+1} is the subgroup of $\mathrm{Aut}(E_n \times C_2)$ which induces the identity on $A_n/\langle P, C_{A_n}\rangle \cong C_2$. When q is a prime, E_n consists of all automorphism of $\mathrm{Aut}(E_n \times C_2)$ which leave E_n invariant. We therefore have that $E_{n+1} = \mathrm{Stab}_{\mathrm{Aut}(C_2 \times E_n)}(E_n)$. □

When working over a prime-field $\mathbb{F}_p$, corollary 5.1.4 lets us reduce the calculation of automorphism towers of $\mathrm{GL}(2,p)$ to the calculation of smaller towers:

Definition 5.1.5 (Reduced tower of $\mathrm{GL}(2,p)$). *Let A be the automorphism group of $\mathrm{GL}(2,p)$. The reduced tower of $\mathrm{GL}(2,p)$ is the sequence of groups $E_1, E_2, \ldots$, where*

$E_1 = C_{A_1}(\mathrm{PSL}(2,p))$

$E_n = \mathrm{Stab}_{\mathrm{Aut}(E_{n-1} \times C_2)}(E_{n-1})$ *for* $n > 1$.

We are interested in knowing whether the automorphism tower of $\mathrm{GL}(2,p)$ terminates. With the help of the following lemma, we can also reduce that question to the reduced towers:

Lemma 5.1.6. *Let A_n be the n^{th} group in the automorphism tower of* $\mathrm{GL}(2,p)$*, where p is an odd prime. Then A_n has a center if and only if the n^{th} group in the reduced tower of* $\mathrm{GL}(2,p)$ *has a center.*

Proof. The center of a direct product of groups is the direct product of the centers of the two groups. Since $\mathrm{Aut}(\mathrm{PSL}(2,p))$ does not have a center then the center of A is the center of E_n. □

Theorem 5.1.7. *The automorphism tower of* $\mathrm{GL}(2,p)$ *terminates if and only if the n^{th} group in the reduced tower of* $\mathrm{GL}(2,p)$ *has a trivial center for some n.*

Proof. Since an automorphism tower terminates if and only if the center of some group in its tower is trivial, this follows directly from lemma 5.1.6. □

5.2 Case study of automorphism towers of $\mathrm{GL}(2,q)$

We have reduced the building of automorphism towers of $\mathrm{GL}(2,q)$ for odd prime numbers q to the building of the reduced towers in definition 5.1.5. In this section we identify some prime powers q that give certain nice groups as first groups in the reduced tower of $\mathrm{GL}(2,q)$.

Recall that if G is a cyclic group of order p^m, where p is a prime, then we have by lemma 3.1.8

$$\mathrm{Aut}(G) = \begin{cases} C_2 \times C_{2(m-2)} & \text{if } p = 2 \\ C_{p-1} \times C_p^{m-1} & \text{if } p \text{ is odd} \end{cases}$$

We are interested in the two subgroups of $\mathrm{Aut}(\mathrm{GL}(2,q))$ given in definition 5.1.5, namely

$$\begin{cases} \mathrm{Aut}(C_{2(q-1)}) & \text{if } q \equiv 1 \mod 4 \\ \mathrm{Aut}(C_{q-1}) & \text{if } q \equiv 3 \mod 4 \end{cases}$$

One nice looking family of automorphism groups we can obtain are ones of the form $A = (C_2)^k \times C_p$, where p is an odd prime. Using lemma 3.1.8, we obtain

conditions on the prime power q, that need to be satisfied for the automorphism group to have this structure. There are two conditions that need to be satisfied:

- A does not have a subgroup isomorphic to C_4
- $|A|$ is divisible by exactly one odd prime.

Lemma 5.2.1. *Suppose r is an odd integer and p and q are two odd prime divisors of r with $p < q$. Then one of the following three holds:*

- $|\operatorname{Aut}(C_r)|$ *is divisible kt where k, t are two, not necessarily distinct, odd primes*
- $\operatorname{Aut}(C_r)$ *has a subgroup isomorphic to C_{2^k} with $k > 1$*
- $p = 3$ *and* $r = 3q$.

Proof. By lemma 3.1.8, we have that $|\operatorname{Aut}(C_r)|$ is divisible by $(p-1)(q-1)$. We write p as $p = 2^{k_p}p_1 + 1$ and q as $q = 2^{k_q}q_1 + 1$ where p_1 and q_1 are odd. Suppose $|\operatorname{Aut}(C_r)|$ is not divisible by kt, where k, t are odd primes. This means that either $p_1 = 1$ or $q_1 = 1$. First consider the case when $q_1 = 1$. Then $k_q > 1$ because $q > p \geq 3$ and therefore $C_{2^{k_q}}$ is a subgroup of $\operatorname{Aut}(C_r)$ and we are in case two.

Now suppose $q_1 \neq 1$. Then q must be divisible by at least one odd prime and since we are assuming that $|\operatorname{Aut}(C_r)|$ is divisible by at most one odd prime, we have $p_1 = 1$. If $k_p > 1$, then $\operatorname{Aut}(C_r)$ has a subgroup isomorphic to $C_{2^{k_p}}$ and we are in the second case. If $k_p = 1$ we have $p = 3$. If 3^2 divides r then $|\operatorname{Aut}(C_r)|$ is divisible by 3 as well as an odd prime divisor of q. We are assuming only one odd prime divides $|\operatorname{Aut}(C_r)|$, so we have that 3^1 is the largest powers of 3 dividing r. We also have that if another odd prime divides r, then we must be in one of the first two cases, so we have $r = 3q$. □

From this lemma we see that for $\mathrm{Aut}(C_{2(q-1)})$ and $\mathrm{Aut}(C_{q-1})$ to have the structure $(C_2)^n \times C_p$, where p is a prime, we must have that $q-1 = 2^l r$, where r is a prime, or $q-1 = 2^l \cdot 3r$, where r is a prime. We also have as a corollary to the proof that $r = 2r_1 + 1$, where r_1 is a prime.

Definition 5.2.2. *A prime p is called a Germain prime if $2p+1$ is a prime.*

Proposition 5.2.3. *Suppose q is a prime power with $q \equiv 3 \mod 4$. Then*

$$\mathrm{Aut}(C_{q-1}) \cong C_p \times (C_2)^k$$

if and only if $q = 2 \cdot 3^i(2p+1)+1$ where p is a Germain prime and $i \in \{0,1\}$.

$$\mathrm{Aut}(C_{q-1}) \cong \begin{cases} C_2 \times C_p & \text{if } q = 2(2p+1)+1 \\ (C_2)^2 \times C_p & \text{if } q = 6(2p+1)+1 \end{cases}$$

Proof. $q \equiv 3 \mod 4$, so $q-1 = 4k+3-1 = 4k+2 = 2r$ for some number k and an odd number r. Therefore we have $\mathrm{Aut}(C_{q-1}) \cong \mathrm{Aut}(C_2) \times \mathrm{Aut}(C_r) = \mathrm{Aut}(C_r)$. By lemma 5.2.1 we have that $\mathrm{Aut}(C_r) \cong C_p \times (C_2)^k$ only if $r = 3^i s$ for some odd prime s and $i \in \{0,1\}$. We also see from the proof of that lemma that $s = 2p+1$ where p is a prime. Then $\mathrm{Aut}(C_{q-1}) \cong \mathrm{Aut}(C_2) \times \mathrm{Aut}(C_r) \cong \mathrm{Aut}(C_{3^i}) \times \mathrm{Aut}(C_s) \cong (C_2)^{i+1} \times C_p$. □

Proposition 5.2.4. *Suppose q is a prime power with $q \equiv 1 \mod 4$. Then*

$$\mathrm{Aut}(C_{q-1}) \cong C_p \times (C_2)^k$$

if and only if $q = 2^2 \cdot 3^i(2p+1)+1$ where p is a Germain prime and $i \in \{0,1\}$.

$$\mathrm{Aut}(C_{2(q-1)}) \cong \begin{cases} (C_2)^3 \times C_p & \text{if } q = 2^2(2p+1)+1 \\ (C_2)^4 \times C_p & \text{if } q = 2^2 \cdot 3(2p+1)+1 \end{cases}$$

Proof. $q \equiv 1 \mod 4$, so $q-1 = 4k+1-1 = 4k = 4 \cdot 2^j r$ for some numbers k, j and an odd number r. If $j > 1$ we have from lemma 3.1.8 that $\mathrm{Aut}(C_{2(q-1)})$ contains a subgroup isomorphic to C_{2^j} with $j > 1$, so we must have $j = 0$ and $k = r$ is odd. Then, as in proposition 5.2.3, we have that $r = 3^i s$, where s is a prime of the form $2p + 1$, with p prime, and $i \in \{0, 1\}$. Then

$$\mathrm{Aut}(C_{2(q-1)}) \cong \mathrm{Aut}(C_{2^3}) \times \mathrm{Aut}(C_r) \cong (C_2)^2 \times \mathrm{Aut}(C_{3^i}) \times \mathrm{Aut}(C_s) \cong (C_2)^{i+3} \times C_p.$$

□

We now know exactly the prime powers which give $E_1 = C_{\mathrm{Aut}(\mathrm{GL}(2,q))}(\mathrm{PSL}(2,q))$ with the structure $(C_2)^n \times C_p$, where p is a prime. This structure gives towers that are easier to build and describe. We cannot say whether this family of primes is infinite. For the family to infinite, there needs to exist an infinite number of Germain primes such that $q = 2^2(2p+1)+1$, $q = 2^2 \cdot 3(2p+1)+1$, $q = 2(2p+1)+1$ or $q = 6(2p+1)+1$ are prime powers. We call such prime powers q good prime powers. A necessary condition for there to exist an infinite number of good primes is that there exists an infinite number of Germain primes. Though it is conjectured that infinitely many Germain primes exist[MTB99], it has not been proven. The number of good prime powers q smaller than a number n is shown in figure 5.2.

5.3 Examples of building automorphism towers of $\mathrm{GL}(2, q)$

Once we have a way to reduce the building of automorphism towers to the reduced towers, it only remains to calculate and understand the groups in the reduced towers. Restricting ourselves to the prime powers in 5.2 we see that we need to understand stabilizers of the type $\mathrm{Stab}\,\mathrm{Aut}(C_p \times (C_2)^{n+1})(C_p \times (C_2)^n)$,

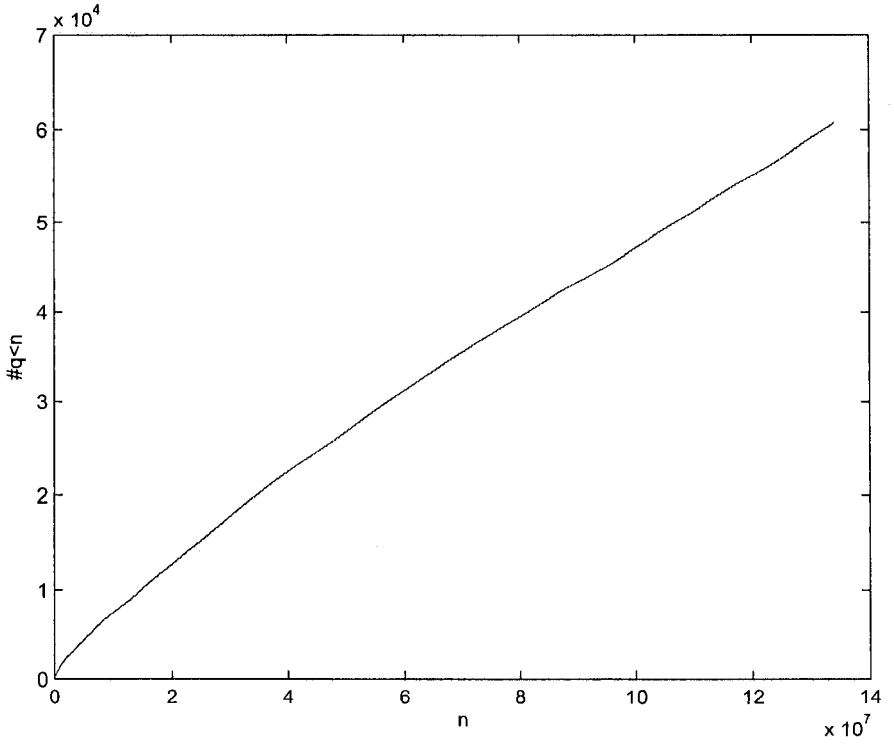


Figure 5.2: Number of good prime powers q

where p is an odd prime and $n \in \{1, 2, 3, 4, 5\}$. In this section we study these stabilizers and use them to build automorphism towers of $\mathrm{GL}(2, q)$.

Lemma 5.3.1. *Suppose* $E = S_4 \times (C_2)^n$. *Then* $\mathrm{Aut}(E) \cong S_4 \times ((C_2)^n \rtimes \mathrm{GL}(n, 2))$.

Proof. Suppose $E = \langle (1,2), (1,2,3,4), (a_1, b_1), \ldots, (a_n, b_n) \rangle$. First note that $Z = (C_2)^n$ is the center of E and is therefore a characteristic subgroup of E. Also note that the automorphism group of Z is $\mathrm{GL}(n, 2)$.

Suppose $\phi \in \mathrm{Aut}(E)$ and consider the images of $(1,2)$ and $(1,2,3,4)$. The automorphism ϕ must preserve the order of elements, so $(1,2)^\phi = (c_1, c_2)v$ and $(1,2,3,4)^\phi = (d_1, d_2, d_3, d_4)w$ where $v, w \in Z$. Note that $((1,2,3,4)(1,2))^\phi =$

$(2,3,4)^\phi = (d_1, d_2, d_3, d_4)(c_1, c_2)vw$, so we see that vw is trivial and, because v and w have order 1 or 2, we have $v = w$. By following ϕ by an inner automorphism of E we see that we can assume without loss of generality that $(1,2,3,4)^\phi = (1,2,3,4)v$ and $(1,2)^\phi = (1,2)v$. We write an automorphism of this type as ϕ_v. It is easily seen that ϕ_v is an automorphism of E for any choice of $v \in Z$. We therefore have a subgroup of $\mathrm{Aut}(E)$ isomorphic to $(C_2)^n$ corresponding to multiplication of the generators of S_4 by an element from Z. Because any automorphism of E must preserve the order of elements and we have considered all elements of E of orders 2 and 4, we know that any automorphism of E which moves a generator of S_4 is an inner automorphism, an automorphism of the type ϕ_v or a product of the two. We have already considered the automorphisms of Z and thus have the full automorphism group of E. It is clear that the inner automorphism form a normal subgroup of $\mathrm{Aut}(E)$ and it just remains to show that $(C_2)^n \rtimes \mathrm{GL}(n,2)$ is a normal subgroup of $\mathrm{Aut}(E)$.

Let $(s,z) \in E$ with $s \in S_4$ and $z \in Z$. Consider an inner automorphism of E induced by $r \in S_4$ and let $\psi = (v, A) \in (C_2)^n \rtimes \mathrm{GL}(n,2)$. For $(s,z) \in S_4 \times (C_2)^n$ we have $(s,z)^\psi = (sv, zA)$. We then have

$$\begin{aligned}
(s,z)^{\psi^r} &= (r^{-1}sr, z)^{\psi r} \\
&= (r^{-1}srv, zA)^r \\
&= (r^1srv, zA)^r \\
&= (rr^{-1}srvr^{-1}, zA) \\
&= (sv, z) \\
&= (s,z)^\psi.
\end{aligned}$$

We have that the inner automorphisms of E centralize $(C_2)^n \rtimes \mathrm{GL}(n,2)$ in $\mathrm{Aut}(E)$, so

$$\mathrm{Aut}(E) \cong S_4 \times ((C_2)^n \rtimes \mathrm{GL}(n,2)).$$

□

Corollary 5.3.2. *Suppose* $E = S_4 \times (C_2)^n$ *and* $K = \langle k_1 \rangle = C_2$. *Then*

$$\mathrm{Stab}_{\mathrm{Aut}(E\times K)}(E) \cong S_4 \times (((C_2)^n \times (C_2)^n) \rtimes \mathrm{GL}(n,2)).$$

Proof. We are looking for the stabilizer of E and already know the full automorphism group of E, so we need only consider the possible images of k_1. The stabilizer of a single copy of C_2 in $(C_2)^{n+1}$ is $\mathrm{AGL}(n,2) \cong (C_2)^n \rtimes \mathrm{GL}(n,2)$, so we have that $\mathrm{Stab}_{\mathrm{Aut}(E\times K)}(E) \cong S_4 \times ((C_2)^n \rtimes \mathrm{GL}(n,2))$. □

Lemma 5.3.3. *The derived subgroup of* $\mathrm{AGL}(k,2)$ *is* $\mathrm{AGL}(k,2)$ *for all* $k \geq 3$.

Proof. $\mathrm{AGL}(n,2) = (C_2)^n \rtimes \mathrm{GL}(n,2)$. Suppose N is a normal subgroup such that $\mathrm{AGL}(n,2)/N$ is an abelian group. Let ϕ be the natural map from $\mathrm{AGL}(n,2)$ to $\mathrm{AGL}(n,2)/(C_2)^n$. The image of N under ϕ is either trivial or all of $\mathrm{GL}(n,2)$ since $\mathrm{GL}(n,2)$ is simple. If the image is trivial, then $N \leq (C_2)^n$ which is not possible because that would imply that $\mathrm{GL}(n,2) \leq \mathrm{AGL}(n,2)/N$. Therefore $N^\phi = \mathrm{GL}(n,2)$. We therefore have $\mathrm{AGL}(n,2) = \langle N, (C_2)^n \rangle$. The intersection of $(C_2)^n \cap N$ is a submodule of $(C_2)^n$ that is invariant under $\mathrm{GL}(n,2)$. This is not possible unless the intersection is trivial or $(C_2)^n \leq N$. In the first case we have that $N = \mathrm{GL}(n,2)$ and $\mathrm{AGL}(n,2)$ is a direct product of $\mathrm{GL}(n,2)$ and $(C_n)^2$ which is not the case, so we have $(C_2)^n \leq N$ and $\mathrm{AGL}(n,2) = N$. □

Lemma 5.3.4. $\mathrm{AGL}(3,2)$ *is a characteristic subgroup of* $\mathrm{Aut}(\mathrm{AGL}(3,2))$.

Proof. By lemma 2.1.16 we have $\mathrm{Aut}(\mathrm{AGL}(3,2)) = \mathrm{AGL}(3,2) \rtimes C_2$ and therefore $\mathrm{Aut}(\mathrm{AGL}(3,2))' = \mathrm{AGL}(3,2)$. □

Lemma 5.3.5. $\mathrm{AGL}(k,2)$ *is a characteristic subgroup of* $\mathrm{AGL}(k,2) \times (C_2)^n$ *for any value of* n *and* $k \geq 3$.

Proof. $\mathrm{AGL}(k,2)$ is the derived subgroup of $\mathrm{AGL}(k,2) \times (C_2)^n$ for any $k \geq 3$. □

Lemma 5.3.6. $\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2))) \cong \mathrm{Aut}(\mathrm{AGL}(3,2))$.

Proof. We identify $\mathrm{Aut}(\mathrm{AGL}(3,2))$ with the group of inner automorphism of $\mathrm{Aut}(\mathrm{AGL}(3,2))$ contained in $\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2)))$. The derived subgroup of $\mathrm{Aut}(\mathrm{AGL}(3,2))$ is a characteristic subgroup of $\mathrm{Aut}(\mathrm{AGL}(3,2))$ by lemma 5.3.5. Let $\phi \in \mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2)))$. There exists an inner automorphism τ of $\mathrm{Aut}(\mathrm{AGL}(3,2))$ such that ϕ and τ have the same action on $\mathrm{AGL}(3,2)$. Let $\psi = \tau\phi^{-1}$. The automorphism ψ acts trivially on $\mathrm{AGL}(3,2)$. Let $g \in \mathrm{AGL}(3,2)$ and $\alpha \in \mathrm{Aut}(\mathrm{AGL}(3,2))$. Then we have

$$\begin{aligned} g^{\alpha^\psi} &= g^{\psi^{-1}\alpha\psi} \\ &= (g^{\psi^{-1}})^{\alpha\psi} \\ &= g^{\alpha\psi} \\ &= (g^{\alpha})^{\psi} \\ &= g^{\alpha}. \end{aligned}$$

We thus have that $\alpha^\psi = \alpha$ for all $\alpha \in \mathrm{Aut}(\mathrm{AGL}(3,2))$, so ψ is trivial and therefore $\phi = \tau$ is an inner automorphism of $\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2)))$ and $\mathrm{Aut}(\mathrm{AGL}(3,2))$ only has inner automorphisms. Because $\mathrm{AGL}(3,2)$ has a trivial center this implies that $\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2))) \cong \mathrm{Aut}(\mathrm{AGL}(3,2))$. □

Corollary 5.3.7. $\mathrm{Aut}(\mathrm{AGL}(3,2) \times (C_2)^n) \cong \mathrm{Aut}(\mathrm{AGL}(3,2)) \times \mathrm{GL}(n,2)$.

Corollary 5.3.8. *Let* $E = \mathrm{AGL}(3,2) \times (C_2)^n$ *and* $K = \langle k \rangle \cong C_2$. *Then* $\mathrm{Stab}_{\mathrm{Aut}(E \times K)}(E) \cong \mathrm{Aut}(\mathrm{AGL}(3,2)) \times \mathrm{AGL}(n,2)$.

Corollary 5.3.9. $\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n) \cong \mathrm{Aut}(\mathrm{AGL}(3,2)) \times ((C_2)^n \rtimes \mathrm{GL}(n,2))$.

Proof. $(C_2)^n$ is the center of $\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$ and $\mathrm{AGL}(3,2)$ is the derived subgroup of $\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$ and therefore both groups are characteristic. Because we know the automorphism group of each group it only remains to find all possible images of the C_2 factor in $\mathrm{AGL}(3,2) \rtimes C_2 \cong \mathrm{Aut}(\mathrm{AGL}(3,2))$. It is easily seen that the map which fixes $\mathrm{AGL}(3,2)$ and the center of $\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$ and takes the generator of the C_2 to itself multiplied by an element of the center is an automorphism of $\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$. We therefore have

$$\mathrm{Aut}(\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n) \cong \mathrm{Aut}(\mathrm{AGL}(3,2)) \times ((C_2)^n \rtimes \mathrm{GL}(n,2)).$$

□

Corollary 5.3.10. *Let* $E = \mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$ *and* $K = \langle k \rangle = C_2$. *Then* $\mathrm{Stab}_{\mathrm{Aut}(E \times K)}(E) \cong \mathrm{Aut}(\mathrm{AGL}(3,2)) \times \left(((C_2)^n)^2 \rtimes \mathrm{GL}(n,2)\right)$ *and this group has a trivial center for* $n \geq 2$.

Corollary 5.3.11. $\mathrm{Aut}(\mathrm{AGL}(k,2) \times (C_2)^n) \cong \mathrm{GL}(n,2) \times \mathrm{AGL}(k,2)$ *for* $k \in \{4,5\}$ *and any* n.

Proof. Let $k \in \{4,5\}$. By lemma 2.1.16 we have that $\mathrm{Aut}(\mathrm{AGL}(k,2)) \cong \mathrm{AGL}(k,2)$. The group $(C_2)^n$ is the center of $\mathrm{AGL}(k,2) \times (C_2)^n)$ and $\mathrm{AGL}(k,2)$ and $\mathrm{AGL}(k,2)$ is the derived subgroup of $\mathrm{AGL}(k,2) \times (C_2)^n$. This implies that both groups are characteristic subgroups and therefore the automorphism group of $\mathrm{AGL}(k,2) \times (C_2)^n$ is the direct product of the automorphism group of the two characteristic subgroups. □

Corollary 5.3.12. *Let* $E = \mathrm{AGL}(m,2) \times (C_2)^n$ *for* $m \geq 4$ *and* $K = \langle k \rangle \cong C_2$. *Then* $\mathrm{Stab}_{\mathrm{Aut}(E \times K)}(E) \cong \mathrm{AGL}(m,2) \times ((C_2)^n \rtimes \mathrm{GL}(n,2))$ *which has a trivial center for* $n \geq 2$.

Using the results from this section we can fill in the results in table 5.3 that describe the behavior of the automorphism towers of the general linear groups which have these groups in their reduced towers.

E_m	E_{m+1}	tower behavior
$S_4 \times (C_2)^n$, $n \geq 2$	$S_4 \times \left((C_2)^{2n} \rtimes \mathrm{GL}(n,2)\right)$ $S_4 \times \left((C_2)^{2n} \rtimes \mathrm{GL}(n,2)\right)$	$Z(E_{n+1})$ is trivial $\Rightarrow$ tower terminates
$S_4 \times C_2$	$S_4 \times (C_2)^2$	Reduces to line above $\Rightarrow$ tower terminates
$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^n$, $n \geq 2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times$ $\left((C_2)^{2n} \rtimes \mathrm{GL}(n,2)\right)$	$Z(E_{n+1})$ is trivial $\Rightarrow$ tower terminates
$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2)^2$	Reduces to line above $\Rightarrow$ tower terminates
$\mathrm{AGL}(3,2) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2$	Reduces to line above $\Rightarrow$ tower terminates
$\mathrm{AGL}(3,2) \times (C_2)^n$, $n \geq 2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times$ $((C_2)^n \rtimes \mathrm{GL}(n,2))$	$Z(E_{n+1})$ trivial $\Rightarrow$ tower terminates
$\mathrm{AGL}(k,2) \times (C_2)^n$, $n \geq 2$, $k = 4,5$	$\mathrm{AGL}(k,2) \times$ $((C_2)^n \rtimes \mathrm{GL}(n,2))$	$Z(E_{n+1})$ is trivial $\Rightarrow$tower terminates
$\mathrm{AGL}(k,2) \times C_2$ $k = 4,5$	$\mathrm{AGL}(k,2) \times C_2 \cong E_m$	period one

Table 5.1: Building and behavior of reduced towers

5.3.1 Examples of automorphism towers of $\mathrm{GL}(2,q)$

Now that we understand the behavior of the reduced towers for a certain groups we can apply this to $\mathrm{GL}(2,q)$. The results of this are shown in table 5.2. The table shows the behavior for the automorphism tower of $\mathrm{GL}(2,q)$ for all

"good" prime powers q, $q < 100$. The two last lines in the table were computed using ad hoc methods and the computer algebra system GAP[GAP04]. This was necessary because a normal subgroup isomorphic to C_4 gets introduced and this gives an idea of the technical difficulties that arise when computing reduced towers for large prime powers.

Prime power	E_1	E_2	E_3	E_4	E_5	behavior of tower
3	C_2	C_2	C_2			period one
5	C_2^2	S_4				$Z(E_2) = \langle 1 \rangle$ terminates
7	C_2^2	S_4				$Z(E_2) = \langle 1 \rangle$ terminates
13	C_2^3	$\mathrm{AGL}(3,2)$				$Z(E_2) = \langle 1 \rangle$ terminates
19	$C_2^2 \times C_3$	$S_4 \times C_2$	$S_4 \times C_2^2$	$S_4 \times (C_2^{2\cdot 2} \rtimes \mathrm{GL}(2,2))$		$Z(E_4) = \langle 1 \rangle$ terminates
23	$C_2^2 \times C_5$	$S_4 \times C_4$	$S_4 \times C_2^3$	$S_4 \times (C_2^{3\cdot 2} \rtimes \mathrm{GL}(2,2))$		$Z(E_4) = \langle 1 \rangle$ terminates
29	$C_2^3 \times C_3$	$\mathrm{AGL}(3,2) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^{2\cdot 2} \rtimes \mathrm{GL}(2,2)$	$Z(E_5) = \langle 1 \rangle$ terminates
37	$C_2^3 \times C_3$	$\mathrm{AGL}(3,2) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^{2\cdot 2} \rtimes \mathrm{GL}(2,2)$	$Z(E_5) = \langle 1 \rangle$ terminates
43	$C_2^3 \times C_3$	$\mathrm{AGL}(3,2) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^{2\cdot 2} \rtimes \mathrm{GL}(2,2)$	$Z(E_5) = \langle 1 \rangle$ terminates
47	$C_2^2 \times C_{11}$	$S_4 \times C_2 \times C_5$	$S_4 \times C_2^2 \times C_4$	$(C_2^3)^3 \rtimes \mathrm{AGL}(2,2) \times S_4$	$\lvert E_5 \rvert = 25367150592$	$Z(E_5) = \langle 1 \rangle$ terminates
67	$C_2^3 \times C_5$	$\mathrm{AGL}(3,2) \times C_4$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times C_2^2$	$\mathrm{Aut}(\mathrm{AGL}(3,2)) \times (C_2^2)^2 \rtimes \mathrm{SL}(2,2)$		$Z(E_4) = \langle 1 \rangle$ terminates

Table 5.2: Automorphism towers of $\mathrm{GL}(2,q)$

Bibliography

[Cam99] Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, Cambridge University Press, 1999.

[Car89] Roger W. Carter, *Simple groups of Lie type*, Wiley, 1989.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[CH03] John J. Cannon and Derek F. Holt, *Automorphism group computation and isomorphism testing in finite groups*, J. Symbolic Comput. **35** (2003), no. 3, 241–267.

[CNW90] Frank Celler, Joachim Neubüser, and Charles R. B. Wright, *Some remarks on the computation of complements and normalizers in soluble groups*, 57–76.

[DF99] David S. Dummit and Richard M. Foote, *Abstract algebra*, Wiley, 1999.

[Die07] Jill Dietz, *On automorphisms of product of groups*, Groups St Andrews 2005 (C. M. Campbell, M. R. Quick, E. F. Robertson, and G. C. Smith, eds.), London Mathematical Society Lecture Note Series, vol. 339, 1, Cambridge University Press, 2007.

[GAP04] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004, (`http://www.gap-system.org`).

[Ham98] Joel David Hamkins, *Every group has a terminating transfinite automorphism tower*, Proc. Amer. Math. Soc **126** (1998), 3223–3226.

[HM06] Geir T. Helleloid and Ursula Martin, *The automorphism group of a finite p-group is almost always a p-group*, 2006.

[HM07] ———, *The automorphism group of a finite p-group is almost always a p-group*, Journal of Algebra **312** (2007), 294–329.

[Hup] B. Huppert, *Endlichen Gruppen I.*, Springer-Verlag.

[Isa08] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, American Mathematical Society, 2008.

[Jon] Gareth Jones, Private correspondence.

[MP03] John Martino and Stewart Priddy, *Group extensions and automorphism group rings*, Homology, Homotopy and Applications **5(1)** (2003), 53–70.

[MTB99] Steven J. Miller and Ramin Takloo-Bighash, *An invitation to modern number theory*, Wiley, 1999.

[Neu92] Jürgen Neukich, *Algebraische Zahlentheorie*, SpringerVerlag, 1992.

[Pet83] Martin R. Petter, *A note on the automorphism tower theorem for finite groups*, The Proceedings of the American Mathematical Society **89(1)** (1983), 182–183.

[Sch55] Eugene Schenkman, *On the tower theorem for finite groups*, Pacific Journal of Mathematics **5** (1955), 995–998.

[Sch68] ———, *The tower theorem for finite groups*, Pacific Journal of Mathematics **5** (1968), 458–459.

[Tho] Simon Thomas, *The automorphism tower problem*, http://www.math.rutgers.edu/ sthomas/book.dvi.

[Tho85] ———, *The automorphism tower problem*, Proc. Amer. Math. Soc. **95** (1985), 166–168.

[Wie39] Helmut Wielandt, *Eine Verallgemeinung der invarianten Untergruppen*, Math. Z. **45** (1939), 209–244.