On the representations of solvable linear groups

by
Zoltán Halasi

Submitted to
Central European University
Department of Mathematics and its Applications

In partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Mathematics and its Applications

Supervisor: Péter Pál Pálfy

Budapest, Hungary

2009

Contents

1 Introduction **1**

2 Commutators and characters of finite algebra groups **4**

2.1 Commutators in algebra groups 6

2.2 Characters in algebra groups 11

3 On the characters of the unit group of DN-algebras **14**

3.1 The structure of DN-algebras 16

3.2 Characters of the unit group of a DN-algebra 19

4 On the class number of partition subgroups of $U_n(q)$ **25**

4.1 Number of matrices over finite fields having submatrices with specified rank 27

4.2 Number of conjugacy classes in partition subgroups of nilpotency class two 30

5 Small bases of solvable linear groups **41**

5.1 Finding regular partitions for solvable permutation groups 43

5.2 Primitive linear groups 52

5.2.1 The structure of the Fitting subgroup 53

5.2.2 Finding $x, y \in V$ in case of F is monomial 55

5.2.3 Finding $x, y \in V$ in case of F is not monomial 66

5.3 Imprimitive linear groups 70

Bibliography **73**

Abstract

We discuss three topic concerning the representations of solvable linear groups. First, we give a positive answer to a question of I. M. Isaacs about the characters of finite algebra groups. To answer Isaacs' question we prove a new identity for the commutators in finite algebra groups. To confirm this identity we use Lie theoretic methods. Then we generalise Isaacs' question to the unit group of a DN-algebra by using ordinary character theory.

Next, we examine a natural generalisation of a conjecture of G. Higman about the number of conjugacy classes in the group of upper unitriangular matrices $U_n(q)$. We prove that the analogue of Higman's conjecture does not hold to the so-called partition subgroups of $U_n(q)$ by using linear algebra and a few algebraic geometry.

Finally, we give a partly constructive proof to the widely asked conjecture that if $G \leq GL(V)$ is a solvable linear group such that $(|G|, |V|) = 1$, then there exist $x, y \in V$ such that only the identity element of G fixes both x and y. To find such a pair of vectors we use tools from the theory of permutation groups, some linear algebra, some representation theory of finite gorups and a nice description of maximal solvable primitive linear groups.

Acknowledgment

First of all, I would like to express my gratitude to my supervisor Prof. Péter Pál Pálfy for his guidance, support and patience during my research. His continuous help was invaluable for writing both my master thesis at ELTE and this doctoral thesis at CEU. I am also grateful to Prof. László Pyber. He suggested me a number of questions and conjectures, in particular the problem discussed in Chapter 5. I would also like to thank the Central European University and the Rényi Institute of Mathematics, where I started my research work as a young researcher. Thanks for their financial support and for the inspiring lectures. My friends, Károly Podoski and Balázs Szegedy have also helped me a lot. The first problem I solved was suggested to me by Balázs, while Károly, my co-author, has inspired me a lot by talking many occasions about unsolved problems. Many thanks for them. Last, but not least I would like to thank my parents and my brothers. Without their continuous support and love I would not have become a mathematician.

Chapter 1

Introduction

One of the most effective tools for investigating a group is to study the linear representations of the group. If G is a group, and K is a field, then a K-representation of G is a group homomorphism into the matrix group $GL(n, K)$. In the following, we restrict our attention to finite groups and to their ordinary representations, that is, we assume that the characteristic of K does not divide the order of G. By Maschke's theorem, we know that every representation of the group is just the sum of irreducible ones, so it is enough to investigate the irreducible representations of the given group.

If the representation $G \to GL(n, K)$ is faithful, that is, its kernel is trivial, then G can be viewed as a subgroup of the general linear group. Such groups are called linear groups. Of course, every abstract group can be represented as a linear group by taking its regular action on the group algebra KG. In this thesis we examine that for a given linear group $G \leq GL(n, K) \simeq GL(V)$, what can be said about its action on V, about its other representations, maybe over a different field, etc.

If $X : G \to GL(n, \mathbb{C})$ is a representation of the finite group G, then its character is defined as $\chi(g) = \mathrm{Tr}(X(g))$. It is known that the character of a representation defines the representation itself, so usually it is enough to search for characters of a group, not for the more complicated representations.

One effective way is to find characters (or representations) of a given group is the tool of induction. Starting from a subgroup $H \leq G$ and a character ϕ of H, one can construct a character ϕ^G of G. A character χ of G is said to be monomial if there exist a subgroup $H \leq G$ and a linear (i.e. one-dimensional) character λ of H such that $\chi = \lambda^G$. A group is said to be an M-group if all of its irreducible characters are monomial. It is known that every M-group is solvable and every supersolvable (specifically, every nilpotent) group is an M-group.

In Chapter 2 we investigate the characters of finite algebra groups defined by I. M. Isaacs [15]. Let K be a finite field of order q and of characteristic p. If A is a finite dimensional associative algebra over K with Jacobson radical $J(A)$, then $1+J(A)$ is called a K-algebra group. Such a group is a p-group, so it is also an M-group. Therefore, if χ is an irreducible character of $1 + J(A)$, then there is a subgroup H and a linear character λ of H such that $\lambda^{1+J(A)} = \chi$. We prove that H can be chosen in a more specific way: The main result of Chapter 2 is that every irreducible character of an algebra group is induced from a linear character of some algebra subgroup, that is, a subgroup of the form $1 + U$, where U is a subalgebra of J. To prove this, we found a new commutator identity in algebra groups. In the proof of this identity we use mainly Lie theoretic methods.

In Chapter 3 we examine a similar question as we did in Chapter 2 but to another class of groups, to the unit group of DN-algebras. By the definition of B. Szegedy [26], if A is a finite dimensional algebra over the field K, then A is called a DN-algebra if the nilpotent elements in A form an ideal of A (this ideal is just the Jacobson radical of A) and $A/J(A)$ is isomorphic to a direct sum of copies of K. Szegedy proved in his paper that the unit group of a DN-algebra is always an M-group. Like we did for algebra groups, we show that if A is a DN-algebra with unit group $U(A)$ and χ is an irreducible character of $U(A)$, then there is a subalgebra $B \leq A$ and a linear character λ of $U(B)$ such that $\lambda^{U(A)} = \chi$.

A very good example for algebra groups is the group of upper unitriangular matrices $U_n(q) \leq GL(n, q)$. If one would like to describe the irreducible characters of a group,

maybe the first question is, how many characters the group has. It is well-known that the number of complex irreducible characters is equal to the number of conjugacy classes of the group. Concerning the number of conjugacy classes of $U_n(q)$, there is the following long-standing conjecture: Let n be fixed, and let $k(U_n(q))$ denote the number of conjugacy classes of $U_n(q)$. Then there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that for all prime powers q we have $k(U_n(q)) = f(q)$. In Chapter 4 we generalize this conjecture to the so-called partition subgroups of $U_n(q)$. We confirm the analogous conjecture to normal partition subgroups of nilpotency class two. On the other hand, more interestingly, we prove that there are partition subgroups for which this generalized conjecture does not hold.

The last chapter is about the base problem for coprime solvable linear groups. Let V be a finite vector space, and let $G \leq GL(V)$ be a linear group acting naturally on V. If we forget the structure on V, then we can think of G as merely a group of permutations acting on the set V. A base for a permutation group $G \leq \mathrm{Sym}(V)$ is a subset of V such that only the identity element of G fixes every element of this subset. For both theoretical and computational reasons it is useful to find small bases for permutation groups. It was asked by I. M. Isaacs that for coprime solvable linear groups $G \leq GL(V)$ whether there exists a base for G of size two, that is, two vectors $x, y \in V$, such that if $g \in G$ fixes both x and y then $g = 1$. In a joint work with K. Podoski [12] we proved the existence of such vectors in the case when the characteristic of the ground field is not equal to 2. As the other cases were already proved by A. Moreto, T. R. Wolf [20], and S. Dolfi [4], this answers Isaacs' question.

Chapter 2

Commutators and characters of finite algebra groups

The material of this chapter is based on [9]. Let A be a finite $\mathbb{F}_q$-algebra with identity, where $\mathbb{F}_q$ is a finite field of characteristic p. Let $J = J(A)$ be the Jacobson radical of A. Then the group $1 + J$ is called an $\mathbb{F}_q$-*algebra group*. The subgroups of an algebra group which are of the form $1+U$, where $U \leq J$ is a subalgebra of J are called *algebra subgroups*.

If A is a finite dimensional algebra, then $J(A)$ is a nilpotent algebra, so $1 + J(A)$ is a nilpotent subgroup of the group of units of A. If J is a finite dimensional nilpotent algebra then we can define an algebra $A = \mathbb{F}_q \cdot 1 + J$ such that $J = J(A)$. So the algebra groups are exactly the groups $1 + J$ associated to the finite nilpotent algebras J with multiplication defined by $(1 + j_1) \cdot (1 + j_2) := 1 + j_1 + j_2 + j_1 j_2$. Concerning the characters of such groups, the following theorem was proved by I. M. Isaacs.

Theorem 2.1. (Isaacs [15, Theorem A]) *Let G be an $\mathbb{F}_q$-algebra group. Then all irreducible complex characters of G have q-power degree.*

If G is an $\mathbb{F}_q$-algebra group, then G is a finite p-group, hence it is an M-group, that is, any irreducible character of G is induced from a linear character of some subgroup of G.

Isaacs' theorem says that such a subgroup must have q-power index. The next theorem states that one can choose this subgroup in a more specific way.

Theorem 2.2. *Let G be an $\mathbb{F}_q$-algebra group and $\chi \in \mathrm{Irr}(G)$. Then there exist an $\mathbb{F}_q$-algebra subgroup $H \leq G$ and a linear character λ of H such that $\chi = \lambda^G$.*

This result appears as a question in the paper of Isaacs and it was proved by Carlos A. M. André in [1] for the case $J^p = 0$, where $p = \mathrm{char}\,\mathbb{F}_q$. We note that Theorem A, Corollary B and Theorem C in [15] are immediate consequences of our Theorem 2.2. However, our proof of Theorem 2.2 uses Isaacs' theorem. Recently, M. Boyarchenko [2] gave a new proof, which does not use Isaacs' theorem any longer. To prove the theorem, we use induction on $|G|$. The key of the induction step is the following result, which is interesting in its own:

Theorem 2.3. *Let $G = 1 + J$ be an $\mathbb{F}_q$-algebra group and $\varphi \in \mathrm{Irr}(1 + J^2)$. If φ is a G-invariant character, then φ is linear.*

Exchanging $1 + J^2$ for G' in the above theorem, we get that any irreducible G-invariant character of G' is linear, a similar statement that holds for any finite nilpotent group. In the proof of this similar statement the central series

$$G = \gamma_1 \geq G' = \gamma_2 \geq \ldots \gamma_k = 1$$

and the identity $[\gamma_m, \gamma_n] \leq [\gamma_1, \gamma_{m+n-1}] = \gamma_{m+n}$ play a significant role. To prove Theorem 2.3 we use the central series

$$G = 1 + J \geq 1 + J^2 \geq \ldots \geq 1 + J^k = 1.$$

We have found the following identity for the commutators of the elements of this central series.

Theorem 2.4. *Let J be an arbitrary nilpotent ring and let $1 + J$ be the group associated to J. Then for all $m, n \in \mathbb{N}$:*

$$[1 + J^m, 1 + J^n] \subseteq [1 + J, 1 + J^{m+n-1}]. \tag{2.1}$$

In the following, we prove this identity in section 2.1. Then, we use this identity in section 2.2 to prove Theorems 2.3 and 2.2.

2.1 Commutators in algebra groups

The main purpose of this section is to prove Theorem 2.4. First we show an easy lemma:

Lemma 2.5. *If* $[1 + A^k, 1 + A^l] \subseteq [1 + A, 1 + A^{k+l-1}]$ *for a nilpotent ring* A*, then* $[1 + B^k, 1 + B^l] \subseteq [1 + B, 1 + B^{k+l-1}]$ *for every quotient ring* B *of* A*.*

Proof. Let $\varphi : A \to B$ denote the natural ring homomorphism from A to B. Then we can extend this homomorphism to a group homomorphism $\overline{\varphi} : 1 + A \to 1 + B$ by the rule $\overline{\varphi}(1 + a) := 1 + \varphi(a)$. It is clear that $\overline{\varphi}(1 + A^k) = 1 + B^k$ for all k and $\overline{\varphi}([H, K]) = [\overline{\varphi}(H), \overline{\varphi}(K)]$ for all subgroups H, K of $1 + A$. The assertion follows. □

In the following let $R = \mathbb{Q}$ or $\mathbb{Z}$ and denote by $F_R(X)$ the free algebra over R generated by the set X and by $F_R(n, X)$ the free nilpotent algebra over R with nilpotency class n generated by the set X. Then $F_R(n, X) \simeq F_R(X)/F_R(X)^n$. This means that $F_R(n, X)$ is the algebra of polynomials with noncommuting indeterminates in the set X subject to the relations that any product of n elements is zero. It is clear that every nilpotent ring is a quotient of $F_{\mathbb{Z}}(n, X)$ for some n and X, so by Lemma 2.5, in order to prove Theorem 2.4 it is enough to show formula (2.1) for the free nilpotent algebras over $\mathbb{Z}$.

To the examination of commutators in $1 + J$ it is worth rephrasing the problem to Lie commutators of the Lie algebra J, as in general it is much easier to handle Lie commutators than group commutators. To achieve this, the exponential map will be useful.
If J is a nilpotent algebra over the field R such that either $\operatorname{char} R = 0$ or $\operatorname{char} R = p$ and $x^p = 0$ for all $x \in J$ then one can define the map $\exp : J \to 1 + J$ and the inverse of this

map $\ln : 1 + J \to J$ by the usual power series:

$$\exp(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^k}{k!} + \cdots ,$$
$$\ln(1 + x) = x - \frac{x^2}{2} + \cdots + (-1)^{k+1}\frac{x^k}{k} + \cdots .$$

The Campbell–Hausdorff formula says that for all $a, b \in J$:

$$\exp(a)\exp(b) = \exp\Big(a + b + z(a, b)\Big) \tag{2.2}$$

where $z(a, b)$ is a rational linear combination of iterated Lie commutators of a and b of weight ≥ 2. This formula can be found for example in [17, pp. 170–174] and it holds if either $\operatorname{char} R = 0$ or $\operatorname{char} R = p$ and $J^p = 0$. The following connection between group commutators and Lie commutators can be found in [18, Lemma 9.15]:

$$[\exp a, \exp b] = \exp([a, b] + w(a, b)) \qquad \text{for all } a, b \in J. \tag{2.3}$$

In the above equation $w(a, b)$ is a rational linear combination of iterated Lie commutators of a, b of weight ≥ 3.

Unfortunately, the exponential map cannot be used to algebras over $\mathbb{Z}$. However, $F_{\mathbb{Q}}(n, X) = \mathbb{Q} \cdot F_{\mathbb{Z}}(n, X)$, hence results to $\mathbb{Q}$-algebras will be useful in the examination of $\mathbb{Z}$-algebras. Therefore, we first assume that J is a nilpotent $\mathbb{Q}$-algebra.

In the following, it will be more useful to find connections between subgroups and Lie subalgebras, than between elements. The next lemma shows such a connection.

Lemma 2.6. *Let J be a nilpotent algebra over $\mathbb{Q}$. Then the exponential map establishes a bijection between J^k and $1 + J^k$ for all k. Furthermore, it is a bijection between the Lie commutator $[J^k, J^l]$ and the group commutator $[1 + J^k, 1 + J^l]$ for all k, l.*

Proof. The first part of the Lemma is obvious. Using formula (2.2) and the fact that $[J^k, J^l]$ is a Lie subalgebra of J it follows that $\exp[J^k, J^l]$ is a subgroup in $1 + J$. Let $x \in J^k$ and $y \in J^l$. Then $[\exp x, \exp y] \in \exp[J^k, J^l]$ by formula (2.3). It is clear that the

set $\{[\exp x, \exp y]] \mid x \in J^k,\ y \in J^l\}$ generates the subgroup $[1+J^k, 1+J^l]$. The inclusion $[1+J^k, 1+J^l] \subseteq \exp[J^k, J^l]$ is clear from this.

To see that $\exp(u) \in [1+J^k, 1+J^l]$ for any $u \in [J^k, J^l]$ we assume $k \geq l$ and we use reverse induction on k. The statement is obvious if $J^k = 0$. Let $u = \sum_{i=1}^{n} [u_i, v_i]$, where $u_i \in J^k$ and $v_i \in J^l$. Using equations (2.2) and (2.3) we get

$$\exp(u)\Big(\prod_{i=1}^{n}[\exp(u_i), \exp(v_i)]\Big)^{-1} = \exp(u)\prod_{i=n}^{1}\exp(-[u_i, v_i] - w(u_i, v_i)) = \exp(w),$$

where each $w(u_i, v_i)$, so also w, is a rational linear combination of commutators in the elements u_i, v_i of weight ≥ 3. Thus $w \in [J^{k+l}, J^l]$ and $\exp(w) \in [1+J^{k+l}, 1+J^l] \subseteq [1+J^k, 1+J^l]$ by reverse induction on k. Therefore, $\exp(u) \in [1+J^k, 1+J^l]$ and we are done. □

In fact, if J is a nilpotent algebra over $\mathbb{Q}$ then equation (2.1) follows easily from this last lemma, since the inclusion $[J^k, J^l] \subseteq [J, J^{k+l-1}]$ can easily be proved. However, to prove equation (2.1) in general, we first prove an other equation to free nilpotent algebras first over $\mathbb{Q}$ and then over $\mathbb{Z}$.

Lemma 2.7. *If $J = F_{\mathbb{Q}}(n, X)$ is a free nilpotent algebra over $\mathbb{Q}$ then for all $k \geq 2$:*

$$[1+J, 1+J] \cap (1+J^k) = [1+J, 1+J^{k-1}]. \tag{2.4}$$

Proof. Applying the ln map to (2.4) and using Lemma 2.6 we get the equation

$$[J, J] \cap J^k = [J, J^{k-1}] \tag{2.5}$$

is equivalent to equation (2.4). For all $i < n$ let $X^i = \{u_1 u_2 \cdots u_i \mid u_j \in X,\ 1 \leq j \leq i\}$. Then $B = \bigcup_{i=1}^{n-1} X^i$ is a basis of J. Using that the Lie bracket is a bilinear function and X is a free generator set, it follows that $[J, J] \cap J^k$ can be generated (as a vector space) by the set

$$Y = \big\{[a, b] \mid a \in X^l, b \in X^m,\ l + m \geq k\big\}$$

Let $a = x_1 x_2 \cdots x_l \in X^l$ and $b = y_1 y_2 \cdots y_m \in X^m$ such that $l + m \geq k$. Then

$$\begin{aligned}[a,b] &= x_1 \cdots x_l y_1 \cdots y_m - y_1 \cdots y_m x_1 \cdots x_l \\ &= x_1 \cdot x_2 \cdots x_l y_1 \cdots y_m - x_2 \cdots x_l y_1 \cdots y_m \cdot x_1 \\ &\quad + x_2 \cdot x_3 \cdots x_l y_1 \cdots y_m x_1 - x_3 \cdots x_l y_1 \cdots y_m x_1 \cdot x_2 + \cdots \in [J, J^{k-1}].\end{aligned}$$

Therefore $Y \subseteq [J, J^{k-1}]$ and $[J, J] \cap J^k \subseteq [J, J^{k-1}]$. It is clear that $[J, J] \cap J^k \supseteq [J, J^{k-1}]$, so the proof is complete. □

Remark. If J is any nilpotent algebra then equation (2.5) is not true in general. P. P. Pálfy showed me the following example: Let $J \leq M_4(\mathbb{Q})$ be the algebra of strictly upper triangular matrices with equal elements next to the main diagonal. Then

$$J = \begin{pmatrix} 0 & a & * & * \\ 0 & 0 & a & * \\ 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad J^2 = \begin{pmatrix} 0 & 0 & b & * \\ 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \qquad J^3 = [J, J] = \begin{pmatrix} 0 & 0 & 0 & c \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

In this case $[J, J] \cap J^3 = J^3 \neq 0$ but $[J, J^2] = 0$.

Up till now we have worked with rational nilpotent algebras. Now we consider free nilpotent rings over $\mathbb{Z}$. Our next purpose is to prove (2.4) for such rings. First we prove an easy lemma.

Lemma 2.8. *Let V be a vector space over $\mathbb{Q}$ and let $B \subseteq V$ be a basis of V. For any subset Y we denote by $\langle Y \rangle_{\mathbb{Z}}$ the set of all linear combinations of elements from Y with integer coefficients. If $Y \subseteq \{a - b \mid a, b \in B\}$, then $\langle Y \rangle_{\mathbb{Q}} \cap \langle B \rangle_{\mathbb{Z}} = \langle Y \rangle_{\mathbb{Z}}$.*

Proof. Let $z = \sum_{i=1}^{m} \alpha_i y_i \in \langle Y \rangle_{\mathbb{Q}} \cap \langle B \rangle_{\mathbb{Z}}$ be such that $\{y_1, y_2, \ldots, y_m\} \subseteq Y$ is linearly independent, and each $\alpha_i \in \mathbb{Q}$ is nonzero. Then there is a minimal subset $B' \subseteq B$ such that $\{y_1, y_2, \ldots, y_m\} \subseteq \langle B' \rangle_{\mathbb{Z}}$. Since $m = \dim \langle y_1, y_2, \ldots, y_m \rangle < |B'|$, there is an element

$b \in B'$ for which there exists exactly one y_k such that b appears with non-zero coefficient in y_k. Then α_k is integer, thus

$$z - \alpha_k y_k = \sum_{i \neq k} \alpha_i y_i \in \langle Y \rangle_{\mathbb{Q}} \cap \langle B \rangle_{\mathbb{Z}} .$$

The result follows by induction on m. □

Lemma 2.9. *If $J(\mathbb{Z}) = F_{\mathbb{Z}}(n, X)$ is a free nilpotent ring then for all $k \geq 2$*

$$[1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})] \cap (1 + J(\mathbb{Z})^k) = [1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})^{k-1}].$$

Proof. It is evident that

$$[1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})] \cap (1 + J(\mathbb{Z})^k) \supseteq [1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})^{k-1}].$$

Let $J(\mathbb{Q}) = F_{\mathbb{Q}}(n, X)$ be the free nilpotent algebra over $\mathbb{Q}$ having the same generator set and nilpotency class as $J(\mathbb{Z})$ has. Since $1 + J(\mathbb{Z})^k \leq 1 + J(\mathbb{Q})^k$, it follows that

$$\begin{aligned}[1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})] \cap (1 + J(\mathbb{Z})^k) &\leq [1 + J(\mathbb{Q}), 1 + J(\mathbb{Q})] \cap (1 + J(\mathbb{Q})^k) \\ &= [1 + J(\mathbb{Q}), 1 + J(\mathbb{Q})^{k-1}],\end{aligned}$$

using Lemma 2.7. As $J(\mathbb{Q})$ is a free nilpotent algebra, we can write all elements of $J(\mathbb{Q})$ uniquely as polynomials in elements of X such that all terms of these polynomials have degree $< n$. Furthermore, $J(\mathbb{Z}) \leq J(\mathbb{Q})$ is exactly the set of polynomials with integer coefficients. So it is enough to prove that the elements of $[1 + J(\mathbb{Q}), 1 + J(\mathbb{Q})^{k-1}]$ with integer coefficients belong to $[1 + J(\mathbb{Z}), 1 + J(\mathbb{Z})^{k-1}]$.

We define the degree of an element $z \in J(\mathbb{Z})$ as the smallest degree of its terms. In other words, the degree of z is the largest l such that $z \in J(\mathbb{Z})^l$. Choose an element $1 + z \in [1 + J(\mathbb{Q}), 1 + J(\mathbb{Q})^{k-1}] \cap (1 + J(\mathbb{Z}))$. If z has degree $l \geq k$ then $1 + z \in [1 + J(\mathbb{Q}), 1 + J(\mathbb{Q})^{l-1}]$ by equation (2.4). In case of $l > k$ we can use reverse induction

on l to prove that $1+z \in [1+J(\mathbb{Z}), 1+J(\mathbb{Z})^{l-1}]$ noting that the result is certainly true for l large enough. Hence we can assume that $l = k$.

Let $[X, X^{k-1}] = \{[u, v] \mid u \in X, v \in X^{k-1}\}$. We write $1+z = \prod [1+x_i, 1+y_i]^{\pm 1}$, where $x_i \in J(\mathbb{Q})$ and $y_i \in J(\mathbb{Q})^{k-1}$. It is clear that $[x_i, y_i] \in \left\langle [X, X^{k-1}] \right\rangle_{\mathbb{Q}} + J(\mathbb{Q})^{k+1}$, so

$$1+z = \prod [1+x_i, 1+y_i]^{\pm 1} \in \left(1 + \sum \pm [x_i, y_i] + J(\mathbb{Q})^{k+1}\right) \cap (1+J(\mathbb{Z})) \\ \subseteq 1 + \left(\left\langle [X, X^{k-1}] \right\rangle_{\mathbb{Q}} \cap J(\mathbb{Z})\right) + J(\mathbb{Q})^{k+1}.$$

Using that $\left\langle [X, X^{k-1}] \right\rangle_{\mathbb{Q}} \cap J(\mathbb{Z}) = \left\langle [X, X^{k-1}] \right\rangle_{\mathbb{Z}}$ by Lemma 2.8, it follows that $1+z \in 1 + \left\langle [X, X^{k-1}] \right\rangle_{\mathbb{Z}} + J(\mathbb{Q})^{k+1}$. From this we get $z \in \sum_{j=1}^{m} \alpha_j [a_j, b_j] + J(\mathbb{Q})^{k+1}$, where $\alpha_j \in \mathbb{Z}$, $a_j \in X$ and $b_j \in X^{k-1}$ for all j. Then

$$1 + z' := (1+z) \cdot (\prod [1+\alpha_j a_j, 1+b_j])^{-1}$$

is an element of $[1+J(\mathbb{Q}), 1+J(\mathbb{Q})^{k-1}] \cap (1+J(\mathbb{Z}))$ and z' has degree greater than k. Thus $1+z' \in [1+J(\mathbb{Z}), 1+J(\mathbb{Z})^{k-1}]$ by reverse induction and so $1+z \in [1+J(\mathbb{Z}), 1+J^(\mathbb{Z})^{k-1}]$, too. This completes the proof. □

Proof of Theorem 2.4. It was shown at the beginning of this section that it is enough to prove equation (2.1) in the case when $J = J(\mathbb{Z})$ is a free nilpotent ring. It is clear that

$$[1+J(\mathbb{Z})^m, 1+J(\mathbb{Z})^n] \subseteq [1+J(\mathbb{Z}), 1+J(\mathbb{Z})] \cap \left(1+J(\mathbb{Z})^{m+n}\right).$$

The right-hand side of this inclusion is exactly $[1+J(\mathbb{Z}), 1+J(\mathbb{Z})^{m+n-1}]$ by Lemma 2.9, so we are done. □

Remark. In fact, Theorem 2.4 holds if we only assume that J is a locally nilpotent ring.

2.2 Characters in algebra groups

Let $G = 1+J$ be a finite algebra group over $\mathbb{F}_q$ where $q = p^f$ for some prime p. In this section we prove Theorem 2.2 and Theorem 2.3. The induction step depends on the

following lemma. In case of $q \neq p$, our proof uses also Isaacs' theorem.

Lemma 2.10. *Let $G = 1 + J$ be a finite algebra group over $\mathbb{F}_q$ and $\chi \in \mathrm{Irr}(G)$. Then the following properties are equivalent:*

1. *There exist a proper algebra subgroup $H < G$ and $\varphi \in \mathrm{Irr}(H)$ such that $\chi = \varphi^G$.*
2. *χ_{1+J^2} is not irreducible.*

Proof. Suppose $H = 1 + U \neq G$ is an algebra subgroup and $\varphi \in \mathrm{Irr}(H)$ is such that $\chi = \varphi^G$. Let $K = H(1 + J^2) = 1 + U + J^2$. Then $1 + J^2 \leq K \neq G$ by [15, Lemma 3.1]. Thus $\chi = (\varphi^K)^G$ and χ_K is not irreducible. Then χ_{1+J^2} is not irreducible, too.

Assume now that χ_{1+J^2} is not irreducible and let $\psi \in \mathrm{Irr}(1 + J^2)$ be a constituent of χ_{1+J^2}. Let $H = 1+U \geq 1+J^2$ be a maximal $\mathbb{F}_q$-algebra subgroup such that ψ is extendible to H. Then $H \neq G$. We choose a $\varphi \in \mathrm{Irr}(H)$ such that φ is an extension of ψ and φ is a constituent of χ_H. Then for an arbitrary $x \in J \setminus U$ the subgroup $N_x = 1 + \mathbb{F}_q x + U$ is an $\mathbb{F}_q$-algebra subgroup and $|N_x : H| = q$. Let $\vartheta \in \mathrm{Irr}(N_x)$ be a character over φ, that is, φ is a constituent of ϑ_H. By Theorem 2.1, $\vartheta(1)$ and $\varphi(1)$ are both q-powers hence either $\vartheta_H = \varphi$ or $\vartheta = \varphi^{N_x}$. The first case cannot occur by the maximal choice of H, thus $\vartheta = \varphi^{N_x}$. Therefore, $I_{N_x}(\varphi) = H$ for all $x \in J \setminus U$ by [14, Problem 6.1], thus $I_G(\varphi) = H$. Using [14, Problem 6.1] again, we get φ^G is irreducible, so $\chi = \varphi^G$. □

Proof of Theorem 2.3. Let $G = 1 + J$ be an algebra group and $\varphi \in \mathrm{Irr}(1 + J^2)$ be a G-invariant character. We prove by reverse induction that $[1 + J^2, 1 + J^k] \leq \ker \varphi$ for all $k \geq 2$. This is clear if $J^k = 0$. Assuming that $[1 + J^2, 1 + J^k] \leq \ker \varphi$ it follows that $1 + J^k \leq Z(\varphi)$, where $Z(\varphi)$ denotes the center of φ. Hence $\varphi_{1+J^k} = \lambda \cdot \varphi(1)$, where λ is a G-invariant linear character of $1 + J^k$. It follows that $[1 + J, 1 + J^k] \leq \ker \varphi$. Using Theorem 2.4 we have $[1 + J^2, 1 + J^{k-1}] \leq [1 + J, 1 + J^k]$, thus $[1 + J^2, 1 + J^{k-1}] \leq \ker \varphi$. We get $(1 + J^2)' = [1 + J^2, 1 + J^2] \leq \ker \varphi$, so φ is a linear character. □

Proof of Theorem 2.2. If $\chi \in \mathrm{Irr}(G)$ is not linear, then χ_{1+J^2} is not irreducible by Theorem 2.3. By Lemma 2.10 there exist an algebra subgroup $H \neq G$ and $\varphi \in \mathrm{Irr}(H)$ such that $\chi = \varphi^G$. Using induction on $|G|$, we obtain that there exist an algebra subgroup $L \leq H$ and $\lambda \in \mathrm{Irr}(L)$ such that λ is a linear character of L and $\varphi = \lambda^H$. The theorem follows from the transitivity of induction. $\square$

Chapter 3

On the characters of the unit group of DN-algebras

The results of this chapter has appeard in [10]. In the following we continue to examine the structure and the characters of the unit group of some special algebras. The main result of this chapter is Theorem 3.3, which is the analogoue of Theorem 2.2 for the unit group of DN-algebras. The name "DN-algebra" is due to B. Szegedy [26]. Here we recall its definition:

Definition 3.1. (Szegedy [26]) Let A be a finite dimensional algebra with unit element over the finite field K. We say that A is a *DN-algebra* if the set of the nilpotent elements is an ideal of A (this ideal is equal to the Jacobson radical of A, denoted by $J(A)$), and $A/J(A)$ is isomorphic to a direct sum of copies of K.

A significant example of DN-algebras is the algebra of all $n \times n$ upper triangular matrices over K. Its unit group, called the Borel subgroup of $GL(n, K)$, is the group of all invertible upper triangular matrices in $GL(n, K)$. The following theorem shows that the Borel subgroup is an M-group.

Theorem 3.2. (Szegedy [26]) *If A is a DN-algebra over the q-element field then the unit group of A is an M-group.*

If the characteristic of the ground field is p, then the unique Sylow p-subgroup of $U(A)$ has the form $1 + J(A)$, i.e., it is an algebra group examined in the previous chapter. By Theorem 2.2, the irreducible characters of $1 + J(A)$ are induced from linear characters of algebra subgroups. Comparing this result with the result of B. Szegedy it is natural to ask whether a similar statement holds for the unit group of a DN-algebra. It is true indeed, and our goal is to prove the following theorem:

Theorem 3.3. *Let A be a DN-algebra and let $U(A)$ denote the unit group of A. Then for every $\omega \in \mathrm{Irr}(U(A))$ there exist a subalgebra $C \leq A$ and a linear character λ of $U(C)$ such that $\omega = \lambda^{U(A)}$.*

Remarks.

- The subalgebras of a DN-algebra containing 1 are DN-algebras themselves by a lemma of B. Szegedy [26, Lemma 2.2].

- It is easy to check that the number of units in a DN-algebra over the field $\mathbb{F}_q$ has the form $q^r(q-1)^s$ where r and s are nonnegative integers. Hence our Theorem 3.3 implies that the degrees of irreducible characters of $U(A)$ have the same form.

- If A is a DN-algebra over the field $K \simeq \mathbb{F}_2$, then $U(A) = 1 + J(A)$, so in this case Theorem 3.3 says the same as Theorem 2.2. Hence we assume $K \not\simeq \mathbb{F}_2$ in the following.

- In the case when $A/J(A) \simeq K$, i.e., if A is a local algebra, $U(A)$ can be written in the form $U(A) = (K^* \cdot 1) \times (1 + J(A))$. So, if $\omega \in \mathrm{Irr}(U(A))$, then $\omega = \mu \times \chi$ where $\mu \in \mathrm{Irr}(K^* \cdot 1)$ and $\chi \in \mathrm{Irr}(1 + J(A))$. If $C \leq J(A)$ is a multiplicatively closed subspace and $\lambda \in \mathrm{Irr}(1 + C)$ such that $\lambda^{1+J(A)} = \chi$, then $K \cdot 1 + C$ is a

subalgebra of A and $\mu \times \lambda \in \mathrm{Irr}(U(K \cdot 1 + C))$ is a linear character. Furthermore, $(\mu \times \lambda)^{U(A)} = \mu \times \chi = \omega$, which proves Theorem 3.3 for local algebras.

3.1 The structure of DN-algebras

In this section we prove some lemmas about the structure of DN-algebras which will be used in the next section.

Lemma 3.4. *Let A be a DN-algebra over the finite field K and let $J = J(A)$ denote the Jacobson radical of A.*

(a) There is a set of non-zero orthogonal idempotents $e_1, e_2, \ldots, e_k \in A$, where $e_1 + e_2 + \ldots + e_k = 1$ and k is the dimension of A/J over K.

(b) Let $B = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_k$. Then $A = B + J$ and $B \cap J = 0$. Hence $U(A) = (1 + J) \rtimes U(B)$ is a semidirect product.

(c) If M is a B-bimodule, then it is the direct sum of the homogeneous sub-bimodules $e_i M e_j$.

(d) If $M_1 \leq M$ are B-bimodules, then there exists a sub-bimodule $M_2 \leq M$, such that $M = M_1 \oplus M_2$.

(e) Every B-bimodule is a direct sum of one-dimensional sub-bimodules.

(f) If $u \in M$ generates a one-dimensional sub-bimodule, then there exist uniquely determined idempotents $e_l(u), e_r(u) \in \{e_1, e_2, \ldots, e_k\}$ such that $e_l(u)u = ue_r(u) = u$.

(g) If $u, v \in J$ both generate one-dimensional B-bimodules and $e_l(u) \neq e_r(v)$, then $vu = 0$.

Proof. Part (a) follows by "lifting idempotents" (see [3, Corollary 1.7.4]).

To prove (b) it is clear that B is a semisimple algebra and J is a nilpotent ideal of A such that $\dim B = \dim A/J$, so $B \cap J = 0$ and $A = B + J$. Let $\varphi : A \to A/J$ be the natural algebra homomorphism. The restriction of φ to $U(A)$ will be a surjective group homomorphism $U(A) \to U(A/J) \simeq U(B)$ with kernel $1 + J$, so $U(A) = (1 + J) \rtimes U(B)$ follows.

Let $\sum_m \alpha_m e_m, \sum_m \beta_m e_m \in B$ and $e_i v e_j \in e_i M e_j$. Then

$$\sum_m \alpha_m e_m (e_i v e_j) \sum_m \beta_m e_m = (\alpha_i \beta_j) e_i v e_j,$$

which proves the $e_i M e_j$'s are homogenous sub-bimodules for all $1 \leq i, j \leq k$. If $v \in M$, then there is a unique decomposition of $v = \sum v_{ij}$ such that $v_{ij} \in e_i M e_j$, namely $v_{ij} = e_i v e_j$. Hence M is the direct sum of the $e_i M e_j$'s and (c) is proved.

If $M_1 \leq M$ are B-bimodules, then for any $1 \leq i, j \leq k$ we have $e_i M_1 e_j \leq e_i M e_j$. Using that $e_i M e_j$ is homogenous it follows that all of its subspaces are sub-bimodules, so clearly there exists a sub-bimodule $M_{2,ij} \leq e_i M e_j$ such that $e_i M e_j = e_i M_1 e_j \oplus M_{2,ij}$. Now, let $M_2 = \oplus M_{2,ij}$. It is clear that $M = M_1 \oplus M_2$.

(e) follows easily from (c), because any subspace of a homogenous sub-bimodule is also a sub-bimodule, so any direct decomposition of a homogenous sub-bimodule to one dimensional subspaces is a direct decomposition to sub-bimodules.

If Ku is a B-bimodule, then clearly it is directly indecomposable, so using (c) there exist uniquely determined idempotents $e_l(u), e_r(u)$ such that $e_l(u) K u e_r(u) = Ku$. Then $e_i u = 0$ for all $e_i \neq e_l(u)$ and $u e_j = 0$ for all $e_j \neq e_r(u)$. Hence $e_l(u)u = (\sum e_i)u = u = u(\sum e_j) = u e_r(u)$, and (f) is proved.

Finally, (g) follows from the identity $vu = v e_r(v) e_l(u) u = 0$. □

In the following we fix a set of orthogonal idempotents $\{e_1, e_2, \ldots, e_k\} \subseteq A$ and the subalgebra $B = Ke_1 \oplus Ke_2 \oplus \cdots \oplus Ke_k$. So $U(A) = (1 + J) \rtimes U(B)$.

Lemma 3.5. *Let V be a B-bimodule with a direct decomposition $V = Kx_1 \oplus Kx_2 \oplus \cdots \oplus Kx_m$ to one-dimensional sub-bimodules, and let $0 \neq W < V$ be a subspace satisfying the following conditions:*

1. *$U(B)$ normalizes W.*
2. *$V' \cap W = 0$ for all proper sub-bimodules $V' < V$.*

Then

(a) $W \not\leq \oplus_{j \neq i} Kx_j$ for $1 \leq i \leq m$. Furthermore, W is a one-dimensional subspace.

(b) For $1 \leq i \neq j \leq m$ we have $e_l(x_i) \neq e_l(x_j)$ and $e_r(x_i) \neq e_r(x_j)$.

Proof. Let $V_i = \oplus_{j \neq i} Kx_j$. Then $V_i < V$ is a one-codimensional sub-bimodule, so $V_i \cap W = 0$ by condition 2 and both part of (a) follows.

If $e_l(x_i) = e_l(x_j)$ for $i \neq j$ then Kx_i and Kx_j are isomorphic as left submodules. So each subspace of $Kx_i \oplus Kx_j$ is a left submodule. Then $V' = \oplus_{s \notin \{i,j\}} Kx_s \oplus W$ is both a left submodule and invariant under the action of $U(B)$ by conjugation. Hence if $v \in V'$ and $b \in U(B)$ then $vb = b(b^{-1}vb) \in V'$. As the subspace generated by $U(B)$ is B, we get V' is a proper sub-bimodule containing W, contrary to the second assumption. The proof of the statement $e_r(x_i) \neq e_r(x_j)$ for $i \neq j$ is similar. □

We say that $1 + I \leq 1 + J$ is an *ideal subgroup* of $U(A)$, if $I \leq J$ is an ideal of A. We note that in this case $1 + I$ is a normal subgroup of $U(A)$. The next lemma gives us a specific generator set of an ideal subgroup.

Lemma 3.6. *Let $1 + I \leq 1 + J$ be an ideal subgroup. Then $1 + I$ is generated as a group by the set $Y = \{1 + x \,|\, x \in I,\ Kx$ is a B-sub-bimodule $\}$.*

Proof. We prove by reverse induction that $Y_k = Y \cap (1+J^k)$ generates $1+I_k = 1+(I \cap J^k)$ for all k. This is clear if $J^k = 0$. Assuming that Y_k generates $1 + I_k$ for some k we can choose $x_1, x_2, \ldots, x_l \in I_{k-1}$ by Lemma 3.4 such that $I_{k-1} = I_k \oplus Kx_1 \oplus \cdots \oplus Kx_l$ and each Kx_i is a B-sub-bimodule. Then $\{1 + Kx_i + I_k,\ i = 1, 2, \ldots, l\}$ generates $1 + (I_{k-1}/I_k) \simeq (1 + I_{k-1})/(1 + I_k)$, because $(1 + x + I_k)(1 + y + I_k) = 1 + x + y + I_k$ for $x, y \in I_{k-1}$. So $\{1 + Kx_i \,|\, i = 1, 2, \ldots, l\} \cup Y_k \subseteq Y_{k-1}$ generates $1 + I_{k-1}$. □

3.2 Characters of the unit group of a DN-algebra

We prove Theorem 3.3 in this section. We use all the notations of the previous section. The essential point of our proof is to prove that if χ is a non-linear, $U(B)$-invariant irreducible character of $1 + J$ then it can be obtained by induction from a proper ideal subgroup $L \geq 1 + J^2$. To see this we examine the action of $U(B)$ by conjugation on J as well as on $\mathrm{Irr}(1 + J)$. First, we introduce some notation.

In the following let $\mathrm{Irr}_{U(B)}(L)$ denote the set of all $U(B)$-invariant irreducible characters of an ideal subgroup L. For a subspace $V \subseteq J$ and for an irreducible character $\varphi \in \mathrm{Irr}(L)$ let $I_V(\varphi) = \{v \in V \,|\, 1 + v \in I_{1+J}(\varphi)\}$.

Lemma 3.7. *Let $L \leq 1 + J$ be an ideal subgroup of $U(A)$. If $\varphi \in \mathrm{Irr}(L)$, then the inertia subgroup $I_{U(B)}(\varphi)$ is the unit group of a subalgebra of B.*

Proof. If $L = 1 + I$, then I is an ideal of A, so $B + I$ is a subalgebra of A with unit group $U(B + I) = L \rtimes U(B)$. Hence we can assume without loss of generality that $L = 1 + J$. The subgroup $U(B)$ acts on $1 + J$ by conjugation. This action determines an action of $U(B)$ on $\mathrm{Irr}(1+J)$ and an action on $\mathrm{Cl}(1+J)$, on the set of conjugacy classes of the group $1 + J$. As $(|U(B)|, |1 + J|) = 1$ and $U(B)$ is solvable (even abelian), the two actions are permutation isomorphic by [14, Theorem 13.24]. It follows that $I_{U(B)}(\varphi) = St(\mathcal{C})$ for some

$\mathcal{C} \in \mathrm{Cl}(1+J)$, where $St(\mathcal{C})$ denotes the stabilizer of $\mathcal{C}$ in $U(B)$. If $x \in \mathcal{C}$ is an arbitrary element, then $St(\mathcal{C}) = U(B) \cap (C_{U(A)}(x)(1+J))$. Since $C_{U(A)}(x) = U(C_A(x))$ is the unit group of the subalgebra $C_A(x)$, we get $I_{U(B)}(\varphi) = U(B \cap (C_A(x) + J))$. Furthermore, $B \cap (C_A(x) + J)$ is a subalgebra of B and the proof is complete. □

The following consequences of Glaubermann's Lemma will be used to find $U(B)$-invariant characters of ideal subgroups.

Lemma 3.8. *Let S act on G such that $(|S|, |G|) = 1$ and let $N < L < G$ be S-invariant normal subgroups of G.*

1. *Let $\chi \in \mathrm{Irr}(G)$ be S-invariant. Then χ_N has an S-invariant irreducible constituent. Furthermore, any two such constituents are conjugate via an element of $C_G(S)$.*

2. *Let $\chi \in \mathrm{Irr}(G)$ and $\varphi \in \mathrm{Irr}(N)$ be S-invariant such that φ is a constituent of χ_N. Then there is an S-invariant $\psi \in \mathrm{Irr}(L)$ between χ and φ, that is, ψ is a constituent of χ_L and φ is a constituent of ψ_N.*

Proof. The first part of *1.* is a special case of [14, Theorem 13.27]. This Theorem also says that the hypotheses of Glaubermann's Lemma are satisfied, so the second part of *1.* follows from [14, Corollary 13.9]

To see *2.* we can apply *1.* twice. So we get S-invariant characters $\psi' \in \mathrm{Irr}(L)$ and $\varphi' \in \mathrm{Irr}(N)$ such that ψ' is a constituent of χ_L and φ' is a constituent of ψ'_N, so it is also a constituent of χ_N. By the second part of *1.* there is a $c \in C_G(S)$ such that $\varphi = (\varphi')^c$. Then $\psi = (\psi')^c \in \mathrm{Irr}(L)$ is an S-invariant character between χ and φ. □

Lemma 3.9. *Suppose that $1 + J$ is a K-algebra group, where K is a finite field with q elements and of characteristic p. Let $I \leq J$ be an ideal of J and let $\lambda \in \mathrm{Irr}(1 + I)$ be a linear character of $1 + I$ such that $J^2 \leq I_J(\lambda)$. Then $I_J(\lambda)$ is an ideal of J over K.*

Proof. It is clear that $I_J(\lambda)$ is an ideal of J over $\mathbb{F}_p$. So it is enough to show that if $x \in I_J(\lambda)$, then $Kx \subseteq I_J(\lambda)$.

By the definition of Isaacs [15] a subgroup $S \leq 1+J$ is called strong, if $|S \cap H|$ is a power of q for all algebra subgroups $H \leq 1+J$. We know that $I_{1+J}(\lambda)$ is a strong subgroup by [15, Theorem 8.3]. Let $x \in J$ be an arbitrary element. Then $1+Kx+J^2$ is an algebra subgroup, so either $1+Kx+J^2 \leq I_{1+J}(\lambda)$ or $(1+Kx+J^2) \cap I_{1+J}(\lambda) = 1+J^2$. The result follows. □

The following lemma will be used in two particular cases: If $L \geq 1+J^2$ or if $L = 1+J^k$ for some k.

Lemma 3.10. *Let $L = 1+I \leq 1+J$ be an ideal subgroup of $U(A)$. Assume that $\lambda \in Irr_{U(B)}(L)$ is a linear character such that $J^2 \leq I_J(\lambda)$. Then $I_J(\lambda)$ is an ideal of A.*

Proof. Let $I' \geq J^2$ be the unique maximal ideal of A in $I_J(\lambda)$. If $I' = J$, then there is nothing to prove. Otherwise, let us choose a sub-bimodule $V \leq J$ such that $J = I' \oplus V$ by Lemma 3.4 (d). Let $W = I_V(\lambda)$, so $I_J(\lambda) = I' + W$. What we need to show is that $W = 0$. Assume by contradiction that $0 \neq W < V$.

If J' is a proper ideal of A such that $J > J' \geq I'$, then $J'^2 \leq J^2 \cap J' \leq I_{J'}(\lambda)$, so $I_{J'}(\lambda)$ is an ideal of $A' = J' + B$ by using induction on $|A'|$. It follows that $I_{J'}(\lambda) \geq J^2$ is an ideal of A, so $I_{J'}(\lambda) = I'$ for such an ideal. If $V' < V$ is a proper sub-bimodule then $I' + V' < J$ is a proper ideal of A, hence $V' \cap W = I_{V'}(\lambda) = 0$. Furthermore, W is a K-subspace by Lemma 3.9 and $U(B)$ normalizes W. Hence all the assumptions of Lemma 3.5 hold for V and W. Let $V = Kx_1 \oplus Kx_2 \oplus \ldots \oplus Kx_l$ be a direct decomposition of V to one-dimensional sub-bimodules and let $Kz \leq I$ be a one-dimensional sub-bimodule. Choosing an $x \in \{x_1, x_2, \ldots, x_l\}$ we will prove that $[1+x, 1+z] \subseteq \ker \lambda$, or equivalently $\lambda^{1+x}(1+z) = \lambda(1+z)$. We distinguish two cases.

If $e_l(z) = e_r(x)$ and $e_r(z) = e_l(x)$, then it follows directly from Lemma 3.5 (b) and from Lemma 3.4 (g) that $x_j z = z x_j = 0$ for all $x_j \neq x$. Hence $[1+Kx_j, 1+z] = 0$ for

all $x_j \neq x$. On the other hand $[1 + I' + W, 1 + z] \subseteq \ker \lambda$ by the definition of I' and W. Clearly $\{1 + t \in 1 + J \mid \lambda^{1+t}(1 + z) = \lambda(1 + z)\}$ is a subgroup of $1 + J$, so it is enough to prove that

$$\langle 1 + Kx_j \,|\, x_j \neq x \rangle \, (1 + I' + W) = 1 + J.$$

It is clear that $1+J/1+I'$ is isomorphic to the additive group of V. On the other hand V is generated (as an additive group) by the set $\cup_{x_j \neq x} Kx_j \cup W$ by Lemma 3.5 (a). Therefore, $\langle 1 + Kx_j \,|\, x_j \neq x \rangle \, (1 + I' + W)/(1 + I') \simeq V$, which proves the above identity. Hence $\lambda^{1+x}(1 + z) = \lambda(1 + z)$, as we have claimed.

Now assume that, for example, $e_l(z) \neq e_r(x)$. Then $xz = 0$. Easy calculation shows that

$$[1 + x, 1 + z] = 1 + (1 + x)^{-1}(1 + z)^{-1}(xz - zx) = (1 - zx + z^2x - z^3x + \ldots).$$

It follows that $[1 + x, 1 + z] - 1 \in zAx$, so $([1 + x, 1 + z] - 1)^2 = 0$.

Let $a \in K^*$ be a non-zero field element. Then there exists $b \in U(B)$ such that $b^{-1}z = az$ and $xb = x$. Conjugating the commutator $[1 + x, 1 + z]$ by b we get

$$[1 + x, 1 + z]^b = (1 - zx + z^2x - z^3x + \ldots)^b = (1 - b^{-1}zxb + b^{-1}z^2xb - \ldots) =$$
$$1 + a(-zx + z^2x - z^3x + \ldots) = 1 + a\left([1 + x, 1 + z] - 1\right).$$

Let $C = K\left([1 + x, 1 + z] - 1\right)$. We have already seen that $([1 + x, 1 + z] - 1)^2 = 0$, hence C is a one dimensional algebra and $1 + C$ is an algebra subgroup. The above formula shows that all elements of $(1 + C) \setminus \{1\}$ are conjugate under the action of $U(B)$. Using the fact that λ is a $U(B)$-invariant character it follows that λ_{1+C} is a linear character such that λ_{1+C} is constant on $(1 + C) \setminus \{1\}$. Using that $|K| > 2$ we get $\lambda_{1+C} = 1_{1+C}$, i.e., $[1 + x, 1 + z] \in \ker \lambda$.

Let $Y = \{1 + z \,|\, Kz \leq I \text{ is a } B\text{-sub-bimodule}\}$. Then $\lambda^{1+x}(y) = \lambda(y)$ for all $x \in \{x_1, x_2, \ldots, x_l\}$ and for all $y \in Y$. But the subgroup generated by Y is equal to $1 + I$ by Lemma 3.6 and the values of a linear character on a set of generators determine

the character. Hence $\{x_1, x_2, \ldots, x_l\} \subseteq I_V(\lambda)$. But $I_V(\lambda)$ is a K-subspace with basis $\{x_1, x_2, \ldots, x_l\}$, so $I_V(\lambda) = V$, which is a contradiction to our assumption $I_V(\lambda) = W < V$. $\square$

The key step of the proof is the following theorem:

Theorem 3.11. *Suppose that A is a DN-algebra over the q-element field and let $U(A) = (1+J) \rtimes U(B)$. Let $\chi \in Irr_{U(B)}(1+J)$ be a non-linear, $U(B)$-invariant character of $1+J$. Then there exist a proper ideal subgroup $L < 1+J$ and a character $\psi \in Irr_{U(B)}(L)$ such that $\psi^{1+J} = \chi$.*

Proof. Let $\vartheta \in \mathrm{Irr}_{U(B)}(1+J^2)$ be a constituent of χ_{1+J^2}.

Assuming first that ϑ is a linear character, choose a maximal ideal subgroup L such that ϑ is extendible to L. Then $L < 1+J$, because χ is not a linear character. Furthermore, there exists a $\psi \in \mathrm{Irr}_{U(B)}(L)$ between χ and ϑ by Lemma 3.8 and this character is an extension of ϑ to L, because $L/(1+J^2)$ is abelian. Then $I_{1+J}(\psi)$ is an ideal subgroup by Lemma 3.10. We prove that $I_{1+J}(\psi) = L$. Otherwise, we could choose an ideal subgroup L' such that $|L' : L| = q$ and $L' \leq I_{1+J}(\psi) \leq I_{1+J}(\vartheta)$. The degree of each irreducible character of an ideal subgroup is a power of q by Theorem 2.1, so either $\psi^{L'}$ is irreducible, or ψ is extendible to L'. However, $I_{L'}(\psi) = L' > L$ so $\psi^{L'}$ cannot be irreducible by [14, Problem 6.1], and ψ cannot be extendible to L' by the maximal choice of L. So $I_{1+J}(\psi) = L$ and $\psi^{1+J} = \chi$.

If ϑ is not a linear character, then $I_{1+J}(\vartheta) < 1+J$ by Theorem 2.3. We prove the existence of a proper ideal subgroup $L \geq I_{1+J}(\vartheta)$. To see this let $k > 2$ be the smallest integer such that $1 + J^k \leq Z(\vartheta)$. Then $\vartheta_{1+J^k} = \vartheta(1) \cdot \lambda$, where $\lambda \in \mathrm{Irr}_{U(B)}(1+J^k)$ is a linear character such that $I_{1+J}(\lambda) \geq I_{1+J}(\vartheta) \geq 1 + J^2$. Applying Lemma 3.10 we get that $I_{1+J}(\lambda)$ is an ideal subgroup of $1+J$, so it remains to show that $I_{1+J}(\lambda) < 1+J$. On the one hand, $[1+J^2, 1+J^{k-1}] \not\leq (1+J^k) \cap \ker\vartheta = \ker\lambda$ by the minimal choice of k. On the

other hand, $[1+J^2, 1+J^{k-1}] \leq [1+J, 1+J^k]$ by Theorem 2.4. Hence $[1+J, 1+J^k] \not\leq \ker\lambda$, which is equivalent to the inequality $I_{1+J}(\lambda) \neq 1+J$. So $L = I_{1+J}(\lambda)$ is a proper ideal subgroup containing $I_{1+J}(\vartheta)$.

By the Clifford correspondence [14, Theorem 6.11] there exists an irreducible character φ of $I_{1+J}(\vartheta)$ such that $\varphi^{1+J} = \chi$. So $\chi = (\varphi^L)^{1+J}$ and χ is induced from a character of the proper ideal subgroup L. It follows directly from Clifford's theorem [14, Theorem 6.2] that $\chi = \psi^{1+J}$ for each component ψ of χ_L. Finally, we can choose ψ such that $\psi \in \mathrm{Irr}_{U(B)}(L)$ by Lemma 3.8. The proof is complete. □

Proof of Theorem 3.3. By the transitive property of induction and by the fact that all subalgebras of a DN-algebra are again DN-algebras it is enough to prove that if $\omega \in \mathrm{Irr}(U(A))$ is not a linear character then there exists a proper subalgebra $A' < A$ such that ω is induced from a character ω' of $U(A')$.

Let $U(A) = (1+J) \rtimes U(B)$ and let χ be a component of ω_{1+J}. Then $I_{U(B)}(\chi) = U(B')$ for a subalgebra B' of B by Lemma 3.7. Hence $I_{U(A)}(\chi) = U(A')$ is the unit group of the subalgebra $A' = B' + J$. By [14, Theorem 6.11], ω is induced from a character ω' of $U(A')$. If $B' < B$ then $A' = B' + J$ is a proper subalgebra of A.

Assume that $\chi \in \mathrm{Irr}_{U(B)}(1+J)$. Then χ is extendible to $U(A)$ by [14, Corollary 6.28]. (Note that $(|U(A) : 1+J|, |1+J|) = 1$.) Using [14, Corollary 6.17] we get ω is an extension of χ. So χ is not a linear character.

By Theorem 3.11 there exist a proper ideal subgroup $L = 1+I < 1+J$ and a character $\psi \in \mathrm{Irr}_{U(B)}(1+I)$ such that $\psi^{1+J} = \chi$. Then $A' = B + I$ is a proper subalgebra of A. Let φ be an extension of ψ to $U(A')$ by [14, Corollary 6.28]. Then $(\varphi^{U(A)})_{1+J} = \psi^{1+J} = \chi$ by [14, Problem 5.2], so $\varphi^{U(A)} = \omega\mu$ for some $\mu \in \mathrm{Irr}(U(A)/(1+J))$. Let $\omega' = \varphi\mu^{-1}_{U(A')}$. Hence $(\omega')^{U(A)} = \omega$ using [14, Problem 5.3]. The proof is complete. □

Chapter 4

On the class number of partition subgroups of $U_n(q)$

For a fixed natural number n let $U_n(q)$ denote the upper unitriangular $n \times n$ matrices over the finite field $\mathbb{F}_q$. A long-standing conjecture of G. Higman [13] says that for every $n \in \mathbb{N}$ there exists a polynomial $f_n(x) \in \mathbb{Z}[x]$ such that $f_n(q)$ equals the number of conjugacy classes in $U_n(q)$, that is, $k(U_n(q))$ is a polynomial expression of q. This conjecture was examined principally by A. Vera-Lopez and J. M. Arregi [28], [29], [30]. They managed to find such polynomials for $n \leq 13$. The problem was also studied by J. Thompson [27]. Our purpose is to examine a similar question about the so-called partition subgroups of $U_n(q)$ defined by A. J. Weir [32]. In the following let $B_n = \{E_{ij} \mid 1 \leq i < j \leq n\}$ denote the standard basis of the vector space of $n \times n$ strictly upper triangular matrices over $\mathbb{F}_q$. Then we have

$$U_n(q) = I_n + \left\{ \sum a_{ij} E_{ij} \mid E_{ij} \in B_n,\, a_{ij} \in \mathbb{F}_q \right\}.$$

In the following we consider subsets $X \subseteq B_n$ having the property that if $E_{ij}, E_{jk} \in X$, then $E_{ik} \in X$, as well. In other words, $X \cup \{0\}$ is a subsemigroup of $B_n \cup \{0\}$. Throughout this chapter, such subsets will be denoted by $X \leq B_n$. The *partition subgroup* over the

field $\mathbb{F}_q$ corresponding to $X \leq B_n$ is defined as

$$H_X(q) = I_n + \left\{ \sum a_{ij} E_{ij} \mid E_{ij} \in X,\ a_{ij} \in \mathbb{F}_q \right\}.$$

For example, the normal partition subgroups of $U_n(q)$ are easy to describe: $H_X(q)$ is a normal partition subgroup of $U_n(q)$ if and only if $\{E_{uv} \mid u \leq i,\ v \geq j\} \subseteq X$ for all $E_{ij} \in X$. In particular, the property that $H_X(q) \lhd U_n(q)$ depends only on X.

In a joint work with Péter Pál Pálfy [11] we examined a generalisation of Higman's conjecture to partition subgroups of nilpotency class two, that is, to subgroups of the form $H_X(q)$ such that $X^3 = 0$. The material of this chapter contains our results in this subject.

On the one hand, we prove that if $H_X(q)$ is a normal subgroup of $U_n(q)$, then $k(H_X(q))$ is really a polynomial expression of q (Theorem 4.7).

On the other hand, which we find more interesting, there are partition subgroups of nilpotency class two for which this statement does not hold. In fact, we discuss a more general question. In the following, if $S \subseteq \mathbb{N}$ and $g : S \to \mathbb{N}$ is a function then we say that g can be described by finitely many polynomials if there exists a finite set of polynomials $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$ such that for any $s \in S$ there is an $1 \leq i \leq k$ depending on s such that $g(s) = f_i(s)$. It was asked by B. Szegedy that even if $q \to k(H_X(q))$ cannot be expressed by a single polynomial, maybe it can be described by a finite set of polynomials. Of course, this question is also sensible if we do not require the existence of such a set of polynomials to all prime powers but to any infinite subset of the set of prime powers. We show that this generalised question is strongly connected to a similar question about the number of matrices over finite fields with fixed submatrix rank function (Theorem 4.8), and confirm the existence of an $X \leq B_n$ (for some big n) such that $k(H_X(q))$ cannot be described by a finite set of polynomials (Theorem 4.9).

4.1 Number of matrices over finite fields having submatrices with specified rank

Let $M_{k\times m}(q)$ denote the set of all $k \times m$ matrices over the finite field $\mathbb{F}_q$. Let

$$\Omega_{k,m} = \{(S,T) \mid S \subseteq \{1,2,\ldots,k\} \text{ and } T \subseteq \{1,2,\ldots,m\}\}.$$

For a matrix $M \in M_{k\times m}(q)$ and $(S,T) \in \Omega_{k,m}$ we denote by $M_{S,T}$ the submatrix of M corresponding to the rows from S and to the columns from T. Finally, if $D_r \subseteq \Omega_{k,m}$ and $r : D_r \to \mathbb{N}$ is a function, let

$$\mathcal{M}_r(q) = \{M \in M_{k\times m}(q) \mid \rho(M_{S,T}) = r(S,T) \text{ for all } (S,T) \in D_r\},$$

where $\rho(M_{S,T})$ denotes the rank of $M_{S,T}$. In the following, we say that r is a submatrix rank function, or just a rank function, and $\mathcal{M}_r(q)$ is the set of matrices over the field $\mathbb{F}_q$ with specified rank function r. We note that in our terminology S or T maybe the empty set. In this case the rank of $M_{S,T}$ (which is in fact an empty matrix) is defined as zero.

In this section we examine the question that for a fixed rank function r whether $|\mathcal{M}_r(q)|$ can be described by finitely many polynomials. The following theorem says that if we assume some additional condition on the domain of r then $|\mathcal{M}_r(q)|$ can be described by a single polynomial.

Theorem 4.1. *Let $\Omega_{k,m}$ and r be as defined above. Let $\Omega'_{k,m} \subseteq \Omega_{k,m}$ denote the set*

$$\{(S_i,T_j) \mid S_i = \{1,2,\ldots,i\},\ T_j = \{j,j+1,\ldots,m\},\ 1 \le i \le k,\ 1 \le j \le m\}.$$

Assuming that $D_r \subseteq \Omega'_{k,m}$ there exists a polynomial $p_r(x) \in \mathbb{Z}[x]$ such that $|\mathcal{M}_r(q)| = p_r(q)$ for all prime powers q.

Proof. In case of $D_r \neq \Omega'_{k,m}$ let $\mathcal{F}_r$ be the set of all extensions $r' : \Omega'_{k,m} \to \mathbb{N}$ of r to $\Omega'_{k,m}$. Clearly $|\mathcal{M}_r(q)| = \sum_{r' \in \mathcal{F}_r} |\mathcal{M}_{r'}(q)|$. So it is enough to prove the statement for the elements of $\mathcal{F}_r$. Therefore, in the following we can assume that $D_r = \Omega'_{k,m}$.

In case of $r(S_1, T_1) = 0$ the first row of every element of $M_r(q)$ contains only 0-s, so $|\mathcal{M}_r(q)| = |\mathcal{M}_{r'}(q)|$ for an $r' : \Omega'_{k-1,m} \to \mathbb{N}$ and we can use induction on k. Otherwise, let l be the largest number such that $r(S_1, T_l) \neq 0$. The key observation is that because of our assumption to D_r the set $\mathcal{M}_r(q)$ is closed under the following operations:

1. Multiplication of the l-th column by a non-zero element of $\mathbb{F}_q$.

2. Adding a multiple of the first row to the i-th row for $1 < i \leq k$.

3. Adding a multiple of the l-th column to the j-th column for $1 \leq j < l$.

These operations define an equivalence relation on the set $\mathcal{M}_r(q)$. On the one hand, it is easy to see that each equivalence class consists of exactly $(q-1)q^{k+l-2}$ matrices. On the other hand, each equivalence class contains exactly one element $M = (M_{ij})$ such that $M_{1l} = 1$ and $M_{1j} = M_{il} = 0$ if $j \neq l$ and $i \neq 1$. Omitting the first row and the l-th column we get a bijection from this set of representatives to the set $\mathcal{M}_{r'}(q)$ for a suitable rank function $r' : \Omega'_{k-1,l-1} \to \mathbb{N}$. Hence $|\mathcal{M}_r(q)| = (q-1)q^{k+l-2}|\mathcal{M}_{r'}(q)|$ and the result follows by induction on k. □

The following example shows that in general $|\mathcal{M}_r(q)|$ cannot be described by finitely many polynomials .

Example 4.2. *There is a $D_r \subseteq \Omega_{6,6}$ and a rank function $r : D_r \to \mathbb{N}$ such that $|\mathcal{M}_r(q)| = (q-1)^{11} \cdot (\#E(q) - 1)$, where $\#E(q)$ denotes the number of points of the elliptic curve $y^2 = x^3 - 1$ over the q-element field (including the extra point out at infinity, which we do not take into account). Consequently, $|\mathcal{M}_r(q)|$ cannot be described by finitely many polynomials.*

Proof. Fixing the rank of every 1×1 submatrix in the first row and in the first column to be 1, we can achieve that the first row and the first column of any element of $\mathcal{M}_r(q)$ do not contain any zeros. Multiplication of a row or a column by a non-zero element of $\mathbb{F}_q$ does not change the rank of any submatrix of a matrix, so these operations define an equivalence relation on the set $\mathcal{M}_r(q)$. Clearly, each equivalence class contains $(q-1)^{11}$ elements, and each equivalence class contains exactly one matrix having only 1-s in the first row and in the first column. Let M be such a matrix and let $x = M_{3,2}$, $y = M_{4,2}$. Next, specifying the rank of a number of submatrices of M, we can achieve that M must be of the form

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & x & x & x^2 & x^2 \\ 1 & x & x & x^2 & x^2 & x^3 \\ 1 & y & 1 & 1 & 0 & 1 \\ 1 & y & y & 0 & 1 & 1 \\ 1 & y^2 & y & 1 & y^2 & x^3 \end{pmatrix}.$$

Finally, if we specify the rank of the 3×3 submatrix in the right lower corner as 2, then we get $x^3 - y^2 - 1 = 0$. It follows that $|\mathcal{M}_r(q)| = (q-1)^{11} \cdot (\#E(q) - 1)$.

It remains to prove that $|\mathcal{M}_r(q)|$ (or, equivalently, $\#E(q)$) cannot be described by finitely many polynomials. Fixing a prime p, there is the following formula for the number of points over the p^n-element field ([24, top of p. 136]).

$$\#E(p^n) = 1 - \alpha^n - \beta^n + p^n,$$

where $\alpha, \beta \in \mathbb{C}$ are complex conjugates of absolut value $\sqrt{p}$ such that α and β do not depend on n. If the trigonometric form of α is $\alpha = \sqrt{p}(\cos(t) + i\sin(t))$, then $\#E(p^n) = 1 - \sqrt{p}^n 2\cos(nt) + p^n$. Choosing a small $\varepsilon > 0$, there are infinitely many n such that $\cos(nt) > \varepsilon$. Hence we get infinitely many prime powers such that $2\varepsilon\sqrt{p}^n < |\#E(p^n) - 1 - p^n| \leq 2\sqrt{p}^n$. It follows that $\#E(p^n)$ cannot be described by finitely many polynomials even for this set of prime powers. $\square$

Remark. The previous example can be generalized as follows. Taking any finite set of polynomials in n variables over $\mathbb{Z}$, there are some (big) $k, l \in \mathbb{N}$, a $D_r \subseteq \Omega_{k,l}$ and a rank function $r : D_r \to \mathbb{N}$ such that $|\mathcal{M}_r(q)|$ equals to the number of common roots of these polynomials over $\mathbb{F}_q$ multiplied by $(q-1)^{k+l-1}$.

4.2 Number of conjugacy classes in partition subgroups of nilpotency class two

If $H_X(q)$ is a partition subgroup of nilpotency class two, then $H_X(q) = 1 + L_X(q)$, where $L_X(q)$ is a Lie algebra of nilpotency class two. Clearly, the number of commuting pairs in $H_X(q)$ is the same as it is in $L_X(q)$, and the number of conjugacy classes of $H_X(q)$ is closely related to this number. Therefore, we first prove a general formula to the number of commuting pairs in a Lie algebra of nilpotency class two.

Let L be a finite Lie algebra of nilpotency class two over the field $\mathbb{F}_q$. Let $[L, L] \leq W \leq Z(L)$ and $V = L/W$ of dimensions $\dim_{\mathbb{F}_q} V = n$, and $\dim_{\mathbb{F}_q} W = k$. The Lie bracket gives a symplectic bilinear map from V into W. By fixing bases $e_1, e_2, \ldots, e_n \in V$ and $f_1, f_2, \ldots, f_k \in W$ this bilinear map is defined by matrices $A_1, A_2, \ldots, A_k \in M_n(q)$ as

$$[e_i, e_j] = \sum_{s=1}^{k} A_s(i,j) f_s.$$

In the following let $n_t(L) = n_t(L, W) = n_t(A_1, A_2, \ldots, A_k)$ denote the number of linear combinations of the matrices $A_1, A_2, \ldots, A_k$ having rank t. It is easy to see that these numbers depend only on L and on the choice of W but they do not depend how the bases $e_1, e_2, \ldots, e_n$ and $f_1, f_2, \ldots, f_k$ were chosen. The next theorem says that the number of commutating pairs in L can be calculated by knowing the numbers $n_t(L)$.

Theorem 4.3. *Using the notation as above, for the number of commutating pairs in L we have*

$$|\{(x,y) \mid x,y \in L,\ [x,y]=0\}| = |L| \sum_{t=0}^{n} q^{n-t} \cdot n_t(L).$$

Proof. For an $x = \sum x_i e_i = (x_1, x_2, \ldots, x_n)^T \in V$ let M_x denote the matrix

$$M_x = \begin{pmatrix} x^T A_1 \\ x^T A_2 \\ \vdots \\ x^T A_k \end{pmatrix}$$

Clearly $[x,y]=0$ if and only if $M_x y = 0$, so we get

$$\begin{aligned}
|\{(x,y) \mid x,y \in L,\ [x,y]=0\}| &= q^{2k} |\{(x,y) \mid x,y \in V,\ [x,y]=0\}| \\
&= q^{2k} \sum_{x \in V} q^{n-\rho(M_x)} = q^{k+n} \sum_{x \in V} q^{k-\rho(M_x)} \\
= |L| \sum_{x \in V} |\{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{F}_q^k \mid \alpha_1 x^T A_1 + \alpha_2 x^T A_2 + \cdots + \alpha_k x^T A_k = 0\}| \\
&= |L| \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k) \in \mathbb{F}_q^k} |\{x \in V \mid x^T(\alpha_1 A_1 + \alpha_2 A_2 + \cdots + \alpha_k A_k) = 0\}| \\
&= |L| \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k) \in \mathbb{F}_q^k} q^{n-\rho(\alpha_1 A_1 + \alpha_2 A_2 + \cdots + \alpha_k A_k)} \\
&= |L| \sum_{t=0}^{n} n_t(A_1, A_2, \ldots, A_k) \cdot q^{n-t} = |L| \sum_{t=0}^{n} q^{n-t} \cdot n_t(L).
\end{aligned}$$

□

In the following let $X \leq B_n$ and let us assume that $X^3 = 0$, that is, $H_X(q)$ has nilpotency class two. The following lemma says that $H_X(q)$ can be converted to a more special form.

Lemma 4.4. *If $X \leq B_n$ such that $X^3 = 0$, then there is a permutation matrix P such that $PH_X(q)P^{-1} = H_{X'}(q)$, where $H_{X'}(q)$ has the form*

$$H_{X'}(q) = \begin{pmatrix} I_k & L_{X_1}(q) & L_{X_3}(q) \\ & I_l & L_{X_2}(q) \\ & & I_m \end{pmatrix}. \tag{4.1}$$

for some $k, l, m \in \mathbb{N}$ and $X' = X_1 \cup X_2 \cup X_3 \subseteq B_n$. (Here $L_{X_i}(q)$ simpy means the subspace generated by the set X_i.)

Proof. We define a directed graph corresponding to X. Let $\{1, 2, \ldots, n\}$ be the set of vertices of V and let (i, j) be a directed edge in this graph if and only if $E_{ij} \in X$. Now, $X^3 = 0$ means that the length of every directed path in this graph is at most 2. It follows that there is a partition $V_1 \cup V_2 \cup V_3 = \{1, 2, \ldots, n\}$ such that there is no edge in this graph from V_s to $V_{s'}$ if $s \geq s'$. Let σ be a permutation of $\{1, 2, \ldots, n\}$ such that

$$\begin{aligned} \sigma(i) &\in V_1 \quad \text{for} \quad 1 \leq i \leq |V_1|, \\ \sigma(i) &\in V_2 \quad \text{for} \quad |V_1| < i \leq |V_1 + V_2|, \\ \sigma(i) &\in V_3 \quad \text{for} \quad |V_1 + V_2| < i \leq n, \end{aligned}$$

and let P be the permutation matrix corresponding to σ. Choosing $X' = P^{-1}XP$ we get that $H_{X'}(q)$ has the form (4.1). □

Using this lemma, in the following we always assume that $H_X(q)$ is already of the form (4.1). For further investigations, it will be useful to introduce a notation to some special partition groups. For some $k, l, m \in \mathbb{N}$ with $k + l + m = n$, let the partition subgroup $U_{k,l,m}(q) \leq U_n(q)$ be defined as

$$U_{k,l,m}(q) = \begin{pmatrix} I_k & M_{k\times l}(q) & M_{k\times m}(q) \\ & I_l & M_{l\times m}(q) \\ & & I_m \end{pmatrix},$$

and let $B_{k,l,m}$ be the corresponding standard basis, so $U_{k,l,m}(q) = H_{B_{k,l,m}}(q)$. In other words, these subgroups are the maximal partition subgroups of the form (4.1), and our goal is to examine the number of conjugacy classes in partition subgroups of these groups.

If k, l, m have already been fixed and $X \leq B_{k,l,m}$, then

$$H_X(q) = I_n + L_X(q) = I_n + L_{X_1}(q) + L_{X_2}(q) + L_{X_3}(q),$$
$$U_{k,l,m}(q) = I_n + L_{B_{k,l,m}}(q) = I_n + L_{Y_1}(q) + L_{Y_2}(q) + L_{Y_3}(q),$$

where $L_X(q)$, $L_{X_i}(q)$, $L_{B_{k,l,m}}(q)$ and $L_{Y_i}(q)$ denote the subspaces generated by the sets X, X_i, $B_{k,l,m}$ and Y_i, respectively. Furthermore,

$$\begin{aligned} X_1 \subseteq Y_1 &= \{f_{ij} = E_{i,j+k} \mid 1 \leq i \leq k,\ 1 \leq j \leq l\}, \\ X_2 \subseteq Y_2 &= \{g_{ij} = E_{i+k,j+k+l} \mid 1 \leq i \leq l,\ 1 \leq j \leq m\}, \\ X_3 \subseteq Y_3 &= \{h_{ij} = E_{i,j+k+l} \mid 1 \leq i \leq k,\ 1 \leq j \leq m\}. \end{aligned} \tag{4.2}$$

Here $L_X(q)$ is a nilpotent Lie algebra of nilpotency class two with the usual Lie bracket $[x, y] = xy - yx$. Clearly $(1 + x)(1 + y) = (1 + y)(1 + x)$ if and only if $[x, y] = 0$. It is also clear that $X_1 \cdot X_2 \subseteq X_3$ and any other product is zero in X, so $[L_X(q), L_X(q)] \leq L_{X_3}(q) \leq Z(L_X(q))$. Therefore, using Theorem 4.3 to $W = L_{X_3}(q)$ and $V = L_X(q)/L_{X_3}(q)$, for the number of conjugacy classes of $H_X(q)$ we get:

$$\begin{aligned} k(H_X(q)) &= \frac{|\{(g, h) \mid g, h \in H_X(q),\ gh = hg\}|}{|H_X(q)|} \\ &= \frac{|\{(x, y) \mid x, y \in L_X(q),\ [x, y] = 0\}|}{|L_X(q)|} = \sum_{t=0}^{|X_1 \cup X_2|} q^{|X_1 \cup X_2| - t} \cdot n_t(L_X(q)). \end{aligned} \tag{4.3}$$

We will use the notation defined in Section 4.1. The following theorem says that the calculation of $n_t(L_X(q))$ leads us to the determination of some $|\mathcal{M}_r(q)|$'s. Before the theorem we set up some terminology.

If $s_1, s_2, \ldots, s_l$ are not necessarily different elements of the set H, then we say that $\mathcal{S} = (s_1, s_2, \ldots, s_l)$ is an (ordered) list of elements from H. Such a list will be denoted by $\mathcal{S} \subseteq_l H$. For an $\mathcal{S} \subseteq_l \Omega_{k,m}$ let $\mathcal{F}_{\mathcal{S}}^{\Sigma=t}$ denote the set of rank functions

$$\mathcal{F}_{\mathcal{S}}^{\Sigma=t} = \{r : \mathcal{S} \to \mathbb{N} \mid \textstyle\sum_{s \in \mathcal{S}} r(s) = t.\}$$

Theorem 4.5. *Let $X = X_1 \cup X_2 \cup X_3 \leq B_{k,l,m}$ for some $k, l, m \in \mathbb{N}$. Then there exists a list $\mathcal{S} = \{(S_i, T_i) \mid 1 \leq i \leq l\} \subseteq \Omega_{k,m}$ such that for every $0 \leq t \leq \frac{|X_1 \cup X_2|}{2}$ we have*

$$n_{2t+1}(L_X(q)) = 0, \qquad n_{2t}(L_X(q)) = \frac{1}{q^{km-|X_3|}} \sum_{r \in F_{\mathcal{S}}^{\sum=t}} |\mathcal{M}_r(q)|. \tag{4.4}$$

Conversely, for any list $\mathcal{S} = \{(S_i, T_i) \mid 1 \leq i \leq l\} \subseteq_l \Omega_{k,m}$ one can define an $X = X_1 \cup X_2 \cup X_3 \leq B_{k,l,m}$ such that Equation (4.4) holds.

Proof. Let $B_{k,l,m} = Y_1 \cup Y_2 \cup Y_3$ as it was defined by equations (4.2), so $U_{k+l+m}(q) = I_n + L_{Y_1}(q) + L_{Y_2}(q) + L_{Y_3}(q)$. It is clear that $L_{Y_3}(q) = [L_Y(q), L_Y(q)] = Z(L_Y(q))$. We define the following subsets of Y_1 and Y_2.

$$Y_1^{j,c} = \{f_{1j}, f_{2j}, \ldots, f_{kj}\}, \quad \text{for } 1 \leq j \leq l, \qquad \text{and}$$
$$Y_2^{i,r} = \{g_{i1}, g_{i2}, \ldots, g_{im}\}, \quad \text{for } 1 \leq i \leq l.$$

(In this notation "c" and "r" refer to the words "column" and "row".)

Now, $L_{Y_1 \cup Y_2}(q) \simeq L_Y(q)/L_{Y_3}(q)$ has basis

$$B = Y_1^{1,c} \cup Y_1^{2,c} \cup \ldots \cup Y_1^{l,c} \cup Y_2^{1,r} \cup Y_2^{2,r} \cup \ldots \cup Y_2^{l,r}.$$

Corresponding to this basis the Lie bracket is determined by the set of square matrices $\{A_{ij} \in M_{kl+lm}(q) \mid 1 \leq i \leq k,\ 1 \leq j \leq m\}$. Furthermore, each A_{ij} is of the form

$$A_{ij} = \begin{pmatrix} 0 & I_l \otimes E_{ij} \\ -(I_l \otimes E_{ij})^T & 0 \end{pmatrix},$$

where E_{ij} is an element of the standard basis of $M_{k \times m}(q)$ and $I_l \otimes E_{ij}$ denotes the usual Kronecker product of the matrices I_l and E_{ij}. Let $Z = (z_{ij}) \in M_{k \times m}(q)$. We get

$$M(Z) = \sum_{1 \leq i \leq k} \sum_{1 \leq j \leq m} z_{ij} A_{ij} = \begin{pmatrix} 0 & I_l \otimes Z \\ -(I_l \otimes Z)^T & 0 \end{pmatrix}.$$

The set of basis vectors $X_1 \cup X_2 \subseteq B$ determines an antisymmetric submatrix of $M(Z)$. This submatrix has the form

$$M_X(Z) = \begin{pmatrix} 0 & A(Z) \\ -A(Z)^T & 0 \end{pmatrix}, \quad \text{where} \quad A(Z) = \begin{pmatrix} Z_1 & & & \\ & Z_2 & & \\ & & \ddots & \\ & & & Z_l \end{pmatrix}.$$

In the above matrix $Z_1, Z_2, \ldots, Z_l$ are not necessarily different submatrices of Z.

For each A_{ij}, let $A_{ij,X}$ be the submatrix of A_{ij} determined by $X_1 \cup X_2$. The Lie bracket is defined by the set of matrices $\{A_{ij,X} \mid h_{ij} \in X_3\}$. If $Z = (z_{ij})$ and $Z' = (z'_{ij})$ are two elements of $M_{k\times m}(q)$, then $\sum z_{ij}A_{ij,X}$ and $\sum z'_{ij}A_{ij,X}$ define the same linear combination of the elements of $\{A_{ij,X} \mid h_{ij} \in X_3\}$ if and only if $z_{ij} = z'_{ij}$ for all $h_{ij} \in X_3$. Using the definition of $n_t(L_X(q))$ we get

$$n_t(L_X(q)) = \frac{1}{q^{km-|X_3|}} \left|\{Z \in M_{k\times m}(q) \mid \rho(M_X(Z)) = t\}\right|.$$

It is clear that

$$\rho(M_X(Z)) = \rho(A(Z)) + \rho(-A(Z)^T) = 2\rho(A(Z)) = 2(\rho(Z_1) + \rho(Z_2) + \ldots + \rho(Z_l)),$$

which is always even, so $n_t(L_X(q)) = 0$ if t is odd. Let $(S_i, T_i) \in \Omega_{k,m}$ be the element of $\Omega_{k,m}$ corresponding to Z_i. Choosing $\mathcal{S} = \{(S_i, T_i) \mid 1 \le i \le l\}$ we get

$$\begin{aligned} n_{2t}(L_X(q)) &= \frac{1}{q^{km-|X_3|}} |\{Z \in M_{k\times m}(q) \mid \rho(Z_1) + \rho(Z_2) + \ldots + \rho(Z_l) = t\}| \\ &= \frac{1}{q^{km-|X_3|}} \sum_{r_1+r_2+\ldots+r_l=t} |\{Z \in M_{k\times m}(q) \mid \rho(Z_1) = r_1,\ \rho(Z_2) = r_2,\ \ldots,\ \rho(Z_l) = r_l\}| \\ &= \frac{1}{q^{km-|X_3|}} \sum_{r \in F_{\mathcal{S}}^{\sum=t}} |\{Z \in M_{k\times m}(q) \mid \rho(Z_{S_i,T_i}) = r(S_i, T_i),\ 1 \le i \le l\}| \\ &= \frac{1}{q^{km-|X_3|}} \sum_{r \in F_{\mathcal{S}}^{\sum=t}} |\mathcal{M}_r(q)|. \end{aligned}$$

So the first part of the theorem is proved.

For any list $\mathcal{S} = \{(S_i, T_i) \mid 1 \leq i \leq l\} \subseteq_l \Omega_{k,m}$ we define the sets $X_1 \subseteq Y_1,\ X_2 \subseteq Y_2$ as follows

$$X_1 = \{E_{i,j+k} \mid 1 \leq i \leq k,\ 1 \leq j \leq l,\ i \in S_j\},$$
$$X_2 = \{E_{i+k,j+k+l} \mid 1 \leq i \leq l,\ 1 \leq j \leq m,\ j \in T_i\}.$$

Furthermore, let $X_3 \leq Y_3$ be an arbitrary set containing $X_1 \cdot X_2$. Let $X = X_1 \cup X_2 \cup X_3$. Applying the first part of the proof to $H_X(q) \leq U_{k,l,m}(q)$ we get exactly $\mathcal{S}$, which proves the second part of the theorem. □

Lemma 4.6. *Let $s(x), t(x) \in \mathbb{Z}[x]$ be two polynomials such that the leading coefficient of $t(x)$ is ± 1 and let $r(x) = \frac{s(x)}{t(x)} \in \mathbb{Z}(x)$. If $r(q) \in \mathbb{Z}$ for infinitely many $q \in \mathbb{N}$, then $r(x) \in \mathbb{Z}[x]$.*

Proof. One can use the Euclidean algorithm to get the form $r(x) = r_0(x) + \frac{s_0(x)}{t(x)}$, where $r_0(x), s_0(x) \in \mathbb{Z}[x],\ \deg s_0(x) < \deg t(x)$. It follows that $\frac{s_0(q)}{t(q)} \in \mathbb{Z}$ for infinitely many $q \in \mathbb{N}$. On the other hand $\lim_{q\to\infty} \frac{s_0(q)}{t(q)} = 0$, which shows that $s_0(x) = 0$. □

Now we are ready to state and to prove our theorems mentioned at the beginning of this chapter.

Theorem 4.7. *Let $X \leq B_n$ such that $H_X(q) \leq U_n(q)$ is a normal partition subgroup of $U_n(q)$ of nilpotency class two. Then there exists a polynomial $f_X(x) \in \mathbb{Z}[x]$ such that $k(H_X(q)) = f_X(q)$ for all prime powers q.*

Proof. As we mentioned above, the assumption that $H_X(q)$ is a normal subgroup of $U_n(q)$ is equivalent to the assumption that X has the following property:

$$\text{If } E_{ij} \in X, \text{ then } E_{uv} \in X, \text{ for all } u \leq i,\ v \geq j.$$

On the other hand, $X^3 = 0$ because $H_X(q)$ has nilpotency class two. Using these two properties of X it is easy to see that $H_X(q)$ already is of the form (4.1). So, we do not need to conjugate by any permutation matrix P to reach this figure. It follows that X_1 and X_2 have the following properties:

$$\text{If } f_{ij} \in X_1, \text{ then } f_{uj} \in X_1 \text{ for all } 1 \leq u \leq i,$$
$$\text{If } g_{ij} \in X_2, \text{ then } g_{iv} \in X_2 \text{ for all } j \leq v \leq m.$$

It follows directly that the set $\mathcal{S}$ constructed in Theorem 4.5 is a subset of $\Omega'_{k,m}$ defined in Theorem 4.1. Using this latter theorem we get that for any rank function $r : \mathcal{S} \to \mathbb{N}$ there exists a polynomial $p_r(x) \in \mathbb{Z}[x]$ such that $|\mathcal{M}_r(q)| = p_r(q)$. Using Theorem 4.5 and Lemma 4.6, we get $n_t(L_X(q))$ is a sum of such polynomials for each $0 \leq t \leq |X_1 \cup X_2|$, so it is also a polynomial expression of q with integer coefficients. Therefore, the result follows from Equation (4.3). □

In the following theorem we require a single polynomial but we allow ourselves to take some restriction to q.

Theorem 4.8. *Let k, m be natural numbers and let π be any infinite subset of prime powers. Then the following two statements are equivalent.*

1. *For every $l \in \mathbb{N}$ and and for every $X \leq B_{k,l,m}$ there exists a polynomial $f_X(x) \in \mathbb{Z}[x]$ such that $k(H_X(q)) = f_X(q)$ for all $q \in \pi$.*

2. *For every $D_r \subseteq \Omega_{k,m}$ and for every rank function $r : D_r \to \mathbb{N}$ there exists a polynomial $f_r(x) \in \mathbb{Z}[x]$ such that $|\mathcal{M}_r(q)| = f_r(q)$ for all $q \in \pi$.*

Proof. To prove direction *2→1* let $X \leq B_{k,l,m}$. Applying the equations (4.3) and (4.4) we get $k(H_X(q)) = \sum q^{s(r)} |\mathcal{M}_r(q)|$ for a set of rank functions $r : D_r \to \mathbb{N}$, where D_r is defined by X and the value of $s(r)$ depends only on r and on X. (Of course, $\mathcal{M}_r(q) = \emptyset$

for all but a finite number of rank functions.) If *2* holds, then for every rank function $r : D_r \to \mathbb{N}$ we have a polynomial $f_r(x) \in \mathbb{Z}[x]$ such that $|\mathcal{M}_r(q)| = f_r(q)$ for all $q \in \pi$. Let $f_X(x)$ be defined as $f_X(x) = \sum x^{s(r)} f_r(x) \in \mathbb{Z}[x]$. Then $k(H_X(q)) = f_X(q)$ for all $q \in \pi$, which proves this direction.

Now, we prove *1*→*2*. Starting from the assumption that *2* does not hold, we prove the existence of an $X \leq B_{k,l,m}$ for some l such that *1* does not hold to $H_X(q)$. Let $r_0 : D_{r_0} \to \mathbb{N}$ be a rank function such that $|\mathcal{M}_{r_0}(q)|$ is not a polynomial expression for $q \in \pi$. Let $D_{r_0} = \{(S_i, T_i) \mid 1 \leq i \leq l_0\} \subseteq \Omega_{k,m}$ be its domain.

First, we construct $l', t' \in \mathbb{N}$ and $X' \leq B_{k,l',m}$ such that the expression $n_{2t'}(L_{X'}(q))$ appearing in formulas (4.3) and (4.4) is not a polynomial expression of $q \in \pi$. Choose $z = \min(k, m) + 1$. Starting from D_{r_0} we define a list $\mathcal{S}' \subseteq_l \Omega_{k,m}$ in such a way that $\mathcal{S}'$ and D_{r_0} have the same elements, but for every $1 \leq i \leq l_0$ the element (S_i, T_i) occurs in $\mathcal{S}'$ exactly z^{i-1} times. Hence $|\mathcal{S}'| = 1 + z + z^2 + \ldots + z^{l_0-1} =: l'$. Using the second part of Theorem 4.5 we can define a subset $X' = X'_1 \cup X'_2 \cup X'_3 \leq B_{k,l',m}$ corresponding to the list $\mathcal{S}'$. We claim that $q^{km-|X'_3|} \cdot n_{2t'}(L_{X'}(q)) = |\mathcal{M}_{r_0}(q)|$ for $t' = \sum_{i=1}^{l_0} r_0(S_i, T_i) z^{i-1}$.

To prove this, let $r \in \mathcal{F}_{\mathcal{S}'}^{\sum = t'} \setminus \{r_0\}$ such that $\mathcal{M}_r(q)$ is not empty for at least one $q \in \pi$. Then, by the choice of z, we get $r(S_i, T_i) < z$ for all $1 \leq i \leq l_0$. For the same reason, $r(S_i, T_i) < z$ for all $1 \leq i \leq l_0$. It follows that

$$t' = \sum_{i=1}^{l_0} r(S_i, T_i) z^{i-1} = \sum_{i=1}^{l_0} r_0(S_i, T_i) z^{i-1}.$$

Clearly every natural number can be uniquely represented by powers of z with natural coefficients less than z. Hence $r(S_i, T_i) = r_0(S_i, T_i)$ for all $1 \leq i \leq l_0$, that is, $r = r_0$. Using Theorem 4.5 we get

$$q^{km-|X'_3|} \cdot n_{2t'}(L_{X'}(q)) = \sum_{r \in \mathcal{F}_{\mathcal{S}'}^{\sum = t'}} |\mathcal{M}_r(q)| = |\mathcal{M}_{r_0}(q)|.$$

So $n_{2t'}(L_{X'}(q))$ is not a polynomial expression of $q \in \pi$.

In the following we denote by $i\mathcal{S}' \subseteq_l \Omega_{k,m}$ the list which has the same elements as S', but the multiplicity of any element in $i\mathcal{S}'$ is i times as much as it is in $\mathcal{S}'$. Let $iX' \subseteq B_{k,il',m}$ be the corresponding subset of $i\mathcal{S}'$. Furthermore, let $d = |X'_1 \cup X'_2|$. We claim that there exists an $i \leq d+1$ such that $k(H_{iX'}(q))$ is not a polynomial expression of $q \in \pi$.

It is easy to see that $|iX'_1 \cup iX'_2| = i \cdot d$ and $n_{it}(L_{iX'}(q)) = n_t(L_{X'}(q))$ for each $i, t \in \mathbb{N}$. Furthermore, $n_t(L_{iX'}(q)) = 0$ if i does not divide t. Using Equation (4.3) for $X', 2X', \ldots, (d+1)X'$ we get

$$k(H_{iX'}(q)) = \sum_{t=0}^{d} q^{i(d-t)} \cdot n_t(L_{X'}(q)) \quad \text{for all } 1 \leq i \leq d+1.$$

This system of linear equations has the form

$$\begin{bmatrix} k(H_{X'}(q)) \\ k(H_{2X'}(q)) \\ k(H_{3X'}(q)) \\ \vdots \\ k(H_{(d+1)X'}(q)) \end{bmatrix} = \begin{bmatrix} q^d & q^{d-1} & \cdots & 1 \\ q^{2d} & q^{2(d-1)} & \cdots & 1 \\ q^{3d} & q^{3(d-1)} & \cdots & 1 \\ \vdots & \vdots & \ddots & 1 \\ q^{(d+1)d} & q^{(d+1)(d-1)} & \cdots & 1 \end{bmatrix} \begin{bmatrix} n_0(L_{X'}(q)) \\ n_1(L_{X'}(q)) \\ n_2(L_{X'}(q)) \\ \vdots \\ n_d(L_{X'}(q)) \end{bmatrix}$$

The matrix appearing in the right-hand side of this system of equations is a Vandermonde-matrix, so its determinant is a polynomial of q with leading coefficient ± 1 and this polynomial is non-zero for all prime power q. Using the Cramer rule it follows that if $k(H_{iX'}(q))$ is a polynomial of $q \in \pi$ for each $i \leq d+1$, then each $n_t(L_{X'}(q))$ is a rational function of $q \in \pi$. However, $n_t(L_{X'}(q))$ is an integer for every $q \in \pi$, so using Lemma 4.6 we get $n_t(L_{X'}(q))$ is a polynomial of $q \in \pi$ for all $t \leq d$. But we have already seen that this is not true for $2t' \leq d$, a contradiction. □

Combining this last theorem with our Example 4.2 we get the last result of this chapter, which says that in general $k(H_X(q))$ cannot be described by finitely many polynomials.

Theorem 4.9. *For some $n \in \mathbb{N}$ there is an $X \leq B_n$ such that $X^3 = 0$ and $k(H_X(q))$ cannot be described by a finite set of polynomials.*

Proof. Starting from Example 4.2 we have a $D_r \subseteq \Omega_{6,6}$ and a rank function $r : D_r \to \mathbb{N}$ such that $|\mathcal{M}_r(q)|$ cannot be described by finitely many polynomials. Following the proof of Theorem 4.8 we can define subsets $X' \leq B_{k,l',m},\ 2X' \leq B_{k,2l',m}, \ldots, (d+1)X' \leq B_{k,(d+1)l',m}$. Let us assume that $k(H_{iX'}(q))$ can be described by a finite number of polynomials for each $1 \leq i \leq d+1$. Then for each $1 \leq i \leq d+1$ the corresponding set of polynomials defines an equivalence relation on the set of all prime powers, namely two prime powers q_1 and q_2 are equivalent, if $k(H_{iX'}(q_1))$ and $k(H_{iX'}(q_2))$ can be described by the same polynomial. Taking the intersection of these $d+1$ equivalence relations we get another equivalence relation on the set of prime powers, which still has only finitely many classes. Let π be such an equivalence class. If $|\pi| = \infty$, then $|\mathcal{M}_r(q)|$ is a polynomial expression of q for $q \in \pi$ by the proof of Theorem 4.8. On the other hand, if π has only finitely many elements, then $|\mathcal{M}_r(q)|$ can clearly be described by at most $|\pi|$ many polynomials for $q \in \pi$. (For example, taking constant polynomials.) Hence $|\mathcal{M}_r(q)|$ can be described by a finite number of polynomials, a contradiction. □

Chapter 5

Small bases of solvable linear groups

One basic concept for computing with permutation groups is the notion of a base: For a permutation group $G \leq \mathrm{Sym}\,(\Omega)$ a set $\{\omega_1, \omega_2, \ldots, \omega_n\} \subseteq \Omega$ (or rather an ordered list) is called a base for G if only the identity permutation fixes all elements of this set. There are a number of algorithms for permutation groups related to the concept of base, and these algorithms run faster if the size of the base is small. Hence it is useful to find small bases for permutation groups. Of course, we cannot expect to have one in general, since taking the natural action of S_n, the minimal size of a base is $n-1$. On the other hand, there are a number of results if G is solvable, the action of G is primitive, or $(|G|, |\Omega|) = 1$.

It is easy to see that the size of a base of a permutation group $G \leq \mathrm{Sym}\,(\Omega)$ is at least $\log|G|/\log|\Omega|$. It is a conjecture of L. Pyber [22] that for a primitive permutation group G there is a base of size less than $C\log|G|/\log|\Omega|$ for some universal constant C. For solvable groups, there is a precise result: It was proved by Á. Seress [23] that all primitive solvable permutation group have a base of size at most four. According to the classification in the O'Nan–Scott Theorem, any such group is of affine type. However, in general there is no universal upper bound on the minimal base size of an affine group.

The situation changes if we consider coprime affine groups. For a finite vector space V and $G \leq GL(V)$ the affine group $V \rtimes G$ is said coprime if $(|G|, |V|) = 1$. It turns out that

for coprime affine groups there is an upper bound for the minimal base size: It was proved by D. Gluck and K. Magaard [8] that any such group has a base of size at most 95. As the result of Seress is sharp, the value of 95 can probably be improved.

Maybe the most examined case is when V is a finite vector space, $G \leq GL(V)$ is a solvable linear group and $(|G|, |V|) = 1$. It was asked by I. M. Isaacs [16] whether there always exists a G-orbit in V of size at least $|G|^{1/2}$ for such groups. This follows immediately if we find $x, y \in V$ such that $C_G(x) \cap C_G(y) = 1$, that is, a base of size two for the action of G on V. The existence of such vectors was confirmed by T. R. Wolf [33] in case of supersolvable G. Later, in a joint work with A. Moreto [20] they solved this problem in case when $|G|$ and $|V|$ are both odd. Finally, S. Dolfi [4] proved that it is enough to assume that $|G|$ is odd.

In a joint work with K. Podoski [12] we proved the following theorem, which settles the remaining cases.

Theorem 5.1. *Let V be a finite vector space over a finite field of characteristic $p \neq 2$, and let $G \leq GL(V)$ be a solvable linear group with $(|G|, |V|) = 1$. Then there exist $x, y \in V$ such that $C_G(x) \cap C_G(y) = 1$.*

Remark. The material of this chapter appeared at arXiv in July 2007. Some weeks later we were informed that in the meantime the same result has been proved using different methods by S. Dolfi [5] and also by E. P. Vdovin [31].

If $G \leq GL(V)$ is an imprimitive as a linear group, then there is a proper decomposition $V = V_1 \oplus V_2 \oplus \ldots \oplus V_t$ such that G permutes the subspaces $V_1, V_2, \ldots, V_t$. A main result of the next section is Theorem 5.4, which says that if G is a solvable permutation group acting on Ω and the prime p does not divide the order of $|G|$, then there is a partition Ω into at most p parts such that only the identity element of G fixes every element of this partition. Using this theorem we can reduce Theorem 5.1 to primitive solvable linear groups in Section 5.3. To prove the theorem in the primitive linear case, we use a nice description

of maximal solvable primitive linear groups. This help us to confirm the existence on a normal subgroup $F \leq G$, which has a very clear action on V. Using this subgroup, in Section 5.2 we construct a 2-element base for the action of G on V. We remark that our construction deeply depends on the order of the base field and on the dimension of the vector space, so we distinguish a number of cases throughout the proof.

5.1 Finding regular partitions for solvable permutation groups

In this section let Ω be a finite set and let $G \leq \mathrm{Sym}(\Omega)$ be a solvable permutation group. For a subset $X \subseteq \Omega$ let $G(X)$ denote the set-wise stabilizer of X in G, that is, $G(X) = \{g \in G \mid gx \in X \text{ for all } x \in X\}$. We say that the partition $\{\Omega_1, \Omega_2, \ldots, \Omega_k\}$ of Ω is G-regular if only the identity element of G fixes all elements of this partition, i.e., if $\bigcap_{i=1}^{k} G(\Omega_i) = 1$.

With the additional assumption that G is a p'-group, one goal of this section is to find a G-regular partition of Ω into at most p parts. Such a partition will be used in Section 5.3 to reduce the problem to primitive linear groups. Moreover, our constructions for primitive permutation groups will be used in the investigation of the primitive linear case. Since a primitive solvable permutation group is of affine type, first we construct such partitions for affine groups.

Theorem 5.2. *Let W be an n-dimensional vector space over the q-element field for some prime number q, and let $AGL(W)$ denote the full affine group acting on W. Furthermore, let $G = W \rtimes G_0 \leq AGL(W)$ for some linear group $G_0 \leq GL(W)$. If $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$ is a basis of W, then, depending on n and q, the following partitions are G-regular.*

Case 1: $|W| \leq 3$ or $|W| = 4$ and the order of G is divisible by 3

Take the trivial partition, that is, each element of the partition consists of a single vector.

Case 2: $n = 1,\ q \geq 5$

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Case 3: $n \geq 2,\ q \geq 5$

$$\Omega_1 = \{\underline{0}\},$$
$$\Omega_2 = \{\underline{e}_1, 2\underline{e}_1, \underline{e}_2, \underline{e}_3, \ldots, \underline{e}_n, \underline{e}_1 + \underline{e}_2, \underline{e}_2 + \underline{e}_3, \ldots, \underline{e}_{n-1} + \underline{e}_n\},$$
$$\Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Case 4: $n \geq 2,\ q = 3$

$$\Omega_1 = \{\underline{0}\},\ \Omega_2 = \{\underline{e}_1\},\ \Omega_3 = \{\underline{e}_2, \underline{e}_3, \ldots, \underline{e}_n, \underline{e}_1 + \underline{e}_2, \underline{e}_2 + \underline{e}_3, \ldots, \underline{e}_{n-1} + \underline{e}_n\},$$
$$\Omega_4 = W \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3).$$

Case 5: $n = 3,\ q = 2$

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = \{\underline{e}_2\}, \quad \Omega_4 = \{\underline{e}_3\},$$
$$\Omega_5 = W \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4).$$

Case 6: $n \geq 4,\ q = 2$

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = \{\underline{e}_2\},$$
$$\Omega_4 = \{\underline{e}_3, \ldots, \underline{e}_n, \underline{e}_3 + \underline{e}_4, \underline{e}_4 + \underline{e}_5, \ldots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_3 + \underline{e}_2, \underline{e}_n + \underline{e}_1\},$$
$$\Omega_5 = W \setminus (\Omega_1 \cup \Omega_2 \cup \Omega_3 \cup \Omega_4).$$

Case 7: $n = 2,\ q = 2$, *and the order of* G *is not divisible by* 3

Let $\Omega_1 = \{\underline{0}\}$. *The action of* $G(\Omega_1)$ *on* $W \setminus \Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + e_2\}$ *cannot be transitive, so it has a fixed point in* $W \setminus \Omega_1$, *say,* $\underline{e}_1$. *Then let*

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_2\}, \quad \Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Case 8: $n = 3,\ q = 2$, and the order of G is not divisible by 3

In this case G_0 is a $3'$-subgroup of $GL(W) \simeq PSL(3,2)$. As $PSL(3,2)$ does not contain a subgroup of order 14, it follows that either $|G_0| = 7$ or $|G_0|$ divides 8.

In case of $|G_0| = 7$ let

$$\Omega_1 = \{\underline{0}\}, \quad \Omega_2 = \{\underline{e}_1\}, \quad \Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Otherwise, we can assume that G_0 is contained in the group of upper unitriangular matrices. In this case let

$$\Omega_1 = \{\underline{e}_1, \underline{e}_3, \underline{e}_1 + \underline{e}_3\}, \quad \Omega_2 = \{\underline{e}_2, \underline{e}_2 + \underline{e}_3\}, \quad \Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Case 9: $n \geq 4,\ q = 2$, and the order of G is not divisible by 3

Let $\Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\}$. The action of $G(\Omega_1)$ on Ω_1 cannot be transitive, so it has a fixed point in Ω_1, say, $\underline{e}_1$. Then let

$$\Omega_1 = \{\underline{e}_1, \underline{e}_2, \underline{e}_1 + \underline{e}_2\},$$
$$\Omega_2 = \{\underline{e}_3, \underline{e}_4, \ldots, \underline{e}_n, \underline{e}_3 + \underline{e}_4, \ldots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_3 + \underline{e}_2, \underline{e}_n + \underline{e}_1\},$$
$$\Omega_3 = W \setminus (\Omega_1 \cup \Omega_2).$$

Proof. In any of the above cases we prove that if $g \in G$ fixes every element of the given partition, then it fixes $\underline{0}$ and it also fixes every element of the basis $\{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n\}$. These conditions are specified explicitly in cases *1, 2, 5,* and *7*, so the theorem holds in these cases evidently.

In case *4* we remark that the given partition is G-regular for each prime $q \geq 3$. However, for primes $q \geq 5$ we need a G-regular partition consisiting of at most 3 parts. To prove that the given partition is G-regular, first note that if $g \in G$ fixes every element of the given partition, then $g \in G(\Omega_1) = G_0 \leq GL(W)$ is a linear transformation of W fixing $\underline{e}_1$.

Now, we prove that $g(\underline{e}_k) = \underline{e}_k$ for all $2 \leq k \leq n$ by using induction on k. Assuming that $g(\underline{e}_i) = \underline{e}_i$ for all $1 \leq i < k \leq n$, it follows that $g(\underline{e}_k)$ and $g(\underline{e}_{k-1} + \underline{e}_k)$ are elements of the set

$$\Omega_3 \setminus \langle \underline{e}_1, \ldots, \underline{e}_{k-1} \rangle = \{\underline{e}_k, \underline{e}_{k+1}, \ldots, \underline{e}_n, \underline{e}_{k-1} + \underline{e}_k, \ldots, \underline{e}_{n-1} + \underline{e}_n\}.$$

Since $g(\underline{e}_{k-1} + \underline{e}_k) - g(\underline{e}_k) = \underline{e}_{k-1}$, we have either $g(\underline{e}_k)$ or $g(\underline{e}_{k-1} + \underline{e}_k)$ contains $\underline{e}_{k-1}$ with non-zero coefficient. However, the only such element in $\Omega_3 \setminus \langle \underline{e}_1, \ldots, \underline{e}_{k-1} \rangle$ is $\underline{e}_{k-1} + \underline{e}_k$. So either $g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$ or $g(\underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$. In the latter case $g(\underline{e}_{k-1} + \underline{e}_k) = 2\underline{e}_{k-1} + \underline{e}_k \notin \Omega_3$, since $q \neq 2$, a contradiction. It follows that $g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$, so $g(\underline{e}_k) = g(\underline{e}_{k-1} + \underline{e}_k) - g(\underline{e}_{k-1}) = \underline{e}_k$.

In case *3* let $g \in G(\Omega_1) \cap G(\Omega_2)$. Then $g \in G(\Omega_1) \leq GL(W)$ is a linear transformation of W fixing Ω_2. As $q \geq 5$, there is only one element $x \in \Omega_2$ such that $2x \in \Omega_2$, namely $x = \underline{e}_1$. It follows that g fixes $\underline{0}$ and $\underline{e}_1$, so it also fixes the set $\{\underline{e}_2, \underline{e}_3, \ldots, \underline{e}_n, \underline{e}_1 + \underline{e}_2, \ldots, \underline{e}_{n-1} + \underline{e}_n\}$. We get g fixes every element of the partition given in case *4*, hence $g = 1$.

In case *6* let $g \in G(\Omega_1) \cap G(\Omega_2) \cap G(\Omega_3) \cap G(\Omega_4)$. To prove that $g(\underline{e}_k) = \underline{e}_k$ for all $3 \leq k < n$ we use a similar induction argument as we did in case *4*. Assuming that $g(\underline{e}_i) = \underline{e}_i$ for all $1 \leq i < k < n$ we get $g(\underline{e}_k)$ and $g(\underline{e}_{k-1} + \underline{e}_k)$ are elements of the set

$$\Omega_2 \setminus \langle \underline{e}_1, \ldots, \underline{e}_{k-1} \rangle = \{\underline{e}_k, \underline{e}_{k+1}, \ldots, \underline{e}_n, \underline{e}_{k-1} + \underline{e}_k, \ldots, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_n + \underline{e}_1\}.$$

Since $g(\underline{e}_k) + g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1}$, we have either $g(\underline{e}_{k-1} + \underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$ or $g(\underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$. In the former case we get $g(\underline{e}_k) = \underline{e}_k$, while in the latter case we take $\underline{e}_k + \underline{e}_{k+1} \in \Omega_2$, since $k < n$. Now $\underline{e}_{k-1}$ occurs with 0 coefficient both in $g(\underline{e}_k + \underline{e}_{k+1})$ and $g(\underline{e}_{k+1})$, since the only element of $\Omega_2 \setminus \langle \underline{e}_1, \ldots, \underline{e}_{k-1} \rangle$ containing $\underline{e}_{k-1}$ with nonzero coefficient is $g(\underline{e}_k)$. However, $g(\underline{e}_k + \underline{e}_{k+1}) + g(\underline{e}_{k+1}) = g(\underline{e}_k) = \underline{e}_{k-1} + \underline{e}_k$, a contradiction. It remains to prove that $g(\underline{e}_n) = \underline{e}_n$. It is clear that

$$g(\underline{e}_n) \in \Omega_2 \setminus \langle \underline{e}_1, \underline{e}_2, \ldots, \underline{e}_{n-1} \rangle = \{\underline{e}_n, \underline{e}_{n-1} + \underline{e}_n, \underline{e}_n + \underline{e}_1\}.$$

If $g(\underline{e}_n) = \underline{e}_{n-1} + \underline{e}_n$, then $g(\underline{e}_n + \underline{e}_1) = \underline{e}_{n-1} + \underline{e}_n + \underline{e}_1 \notin \Omega_2$. If $g(\underline{e}_n) = \underline{e}_n + \underline{e}_1$, then

$g(\underline{e}_{n-1}+\underline{e}_n)=\underline{e}_{n-1}+\underline{e}_n+\underline{e}_1\notin\Omega_2$. Thus $g(\underline{e}_n)=\underline{e}_n$ also holds. It follows that $g=1$, so the given partition is G-regular.

In case *8* if $|G_0|=7$, then G_0 acts regularly on the 7-element set $W\setminus\{\underline{0}\}$, so the given partition is clearly G-regular. Otherwise, $\Omega_1\cup\{\underline{0}\}$ is the only 2-dimensional affine subspace containing Ω_1. It follows that $G(\Omega_1)\leq G_0$ is a subgroup of the upper unitriangular matrices. So every element of $G(\Omega_1)$ fixes $\underline{e}_1$ and it moves $\underline{e}_2$ into $\langle\underline{e}_1,\underline{e}_2\rangle$. Hence $G(\Omega_1)\cap G(\Omega_2)$ fixes $\underline{e}_2$ and $\underline{e}_2+\underline{e}_3$. Therefore, $G(\Omega_1)\cap G(\Omega_2)=1$.

Finally, in case *9* our first observation is that $G(\Omega_1)$ fixes $\underline{0}$, since $\Omega_1\cup\{\underline{0}\}$ is the only 2-dimensional affine subspace containing Ω_1. Hence $G(\Omega_1)\leq GL(W)$. Let $g\in G(\Omega_1)\cap G(\Omega_2)$. Now, $g(\underline{e}_2)=\underline{e}_2$ or $g(\underline{e}_2)=\underline{e}_1+\underline{e}_2$ by our assumption on $\underline{e}_1$. In the second case $g(\underline{e}_3)\in\Omega_2$ and $g(\underline{e}_2+\underline{e}_3)=\underline{e}_1+\underline{e}_2+g(\underline{e}_3)\in\Omega_2$. It is easy to check that there is no $\underline{x}\in\Omega_2$ such that $\underline{e}_1+\underline{e}_2+\underline{x}\in\Omega_2$. (Here we need $n\geq 4$). So $g(\underline{e}_2)=\underline{e}_2$. It follows that g fixes every element of the partition given in case *6*, so $g=1$. The proof is complete. □

The above constructions have the following property.

Corollary 5.3. *If $W\leq G\leq AGL(W)$ is an affine group, $p\geq 3$ a prime, and p does not divide the order of G, then there exists a G-regular partition of W into at most p parts. Moreover, in Case 1 the partition is trivial and it consists of at most $p-1$ parts. In any other case there is a part of "unique size", that is, a part Ω_i such that $|\Omega_i|\neq|\Omega_j|$ if $i\neq j$.*

Proof. If W is a vector space over the q-element field, then $(q,p)=1$, since $G\geq W$. If $p=3$, then $q\neq 3$, so one of the cases *1, 2, 3, 7, 8,* or *9* holds, and the given partition has at most 3 parts. If $p\neq 3$, then $p\geq 5$. Even in the remaining cases the given partition has at most 5 parts. The remaining part of the statement can be easily checked. □

Using this Corollary we can prove the existence of the wanted G-regular partition for any solvable p'-group.

Theorem 5.4. *Let $G \leq \mathrm{Sym}(\Omega)$ be a solvable permutation group, Assuming that the order of G is not divisible by the prime p, there exists a G-regular partition of Ω into at most p parts.*

Before the proof we give an alternative form of this statement, which will be easier to handle. Besides that, from this form it is clearer what the connection is between finding a G-regular partition for a permutation group and finding a two-element base for a linear group. If $\Omega = \{1, 2, \ldots, n\}$, then we have a natural inclusion $\mathrm{Sym}(\Omega) \to GL(n, p)$, that is, $\mathrm{Sym}(\Omega)$ acts on $\mathbb{F}_p^n$ by permuting the coordinates. If we have a partition of Ω into at most p parts, then we can color the elements of the partition by the elements of $\mathbb{F}_p$, that is, there is an $f : \Omega \to \mathbb{F}_p$ such that $x, y \in \Omega$ are in the same part of the partition if and only if $f(x) = f(y)$. Thus, Theorem 5.4 is equivalent to the following theorem.

Theorem 5.5. *If G is a solvable permutation group of degree n, and p does not divide the order of G, then there is a vector $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_p^n$ such that only the identity element of G fixes this vector.*

Proof. Although we do not deal with the case $p = 2$, we note that this follows from a Theorem of D. Gluck [7]. A direct short proof is given by H. Matsuyama [19]. Thus, in the following let $p \geq 3$.

If G is a primitive permutation group, then it is an affine group, so Corollary 5.3 guarantees the existence of such a vector (or partition). In the following let G be a transitive, but not primitive permutation group. Then there is a partition $\Omega = \Delta_1 \cup \Delta_2 \cup \ldots \cup \Delta_k$ such that $1 < |\Delta_1| < |\Omega|$ and G permutes the elements of this partition transitively. We can assume that $|\Delta_1|$ is as small as possible. Let $H_i = G(\Delta_i)$ for all $1 \leq i \leq k$ and let $N = \cap_{i=1}^k H_i$. Then G/N acts transitively on the set $\widetilde{\Omega} = \{\Delta_1, \Delta_2, \ldots, \Delta_k\}$. Using induction on $|\widetilde{\Omega}|$ we get a vector $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k$ such that only the identity element of G/N fixes this vector.

On the other hand, let $C_{H_i}(\Delta_i) = \{g \in H_i \mid g(\omega) = \omega,\ \forall \omega \in \Delta_i\}$ be the pointwise stabilizer of Δ_i in H_i for all $1 \leq i \leq k$. Taking the restriction of H_1 to Δ_1 we get a homomorphism $H_1 \to \mathrm{Sym}(\Delta_1)$ with kernel $C_{H_1}(\Delta_1)$, which gives us an inclusion $H_1/C_{H_1}(\Delta_1) \subseteq \mathrm{Sym}(\Delta_1)$. By the minimality of Δ_1, the action of $H_1/C_{H_1}(\Delta_1)$ on Δ_1 is primitive, so we can find a $H_1/C_{H_1}(\Delta_1)$-regular partition of Δ_1 by Corollary 5.3, say $\Delta_1 = X_{1,1} \cup \ldots \cup X_{1,l}$. Taking elements $g_i \in G$ $(i = 2, \ldots, k)$ such that $g_i(\Delta_1) = \Delta_i$, we define the sets $X_{i,j} = g_i(X_{1,j})$ for all $1 < i \leq k$ and for all $1 \leq j \leq l$. Then $\Delta_i = X_{i,1} \cup \ldots \cup X_{i,l}$ is a $H_i/C_{H_i}(\Delta_i)$-regular partition of Δ_i.

If the first case of Corollary 5.3 holds, then $|\Delta_i| \leq p - 1$. In this case let us choose a subset $B \subsetneq \mathbb{F}_p$ such that $|B| = |\Delta_i|$, and let $f_i : \Delta_i \to B + a_i = \{b + a_i \mid b \in B\}$ be a bijection for every $1 \leq i \leq k$.

If the second case of Corollary 5.3 holds, then let $X_{1,l} \in \{X_{1,1}, X_{1,2}, \ldots, X_{1,l}\}$ be a part of the partition of Δ_1 of unique size. Now, let the function $f_i : \Delta_i \to \mathbb{F}_p$ be defined as a coloring of the partition of Δ_i satisfying $f_i(X_{i,l}) = a_i$.

Let the function $f : \Omega \to \mathbb{F}_p$ be defined as

$$f(x) = f_i(x), \quad \text{if} \quad x \in \Delta_i.$$

Let $g \in G$ such that it fixes the vector $(f(1), f(2), \ldots, f(n)) \in \mathbb{F}_p^n$ and assume that $g(\Delta_i) = \Delta_j$ for some $i \neq j$. If $x \in \Delta_i$, then $f_i(x) = f(x) = f(g(x)) = f_j(g(x))$. In the first case we get the range of f_i is equal to the range of f_j, so $B + a_i = B + a_j$. As the additive group of $\mathbb{F}_p$ is a cyclic group of prime order, and $B \neq \mathbb{F}_p$, it follows that $a_i = a_j$. In the second case we have $|\{x \in \Delta_j \mid f(x) = a_i\}| = |\{y \in \Delta_i \mid f(y) = a_i| = |X_{i,l}| = |X_{j,l}|$. As $X_{j,l}$ is a part of the partition $\Delta_j = X_{j,1} \cup X_{j,2} \cup \ldots \cup X_{j,l}$ such that it is of unique size, it follows from the construction of f_j that $a_i = a_j$. So we proved that if $g \in G$ fixes the vector $(f(1), f(2), \ldots, f(n)) \in \mathbb{F}_p^n$, then gN fixes the vector $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k$, so $g \in N$ and $g(\Delta_i) = \Delta_i$ for each $1 \leq i \leq k$. Therefore, from the construction of the f_i's we get $g \in \cap_{i=1}^k C_{H_i}(\Delta_i) = 1$.

Finally, if the action of G on Ω is not transitive, then let $\Omega = \Omega_1 \cup \Omega_2 \cup \ldots \cup \Omega_k$ be the decomposition of Ω to the orbits of G. This decomposition defines a direct decomposition $\mathbb{F}_p^n = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ to G-invariant subspaces. Using induction on $|V_i|$ we get vectors $x_i \in V_i$ such that $C_G(x_i) = C_G(V_i)$. Then $C_G(x_1 + x_2 + \ldots + x_k) = \cap_{i=1}^k C_G(V_i) = 1$. $\square$

Remark. It was proven by Á. Seress [23, Theorem 1.2.] that for any solvable permutation group $G \leq \mathrm{Sym}(\Omega)$ there always exists a G-regular partition of Ω into at most five parts.

Our next result concerning permutation groups is constructing regular partitions for products of linear groups.

Theorem 5.6. *For each $1 \leq i \leq k$ let W_i be a finite vector space over the p_i-element field, where $p_1 < p_2 < \ldots < p_k$ are primes and $k \geq 2$, and let $W = W_1 \oplus W_2 \oplus \cdots \oplus W_k$. Furthermore, let $G \leq Aut(W) \simeq GL(W_1) \times GL(W_2) \times \cdots \times GL(W_k)$. Then there exists a G-regular partition $W = \{\underline{0}\} \cup \Omega_2 \cup \Omega_3$ such that $|\Omega_2| < \frac{1}{4}|W|$.*

Proof. For each $1 \leq i \leq k$ let $\underline{e}_{i,1}, \underline{e}_{i,2}, \ldots, \underline{e}_{i,n_i}$ be a basis of W_i, where $n_i = \dim W_i$, and let $l = n_1 + \ldots + n_k$. Then $|W| \geq 2^{l-1}3$, since $k \geq 2$. As G is a subgroup of the automorphism group of $\oplus W_i$, it fixes each W_i. Let $G_i \simeq G/C_G(W_i)$ be the restriction of G to W_i. To construct a suitable Ω_2 we use the cases 1-6 of Theorem 5.2. We saw that there are subsets $\Omega_i^* \subseteq W_i$ $(i = 1, \ldots, k)$ such that

$$\begin{array}{ll} G_i(\Omega_i^*) = 1 & \text{for } p_i \geq 5, \text{ or } |W_i| \leq 3; \\ G_i(\Omega_i^*) \cap G_i(\underline{e}_{i,1}) = 1 & \text{for } p_i = 3 \text{ or } |W_i| = 4; \\ G_i(\Omega_i^*) \cap G_i(\underline{e}_{i,1}) \cap G_i(\underline{e}_{i,2}) = 1 & \text{for } p_i = 2, n_i \geq 3. \end{array}$$

Now, let Ω_2 be defined as

$$\begin{array}{ll} \{\sum_i \underline{e}_{i,1}\} \cup \{\underline{e}_{j,2} \,|\, n_j = 2\}, & \text{if each } n_i \leq 2; \\ \{\underline{e}_{1,1} + \underline{e}_{2,1}, \underline{e}_{1,1} + 2\underline{e}_{2,1}, \underline{e}_{1,2} + \underline{e}_{2,1}\} \cup \Omega_1^* \cup \Omega_2^* \cup \ldots \cup \Omega_k^*, & \text{if } p_1 = 2, n_1 \geq 3; \\ \{\underline{e}_{1,1} + \underline{e}_{2,1}\} \cup \Omega_1^* \cup \Omega_2^* \cup \ldots \cup \Omega_k^*, & \text{otherwise.} \end{array}$$

In the first case if $g \in G(\Omega_2)$, then g fixes each $\underline{e}_{j,2}$ and $\sum_i \underline{e}_{i,1}$. It follows that g also fixes each $\underline{e}_{i,1}$, so $g = 1$ and the given partition is G-regular. Furthermore, $|\Omega_2| = l - k + 1 \leq l - 1 < \frac{1}{4}2^{l-1}3 \leq \frac{1}{4}|W|$ holds.

Otherwise, if $g \in G(\Omega_2)$, then g fixes each $W_i \cap \Omega_2 = \Omega_i^*$, and it permutes the one or three exceptional elements. Using that $g(\underline{e}_{1,1}), g(\underline{e}_{1,2}) \in W_1$, $\underline{g}(e_{2,1}) \in W_2$, we get g fixes also these elements. Hence g acts trivially on every W_i, so $g = 1$, and we found a G-regular partition.

It is easy to check that $|\Omega_i^*| \leq 2n_i$ and $|\Omega_1^*| \leq 2n_1 - 3$ if $p_1 = 2,\ n_1 \geq 3$. It follows that $|\Omega_2| \leq 1 + 2l < \frac{1}{4}2^{l-1}3 \leq \frac{1}{4}|W|$ holds unless $l \leq 4$. Now, assume that $l \leq 4$. As some $n_i \geq 3$ we have $|W| = p^3q$ for some primes $p \neq q$. In case of $p = 2$ we have $|\Omega_1^*| = |\Omega_2^*| = 1$, so $|\Omega_2| = 3 + 1 + 1 < \frac{1}{4}2^3 3 \leq \frac{1}{4}|W|$. Finally, if $|W| = p^3q$ for some primes $p \neq 2, q$, then $|\Omega_2| \leq 1 + 6 + 1 < \frac{1}{4}3^3 2 \leq \frac{1}{4}|W|$. □

The last corollary of this section says that with a few exceptions the second largest part of the G-regular partitions given above is relatively small.

Corollary 5.7. *Let W be a product of finite vector spaces and $G \leq Aut(W)$. Then, depending of W, the G-regular partition of W given above has the following property:*

a) In case of $|W|$ is neither a 2-power, nor a 3-power:
$W = \{\underline{0}\} \cup \Omega_2 \cup \Omega_3$ *such that* $|\Omega_2| < \frac{1}{4}|W|$.

b) In case of $|W|$ is a 3-power:
$W = \{\underline{0}\} \cup \Omega_2 \cup \Omega_3 \cup \Omega_4$ *such that* $|\Omega_2| = 1$ *and* $|\Omega_3| + 2 < \frac{1}{4}|W|$, *if* $|W| > 9$.

c) In case of $|W|$ is a 2-power:
$W = \{\underline{0}\} \cup \{\underline{e}_1\} \cup \{\underline{e}_2\} \cup \Omega_4 \cup \Omega_5$ *such that* $|\Omega_4| < \frac{1}{4}|W|$, *if* $|W| > 16$ *or* $|W| = 8$.

Proof. First, if $|W|$ is not a prime power, then Theorem 5.6 gives us a G-regular partition $W = \{\underline{0}\} \cup \Omega_2 \cup \Omega_3$ such that $|\Omega_2| < \frac{1}{4}|W|$. If W is a one-dimensional vector space over the

q-element field for some prime $q \geq 5$, then by choosing $\Omega_2 = \{\underline{e}_1\}$ (see case *2* of Theorem 5.2) we have $|\Omega_2| = 1 < \frac{5}{4} \leq \frac{1}{4}|W|$. Finally, if $|W| = q^n$ for some $n \geq 2$ and for some prime $q \geq 5$, then we use case *3* of Theorem 5.2. Now, we have $|\Omega_2| = 2n < \frac{1}{4}5^n \leq \frac{1}{4}|W|$. Hence *a)* is proved.

In case of $|W| = 3^n$, case *4* of Theorem 5.2 gives us a G-regular permutation. Then $|\Omega_2| = 1$ and $|\Omega_3| + 2 = 2n < \frac{1}{4}3^n = \frac{1}{4}|W|$ holds if $n \geq 3$.

In case of $|W| = 2^n$ for some $n \geq 3$, we use cases *5* and *6* of Theorem 5.2. If $|W| = 8$, then $|\Omega_4| = 1 < \frac{8}{4} = \frac{1}{4}|W|$. If $|W| > 16$, that is, $n \geq 5$, then $|\Omega_4| = 2n - 3 < \frac{1}{4}2^n = \frac{1}{4}|W|$. The Corollary is proved. □

5.2 Primitive linear groups

In the following let $V \simeq \mathbb{F}_p^n$ be a finite vector space and let $G \leq GL(V) \simeq GL(n,p)$ be a solvable linear group such that $(|G|, p) = 1$. In this section we assume that G is primitive as a linear group, that is, there does not exists a proper decomposition

$$V = V_1 \oplus V_2 \oplus \ldots \oplus V_t$$

such that G permutes the terms of this decomposition. In order to find vectors $x, y \in V$ such that $C_G(x) \cap C_G(y) = 1$, we can clearly assume that G is maximal (with respect to inclusion) among the solvable p'-subgroups of $GL(V)$. The main idea of our construction is the following. We find a normal subgroup $F \lhd G$ which has a very special structure and we show the existence of a basis of V such that every element of F is an "almost" monomial matrix in this basis. Next, we choose $x \in V$ in such a way that any element $C_G(x)$ is also an "almost" monomial matrix in this basis. Then the permutation part of F defines a product of linear spaces on this special basis, and the permutation part of $C_G(x)$ acts on this structure. Therefore, we can use the partitions given in the previous section to find a suitable vector y.

5.2.1 The structure of the Fitting subgroup

If $G \leq GL(V)$ is a maximal solvable primitive p'-group, then it is a Hall p'-subgroup of some maximal solvable primitive group $H \leq GL(V)$. Using the description of such groups, we have the following theorem for G.

Theorem 5.8. *Let $G \leq GL(V)$ be a maximal solvable primitive p'-group. Then there is a chain of normal subgroups $A \leq F \leq C \leq G$ with the following properties.*

1. *A is cyclic and $|A| = p^a - 1$ for some a.*
2. *The linear span of A is isomorphic to the field $\mathbb{F}_{p^a}$.*
3. *The action of G/C on A gives us an inclusion $G/C \hookrightarrow \mathrm{Gal}(\mathbb{F}_{p^a}|\mathbb{F}_p)$.*
4. *$F = AP_1P_2 \dots P_k$, where P_i is an extraspecial p_i-group of order $p_i^{2e_i+1}$ for each i. Furthermore, $Z(P_i) = A \cap P_i$, and $\mathbb{F}_{p^a}$ contains all the p_i-th roots of unity. If $p_i > 2$, then the exponent of P_i is p_i.*
5. *Let $e = \prod p_i^{e_i}$. Then $n = ea$.*
6. *C is included in $GL(e, p^a)$.*
7. *$F \leq GL(e, p^a)$ gives an irreducible representation of F.*

Proof. Let $H \leq GL(V)$ be a maximal solvable primitive linear group containing G. Some relevant properties of such a group can be found in [21, Proposition 2.1], [23, Lemma 2.2] and in [25, §§19–20]. First, H contains a unique maximal abelian normal subgroup, denoted by A. Let $F = \mathrm{Fit}(C_H(A))$, the Fitting subgroup of $C_H(A)$. Then we have a chain of normal subgroups $A \leq F \leq C_H(A) \leq H$. Using $C_H(A)$ instead of C in the enumerated statements of the theorem, it is known that any of these statements holds. Specifically, A and F both are normal p'-subgroups of H, so they are contained in any

Hall p'-subgroup of H. As G is a Hall p'-subgroup of H, we get $A \leq F \leq G$. Finally, let $C = C_G(A) = G \cap C_H(A)$. It is clear that statements *3* and *6* hold for C, so we are done. $\square$

The next lemma says that it is enough to find $x, y \in V$ such that $C_C(x) \cap C_C(y) = 1$.

Lemma 5.9. *Let $x, y \in V$ be non-zero vectors such that $C_C(x) \cap C_C(y) = 1$. Then for some $\gamma \in A \cup \{0\} = \mathbb{F}_{p^a}$ we have $C_G(x) \cap C_G(y + \gamma x) = 1$.*

Proof. For any $g \in G$ let $\sigma_g \in \mathrm{Gal}(\mathbb{F}_{p^a}|\mathbb{F}_p)$ denote the action of gC on $\mathbb{F}_{p^a}$ by part *3* of Theorem 5.8. For all $\alpha \in \mathbb{F}_{p^a}$ let $H_\alpha = C_G(x) \cap C_G(y + \alpha x) \leq G$. Our goal is to prove that $H_\alpha = 1$ for some $\alpha \in \mathbb{F}_{p^a}$.

Let $g \in H_\alpha$. Thus, $g(x) = x$ and $y + \alpha x = g(y + \alpha x) = g(y) + \alpha^{\sigma_g} x$. Hence $g(y) = y + (\alpha - \alpha^{\sigma_g})x$. If $g \in \langle \cup H_\alpha \rangle$, then g is the product of elements from several H_α's. It follows that $g(y) = y + \delta x$ for some $\delta \in \mathbb{F}_{p^a}$.

We claim that $\langle \cup H_\alpha \rangle \cap C = 1$. Let $g \in \langle \cup H_\alpha \rangle \cap C$. On the one hand, the action of g on V is $\mathbb{F}_{p^a}$-linear, since $g \in C = C_G(A)$. On the other hand, $g(x) = x$ and $g(y) = y + \delta x$ for some $\delta \in \mathbb{F}_{p^a}$ by the previous paragraph. If $g^n = 1$, then $y = g^n(y) = y + n\delta x$, so $n\delta = 0$. Using that $|G|$ is coprime to p, we get n is not divisible by p, hence $\delta = 0$. Therefore, $g(y) = y$ and $g \in C_C(x) \cap C_C(y) = 1$.

Let g, h be two distinct elements of $\cup H_\alpha$, so $gh^{-1} \notin C$. Since G/C is embedded into $\mathrm{Gal}(\mathbb{F}_{p^a}|\mathbb{F}_p)$, we get $\sigma_g \neq \sigma_h$. Furthermore, the subfields of $\mathbb{F}_{p^a}$ fixed by σ_g and σ_h are the same if and only if $\langle g \rangle = \langle h \rangle$.

If $g \in H_\alpha \cap H_\beta$, then $g(y) = y + (\alpha - \alpha^{\sigma_g})x = y + (\beta - \beta^{\sigma_g})x$, so $\alpha - \beta$ is fixed by σ_g. Let $K_g = \{\alpha \in \mathbb{F}_{p^a} \mid g \in H_\alpha\}$. The previous calculation shows that K_g is an additive coset of the subfield fixed by σ_g, so $|K_g| = p^d$ for some $d|a$. Since for any $d|a$ there is a unique p^d-element subfield of $\mathbb{F}_{p^a}$, we get $|K_g| \neq |K_h|$ unless the subfields fixed by σ_g and σ_h are the same. As we have seen, this means $\langle g \rangle = \langle h \rangle$. Consequently, $|K_g| \neq |K_h|$ unless

$K_g = K_h$. Hence we get

$$|\bigcup_{g \in \cup H_\alpha \setminus \{1\}} K_g| \leq \sum_{d|a,\, d<a} p^d \leq \sum_{d<a} p^d = \frac{p^a - 1}{p - 1} < p^a.$$

So there is a $\gamma \in \mathbb{F}_{p^a}$ which is not contained in K_g for any $g \in \cup H_\alpha \setminus \{1\}$. This exactly means that $H_\gamma = C_G(x) \cap C_G(y + \gamma x) = 1$. □

Henceforth, in the following we can assume that $V \simeq \mathbb{F}_{p^a}^e$, furthermore, $G \leq GL(V) \simeq GL(e, p^a)$ is a solvable p'-group having normal subgroups $A \leq F \leq G$, where A is the subgroup of all non-zero scalar matrices, and parts *4, 5, 7* of Theorem 5.8 hold for F.

Observe that for each prime $p \neq 2$, part *4* of Theorem 5.8 determines the isomorphic type of the Sylow p-subgroup of F, since there are two types of extraspecial groups of order p^{2d+1} for any p: For $p \neq 2$ one of them has exponent p, the other one has exponent p^2. However, for $p = 2$ both of them has exponent 4. In this later case one of them is the central product of d copies of the dihedral group D_4, the other one is the central product of a quaternion group Q and $d - 1$ copies of D_4. This gives us two possible isomorphism types of F if $p^a \equiv 3 \pmod 4$. We say that F is monomial, if in the above decomposition of F either each $p_i \neq 2$ (that is, e is odd), or the extraspecial 2-subgroup in F is a central power of D_4. Otherwise we say that F is not monomial. (The explanation of our term "monomial" is that in the first case we can choose a basis such that written in this basis every element of F will be a monomial matrix.)

5.2.2 Finding $x, y \in V$ in case of F is monomial

In the following let $F \lhd G \leq GL(V) \simeq GL(e, p^a)$ as in the previous subsection and assume that F is monomial. The next theorem helps us to find a "good" basis to F.

Theorem 5.10. *With the above assumptions, the following properties hold for $F \leq GL(V)$:*

1. *There is a decomposition $F = D \rtimes S$ such that $D = A \times D_0$, and*

$$D_0 \simeq S \simeq Z_{p_1}^{e_1} \times Z_{p_2}^{e_2} \times \ldots \times Z_{p_k}^{e_k}.$$

2. *There is a basis* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e \in V$ *such that in this basis* D *consists of diagonal matrices and* S *regularly permutes the elements of this basis.*

3. *The subspaces* $\langle \underline{u}_i \rangle$, $1 \leq i \leq e$ *are all the irreducible representations of* D_0 *over* $\mathbb{F}_{p^a}$*, and they are pairwise non-equivalent.*

4. *Written in the above basis, the main diagonal of any* $g \in D_0$ *contains all of the* $o(g)$*-th roots of unity with the same multiplicity.*

Proof. It is well-known that any extraspecial p-group is a central product of non-abelian groups of order p^3. Using that P_i is a central power of D_4 for $p_i = 2$ and the exponent of P_i is p_i for $p_i > 2$ we can find generators

$$P_i = \langle x_{i,1}, x_{i,2}, \ldots, x_{i,e_i}, y_{i,1}, y_{i,2}, \ldots y_{i,e_i}, z_i \rangle \,,$$

such that any generator is of order p_i, $Z(P_i) = \langle z_i \rangle$, $[x_{i,l}, y_{i,l}] = z_i$ for all $1 \leq l \leq e_i$, and any other pair of generators are commuting. Now, let $D_i = \langle x_{i,1}, x_{i,2}, \ldots, x_{i,e_i} \rangle$, and $S_i = \langle y_{i,1}, y_{i,2}, \ldots, y_{i,e_i} \rangle$. Finally, let

$$D = A \times D_1 \times D_2 \times \cdots \times D_k \quad \text{and} \quad S = S_1 \times S_2 \times \cdots \times S_k.$$

Using part *4* of Theorem 5.8, we get $A = \mathbb{F}_{p^a}^*$ contains all of the $\exp(D)$-th roots of unity, hence every irreducible representation of D over $\mathbb{F}_{p^a}$ is one dimensional. Fix an $\underline{u}_1 \in V$ in such a way that $\mathbb{F}_{p^a}\underline{u}_1$ is a D-invariant subspace. Choosing $D_0 = C_D(\underline{u}_1)$ we have $D = A \times D_0$, and $D_0 \simeq D_1 \times \cdots \times D_k \simeq S \simeq Z_{p_1}^{e_1} \times \cdots \times Z_{p_k}^{e_k}$.

Let the basis $\{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e\}$ be defined as the set $\{s(\underline{u}_1) \,|\, s \in S\}$. First, $e = |S| = \dim V$. As $D \lhd F$, it follows that $Ds(\underline{u}_1) = sD(\underline{u}_1)$, so $\mathbb{F}_{p^a} s\underline{u}_1$ is also a D-invariant subspace for all $s \in S$. Hence $\langle \underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e \rangle$ is an $F = DS$-invariant subspace, so it is equal to V by part *7* of Theorem 5.8. Therefore, $\{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e\}$ is indeed a basis of V. Then *2* clearly follows from our construction.

The *3*rd part of the statement follows easily from the fact $C_S(D_0) = 1$. Indeed, let $\underline{u}_i \neq \underline{u}_j$ be two basis elements. Then $\underline{u}_j = s(\underline{u}_i)$ for some $1 \neq s \in S$. Furthermore, let $d \in D_0$ such that $[d, s] \in A \setminus \{1\}$. Then

$$d_{jj}\underline{u}_j = d(\underline{u}_j) = ds(\underline{u}_i) = sd[d, s](\underline{u}_i) = [d, s](d_{ii}\underline{u}_j).$$

It follows that $d_{jj} \neq d_{ii}$, which proves that these representations of D_0 are pairwise non-isomorphic. The statement that these representations give us all the irreducible representations of D_0 follows from the fact $|D_0| = e$.

Finally, any linear representation of $\langle g \rangle$ can be extended to D_0 in exactly $|D_0|/o(g)$ ways, which proves *4*. □

In the following we fix a basis $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e$, which fulfill the requirements of the above theorem. With respect to this basis, we identify $GL(V)$ with the matrix group $GL(e, p^a)$. Thus, $F = DS \lhd G \leq GL(e, p^a)$, where D is the group of diagonal matrices in F and S is the group of permutation matrices in F acting regularly on the selected basis. Furthermore, $D = A \times D_0$, where $D_0 = C_D(\underline{u}_1) = C_F(\underline{u}_1)$.

To find a base $x, y \in V$ we write them as a linear combination of the basis vectors $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e$ in such a way that x contains only a few (one or three) $\underline{u}_i$ with non-zero coefficients, while y contains a lot of them.

Our next lemma collects some consequences of the choice $x = \underline{u}_1$:

Lemma 5.11. *Let $g \in G$ be any group element fixing $g(\underline{u}_1) = \underline{u}_1$. Then*

1. *$D_0^g = D_0$ and g is a monomial matrix. Hence there exists a unique decomposition $g = \delta(g)\pi(g)$ to a product of a diagonal matrix $\delta(g)$ and a permutation matrix $\pi(g)$.*
2. *$\pi(g)$ normalizes S, that is, $S^{\pi(g)} = S$.*
3. *Both $\delta(g)$ and $\pi(g)$ normalize F, so $F = F^{\delta(g)} = F^{\pi(g)}$. Moreover, $[\delta(g), S] \leq D$.*
4. *If $\delta(g) \neq 1$, then the number of 1's in the main diagonal of $\delta(g)$ is at most $\frac{3}{4}e$.*

Proof. The statement $D_0^g = D_0$ follows from the fact $D_0 = C_F(\underline{u}_1) \lhd C_G(\underline{u}_1)$. Consequently, g permutes the homogeneous components of the D_0-module V. By part *3* of Theorem 5.10, these homogeneous components are just the one-dimensional subspaces $\langle \underline{u}_i \rangle$ for $1 \leq i \leq e$. It follows that g is a monomial matrix. Of course, a monomial matrix g has a unique decomposition $g = \delta(g)\pi(g)$, and part *1* is proved.

The map $\pi : g \to \pi(g)$ gives us a homomorphism from the group of monomial matrices into the group of permutation matrices. As $g \in G$ normalizes F, we have $\pi(g)$ normalizes $\pi(F) = S$ and *2* follows.

Both g and $\delta(g)$ normalize D, hence $\pi(g) = \delta(g)^{-1}g$ normalizes D, too. We have already seen that $\pi(g)$ normalizes S, so it also normalizes $F = DS$. We get $\delta(g) = g\pi(g)^{-1}$ also normalizes F. Finally, $[\delta(g), S]$ is a subset of F and it consists of diagonal matrices, so $[\delta(g), S] \leq D$ and *3* holds.

If $\delta(g) \neq 1$, then $\delta(g)$ is not a scalar matrix, so there exists an $s \in S$ such that $[\delta(g), s] \in D \setminus \{1\}$. Using part *4* of Theorem 5.10, we get the number of 1's in the main diagonal of $[\delta(g), s]$ is at most $\frac{1}{2}e$. This cannot be true if the number of 1's in $\delta(g)$ is more than $\frac{3}{4}e$. We are done. □

By part *2* of Lemma 5.11, $\pi(C_G(\underline{u}_1)) \leq C_{GL(e,p^a)}(\underline{u}_1)$ normalizes S, so it acts on S by conjugation, which defines a homomorphism from $\pi(C_G(\underline{u}_1))$ to $\mathrm{Aut}(S)$. In fact, this homomorphism is an inclusion, since $C_{GL(e,p^a)}(\underline{u}_1) \cap C_{GL(e,p^a)}(S) = 1$. Therefore, $\pi(C_G(\underline{u}_1)) \leq \mathrm{Aut}(S) \simeq GL(e_1, p_1) \times GL(e_2, p_2) \times \cdots GL(e_k, p_k)$.

Thus, we can apply Corollary 5.7 to find a $\pi(C_G(\underline{u}_1))$-regular partition of S. Since S acts on the basis $W = \{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e\}$ regularly, using the bijection $s \to s(\underline{u}_1)$ we can define a partition $W = \{\underline{u}_1\} \cup \Omega_2 \cup \ldots \cup \Omega_l$, which is also $\pi(C_G(\underline{u}_1))$-regular.

Case $e \neq 2^k$

In the following we will assume that $|D_0| = |S| = e$ is not a 2-power. In every such case let $x = \underline{u}_1$. By the last paragraph, we have a $\pi(C_G(\underline{u}_1))$-regular partition $W = \{\underline{u}_1\} \cup \Omega_2 \cup \ldots \cup \Omega_l$. Let $\alpha \in \mathbb{F}_{p^a}$ be a generator element of the multiplicative group of $\mathbb{F}_{p^a}$. Now, $o(\alpha) = |A| \geq 6$, since $|A|$ is even (because $p \neq 2$) and every prime divisor of e divides $|A|$.

Theorem 5.12. *With the above notations let y be defined as follows*

$$\begin{aligned}
&\textit{For } e \neq 3^k: && y = 0 \cdot \sum_{\underline{u}_i \in \Omega_2} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_3} \underline{u}_i, \\
&\textit{For } e = 3^k,\ k \geq 2: && y = \alpha \cdot \sum_{\underline{u}_i \in \Omega_2} \underline{u}_i + 0 \cdot \sum_{\underline{u}_i \in \Omega_3} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_4} \underline{u}_i, \\
&\textit{For } e = 3: && y = \alpha \underline{u}_2 + \underline{u}_3.
\end{aligned}$$

Then $C_G(x) \cap C_G(y) = 1$.

Proof. Let $g \in C_G(x) \cap C_G(y)$. Since g fixes $\underline{u}_1 = x$, we get g is a monomial matrix by Lemma 5.11, so we have a decomposition $g = \delta(g)\pi(g)$.

In case of $e \neq 3^k$ our first observation is that $\pi(g)$ fixes the subset $\Omega_2 \subseteq W$. To see this, notice that if the monomial matrix g fixes y, then $\pi(g)$ permutes the basis elements appearing in y with zero coefficients between each other. So $\pi(g)$ fixes both $\underline{u}_1 \cup \Omega_2$ and $\underline{u}_1$ (since g does), therefore it fixes Ω_2. As $W = \{\underline{u}_1\} \cup \Omega_2 \cup \Omega_3$ is a $\pi(C_G(\underline{u}_1))$-regular partition, we get $\pi(g) = 1$. Hence $g = \delta(g)$ is a diagonal matrix. If g_{ii} denote the i-th element of the main diagonal of g, then $g \in C_G(y)$ holds only if $g_{ii} = 1$ for all $\underline{u}_i \in \Omega_3$. We also have $g_{11} = 1$. Since e is neither a 2-power nor a 3-power, we can apply part *a)* of Corollary 5.7 to get $|\Omega_2| < \frac{1}{4}e$. Using part *4* of Lemma 5.11 it follows that $g = 1$.

In case of $e = 3^k,\ k \geq 2$ we see that $\pi(g)$ fixes the subset $\Omega_3 \subseteq W$, since these elements occur with coefficient 0 in y (not counting $x = \underline{u}_1$ which is already fixed by g). However, in this case it is possible that $\pi(g)$ moves the unique element of Ω_2 into an element of Ω_4.

Of course, in that case it moves an element of Ω_4 into the element of Ω_2. This results the appearance of an α and an α^{-1} in the main diagonal of $\delta(g)$. It follows that the number of elements different from 1 in the main diagonal of $\delta(g)$ is at most $|\Omega_3|+2$, which is less than $\frac{1}{4}e$ if $e>9$ by part *b)* of Corollary 5.7. By part *4* of Lemma 5.11 we get $\delta(g)=1$, hence $\pi(g)$ also fixes the unique element of Ω_2, so $g=\pi(g)=1$.

In case of $e=9$ we have $y=\alpha\cdot\underline{u}_i+0\cdot\underline{u}_j+1\cdot\sum_{k\neq i,j,1}\underline{u}_k$. Then $\pi(g)$ fixes $\underline{u}_j$. If $\pi(g)$ does not fix $\underline{u}_i$, then in the main diagonal of $\delta(g)$ there are an α and an α^{-1}, possibly $\delta(g)_{jj}\neq 1$, any other element is 1. Since S acts regularly on W, we can choose an element $s\in S$ which takes the basis element corresponding to α^{-1} into the basis element corresponding to α. Then, the main diagonal of $[\delta(g),s]\in D$ contains an $\alpha^2\neq 1$ and at least four 1's. However, there is no such an element in $D=A\times D_0$ by part *4* of Theorem 5.10, a contradiction. So $\pi(g)$ fixes also $\underline{u}_i$. It follows that $\pi(g)=1$. Furthermore, g_{jj} is the only element in the main diagonal of $g=\delta(g)$ which can be different from 1. Using part *4* of Lemma 5.11 we get $g=1$.

Finally, let $e=3$. If $g\in C_G(x)\cap C_G(y)$ is a diagonal matrix, then clearly $g=1$. Otherwise,

$$\delta(g)=\begin{pmatrix}1&0&0\\0&\alpha&0\\0&0&\alpha^{-1}\end{pmatrix}\text{ and }[\delta(g),s]=\begin{pmatrix}\alpha&0&0\\0&\alpha^{-2}&0\\0&0&\alpha\end{pmatrix},\text{ for }s=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\in S.$$

Since $o(\alpha)\geq 6$ we get $\alpha\neq\alpha^{-2}$, so $[\delta(g),s]\notin D$ by part *4* of Theorem 5.10, which contradicts to part *3* of Lemma 5.11. □

Case $e=2^k$

Still assuming that F is monomial, now we handle the case $e=2^k$ for some k. We note that in case of $e\geq 128$ we could give similar constructions as we did in Theorem 5.12. However, for a more uniform discussion we alter these constructions a bit, so it will be adequate even in smaller dimensions. The point of our modification is that we do not

choose x as a basis element this time, rather as a linear combination of exactly three basis vectors. Although this effects that $C_G(x)$ will not be monomial any more, we can cure this problem by a good choice of y.

In case of $e = 2$ any basis will be obviously good, let for example $x = \underline{u}_1, y = \underline{u}_2$. Now, we analyze the case $e = 4$. According to Theorem 5.10, we choose a basis $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4 \in V$. In this case $F = AD_0S$, where the Klein groups $D_0 = \langle d_1, d_2 \rangle$ and $S = \langle s_1, s_2 \rangle$ are generated (independently from the base field) by the matrices:

$$d_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}, \; d_2 = \begin{pmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}, \; s_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \; s_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

If the size of the base field is not equal to $3, 5$ or 9, then the following theorem gives us a good pair of vectors x and y.

Theorem 5.13. *Let $F = A \langle d_1, d_2, s_1, s_2 \rangle \lhd G \leq GL(4, p^a)$, and assume that $p^a \neq 3, 5, 9$. Furthermore, let $\alpha \in \mathbb{F}_{p^a} \setminus \{0\}$ such that $\alpha^8 \neq 1$. Set $x = \underline{u}_2 + \alpha \underline{u}_3 + \alpha^{-1} \underline{u}_4$, $y = \underline{u}_1$. Then $C_G(x) \cap C_G(y) = 1$.*

Proof. Let $g \in C_G(x) \cap C_G(y)$. By the choice of y we know that g is a monomial matrix. The first element in the main diagonal of $\delta(g)$ is 1, and the others are from the set $\{1, \alpha, \alpha^{-1}, \alpha^2, \alpha^{-2}\}$. If $\delta(g)$ contains an α or an α^{-1}, then for some $s \in S$ we get $[\delta(g), s] \in A \times D_0$ contains both α and α^{-1}. By part *4* of Theorem 5.10, this is impossible unless $o(\alpha^2)|4$ which does not hold. It follows that either $g = 1$, or

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^2 \\ 0 & 0 & \alpha^{-2} & 0 \end{pmatrix}, \qquad \text{and} \qquad [\delta(g), s_1] = \begin{pmatrix} \alpha^2 & 0 & 0 & 0 \\ 0 & \alpha^{-2} & 0 & 0 \\ 0 & 0 & \alpha^{-2} & 0 \\ 0 & 0 & 0 & \alpha^2 \end{pmatrix}.$$

As $[\delta(g), s_1] \in D$ we get $o(\alpha^4)|2$, which is again impossible. $\square$

The aim of the next theorem is to make the problem clear for $G \leq GL(4,3)$ and for $G \leq GL(4,9)$. However, our construction works equally well over every finite field of characteristic 3. In the proof we need to use the assumption $(|G|, |V|) = 1$.

Theorem 5.14. *Let $F = A\langle d_1, d_2, s_1, s_2\rangle \lhd G \leq GL(4, 3^k)$. Furthermore, set $x_1 = \underline{u}_2 + \underline{u}_3 + \underline{u}_4$, and $y_1 = \underline{u}_1$. Then $|C_G(x_1) \cap C_G(y_1)| \leq 2$. If x_1, y_1 is not a base for G, then let $1 \neq g_0 \in C_G(x_1) \cap C_G(y_1)$. Then g_0 is a permutation matrix fixing one of the elements $\underline{u}_2, \underline{u}_3, \underline{u}_4$. If, for example, $g_0(\underline{u}_2) = \underline{u}_2$, then let us define the vectors $x_2, y_2, x_3, y_3 \in V$ as*

$$x_2 = \underline{u}_1 + \underline{u}_2 + \underline{u}_4, \qquad y_2 = \underline{u}_1 + \underline{u}_3;$$
$$x_3 = \underline{u}_1 + \underline{u}_2 - \underline{u}_4, \qquad y_3 = \underline{u}_1 + \underline{u}_3.$$

Now, either $C_G(x_2) \cap C_G(y_2) = 1$, or $C_G(x_3) \cap C_G(y_3) = 1$.

Proof. We know that $C_G(y_1)$ consists of monomial matrices by part *1* of Lemma 5.11, so any $g \in C_G(x_1) \cap C_G(y_1)$ acts as a permutation on the set $\{\underline{u}_2, \underline{u}_3, \underline{u}_4\}$. Since the order of $|G|$ is not divisible by 3, we get $C_G(x_1) \cap C_G(y_1)$ is isomorphic to a $3'$-subgroup of the symmetric group S_3, so $|C_G(x_1) \cap C_G(y_1)| \leq 2$.

Let us assume that

$$g_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in G.$$

Now, $C_G(\underline{u}_1 + \underline{u}_3)$ normalizes the subgroup $N = C_F(\underline{u}_1 + \underline{u}_3)$ generated by the elements d_2, s_1. It is easy to check that the N-invariant subspaces

$$\langle \underline{u}_1 + \underline{u}_3 \rangle, \ \langle \underline{u}_1 - \underline{u}_3 \rangle, \ \langle \underline{u}_2 + \underline{u}_4 \rangle, \ \langle \underline{u}_2 - \underline{u}_4 \rangle$$

are pairwise non-equivalent representations of N. Hence $C_G(\underline{u}_1 + \underline{u}_3)$ permutes these subspaces. (In other words, it consists of momomial matrices with respect to this new basis.)

Of course, $C_G(\underline{u}_1 + \underline{u}_3)$ fixes the subspace $\langle \underline{u}_1 + \underline{u}_3 \rangle$. Using again that $|G|$ is not divisible by 3, we get at least one of the following holds:

$$\forall g \in C_G(\underline{u}_1 + \underline{u}_3) : g(\underline{u}_1 - \underline{u}_3) = \alpha_g(\underline{u}_1 - \underline{u}_3) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*,$$
$$\forall g \in C_G(\underline{u}_1 + \underline{u}_3) : g(\underline{u}_2 + \underline{u}_4) = \alpha_g(\underline{u}_2 + \underline{u}_4) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*,$$
$$\forall g \in C_G(\underline{u}_1 + \underline{u}_3) : g(\underline{u}_2 - \underline{u}_4) = \alpha_g(\underline{u}_2 - \underline{u}_4) \quad \text{for some } \alpha_g \in \mathbb{F}_{p^a}^*.$$

In the first case $C_G(\underline{u}_1 + \underline{u}_3)$ fixes both subspaces $\langle \underline{u}_1, \underline{u}_3 \rangle$ and $\langle \underline{u}_2, \underline{u}_4 \rangle$. Thus, if $g \in C_G(\underline{u}_1 + \underline{u}_3)$ fixes either x_2 or x_3, then $g(\underline{u}_1) = \underline{u}_1$, and g is a monomial matrix. Furthermore, either $g = 1$, or $g(\underline{u}_2) = \beta \underline{u}_4$ and $g(\underline{u}_4) = \gamma \underline{u}_2$ for some $\beta, \gamma \in \mathbb{F}_{p^a}^*$. However, it that case the order of $g_0 g \in G$ is divisible by three, a contradiction. We get $C_G(x_2) \cap C_G(y_2) = C_G(x_3) \cap C_G(y_3) = 1$.

In the second case we claim that $C_G(x_2) \cap C_G(y_2) = 1$. Let $g \in C_G(x_2) \cap C_G(y_2)$. If $g(\underline{u}_1 - \underline{u}_3) = \beta(\underline{u}_1 - \underline{u}_3)$ for some $\beta \in \mathbb{F}_{p^a}^*$, then $g = 1$ by the previous paragraph. Otherwise, $g(\underline{u}_1 - \underline{u}_3) = \gamma(\underline{u}_2 - \underline{u}_4)$ holds for some $\gamma \in \mathbb{F}_{p^a}^*$. Using that $\frac{1}{2} = -1$ in $\mathbb{F}_{3^k}$ we get

$$g(\underline{u}_1 + \underline{u}_2 + \underline{u}_4) = \frac{1}{2}(g(\underline{u}_1 + \underline{u}_3) + g(\underline{u}_1 - \underline{u}_3)) + g(\underline{u}_2 + \underline{u}_4) =$$
$$- (\underline{u}_1 + \underline{u}_3) - \gamma(\underline{u}_2 - \underline{u}_4) + \alpha_g(\underline{u}_2 + \underline{u}_4) \neq \underline{u}_1 + \underline{u}_2 + \underline{u}_4.$$

This contradiction shows that $C_G(x_2) \cap C_G(y_2) = 1$.

Finally, in the third case the proof of $C_G(x_3) \cap C_G(y_3) = 1$ is essentially the same as the proof was in the second case. □

Remark. In the above example, if we start from the decomposition $F = AD_0'S'$, where $D_0' = \langle d_2, s_1 \rangle$ and $S' = \langle s_2, d_1 \rangle$, then the corresponding basis $\{\underline{u}_1', \underline{u}_2', \underline{u}_3', \underline{u}_4'\}$ suitable to Theorem 5.10 will be the following

$$\underline{u}_1' = \underline{u}_1 + \underline{u}_3, \quad \underline{u}_2' = \underline{u}_1 - \underline{u}_3, \quad \underline{u}_3' = \underline{u}_2 + \underline{u}_4, \quad \underline{u}_4' = \underline{u}_2 - \underline{u}_4.$$

Written in this new basis, the vectors x_2, y_2, x_3, y_3 have the following form

$$x_2 = -\underline{u}'_1 - \underline{u}'_2 + \underline{u}'_3, \qquad y_2 = \underline{u}'_1;$$
$$x_3 = -\underline{u}'_1 - \underline{u}'_2 + \underline{u}'_4, \qquad y_3 = \underline{u}'_1.$$

Hence in case of $G \leq GL(4, 3^k)$ we can assume that there exists a pair x, y such that $C_G(x) \cap C_G(y) = 1$, where $y = \underline{u}_1$, and x is the linear combination of exactly three basis vectors with non-zero coefficients.

In case of $GL(4, 5)$ we used the GAP system [6] to find x and y.

Theorem 5.15. *As before, let $F = A\langle d_1, d_2, s_1, s_2\rangle \leq GL(4, 5)$, and let N denote the normalizer of F in $GL(4, 5)$. Then, for $x = \underline{u}_1 + \underline{u}_2 + 2\underline{u}_3$ and $y = \underline{u}_2 + \underline{u}_3 + 2\underline{u}_4$ we have $C_N(x) \cap C_N(y) = 1$.*

The constructions given in the last three theorems have the common property that x is a sum of exactly three basis vectors with non-zero coefficient. Capitalizing this property, we shall give a uniform construction in any case of $F = AD_0S \lhd G \leq GL(2^k, p^a)$ for all $k \geq 3$. Possibly taking a permutation of the basis vectors $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e$ we can assume that $\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\}$ corresponds to a two dimensional subspace of S, that is,

$$\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\} = S_2(\underline{u}_1) = \{s(\underline{u}_1) \mid s \in S_2\} \quad \text{for some } S_2 \leq S,\ |S_2| = 4.$$

Let $V' = \langle \underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\rangle \leq V$ be the subspace generated by the first four basis vectors, and let $N_F(V')$ be the subgroup of elements of F fixing V'. Then the restriction of $N_F(V')$ to V' defines an inclusion $N_F(V')/C_F(V')$ into $GL(V')$, so we get a subgroup $F' = A\langle d_1, d_2, s_1, s_2\rangle \leq GL(V')$. If $g \in N_G(V')$, then it is clear that $g_{V'}$ normalizes F'. Using the previous results, we can define $x_0, y_0 \in V'$ such that x_0 is the linear combination of exactly three basis vectors and $N_G(V') \cap C_G(x_0) \cap C_G(y_0)$ acts trivially on V'. Starting from the vectors x_0, y_0, we search a base $x, y \in V$ of the form $x = x_0,\ y = y_0 + v$, where $v \in V'' := \langle \underline{u}_5, \underline{u}_6, \ldots, \underline{u}_e\rangle$. The following lemma answers why this form is useful.

Lemma 5.16. *$C_G(x_0)$ fixes both subspaces V' and V'', that is, $C_G(x_0) \leq N_G(V') \cap N_G(V'')$. As a result, for any $v \in V''$ we have $C_G(x_0) \cap C_G(y_0 + v) = C_G(x_0) \cap C_G(y_0) \cap C_G(v)$ acts trivialy on V'. In particular, $C_G(x_0) \cap C_G(y_0 + v)$ consists of monomial matrices.*

Proof. It is enough to prove the inclusion $C_G(x_0) \leq N_G(V') \cap N_G(V'')$, the rest of the statement follows evidently. Our proof is similar to the way we have proved that $C_G(\underline{u}_1)$ consists of monomial matrices. As there are three basis elements in x_0 with non-zero coefficients and $S \simeq Z_2^k$ regularly permutes the basis elements, we get $C_F(x_0) \leq D$, i.e., every element of $C_F(x_0)$ is diagonal. Hence every element of $C_F(x_0)$ fixes the three basis elements appearing in x_0. Using the assumption that $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4$ corresponds to the subspace $S_2 \leq S$, it follows easily that any element of D fixing three of the basis elements $\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4$ must fix the fourth one, too. Let $N = C_F(x_0) = C_F(V')$. It follows that $|D_0 : N| = 4$, so V' is just the homogeneous component of N corresponding to the trivial representation, while V'' is the sum of the other homogeneous components of N. As $N \lhd C_G(x_0)$, every element of $C_G(x_0)$ permutes the homogeneous components of N. Since $x_0 \in V'$, we get $C_G(x_0)$ fixes V', so it also fixes the sum of the other homogeneous components, which is V''. □

It is time to define the vector v, whereby we close the monomial case. We already know by the previous lemma that $C_G(x_0) \cap C_G(y_0 + v)$ consists of monomial matrices for any $v \in V''$, so we can use Corollary 5.7 to define a $\pi(C_G(x_0) \cap C_G(y_0))$-regular partition on $W = \{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e\}$.

Theorem 5.17. *By part c) of Corollary 5.7 let $W = W_2 \cup \Omega_4 \cup \Omega_5$ be a $\pi(C_G(x_0) \cap C_G(y_0))$-regular partition of $W = \{\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_e\}$ such that $W_2 = \{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4\}$ corresponds to a two dimensional subspace of S. Let the vectors $x, y \in V$ be defined as*

$$x = x_0,\ y = y_0 + v, \qquad \text{where } v = 0 \cdot \sum_{\underline{u}_i \in \Omega_4} \underline{u}_i + 1 \cdot \sum_{\underline{u}_i \in \Omega_5} \underline{u}_i, \qquad \text{for } e \neq 16.$$

In case of $e = 16$ this construction does not work (since it was an exceptional case in Corollary 5.7). In this case let $\underline{u}_s, \underline{u}_t \in \{\underline{u}_5, \underline{u}_6 \ldots, \underline{u}_{16}\}$ be two vectors corresponding to elements from different cosets of S_2 in S. In this case let $x, y \in V$ be chosen as

$$x = x_0,\ y = y_0 + v, \qquad \textit{where}\ \ v = 0 \cdot \underline{u}_s + (-1) \cdot \underline{u}_t + 1 \cdot \sum_{\substack{i \in \{5,6,\ldots,16\} \\ i \neq s,t}} \underline{u}_i.$$

Then we have $C_G(x) \cap C_G(y) = 1$.

Proof. We know by the previous lemma that any $g \in C_G(x) \cap C_G(y)$ is a monomial matrix fixing all elements of W_2. Also Ω_4 is fixed by $\pi(g)$, since exactly the elements of $W_2 \cup \Omega_4$ occur with coefficient 0 in v. It follows that $\pi(g) = 1$. Hence $g = \delta(g)$ is a diagonal matrix, and any element in its main diagonal not corresponding to Ω_4 must be 1. Furthermore, $|\Omega_4| < \frac{1}{4}|W|$ in case of $e \neq 16$ by part *c)* of Corollary 5.7, so we get $g = \delta(g) = 1$ by using part *4* of Lemma 5.11.

In case of $e = 16$ for any $g \in C_G(x) \cap C_G(y)$ we have $\pi(g)(\underline{u}_s) = \underline{u}_s$. Now, if $\pi(g)(\underline{u}_t) = \underline{u}_t$ does not hold, then the number of elements in the main diagonal of $\delta(g)$ different from 1 should be 2 or 3, which is again a contradiction to part *4* of Lemma 5.11. Hence $\delta(g) = 1$ and $\pi(g)(\underline{u}_t) = \underline{u}_t$. By our choice of the vectors $\underline{u}_s, \underline{u}_t$ we get $g = \pi(g) = 1$, which proves the identity $C_G(x) \cap C_G(y) = 1$. □

5.2.3 Finding $x, y \in V$ in case of F is not monomial

In the following we examine the case when F is not monomial. Thus, the extraspecial 2-group, say P_1, in part *4* of Theorem 5.8 is the central product of a quaternion group Q by some number of dihedral groups D_4. If $\lambda \in A$ is a field element of order four, and $Q = \langle i, j \rangle \leq P_1$ is the quaternion group generated by the elements i, j of order four, then by defining $H = \langle \lambda i, \lambda j \rangle \leq AQ$ we get $H \simeq D_4$ and $AH = AQ$. Therefore, in the decomposition of F we can exchange Q with a subgroup isomorphic to D_4, so we get the

monomial case. Hence we can assume that A does not contain a fourth root of unity. Our next theorem is analogous to Theorem 5.10.

Theorem 5.18. *With the above assumptions, the subgroup $F \leq GL(V)$ has the following properties*

1. *There exists a product decomposition $F = QF_1$ such that $F_1 = C_F(Q) = D \rtimes S = (A \times D_0) \rtimes S$ and*
$$D_0 \simeq S \simeq Z_2^{e_1-1} \times Z_{p_2}^{e_2} \times \ldots \times Z_{p_k}^{e_k}.$$

2. *There exists a basis $\underline{u}_1, \underline{v}_1, \underline{u}_2, \underline{v}_2, \ldots, \underline{u}_{e/2}, \underline{v}_{e/2} \in V$ such that in this basis the elements of D are diagonal matrices, while S permutes the set of ordered pairs $\{(\underline{u}_i, \underline{v}_i) \,|\, 1 \leq i \leq e/2\}$ regularly.*

3. *The subspaces $\langle \underline{u}_i \rangle$ are all the irreducible representations of D_0 over $\mathbb{F}_{p^a}$ and they are pairwise non-equivalent.*

4. *In the above basis, the main diagonal of any $g \in D_0$ contains all of the $o(g)$-th root of unity with the same multiplicity.*

5. *For all $1 \leq i \leq e/2$ any element of D restricted to $W_i = \langle \underline{u}_i, \underline{v}_i \rangle$ is a scalar matrix.*

6. *If an element $g \in QD$ has an eigenvector in V, then $g \in D$.*

Proof. Let $P_1 = QT$ be the central product of the quaternion group Q by the extraspecial 2-group T, where T is a central power of some D_4's. Applying part *1* of Theorem 5.10 to the group $F_1 = ATP_2P_3 \ldots P_k$ the first statement follows at once.

Let $V_1 \leq V$ be an irreducible F_1-invariant subspace of V. As $Z(F_1) = A$ consists of scalar matrices and F_1 is nilpotent, F_1 acts faithfully on V_1, so the restriction of F_1 to V_1 gives us an inclusion $F_1 \leq GL(V_1)$. It is well-known that if R is an extraspecial r-group of order r^{2m+1} for some prime r, then the degree of every faithful, irreducible

complex character of R is r^m, and the character values of such a character are in the r-th cyclotomic field. It follows that the degree of every faithful, irreducible complex characters of F_1 is equal to $e/2$. Furthermore, the character values of such a character are in the $p^a - 1$-th cyclotomic field. Using [14, Theorem 15.13], we get that every faithful, irreducible $\overline{\mathbb{F}_{p^a}}$-representation of F_1 has dagree $e/2$ and its character values are in $\mathbb{F}_{p^a}$. Such a representation is an extension of an $\mathbb{F}_{p^a}$-representation of F_1 by [14, Theorem 9.14]. It follows that the degree of any faithful, irreducible $\mathbb{F}_{p^a}$-representation of F_1 is equal to $e/2$, hence the dimension of V_1 is $e/2$. By Theorem 5.10, there exists a basis $\{\underline{u}_1, \underline{u}_2, \ldots \underline{u}_{e/2}\} \in V_1$ such that D consists of diagonal matrices with respect to this basis, while S regularly permutes the elements of this basis. So statement *3* follows from the corresponding part of Theorem 5.10.

Let $W_i = \langle q(\underline{u}_i) \,|\, q \in Q \rangle$ be the smallest Q-invariant subspace containing $\underline{u}_i$. Then each W_i is a homogeneous D_0-module, since Q centralizes D_0. Additionally, these subspaces are pairwise non-equivalent D_0-modules.

Since Q centralizes also S, we get S regularly permutes the subspaces W_i. It follows that $W_1 \oplus W_2 \oplus \ldots \oplus W_{e/2}$ is an F-invariant subspace, so it is equal to V. Comparing dimensions we get each W_i is two dimensional. Let us choose elements $\underline{v}_i \in W_i$ such that $\underline{u}_i, \underline{v}_i$ is a basis of W_i for all i, and the set of vectors $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{e/2}\}$ is an orbit of S. Then *2* and *5* follows obviously.

Using part *4* of Theorem 5.10, statement *4* follows immediately.

Finally, let $g = qd \in QD \setminus D$, so $q \in Q \setminus \{\pm I\}$. As the elements of Q are commuting with the elements of D and the exponent of D is not divisible by 4 (here we use that A does not contain a fourth root of unity), we get the order of g is divisible by four. It follows that $g^{o(g)/2}$ is an element of Q of order two, hence $g^{o(g)/2} = -I$. Therefore, if $\lambda \in \mathbb{F}_{p^a}$ is an eigenvalue of g, then $\lambda^{o(g)/4} \in \mathbb{F}_{p^a}$ would be a fourth root of unity, a contradiction. Hence any element of $QD \setminus D$ does not have an eigenvector in V, which proves *6*. $\square$

In the following let $V_1 = \langle \underline{u}_1, \underline{u}_2, \ldots, \underline{u}_{e/2} \rangle$ and $V_2 = \langle \underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{e/2} \rangle$. Then $V = V_1 \oplus V_2$. Let $N_G(V_1)$ denote the elements of G fixing the subspace V_1. The restriction of $N_G(V_1)$ to V_1 gives us a homomorphism $N_G(V_1) \to GL(V_1)$ with image $G_1 \simeq N_G(V_1)/C_G(V_1)$. Furthermore, F_1 is included into G_1 via the restriction of F_1 to V_1, and its image is a normal subgroup of G_1 isomorphic to F_1. So we can use the constructions of the monomial case to find vectors $x_1, y_1 \in V_1$ such that $C_{G_1}(x_1) \cap C_{G_1}(y_1) = 1_{V_1}$. Furthermore, in cases $e/2 \neq 2^k$ and $e/2 = 2$ we have $x_1 = \underline{u}_1$ by Theorem 5.12, while in cases $e/2 = 2^k,\ k \geq 2$ we found $x_1 \in \langle \underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4 \rangle$ as a linear combination of exactly three basis vectors, while $y_1 \in \underline{u}_1 + \langle \underline{u}_5, \underline{u}_6, \ldots, \underline{u}_{e/2} \rangle$. (Theorems 5.13, 5.14, 5.17, and Remark after Theorem 5.14) Using these constructions we define the vectors $x, y \in V$ as follows.

Theorem 5.19. *Using the vectors $x_1, y_1 \in V_1$ defined above let*

$$\begin{aligned} &x = x_1, && y = \underline{v}_1 + y_1, && \text{in cases } e/2 \neq 2^k \text{ or } e/2 = 2; \\ &x = \underline{v}_1 + x_1, && y = y_1, && \text{in cases } e/2 = 2^k,\ k \geq 2. \end{aligned}$$

Then $C_G(x) \cap C_G(y) = 1$.

Proof. First, let $e/2 \neq 2^k$ or $e/2 = 2$. Choosing a $g \in C_G(x) \cap C_G(y)$ it normalizes the subgroup $C_F(x) = C_F(\underline{u}_1) = D_0$, so it permutes the homogeneous components of D_0, that is, the subspaces $W_1, W_2, \ldots, W_{e/2}$. Then it is clear from the construction of y that g also centralizes $\underline{v}_1$, so the restriction of g to W_1 is the identity. As g permutes the subspaces $W_1, W_2, \ldots, W_{e/2}$, it follows that g can be written in a unique way as a product $g = \delta_2(g)\pi_2(g)$, where $\delta_2(g)$ is a 2-block diagonal matrix, while $\pi_2(g) = \pi(g) \otimes I_2$, where $\pi(g)$ denotes the permutation action of g on the set $\{W_1, W_2, \ldots, W_{e/2}\}$. Similarly to part *3* of Lemma 5.11 one can prove that $[\delta_2(g), S] \leq QD$. Now, if $\underline{u}_i$ appears with a non-zero coefficient in y, then the i-th block of $\delta_2(g)$ must be a lower triangular matrix. From our constructions given in Theorem 5.12 (see also parts *a)* and *b)* of Corollary 5.7) it follows that more than half of the blocks of $\delta_2(g)$ are lower triangular matrices. Therefore, for any

$s \in S$ at least one block of $[\delta_2(g), s] \in QD$ is a lower triangular matrix. Using part *6* of Theorem 5.18, we get $[\delta_2(g), s] \in D$ for every $s \in S$. Since the first block of $\delta_2(g)$ is the identity and S regularly permutes the blocks we get every block of $\delta_2(g)$ is a scalar matrix by part *5* of Theorem 5.18. In particular, $\delta_2(g)$ is a diagonal matrix. Hence g is a monomial matrix, and it fixes the subspace $V_1 = \langle \underline{u}_1, \underline{u}_2, \ldots, \underline{u}_{e/2} \rangle$. As $g_{V_1} \in C_{G_1}(x_1) \cap C_{G_1}(y_1) = 1_{V_1}$, we get g acts trivially on V_1, so $\pi(g) = 1$, and g is a diagonal matrix. Finally, using that the restriction of g to any W_i is a scalar matrix, and $g(\underline{u}_i) = \underline{u}_i$ for all i it follows that $g = 1$, what we wanted to prove.

In case of $e = 2^k,\ k \geq 2$ we claim that $C_F(x) = C_F(\underline{v}_1) \cap C_F(x_1) \leq D_0$. As the set of subspaces W_1, W_2, W_3, W_4 corresponds to a subspace of S, it follows that $C_F(x)$ permutes these subspaces. Now, for any $g \in C_F(x)$ there exist $\underline{u}_i, \underline{u}_j$ occuring in x with non-zero coefficients such that g moves $\underline{u}_i$ into a multiple of $\underline{u}_j$, so $\underline{u}_j$ is an eigenvector of the 2-block diagonal matrix $\delta_2(g) \in QD$ of g, hence $\delta_2(g)$ is a diagonal matrix by part *6* of Theorem 5.18. Consequently, g cannot take $\underline{v}_1$ into a multiple of some $\underline{u}_i$. So $C_F(x)$ fixes both $\underline{v}_1$ and x_1, which proves that $C_F(x) = C_F(\underline{v}_1) \cap C_F(x_1) \leq D_0$.

It follows that the homogeneous component corresponding to the trivial representation of $C_F(x) \leq D_0$ is just the subspace $W_1 \oplus W_2 \oplus W_3 \oplus W_4$, while the subspace generated by the other homogeneous components of $C_F(x)$ is $W_5 \oplus W_6 \oplus \cdots \oplus W_{e/2}$. Since any $g \in C_G(x) \cap C_G(y)$ normalizes $C_F(x)$, it fixes both $W_1 \oplus W_2 \oplus W_3 \oplus W_4$ and $W_5 \oplus W_6 \oplus \cdots \oplus W_{e/2}$. As y is of the form $y = \underline{u}_1 + \langle \underline{u}_5, \underline{u}_6, \ldots, \underline{u}_{e/2} \rangle$, it follows that $g(\underline{u}_1) = \underline{u}_1$, so g fixes the subspace W_1. Using the construction of x we get $g(\underline{v}_1) = \underline{v}_1$, so g acts trivially on W_1. From this point the proof is the same as it was for the previous case. □

5.3 Imprimitive linear groups

As before, let V be a finite vector space over $\mathbb{F}_p$ for some prime $p \neq 2$, and let $G \leq GL(V) \simeq GL(n, p)$ be a solvable linear group such that $(|G|, |V|) = 1$. In case of G is a

primitive linear group, the previous section gave us a base $x, y \in V$. Using this result, in this section we handle the case when G is not primitive as a linear group.

It follows from Maschke's theorem that V is a completely reducible G-module. The next obvious lemma reduces the problem to irreducible G-modules.

Lemma 5.20. *Let $V = V_1 \oplus V_2$ be the sum of two G-invariant subspaces. Then $G/C_G(V_i) \leq GL(V_i)$ acts faithfully on V_i. Using inductive hypothesis, for $i = 1, 2$ set $x_i, y_i \in V_i$ such that $C_G(x_i) \cap C_G(y_i) = C_G(V_i)$. Then $C_G(x_1 + x_2) \cap C_G(y_1 + y_2) = 1$.*

In the following let $G \leq GL(V)$ be an irreducible, imprimitive linear group. Thus, there is a decomposition $V = \oplus_{i=1}^{k} V_i$ such that $k \geq 2$ and G permutes the subspaces V_i in a transitive way. We can assume that the decomposition cannot be refined. For each $1 \leq i \leq k$ let $H_i = \{g \in G \mid gV_i = V_i\}$ be the stabilizer of V_i in G. Then $H_i/C_{H_i}(V_i) \leq GL(V_i)$ is a primitive linear group, and the subgroups H_i are conjugate in G. Of course, $(|H_1|, |V_1|) = 1$, so, using the previous section we can find vectors $x_1, y_1 \in V_1$ such that $C_{H_1}(x_1) \cap C_{H_1}(y_1) = C_{H_1}(V_1)$. Let $\{g_1 = 1, g_2, \ldots, g_k\}$ be a set of left coset representatives for H_1 in G such that $V_i = g_i V_1$ for all $1 \leq i \leq k$ and let $x_i = g_i x_1$, $y_i = g_i y_1$. It is clear that $H_i = H_1^{g_i^{-1}}$ and $C_{H_i}(x_i) \cap C_{H_i}(y_i) = C_{H_i}(V_i)$.

Now, $N = \cap_{i=1}^{k} H_i$ is a normal subgroup of G, the quotient group G/N acts faithfully and transitively on the set $\{V_1, V_2, \ldots, V_k\}$, and $|G/N|$ is coprime to p. Using Theorem 5.5, we can choose a vector $(a_1, a_2, \ldots, a_k) \in \mathbb{F}_p^k$ such that only the identity element of G/N fixes this vector.

Theorem 5.21. *Let the vectors $x, y \in V$ be defined as*

$$x = \sum_{i=1}^{k} x_i, \qquad y = \sum_{i=1}^{k} (y_i + a_i x_i).$$

Then $C_G(x) \cap C_G(y) = 1$.

Proof. Let $g \in C_G(x) \cap C_G(y)$. Assuming that $gV_i = V_j$ for some $1 \leq i, j \leq k$ we get $gx_i = x_j$ and $g(y_i + a_i x_i) = (y_j + a_j x_j)$. Choose $g' = g_j^{-1} g g_i \in G$. Then

$$g'x_1 = x_1 \quad \text{and} \quad g'(y_1 + a_i x_1) = (y_1 + a_i x_1) + (a_j - a_i)x_1, \tag{5.1}$$

so g' stabilizes the subspace $\langle x_1, y_1 \rangle \leq V_1$. If $y_1 = cx_1$ for some $c \in \mathbb{F}_p$, then $g'y_1 = y_1$. Using Equation (5.1) we get $a_j = a_i$. Otherwise, $x_1, y_1 + a_i x_1$ form a basis of the $\langle g' \rangle$-invariant subspace $\langle x_1, y_1 \rangle$. With respect to this basis the restriction of g' to this subspace has matrix form

$$\begin{pmatrix} 1 & a_j - a_i \\ 0 & 1 \end{pmatrix}.$$

If $a_j - a_i \neq 0$, then this matrix has order p, so p divides the order of $g' \in G$, a contradiction. Hence in any case $a_i = a_j$ holds for $gV_i = V_j$, which exactly means that $gN \in G/N$ stabilizes the vector $(a_1, a_2, \ldots, a_k)$. It follows that $g \in N$. So $gx_i = x_i$ and $gy_i = y_i$ holds for any $1 \leq i \leq k$, and $g \in \cap_{i=1}^{k} C_{H_i}(V_i) = C_G(V) = 1$ follows. □

Bibliography

[1] C. A. M. André, Irreducible characters of finite algebra groups, *Matrices and group representations (Coimbra, 1998)*, 65–80, Textos Mat. Sér. B, 19, *Univ. Coimbra, Coimbra* 1999.

[2] M. Boyarchenko, Base change maps for unipotent algebra groups, available on-line at arXiv:math/0601133v1.

[3] D. J. Benson, *Representations and cohomology I.*, Cambridge University Press, 1991.

[4] S. Dolfi, Intersections of odd order Hall subgroups, Bull. London Math. Soc. **37** (2005) 67–74.

[5] S. Dolfi, Large orbits in coprime actions of solvable groups, Trans. Amer. Math. Soc. **360** (2008) 135–152.

[6] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; 2002 (http://www.gap-system.org)

[7] D. Gluck, Trivial set-stabilizers in finite permutation groups, Canad. J. Math. **35** (1983) 59–67.

[8] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, J. London Math. Soc. (2) **58** (1998) 603–618.

[9] Z. Halasi, On the characters and commutators of finite algebra groups, J. Algebra **275** (2004) 481–487.

[10] Z. Halasi, On the characters of the unit group of DN-algebras, J. Algebra **302** (2006) 678–685.

[11] Z. Halasi and P. P. Pálfy, On the number of conjugacy classes of some subgroups of the unitriangular group, in preparation.

[12] Z. Halasi and K. Podoski, On the orbits of solvable linear groups, available on-line at arXiv:0707.2873v1.

[13] G. Higman, Enumerating p-groups. I: Inequalities, Proc. London Math. Soc. **3** (1960) 24–30.

[14] I. M. Isaacs, *Character theory of finite groups*, Dover, New York, 1994.

[15] I. M. Isaacs, Characters of groups associated with finite algebras, J. Algebra **177** (1995), 708–730.

[16] I. M. Isaacs, Large orbits in actions of nilpotent groups, Proc. Amer. Math. Soc. **127** (1999) 45–50.

[17] N. Jacobson, *Lie Algebras*, Interscience Publishers, New York, 1962.

[18] E. I. Khukhro, *p-automorphisms of finite p-groups*, Cambridge University Press, Cambridge, 1997.

[19] H. Matsuyama, Another proof of Gluck's theorem, J. Algebra **247** (2002) 703–706.

[20] A. Moreto and T. Wolf, Orbit sizes, character degrees and Sylow subgroups, Adv. Math. **184** (2004) 18–36.

[21] P. P. Pálfy, Bounds for linear groups of odd order, Proc. Second Internat. Group Theory Conf., Bressanone/Brixen 1989, Suppl. Rend. Circ. Mat. Palermo **23** (1990) 253–263.

[22] L. Pyber, Asymptotic results for permutation groups, Groups and computation, DIMACS Ser. Discrete Math. Theoret. Comp. Sci. 11 (ed. L. Finkelstein and W. Kantor, Amer. Math. Soc., Providence, RI, 1993) 197–219.

[23] Á. Seress, The minimal base size of primitive solvable permutation groups, J. London Math. Soc. **53** (1996) 243–255.

[24] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer–Verlag, 1986.

[25] D. A. Suprunenko, Matrix groups, Amer. Math. Soc., Providence, RI, 1976.

[26] B. Szegedy, On the characters of the group of upper-triangular matrices, J. Algebra **186** (1996), 113–119.

[27] J. G. Thompson, $k(U_n(\mathbb{F}_q))$, web manuscript 1998.
Available on-line at http://www.math.ufl.edu/fac/thompson/kUnFq.pdf.

[28] A. Vera-Lopez and J. M. Arregi, Conjugacy classes in sylow p-subgroups of $GL(n, q)$, J. Algebra **152** (1992), 1-19

[29] A. Vera-Lopez and J. M. Arregi, Some algorithms for the calculation of conjugacy classes in the Sylow p-subgroups of $GL(n, q)$, J. Algebra **177** (1995) 899-925.

[30] A. Vera-Lopez and J. M. Arregi, Conjugacy classes in unitriangular matrices, Linear Algebra and its Applications **370** (2003) 85–124.

[31] E. P. Vdovin, Regular orbits of solvable linear p'-groups, Siberian Electronic Mathematical Reports **4** (2007) 345–360.

[32] A. J. Weir, Sylow p-subgroups of the general linear groups over finite fields of characteristic p, Proc. Amer. Math. Soc. **6** (1955) 454–464.

[33] T. Wolf, Large orbits of supersolvable linear groups, J. Algebra **215** (1999) 235–247.