Small self-centralizing subgroups in defect groups of finite classical groups

Pablo Luka

Technische Universität Kaiserslautern
Fachbereich Mathematik
AG Algebra, Geometrie und Computeralgebra

vom Fachbereich Mathematik der Technischen Universität Kaiserslautern
zur Verleihung des akademischen Grades Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation

1. Gutachter: Prof. Dr. Susanne Danz
2. Gutachter: Prof. Dr. Burkhard Külshammer

Datum der Disputation: 03.03.2017

D 386

Danksagung

Ich bedanke mich ganz besonders herzlich bei Prof. Dr. Susanne Danz für die hervorragende Betreuung. Sie hatte immer Zeit für mich und konnte mir auch stets weiterhelfen. Außerdem gilt mein Dank auch allen weiteren Personen, die mich bei dieser Arbeit unterstützt haben, insbesondere Prof. Dr. Gunter Malle und seiner Arbeitsgruppe.
Schließlich möchte ich mich auch besonders bei meiner Frau Katja für ihre Geduld und Unterstützung bedanken und dafür, dass sie mich immer wieder neu motiviert hat.

Contents

Preface **3**

1 Background **7**
- 1.1 Representations . . . 7
- 1.2 Vertices . . . 10
- 1.3 Blocks and defect groups . . . 13
- 1.4 Brauer pairs and Knörr's Theorem . . . 15
- 1.5 Puig's Question . . . 17
- 1.6 Finite classical groups . . . 18

2 Small self-centralizing subgroups in Sylow subgroups of classical groups **31**
- 2.1 Self-centralizing subgroups . . . 31
- 2.2 Rank, normal rank, and wreath products . . . 34
- 2.3 A particular Sylow subgroup of a given finite symmetric group . . . 38
- 2.4 Monomial matrices . . . 41
- 2.5 On Sylow subgroups of general linear groups . . . 43
- 2.6 On Sylow subgroups of symplectic, unitary, and orthogonal groups . . . 48
- 2.7 On Sylow subgroups of special and projective (special) linear groups . . . 57
  - 2.7.1 Reduction to the case $\ell \mid \gcd(n, q-1)$ . . . 57
  - 2.7.2 The setting . . . 58
  - 2.7.3 The groups . . . 59
  - 2.7.4 Exponents and elementary abelian normal subgroups . . . 61
  - 2.7.5 The centers . . . 63
  - 2.7.6 Results about small self-centralizing subgroups . . . 71

3 Bounding defect groups in terms of self-centralizing subgroups **79**
- 3.1 The self-centralizing-bounded-defect property . . . 79
- 3.2 Results for finite classical groups . . . 89
- 3.3 Results for the groups $G_2(q)$ and ${}^3D_4(q^3)$ . . . 96

4 On the vertices of the unipotent simple $\overline{\mathbb{F}}_\ell \, \mathrm{GL}_n(q)$-modules labeled by partitions $(n-1, 1)$ **99**
- 4.1 The module . . . 99
- 4.2 The theorem . . . 103
- 4.3 The proof . . . 104
  - 4.3.1 The case $q \equiv 1 \bmod 4$ . . . 106
  - 4.3.2 The case $q \equiv 3 \bmod 4$ . . . 109

Open problems **115**

Notation **117**

Index **121**

Bibliography **123**

Preface

This thesis deals with a branch of modular representation theory of finite groups. Given a finite group G and a field K, one obtains a K-vector space

$$\mathsf{KG} = \left\{ \sum\nolimits_{g \in G} a_g g \ : \ a_g \in K \right\}$$

with K-basis G. By extending the multiplication of G linearly to KG, this vector space is even a unitary associative algebra, the *group algebra* of G over K. A *module* of the group algebra KG is a finite-dimensional left module.
In modular representation theory of finite groups, one investigates such group algebras and their modules in the case that K has positive characteristic. More precisely, in this thesis, the underlying field K will always be the algebraic closure $\overline{\mathbb{F}}_\ell$ of the prime field $\mathbb{F}_\ell$ of characteristic ℓ, where ℓ is a prime number.

Given a subgroup H of G and an $\overline{\mathbb{F}}_\ell G$-module M, one can restrict the module structure of M from $\overline{\mathbb{F}}_\ell G$ to $\overline{\mathbb{F}}_\ell H$. This $\overline{\mathbb{F}}_\ell H$-module is denoted by $\mathrm{Res}^G_H(M)$. Now, M is called *relatively* H-*projective* if M is isomorphic to a direct summand of the $\overline{\mathbb{F}}_\ell G$-module $\overline{\mathbb{F}}_\ell G \otimes_{\overline{\mathbb{F}}_\ell H} \mathrm{Res}^G_H(M)$. This generalizes the concept of projectivity: M is projective if and only if it is relatively $\{1\}$-projective.
To each indecomposable module M one can associate a unique G-conjugacy class of ℓ-subgroups of G, which are called the *vertices* of M. In fact, an ℓ-subgroup V of G is a vertex of M if and only if M is relatively V-projective and V is minimal with this property with respect to inclusion. For example, the vertices of the trivial $\overline{\mathbb{F}}_\ell G$-module $\overline{\mathbb{F}}_\ell$ are precisely the Sylow ℓ-subgroups of G.

The group algebra $\overline{\mathbb{F}}_\ell G$ has an $\overline{\mathbb{F}}_\ell[G \times G]$-module structure via $(g, h) \cdot a := gah^{-1}$ for $g, h \in G$ and $a \in \overline{\mathbb{F}}_\ell G$. The indecomposable direct summands of this module are subalgebras of $\overline{\mathbb{F}}_\ell G$. They are called the *blocks* of $\overline{\mathbb{F}}_\ell G$ and they have the following property: Given an indecomposable $\overline{\mathbb{F}}_\ell G$-module M, there is a unique block B such that $B \cdot M \neq \{0\}$, and in fact, one has $e \cdot m = m$ for every $m \in M$, where e is the identity element in B. One says that M *lies* in the block B.
The *defect groups* of a block B of $\overline{\mathbb{F}}_\ell G$ are those vertices of indecomposable modules lying in B that are maximal with respect to inclusion. In fact, for every defect group D of an $\overline{\mathbb{F}}_\ell G$-block B there is always even a simple $\overline{\mathbb{F}}_\ell G$-module M such that D is a vertex of M. Blocks and defect groups are very important invariants of finite groups.

Every ℓ-subgroup of G occurs as a vertex of some indecomposable $\overline{\mathbb{F}}_\ell G$-module, but if one restricts to simple $\overline{\mathbb{F}}_\ell G$-modules, this is no longer true. More precisely, a theorem due to Reinhard Knörr shows that every vertex of a simple $\overline{\mathbb{F}}_\ell G$-module M is a self-centralizing subgroup of a defect group of the block that M lies in, see [45]. Thus, if the Sylow ℓ-subgroups of G are abelian, then the vertices of a simple $\overline{\mathbb{F}}_\ell G$-module are always the defect groups of the corresponding block. There are further properties of vertices of simple modules that do not apply to vertices of arbitrary modules. For example, a vertex V of a simple module contains every normal ℓ-subgroup of G.

Lluís Puig asked the question whether the order of the defect groups of a block B of $\overline{\mathbb{F}}_\ell G$ can always be bounded in terms of the order of the vertices of an arbitrary simple module lying in B. For $\ell = 2$, there are examples due to Karin Erdmann (see [25]) showing that this is not possible in general, whereas, for odd ℓ, no such examples are known. By work of Susanne Danz, Burkhard Külshammer, and Lluís Puig, it is known that the answer to this question is positive if G is a symmetric group. More precisely, given a prime number ℓ, a natural number n, and a simple $\overline{\mathbb{F}}_\ell \operatorname{Sym}(n)$-module M in a block of $\overline{\mathbb{F}}_\ell \operatorname{Sym}(n)$ with defect group D, one has $|D| \leq |V|!$ for the vertices V of M, see [55] and [17].

In this thesis, we mainly study the case where G is a finite classical group in non-defining characteristic. More precisely, we generalize Puig's original question by replacing the vertices occurring in his question by arbitrary self-centralizing subgroups of the defect groups, and investigate the set of finite classical groups with respect to this generalized question. We derive positive and negative answers to this generalized question.

Basically, the finite classical groups occur as isometry groups of geometries over finite fields, that is, groups of linear maps over finite fields that are invariant under non-degenerate reflexive sesquilinear forms. There are three types of such sesquilinear forms which lead to finite symplectic, unitary, and orthogonal groups, respectively. Together with the finite linear groups and certain subgroups and quotient groups, these groups form the finite classical groups. Their most important property is that each type provides an infinite family of finite simple groups.

This thesis is organized as follows:

In Chapter 1, we introduce the notation and known facts that we will use later on. Here, we start with basics from modular representation theory such as representations, vertices, blocks, and defect groups. Then, we consider Brauer pairs and Puig's Question, followed by a brief introduction to finite classical groups and a remark on Chevalley groups and twisted Chevalley groups, since we will also consider two types of such groups in Chapter 3.

In the second chapter, we begin with a collection of auxiliary assertions about self-centralizing subgroups, ranks and normal ranks, and wreath products. Moreover, we introduce a particular Sylow subgroup of a given finite symmetric group that will be

very important in Section 2.7.
After that, we consider the Sylow subgroups of finite classical groups in non-defining characteristic and investigate whether it is possible to bound the order of such Sylow subgroups in terms of arbitrary self-centralizing subgroups. For most of the finite classical groups, we can reduce this problem to the general linear groups.
However, in order to answer this question for special linear and projective (special) linear groups, we develop some structural results about the Sylow subgroups of these groups. In particular, we show that it is not possible to bound the order of a Sylow ℓ-subgroup of $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, or $\mathrm{PSL}_n(q)$ if and only if $\ell \mid q-1$ and $n > 1$ is a power of ℓ, except in the case $\ell = 2$ and $q \equiv 3 \bmod 4$, which remains open. We also use this result to prove a similar behaviour of special unitary and projective (special) unitary groups.

In Chapter 3, we first define properties of arbitrary sets of finite groups according to Puig's original question as well as our generalized version where vertices are replaced by arbitrary self-centralizing subgroups. This is followed by auxiliary assertions that we will finally use to present our results for various sets of finite classical groups.
In particular, we show that for $\ell > 2$, the answer to our generalized question is positive for all finite classical groups of symplectic and orthogonal type such that the defining characteristic is odd. Moreover, the same is true for finite general linear and finite general unitary groups. However, our results from Chapter 2 show that the answer to our generalized question is negative if we consider special linear, projective (special) linear, special unitary, or projective (special) unitary groups. For $\ell > 2$, the answer to Puig's original question remains open for those groups.
In addition to sets of finite classical groups, we also consider the set of Chevalley groups $G_2(q)$ and the set of twisted Chevalley groups ${}^3D_4(q)$ in non-defining characteristic.

The fourth chapter is independent of the previous two chapters. Here, we consider the unique non-trivial composition factor D of the permutation $\overline{\mathbb{F}}_\ell \mathrm{GL}_n(q)$-module corresponding to the action of $\mathrm{GL}_n(q)$ on the one-dimensional subspaces of $\mathbb{F}_q^n$. With the notation from [41], this is the unipotent simple $\overline{\mathbb{F}}_\ell \mathrm{GL}_n(q)$-module labeled by the partition $(n-1,1)$, and it can be seen to be the analogue of the simple $\overline{\mathbb{F}}_\ell \mathrm{Sym}(n)$-module labeled by the partition $(n-1,1)$. For the latter, the vertices are known by work of Jürgen Müller and René Zimmermann, see [51].
We determine the vertices of D for $\ell = n = 2$ using a method from [10] known as Brauer construction. In fact, we show that if $q \equiv 1 \bmod 4$, then a vertex of D is a central product of $O_2(\mathbb{F}_q^\times)$ and the dihedral group of order 8 with respect to a central subgroup of order 2, whereas, if $q \equiv 3 \bmod 4$, then the vertices are the Sylow 2-subgroups of $\mathrm{SL}_2(q)$.

Finally, we collect some open problems that occurred while working on this subject.

1 Background

The reader is assumed to be familiar with the standard notation from group theory and representation theory. Notation is also explained on pages 117 to 119.

In this first chapter, we will provide the representation-theoretic background for this thesis. Moreover, we will introduce classical groups, whose Sylow subgroups we will consider. The first four sections are based on [2] and [52]. Section 1.6 is based on [5], [33], [40], and [58].

1.1 Representations

In this section, let K be an arbitrary field, and let G be a finite group. We begin by introducing group algebras and representations.

Remark 1.1.1.

(a) If Ω is a finite set, then $\mathsf{K}\Omega := \mathrm{Map}(\Omega, \mathsf{K})$ is a K-vector space with respect to pointwise operation. By identifying $\omega \in \Omega$ with the map $\Omega \to \mathsf{K} : x \mapsto \delta_{\omega x}$, where δ denotes the Kronecker delta, we obtain

$$\mathsf{K}\Omega = \left\{ \sum_{\omega \in \Omega} a_\omega \omega \ : \ a_\omega \in \mathsf{K} \right\},$$

and Ω is a K-basis of $\mathsf{K}\Omega$.

For $\Omega = \mathsf{G}$, we obtain additionally that KG is a unitary associative K-algebra with respect to the multiplication

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) := \sum_{g,h \in G} a_g b_h gh = \sum_{g \in G} \sum_{\substack{h,k \in G \\ hk = g}} a_h b_k g,$$

the ***group algebra of*** G ***over*** K.

(b) If $\mathsf{G} \times \Omega \to \Omega$ is a group action, then

$$\left(\sum_{g \in G} a_g g \right) \cdot \omega := \sum_{g \in G} a_g (g\omega)$$

induces a left KG-module structure on $\mathsf{K}\Omega$. This module $\mathsf{K}\Omega$ is then called a ***permutation module***. For the regular group action we obtain the regular left KG-module KG.

(c) A ***representation of*** G ***over*** K is a group homomorphism $G \to \mathrm{GL}_K(V)$ for some finite-dimensional K-vector space V.
Two such representations $\Delta_1 : G \to \mathrm{GL}_K(V)$ and $\Delta_2 : G \to \mathrm{GL}_K(W)$ are called ***similar to each other***, if there exists some K-vector space isomorphism $f : W \to V$ satisfying $\Delta_1(g) = f \circ \Delta_2(g) \circ f^{-1}$ for all $g \in G$.

(d) A ***matrix representation of*** G ***over*** K is a group homomorphism $G \to \mathrm{GL}_n(K)$ for some $n \in \mathbb{N}$.
Two such matrix representations $\Gamma_1 : G \to \mathrm{GL}_n(K)$ and $\Gamma_2 : G \to \mathrm{GL}_m(K)$ are called ***similar to each other***, if there exists some $A \in \mathrm{GL}_n(K)$ such that $\Gamma_1(g) = A\Gamma_2(g)A^{-1}$ for all $g \in G$ (in particular, m and n have then to be equal).

The following easily verified proposition shows that the study of (matrix) representations of G over K is equivalent to the study of the finite-dimensional left KG-modules.

Proposition 1.1.2.

(a) *If* $\Delta : G \to \mathrm{GL}_K(V)$ *is a representation of* G *over* K *and* $(v_1, \dots, v_n)$ *is an ordered* K*-basis of* V*, then for* $g \in G$ *we can define the matrix* $\Lambda(g) = (\Lambda(g)_{ij})_{i,j}$ *by*

$$\Delta(g)(v_j) = \sum_{i=1}^{n} \Lambda(g)_{ij} v_i,$$

and obtain a matrix representation $\Lambda : G \to \mathrm{GL}_n(K)$ *of* G *over* K*. Choosing another ordered* K*-basis of* V *or replacing* Δ *by a representation similar to* Δ *yields a matrix representation similar to* Λ*.*

(b) *If* $\Lambda : G \to \mathrm{GL}_n(K)$ *is a matrix representation of* G *over* K*, then* K^n *is a left* KG*-module via* $g \cdot e_i := \sum_{j=1}^{n} \Lambda(g)_{ij} e_j$*, where* $(e_1, \dots, e_n)$ *is the standard basis of* K^n*. Replacing* Λ *by a matrix representation similar to* Λ *yields a left* KG*-module structure on* K^n *such that the two modules are isomorphic to each other.*

(c) *If* M *is a left* KG*-module with* $\dim_K(M) < \infty$*, then*

$$\Delta : G \to \mathrm{GL}_K(M) : g \mapsto (m \mapsto g \cdot m)$$

is a representation of G *over* K*. Replacing* M *by a left* KG*-module isomorphic to* M *yields a representation similar to* Δ*.*

(d) *Starting with a representation of* G *over* K *and applying parts (a), (b), and (c) of this proposition successively, we obtain a representation similar to the original one.*

In this thesis, we choose the module-theoretic point of view, and from now on, by a KG-***module*** we will always mean a finite-dimensional left KG-module.
As we can consider the set of all matrix representations of G over K and use that

similarity defines an equivalence relation on this set, it follows from Proposition 1.1.2 that the set of isomorphism classes of KG-modules exists.

If H is a subgroup of G, then for each $g \in G$, every KH-module X is also a $K[{}^gH]$-module via $a \bullet x := (g^{-1}ag)x$ for $a \in K[{}^gH]$ and $x \in X$, where ${}^gH = gHg^{-1}$ is the conjugate of H by g. The latter module is then denoted by ${}^gX$ and we say that it is ***conjugate to*** X. If g belongs to H, then the KH-modules X and ${}^gX$ are isomorphic to each other.
Moreover, if H is normal in G, then G acts by conjugation on the set of isomorphism classes of KH-modules. The stabilizer subgroup

$$\{g \in G \;:\; {}^gX \cong X \text{ as } KH\text{-modules}\}$$

of a given KH-module X is called the ***inertia group of*** X and contains H.

Again, let H be a subgroup of G. Then every KG-module M is also a KH-module by restricting its scalar multiplication to the group algebra KH. This KH-module is then denoted by $\mathrm{Res}^G_H(M)$ and is called the ***restriction of*** M ***to*** H. Moreover, if X is a KH-module, then the KG-module $\mathrm{Ind}^G_H(X) := KG \otimes_{KH} X$ is called the ***induction of*** X ***to*** G.

For two subgroups U and H of G, the group $U \times H$ acts on G via $(u, h) \cdot g := ugh^{-1}$ for $u \in U$, $h \in H$, and $g \in G$. The orbit of an element $g \in G$ is the ***double coset*** UgH. The set of all such double cosets is denoted by $U\backslash G/H := \{UgH \;:\; g \in G\}$. Mackey's Theorem provides a relation between restriction and induction:

Theorem 1.1.3 ([52, Thm. 2.1.9])**.** *Let U and H be subgroups of G, and let S be a set of representatives for $U\backslash G/H$. Then for every KH-module X, we have*

$$\mathrm{Res}^G_U(\mathrm{Ind}^G_H(X)) \cong \bigoplus_{s \in S} \mathrm{Ind}^U_{{}^sH\cap U}(\mathrm{Res}^{{}^sH}_{{}^sH\cap U}({}^sX)).$$

By definition, the ***kernel*** of a KG-module is the kernel of a corresponding representation. Let H be a normal subgroup of G. Then every $K[G/H]$-module M is also a KG-module via $g \bullet m := gH \cdot m$ for $g \in G$ and $m \in M$. This KG-module is denoted by $\mathrm{Inf}^G_{G/H}(M)$ and it is called the ***inflation of*** M ***to*** G. It is easily verified that inflation induces a bijection between the set of isomorphism classes of $K[G/H]$-modules and the set of isomorphism classes of those KG-modules whose kernel contains H.

Now, let M be a KG-module. If $L|K$ is a field extension, then $M^L := L \otimes_K M$ is an LG-module, called the ***scalar extension of*** M ***to*** L. In the language of matrix representations, this corresponds to viewing a matrix representation $G \to \mathrm{GL}_n(K) \subseteq \mathrm{GL}_n(L)$ of G over K as a matrix representation of G over L.

The module M is called ***simple*** or ***irreducible***, if M is not the zero module and if M and $\{0\}$ are the only submodules of M. Moreover, M is called ***absolutely simple*** or ***absolutely irreducible***, if M^L is simple for all field extensions $L|K$.
Finally, K is called a ***splitting field for*** G, if every simple KG-module is absolutely simple. In this case, every field extension L of K is also a splitting field for G, and the number of isomorphism classes of the simple KG-modules is then the same as the corresponding number for LG-modules.

We recall that the ***exponent*** $\mathrm{Exp}(G)$ is the least $k \in \mathbb{N}_{>0}$ such that $g^k = 1$ for all $g \in G$. The following theorem shows how to find a splitting field L for G and also determines the number of simple LG-modules.

Theorem 1.1.4 ([39, Cor. 2.7, Cor. 9.15, Thm. 10.3], [48, Thm. 8.9]). *Let $\ell \in \mathbb{P} \cup \{0\}$, let F be the prime field of characteristic ℓ, and let L be the splitting field of the polynomial $t^{\mathrm{Exp}(G)} - 1 \in F[t]$ over F.*

(a) *The field L is a splitting field for G. In particular, the algebraic closure of F is a splitting field for all finite groups.*

(b) *The number of isomorphism classes of the simple LG-modules is the number of conjugacy classes of G whose elements have order not divisible by ℓ.*

In this thesis, we will consider group algebras over the algebraic closure $\overline{\mathbb{F}}_\ell$ of the finite field $\mathbb{F}_\ell$, for prime numbers $\ell \in \mathbb{P}$.

1.2 Vertices

Now, we recall the concept of projectivity. In this section, let G be a finite group and let $\ell \in \mathbb{P}$ be fixed.

Proposition 1.2.1 ([52, Thm. 1.10.2]). *For an $\overline{\mathbb{F}}_\ell G$-module M, the following statements are equivalent:*

(a) *Every short exact sequence $0 \to L \to N \to M \to 0$ of $\overline{\mathbb{F}}_\ell G$-modules splits.*

(b) *If $f \in \mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(N, L)$ is surjective, then so is the map*

$$\mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(M, N) \to \mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(M, L) : g \mapsto f \circ g.$$

(c) *M is isomorphic to a direct summand of a free $\overline{\mathbb{F}}_\ell G$-module.*

In the situation of Proposition 1.2.1, M is called ***projective***. Moreover, an $\overline{\mathbb{F}}_\ell G$-module M is called ***indecomposable***, if M is not the zero module and if M is not the direct sum of two submodules different from the zero module. Finally, the ***Jacobson radical***

$\mathrm{Rad}(M)$ is the intersection of all maximal submodules of M (or the zero module, if M itself is the zero module).

The next theorem shows how projective indecomposable modules are related to simple modules:

Theorem 1.2.2 ([27, Cor. I.13.6])**.** *If M is a projective indecomposable $\overline{\mathbb{F}}_\ell G$-module, then its head $M/\mathrm{Rad}(M)$ is simple. Moreover, this induces a bijection between the set of isomorphism classes of projective indecomposable $\overline{\mathbb{F}}_\ell G$-modules and the set of isomorphism classes of simple $\overline{\mathbb{F}}_\ell G$-modules.*

The following generalizes the concept of projectivity:

Proposition 1.2.3 ([52, Thm. 4.2.2])**.** *Let H be a subgroup of G, and let M be an $\overline{\mathbb{F}}_\ell G$-module. The following statements are equivalent:*

(a) *If*
$$0 \to L \to N \to M \to 0$$
is a short exact sequence of $\overline{\mathbb{F}}_\ell G$-modules such that the short exact sequence
$$0 \to \mathrm{Res}^G_H(L) \to \mathrm{Res}^G_H(N) \to \mathrm{Res}^G_H(M) \to 0$$
of $\overline{\mathbb{F}}_\ell H$-modules splits, then the first sequence splits, as well.

(b) *If $f \in \mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(N, L)$ is surjective such that*
$$\mathrm{Hom}_{\overline{\mathbb{F}}_\ell H}(M, N) \to \mathrm{Hom}_{\overline{\mathbb{F}}_\ell H}(M, L) : g \mapsto f \circ g$$
is surjective, then so is the map
$$\mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(M, N) \to \mathrm{Hom}_{\overline{\mathbb{F}}_\ell G}(M, L) : g \mapsto f \circ g.$$

(c) *M is isomorphic to a direct summand of $\mathrm{Ind}^G_H(\mathrm{Res}^G_H(M))$.*

(d) *M is isomorphic to a direct summand of $\mathrm{Ind}^G_H(L)$ for some $\overline{\mathbb{F}}_\ell H$-module L.*

(e) *If $\{s_1, \dots, s_r\}$ is a set of representatives for the set G/H of left cosets, then the image of the map*
$$\mathrm{End}_{\overline{\mathbb{F}}_\ell H}(M) \to \mathrm{End}_{\overline{\mathbb{F}}_\ell G}(M) : f \mapsto s_1 f + \cdots + s_r f$$
contains id_M. Here, for every i, the map $s_i f$ is defined by $(s_i f)(m) := s_i \cdot f(s_i^{-1} m)$ for $m \in M$.

In the situation of Proposition 1.2.3, M is called ***relatively*** ***H-projective***. Obviously, M is projective if and only if M is relatively $\{1\}$-projective. We have the following properties:

Proposition 1.2.4 ([52, Lem. 4.2.1, Thm. 4.2.5, Thm. 4.7.5]). *Let* H *be a subgroup of* G.

(a) *If* $\ell \nmid |\mathsf{G} : \mathsf{H}|$*, then every* $\overline{\mathbb{F}}_\ell\mathsf{G}$*-module is relatively* H*-projective.*

(b) *If an* $\overline{\mathbb{F}}_\ell\mathsf{G}$*-module is relatively* U*-projective for some subgroup* U *of* H*, then it is also relatively* H*-projective.*

(c) *If an* $\overline{\mathbb{F}}_\ell\mathsf{G}$*-module is relatively* H*-projective, then it is also relatively* ${}^{\mathsf{g}}\mathsf{H}$*-projective for all* $\mathsf{g} \in \mathsf{G}$.

(d) *Let* $\mathsf{S} \in \mathrm{Syl}_\ell(\mathsf{G})$*, and let* U *be a subgroup of* S *such that* M *is relatively* U*-projective. Then* $|\mathsf{S} : \mathsf{U}|$ *divides* $\dim_{\overline{\mathbb{F}}_\ell}(\mathsf{M})$.

Theorem 1.2.5 ([52, Thm. 4.3.3]). *Let* M *be an indecomposable* $\overline{\mathbb{F}}_\ell\mathsf{G}$*-module. There exists a unique* G*-conjugacy class* $\mathrm{Vx}(\mathsf{M})$ *of* ℓ*-subgroups of* G *satisfying the following: For every subgroup* H *of* G *one has that* M *is relatively* H*-projective if and only if there exists some* $\mathsf{Q} \in \mathrm{Vx}(\mathsf{M})$ *satisfying* $\mathsf{Q} \subseteq \mathsf{H}$.

In the situation of the previous theorem, we call the elements of $\mathrm{Vx}(\mathsf{M})$ the ***vertices of*** M. The theory of vertices goes back to J. A. Green.

It follows that if ℓ does not divide the group order $|\mathsf{G}|$, then every $\overline{\mathbb{F}}_\ell\mathsf{G}$-module is projective, that is, the group algebra $\overline{\mathbb{F}}_\ell\mathsf{G}$ is then semisimple. This statement is known as Maschke's Theorem.

We can say that vertices somehow "measure" how far the corresponding indecomposable module is from being projective: the smaller the order of the vertices, the closer the corresponding module is to being projective.
We should also mention that every ℓ-subgroup of G occurs as a vertex of an indecomposable module (see, for example, [52, Thm. 4.7.7]).

Later on, we will make use of the following facts about vertices:

Proposition 1.2.6 ([52, Lem. 4.3.4, Lem. 4.3.5, Thm. 4.7.8]). *Let* M *be an indecomposable* $\overline{\mathbb{F}}_\ell\mathsf{G}$*-module, and let* H *be a subgroup of* G.

(a) *Let* N *be an indecomposable* $\overline{\mathbb{F}}_\ell\mathsf{H}$*-module such that* M *is isomorphic to a direct summand of* $\mathrm{Ind}_{\mathsf{H}}^{\mathsf{G}}(\mathsf{N})$*. Then every vertex of* M *is contained in a* G*-conjugate of a vertex of* N.

(b) *Let* N *be an indecomposable* $\overline{\mathbb{F}}_\ell\mathsf{H}$*-module such that* N *is isomorphic to a direct summand of* $\mathrm{Res}_{\mathsf{H}}^{\mathsf{G}}(\mathsf{M})$*. Then every vertex of* N *is contained in a vertex of* M.

(c) *If* M *is relatively* H*-projective, then there exists an indecomposable* $\overline{\mathbb{F}}_\ell\mathsf{H}$*-module* N *satisfying parts (a) and (b). In particular, then every vertex of* N *is also a vertex of* M.

(d) *If* M *is simple, then the vertices of* M *contain every normal* ℓ*-subgroup of* G.

1.3 Blocks and defect groups

In this section, we introduce blocks of group algebras as well as their defect groups. As before, let G be a finite group.

Let K be a field. An element $e \in KG$ satisfying $e^2 = e$ is called an ***idempotent***. Two idempotents $e, f \in KG$ are ***orthogonal***, if $ef = 0$. A non-zero idempotent in KG is ***primitive***, if it cannot be written as the sum of two orthogonal idempotents $e, f \in KG \setminus \{0\}$. There are only finitely many primitive idempotents $e_1, \ldots, e_r$ of the center $Z(KG)$ which are called the ***block idempotents of*** KG. They are pairwise orthogonal and satisfy $e_1 + \cdots + e_r = 1$.
Now, for each $i \in \{1, \ldots, r\}$, the subset KGe_i of KG, called a ***block of*** KG, is a subalgebra with identity element e_i, and we have $KG = \bigoplus_{i=1}^{r} KGe_i$. In particular, if M is an indecomposable KG-module, then there exists a unique block KGe_i such that $e_iM \neq \{0\}$, and in this case we even have $e_im = m$ for all $m \in M$. We then say that M ***lies in the block*** KGe_i. The set of blocks of KG is denoted by $\mathrm{Bl}(KG)$. The ***principal block of*** KG is the one the trivial KG-module K lies in.

Now, we fix a prime number $\ell \in \mathbb{P}$ and consider the field $\overline{\mathbb{F}}_\ell$. The group algebra $\overline{\mathbb{F}}_\ell G$ is an $\overline{\mathbb{F}}_\ell[G \times G]$-module via $(g, h) \cdot a := gah^{-1}$ for $g, h \in G$ and $a \in \overline{\mathbb{F}}_\ell G$, and the indecomposable direct summands of $\overline{\mathbb{F}}_\ell G$ as an $\overline{\mathbb{F}}_\ell[G \times G]$-module are precisely the blocks of $\overline{\mathbb{F}}_\ell G$ (see, for instance, [27, page 133]).
Given $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$, every vertex of B as an indecomposable $\overline{\mathbb{F}}_\ell[G \times G]$-module is the image of a unique subgroup D of G under the diagonal map $G \to G \times G : g \mapsto (g, g)$ (see, for example, [2, Thm. 13.4]). One calls such a group G a ***defect group of*** B and we denote the set of all defect groups of B by $\mathrm{Def}(B)$. Then $\mathrm{Def}(B)$ is a G-conjugacy class of ℓ-subgroups of G.

We will use the following important properties of defect groups:

Proposition 1.3.1 ([2, Thm. 13.5, Cor. 14.5], [52, Thm. 3.6.25, Thm. 5.1.9, Thm. 5.1.11], [50], [24])**.** *Let* $\ell \in \mathbb{P}$*, and let* $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$.

(a) $\mathrm{Def}(B)$ *is the set of those* ℓ*-subgroups of* G *that occur as vertices of indecomposable* $\overline{\mathbb{F}}_\ell G$*-modules lying in* B *and that are maximal with respect to inclusion.*

(b) $\mathrm{Def}(B)$ *is the set of those* ℓ*-subgroups of* G *that occur as vertices of simple* $\overline{\mathbb{F}}_\ell G$*-modules lying in* B *and that are maximal with respect to inclusion.*

(c) *If the defect groups of* B *are cyclic, then every simple* $\overline{\mathbb{F}}_\ell G$*-module* M *lying in* B *satisfies* $\mathrm{Vx}(M) = \mathrm{Def}(B)$.

(d) *If a simple* $\overline{\mathbb{F}}_\ell \mathsf{G}$*-module* M *lying in* B *has cyclic vertices, then* $\mathrm{Vx}(\mathsf{M}) = \mathrm{Def}(\mathsf{B})$.

For example, it follows from part (a) of Proposition 1.3.1 and part (d) of Proposition 1.2.6 that if an indecomposable $\overline{\mathbb{F}}_\ell \mathsf{G}$-module M lying in B satisfies $\ell \nmid \dim_{\overline{\mathbb{F}}_\ell}(\mathsf{M})$, then $\mathrm{Def}(\mathsf{B}) = \mathrm{Syl}_\ell(\mathsf{G})$. In particular, this applies to the principal block.

It should be mentioned that part (c) is known as Michler's Theorem and part (d) is known as Erdmann's Theorem. We will see later a theorem due to Reinhard Knörr that generalizes Michler's Theorem.

The following lemma will be used in Section 3.1:

Lemma 1.3.2. *Let* $\ell \in \mathbb{P}$*, and let* H *be a finite group. Then the algebras* $\overline{\mathbb{F}}_\ell[\mathsf{G} \times \mathsf{H}]$ *and* $\overline{\mathbb{F}}_\ell \mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \overline{\mathbb{F}}_\ell \mathsf{H}$ *are isomorphic, and the blocks of* $\overline{\mathbb{F}}_\ell[\mathsf{G} \times \mathsf{H}]$ *correspond to tensor products* $\mathsf{B}_\mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \mathsf{B}_\mathsf{H}$ *of blocks* B_G *of* $\overline{\mathbb{F}}_\ell \mathsf{G}$ *and* B_H *of* $\overline{\mathbb{F}}_\ell \mathsf{H}$*. Moreover, the defect groups of* $\mathsf{B}_\mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \mathsf{B}_\mathsf{H}$ *are then of the form* $\mathsf{D}_{\mathsf{B}_\mathsf{G}} \times \mathsf{D}_{\mathsf{B}_\mathsf{H}}$*, where* $\mathsf{D}_{\mathsf{B}_\mathsf{G}} \in \mathrm{Def}(\mathsf{B}_\mathsf{G})$ *and* $\mathsf{D}_{\mathsf{B}_\mathsf{H}} \in \mathrm{Def}(\mathsf{B}_\mathsf{H})$.

Proof. It is well known that $(g, h) \mapsto g \otimes h$ defines an isomorphism $\overline{\mathbb{F}}_\ell[\mathsf{G} \times \mathsf{H}] \cong \overline{\mathbb{F}}_\ell \mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \overline{\mathbb{F}}_\ell \mathsf{H}$, and the form of the blocks follows from [60, Lem. 1]. If D is a defect group of $\mathsf{B}_\mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \mathsf{B}_\mathsf{H}$, then D is maximal among the vertices of simple modules in $\mathsf{B}_\mathsf{G} \otimes_{\overline{\mathbb{F}}_\ell} \mathsf{B}_\mathsf{H}$, which are tensor products of simple modules in B_G and B_H by [38, VII.9.14], and whose vertices are direct products of the corresponding vertices by [46, Prop. 1.2]. $\square$

Next, we come to the important concepts of block induction and covering of blocks:

First, let H be any subgroup of G. Given two blocks $\mathsf{b} \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell \mathsf{H})$ and $\mathsf{B} \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell \mathsf{G})$, we say that b^G ***is defined*** and write $\mathsf{b}^\mathsf{G} = \mathsf{B}$, if B is the unique block of $\overline{\mathbb{F}}_\ell \mathsf{G}$ such that the $\overline{\mathbb{F}}_\ell[\mathsf{H} \times \mathsf{H}]$-module b is isomorphic to a direct summand of $\mathrm{Res}^{\mathsf{G}\times\mathsf{G}}_{\mathsf{H}\times\mathsf{H}}(\mathsf{B})$. We then also say that we obtain B from b via ***block induction***. If $\mathrm{C}_\mathsf{G}(\mathsf{D}) \subseteq \mathsf{H}$ for some $\mathsf{D} \in \mathrm{Def}(\mathsf{b})$, then b^G is defined and D is contained in some defect group of b^G (see, for example, [2, Lem. 1]).

Now, suppose that H is normal in G. Then we say that a block $\mathsf{B} \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell \mathsf{G})$ ***covers*** a block $\mathsf{b} \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell \mathsf{H})$, if the product of the corresponding block idempotents e_B and e_b is non-zero.

Remark 1.3.3. Writing $1 \in \overline{\mathbb{F}}_\ell \mathsf{G}$ as the sum of all blocks idempotents in $\overline{\mathbb{F}}_\ell \mathsf{H}$ and multiplying this equation with a given block idempotent of $\overline{\mathbb{F}}_\ell \mathsf{G}$, we see that every block of $\overline{\mathbb{F}}_\ell \mathsf{G}$ covers some block of $\overline{\mathbb{F}}_\ell \mathsf{H}$, see [52, Lem. 5.5.3]. The analogous argument shows also that each block of $\overline{\mathbb{F}}_\ell \mathsf{H}$ is covered by some block of $\overline{\mathbb{F}}_\ell \mathsf{G}$.

We obtain the following further properties:

Proposition 1.3.4 ([52, Section 5.5.1], [2, Thm. 15.1, Lem. 15.3])**.** *Let* $\ell \in \mathbb{P}$*, and let* H *be a normal subgroup of* G.

(a) G *acts on the blocks of* $\overline{\mathbb{F}}_\ell H$ *by conjugation. For every* $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$*, the blocks of* $\overline{\mathbb{F}}_\ell H$ *covered by* B *form a single* G*-conjugacy class.*

(b) *If* $b \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell H)$ *is covered by* $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$*, then each defect group of* b *is the intersection of* H *with some defect group of* B*.*

(c) *If* $b \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell H)$ *such that* b^G *is defined, then* b^G *is the unique block of* $\overline{\mathbb{F}}_\ell G$ *covering* b*.*

Finally, we introduce domination of blocks: Again, let H be normal in G, and let e be a block idempotent of $\overline{\mathbb{F}}_\ell G$. By μ we denote the residue class epimorphism $\mu : \overline{\mathbb{F}}_\ell G \to \overline{\mathbb{F}}_\ell[G/H]$ defined by $g \mapsto gH$. Suppose that $\mu(e) \neq 0$. Then $\mu(e)$ is a sum of block idempotents $f_1, \dots, f_r$ of $\overline{\mathbb{F}}_\ell[G/H]$. We say that the $\overline{\mathbb{F}}_\ell[G/H]$-blocks corresponding to $f_1, \dots, f_r$ are ***dominated*** by the $\overline{\mathbb{F}}_\ell G$-block $\overline{\mathbb{F}}_\ell Ge$ corresponding to e. We will use the following fact:

Proposition 1.3.5 ([52, page 360, Thm. 8.7])**.** *Let* $\ell \in \mathbb{P}$*, let* H *be a normal subgroup of* G*, and let* $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell[G/H])$*. Then* B *is dominated by a unique block* $\tilde{B} \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$*. Moreover, for* $D \in \mathrm{Def}(B)$ *there exists some* $\tilde{D} \in \mathrm{Def}(\tilde{B})$ *such that* $D \leq \tilde{D}H/H$*.*

1.4 Brauer pairs and Knörr's Theorem

In this section, we introduce Brauer pairs and, in particular, a theorem due to Knörr (Theorem 1.4.7). The theory follows [2], [3], and [54].

Let G be a finite group, and let $\ell \in \mathbb{P}$ be fixed.

Lemma 1.4.1. *Let* $Q \leq G$ *be an* ℓ*-subgroup, and let* $b \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell(Q\,\mathrm{C}_G(Q)))$*. Then* b^G *is defined. Moreover, given* $D \in \mathrm{Def}(b)$ *and* $E \in \mathrm{Def}(b^G)$*, we have*

$$Q \leq D \leq_G E.$$

Proof. By Proposition 1.2.6 and Proposition 1.3.1, the normal ℓ-subgroup Q of $Q\,\mathrm{C}_G(Q)$ is contained in every defect group D of b, so $\mathrm{C}_G(D) \leq \mathrm{C}_G(Q) \leq Q\,\mathrm{C}_G(Q)$. Thus, b^G is defined and D is contained in a defect group of b^G. □

In the situation of Lemma 1.4.1, we call the tuple (Q, b) a ***(*b^G*-)Brauer pair of*** $\overline{\mathbb{F}}_\ell G$.

Next, let (R, b_R) and (Q, b_Q) be Brauer pairs of $\overline{\mathbb{F}}_\ell G$. Given $D \in \mathrm{Def}(b_Q)$ and $E \in \mathrm{Def}(b_R)$, then by what we have just seen we have $Q \subseteq D$ and $R \subseteq E$. So from

$$\mathrm{C}_{Q\,\mathrm{C}_G(R)}(D) \leq \mathrm{C}_G(D) \leq \mathrm{C}_G(Q) \leq Q\,\mathrm{C}_G(Q)$$

and

$$C_{Q\,C_G(R)}(E) \leq C_G(E) \leq C_G(R) \leq R\,C_G(R)$$

it follows that $b_Q^{Q\,C_G(R)}$ and $b_R^{Q\,C_G(R)}$ are defined.

- One writes $(R, b_R) \trianglelefteq (Q, b_Q)$ if $R \trianglelefteq Q$, $Q \subseteq \mathrm{Stab}_G(b_R)$, and $b_Q^{Q\,C_G(R)} = b_R^{Q\,C_G(R)}$. In this case, $b_Q^G = b_R^G =: B$ (see, for example, [2, page 114]), so (R, b_R) and (Q, b_Q) are B-Brauer pairs of $\overline{\mathbb{F}}_\ell G$.
- Moreover, we write $(R, b_R) \leq (Q, b_Q)$ if there exist Brauer pairs $(R_1, b_1), \ldots, (R_n, b_n)$ of $\overline{\mathbb{F}}_\ell G$ such that

$$(R, b_R) = (R_1, b_1) \trianglelefteq \cdots \trianglelefteq (R_n, b_n) = (Q, b_Q).$$

One obtains the following easily verified observation:

Observation 1.4.2. *Let $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$. Then $(\{1\}, B)$ is a B-Brauer pair of $\overline{\mathbb{F}}_\ell G$. The relation $\leq$ is a partial ordering on the set of all B-Brauer pairs of $\overline{\mathbb{F}}_\ell G$, and all such B-Brauer pairs (Q, b) satisfy $(\{1\}, B) \trianglelefteq (Q, b)$.*

Theorem 1.4.3 ([2, Thm. 16.3], [54, Prop. 1.9])**.** *Let (Q, b) be a Brauer pair of $\overline{\mathbb{F}}_\ell G$, and let $R \leq Q$. Then there exists a unique block $b_R \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell[R\,C_G(R)])$ such that $(R, b_R) \leq (Q, b)$. This block b_R has a defect group containing $R\,C_Q(R)$. If $R \trianglelefteq Q$, then also $(R, b_R) \trianglelefteq (Q, b)$.*

Definition 1.4.4. Let (Q, b) be a Brauer pair of $\overline{\mathbb{F}}_\ell G$.

(a) (Q, b) is called ***self-centralizing***, if Q is a defect group of b.

(b) (Q, b) is called ***a Sylow (b^G-)Brauer pair of*** $\overline{\mathbb{F}}_\ell G$, if Q is a defect group of b^G.

It follows immediately from Lemma 1.4.1 that every Sylow Brauer pair of $\overline{\mathbb{F}}_\ell G$ is self-centralizing.
The following is a version of Sylow's Theorem translated to our context:

Theorem 1.4.5 ([2, Thm. 16.2])**.** *Let (Q, b) be a Brauer pair of $\overline{\mathbb{F}}_\ell G$. Then (Q, b) is a Sylow b^G-Brauer pair of $\overline{\mathbb{F}}_\ell G$ if and only if (Q, b) is a maximal element of the set of all Brauer pairs of $\overline{\mathbb{F}}_\ell G$ with respect to $\leq$. Moreover, G acts transitively by conjugation on the set of all Sylow b^G-Brauer pairs of $\overline{\mathbb{F}}_\ell G$.*

The following application of Theorem 1.4.5 explains the term "self-centralizing" in part (a) of the previous definition:

Theorem 1.4.6. *A Brauer pair (Q, b) of $\overline{\mathbb{F}}_\ell G$ is self-centralizing if and only if, for all Brauer pairs (R, b_R) of $\overline{\mathbb{F}}_\ell G$ satisfying $(Q, b) \leq (R, b_R)$, we have $C_R(Q) \subseteq Q$.*

Proof. First, let (Q, b) be self-centralizing, and let (R, b_R) be such that $(Q, b) \leq (R, b_R)$. Then by Theorem 1.4.3, the defect group Q of b contains a $Q\,C_G(Q)$-conjugate of $Q\,C_R(Q)$. It follows that $C_R(Q) \subseteq Q$.
Now, we show the converse direction. Let D be a defect group of b. By Theorem 1.4.5, (Q, b_Q) is contained in a Sylow Brauer pair (E, b_E), and we have $C_E(Q) \subseteq Q$ by assumption. As

$$C_{N_G(Q)}(D) \subseteq C_G(D) \subseteq C_G(Q) \subseteq Q\,C_G(Q)$$

by Lemma 1.4.1, $b^{N_G(Q)}$ is defined, and it is the unique block of $\overline{\mathbb{F}}_\ell\, N_G(Q)$ covering b. From [2, Thm. 14.2] it follows that the defect group E of $b^G = (b^{N_G(Q)})^G$ is also a defect group of $b^{N_G(Q)}$. Now, [2, Thm. 15.1] implies that $D = {}^gE \cap Q\,C_G(Q)$, for some $g \in N_G(Q)$. Thus,

$$Q \subseteq {}^{g^{-1}}D = E \cap Q\,C_G(Q) = C_E(Q) \subseteq Q.$$

Now, this shows that $Q = {}^{g^{-1}}D$ and, thus, $Q = D$. □

Finally, we turn to Knörr's Theorem:

Theorem 1.4.7 (Knörr's Theorem, [45, Cor. 3.5])**.** *Let M be a simple $\overline{\mathbb{F}}_\ell G$-module in a block $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$ with vertex V. Then there exists a self-centralizing B-Brauer pair (V, b).*

Corollary 1.4.8. *Let M be a simple $\overline{\mathbb{F}}_\ell G$-module in a block $B \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell G)$ with vertex V. Then there exists some $D \in \mathrm{Def}(B)$ such that $C_D(V) \subseteq V \subseteq D$. In particular, if D is abelian, then $V = D$.*

Proof. By Knörr's Theorem, there exists a self-centralizing B-Brauer pair (V, b). By Theorem 1.4.6, there exists a Sylow B-Brauer pair (D, b_D) such that $(Q, b) \leq (D, b_D)$. Then D is a defect group of B and Q is self-centralizing in D. □

1.5 Puig's Question

We have seen in Section 1.2 that every ℓ-subgroup of a finite group G occurs as a vertex of an indecomposable $\overline{\mathbb{F}}_\ell$-module. If we restrict ourselves to vertices of simple modules, then Erdmann's Theorem (part (d) of Proposition 1.3.1) and Knörr's Theorem (Corollary 1.4.8) show that this is no longer true. More precisely, a vertex V of a simple module lying in a block B of $\overline{\mathbb{F}}_\ell G$ is even a defect group of B, if either V is cyclic or the defect groups of B are abelian. Lluís Puig asked the question whether the order of V induces an upper bound for the order of the defect groups of B. In Chapters 2 and 3 of this thesis, we investigate this question.

Question 1.5.1 (Puig's Question, [60])**.** *If V is a vertex of a simple module in a block B of the group algebra of a finite group, is then the order of the defect groups of B bounded in terms of the order of V?*

In [60], Jiping Zhang proves a reduction theorem to quasi-simple groups.

The following example shows that the answer to Puig's Question is negative for $\ell = 2$:

Example 1.5.2 (Erdmann, [25])**.** If q is a prime power, then the Sylow 2-subgroups of $\mathrm{PSL}_2(q)$ are dihedral groups of order $\frac{1}{2}(q^2-1)_2$ or Klein four-groups C_2^2. If, additionally, $q \equiv 1 \bmod 4$, then there exists a simple module in the principal block having vertices isomorphic to C_2^2. As q can be arbitrarily large, this shows that the answer to Puig's Question is negative for $\ell = 2$.

Until now, there are no counterexamples to Puig's Question known for $\ell > 2$.

Our strategy to study infinite sets of groups with respect to Puig's Question will be as follows: Given a set of finite groups, we will define a property with respect to Puig's Question, and we will generalize it to self-centralizing subgroups instead of vertices. Essentially, we will investigate sets of classical groups with regard to this property. Therefore, we will introduce those groups in the next section.

1.6 Finite classical groups

In this section, we introduce finite classical groups, as well as their order formulae. It is based on [5], [33], [40], and [58]. By $\mathrm{GL}_n(q)$ and $\mathrm{SL}_n(q)$, we denote the general linear and special linear group, respectively, of degree n over the finite field $\mathbb{F}_q$. Moreover, $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ are the symmetric group and alternating group, respectively, on n letters. Finally, $\mathbb{1}_n$ denotes the identity matrix of size $n \times n$.

Theorem 1.6.1. *Let q be a prime power, and let $n \in \mathbb{N}_{>0}$.*

(a) *One has* $|\mathrm{GL}_n(q)| = q^{n(n-1)/2} \prod_{j=1}^{n}(q^j - 1)$ *and* $|\mathrm{SL}_n(q)| = \frac{|\mathrm{GL}_n(q)|}{q-1}$.

(b) *One has*
$$Z(\mathrm{GL}_n(q)) = \mathbb{F}_q^\times \cdot \mathbb{1}_n \cong C_{q-1}$$
and
$$Z(\mathrm{SL}_n(q)) = Z(\mathrm{GL}_n(q)) \cap \mathrm{SL}_n(q) = \left\{a \in \mathbb{F}_q^\times \;:\; a^n = 1\right\} \cdot \mathbb{1}_n \cong C_{\gcd(n,q-1)},$$
and one writes $\mathrm{PGL}_n(q) := \mathrm{GL}_n(q)/Z(\mathrm{GL}_n(q))$ *and* $\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$. *The groups* $\mathrm{PGL}_n(q)$ *and* $\mathrm{PSL}_n(q)$ *are called the* ***projective general linear group*** *and the* ***projective special linear group****, respectively.*

(c) *The group* $\mathrm{PSL}_n(q)$ *is simple, except for* $\mathrm{PSL}_2(2) \cong \mathrm{Sym}(3)$ *and* $\mathrm{PSL}_2(3) \cong \mathrm{Alt}(4)$.

Proof. This is well known, see, for example, [33, Chapter 1]. □

Given a field K, we write $\mathrm{Gal}(K)$ for the group of field automorphisms of K.

Definition 1.6.2. Let K be a field, let $\sigma \in \mathrm{Gal}(K)$, and let V be a K-vector space.

(a) A ***(σ-)sesquilinear form on*** V is a map $\langle \cdot, \cdot \rangle : V^2 \to K$ such that

$$\langle x_1 v_1 + x_2 v_2, w \rangle = x_1 \langle v_1, w \rangle + x_2 \langle v_2, w \rangle$$

and

$$\langle w, x_1 v_1 + x_2 v_2 \rangle = \sigma(x_1) \langle w, v_1 \rangle + \sigma(x_2) \langle w, v_2 \rangle$$

for all $x_1, x_2 \in K$ and all $v_1, v_2, w \in V$. A vector $v \in V$ is called ***isotropic*** if $\langle v, v \rangle = 0$, and a subspace U of V is called ***totally isotropic***, if all of its vectors are isotropic.

(b) A sesquilinear form $\langle \cdot, \cdot \rangle$ on V is called ***alternating***, if it satisfies $\langle v, v \rangle = 0$ for all $v \in V$.

(c) A σ-sesquilinear form $\langle \cdot, \cdot \rangle$ on V is called ***symmetric***, if it satisfies $\langle u, v \rangle = \langle v, u \rangle$ for all $u, v \in V$, and it is called ***hermitian***, if it satisfies $\langle u, v \rangle = \sigma(\langle v, u \rangle)$ for all $u, v \in V$.

(d) An id_K-sesquilinear form is called a ***bilinear form***.

(e) A sesquilinear form $\langle \cdot, \cdot \rangle$ on V is called ***reflexive***, if it satisfies $\langle u, v \rangle = 0$ for all $u, v \in V$ such that $\langle v, u \rangle = 0$.

(f) A reflexive sesquilinear form $\langle \cdot, \cdot \rangle$ is called ***degenerate***, if there exists a $u \in V \setminus \{0\}$ such that $\langle u, v \rangle = 0$ for all $v \in V$.

(g) A ***quadratic form on*** V is a map $Q : V \to K$ satisfying $Q(av) = a^2 Q(v)$ for all $a \in K$ and all $v \in V$, such that the map

$$b_Q : V^2 \to K : (u, v) \mapsto Q(u + v) - Q(u) - Q(v)$$

is a bilinear form on V.
Such a quadratic form Q is called ***degenerate***, if the corresponding bilinear form b_Q is degenerate.

The following are basic properties of sesquilinear forms:

Observation 1.6.3. *Let K be a field, let $\sigma \in \mathrm{Gal}(K)$, and let V be a K-vector space.*

(a) *Every alternating sesquilinear form $\langle \cdot, \cdot \rangle$ on V satisfies $\langle u, v \rangle = -\langle v, u \rangle$ for all $u, v \in V$.*

(b) *Hermitian sesquilinear forms and alternating sesquilinear forms are reflexive.*

(c) *A non-zero symmetric or alternating σ-sesquilinear form is bilinear.*

(d) *A non-zero hermitian σ-sesquilinear form satisfies $\sigma^2 = \mathrm{id}_K$.*

(e) *If $\mathrm{char}(K) \neq 2$, then $Q \mapsto b_Q$ is a bijection between the set of all quadratic forms on V and the set of all symmetric bilinear forms on V.*

Proof.

(a) We have $0 = \langle u+v, u+v \rangle = \langle u, u \rangle + \langle v, v \rangle + \langle u, v \rangle + \langle v, u \rangle = \langle u, v \rangle + \langle v, u \rangle$.

(b) This is obvious for the Hermitian case, and for the alternating case it follows immediately from part (a).

(c) Let $\langle \cdot, \cdot \rangle$ be a non-zero σ-sesquilinear form on V, and let $u, v \in V$ be such that $\langle u, v \rangle \neq 0$. Let $a \in K$. If $\langle \cdot, \cdot \rangle$ is symmetric, then

$$\begin{aligned} a &= a \langle u, v \rangle \langle u, v \rangle^{-1} = \langle au, v \rangle \langle u, v \rangle^{-1} \\ &= \langle v, au \rangle \langle v, u \rangle^{-1} = \sigma(a) \langle v, u \rangle \langle v, u \rangle^{-1} = \sigma(a), \end{aligned}$$

so $\sigma = \mathrm{id}_K$. If $\langle \cdot, \cdot \rangle$ is alternating, then by part (a) we have

$$\begin{aligned} a = a \langle u, v \rangle \langle u, v \rangle^{-1} &= \langle au, v \rangle \langle u, v \rangle^{-1} = -\langle v, au \rangle (-\langle v, u \rangle^{-1}) \\ &= \langle v, au \rangle \langle v, u \rangle^{-1} = \sigma(a) \langle v, u \rangle \langle v, u \rangle^{-1} = \sigma(a), \end{aligned}$$

so $\sigma = \mathrm{id}_K$.

(d) Let $\langle \cdot, \cdot \rangle$ be a non-zero hermitian σ-sesquilinear form on V, and let $u, v \in V$ be such that $\langle u, v \rangle \neq 0$. Then, for all $a \in K$, we have

$$\begin{aligned} a = a \langle u, v \rangle \langle u, v \rangle^{-1} &= \langle au, v \rangle \langle u, v \rangle^{-1} = \sigma(\langle v, au \rangle)\sigma(\langle v, u \rangle)^{-1} \\ &= \sigma(\langle v, au \rangle \langle v, u \rangle^{-1}) = \sigma(\sigma(a) \langle v, u \rangle \langle v, u \rangle^{-1}) = \sigma^2(a), \end{aligned}$$

so $\sigma^2 = \mathrm{id}_K$.

(e) The inverse map is given by $\langle \cdot, \cdot \rangle \mapsto (v \mapsto \frac{1}{2} \langle v, v \rangle)$.

□

The next proposition translates sesquilinear forms on abstract vector spaces into sesquilinear forms given by matrices:

Proposition 1.6.4 ([40, Chapter 6]). *Let K be a field, let $n \in \mathbb{N}$, let $(v_1, \dots, v_n)$ be an ordered basis of a K-vector space V, and let $\sigma \in \mathrm{Gal}(K)$.*

(a) *The set S of all σ-sesquilinear forms on V is a K-vector space, and the map*

$$S \to K^{n\times n} : \langle\cdot,\cdot\rangle \mapsto (\langle v_i, v_j\rangle)_{i,j}$$

is a K-vector space isomorphism with inverse map

$$K^{n\times n} \to S : (a_{ij})_{i,j} \mapsto \left(\left(\sum_{i=1}^{n} x_i v_i, \sum_{j=1}^{n} y_j v_j \right) \mapsto \sum_{i=1}^{n} \sum_{j=1}^{n} x_i \sigma(y_j) a_{ij} \right).$$

*If $\langle\cdot,\cdot\rangle \in S$ is given, then the matrix $(\langle v_i, v_j\rangle)_{i,j} \in K^{n\times n}$ is called the **matrix of $\langle\cdot,\cdot\rangle$ with respect to** $(v_1, \dots, v_n)$.*

(b) *Let $\langle\cdot,\cdot\rangle \in S$. If $(w_1, \dots, w_n)$ is an ordered K-basis of V, and if A is the matrix of $\langle\cdot,\cdot\rangle$ with respect to $(v_1, \dots, v_n)$, then*

$$(c_{ij})_{i,j}^{t} \cdot A \cdot (\sigma(c_{ij}))_{i,j}$$

is the matrix of $\langle\cdot,\cdot\rangle$ with respect to $(w_1, \dots, w_n)$, where $c_{ij} \in K$ are such that $w_j = \sum_{i=1}^{n} c_{ij} v_i$.

(c) *Let $\langle\cdot,\cdot\rangle \in S$, and let A be the matrix of $\langle\cdot,\cdot\rangle$ with respect to some ordered K-basis of V. Then the following hold:*

- *$\langle\cdot,\cdot\rangle$ is degenerate if and only if $\det(A) = 0$.*
- *$\langle\cdot,\cdot\rangle$ is alternating if and only if $A^t = -A$ and the diagonal entries of A are 0.*
- *$\langle\cdot,\cdot\rangle$ is symmetric if and only if $A^t = A$.*
- *$\langle\cdot,\cdot\rangle$ is hermitian if and only if $A^t = \sigma(A)$, where $\sigma(A)$ is the matrix obtained by applying σ to every entry of A.*

Now, we recall the definitions of geometries and corresponding isometries over finite fields.

Definition 1.6.5. Let K be a field, and let V be a K-vector space.

(a) Let $\langle\cdot,\cdot\rangle$ be a non-degenerate sesquilinear form on V, and let $\dim_K(V)$ be finite. The tuple $(V, \langle\cdot,\cdot\rangle)$ is called a ***symplectic geometry over*** K if $\langle\cdot,\cdot\rangle$ is alternating, and it is called a ***unitary geometry over*** K if $\langle\cdot,\cdot\rangle$ is hermitian and not bilinear.

(b) If Q is a non-degenerate quadratic form on V and if $\dim_K(V)$ is finite, then the tuple (V, Q) is called a ***quadratic geometry over*** K.

Proposition 1.6.6. *Let* K *be a field, and let* V *and* V' *be* K*-vector spaces.*

(a) *Let* Q_V *be a quadratic form on* V*, and let* $Q_{V'}$ *be a quadratic form on* V'*. A map* $f \in \mathrm{Hom}_K(V, V')$ *satisfying* $q_V(v) = q_{V'}(f(v))$ *for all* $v \in V$ *is called a* ***K-linear isometry****, and it also satisfies* $b_V(u,v) = b_{V'}(f(u), f(v))$ *for all* $u, v \in V$*, where* b_V *and* $b_{V'}$ *are the corresponding symmetric bilinear forms.*

(b) *Let* s_V *be a sesquilinear form on* V*, and let* $s_{V'}$ *be a sesquilinear form on* V'*. A map* $f \in \mathrm{Hom}_K(V, V')$ *satisfying* $s_V(u,v) = s_{V'}(f(u), f(v))$ *for all* $u, v \in V$ *is called a* ***K-linear isometry****. If* s_V *is not degenerate, then every* K*-linear isometry* $V \to V$ *is injective.*

(c) *Let* V *be finite-dimensional, and let* s *be a sesquilinear form on* V*. Then the set of* K*-linear isometries* $V \to V$ *is a subgroup of* $\mathrm{GL}_K(V)$*. It is called the* ***isometry group of*** V*.*

The following theorem shows that in order to study isometry groups of non-degenerate forms, it suffices to consider symplectic, unitary, and quadratic geometries.

Theorem 1.6.7 ([5, Thm. 3.6])**.** *Let* K *be a field, let* V *be a* K*-vector space, and let* s *be any non-degenerate reflexive sesquilinear form on* V*. Then* s *is alternating or there exists some* $a \in K^\times$ *such that the sesquilinear form* $a \cdot s$ *is hermitian. In the second case, the isometry groups of* s *and* $a \cdot s$ *coincide.*

We now state Witt's Extension Theorem, which is very important in the context of geometries over finite fields. As an application, one can define the Witt index of a geometry.

Theorem 1.6.8 (Witt's Extension Theorem, [33, Thm. 5.2, Thm. 10.12, Thm. 12.10])**.** *Let* K *be a field, and let* V *be a symplectic, unitary, or quadratic geometry over* K*. If* $U \subseteq V$ *is a subspace and* $f : U \to V$ *is an injective* K*-linear isometry, then there exists a* K*-linear isometry* $V \to V$ *extending* f*.*

Corollary 1.6.9. *Let* K *be a field, and let* V *be a symplectic, unitary, or quadratic geometry over* K *with isometry group* G*. Then* G *acts transitively on the set of all maximal totally isotropic subspaces of* V*. In particular, the dimensions of all such maximal totally isotropic subspaces coincide, and this common dimension is called the* ***Witt index of*** V*.*

Proof. Let U and W be two such subspaces, and assume $\dim_K(U) \leq \dim_K(W)$. Then every K-linear injection $U \hookrightarrow W$ is an isometry, so by Witt's Theorem, there exists some $g \in G$ such that $g(U) \subseteq W$. As g^{-1} is also an isometry, $g^{-1}(W)$ is totally isotropic, so the maximality of U and $U \subseteq g^{-1}(W) \subseteq V$ implies $U = g^{-1}(W)$. □

We are ready to present the classical groups of symplectic type:

Theorem 1.6.10. *Let q be a prime power, and let $n \in \mathbb{N}_{>0}$.*

(a) *Up to isometric isomorphism, there exists a unique non-degenerate symplectic geometry of dimension $2n$ over $\mathbb{F}_q$. Its isometry group is denoted by $\mathrm{Sp}_{2n}(q)$ and it is called a* ***symplectic group****. Moreover, there is no non-degenerate symplectic geometry of dimension $2n+1$ over $\mathbb{F}_q$.*

(b) $\mathrm{Sp}_{2n}(q)$ *is isomorphic to* $\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t J A = J\}$, *for all* $J \in \mathrm{GL}_{2n}(q)$ *satisfying* $J^t = -J$. *In particular,*

$$\mathrm{Sp}_{2n}(q) \cong \left\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix} A = \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix}\right\}.$$

(c) $\mathrm{Sp}_{2n}(q)$ *is contained in* $\mathrm{SL}_{2n}(q)$.

(d) $Z(\mathrm{Sp}_{2n}(q)) = \{\pm\mathbb{1}_{2n}\}$. *One writes* $\mathrm{PSp}_{2n}(q) := \mathrm{Sp}_{2n}(q)/Z(\mathrm{Sp}_{2n}(q))$.

(e) $|\mathrm{Sp}_{2n}(q)| = q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$ *and* $|\mathrm{PSp}_{2n}(q)| = \frac{|\mathrm{Sp}_{2n}(q)|}{\gcd(2,q-1)}$.

(f) *The group* $\mathrm{PSp}_{2n}(q)$ *is simple, except for* $\mathrm{PSp}_2(2) \cong \mathrm{Sym}(3)$, $\mathrm{PSp}_2(3) \cong \mathrm{Alt}(4)$, *and* $\mathrm{PSp}_4(2) \cong \mathrm{Sym}(6)$.

Proof.

(a) It follows from [33, Cor. 2.11] that there is no non-degenerate symplectic geometry of odd dimension $2n+1$. Moreover, the uniqueness follows from [33, Cor. 2.12]. The existence is clear, as the matrix $\begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix}$ defines a symplectic geometry of dimension $2n$.

(b) This follows from Proposition 1.6.4 and part (a).

(c) See [33, Cor. 3.5].

(d) See [33, Cor. 3.6].

(e) See [33, Thm. 3.12].

(f) See [33, page 25, page 26, Thm 3.11, Prop. 3.13].

□

Now, we come to unitary groups:

Observation 1.6.11. *Let q be a prime power. If there exists a non-degenerate unitary geometry over $\mathbb{F}_q$, then q is a square and the corresponding field automorphism is given by*

$$\mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^{\sqrt{q}}.$$

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{F}_q)$ be the corresponding field automorphism, and let $p \in \mathbb{P}$ and $n \in \mathbb{N}$ be such that $q = p^n$. Then $\mathrm{Gal}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p)$ is cyclic of order n and is generated by the Frobenius automorphism $\mathbb{F}_q \to \mathbb{F}_q : x \mapsto x^p$. As we consider a unitary geometry, σ is not the identity. Thus, σ has order 2 by part (d) of Observation 1.6.3. The claim follows. □

Theorem 1.6.12. *Let q be a prime power, and let $n \in \mathbb{N}_{>0}$.*

(a) *Up to isometric isomorphism, there exists a unique non-degenerate unitary geometry of dimension n over $\mathbb{F}_{q^2}$. Its isometry group is denoted by $\mathrm{GU}_n(q)$ and it is called a* ***unitary group****.*

(b) $\mathrm{GU}_n(q)$ *is isomorphic to* $\left\{A \in \mathrm{GL}_n(q^2) \;:\; \overline{A}^t J A = J\right\}$*, for all* $J \in \mathrm{GL}_n(q^2)$ *satisfying* $J = \overline{J}^t$*, where* $\overline{(a_{ij})_{i,j}} := (a_{ij}^q)_{i,j}$*. In particular,*

$$\mathrm{GU}_n(q) \cong \left\{A \in \mathrm{GL}_n(q^2) \;:\; \overline{A}^t A = \mathbb{1}_n\right\}.$$

(c) $\mathrm{SU}_n(q) := \mathrm{GU}_n(q) \cap \mathrm{SL}_n(q^2)$ *has index* $q+1$ *in* $\mathrm{GU}_n(q)$*.*

(d) *One has*

$$Z(\mathrm{GU}_n(q)) = Z(\mathrm{GL}_n(q^2)) \cap \mathrm{GU}_n(q) = \left\{c \cdot \mathbb{1}_n \;:\; c \in \mathbb{F}_{q^2}^\times,\ c^{q+1} = 1\right\} \cong C_{q+1}$$

and

$$Z(\mathrm{SU}_n(q)) = Z(\mathrm{GU}_n(q)) \cap \mathrm{SU}_n(q) \cong C_{\gcd(n,q+1)}.$$

One writes $\mathrm{PGU}_n(q) := \mathrm{GU}_n(q)/Z(\mathrm{GU}_n(q))$ *and* $\mathrm{PSU}_n(q) := \mathrm{SU}_n(q)/Z(\mathrm{SU}_n(q))$*.*

(e) $|\mathrm{GU}_n(q)| = q^{n(n-1)/2}\prod_{j=1}^n (q^j - (-1)^j)$ *and* $|\mathrm{PSU}_n(q)| = \frac{|\mathrm{GU}_n(q)|}{(q+1)\gcd(n,q+1)}$*.*

(f) *The group* $\mathrm{PSU}_n(q)$ *is simple, except for* $\mathrm{PSU}_2(2) \cong \mathrm{Sym}(3)$*,* $\mathrm{PSU}_2(3) \cong \mathrm{Alt}(4)$*, and* $\mathrm{PSU}_3(2)$*.*

Proof.

(a) The uniqueness follows from [33, Cor. 10.4]. The existence is clear, as the identity matrix $\mathbb{1}_n$ defines a unitary geometry of dimension n.

(b) This is clear, by Proposition 1.6.4 and by part (a).

(c) See [33, Cor. 11.29].

(d) See [33, Prop. 11.6, Prop. 11.17].

(e) See [33, Thm. 11.28, Cor. 11.29].

(f) See [33, Thm. 11.26, page 110].

□

Finally, we turn to orthogonal groups. Here, we distinguish odd and even dimension. Moreover, as we want to apply a result of Paul Fong and Bhama Srinivasan in Section 3.2 which is only formulated for orthogonal groups over finite fields of *odd* characteristic, we restrict ourselves to this case.

Theorem 1.6.13. *Let q be an odd prime power, and let $n \in \mathbb{N}_{>0}$.*

(a) *Up to isometric isomorphism, there are two non-degenerate quadratic geometries of dimension $2n+1$ over $\mathbb{F}_q$. Both have the same isometry group which is denoted by $\mathrm{GO}_{2n+1}(q)$ and which is called an* ***orthogonal group****.*

(b) $\mathrm{GO}_{2n+1}(q)$ *is isomorphic to* $\left\{A \in \mathrm{GL}_{2n+1}(q) \;:\; A^t J A = J\right\}$*, for all* $J \in \mathrm{GL}_{2n+1}(q)$ *satisfying* $J = J^t$*. In particular,*

$$\mathrm{GO}_{2n+1}(q) \cong \left\{A \in \mathrm{GL}_{2n+1}(q) \;:\; A^t A = \mathbb{1}_{2n+1}\right\}.$$

(c) $\mathrm{SO}_{2n+1}(q) := \mathrm{GO}_{2n+1}(q) \cap \mathrm{SL}_{2n+1}(q)$ *has index* 2 *in* $\mathrm{GO}_{2n+1}(q)$*.*

(d) $Z(\mathrm{GO}_{2n+1}(q)) = \{\pm \mathbb{1}_{2n+1}\}$ *and* $Z(\mathrm{SO}_{2n+1}(q)) = \{\mathbb{1}_{2n+1}\}$*. One writes* $\mathrm{PGO}_{2n+1}(q) := \mathrm{GO}_{2n+1}(q)/Z(\mathrm{GO}_{2n+1}(q))$*.*

(e) $\mathrm{GO}_{2n+1}(q)' = \mathrm{SO}_{2n+1}(q)'$ *has index* 2 *in* $\mathrm{SO}_{2n+1}(q)$*. One writes* $\Omega_{2n+1}(q) := \mathrm{GO}_{2n+1}(q)'$*.*

(f) $|\mathrm{GO}_{2n+1}(q)| = 2q^{n^2}\prod_{i=1}^{n}(q^{2i}-1)$ *and* $|\Omega_{2n+1}(q)| = \frac{|\mathrm{GO}_{2n+1}(q)|}{4} = |\mathrm{PSp}_{2n}(q)|$*.*

(g) *The group* $\Omega_{2n+1}(q)$ *is simple, except for* $\Omega_3(3) \cong \mathrm{PSL}_2(3)$*.*

Proof.

(a) See [33, Cor. 4.10, page 79] and [58, paragraph II on page 139].

(b) This is clear by Proposition 1.6.4 and by part (a).

(c) By part (b), the elements of $\mathrm{GO}_{2n+1}(q)$ have determinant ± 1, hence the index is at most 2. It cannot be 1 since $-\mathbb{1}_{2n+1}$ has determinant -1 and lies in the given group.

(d) See [33, Prop. 6.15] and [15, page xii].

(e) This follows from part (c), part (f), and [33, Prop. 6.14, Prop. 6.28].

(f) See [33, Thm. 9.11, Cor. 9.12].

(g) See [33, Thm. 6.31, page 83].

□

It should be mentioned that for $n \geq 3$, the groups $\Omega_{2n+1}(q)$ and $\mathrm{PSp}_{2n}(q)$ have the same order and are both simple, but they are not isomorphic to each other, see [33, page 83].

In the following theorem, we denote by $(\mathbb{F}_q^\times)^2$ the group of squares in $\mathbb{F}_q^\times$.

Theorem 1.6.14. *Let q be an odd prime power, and let $n \in \mathbb{N}_{>1}$.*

(a) *Up to isometric isomorphism, there are two non-degenerate quadratic geometries of dimension $2n$ over $\mathbb{F}_q$: one of Witt index n, and one of Witt index $n-1$. Their isometry groups are denoted by $\mathrm{GO}_{2n}^+(q)$ and $\mathrm{GO}_{2n}^-(q)$, respectively, and they are also called* ***orthogonal groups****.*

(b) *Let*

$$S := \Big\{\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t J A = J\} \ : \ J \in \mathrm{GL}_{2n}(q),\ J = J^t,\ \det(J) \in (\mathbb{F}_q^\times)^2\Big\}$$

and

$$N := \Big\{\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t J A = J\} \ : \ J \in \mathrm{GL}_{2n}(q),\ J = J^t,\ \det(J) \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2\Big\}.$$

Then, in particular, $\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t A = \mathbb{1}_n\} \in S$. One has the following:

- *If $(-1)^n$ is a square in $\mathbb{F}_q$, then $\mathrm{GO}_{2n}^+(q)$ is isomorphic to all elements of S, and $\mathrm{GO}_{2n}^-(q)$ is isomorphic to all elements of N.*
- *If $(-1)^n$ is a non-square in $\mathbb{F}_q$, then $\mathrm{GO}_{2n}^+(q)$ is isomorphic to all elements of N, and $\mathrm{GO}_{2n}^-(q)$ is isomorphic to all elements of S.*

(c) *For $\varepsilon \in \{\pm 1\}$, the subgroup $\mathrm{SO}_{2n}^\varepsilon(q) := \mathrm{GO}_{2n}^\varepsilon(q) \cap \mathrm{SL}_{2n}(q)$ has index 2 in $\mathrm{GO}_{2n}^\varepsilon(q)$.*

(d) *For $\varepsilon \in \{\pm 1\}$, one has $Z(\mathrm{GO}_{2n}^\varepsilon(q)) = Z(\mathrm{SO}_{2n}^\varepsilon(q)) = \{\pm \mathbb{1}_{2n}\}$. One writes $\mathrm{PGO}_{2n}^\varepsilon(q) := \mathrm{GO}_{2n+1}^\varepsilon(q)/Z(\mathrm{GO}_{2n+1}^\varepsilon(q))$ and $\mathrm{PSO}_{2n}^\varepsilon(q) := \mathrm{SO}_{2n}^\varepsilon(q)/Z(\mathrm{SO}_{2n}^\varepsilon(q))$.*

(e) *For $\varepsilon \in \{\pm 1\}$, the commutator subgroup $\mathrm{GO}_{2n}^\varepsilon(q)' = \mathrm{SO}_{2n}^\varepsilon(q)'$ has index 2 in $\mathrm{SO}_{2n}^\varepsilon(q)$. One writes $\Omega_{2n}^\varepsilon(q) := \mathrm{GO}_{2n}^\varepsilon(q)'$ and $\mathrm{P}\Omega_{2n}^\varepsilon(q) := \Omega_{2n}^\varepsilon(q)/(\Omega_{2n}^\varepsilon(q) \cap \{\pm \mathbb{1}_{2n}\})$.*

(f) *For $\varepsilon \in \{\pm 1\}$, one has $|\mathrm{GO}_{2n}^\varepsilon(q)| = 2q^{n(n-1)}(q^n - \varepsilon)\prod_{i=1}^{n-1}(q^{2i}-1)$ and $|\mathrm{P}\Omega_{2n}^\varepsilon(q)| = \frac{|\mathrm{GO}_{2n}^\varepsilon(q)|}{\gcd(4, q^n - \varepsilon)}$.*

(g) *For $\varepsilon \in \{\pm 1\}$, the group $\mathrm{P}\Omega_{2n}^\varepsilon(q)$ is simple, except for $\mathrm{P}\Omega_4^+(q) \cong \mathrm{PSL}_2(q)^2$.*

Proof.

(a),(b) See [58, page 139] and [33, Thm 4.9, Cor. 4.10, page 79].

(c),(d) See [15, page xii].

(e) See [33, Prop. 6.14, Prop. 6.28, Thm. 9.7].

(f) See [33, Thm. 6.31, Cor. 9.12].

(g) See [33, Thm. 6.31, page 83]. □

Remark 1.6.15. For $n = 1$, parts (a) and (b) from the previous theorem are still true, and $\mathrm{GO}_2^{\varepsilon}(q)$ is the dihedral group of order $2(q - \varepsilon)$ or the Klein four-group C_2^2, see [58, Thm. 11.4]. Here, $\mathrm{GO}_2^{\varepsilon}(q)$ is the Klein four-group C_2^2 if and only if $q = 3$, so one clearly has $\mathrm{Z}(\mathrm{GO}_2^{+}(3)) \neq \{\pm \mathbb{1}_2\}$. This shows that [33, Prop. 6.15] is wrong for $q = 3$ and $\dim(V) = 2$. (The case where $u_i + u_j$ is isotropic is missing in the proof, but must be considered if the underlying field is $\mathbb{F}_3$.)

Orthogonal groups over finite fields of characteristic 2 are not considered in this thesis. However, we state the result corresponding to the previous theorem.

First, note that if V is any non-degenerate quadratic geometry over $\mathbb{F}_q$ for even q, then the induced bilinear form $\langle \cdot, \cdot \rangle$ is alternating since $\langle x, x \rangle = Q(x+x) - Q(x) - Q(x) = Q(0) = 0$, where Q is the corresponding quadratic form. Now part (a) of Theorem 1.6.10 implies that V must have even dimension.

In the literature, one often replaces "non-degeneracy" by different terms in this case (such as "regularity" in [33, page 114]) to obtain also quadratic geometries in odd dimension. However, the corresponding isometry groups are then symplectic groups and have, thus, already been considered in Theorem 1.6.10.

We are left with the case of even dimension:

Remark 1.6.16 ([33, Thm 12.9, Thm 14.43, Thm 14.46])**.** Let q be a power of 2, and let $n \in \mathbb{N}_{>1}$. Then, up to isometric isomorphism, there are two non-degenerate quadratic geometries of dimension $2n$ over $\mathbb{F}_q$: one of Witt index n, and one of Witt index $n-1$. Their isometry groups are denoted by $\mathrm{GO}_{2n}^{+}(q)$ and $\mathrm{GO}_{2n}^{-}(q)$, respectively. Their commutator subgroups are simple, except for the (infinitely many) groups $\mathrm{GO}_4^{+}(q)$.

Definition 1.6.17. The various groups from Theorems 1.6.1, 1.6.14, 1.6.13, 1.6.12, and 1.6.10 are called ***finite classical groups***.

We will also consider spin groups in this thesis:

Remark 1.6.18 ([47, Section 4], see also [11, Section 16.3] and [14])**.** Let q be an odd prime power, and let $n \in \mathbb{N}_{>1}$. Let V be a quadratic geometry over $\mathbb{F}_q$, and let $\Omega(V)$ be the commutator subgroup of the isometry group of V. Then there exists a short exact sequence

$$1 \to Z \to \mathrm{Spin}(V) \to \Omega(V) \to 1$$

of groups, where the ***spin group*** $\mathrm{Spin}(V)$ occurs as a subgroup of a quotient of the tensor algebra of V, and where Z is a central subgroup of $\mathrm{Spin}(V)$ of order 2. We write $\mathrm{Spin}_{2n+1}(q)$ and $\mathrm{Spin}^{\varepsilon}_{2n}(q)$ with $\varepsilon \in \{\pm 1\}$, respectively. In particular, $|\mathrm{Spin}_{2n+1}(q)| = |\mathrm{SO}_{2n+1}(q)|$ and $|\mathrm{Spin}^{\varepsilon}_{2n}(q)| = |\mathrm{SO}^{\varepsilon}_{2n}(q)|$.

We finish this section with the following remark based on [12] to view the classical groups as a part of the wider concept of Chevalley groups.

Remark 1.6.19. Given a simple Lie algebra L over $\mathbb{C}$, one can construct a certain subgroup called ***Lie group of*** L, of the automorphism group of L. There is a particular basis of L over $\mathbb{C}$ (the Chevalley basis), and the subset of L of all $\mathbb{Z}$-linear combinations with respect to this basis is a Lie algebra over $\mathbb{Z}$. By extending scalars, one obtains a Lie algebra over any field K. Now, one can define a group for this Lie algebra analogously to the Lie group. This is the ***Chevalley group of*** L ***over*** K. If K is finite, then this group is finite, too.
The finite-dimensional simple Lie algebras over $\mathbb{C}$ are completely classified and correspond to indecomposable root systems. There are the infinite families labeled by

$$A_n\ (n \geq 1),\ B_n\ (n \geq 2),\ C_n\ (n \geq 3),\ D_n\ (n \geq 4),$$

as well as the five exceptional types labeled by

$$G_2,\ F_4,\ E_6,\ E_7,\ \text{and}\ E_8.$$

If q is a prime power, then one writes $A_n(q)$ for the Chevalley group over $\mathbb{F}_q$ of type A_n, and similarly for the other types. Except for the four groups $A_1(2)$, $A_1(3)$, $B_2(2)$, and $G_2(2)$, the finite Chevalley groups are always simple groups. Moreover,

$$A_n(q) \cong \mathrm{PSL}_{n+1}(q),\ B_n(q) \cong \Omega_{2n+1}(q),\ C_n(q) \cong \mathrm{PSp}_{2n}(q),\ \text{and}\ D_n(q) \cong \mathrm{P}\Omega^{+}_{2n}(q),$$

see [12, Thm. 11.3.2].

For some types of Chevalley groups, one can construct a certain fixed point subgroup with respect to an automorphism coming from a non-trivial field automorphism and a non-trivial graph automorphism of the Dynkin diagram of the corresponding root system. In this way, one obtains the ***twisted Chevalley groups*** (see [12, pages 225, 226]). The finite twisted Chevalley groups are

$$^2A_n(q^2)\ (n \geq 2),\ ^2D_n(q^2)\ (n \geq 4),\ ^2E_6(q^2),\ ^3D_4(q^3),\ ^2B_2(2^{2m+1}),\ ^2G_2(3^{2m+1}),\ ^2F_4(2^{2m+1}),$$

see [12, page 251], where in each case, the power of q indicates the finite field the groups are defined over. There is also the convention to denote these groups by $^2A_n(q)$, $^2D_n(q)$ and so on, see, for example, [15] or [49]. Except for the four groups $^2A_n(2^2)$, $^2B_2(2)$, $^2G_2(3)$, and $^2F_4(2)$, the finite twisted Chevalley are always simple groups, see [12, page 262]. Moreover, one has

$$^2A_n(q^2) \cong \mathrm{PSU}_{n+1}(q) \text{ and } ^2D_n(q^2) \cong \mathrm{P}\Omega^-_{2n}(q).$$

In particular, each finite simple classical group is a Chevalley group or a twisted Chevalley group.

If G is a Chevalley group of a simple Lie algebra L over $\mathbb{C}$, then one can construct a certain subgroup $\tilde{G}$ of the automorphism group of L, the ***universal Chevalley group of*** L ([12, page 198]). It satisfies $\tilde{G}/\,Z(\tilde{G}) \cong G$. Now, for all central subgroups $N \leq Z(\tilde{G})$, one calls $\tilde{G}/N$ a ***Chevalley group***. In particular, G occurs in every Chevalley group of L as a quotient group since we have $(\tilde{G}/N)/(Z(\tilde{G})/N) \cong \tilde{G}/\,Z(\tilde{G}) \cong G$.

2 Small self-centralizing subgroups in Sylow subgroups of classical groups

In this chapter, we introduce Sylow subgroups of finite classical groups and investigate the existence of small self-centralizing subgroups. More precisely, given a Sylow subgroup G of a finite classical group, we want to answer the question whether it is possible to bound the group order $|\mathsf{G}|$ in terms of an arbitrary self-centralizing subgroup. In the first four sections, we provide first mathematical tools that we will use mainly in Section 2.7. Sections 2.5 and 2.6 provide the Sylow subgroups of most of the finite classical groups following [59]. In the last section, we investigate the structure of Sylow subgroups of special and projective (special) linear groups which does not seem to exist in the literature. Our main results of this chapter are Theorem 2.5.10, Theorem 2.6.7, Corollary 2.6.10, Theorem 2.7.14, and Corollary 2.7.15, where we answer the question whether there exist small self-centralizing subgroups of the considered Sylow subgroups.

2.1 Self-centralizing subgroups

First, we introduce some properties of self-centralizing subgroups. Results from [37] and [60] will show that the order of any finite group G of prime power order is always bounded from above in terms of the exponent $\mathrm{Exp}(\mathsf{G})$ and the order of a self-centralizing subgroup.

Definition 2.1.1. Let G be a group, and let $\mathsf{U} \leq \mathsf{G}$ be a subgroup satisfying $\mathrm{C}_{\mathsf{G}}(\mathsf{U}) \subseteq \mathsf{U}$. Then U is called ***self-centralizing in*** G.

The following two observations are immediate.

Observation 2.1.2. *Let* G *be a group, and let* $\mathsf{U} \leq \mathsf{G}$ *be a self-centralizing subgroup. Then one has* $\mathrm{Z}(\mathsf{G}) \subseteq \mathrm{Z}(\mathsf{U}) = \mathrm{C}_{\mathsf{G}}(\mathsf{U}) \subseteq \mathsf{U}$. *In particular, if* G *is abelian, then* $\mathsf{U} = \mathsf{G}$.

Observation 2.1.3. *Let* G *be a group, and let* $\mathsf{U} \leq \mathsf{G}$ *be a subgroup. The following are equivalent:*

(a) U *is self-centralizing in* G.

(b) U *is self-centralizing in all subgroups of* G *containing* U.

(c) *All subgroups of* G *containing* U *are self-centralizing in* G.

We have the following two theorems from [37] and [60]:

Theorem 2.1.4 ([37, Satz III.7.3(b)])**.** *Let* $\ell \in \mathbb{P}$, *and let* G *be a finite* ℓ*-group. If* A *is a maximal normal abelian subgroup of* G, *then*

$$|\mathsf{G}| \leq \sqrt{\ell^{\log_\ell(|\mathsf{A}|)(\log_\ell(|\mathsf{A}|)+1)}}.$$

Theorem 2.1.5. *Let $\ell \in \mathbb{P}$, let G be a finite ℓ-group, and let $V \leq G$ be a self-centralizing subgroup. If $N \trianglelefteq G$ is an elementary abelian normal subgroup, then $|N| \leq |V|^{|V|^{|V|}}$.*

Proof. Let A be the image of the group homomorphism $V \to \mathrm{Aut}(N) : \nu \mapsto (n \mapsto {}^{\nu}n)$. Then $A \leq \mathrm{Aut}(N)$ is an ℓ-subgroup and

$$\{n \in N \ : \ \varphi(n) = n \text{ for all } \varphi \in A\} = C_N(V) \leq C_G(V) \leq V.$$

From [60, Thm. 6] it follows that $|N| \leq |V|^{|A|^{|A|}} \leq |V|^{|V|^{|V|}}$. $\square$

As a corollary, we obtain that for every finite ℓ-group G, the group order $|G|$ can be bounded in terms of the exponent $\mathrm{Exp}(G)$ and an arbitrary self-centralizing subgroup of G. For the proof and for later use, we recall the notation $\Omega_1(G)$ for the characteristic subgroup $\langle g \in G \ : \ g^{\ell} = 1 \rangle$ of G.

Corollary 2.1.6. *Let $\ell \in \mathbb{P}$, let G be a finite ℓ-group, and let $V \leq G$ be a self-centralizing subgroup. Then*

$$|G| \leq \sqrt{\ell^{c^2+c}}, \qquad \textit{where} \qquad c := \log_{\ell}(\mathrm{Exp}(G)^{|V|^{|V|}\log_{\ell}|V|}).$$

Proof. For $|G| = 1$ there is nothing to show, so we assume that $|G| > 1$. We choose a maximal normal abelian subgroup A of G. By the fundamental theorem of finitely generated abelian groups [37, Hauptsatz I.13.12], we can write

$$A \cong C_{\ell^{n_1}} \times \cdots \times C_{\ell^{n_k}}$$

for some $n_1, \ldots, n_k \in \mathbb{N}_{>0}$. Then $\Omega_1(A) \cong C_{\ell}^k$ and $A/\Omega_1(A) \cong C_{\ell^{n_1-1}} \times \cdots \times C_{\ell^{n_k-1}} \leq A \leq G$. It is clear that

$$\mathrm{Exp}(A)/\ell = \mathrm{Exp}(A/\Omega_1(A)) = \ell^{\max\{n_i-1 \ : \ i=1,\ldots,k\}}.$$

Now,

$$|A/\Omega_1(A)| = \ell^{n_1-1} \cdots \ell^{n_k-1} \leq \ell^{k\max\{n_i-1 \ : \ i=1,\ldots,k\}} \leq (\mathrm{Exp}(A)/\ell)^k$$

implies

$$|A| \leq |\Omega_1(A)|(\mathrm{Exp}(A)/\ell)^k = \mathrm{Exp}(A)^k \leq \mathrm{Exp}(G)^k.$$

As $\Omega_1(A)$ is characteristic in A and A is normal in G, it follows from [37, Hilfssatz I.4.8(a)] that $\Omega_1(A)$ is normal in G, so $\ell^k = |\Omega_1(A)| \leq |V|^{|V|^{|V|}}$ by Theorem 2.1.5. This shows $|A| \leq \mathrm{Exp}(G)^{|V|^{|V|}\log_{\ell}|V|}$. Now, the claim follows from Theorem 2.1.4. $\square$

At this point, the question arises whether there exists such a bound only depending on ℓ and $|V|$, where ℓ is of course bounded by $\ell \leq |V|$ if G has more than one element. Corollary 2.1.9 will show that the answer is negative for $\ell = 2$. For arbitrary ℓ, the answer is negative, too, as we will see in Corollary 2.7.16.

As examples and also for later use, we consider the following groups:

Remark 2.1.7 ([32, Thm. 4.3], [36, Prop. 22.7], [57, pages 347, 348])**.**

(a) For $n \in \mathbb{N}_{>2}$, the subgroup $\mathrm{Dih}_{2n} := \langle (1, \dots, n),\ (1, n)(2, n-1)(3, n-2)\cdots \rangle$ of $\mathrm{Sym}(n)$ is called a ***dihedral group***. Its order is $2n$.

(b) For $n \in \mathbb{N}_{>1}$, the finite group with presentation

$$\left\langle x, y \ : \ x^{2n} = 1,\ y^2 = x^n,\ yxy^{-1} = x^{-1} \right\rangle$$

is called a ***dicyclic group***. It has order $4n$, and the unique element $y^2 = x^n$ of order 2 generates the center. In the particular case that n is a power of 2, the dicyclic group of order $4n$ is called a ***generalized quaternion group***. The generalized quaternion group of order 8 is the usual quaternion group.

(c) For $n \in \mathbb{N}_{>3}$, the finite group with presentation

$$\left\langle x, y \ : \ x^{2^{n-1}} = y^2 = 1,\ yxy = x^{2^{n-2}-1} \right\rangle$$

is called a ***semidihedral group***. It has order 2^n, and its center is the subgroup $\left\langle x^{2^{n-2}} \right\rangle$ of order 2.

All of the groups introduced in the previous remark contain self-centralizing subgroups of small order:

Proposition 2.1.8.

(a) *If $n \in \mathbb{N}_{>2}$, then the dihedral group Dih_{2n} of order $2n$ has an elementary abelian self-centralizing subgroup of order $3 + (-1)^n \in \{2, 4\}$.*

(b) *If $n \in \mathbb{N}_{>1}$, then the dicyclic group of order $4n$ has a self-centralizing subgroup isomorphic to C_4.*

(c) *If $n \in \mathbb{N}_{>3}$, then the semidihedral group of order 2^n has a self-centralizing subgroup isomorphic to the Klein four-group C_2^2.*

Proof.

(a) We write $\mathrm{Dih}_{2n} = \langle \sigma, \tau \rangle$ with $\sigma := (1, \dots, n)$ and $\tau := (1, n)(2, n-1)\cdots$. Given $k \in \{1, \dots, n\}$ and $l \in \{0, 1\}$ such that $\sigma^k \tau^l \in C_{\mathrm{Dih}_{2n}}(\tau)$, we have $\sigma^k = \tau\sigma^k\tau = \sigma^{-k}$, so $k \in \left\{0, \frac{n}{2}\right\}$. Therefore, if n is even, then $\langle \sigma^{n/2} \rangle \times \langle \tau \rangle \cong C_2^2$ is self-centralizing in Dih_{2n}, and if n is odd, then $\langle \tau \rangle \cong C_2$ is self-centralizing in Dih_{2n}.

(b) Let $G := \left\langle x, y \ : \ x^{2n} = 1,\ y^2 = x^n,\ yxy^{-1} = x^{-1} \right\rangle$. If $x^i y^j \in C_G(y)$ with $x^i \neq 1$, then $x^i \in C_G(y)$, so $x^i = yx^iy^{-1} = x^{-i}$ implies that x^i has order 2. This shows $x^i = x^n = y^2 \in C_G(y)$. Thus, $\langle y \rangle \cong C_4$ is a self-centralizing subgroup of G.

(c) Let $G := \left\langle x, y \,:\, x^{2^{n-1}} = y^2 = 1, yxy = x^{2^{n-2}-1} \right\rangle$. If $x^i y^j \in C_G(y)$, then $x^i \in C_G(y)$. Thus, $x^i \in Z(G) = \left\langle x^{2^{n-2}} \right\rangle$, and it follows that $x^i y^j \in Z(G)\langle y \rangle$. Therefore, $Z(G)\langle y \rangle \cong C_2^2$ is a self-centralizing subgroup of G.

□

Corollary 2.1.9. *For $\ell = 2$, it is not possible to generalize Corollary 2.1.6 such that the order of a finite ℓ-group can be bounded in terms of the order of an arbitrary self-centralizing subgroup.*

Of course, Corollary 2.1.9 also follows immediately from Corollary 1.4.8 and Example 1.5.2.

2.2 Rank, normal rank, and wreath products

In this section, we recall the well-known notions of the rank and the normal rank of a finite group of prime power order, as well as wreath products, to obtain two propositions that we will use later on.

Definition 2.2.1. Let $\ell \in \mathbb{P}$, and let G be a finite ℓ-group.

(a) The ***rank of*** G, denoted by $\mathrm{rk}(G)$, is the largest integer n such that G has an elementary abelian subgroup of order ℓ^n.

(b) The ***normal rank of*** G, denoted by $\mathrm{nrk}(G)$, is the largest integer n such that G has a normal elementary abelian subgroup of order ℓ^n.

The following lemma summarizes three basic properties of the rank and the normal rank. For the reader's convenience we also give their proofs.

Lemma 2.2.2. *Let $\ell \in \mathbb{P}$, and let G and H be finite ℓ-groups.*

(a) *The rank $\mathrm{rk}(G)$ of G is the largest integer n such that there exists an abelian subgroup $U \leq G$ that can be generated by n elements but not by $n-1$ elements.*

(b) *The normal rank $\mathrm{nrk}(G)$ of G is the largest integer n such that there exists a normal abelian subgroup $U \leq G$ that can be generated by n elements but not by $n-1$ elements.*

(c) *We have $\mathrm{rk}(G \times H) = \mathrm{rk}(G) + \mathrm{rk}(H)$ and $\mathrm{nrk}(G \times H) = \mathrm{nrk}(G) + \mathrm{nrk}(H)$.*

Proof.

(a), (b) By definition, G has an elementary abelian (normal) subgroup U of order $\ell^{\mathrm{rk}(G)}$, and it is clear that U can be generated by $\mathrm{rk}(G)$ elements but not by $\mathrm{rk}(G)-1$ elements.

Conversely, if $U \leq G$ is abelian and can be generated by n elements but not by $n-1$ elements, then it follows from the fundamental theorem of finitely generated abelian groups [37, Hauptsatz I.13.12] that $\Omega_1(U)$ is elementary abelian of order ℓ^n. If U is normal in G, then $\Omega_1(U)$ is also normal in G by part (a) and [37, Hilfssatz I.4.8(a)].

(c) If E_G is elementary abelian in G and E_H is elementary abelian in H, then $E_G \times E_H$ is elementary abelian in $G \times H$. Moreover, if the subgroups E_G and E_H are normal in G and H, respectively, then so is $E_G \times E_H$ in $G \times H$.
Now, let $E \leq G \times H$ be elementary abelian, say $E = \langle (g_1, h_1), \dots, (g_r, h_r) \rangle$. Then $\operatorname{ord}(g_i, h_i) \in \{1, \ell\}$ and, therefore, $\operatorname{ord}(g_i), \operatorname{ord}(h_i) \in \{1, \ell\}$ for each i. So $\langle g_1, \dots, g_r \rangle$ and $\langle h_1, \dots, h_r \rangle$ are elementary abelian, and $E \leq \langle g_1, \dots, g_r \rangle \times \langle h_1, \dots, h_r \rangle$ implies that
$$|E| \leq |\langle g_1, \dots, g_r \rangle| \cdot |\langle h_1, \dots, h_r \rangle| \leq \ell^{\mathrm{rk}(G)} \cdot \ell^{\mathrm{rk}(H)}.$$
If E is normal in $G \times H$, then $\langle g_1, \dots, g_r \rangle$ is normal in G and $\langle h_1, \dots, h_r \rangle$ is normal in H.

□

We continue by introducing wreath products.

Remark 2.2.3 ([37, Section I.15])**.** Let G and H be finite groups, let $n \in \mathbb{N}$, and let $f : H \hookrightarrow \mathrm{Sym}(n)$ be a group monomorphism. Then
$$H \to \mathrm{Aut}(G^n) : h \mapsto ((g_1, \dots, g_n) \mapsto (g_{h^{-1}(1)}, \dots, g_{h^{-1}(n)}))$$
is a group homomorphism, and the corresponding semidirect product $G^n \rtimes_f H$ is called the ***wreath product of*** G ***and*** H ***with respect to*** f. It is denoted by $G \wr_f H$, or by $G \wr H$ if f is clear from the context, for example, if H is a subgroup of $\mathrm{Sym}(n)$ and f is the natural embedding. The elements of $G \wr_f H$ are written as $(g_1, \dots, g_n; h)$. In particular, $G \wr H$ is a group with respect to
$$(g_1, \dots, g_n; h)(g_1', \dots, g_n'; h') = (g_1 g'_{h^{-1}(1)}, \dots, g_n g'_{h^{-1}(n)}; hh'),$$
its order is $|G \wr H| = |G|^n |H|$, and
$$\{(1, \dots, 1; h) \ : \ h \in H\} \cong H$$
is a complement of the normal subgroup
$$\{(g_1, \dots, g_n; 1) \ : \ g_1, \dots, g_n \in G\} \cong G^n,$$
where the latter is also called the ***base group of*** $G \wr H$. By abuse of notation, we identify $\{(1, \dots, 1; h) \ : \ h \in H\}$ with H, and $\{(g_1, \dots, g_n; 1) \ : \ g_1, \dots, g_n \in G\}$ with G^n.
If $g : G \hookrightarrow \mathrm{Sym}(m)$ is a group monomorphism, then
$$\psi_{f,g} : G \wr_f H \hookrightarrow \mathrm{Sym}(mn) : (x_1, \dots, x_n; \sigma) \mapsto \begin{pmatrix} (i-1)m + j \\ (\sigma(i) - 1)m + x_{\sigma(i)}(j) \end{pmatrix}_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$$

is a group monomorphism as well. Now, if U is another finite group and $i : U \hookrightarrow \mathrm{Sym}(l)$ is a group monomorphism, then $(G \wr_f H) \wr_i U$ and $G \wr_{\psi_{i,g}} (H \wr_i U)$ are isomorphic. If the monomorphisms f, g, and i are clear from the context, then we also write $G \wr H \wr U := (G \wr_f H) \wr_i U$.

The following proposition will be used in the next section:

Proposition 2.2.4. *Let $\ell \in \mathbb{P}$, and let G be a finite ℓ-group.*

(a) *Let H be an ℓ-subgroup of $\mathrm{Sym}(n)$ for some $n \in \mathbb{N}$. If E is a normal subgroup of G, then E^n is a normal subgroup of $G \wr H$. In particular, $\mathrm{nrk}(G \wr H) \geq n \cdot \mathrm{nrk}(G)$.*

(b) *If $\mathrm{rk}(G) > 0$, then $\mathrm{rk}(G \wr \langle(1, \ldots, \ell)\rangle) = \ell \cdot \mathrm{rk}(G)$.*

(c) *If $\mathrm{rk}(G) = \mathrm{nrk}(G)$, then also $\mathrm{rk}(G \wr \langle(1, \ldots, \ell)\rangle) = \mathrm{nrk}(G \wr \langle(1, \ldots, \ell)\rangle)$.*

Proof.

(a) For all $g_1, \ldots, g_n \in G$, $e_1, \ldots, e_n \in E$, and $\sigma \in H$ we have

$$\begin{aligned} {}^{(g_1,\ldots,g_n;\sigma)}(e_1, \ldots, e_n; 1) &= (g_1, \ldots, g_n; \sigma)(e_1, \ldots, e_n; 1)(g_{\sigma(1)}^{-1}, \ldots, g_{\sigma(n)}^{-1}; \sigma^{-1}) \\ &= ({}^{g_1}e_{\sigma^{-1}(1)}, \ldots, {}^{g_n}e_{\sigma^{-1}(n)}; 1). \end{aligned}$$

Now, choose an elementary abelian normal subgroup E such that $|E| = \ell^{\mathrm{nrk}(G)}$. Then E^n is elementary abelian and normal in $G \wr H$, so

$$\mathrm{nrk}(G \wr H) \geq \log_\ell(|E|^n) = n \log_\ell(|E|) = n \,\mathrm{nrk}(G).$$

(b) Let $W := G \wr \langle(1, \ldots, \ell)\rangle$, and let $E \leq W$ be elementary abelian with $|E| = \ell^r$, where $r := \mathrm{rk}(W)$. Let $E = \langle g_1, \ldots, g_r\rangle$. If E is contained in the base group $B = G^\ell$, then there is nothing to show because $\mathrm{rk}(G^\ell) \leq \mathrm{rk}(G \wr \langle(1, \ldots, \ell)\rangle)$. So we may suppose that $g_1 \notin B$ and write $g_1 = (x_1, \ldots, x_\ell; \sigma)$. As $g_1 \notin B$, the permutation σ is not the identity.

After renumbering, we may assume that $\sigma = (1, \ldots, \ell)$.
Now, let $j > 2$ and write $g_j = (y_{1j}, y_{2j}, \ldots, y_{\ell j}; \sigma^{l_j})$ for $l_j \in \{0, \ldots, \ell - 1\}$. If $l_j \neq 0$, then we can consider $\tilde{g}_j := g_1^{-1} g_j^{a_j} \in B$, where $a_j := l_j^{-1}$ in $\mathbb{F}_\ell^\times$. From $g_j = g_1^{l_j} \tilde{g}_j^{l_j}$ it follows that $\langle g_1, \ldots, g_r\rangle = \langle\{g_1, \ldots, g_r, \tilde{g}_j\} \setminus \{g_j\}\rangle$, so by replacing g_j by $\tilde{g}_j$ if $l_j \neq 0$, we may assume that $E = \langle g_1, \ldots, g_r\rangle$ with $g_1 \notin B$ and $g_2, \ldots, g_r \in B$.

For all $j > 1$, we have

$$(y_{1j}x_1, \ldots, y_{\ell j}x_\ell; \sigma) = g_j g_1 = g_1 g_j = (x_1 y_{\sigma^{-1}(1),j}, \ldots, x_\ell y_{\sigma^{-1}(\ell),j}; \sigma),$$

so $y_{ij} = {}^{x_i}y_{\sigma^{-1}(i),j}$ for all i. Hence,

$$g_j = (y_{1j}, {}^{x_2}y_{1j}, {}^{x_3x_2}y_{1j}, {}^{x_4x_3x_2}y_{1j}, \dots, {}^{x_\ell \cdots x_3x_2}y_{1j}; 1). \qquad (*)$$

This implies that $\mathrm{ord}(y_{1j}) = \mathrm{ord}(g_j) = \ell$ for all $j > 1$, since taking powers of g_j is the same as taking powers of each component. As for $j, k > 1$ the elements g_j and g_k commute, the same is true for their first components y_{1j} and y_{1k}.

Suppose that there exists some $k > 1$ such that $y_{1k} \in \langle y_{1,k+1}, \dots, y_{1r}\rangle$. If $m_{k+1}, \dots, m_r \in \mathbb{Z}$ are such that $y_{1k} = y_{1,k+1}^{m_{k+1}} \cdots y_{1r}^{m_r}$, then $(*)$ implies

$$g_k = g_{k+1}^{m_{k+1}} \cdots g_r^{m_r} \in \langle g_{k+1}, \dots, g_r\rangle,$$

which is a contradiction.

Therefore, $\langle y_{12}, \dots, y_{1r}\rangle$ is an elementary abelian subgroup of G of order ℓ^{r-1}, which shows that the rank of B is at least $\ell \cdot (r-1)$. As the rank of G is non-zero, it follows from part (a) that the rank of B is at least ℓ, so $r \geq \ell \geq 2$. Thus, we have $\ell \cdot (r-1) \geq r$, that is, $\mathrm{rk}(B)$ satisfies $r \geq \mathrm{rk}(B) \geq \ell(r-1) \geq r$, proving $\mathrm{rk}(B) = r$.

We also observe from the proof that the case $E \not\subseteq B$ can only occur if $r = \ell(r-1)$, which is equivalent to $r = 1 + \frac{1}{\ell-1}$, and this in turn is equivalent to $\ell = r = 2$.

(c) For $\mathrm{rk}(G) = 0$ there is nothing to show, so let $\mathrm{rk}(G) > 0$. Then, by parts (a) and (b),

$$\mathrm{nrk}(G \wr \langle(1, \dots, \ell)\rangle) \geq \ell\, \mathrm{nrk}(G) = \ell\, \mathrm{rk}(G) = \mathrm{rk}(G \wr \langle(1, \dots, \ell)\rangle).$$

Moreover, it is clear by definition that also

$$\mathrm{nrk}(G \wr \langle(1, \dots, \ell)\rangle) \leq \mathrm{rk}(G \wr \langle(1, \dots, \ell)\rangle).$$

□

Finally, the following proposition will be used in Section 2.3, Section 2.7, and Chapter 3:

Proposition 2.2.5. *Let $n \in \mathbb{N}$, and let H be a subgroup of* $\mathrm{Sym}(n)$. *If G is a finite group with more than one element, then $Z(G \wr H)$ is the set of all $(x_1, \dots, x_n; 1) \in Z(G)^n$ such that $x_i = x_j$ whenever i and j lie in the same H-orbit.*
In particular, $Z(G \wr H) \cong Z(G)^k$, where k is the number of H-orbits on $\{1, \dots, n\}$.

Proof. Let $(x_1, \ldots, x_n; \sigma) \in Z(G \wr H)$. If $g \in G \setminus \{1\}$ and $i \in \{1, \ldots, n\}$, then

$$\begin{aligned}(1, \ldots, 1, \underset{\substack{\uparrow\\ i}}{g}, 1, \ldots, 1; 1) &= {}^{(x_1,\ldots,x_n;\sigma)}(1, \ldots, 1, \underset{\substack{\uparrow\\ i}}{g}, 1, \ldots, 1; 1)\\ &= (1, \ldots, 1, \underset{\substack{\uparrow\\ \sigma(i)}}{x_{\sigma(i)} g x_{\sigma(i)}^{-1}}, 1, \ldots, 1; 1)\end{aligned}$$

implies $\sigma(i) = i$ and $x_i g x_i^{-1} = g$. Therefore, $\sigma = 1$ and $x_1, \ldots, x_n \in Z(G)$.
Moreover,

$$(1, \ldots, 1; \tau) = {}^{(x_1,\ldots,x_n;1)}(1, \ldots, 1; \tau) = (x_1 x_{\tau^{-1}(1)}^{-1}, \ldots, x_n x_{\tau^{-1}(n)}^{-1}; \tau)$$

implies $x_{\tau(i)} = x_i$ for all $\tau \in H$.
Conversely, if $(x_1, \ldots, x_n; 1) \in Z(G)^n$ such that $x_i = x_j$ whenever i and j lie in the same H-orbit, then clearly

$${}^{(x_1,\ldots,x_n;1)}(y_1, \ldots, y_n; \tau) = (x_1 y_1 x_{\tau^{-1}(1)}^{-1}, \ldots, x_n y_n x_{\tau^{-1}(n)}^{-1}; \tau) = (y_1, \ldots, y_n; \tau)$$

for all $(y_1, \ldots, y_n; \tau) \in G \wr H$. □

2.3 A particular Sylow subgroup of a given finite symmetric group

Let $\ell \in \mathbb{P}$. Given a finite symmetric group $\mathrm{Sym}(n)$, we fix a particular Sylow ℓ-subgroup of $\mathrm{Sym}(n)$ that we will use several times in this chapter. Here, and in the remainder of this thesis, we denote by n_ℓ the largest power of the prime number ℓ dividing the non-zero integer n.

Proposition 2.3.1 ([56, page 30])**.** *Let $\ell \in \mathbb{P}$, and let $n \in \mathbb{N}$ with ℓ-adic expansion $n = a_0 + a_1\ell + \cdots + a_s\ell^s$. Then*

$$(n!)_\ell = \ell^{\frac{n-(a_0+a_1+\cdots+a_s)}{\ell-1}} = \ell^{\sum_{i=0}^{s} a_i \frac{\ell^i-1}{\ell-1}}.$$

Notation 2.3.2. Let $n \in \mathbb{N}_{>0}$, and let $a \in \mathbb{N}$. For $\sigma \in \mathrm{Sym}(n)$, let $\sigma_{+a} \in \mathrm{Sym}(\{1 + a, \ldots, n + a\})$ denote the permutation

$${}^{(1,1+a)\cdots(n,n+a)}\sigma : \{1 + a, \ldots, n + a\} \to \{1 + a, \ldots, n + a\} : k + a \mapsto \sigma(k) + a,$$

where the product $(1, 1 + a) \cdots (n, n + a)$ of transpositions belongs to $\mathrm{Sym}(1, \ldots, n + a)$. Moreover, for $S \subseteq \mathrm{Sym}(n)$, write $S_{+a} := \{\sigma_{+a} \,:\, \sigma \in \mathrm{Sym}(n)\}$. It is clear that if S is a subgroup of $\mathrm{Sym}(n)$, then S_{+a} is a subgroup of $\mathrm{Sym}(\{1 + a, \ldots, n + a\})$, and the map $S \to S_{+a} : \sigma \mapsto \sigma_{+a}$ is a group isomorphism.

Part (a) of the next proposition is well known and follows easily from [42, 4.1.20]. However, for the reader's convenience we provide a proof.

Proposition 2.3.3. *Let $\ell \in \mathbb{P}$, and let $n \in \mathbb{N}_{>0}$.*

(a) *For $i = 1, \dots, n-1$ let*

$$z_i := (1, \ell^i+1, 2\ell^i+1, \dots, (\ell-1)\ell^i+1)(2, \ell^i+2, \dots, (\ell-1)\ell^i+2)\cdots(\ell^i, 2\ell^i, \dots, \ell^{i+1}).$$

Then $\underbrace{C_\ell \wr \cdots \wr C_\ell}_{n}$ is isomorphic to

$$W_{\ell^n} := \langle (1, \dots, \ell), z_1, \dots, z_{n-1} \rangle,$$

which is a Sylow ℓ-subgroup of $\mathrm{Sym}(\ell^n)$ and whose center is the cyclic group

$$Z(W_{\ell^n}) = \langle (1, \dots, \ell)(\ell+1, \dots, 2\ell)\cdots(\ell^n - \ell + 1, \dots, \ell^n) \rangle$$

of order ℓ.

(b) *Let $n = a_0 + a_1\ell + \cdots + a_s\ell^s$ be the ℓ-adic expansion of n, let $S \in \mathrm{Syl}_\ell(\mathrm{Sym}(n))$, and let $i \in \mathbb{N}_{>0}$.*
If $a_i < \ell - 1$ or $s < i$, then

$$\langle S, (W_{\ell^i})_{+n} \rangle = S \times (W_{\ell^i})_{+n} \in \mathrm{Syl}_\ell(\mathrm{Sym}(n + \ell^i)).$$

Proof.

(a) By Remark 2.2.3 and Proposition 2.3.1, $\underbrace{C_\ell \wr \cdots \wr C_\ell}_{n}$ has order $(\ell^n!)_\ell$, and there is a monomorphism $\underbrace{C_\ell \wr \cdots \wr C_\ell}_{n} \hookrightarrow \mathrm{Sym}(\ell^n)$. The claim is obviously true for $n = 1$, so let $n > 1$. By induction, $W_{\ell^{n-1}} = \langle (1, \dots, \ell), z_1, \dots, z_{n-2} \rangle \in \mathrm{Syl}_\ell(\mathrm{Sym}(\ell^{n-1}))$ with order $|W_{\ell^{n-1}}| = (\ell^{n-1}!)_\ell = \ell^{\frac{\ell^{n-1}-1}{\ell-1}}$.
Write $z := z_{n-1}$ and

$$H := \left\langle z^i W_{\ell^{n-1}} z^{-i} \ : \ i = 0, \dots, \ell - 1 \right\rangle \leq \mathrm{Sym}(\ell^n).$$

By the definition of z, each conjugate $z^i W_{\ell^{n-1}} z^{-i}$ belongs to $\mathrm{Sym}(\left\{i\ell^{n-1} + 1, \dots, (i+1)\ell^{n-1}\right\})$, and as the sets $\left\{i\ell^{n-1} + 1, \dots, (i+1)\ell^{n-1}\right\}$ are pairwise disjoint this implies that H is an inner direct product $H = \bigtimes_{i=0}^{\ell-1} z^i W_{\ell^{n-1}} z^{-i}$.
Thus, $|H| = |W_{\ell^{n-1}}|^\ell$.
Finally, it is clear that $W_{\ell^n} = \langle W_{\ell^{n-1}}, z \rangle = \langle H, z \rangle$, and this group is an inner semidirect product $H \rtimes \langle z \rangle$. Therefore, its order is

$$|W_{\ell^n}| = |H| \cdot \ell = |W_{\ell^{n-1}}|^\ell \cdot \ell = \ell^{\ell\frac{\ell^{n-1}-1}{\ell-1}+1} = |\ell^n!|_\ell.$$

Conjugating $(1,\dots,\ell)$ with all z_i it is clear that

$$(1,\dots,\ell),(\ell+1,\dots,2\ell),\dots,(\ell^n-\ell+1,\dots,\ell^n)\in W_{\ell^n}.$$

Now, let $\sigma\in Z(W_{\ell^n})$. Then

$$\begin{aligned}\sigma &\in \bigcap_{i=1}^{\ell^{n-1}} C_{\mathrm{Sym}(\ell^n)}(\langle((i-1)\ell+1,\dots,i\ell)\rangle)\\ &= \bigcap_{i=1}^{\ell^{n-1}} \langle((i-1)\ell+1,\dots,i\ell)\rangle\times(\mathrm{Sym}(\{1,\dots,\ell^n\}\setminus\{(i-1)\ell+1,\dots,i\ell\}))\\ &= \langle(1,\dots,\ell),(\ell+1,\dots,2\ell),\dots,(\ell^n-\ell+1,\dots,\ell^n)\rangle,\end{aligned}$$

where the last equality follows from cycle decomposition in symmetric groups. This last group is elementary abelian, so σ is a unique product $\sigma=(1,\dots,\ell)^{k_1},(\ell+1,\dots,2\ell)^{k_2},\dots,(\ell^n-\ell+1,\dots,\ell^n)^{k_{\ell^{n-1}}}$. As σ has to be invariant under conjugation with all of the z_i, it follows that $k_1=k_2=\dots=k_{\ell^{n-1}}$.

(b) As $(W_{\ell^i})_{+n}$ belongs to $\mathrm{Sym}(\{n+1,\dots,n+\ell^i\})$, it follows that $\langle S,(W_{\ell^i})_{+n}\rangle$ is an inner direct product and, thus, has order $|S|\cdot|W_{\ell^i}|$. By assumption, this is

$$|S|\cdot|W_{\ell^i}|=\ell^{\frac{n-(a_0+a_1+\dots+a_r)+\ell^i-1}{\ell-1}}=((n+\ell^i)!)_\ell.$$

□

Now, we obtain the following particular Sylow subgroup of a given symmetric group. We will use this Sylow ℓ-subgroup several times in this chapter, mainly in Section 2.7.

Corollary 2.3.4. *Let $\ell\in\mathbb{P}$, and let $n\in\mathbb{N}_{>0}$ with ℓ-adic expansion $n=a_0+a_1\ell+\dots+a_s\ell^s$. Then*

$$\begin{array}{cccccc}\langle & W_{\ell^1}, & (W_{\ell^1})_{+\ell}, & \dots, & (W_{\ell^1})_{+(a_1-1)\ell}, & \\ & (W_{\ell^2})_{+a_1\ell}, & (W_{\ell^2})_{+a_1\ell+\ell^2}, & \dots, & (W_{\ell^2})_{+a_1\ell+(a_2-1)\ell^2}, & \\ & \vdots & \vdots & & \vdots & \\ & (W_{\ell^s})_{+n-a_0-a_s\ell^s}, & (W_{\ell^s})_{+n-a_0-a_s\ell^s+\ell^s}, & \dots, & (W_{\ell^s})_{+n-a_0-\ell^s} & \rangle\end{array}$$

$$= W_{\ell^1}\times(W_{\ell^1})_{+\ell}\times\dots\times(W_{\ell^1})_{+(a_1-1)\ell}\times\dots\times(W_{\ell^s})_{+n-a_0-a_s\ell^s}\times\dots\times(W_{\ell^s})_{+n-a_0-\ell^s}$$

$$\cong W_{\ell^1}^{a_1}\times\dots\times W_{\ell^s}^{a_s}$$

is a Sylow ℓ-subgroup of $\mathrm{Sym}(n)$.

Example 2.3.5. The group

$$\begin{aligned}&\langle(1,2,3)\rangle\ \times\\ &\quad\langle(4,5,6),\ (4,7,10)(5,8,11)(6,9,12),\ (4,13,22)(5,14,23)(6,15,24)\cdots(12,21,30)\rangle\end{aligned}$$

is a Sylow 3-subgroup of $\mathrm{Sym}(30)$, $\mathrm{Sym}(31)$, and $\mathrm{Sym}(32)$.

We conclude this section with the following proposition which will also be used several times in the remainder of this chapter:

Proposition 2.3.6. *Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>0}$ with ℓ-adic expansion $n = a_0 + a_1\ell + \cdots + a_s\ell^s$, and let $S \in \mathrm{Syl}_\ell(\mathrm{Sym}(n))$.*

(a) *The number of orbits of S on $\{1, \ldots, n\}$ is the ℓ-adic digit sum $a_0 + a_1 + \cdots + a_s$ of n.*

(b) *We have $\mathrm{rk}(S) = \mathrm{nrk}(S) = \frac{n-a_0}{\ell}$.*

(c) *Let G be a cyclic ℓ-group with more than one element. Then $|Z(G \wr S)| = |G|^{a_0+a_1+\cdots+a_s}$, and $G \wr S$ has an elementary abelian normal subgroup of order ℓ^n.*

Proof.

(a) It is clear that this holds for the particular Sylow ℓ-subgroup from Corollary 2.3.4. Now, as any two Sylow ℓ-subgroups are conjugate, taking another Sylow ℓ-subgroup is the same as renumbering the elements $1, \ldots, n$.

(b) By Proposition 2.3.3 and Corollary 2.3.4, S is isomorphic to

$$C_\ell^{a_1} \times (C_\ell \wr C_\ell)^{a_2} \times \cdots \times (\underbrace{C_\ell \wr \cdots \wr C_\ell}_{s})^{a_s}.$$

By part (d) of Lemma 2.2.2 and by Proposition 2.2.4, both the rank and the normal rank of this group are $a_1 + a_2\ell + \cdots + a_s\ell^{s-1} = \frac{n-a_0}{\ell}$.

(c) Part (a) and Proposition 2.2.5 imply that $|Z(G \wr S)| = |Z(G)|^{a_1+\cdots+a_s} = |G|^{a_1+\cdots+a_s}$. Moreover, by Proposition 2.2.4, the normal rank of $G \wr S$ is at least $n \cdot \mathrm{nrk}(G) = n$. □

2.4 Monomial matrices

In this short section, let $n \in \mathbb{N}_{>0}$, and let q be a prime power. Moreover, let

$$\mathrm{PerMat} : \mathrm{Sym}(n) \to \mathrm{GL}_n(q) : \sigma \mapsto (e_{\sigma(1)} \ \cdots \ e_{\sigma(n)}) = (\delta_{i\sigma(j)})_{i,j}$$

map a permutation to its permutation matrix, where e_i denotes the i-th standard basis vector.
It is well known and easily verified that

$$\det(\mathrm{PerMat}(\sigma)) = \mathrm{sign}(\sigma)$$

and

$$\mathrm{PerMat}(\sigma)^{-1} = \mathrm{PerMat}(\sigma^{-1}) = \mathrm{PerMat}(\sigma)^t$$

for all $\sigma \in \mathrm{Sym}(n)$.

We should mention that there are two different conventions in the literature for permutation matrices, differing by transposing the corresponding matrices. In our definition, $\sigma(i) = j$ means that multiplying the i-th standard basis vector e_i with $\mathrm{PerMat}(\sigma)$ from the left yields e_j, that is, e_j is the i-th column of $\mathrm{PerMat}(\sigma)$. This convention assures that the map PerMat above is a group homomorphism. Clearly, it is even a group monomorphism.

Definition 2.4.1. A matrix in $\mathrm{GL}_n(q)$ is called ***monomial***, if in each row and each column it has a unique non-zero entry. In this thesis, the set of monomial matrices in $\mathrm{GL}_n(q)$ will be denoted by $\mathrm{MonGL}_n(q)$.

Monomial matrices occur, for instance, as normalizers of tori: For $q \neq 2$, we have $\mathrm{MonGL}_n(q) = \mathrm{N}_{\mathrm{GL}_n(q)}(\{\mathrm{diag}(a_1, \ldots, a_n) \ : \ a_1, \ldots, a_n \in \mathbb{F}_q^\times\})$, see [49, Example 3.11].

The following easy and well-known facts are very important for Section 2.7:

Proposition 2.4.2.

(a) *Let $a_1, \ldots, a_n \in \mathbb{F}_q^\times$, and let $\sigma \in \mathrm{Sym}(n)$. If, for all $i = 1, \ldots, n$, we replace the entry 1 of the i-th row of $\mathrm{PerMat}(\sigma)$ by a_i, then we obtain the monomial matrix*

$$A := \mathrm{diag}(a_1, \ldots, a_n)\,\mathrm{PerMat}(\sigma) = \mathrm{PerMat}(\sigma)\,\mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)}).$$

If $A = DP = P'D'$ for permutation matrices P, P', and diagonal matrices D, D', then $P = P' = \mathrm{PerMat}(\sigma)$, $D = \mathrm{diag}(a_1, \ldots, a_n)$, and $D' = \mathrm{diag}(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$.

(b) *For all $U \leq \mathbb{F}_q^\times$ and all $H \leq \mathrm{Sym}(n)$, the map*

$$U \wr H \hookrightarrow \mathrm{GL}_n(q) : (u_1, \ldots, u_n; \sigma) \mapsto \mathrm{diag}(u_1, \ldots, u_n)\,\mathrm{PerMat}(\sigma)$$

is a group monomorphism. In particular, $\mathrm{MonGL}_n(q)$ is a subgroup of $\mathrm{GL}_n(q)$ isomorphic to $\mathbb{F}_q^\times \wr \mathrm{Sym}(n)$.

Proof.

(a) The first statement is easily verified. The second statement follows immediately from the fact that the only diagonal permutation matrix is the identity matrix.

(b) It follows from part (a) that this map is a homomorphism. The injectivity is obvious.

□

2.5 On Sylow subgroups of general linear groups

The Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{GU}_n(q)$, and $\mathrm{GO}_n^{\varepsilon}(q)$ (where $\varepsilon \in \{-1, 1\}$ whenever n is even, and where ε has no meaning for odd n) have been determined by Weir in [59] in the case $2 \neq \ell \nmid q$. Weir states that these Sylow subgroups are always direct products of iterated wreath products of certain cyclic groups, but the proofs also show that each of these Sylow subgroups of a symplectic, unitary, or orthogonal group is always isomorphic to a Sylow subgroup of a general linear group. In this section, we introduce the Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$ for $2 \neq \ell \nmid q$ following [1] and [59], and also for $\ell = 2 \nmid q$ following [13], before proving our result about the existence of small self-centralizing subgroups in such Sylow subgroups, see Theorem 2.5.10.

The following facts are well known:

Lemma 2.5.1. *Let q be a prime power, and let $m, n \in \mathbb{N}$.*

(a) *If $G \leq \mathrm{GL}_m(q)$ and $H \leq \mathrm{GL}_n(q)$, then $G \times H \hookrightarrow \mathrm{GL}_{m+n}(q) : (A, B) \mapsto \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ is a group monomorphism.*

(b) *Let $G \leq \mathrm{GL}_m(q)$, and let $P \leq \mathrm{Sym}(n)$. Then*

$$G \wr P \hookrightarrow \mathrm{GL}_{mn}(q) : (A_1, \ldots, A_n; \sigma) \mapsto \mathrm{diag}(A_1, \ldots, A_n)\,\mathrm{PerMat}(\sigma)$$

is a group monomorphism; here $\mathrm{PerMat}(\sigma)$ is the permutation matrix of σ, where the entries 0 and 1 are replaced by the zero matrix and by $\mathbb{1}_m$, respectively.

(c) *$\mathrm{GL}_n(q)$ has an element of order $q^n - 1$.*

Proof.

(a) This is obvious.

(b) Apply part (b) of Proposition 2.4.2 to block diagonal matrices instead of diagonal matrices.

(c) Choose a generator $a \in \mathbb{F}_{q^n}^{\times}$. Then the $\mathbb{F}_q$-linear map $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n} : x \mapsto ax$ has order $q^n - 1$ and may be viewed as an element of $\mathrm{GL}_n(q)$ after choosing an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$.

□

Lemma 2.5.2 ([1, Lem. 2.2]). *Let $i \in \mathbb{N}_{>0}$, let $q \in \mathbb{Z}$, and let ℓ be a prime divisor of $q - 1$. Then*

$$(q^i - 1)_\ell = \begin{cases} i_2 (q+1)_2, & \ell = 2 \mid i \text{ and } q \equiv 3 \bmod 4, \\ i_\ell (q-1)_\ell, & \text{else.} \end{cases}$$

The order of the Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$ follows immediately from Lemma 2.5.2 and the order formula $|\mathrm{GL}_n(q)| = q^{n(n-1)/2} \prod_{j=1}^{n} (q^j - 1)$.

Corollary 2.5.3. *Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>0}$, and let q be a prime power not divisible by ℓ. Let $e := \operatorname{ord}(q)$ in $\mathbb{F}_\ell^\times$, and let $r := \log_\ell((q^e-1)_\ell)$.*

(a) *Suppose that $\ell \in \mathbb{P}_{>2}$ or $q \equiv 1 \bmod 4$. Then*

$$|\operatorname{GL}_n(q)|_\ell = (q^e-1)_\ell^{\lfloor \frac{n}{e} \rfloor}(\lfloor \tfrac{n}{e} \rfloor!)_\ell = \ell^{r\lfloor \frac{n}{e} \rfloor}(\lfloor \tfrac{n}{e} \rfloor!)_\ell.$$

(b) *For $q \equiv 3 \bmod 4$ and even n one has $|\operatorname{GL}_n(q)|_2 = 2^n(q+1)_2^{n/2}((n/2)!)_2$.*

(c) *For $q \equiv 3 \bmod 4$ and odd n one has $|\operatorname{GL}_n(q)|_2 = 2|\operatorname{GL}_{n-1}(q)|_2$.*

Before stating the result on Sylow subgroups, we obtain the following easy corollary, which is important for Section 2.7:

Corollary 2.5.4. *Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>0}$, and let q be a prime power such that $\ell \mid q-1$. Moreover, let $q \equiv 1 \bmod 4$ if $\ell = 2$. Then we have $\operatorname{Syl}_\ell(\operatorname{MonGL}_n(q)) \subseteq \operatorname{Syl}_\ell(\operatorname{GL}_n(q))$.*

Proof. By part (b) of Proposition 2.4.2, $|\operatorname{MonGL}_n(q)| = |\mathbb{F}_q^\times|^n|\operatorname{Sym}(n)| = (q-1)^n n!$, so part (a) of Corollary 2.5.3 implies $|\operatorname{MonGL}_n(q)|_\ell = (q-1)_\ell^n(n!)_\ell = |\operatorname{GL}_n(q)|_\ell$. □

Remark 2.5.5. We should mention that it follows from [49, Chapter 25] and [23] that under suitable assumptions, the Sylow subgroups of finite groups of Lie type in non-defining characteristic are always contained in normalizers of tori. As already mentioned in Section 2.4, the group of monomial matrices is the normalizer of the subgroup of diagonal matrices in the general linear group, so Corollary 2.5.4 is actually a special case of this more general result. However, it is more appropriate for us to work with concrete matrices, and we will see in this chapter that the structure of the Sylow subgroups of finite classical groups of our interest can be deduced from the knowledge of the structure of the groups $\operatorname{MonGL}_n(q)$.

Now, we come to the structure of the Sylow subgroups:

Proposition 2.5.6. *Let $n \in \mathbb{N}_{>0}$, and let q be a prime power.*

(a) *Let $\ell \in \mathbb{P}$ be such that $\ell \nmid q$, and such that $q \equiv 1 \bmod 4$ if $\ell = 2$. Then the Sylow ℓ-subgroups of $\operatorname{GL}_n(q)$ are isomorphic to $C_{(q^e-1)_\ell} \wr S$, where $e := \operatorname{ord}(q)$ in $\mathbb{F}_\ell^\times$, and where $S \in \operatorname{Syl}_\ell(\operatorname{Sym}(\lfloor \frac{n}{e} \rfloor))$.*

(b) *Let $q \equiv 3 \bmod 4$.*
   - *If n is even and if $G \in \operatorname{Syl}_2(\operatorname{GL}_2(q))$, then the Sylow 2-subgroups of $\operatorname{GL}_n(q)$ are isomorphic to $G \wr S$, where $S \in \operatorname{Syl}_2(\operatorname{Sym}(\frac{n}{2}))$.*
   - *If n is odd, then the Sylow 2-subgroups of $\operatorname{GL}_n(q)$ are isomorphic to $P \times C_2$, where $P \in \operatorname{Syl}_2(\operatorname{GL}_{n-1}(q))$.*

Proof. This follows from Lemma 2.5.1 and Corollary 2.5.3 (for odd n in (b) apply part (a) of Lemma 2.5.1 to $\operatorname{GL}_{n-1}(q)$ and $\operatorname{GL}_1(q)$, and observe that a Sylow 2-subgroup of $\operatorname{GL}_1(q) = \mathbb{F}_q^\times$ has order 2). □

To complete the description of the Sylow ℓ-subgroups of the groups $\mathrm{GL}_n(q)$ for $\ell \nmid q$, it remains to determine the Sylow 2-subgroups of $\mathrm{GL}_2(q)$ for $q \equiv 3 \bmod 4$. This is done in part (b) of the following theorem. For later use, we also consider the Sylow 2-subgroups of $\mathrm{SL}_2(q)$, $\mathrm{PGL}_2(q)$, and $\mathrm{PSL}_2(q)$ for arbitrary $q > 2$:

Theorem 2.5.7. *Let q be an odd prime power.*

(a) *If $q \equiv 1 \bmod 4$, then the Sylow 2-subgroups of $\mathrm{GL}_2(q)$ are isomorphic to $C_{(q-1)_2} \wr C_2$. Their order is $2(q-1)_2^2$.*

(b) *If $q \equiv 3 \bmod 4$, then the Sylow 2-subgroups of $\mathrm{GL}_2(q)$ are semidihedral of order $4(q+1)_2$.*

(c) *The Sylow 2-subgroups of $\mathrm{SL}_2(q)$ are generalized quaternion of order $(q^2-1)_2$.*

(d) *The Sylow 2-subgroups of $\mathrm{PGL}_2(q)$ are dihedral of order $(q^2-1)_2$.*

(e) *The Sylow 2-subgroups of $\mathrm{PSL}_2(q)$ are dihedral of order $\frac{1}{2}(q^2-1)_2$ or Klein four-groups.*

Proof.

(a), (b) This is shown in [13, page 142]. Alternatively, part (a) is a special case of part (a) of Proposition 2.5.6.

(c), (e) See [37, Satz II.8.10].

(d) See [13, page 143].

□

Now, we turn to the existence of small self-centralizing subgroups of Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$ for $\ell \nmid q$.
The following fact about self-centralizing subgroups will also be helpful in the next chapter. We have not been able to find it in the existing literature.

Proposition 2.5.8. *Let G be a finite ℓ-group, let H be a subgroup of G, and let V be a self-centralizing subgroup of H. Then there exists a self-centralizing subgroup $\tilde{V}$ of G containing V such that $|\tilde{V} : V| \leq |G : H|$ and such that $\tilde{V}$ is abelian if V is.*

Proof. As there exist subgroups $H_1, \ldots, H_r$ of G such that $H = H_1 \leq H_2 \leq \cdots \leq H_r = G$ and $|H_{i+1} : H_i| = \ell$ for all $i = 1, \ldots, r-1$, it suffices to prove the claim in the case where $|G : H| = \ell$. In particular, H is normal in G.
We may assume that V is not self-centralizing in G. Then

$$C_H(V) \subseteq C_G(V) \cap V \neq C_G(V),$$

by assumption.
We choose an element $g \in C_G(V) \setminus H$. As the normal subgroup H has index ℓ in G, it

follows that $g^\ell \in H$, so $g^\ell \in H \cap C_G(V) = C_H(V) \subseteq V$.
Now, we consider the subgroup

$$\tilde{V} := \langle g \rangle V = V \langle g \rangle$$

of G, and let $x \in C_G(\tilde{V}) \subseteq C_G(V)$. Clearly, if V is abelian, then so is $\tilde{V}$. The set $\{1, g, \dots, g^{\ell-1}\}$ is a set of representatives for G/H, so there exists some $i \in \{0, \dots, \ell-1\}$ such that $x \in g^i H$. Thus, $g^{\ell-i}x \in H$. But also $g^{\ell-i}x \in C_G(V)$, so it follows that $g^{\ell-i}x \in C_G(V) \cap H = C_H(V) \subseteq V$, that is, $x \in \tilde{V}$.
Finally, we have

$$|\tilde{V} : V| = \frac{|\langle g \rangle V|}{|V|} = \frac{|\langle g \rangle||V|}{|V||\langle g \rangle \cap V|} = \frac{|\langle g \rangle|}{|\{1, g^\ell, g^{2\ell}, \dots, g^{(\mathrm{ord}(g)/\ell-1)\ell}\}|} = \frac{\mathrm{ord}(g)}{\mathrm{ord}(g)/\ell} = \ell$$

since $g^\ell \in V$. □

We need the following lemma:

Lemma 2.5.9. *Let* G *be a finite group, and let* $V \leq G$ *be a self-centralizing subgroup of* G*. If* $H \leq \mathrm{Sym}(n)$ *for some* $n \in \mathbb{N}_{>0}$*, then* V^n *is self-centralizing in* $G \wr H$*.*

Proof. Let $v \in V \setminus \{1\}$ be arbitrary, and let $x = (x_1, \dots, x_n; \sigma) \in C_{G \wr H}(V^n)$. Then, for all $i = 1, \dots, n$, it follows that

$$(1, \dots, 1, \underset{\substack{\uparrow \\ i}}{v}, 1, \dots, 1; 1) = x(1, \dots, 1, \underset{\substack{\uparrow \\ i}}{v}, 1, \dots, 1; 1)x^{-1} = (1, \dots, 1, \underset{\substack{\uparrow \\ \sigma(i)}}{x_{\sigma(i)} v x_{\sigma(i)}^{-1}}, 1, \dots, 1; 1).$$

Thus, $\sigma = 1$ and $x_i \in C_G(v)$ for all i. As v was chosen arbitrarily, this implies $x_i \in C_G(V) \subseteq V$ for all i. □

Now, we can prove our main result of this section. It turns out that the order of a Sylow ℓ-subgroup of $\mathrm{GL}_n(q)$ for $\ell \nmid q$ can always be bounded in terms of an arbitrary self-centralizing subgroup, except in the case $\ell = 2$ and $q \equiv 3 \bmod 4$, where this is not possible, as q can be arbitrarily large for fixed n:

Theorem 2.5.10. *Let* $\ell \in \mathbb{P}$*, let* $n \in \mathbb{N}_{>0}$*, let* q *be a prime power such that* $\ell \nmid q$*, and let* $G \in \mathrm{Syl}_\ell(\mathrm{GL}_n(q))$*.*

(a) *Suppose that* $\ell \in \mathbb{P}_{>2}$ *or* $q \equiv 1 \bmod 4$*. If* V *is a self-centralizing subgroup of* G*, then*
$$|G| \leq |V|^{|V|^{|V|}\log_\ell(|V|)}(|V|^{|V|}\log_\ell(|V|))!.$$

(b) *If* $\ell = 2$ *and* $q \equiv 3 \bmod 4$*, then* G *has an abelian self-centralizing subgroup of order* 2^n*.*

Proof.

(a) Let $e := \mathrm{ord}(q)$ in $\mathbb{F}_\ell^\times$. Part (c) of Proposition 2.3.6 and Theorem 2.1.5 imply

$$|(q^e - 1)_\ell| \le |Z(G)| \le |C_G(V)| \le |V|$$

and $\ell^n \le |V|^{|V|^{|V|}}$. Thus, we obtain

$$|G| = (q^e - 1)_\ell^{\lfloor \frac{n}{e} \rfloor}(\lfloor \tfrac{n}{e} \rfloor !)_\ell \le (q-1)_\ell^n (n!)_\ell \le |V|^{|V|^{|V|}\log_\ell(|V|)}(|V|^{|V|}\log_\ell(|V|))!.$$

(b) First, let n be even. By Proposition 2.5.6 and Theorem 2.5.7, G is isomorphic to $\tilde{G} \wr S$, where $\tilde{G}$ is semidihedral of order $4(q+1)_2$ and where $S \in \mathrm{Syl}_2(\mathrm{Sym}(\frac{n}{2}))$. Now, $\tilde{G}$ has a self-centralizing subgroup isomorphic to C_2^2 by Proposition 2.1.8. Therefore, the claim follows from Lemma 2.5.9.
Now, let n be odd. If $n = 1$, then the claim is certainly true. If $n > 1$, then by part (b) of Proposition 2.5.6 G isomorphic to $P \times C_2$, where $P \in \mathrm{Syl}_2(\mathrm{GL}_{n-1}(q))$. Thus, P has an abelian self-centralizing subgroup V of order 2^{n-1}. Now, Proposition 2.5.8 implies that G has an abelian self-centralizing subgroup $\tilde{V}$ containing $V \times \{1\}$ such that $|\tilde{V} : (V \times \{1\})| \le 2$. As $\{1\} \times C_2 \subseteq C_G(V \times \{1\}) \setminus (V \times \{1\})$, it follows that $|\tilde{V} : (V \times \{1\})| = 2$, so

$$|\tilde{V}| = 2 \cdot 2^{n-1} = 2^n.$$

□

Before we conclude this section, we consider the case $\ell \mid q$. First, we have the following easy observation:

Observation 2.5.11. *Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>0}$, and let q be a prime power such that $\ell \nmid q - 1$. Then the Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ are pairwise isomorphic.*

Proof. This follows immediately from $|\mathrm{GL}_n(q) : \mathrm{SL}_n(q)| = q - 1 = |Z(\mathrm{GL}_n(q))|$ and $|Z(\mathrm{SL}_n(q))| = \gcd(n, q-1) \mid q - 1$. □

Observation 2.5.12. *Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>0}$, and let q be a power of ℓ.*

(a) *The Sylow ℓ-subgroups of $\mathrm{SL}_n(q)$, $\mathrm{GL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ are isomorphic to the group $\mathrm{UT}_n(q)$ of upper unitriangular matrices.*

(b) *The center of $\mathrm{UT}_n(q)$ is the subgroup of those upper unitriangular matrices such that the only non-zero off-diagonal entry has position $(1, n)$.*

(c) *If V is a self-centralizing subgroup of $\mathrm{UT}_n(q)$, then $q \le |V|$.*

Proof.

(a) It is obvious that $\mathrm{UT}_n(q)$ is a subgroup of $\mathrm{SL}_n(q)$ of order $q^{n(n-1)/2} = |\mathrm{SL}_n(q)|_\ell$. As q is a power of ℓ, the claim follows from Observation 2.5.11.

(b) This is well known and easily verified.

(c) By part (b) and by Observation 2.1.2 we have $q = |Z(\mathrm{UT}_n(q))| \leq |C_{\mathrm{UT}_n(q)}(V)| \leq |V|$. □

Here, the question arises whether the order of a self-centralizing subgroup of $\mathrm{UT}_n(q)$ always depends on n. We will leave this question open, as it seems to be very difficult.

2.6 On Sylow subgroups of symplectic, unitary, and orthogonal groups

Following the ideas of [59], we describe the Sylow ℓ-subgroups of $\mathrm{Sp}_{2n}(q)$, $\mathrm{GU}_n(q)$, and $\mathrm{GO}_n^\varepsilon(q)$ (for $\varepsilon \in \{-1, 1\}$ whenever n is even) for $2 \neq \ell \nmid q$ and also find them as Sylow subgroups of general linear groups. Except for the unitary case, we immediately obtain the corresponding Sylow subgroups for $\mathrm{PSp}_{2n}(q)$ and the other orthogonal groups. In the unitary case, we will also find the Sylow subgroups of $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, and $\mathrm{PSU}_n(q)$ as Sylow subgroups of certain general linear groups, special linear groups, and projective (special) linear groups for odd ℓ, results that do not seem to exist in the literature. Our main results in this section are Theorem 2.6.7 and Corollary 2.6.10 about the existence of small self-centralizing subgroups of Sylow subgroups of classical groups. Thus, after this section, it remains to consider the Sylow subgroups of $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$, which will then be done in Section 2.7.

We start with symplectic and orthogonal groups. The symplectic case is very easy:

Proposition 2.6.1. *Let $\ell \in \mathbb{P}_{>2}$, let $n \in \mathbb{N}_{>0}$, let q be a prime power such that $\ell \nmid q$, and let $e := \mathrm{ord}(q)$ in $\mathbb{F}_\ell^\times$.*

(a) *Let e be even. Then*

$$|\mathrm{PSp}_{2n}(q)|_\ell = |\mathrm{Sp}_{2n}(q)|_\ell = |\mathrm{GL}_{2n}(q)|_\ell = |\mathrm{GL}_{2n+1}(q)|_\ell.$$

In particular, the Sylow ℓ-subgroups of $\mathrm{PSp}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{GL}_{2n}(q)$, and $\mathrm{GL}_{2n+1}(q)$ are pairwise isomorphic.

(b) *If e is odd, then the Sylow ℓ-subgroups of $\mathrm{PSp}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$, and $\mathrm{GL}_n(q)$ are pairwise isomorphic.*

Proof. As ℓ is odd, it follows from the order formulae of $\mathrm{PSp}_{2n}(q)$ and $\mathrm{Sp}_{2n}(q)$ that the Sylow ℓ-subgroups of these groups are pairwise isomorphic.

(a) Since e is even, ℓ does not divide $q^m - 1$ for odd m. Thus, the claim follows immediately from the order formulae for these groups because $\mathrm{Sp}_{2n}(q) \subseteq \mathrm{GL}_{2n}(q)$.

(b) If e is odd, then ℓ divides $q^m - 1$ if and only if ℓ divides $q^{2m} - 1$. Thus, it follows from the order formulae that the Sylow ℓ-subgroups of $\mathrm{PSp}_{2n}(q)$, $\mathrm{Sp}_{2n}(q)$, and $\mathrm{GL}_n(q)$ have the same order. Moreover,

$$\mathrm{GL}_n(q) \hookrightarrow \left\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix} A = \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix}\right\} : A \mapsto \begin{pmatrix} A & 0 \\ 0 & A^{t^{-1}} \end{pmatrix}$$

is a group monomorphism, and the group on the right-hand side is isomorphic to $\mathrm{Sp}_{2n}(q)$ by Theorem 1.6.10.

□

As in Section 1.6, we only consider odd q in the orthogonal case:

Proposition 2.6.2. *Let* $\ell \in \mathbb{P}_{>2}$*, let* $n \in \mathbb{N}_{>0}$*, let* q *be an odd prime power such that* $\ell \nmid q$*, and let* $e := \mathrm{ord}(q)$ *in* $\mathbb{F}_\ell^\times$*.*

(a) *Let* e *be even. Then* $|\mathrm{Spin}_{2n+1}(q)|_\ell = |\Omega_{2n+1}(q)|_\ell = |\mathrm{PGO}_{2n+1}(q)|_\ell = |\mathrm{SO}_{2n+1}(q)|_\ell = |\mathrm{GO}_{2n+1}(q)|_\ell = |\mathrm{GL}_{2n+1}(q)|_\ell = |\mathrm{GL}_{2n}(q)|_\ell$*. In particular, the Sylow* ℓ*-subgroups of* $\mathrm{Spin}_{2n+1}(q)$, $\Omega_{2n+1}(q)$, $\mathrm{PGO}_{2n+1}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{GO}_{2n+1}(q)$, $\mathrm{GL}_{2n+1}(q)$*, and* $\mathrm{GL}_{2n}(q)$ *are pairwise isomorphic.*

(b) *If* e *is odd, then the Sylow* ℓ*-subgroups of* $\mathrm{Spin}_{2n+1}(q)$, $\Omega_{2n+1}(q)$, $\mathrm{PGO}_{2n+1}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{GO}_{2n+1}(q)$*, and* $\mathrm{GL}_n(q)$ *are pairwise isomorphic.*

(c) *Let* $\varepsilon \in \{\pm 1\}$*. The Sylow* ℓ*-subgroups of* $\mathrm{Spin}_{2n}^\varepsilon(q)$, $\Omega_{2n}^\varepsilon(q)$, $\mathrm{P}\Omega_{2n}^\varepsilon(q)$, $\mathrm{PGO}_{2n}^\varepsilon(q)$, $\mathrm{SO}_{2n}^\varepsilon(q)$, $\mathrm{PSO}_{2n}^\varepsilon(q)$*, and* $\mathrm{GO}_{2n}^\varepsilon(q)$ *are pairwise isomorphic. Moreover, they are isomorphic to the Sylow* ℓ*-subgroups of* $\mathrm{GO}_{2n-1}(q)$ *or to the Sylow* ℓ*-subgroups of* $\mathrm{GO}_{2n+1}(q)$*.*

Proof. As ℓ is odd, it is clear that the Sylow ℓ-subgroups of $\mathrm{Spin}_{2n+1}(q)$, $\Omega_{2n+1}(q)$, $\mathrm{PGO}_{2n+1}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{GO}_{2n+1}(q)$ are pairwise isomorphic, and that the Sylow ℓ-subgroups of $\mathrm{Spin}_{2n}^\varepsilon(q)$, $\Omega_{2n}^\varepsilon(q)$, $\mathrm{P}\Omega_{2n}^\varepsilon(q)$, $\mathrm{PGO}_{2n}^\varepsilon(q)$, $\mathrm{SO}_{2n}^\varepsilon(q)$, $\mathrm{PSO}_{2n}^\varepsilon(q)$, and $\mathrm{GO}_{2n}^\varepsilon(q)$ are pairwise isomorphic.

(a), (b) Here, the proof is the same as for Proposition 2.6.1, if we replace the group monomorphism

$$\mathrm{GL}_n(q) \hookrightarrow \left\{A \in \mathrm{GL}_{2n}(q) \ : \ A^t \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix} A = \begin{pmatrix} & \mathbb{1}_n \\ -\mathbb{1}_n & \end{pmatrix}\right\} : A \mapsto \begin{pmatrix} A & 0 \\ 0 & A^{t^{-1}} \end{pmatrix}$$

by

$$\begin{aligned} \mathrm{GL}_n(q) &\hookrightarrow \left\{ A \in \mathrm{GL}_{2n+1}(q) \ : \ A^t \begin{pmatrix} & & \mathbb{1}_n \\ & 1 & \\ \mathbb{1}_n & & \end{pmatrix} A = \begin{pmatrix} & & \mathbb{1}_n \\ & 1 & \\ \mathbb{1}_n & & \end{pmatrix} \right\} : \\ A &\mapsto \begin{pmatrix} A & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & A^{t-1} \end{pmatrix}. \end{aligned}$$

By Theorem 1.6.13, the group on the right-hand side is isomorphic to $\mathrm{GO}_{2n+1}(q)$.

(c) We fix some $\varepsilon \in \{\pm 1\}$. By Theorem 1.6.14, we can choose an element $c \in \mathbb{F}_q^\times$ such that $\mathrm{GO}_{2n}^\varepsilon(q)$ is isomorphic to

$$G := \left\{ A \in \mathrm{GL}_{2n}(q) \ : \ A^t \operatorname{diag}(\mathbb{1}_{2n-1}, c) A = \operatorname{diag}(\mathbb{1}_{2n-1}, c) \right\}$$

(this only depends on whether or not c is a square in $\mathbb{F}_q$). Now, the map

$$\left\{ A \in \mathrm{GL}_{2n-1}(q) \ : \ A^t \operatorname{diag}(\mathbb{1}_{2n-2}, c) A = \operatorname{diag}(\mathbb{1}_{2n-2}, c) \right\} \hookrightarrow G : A \mapsto \left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

is a group monomorphism and the group on the left-hand side is isomorphic to $\mathrm{GO}_{2n-1}(q)$ by Theorem 1.6.13.
Moreover, the map

$$G \hookrightarrow \left\{ A \in \mathrm{GL}_{2n+1}(q) \ : \ A^t \operatorname{diag}(\mathbb{1}_{2n}, c) A = \operatorname{diag}(\mathbb{1}_{2n}, c) \right\} : A \mapsto \left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

is a group monomorphism and the group on the right-hand side is isomorphic to $\mathrm{GO}_{2n+1}(q)$ by Theorem 1.6.13.
Finally, recall that

$$|\,\mathrm{GO}_{2n+1}(q)| = 2q^{n^2} \prod_{i=1}^{n} (q^{2i} - 1)$$

and

$$|\,\mathrm{GO}_{2n}^\varepsilon(q)| = 2q^{n(n-1)}(q^n - \varepsilon) \prod_{i=1}^{n-1} (q^{2i} - 1).$$

If $\ell \nmid (q^n - \varepsilon)$, then it follows that the Sylow ℓ-subgroups of $\mathrm{GO}_{2n}^\varepsilon(q)$ are isomorphic to those of $\mathrm{GO}_{2n-1}(q)$. If $\ell \mid (q^n - \varepsilon)$, then the Sylow ℓ-subgroups of $\mathrm{GO}_{2n}^\varepsilon(q)$ are isomorphic to those of $\mathrm{GO}_{2n+1}(q)$.

□

Now, we come to the unitary case.

Lemma 2.6.3. *Let q be a prime power, and let $m, n \in \mathbb{N}$.*

(a) *If $G \leq \mathrm{GU}_m(q)$ and $H \leq \mathrm{GU}_n(q)$, then $G \times H \hookrightarrow \mathrm{GU}_{m+n}(q) : (A, B) \mapsto \left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$ is a group monomorphism.*

(b) *Let* $G \leq \mathrm{GU}_m(q)$*, and let* $P \leq \mathrm{Sym}(n)$*. Then*

$$G \wr P \hookrightarrow \mathrm{GU}_{mn}(q) : (A_1, \ldots, A_n; \sigma) \mapsto \mathrm{diag}(A_1, \ldots, A_n)\,\mathrm{PerMat}(\sigma)$$

is a group monomorphism, where $\mathrm{PerMat}(\sigma)$ *is the permutation matrix of* σ*, where the entries* 0 *and* 1 *are replaced by the zero matrix and by* $\mathbb{1}_m$*, respectively.*

(c) *There exists a group monomorphism* $\mathrm{GL}_{\lfloor n/2 \rfloor}(q^2) \hookrightarrow \mathrm{GU}_n(q)$*.*

Proof.

(a) This follows immediately from the description

$$\mathrm{GU}_n(q) \cong \left\{ A \in \mathrm{GL}_n(q^2) \ : \ \overline{A}^t A = \mathbb{1}_n \right\}$$

of Theorem 1.6.12.

(b) Again, use the description

$$\mathrm{GU}_n(q) \cong \left\{ A \in \mathrm{GL}_n(q^2) \ : \ \overline{A}^t A = \mathbb{1}_n \right\}.$$

Let $(A_1, \ldots, A_n; \sigma) \in G \wr P$, and write $X := \mathrm{diag}(A_1, \ldots, A_n)\,\mathrm{PerMat}(\sigma)$. Then

$$\begin{aligned} \overline{X}^t X &= (\mathrm{diag}(\overline{A}_1, \ldots, \overline{A}_n)\,\mathrm{PerMat}(\sigma))^t X \\ &= \mathrm{PerMat}(\sigma)^t\,\mathrm{diag}(\overline{A}_1^t, \ldots, \overline{A}_n^t)\,\mathrm{diag}(A_1, \ldots, A_n)\,\mathrm{PerMat}(\sigma) \\ &= \mathbb{1}_{mn}. \end{aligned}$$

Thus, the claim follows from part (b) of Lemma 2.5.1.

(c) We write $m := \lfloor \frac{n}{2} \rfloor$. By part (b) of Theorem 1.6.12, the group $\mathrm{GU}_{2m}(q)$ is isomorphic to

$$G := \left\{ A \in \mathrm{GL}_{2m}(q^2) \ : \ \overline{A}^t \begin{pmatrix} 0 & \mathbb{1}_m \\ \mathbb{1}_m & 0 \end{pmatrix} A = \begin{pmatrix} 0 & \mathbb{1}_m \\ \mathbb{1}_m & 0 \end{pmatrix} \right\}.$$

The map

$$\mathrm{GL}_m(q^2) \to G : A \mapsto \begin{pmatrix} A & 0 \\ 0 & \overline{A^t}^{-1} \end{pmatrix}$$

is a group monomorphism, and it follows from part (a) that there exists a group monomorphism

$$G \cong \mathrm{GU}_{2m}(q) \hookrightarrow \mathrm{GU}_n(q).$$

□

Proposition 2.6.4. *Let* $\ell \in \mathbb{P}_{>2}$*, let* $n \in \mathbb{N}_{>0}$*, and let* q *be a prime power not divisible by* ℓ*. Let* $e := \mathrm{ord}(q)$ *in* $\mathbb{F}_\ell^\times$*, and let* $r := \log_\ell((q^e - 1)_\ell)$*. Then*

$$|\,\mathrm{GU}_n(q)|_\ell = \begin{cases} |\,\mathrm{GL}_n(q^2)|_\ell, & e \equiv 2 \bmod 4, \\ |\,\mathrm{GL}_n(q)|_\ell, & e \equiv 0 \bmod 4, \\ |\,\mathrm{GL}_{\lfloor n/2 \rfloor}(q^2)|_\ell, & e \text{ odd.} \end{cases}$$

Proof. Recall from Theorem 1.6.12 that $|\,\mathrm{GU}_n(q)| = q^{n(n-1)/2}\prod_{j=1}^{n}(q^j-(-1)^j)$. Let $j \in \{1,\dots,n\}$ be such that $\ell \mid q^j-(-1)^j$. First, let e be even. Then $q^{2j}=1$ in $\mathbb{F}_\ell^\times$ implies that $e \mid 2j$.
If $e \equiv 0 \bmod 4$, then this shows that j is even, so it follows that

$$|\,\mathrm{GU}_n(q)|_\ell = \prod_{j=1}^{n}(q^j-(-1)^j)_\ell = \prod_{j=1}^{n}(q^j-1)_\ell = |\,\mathrm{GL}_n(q)|_\ell$$

in this case.
Now, let $e \equiv 2 \bmod 4$. Then $t := \frac{2j}{e}$ is odd, since otherwise $q^j = (q^e)^{\frac{t}{2}} = 1 \neq -1$ in $\mathbb{F}_\ell^\times$ would imply that $\ell \nmid q^j+1 = q^j-(-1)^j$. It follows that j is odd, too, and that $(q^j-(-1)^j)_\ell = (q^j+1)_\ell = (q^j-1)_\ell(q^j+1)_\ell = (q^{2j}-1)_\ell$. Therefore,

$$|\,\mathrm{GU}_n(q)|_\ell = \prod_{j=1}^{n}(q^j-(-1)^j)_\ell = \prod_{j=1}^{n}(q^{2j}-1)_\ell = |\,\mathrm{GL}_n(q^2)|_\ell.$$

Finally, let e be odd. Then j must be even since otherwise we would have $1 = q^{je} = (q^j)^e = (-1)^e = -1$ in $\mathbb{F}_\ell^\times$. Thus,

$$|\,\mathrm{GU}_n(q)|_\ell = \prod_{j=1}^{n}(q^j-(-1)^j)_\ell = \prod_{i=1}^{\lfloor n/2\rfloor}(q^{2i}-1)_\ell = |\,\mathrm{GL}_{\lfloor n/2\rfloor}(q^2)|_\ell.$$

□

Proposition 2.6.5. *Let $n \in \mathbb{N}_{>0}$, and let q be a prime power. Let $\ell \in \mathbb{P}_{>2}$ be such that $\ell \nmid q$. Moreover, let $e := \mathrm{ord}(q)$ in $\mathbb{F}_\ell^\times$.*

(a) *If $e \equiv 2 \bmod 4$, then $\mathrm{Syl}_\ell(\mathrm{GU}_n(q)) \subseteq \mathrm{Syl}_\ell(\mathrm{GL}_n(q^2))$, $\mathrm{Syl}_\ell(\mathrm{SU}_n(q)) \subseteq \mathrm{Syl}_\ell(\mathrm{SL}_n(q^2))$, the Sylow ℓ-subgroups of $\mathrm{PGU}_n(q)$ are isomorphic to those of $\mathrm{PGL}_n(q^2)$, and the Sylow ℓ-subgroups of $\mathrm{PSU}_n(q)$ are isomorphic to those of $\mathrm{PSL}_n(q^2)$.*

(b) *If $e \equiv 0 \bmod 4$, then the Sylow ℓ-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to the Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$.*

(c) *If e is odd, then the Sylow ℓ-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to the Sylow ℓ-subgroups of $\mathrm{GL}_{\lfloor n/2\rfloor}(q^2)$.*

Proof.

(a) If $e \equiv 2 \bmod 4$, then the inclusion $\mathrm{Syl}_\ell(\mathrm{GU}_n(q)) \subseteq \mathrm{Syl}_\ell(\mathrm{GL}_n(q^2))$ is clear by Proposition 2.6.4. As $e \neq 1$, we have $\ell \nmid q-1$. This implies

$$|\,\mathrm{GL}_n(q^2):\mathrm{SL}_n(q^2)|_\ell = (q^2-1)_\ell = (q+1)_\ell(q-1)_\ell = (q+1)_\ell = |\,\mathrm{GU}_n(q):\mathrm{SU}_n(q)|_\ell,$$

so it follows that $\mathrm{Syl}_\ell(\mathrm{SU}_n(q)) \subseteq \mathrm{Syl}_\ell(\mathrm{SL}_n(q^2))$ as we have $\mathrm{SU}_n(q) \subseteq \mathrm{SL}_n(q^2)$. Moreover, it follows from $Z(\mathrm{GU}_n(q)) = Z(\mathrm{GL}_n(q^2)) \cap \mathrm{GU}_n(q)$ in part (d) of Theorem 1.6.12 that the maps

$$\mathrm{PGU}_n(q) \to \mathrm{PGL}_n(q^2) : A\, Z(\mathrm{GU}_n(q)) \mapsto A\, Z(\mathrm{GL}_n(q^2))$$

and

$$\mathrm{PSU}_n(q) \to \mathrm{PSL}_n(q^2) : A\, Z(\mathrm{SU}_n(q)) \mapsto A\, Z(\mathrm{SL}_n(q^2))$$

are (well defined and) group monomorphisms. Thus, the claim follows from

$$|\,\mathrm{PGU}_n(q)|_\ell = \frac{|\,\mathrm{GU}_n(q)|_\ell}{(q+1)_\ell} = \frac{|\,\mathrm{GL}_n(q^2)|_\ell}{(q+1)_\ell} = \frac{|\,\mathrm{GL}_n(q^2)|_\ell}{(q^2-1)_\ell} = |\,\mathrm{PGL}_n(q^2)|_\ell$$

and

$$|\,\mathrm{PSU}_n(q)|_\ell = \frac{|\,\mathrm{GU}_n(q)|_\ell}{(q+1)_\ell \gcd(n, q+1)_\ell} = \frac{|\,\mathrm{GL}_n(q^2)|_\ell}{(q^2-1)_\ell \gcd(n, q^2-1)_\ell} = |\,\mathrm{PSL}_n(q^2)|_\ell.$$

(b) Now, let $e \equiv 0 \bmod 4$. By part (c) of Lemma 2.5.1 and part (d) of Lemma 2.6.3, $\mathrm{GU}_e(q)$ has an element of order $(q^2)^{\frac{e}{2}} - 1 = q^e - 1$. Now parts (a) and (b) of Lemma 2.6.3 and Proposition 2.6.4 imply that the Sylow ℓ-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to $C_{(q^e-1)_\ell} \wr S$, where $S \in \mathrm{Syl}_\ell(\mathrm{Sym}(\lfloor \frac{n}{e} \rfloor))$. By part (a) of Proposition 2.5.6, this group is isomorphic to a Sylow ℓ-subgroup of $\mathrm{GL}_n(q)$.

(c) Finally, if e is odd, then the claim follows from part (c) of Lemma 2.6.3 and Proposition 2.6.4.

□

We obtain the following corollary:

Corollary 2.6.6. *Let $n \in \mathbb{N}_{>0}$, let q be a prime power, and let $\ell \in \mathbb{P}_{>2}$ be such that $\ell \nmid q$.*

(a) *There exists some $H \in \{\mathrm{GL}_n(q^2), \mathrm{GL}_n(q), \mathrm{GL}_{\lfloor n/2 \rfloor}(q^2)\}$ such that the Sylow ℓ-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to the Sylow ℓ-subgroups of H.*

(b) *If $\ell \nmid q+1$, then the Sylow ℓ-subgroups of $\mathrm{GU}_n(q)$, $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, and $\mathrm{PSU}_n(q)$ are pairwise isomorphic.*

(c) *If $\ell \mid q+1$, then the Sylow ℓ-subgroups of $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, and $\mathrm{PSU}_n(q)$ are isomorphic to those of $\mathrm{SL}_n(q^2)$, $\mathrm{PGL}_n(q^2)$, and $\mathrm{PSL}_n(q^2)$, respectively.*

Proof.

(a) This is clear by Proposition 2.6.5.

(b) This follows immediately from $|\mathrm{GU}_n(q) : \mathrm{SU}_n(q)| = q+1 = |Z(\mathrm{GU}_n(q))|$ and $|Z(\mathrm{SU}_n(q))| = \gcd(n, q+1) \mid q+1$.

(c) If $\ell \mid q+1$, then $\ell > 2$ implies that the order of q in $\mathbb{F}_\ell^\times$ is 2. Thus, the claim follows immediately from part (a) of Proposition 2.6.5. □

Now, we come to the main result of this section:

Theorem 2.6.7. *Let $n \in \mathbb{N}_{>0}$, let q be a prime power, and let $\ell \in \mathbb{P}_{>2}$ be such that $\ell \nmid q$. Let $\varepsilon \in \{\pm 1\}$ and let G be a Sylow ℓ-subgroup of one of the classical groups $\mathrm{GL}_n(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{PSp}_{2n}(q)$, $\mathrm{Spin}_{2n+1}(q)$, $\Omega_{2n+1}(q)$, $\mathrm{PGO}_{2n+1}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{GO}_{2n+1}(q)$, $\mathrm{Spin}^\varepsilon_{2n}(q)$, $\Omega^\varepsilon_{2n}(q)$, $\mathrm{P}\Omega^\varepsilon_{2n}(q)$, $\mathrm{PGO}^\varepsilon_{2n}(q)$, $\mathrm{SO}^\varepsilon_{2n}(q)$, $\mathrm{PSO}^\varepsilon_{2n}(q)$, $\mathrm{GO}^\varepsilon_{2n}(q)$, or $\mathrm{GU}_n(q)$. Then $|G|$ can be bounded in terms of any self-centralizing subgroup of G.*

Proof. We have seen in this section that G is isomorphic to a Sylow ℓ-subgroup of some general linear group $\mathrm{GL}_{\tilde{n}}(\tilde{q})$ such that $\ell \nmid \tilde{q}$. Therefore, the claim follows immediately from part (a) of Theorem 2.5.10. □

For the remainder of this section, we consider the Sylow 2-subgroups for unitary groups and study the existence of small self-centralizing subgroups in this case, too. This is done similarly to the case of general linear groups in the previous section.

Proposition 2.6.8. *Let $n \in \mathbb{N}_{>0}$, and let q be an odd prime power.*

(a) *If $q \equiv 3 \bmod 4$, then $|\mathrm{GU}_n(q)|_2 = (q+1)_2^n (n!)_2$, and the Sylow 2-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to $C_{(q+1)_2} \wr S$, where $S \in \mathrm{Syl}_\ell(\mathrm{Sym}(n))$.*

(b) *For $q \equiv 1 \bmod 4$ and even n we have $|\mathrm{GU}_n(q)|_2 = 2^n (q-1)_2^{n/2}((n/2)!)_2$, and the Sylow 2-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to $G \wr S$, where $G \in \mathrm{Syl}_2(\mathrm{GU}_2(q))$ and $S \in \mathrm{Syl}_2(\mathrm{Sym}(\frac{n}{2}))$.*

(c) *For $q \equiv 1 \bmod 4$ and odd n we have $|\mathrm{GU}_n(q)|_2 = 2|\mathrm{GU}_{n-1}(q)|_2$, and the Sylow 2-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to $P \times C_2$, where $P \in \mathrm{Syl}_2(\mathrm{GU}_{n-1}(q))$.*

Proof.

(a) We have

$$|\mathrm{GU}_n(q)|_2 = \prod_{j=1}^{n} (q^j - (-1)^j)_2 = \prod_{\substack{j=1 \\ 2\nmid j}}^{n} (q^j+1)_2 \cdot \prod_{\substack{j=1 \\ 2\mid j}}^{n} (q^j-1)_2.$$

Now, the first claim follows from $(q^j+1)_2 = \frac{1}{2}(q^{2j}-1)_2$ and from Lemma 2.5.2. Moreover, from the description

$$\mathrm{GU}_n(q) \cong \left\{ A \in \mathrm{GL}_n(q^2) \ : \ \overline{A}^t A = \mathbb{1}_n \right\}$$

in Theorem 1.6.12 it follows that $\mathrm{GU}_1(q)$ is cyclic of order $q+1$. Therefore, part (b) of Lemma 2.6.3 implies that the Sylow 2-subgroups of $\mathrm{GU}_n(q)$ are isomorphic to $C_{(q+1)_2} \wr S$.

(b), (c) The orders of the Sylow 2-subgroups follow from Lemma 2.5.2 similarly as in part (a). Now, their structure follows from parts (a) and (b) of Lemma 2.6.3. □

It remains to determine the Sylow 2-subgroups of $\mathrm{GU}_2(q)$ for $q \equiv 1 \bmod 4$. As in the case of general linear groups, we also provide the Sylow 2-subgroups of special and projective (special) unitary groups for later use. For the latter we also give proofs for the reader's convenience, since they seem to be hard to find in the literature.

Theorem 2.6.9. *Let q be an odd prime power.*

(a) *If $q \equiv 3 \bmod 4$, then the Sylow 2-subgroups of $\mathrm{GU}_2(q)$ are isomorphic to $C_{(q+1)_2} \wr C_2$. Their order is $2(q+1)_2^n$.*

(b) *If $q \equiv 1 \bmod 4$, then the Sylow 2-subgroups of $\mathrm{GU}_2(q)$ are semidihedral of order $4(q-1)_2$.*

(c) *The Sylow 2-subgroups of $\mathrm{PGU}_2(q)$ are isomorphic to those of $\mathrm{PGL}_2(q)$ and, thus, dihedral of order $(q^2-1)_2$.*

(d) *The Sylow 2-subgroups of $\mathrm{SU}_2(q)$ are isomorphic to those of $\mathrm{SL}_2(q)$ and, thus, generalized quaternion of order $(q^2-1)_2$.*

(e) *The Sylow 2-subgroups of $\mathrm{PSU}_2(q)$ are isomorphic to those of $\mathrm{PSL}_2(q)$ and, thus, dihedral of order $\frac{1}{2}(q^2-1)_2$ or Klein four-groups.*

Proof.

(a), (b) See [13, page 143]. Alternatively, part (a) is a special case of part (a) of Proposition 2.6.8.

(c), (d), (e) Even the groups themselves are isomorphic: $\mathrm{PGU}_2(q) \cong \mathrm{PGL}_2(q)$, $\mathrm{SU}_2(q) \cong \mathrm{SL}_2(q)$, and $\mathrm{PSU}_2(q) \cong \mathrm{PSL}_2(q)$, see, for example, [49]. We give an alternative proof for the assertions of the theorem. For a finite group G, we denote by $O_2(G)$ the largest normal 2-subgroup of G.
We easily obtain $|\mathrm{PGU}_2(q)|_2 = |\mathrm{PGL}_2(q)|_2$, $|\mathrm{SU}_2(q)|_2 = |\mathrm{SL}_2(q)_2$, and $|\mathrm{PSU}_2(q)|_2 = |\mathrm{PSL}_2(q)|_2$ from the order formulae in Theorem 1.6.12.
First, let $q \equiv 3 \bmod 4$. Let

$$T := \mathrm{PerMat}(1,2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GU}_2(q).$$

Then

$$G := \{\mathrm{diag}(a, b) \ : \ a, b \in O_2(\mathrm{GU}_1(q))\} \rtimes \langle T \rangle$$

is a Sylow 2-subgroup of $\mathrm{GU}_2(q)$ by part (a) using the description

$$\mathrm{GU}_n(q) \cong \left\{ A \in \mathrm{GL}_n(q^2) \ : \ \overline{A}^t A = \mathbb{1}_n \right\}$$

in Theorem 1.6.12. (In fact, this is the Sylow 2-subgroup from [13, page 143]). Writing $Z := O_2(\mathrm{GU}_1(q)) \cdot \mathbb{1}_2$, we have $G/Z \in \mathrm{Syl}_2(\mathrm{PGU}_2(q))$. Let $\alpha \in \mathrm{GU}_1(q)$ have order $(q+1)_2$. Then $X := \mathrm{diag}(\alpha, 1)$ satisfies $\mathrm{ord}(XZ) = (q+1)_2$ and $XTXT = \mathrm{diag}(\alpha, \alpha) \in Z$, so $TXTZ = (XZ)^{-1}$ in G/Z. As T has order 2 and G/Z has order $|\mathrm{PGU}_2(q)|_2 = (q^2-1)_2 = 2(q+1)_2$, it follows that G/Z is dihedral. Now, let us write $A := \mathrm{diag}(\alpha, \alpha^{-1})$ and $X := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Obviously, the group $G := \langle A, X \rangle$ is contained in $\mathrm{SU}_2(q)$ and we have $XAX^{-1} = A^{-1}$. Thus, $G = \langle A \rangle \langle X \rangle$ with $\langle A \rangle \cap \langle X \rangle = \{\pm \mathbb{1}_2\}$. It follows that G is generalized quaternion of order $2(q+1)_2 = |\mathrm{SU}_2(q)|_2$. Moreover, G/Z is a Sylow 2-subgroup of $\mathrm{PSU}_2(q)$, where $Z := O_2(\mathrm{GU}_1(q)) \cdot \mathbb{1}_2 \cap \mathrm{SL}_2(q) = \{\mathbb{1}_2, -\mathbb{1}_2\}$. As AZ has order $\frac{1}{2}\,\mathrm{ord}(\alpha) = \frac{1}{2}(q+1)_2$ and XZ has order 2 in G/Z, it follows from $XAX^{-1} = A^{-1}$ that G/Z is a dihedral group of order $(q+1)_2$ or a Klein four-group.

Now, let $q \equiv 1 \bmod 4$. We use the description

$$\mathrm{GU}_2(q) \cong \left\{ A \in \mathrm{GL}_2(q^2) \ : \ A \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \overline{A}^t = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$$

in Theorem 1.6.12. The Sylow 2-subgroup for $\mathrm{GU}_2(q)$ in part (b) from [13, page 143] is given by $\langle A, X \rangle$, where $A := \mathrm{diag}(\alpha, \alpha^{-q})$ and $X := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and where $\alpha \in \mathbb{F}_{q^2}^\times$ has order $(q^2-1)_2 = 2(q-1)_2$. We have $\alpha^q = -\alpha$ and $XAX = \mathrm{diag}(\alpha^{-q}, \alpha) = A^{(q-1)_2 - 1}$. Now, we write $Z := O_2(\mathrm{GU}_1(q)) \cdot \mathbb{1}_n$. Then $\langle A, X \rangle / Z \in \mathrm{Syl}_2(\mathrm{PGU}_2(q))$ by Theorem 1.6.12. As $\mathrm{ord}(AZ) = (q-1)_2$ and $\mathrm{ord}(XZ) = 2$ in $\langle A, X \rangle / Z$, and as $AXAX = \mathrm{diag}(\alpha^{1-q}, \alpha^{1-q}) \in Z$, it follows that $XAXZ = (AZ)^{-1}$ in $\langle A, X \rangle / Z$. Therefore, $\langle A, X \rangle / Z$ is dihedral. Moreover, as $\det(A^2) = 1$ and $\det(AX) = 1$ (this holds since $\alpha^{q-1} = (-1)^{(q-1)_{2'}} = -1$), we have that $\left\langle A^2, AX \right\rangle$ must be a generalized quaternion group as the generators satisfy the relation from Remark 2.1.7 and the group has the correct order. Now, for $\mathrm{PSU}_2(q)$, we easily obtain a dihedral group or a Klein four-group with the same argument as for $\mathrm{PGU}_2(q)$. □

Finally, we obtain the following result for self-centralizing subgroups of Sylow 2-subgroups for general unitary groups:

Corollary 2.6.10. *Let $n \in \mathbb{N}_{>0}$, let q be an odd prime power, and let $G \in \mathrm{Syl}_2(\mathrm{GU}_n(q))$.*

(a) *If $q \equiv 3 \bmod 4$ and if V is a self-centralizing subgroup of G, then*

$$|G| \leq |V|^{|V|^{|V|} \log_2(|V|)} (|V|^{|V|} \log_2(|V|))!.$$

(b) *If* $q \equiv 1 \bmod 4$*, then* G *has an abelian self-centralizing subgroup of order* 2^n*.*

Proof.

(a) Part (c) of Proposition 2.3.6 and Theorem 2.1.5 show that $|(q+1)_2| \le |Z(G)| \le |C_G(V)| \le |V|$ and $2^n \le |V|^{|V|^{|V|}}$. Hence, in this case the claim follows from $|G| = (q+1)_2^n (n!)_2$.

(b) Here, the proof is analogous to the proof of part (b) of Theorem 2.5.10. □

2.7 On Sylow subgroups of special and projective (special) linear groups

Now, we turn to Sylow ℓ-subgroups of $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ for $\ell \nmid q$. First, we reduce to the case $\ell \mid \gcd(n, q-1)$. Then, we define particular Sylow ℓ-subgroups that we can work with.
Calculations involving the exponents and the center of the groups as well as particular elementary abelian normal subgroups will finally lead to the following result (Theorem 2.7.14): If we are not in the case $\ell = 2$ and $q \equiv 3 \bmod 4$, then small self-centralizing subgroups of the considered Sylow ℓ-subgroups exist if and only if $\ell \mid q-1$ and $n > 1$ is a power of ℓ. The case $\ell = 2$ and $q \equiv 3 \bmod 4$ will not be considered as it seems to be much more complicated. We did not find any of the statements and proofs of this section in the literature.

2.7.1 Reduction to the case $\ell \mid \gcd(n, q-1)$

Proposition 2.7.1. *Let* $\ell \in \mathbb{P}$*, let* $n \in \mathbb{N}_{>0}$*, and let* q *be a prime power such that* $\ell \mid q-1$ *and* $\ell \nmid n$*. Then the Sylow* ℓ*-subgroups of* $\mathrm{SL}_n(q)$*,* $\mathrm{PGL}_n(q)$*, and* $\mathrm{PSL}_n(q)$ *are isomorphic to those of* $\mathrm{GL}_{n-1}(q)$*.*

Proof. It follows from $|Z(\mathrm{SL}_n(q))|_\ell = \gcd(n, q-1)_\ell = 1$ that the Sylow ℓ-subgroups of $\mathrm{PSL}_n(q)$ are isomorphic to those of $\mathrm{SL}_n(q)$.
Moreover, if $r \in \mathbb{N}_{>0}$ satisfies $\ell^r = (q-1)_\ell$, then $|\mathrm{SL}_n(q)|_\ell = \frac{|\mathrm{GL}_n(q)|_\ell}{\ell^r} = |\mathrm{PGL}_n(q)|_\ell$. Thus, if $\ell > 2$, or $\ell = 2$ and $q \equiv 1 \bmod 4$, then

$$\frac{|\mathrm{GL}_n(q)|_\ell}{\ell^r} = \ell^{r(n-1)}(n!)_\ell = n_\ell |\mathrm{GL}_{n-1}(q)|_\ell = |\mathrm{GL}_{n-1}(q)|_\ell$$

by part (a) of Corollary 2.5.3. If $\ell = 2$ and $q \equiv 3 \bmod 4$, then part (c) of Corollary 2.5.3 shows

$$\frac{|\mathrm{GL}_n(q)|_2}{2^r} = \frac{1}{2}|\mathrm{GL}_n(q)|_2 = |\mathrm{GL}_{n-1}(q)|_2.$$

Moreover,

$$\mathrm{GL}_{n-1}(q) \hookrightarrow \mathrm{SL}_n(q) : A \mapsto \begin{pmatrix} A & \\ & \det(A)^{-1} \end{pmatrix}$$

and

$$\mathrm{GL}_{n-1}(q) \hookrightarrow \mathrm{PGL}_n(q) : A \mapsto \begin{pmatrix} A & \\ & 1 \end{pmatrix} Z(\mathrm{GL}_n(q))$$

are group monomorphisms. □

Together with Observation 2.5.11, Proposition 2.7.1 now implies that in order to study Sylow ℓ-subgroups of $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ for $\ell \nmid q$, it suffices to consider the case $\ell \mid \gcd(n, q-1)$.

2.7.2 The setting

We will use the following objects. Here and in the remainder of this thesis, $O_\ell(G)$ denotes the largest normal ℓ-subgroup of the finite group G. Thus, if G is abelian, then $O_\ell(G)$ is the unique Sylow ℓ-subgroup of G.

For the remainder of Section 2.7, we fix a prime $\ell \in \mathbb{P}$, a positive integer $n \in \mathbb{N}_{>0}$, and a prime power q such that $\ell \mid \gcd(n, q-1)$, and such that $q \equiv 1 \bmod 4$ if $\ell = 2$.

Let $n = a_1\ell + \cdots + a_s\ell^s$ be the ℓ-adic expansion of n, and let $Q = a_1 + \cdots + a_s$ be its ℓ-adic digit sum.

Let $r \in \mathbb{N}_{>0}$ such that $\ell^r = (q-1)_\ell$, and let $\alpha \in \mathbb{F}_q^\times$ be an element of order ℓ^r. Thus, α generates $O_\ell(\mathbb{F}_q^\times)$.

Moreover, we write

$$T := \left\{\mathrm{diag}(d_1, \ldots, d_n) \;:\; d_1, \ldots, d_n \in O_\ell(\mathbb{F}_q^\times)\right\} \cong C_{\ell^r}^n$$

and

$$\begin{aligned} \tilde{T} &:= T \cap \mathrm{SL}_n(q) \\ &= \left\{\mathrm{diag}(d_1, \ldots, d_{n-1}, (d_1 \cdots d_{n-1})^{-1}) \;:\; d_1, \ldots, d_{n-1} \in O_\ell(\mathbb{F}_q^\times)\right\} \cong C_{\ell^r}^{n-1}, \end{aligned}$$

and we denote by S the particular Sylow ℓ-subgroup of $\mathrm{Sym}(n)$ from Corollary 2.3.4.

Finally, we write

$$\begin{aligned} Z &:= O_\ell(Z(\mathrm{GL}_n(q))) = O_\ell(\mathbb{F}_q^\times) \cdot \mathbb{1}_n \cong C_{\ell^r}, \\ \delta &:= \mathrm{diag}(-1, 1, \ldots, 1) \in \mathbb{F}_q^{n \times n}, \end{aligned}$$

and

$$A := \left\{\mathrm{diag}(\mathbb{1}_{n/\ell}, c \cdot \mathbb{1}_{n/\ell}, c^2 \cdot \mathbb{1}_{n/\ell}, \ldots, c^{\ell-1} \cdot \mathbb{1}_{n/\ell}) \;:\; c \in \left\langle \alpha^{\ell^{r-1}} \right\rangle\right\} \cong C_\ell.$$

2.7.3 The groups

Proposition 2.7.2. *The group*

$$G := \langle T, \mathrm{PerMat}(S)\rangle = T \rtimes \mathrm{PerMat}(S) \cong O_\ell(\mathbb{F}_q^\times) \wr S$$

is a Sylow ℓ-subgroup of $\mathrm{MonGL}_n(q)$ *and, thus, also of* $\mathrm{GL}_n(q)$. *In particular,* $|G| = \ell^{rn}(n!)_\ell$. *Its center has order* $|Z(G)| = \ell^{rQ}$. *In fact,*

$$Z(G) = C_T(\mathrm{PerMat}(S)),$$

that is, $Z(G)$ *is the set of all* $\mathrm{diag}(d_1, \ldots, d_n) \in T$ *such that for all* $i = 1, \ldots, s$ *with* $a_i > 0$ *and all* $j = 0, \ldots, a_i - 1$ *we have*

$$d_{a_1\ell+\cdots+a_{i-1}\ell^{i-1}+j\ell^i+1} = d_{a_1\ell+\cdots+a_{i-1}\ell^{i-1}+j\ell^i+2} = \cdots = d_{a_1\ell+\cdots+a_{i-1}\ell^{i-1}+(j+1)\ell^i}.$$

Moreover, if $D \in T$ *and* $P \in \mathrm{PerMat}(S)$ *are such that* $DP \in C_G(\mathrm{PerMat}(S))$, *then* $D \in Z(G)$ *and*

$$P \in Z(\mathrm{PerMat}(S)) \subseteq \mathrm{PerMat}(\big\langle (1, \ldots, \ell), (\ell+1, \ldots, 2\ell), \ldots, ((\tfrac{n}{\ell}-1)\ell+1 \ldots, n)\big\rangle).$$

Proof. It follows from Proposition 2.4.2 and Corollary 2.5.4 that $G = \langle T, \mathrm{PerMat}(S)\rangle = T \rtimes \mathrm{PerMat}(S)$ is a Sylow ℓ-subgroup of $\mathrm{MonGL}_n(q)$ and $\mathrm{GL}_n(q)$. The description of $C_T(\mathrm{PerMat}(S))$ shows that $C_T(\mathrm{PerMat}(S)) \cong C_{\ell^r}^Q$, and it is clear that this group is contained in $Z(G)$. As $|Z(G)| = \ell^{rQ}$ by Proposition 2.2.5 and Proposition 2.3.6, it follows that $Z(G) = C_T(\mathrm{PerMat}(S))$.
Now, let $D \in T$ and $P \in \mathrm{PerMat}(S)$ such that $DP \in C_G(\mathrm{PerMat}(S))$. Then

$$(RDR^{-1})(RPR^{-1}) = RDPR^{-1} = DP$$

for all $R \in \mathrm{PerMat}(S)$, and from the uniqueness of the decomposition of a monomial matrix as a product of a diagonal matrix and a permutation matrix, it follows that $RDR^{-1} = D$ and $RPR^{-1} = P$. Thus, $D \in C_T(\mathrm{PerMat}(S)) = Z(G)$ and $P \in Z(\mathrm{PerMat}(S))$.
Finally, the inclusion

$$Z(\mathrm{PerMat}(S)) \subseteq \mathrm{PerMat}(\big\langle (1, \ldots, \ell), (\ell+1, \ldots, 2\ell), \ldots, ((\tfrac{n}{\ell}-1)\ell+1 \ldots, n)\big\rangle)$$

follows from Proposition 2.3.3 and Corollary 2.3.4. $\square$

Proposition 2.7.3. *Let* G *be the group from Proposition 2.7.2. The intersection* $\tilde{G} := G \cap \mathrm{SL}_n(q)$ *is a Sylow ℓ-subgroup of* $\mathrm{SL}_n(q)$. *In particular,* $|\tilde{G}| = \ell^{r(n-1)}(n!)_\ell$. *Moreover,*

$$\tilde{G} = \begin{cases} \tilde{T} \rtimes \mathrm{PerMat}(S), & \ell > 2, \\ (\tilde{T} \rtimes \mathrm{PerMat}(S \cap \mathrm{Alt}(n))) \sqcup (\tilde{T} \cdot \delta \cdot \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))), & \ell = 2. \end{cases}$$

Proof. As $\mathrm{SL}_n(q)$ is a normal subgroup of $\mathrm{GL}_n(q)$, it follows from Proposition 2.7.2 that $G \cap \mathrm{SL}_n(q) \in \mathrm{Syl}_\ell(\mathrm{SL}_n(q))$.
If ℓ is odd, then every element of S has odd order and lies therefore in $\mathrm{Alt}(n)$. Since the determinant of a permutation matrix is the sign of the corresponding permutation, this implies that $\mathrm{PerMat}(S) \subseteq \mathrm{SL}_n(q)$. Therefore, a monomial matrix $DP \in G$ with $D \in T$ and $P \in \mathrm{PerMat}(S)$ belongs to $G \cap \mathrm{SL}_n(q)$ if and only if $\det(D) = 1$.
Now, let $\ell = 2$. Since $G = T \rtimes \mathrm{PerMat}(S)$, it follows that the union in the claim is disjoint. Moreover, a monomial matrix $DP \in G$ lies in $\mathrm{SL}_n(q)$ if and only if $\det(D) = \det(P) \in \{\pm 1\}$. If $D \in T$ with $\det(D) = -1$ is given, then clearly $D = (D\delta)\delta \in \tilde{T} \cdot \delta$. Thus, we have $\tilde{T} \cdot \delta = \{D \in T \ : \ \det(D) = -1\}$, and the claim follows. □

For the remainder of Section 2.7, let G be the group from Proposition 2.7.2, and let $\tilde{G}$ be the group from Proposition 2.7.3.

Proposition 2.7.4. *The Sylow ℓ-subgroups of* $\mathrm{PGL}_n(q)$ *are isomorphic to* G/Z*, and the Sylow ℓ-subgroups of* $\mathrm{PSL}_n(q)$ *are isomorphic to* $\tilde{G}Z/Z \leq G/Z$*. In particular,* $|G/Z| = |\tilde{G}| = \ell^{r(n-1)}(n!)_\ell$ *and* $|\tilde{G}Z/Z| = \frac{\ell^{r(n-1)}(n!)_\ell}{\gcd(n,q-1)_\ell}$.

Proof. From Proposition 2.7.2 it follows that

$$G/Z = G/(G \cap Z(\mathrm{GL}_n(q))) \cong (G\,Z(\mathrm{GL}_n(q)))/\,Z(\mathrm{GL}_n(q)) \in \mathrm{Syl}_\ell(\mathrm{PGL}_n(q)).$$

Moreover, from $Z(\mathrm{SL}_n(q)) = Z(\mathrm{GL}_n(q)) \cap \mathrm{SL}_n(q)$ it follows that

$$\tilde{G} \cap Z(\mathrm{SL}_n(q)) = Z(\mathrm{GL}_n(q)) \cap \tilde{G} = Z \cap \tilde{G},$$

implying

$$\tilde{G}Z/Z \cong \tilde{G}/(\tilde{G} \cap Z) = \tilde{G}/(\tilde{G} \cap Z(\mathrm{SL}_n(q))) \cong (\tilde{G}\,Z(\mathrm{SL}_n(q)))/\,Z(\mathrm{SL}_n(q)).$$

By Proposition 2.7.3, $(\tilde{G}\,Z(\mathrm{SL}_n(q)))/\,Z(\mathrm{SL}_n(q))$ is a Sylow ℓ-subgroup of $\mathrm{PSL}_n(q)$. □

Let us recall the Sylow ℓ-subgroups that we found in this subsection:

- $G = T \rtimes \mathrm{PerMat}(S)$ is a Sylow ℓ-subgroup of $\mathrm{MonGL}_n(q)$ and of $\mathrm{GL}_n(q)$.
- $\tilde{G} := G \cap \mathrm{SL}_n(q)$ is a Sylow ℓ-subgroup of $\mathrm{SL}_n(q)$.
- The Sylow ℓ-subgroups of $\mathrm{PGL}_n(q)$ are isomorphic to G/Z.
- The Sylow ℓ-subgroups of $\mathrm{PSL}_n(q)$ are isomorphic to $\tilde{G}Z/Z \leq G/Z$.

In what follows, we will study the structure of the groups $\tilde{G}$, G/Z, and $\tilde{G}Z/Z$.

2.7.4 Exponents and elementary abelian normal subgroups

Proposition 2.7.5.

(a) *We have* $\mathrm{Exp}(\tilde{G}) \geq \ell^r$ *and* $\mathrm{Exp}(G/Z) \geq \ell^r$. *If* $n = \ell$, *then* $\mathrm{Exp}(\tilde{G}) = \ell^r$ *and* $\mathrm{Exp}(G/Z) = \ell^r$.

(b) *Let* $(\ell, n, r) \neq (2, 2, 2)$. *Then also* $\mathrm{Exp}(\tilde{G}Z/Z) \geq \ell^r$, *and for* $n = \ell$ *also* $\mathrm{Exp}(\tilde{G}Z/Z) = \ell^r$.

(c) *If* $(\ell, n, r) = (2, 2, 2)$, *then* $\mathrm{Exp}(\tilde{G}Z/Z) = 2$.

Proof.

(a) It is clear that the exponent of $\tilde{T} \cong C_{\ell^r}^{n-1}$ is ℓ^r. Considering the element $\mathrm{diag}(\alpha, 1, \dots, 1)Z \in T/Z$, we obtain that T/Z has exponent ℓ^r, too, so it is clear that each of $\mathrm{Exp}(\tilde{G})$, $\mathrm{Exp}(G/Z)$ is at least ℓ^r. Next, let $n = \ell = 2$. Then the order of $\tilde{G}$ and G/Z is 2^{r+1}. As

$$\mathrm{diag}(\alpha^{2^{r-2}},\ \alpha^{-2^{r-2}}),\ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),\ \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\ \in \tilde{G}$$

are pairwise different elements of order 4, and as

$$\mathrm{diag}(\alpha^{2^{r-2}},\ \alpha^{-2^{r-2}})Z,\ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) Z\ \in G/Z$$

are different elements of order 2, the groups $\tilde{G}$ and G/Z cannot be cyclic, so it follows that their exponents are at most 2^r.

Now, let $n = \ell > 2$.
To show that $\mathrm{Exp}(\tilde{G}) = \ell^r$, it suffices to show that every $X \in G \setminus T$ has order ℓ. Write $X = DP$ with $D = \mathrm{diag}(d_1, \dots, d_\ell) \in \tilde{T}$ and $P \in \mathrm{PerMat}(S)$. Then $P = \mathrm{PerMat}(1, \dots, \ell)^i$ for some $i \in \{1, \dots, \ell - 1\}$, and it follows that

$$\begin{aligned} X^\ell &= (DP)\cdots(DP) \\ &= (DP)(DP^{-1}P^2)(DP^{-2}P^3)\cdots(DP^{-(\ell-1)}P^\ell) \\ &= D(PDP^{-1})(P^2DP^{-2})\cdots(P^{\ell-1}DP^{-(\ell-1)})P^\ell \\ &= \mathrm{diag}(d_1\cdots d_\ell, \dots, d_1\cdots d_\ell)P^\ell \\ &= \mathbb{1}_\ell. \end{aligned}$$

Now, together with the first part, $\mathrm{Exp}(\tilde{G}) = \ell^r$ implies $\mathrm{Exp}(\tilde{G}Z/Z) = \ell^r$.
Finally, consider G/Z. Again, it suffices to show that for every $X \in G$ such that $XZ \notin T/Z$ we have $\mathrm{ord}(XZ) = \ell$. Writing $X = DP$ as above, it follows that

$$\begin{aligned} X^\ell &= (DP)\cdots(DP) \\ &= (DP)(DP^{-1}P^2)(DP^{-2}P^3)\cdots(DP^{-(\ell-1)}P^\ell) \\ &= D(PDP^{-1})(P^2DP^{-2})\cdots(P^{\ell-1}DP^{-(\ell-1)})P^\ell \\ &= \mathrm{diag}(d_1\cdots d_\ell, \dots, d_1\cdots d_\ell)P^\ell \\ &= (d_1\cdots d_\ell)\mathbb{1}_\ell \in Z. \end{aligned}$$

Thus, $X^\ell \in Z$.

(b) Considering the matrix $\operatorname{diag}(\alpha, \alpha^{-1}, 1, \dots, 1)Z \in T/Z$, it is clear that $\tilde{T}Z/Z$ has exponent ℓ^r. Therefore, $\operatorname{Exp}(\tilde{G}Z/Z) \geq \ell^r$. Now, if $n = \ell$, then $\operatorname{Exp}(\tilde{G}Z/Z) = \ell^r$ follows from $\operatorname{Exp}(\tilde{G}) = \ell^r$ in part (a).

(c) Let $(\ell, n, r) = (2, 2, 2)$. Then $\tilde{G}Z/Z$ has order 4, and it is not cyclic since $\operatorname{diag}(\alpha, \alpha^{-1})Z$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) Z$ are two different elements of order 2. Thus, $\operatorname{Exp}(\tilde{G}Z/Z) = 2$.

□

Proposition 2.7.6. *The groups $\Omega_1(T)$, $\Omega_1(\tilde{T})$, $\Omega_1(T)Z/Z$, and $\Omega_1(\tilde{T})Z/Z$ are elementary abelian normal subgroups of G, $\tilde{G}$, G/Z, and $\tilde{G}Z/Z$, respectively, with orders*

$$|\Omega_1(T)| = \ell^n, \quad |\Omega_1(\tilde{T})| = |\Omega_1(T)Z/Z| = \ell^{n-1}, \quad \textit{and} \quad |\Omega_1(\tilde{T})Z/Z| = \ell^{n-2}.$$

Proof. As T is abelian, it is clear that $\Omega_1(T)$, $\Omega_1(\tilde{T})$, $\Omega_1(T)Z/Z \cong \Omega_1(T)/(\Omega_1(T) \cap Z)$, and $\Omega_1(\tilde{T})Z/Z \cong \Omega_1(\tilde{T})/(\Omega_1(\tilde{T}) \cap Z)$ are elementary abelian.
Moreover, $T \cong C_{\ell^r}^n$, $\tilde{T} \cong C_{\ell^r}^{n-1}$, and $Z = O_\ell(\mathbb{F}_q^\times) \cdot \mathbb{1}_n$ imply the assertion about their orders.
Finally, $\Omega_1(T)$ is characteristic in T and T is normal in G, so $\Omega_1(T)$ is normal in G, and with the same argument $\Omega_1(\tilde{T})$ is normal in $\tilde{G}$. Now, $\Omega_1(T)Z/Z$ and $\Omega_1(\tilde{T})Z/Z$ are also normal in G/Z and $\tilde{G}Z/Z$, respectively. □

We obtain the following result for the case $\ell^r \mid n$:

Corollary 2.7.7. *Let $\ell^r \mid n$, let V be a finite group, and write $c_V := |V|^{|V|} \log_\ell(|V|)$.*

(a) *If V is a self-centralizing subgroup of $\tilde{G}$ or of G/Z, then*

$$|\tilde{G}| = |G/Z| \leq (c_V + 1)^{c_V} \cdot (c_V + 1)!.$$

(b) *If V is a self-centralizing subgroup of $\tilde{G}Z/Z$, then*

$$|\tilde{G}Z/Z| \leq (c_V + 2)^{c_V} \cdot (c_V + 2)!.$$

Proof.

(a) From Theorem 2.1.5 and Proposition 2.7.6 it follows that $\ell^{n-1} \leq |V|^{|V|^{|V|}}$, so $n \leq c_V + 1$. Now, the claim follows from $\ell^r \leq n$ and $|G/Z| = |\tilde{G}| = \ell^{r(n-1)}(n!)_\ell$.

(b) As in part (a), Theorem 2.1.5 and Proposition 2.7.6 imply $\ell^{n-2} \leq |V|^{|V|^{|V|}}$, so $n \leq c_V + 2$. The claim follows from $\ell^r \leq n$ and

$$|\tilde{G}Z/Z| = \frac{\ell^{r(n-1)}(n!)_\ell}{\gcd(n, q-1)_\ell} = \frac{\ell^{r(n-1)}(n!)_\ell}{\ell^r} = \ell^{r(n-2)}(n!)_\ell.$$

□

2.7.5 The centers

Lemma 2.7.8. *Let* $\mathsf{P} \in \mathrm{Z}(\mathrm{PerMat}(\mathsf{S}))$.

(a) *If* $\mathsf{P} \in \mathrm{C}_{\mathsf{G}}(\tilde{\mathsf{T}})$*, then* $\mathsf{P} = \mathbb{1}_n$.

(b) *Let* $(\ell, n, r) \notin \{(2,2,2),(3,3,1)\}$*. If for all* $\mathsf{Y} \in \tilde{\mathsf{T}}$ *there exists some* $y \in \mathrm{O}_\ell(\mathbb{F}_q^\times)$ *such that* $\mathsf{Y} = y(\mathsf{P}\mathsf{Y}\mathsf{P}^{-1})$*, then* $\mathsf{P} = \mathbb{1}_n$.

Proof. In the proof, we write

$$\mathsf{Y}_i := \mathrm{diag}(1, \ldots, 1, \underset{(i-1)\ell+1}{\underset{\uparrow}{\alpha}}, \underset{(i-1)\ell+2}{\underset{\uparrow}{\alpha^{-1}}}, 1, \ldots, 1)$$

for $i \in \left\{1, \ldots, \frac{n}{\ell}\right\}$.
By Proposition 2.3.3 and Corollary 2.3.4, $\mathrm{Z}(\mathrm{PerMat}(\mathsf{S}))$ is contained in the elementary abelian group $\left\langle \mathsf{P}_1, \ldots, \mathsf{P}_{n/\ell} \right\rangle$, where $\mathsf{P}_1, \ldots, \mathsf{P}_{n/\ell}$ denote the permutation matrices of

$$(1, \ldots, \ell), (\ell+1, \ldots, 2\ell), \ldots, ((\tfrac{n}{\ell}-1)\ell + 1 \ldots, n) \in \mathsf{S},$$

respectively. Being an elementary abelian ℓ-group, the group $\left\langle \mathsf{P}_1, \ldots, \mathsf{P}_{n/\ell} \right\rangle$ is an $\mathbb{F}_\ell$-vector space, and a basis is given by the minimal set of generators $\left\{\mathsf{P}_1, \ldots, \mathsf{P}_{n/\ell}\right\}$. Therefore, in order to show that $\mathsf{P} = \mathbb{1}_n$, it suffices to show that in the $\mathbb{F}_\ell$-linear combination of P in the basis $\mathsf{P}_1, \ldots, \mathsf{P}_{n/\ell}$ no basis element P_i really occurs.

(a) As P commutes with Y_i for all $i \in \left\{1, \ldots, \frac{n}{\ell}\right\}$, it follows that no P_i can occur in P. Therefore, $\mathsf{P} = \mathbb{1}_n$.

(b) First case: $\ell > 3$.
For each $i \in \left\{1, \ldots, \frac{n}{\ell}\right\}$ let $y_i \in \mathrm{O}_\ell(\mathbb{F}_q^\times)$ be such that $\mathsf{Y}_i = y_i(\mathsf{P}\mathsf{Y}_i\mathsf{P}^{-1})$. As $\ell \geq 5$, for each i there exists some $j_i \in \{(i-1)\ell+1, \ldots, i\ell\}$ such that the j_i-th diagonal entries of Y_i and $y_i(\mathsf{P}\mathsf{Y}_i\mathsf{P}^{-1})$ are both $\mathbb{1}_n$. This forces $y_i = 1$. Thus, no P_i can occur in P, so $\mathsf{P} = \mathbb{1}_n$.

Second case: $\ell \in \{2,3\}$ and $n > \ell$.
We fix some $i, j \in \left\{1, \ldots, \frac{n}{\ell}\right\}$ with $i < j$, and consider the matrix

$$\mathsf{Y} := \mathrm{diag}(1, \ldots, 1, \underset{(i-1)\ell+1}{\underset{\uparrow}{\alpha}}, 1, \ldots, 1, \underset{(j-1)\ell+1}{\underset{\uparrow}{\alpha^{-1}}}, 1, \ldots, 1).$$

Let $y \in \mathrm{O}_\ell(\mathbb{F}_q^\times)$ be such that $\mathsf{Y} = y(\mathsf{P}\mathsf{Y}\mathsf{P}^{-1})$.
If $\ell = 3$, then by comparing coefficients we obtain $y = 1$, so P_i and P_j do not occur in P.

If $\ell = 2$ and P_i or P_j occur in P, then this forces $\alpha^2 = 1$, a contradiction to $q \equiv 1 \bmod 4$.
Therefore, $P = \mathbb{1}_n$ in both cases.

Third case: $n = \ell = 2$ and $r > 2$.
Let $Y := Y_1 = \operatorname{diag}(\alpha, \alpha^{-1})$, and let $y \in O_2(\mathbb{F}_q^\times)$ be such that $Y = y(PYP^{-1})$. If $P \neq \mathbb{1}_2$, then $P = P_1 = \operatorname{PerMat}(1,2)$, and by comparing coefficients we obtain $y = \alpha^2 = \alpha^{-2}$. It follows that $\alpha^4 = 1$, so the order 2^r of α divides 4. As $q \equiv 1 \bmod 4$, this yields $r = 2$, contradiction.

Fourth case: $n = \ell = 3$ and $r > 1$.
Again, consider the matrix $Y := Y_1 = \operatorname{diag}(\alpha, \alpha^{-1}, 1)$, and let $y \in O_3(\mathbb{F}_q^\times)$ be such that $Y = y(PYP^{-1})$.
If $P \neq \mathbb{1}_3$, then $P = P_1 \in \{\operatorname{PerMat}(1,2,3), \operatorname{PerMat}(1,3,2)\}$, and by comparing coefficients we obtain $\alpha^3 = 1$, so $r = 1$. This contradicts the assumption $r \neq 1$.

□

Lemma 2.7.9. *We have* $|Z \cap \mathrm{SL}_n(q)| = \min\{\ell^r, n_\ell\}$.

Proof. If $\ell^r \leq n_\ell$, then we have $Z \subseteq \mathrm{SL}_n(q)$, and so $|Z \cap \mathrm{SL}_n(q)| = |Z| = \ell^r$.
Now, let $\ell^r > n_\ell$. Then $\alpha^n = \alpha^{n_\ell \cdot n_{\ell'}} = (\alpha^{n_{\ell'}})^{n_\ell}$. As $\operatorname{ord}(\alpha) = \ell^r$ and $n_{\ell'}$ are coprime, $\alpha^{n_{\ell'}}$ has order ℓ^r, too. Therefore, the image $\langle \alpha^n \rangle = \langle (\alpha^{n_{\ell'}})^{n_\ell} \rangle = \langle \alpha^{n_\ell} \rangle$ of the determinant homomorphism

$$Z \to \mathbb{F}_q^\times : \alpha^k \cdot \mathbb{1}_n \mapsto \alpha^{kn}$$

has order $\frac{\ell^r}{n_\ell}$. As the kernel of this homomorphism is $Z \cap \mathrm{SL}_n(q)$, it follows that

$$|Z \cap \mathrm{SL}_n(q)| = \frac{|Z|}{\ell^r / n_\ell} = n_\ell.$$

□

We continue with the structure and the order of the centers of our groups $\tilde{G}$, G/Z, and $\tilde{G}Z/Z$:

Theorem 2.7.10.

(a) *We have* $Z(\tilde{G}) = Z(G) \cap \mathrm{SL}_n(q)$ *with order*

$$|Z(\tilde{G})| = \ell^{r(Q-1)} \cdot \min\{\ell^r, n_\ell\}.$$

(b) *Let* $H := \left\{ D \in T \ : \ \forall\, R \in \operatorname{PerMat}(S)\ \exists\, c_R \in O_\ell(\mathbb{F}_q^\times) : D = c_R R D R^{-1} \right\}$. *Then* H *is a subgroup of* T *containing* Z, *and we have*

$$Z(G/Z) = H/Z \qquad \text{and} \qquad H = \begin{cases} Z(G), & Q > 1, \\ Z(G)A, & Q = 1. \end{cases}$$

In particular,

$$|Z(G/Z)| = \begin{cases} \ell^{r(Q-1)}, & Q > 1, \\ \ell, & Q = 1. \end{cases}$$

(c) *If* $(\ell, n, r) \notin \{(2,2,2),(3,3,1)\}$, *then*

$$Z(\tilde{G}Z/Z) = (H \cap \mathrm{SL}_n(q))Z/Z \cong Z(G/Z).$$

If $(\ell, n, r) = (2,2,2)$, *then* $\tilde{G}Z/Z$ *is elementary abelian of order* 4, *and if* $(\ell, n, r) = (3,3,1)$, *then* $\tilde{G}Z/Z$ *is elementary abelian of order* 9.

Proof.

(a) The inclusion $Z(G) \cap \mathrm{SL}_n(q) \subseteq Z(\tilde{G})$ is clear.
First, let $\ell > 2$. Let $D \in \tilde{T}$, and let $P \in \mathrm{PerMat}(S)$ be such that $DP \in Z(\tilde{G})$. Then Proposition 2.7.2 implies $D \in Z(G) \cap \mathrm{SL}_n(q)$ and $P \in Z(\mathrm{PerMat}(S))$. As $DP \in Z(\tilde{G}) \subseteq C_G(\tilde{T})$ and $D \in C_G(\tilde{T})$, it follows that also $P \in C_G(\tilde{T})$. Thus, $P \in Z(\mathrm{PerMat}(S)) \cap C_G(\tilde{T}) = \{\mathbb{1}_n\}$ by part (a) of Lemma 2.7.8, and this shows that

$$DP = D \in Z(G) \cap \mathrm{SL}_n(q).$$

Therefore, $Z(G) \cap \mathrm{SL}_n(q) = Z(\tilde{G})$ holds for $\ell > 2$.
Now, let $\ell = 2$. First, let $D \in \tilde{T}$, and let $P \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ be such that $DP \in Z(\tilde{G})$. Let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n)) \subseteq \tilde{G}$, and let $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. Then

$$(RDR^{-1})(RPR^{-1}) = RDPR^{-1} = DP$$

shows that $RDR^{-1} = D$ and $RPR^{-1} = P$. Moreover, $\delta U \in \tilde{G}$, and

$$\delta(UDU^{-1})(UPU^{-1})\delta = (\delta U)DP(\delta U)^{-1} = DP$$

implies $\delta(UDU^{-1})(UPU^{-1}) = DP\delta = D(P\delta P^{-1})P$. It follows that

$$\delta(UDU^{-1})(UPU^{-1}) = DP\delta = D(P\delta P^{-1})P,$$

so $\delta(UDU^{-1}) = D(P\delta P^{-1})$ and $UPU^{-1} = P$. As R and U have been chosen arbitrarily, $P \in Z(\mathrm{PerMat}(S))$. As before, since $DP \in Z(\tilde{G}) \subseteq C_G(\tilde{T})$ and $D \in C_G(\tilde{T})$, it follows that also $P \in C_G(\tilde{T})$, so $P \in Z(\mathrm{PerMat}(S)) \cap C_G(\tilde{T}) = \{1\}$ by part (a) of Lemma 2.7.8.
Now, $\delta(UDU^{-1}) = D\delta$ implies $UDU^{-1} = D$ since the diagonal matrices δ and D commute. As R and U have been chosen arbitrarily, Proposition 2.7.2 implies

$$D \in C_T(\mathrm{PerMat}(S)) \cap \mathrm{SL}_n(q) = Z(G) \cap \mathrm{SL}_n(q).$$

Next, suppose that there exist $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$ such that $D\delta P \in Z(\tilde{G})$. Again, choose $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ and $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. Then

$$(RD\delta R^{-1})(RPR^{-1}) = RD\delta PR^{-1} = D\delta P$$

shows in particular that $RPR^{-1} = P$. Moreover,

$$\delta(UD\delta U^{-1})(UPU^{-1})\delta = (\delta U)D\delta P(\delta U)^{-1} = D\delta P$$

implies $\delta(UD\delta U^{-1})(UPU^{-1}) = D\delta(P\delta P^{-1})P$, so $UPU^{-1} = P$. Similar as above, since $D\delta P \in Z(\tilde{G}) \subseteq C_G(\tilde{T})$ and $D\delta \in C_G(\tilde{T})$, also $P \in C_G(\tilde{T})$, so $P \in Z(\mathrm{PerMat}(S)) \cap C_G(\tilde{T}) = \{1\}$. The latter is a contradiction to the choice of P. This finishes the proof of $Z(G) \cap \mathrm{SL}_n(q) = Z(\tilde{G})$.

Now, let $m \in \{1, \dots, s\}$ be minimal such that $a_m \neq 0$, that is, $\ell^m = n_\ell$. The image of the determinant homomorphism $Z(G) \to O_\ell(\mathbb{F}_q^\times)$ is $\langle \alpha^{\ell^m} \rangle$. Thus, for $m \geq r$, we have $Z(G) \subseteq \mathrm{SL}_n(q)$, so $Z(G) = Z(\tilde{G})$. If $m < r$, then $\langle \alpha^{\ell^m} \rangle$ has order ℓ^{r-m}, and the first Isomorphism Theorem and Proposition 2.7.2 imply

$$|Z(\tilde{G})| = \frac{|Z(G)|}{\ell^{r-m}} = \ell^{r(Q-1)+m} = \ell^{r(Q-1)} \cdot n_\ell.$$

(b) It is clear that $Z = O_\ell(\mathbb{F}_q^\times) \cdot \mathbb{1}_n \subseteq H$. Moreover, if $D, E \in H$ and $R \in \mathrm{PerMat}(S)$ are given and $c_R, d_R \in O_\ell(\mathbb{F}_q^\times)$ satisfy $D = c_R RDR^{-1}$ and $E = d_R RER^{-1}$, then $DE = (c_R RDR^{-1})(d_R RER^{-1}) = c_R d_R RDER^{-1}$. Therefore, H is a subgroup of T containing Z.

As $G = T \rtimes \mathrm{PerMat}(S)$ and T is abelian, it is obvious that $H/Z \subseteq Z(G/Z)$. Now, let $D \in T$ and $P \in \mathrm{PerMat}(S)$ be such that $DPZ \in Z(G/Z)$, and let $R \in \mathrm{PerMat}(S)$. We write $X := DP$. Then

$$DPRP^{-1}D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$. It follows that $PRP^{-1}R^{-1} = c_R D^{-1}RDR^{-1}$. As the right-hand side of this equation is a diagonal matrix and the left-hand side is an element of $\mathrm{PerMat}(S)$, it follows that both sides are $\mathbb{1}_n$. Thus, $D = c_R(RDR^{-1})$ and $PRP^{-1}R^{-1} = 1$. It remains to show that $P = \mathbb{1}_n$. For $i = 1, \dots, n$ consider the matrix

$$B_i := \mathrm{diag}(1, \dots, 1, \underset{\substack{\uparrow \\ i}}{\alpha}, 1, \dots, 1).$$

For all i, the matrix $PB_i^{-1}P^{-1}$ belongs to the abelian group T, so the matrix

$$B_i P B_i^{-1} P^{-1} = B_i D P B_i^{-1} P^{-1} D^{-1} = B_i X B_i^{-1} X^{-1} \in Z$$

is a scalar matrix, say $b_i \cdot \mathbb{1}_n$. Then $B_i = b_i(PB_iP^{-1})$ for all i. Now, if $n > 2$, then for each i there exists some $j_i \in \{(i-1)\ell+1,\ldots,i\ell\}$ such that the j_i-th diagonal entries of B_i and $b_i(PB_iP^{-1})$ are both 1. This forces $b_i = 1$. Moreover, if $n = 2$, then also $\ell = 2$, and if $P = \mathrm{PerMat}(1,2)$ then $\alpha^2 = 1$ contradicts $q \equiv 1 \bmod 4$. Thus, $b_i = 1$ for all i, and it follows that P must be the identity matrix. This finishes the proof of the equality $Z(G/Z) = H/Z$.

Now, let $i \in \{1,\ldots,s\}$ be such that $a_i \neq 0$. Let $D \in H$ be given, say $D = \mathrm{diag}(d_1,\ldots,d_n)$.

First case: $Q > 1$.
Consider the part $(P_{\ell^i})_{+u}$ of S, where $u := a_1\ell + \cdots + a_{i-1}\ell^{i-1} + k\ell^i$ for some $k \in \{0,\ldots,a_i-1\}$. Then $(P_{\ell^i})_{+u}$ contains an element of order ℓ^i, say σ.
As D belongs to H, there exists some $c \in (\mathbb{F}_q^\times)_\ell$ such that

$$D = c\,\mathrm{PerMat}(\sigma) D\,\mathrm{PerMat}(\sigma)^{-1}.$$

Since Q is greater than 1 and $\mathrm{PerMat}(\sigma)$ permutes only ℓ^i diagonal entries of D, it follows that there exists some $j \in \{1,\ldots,n\}$ such that d_j is the j-th diagonal entry of both D and $\mathrm{PerMat}(\sigma)D\,\mathrm{PerMat}(\sigma)^{-1}$, so $c = 1$.
Thus, $D = \mathrm{PerMat}(\sigma)D\,\mathrm{PerMat}(\sigma)^{-1}$, implying that $d_{u+1} = \cdots = d_{u+\ell^i}$. Since i was chosen arbitrarily, it follows that $D \in Z(G)$. The inclusion $Z(G) \subseteq H$ is obvious.

Second case: $Q = 1$. Then $n = \ell^m$ for some $m \in \mathbb{N}_{>0}$, so $S = P_{\ell^m}$ with generators $z_0,\ldots,z_{m-1}$, where $z_0 = (1,\ldots,\ell)$, and where

$$z_i = (1,\ell^i{+}1,2\ell^i{+}1,\ldots,(\ell{-}1)\ell^i{+}1)(2,\ell^i{+}2,\ldots,(\ell{-}1)\ell^i{+}2)\cdots(\ell^i,2\ell^i,\ldots,\ell^{i+1})$$

for $i = 1,\ldots,m-1$. For $k \in \mathbb{N}$ write $D_k := \mathrm{diag}(d_1,\ldots,d_k)$.
Let $R_i \in S$ be the permutation matrix of z_i for $i = 0,\ldots,m-1$, and let $c_i \in (\mathbb{F}_q^\times)_\ell$ satisfy $D = c_iR_iDR_i^{-1}$. Since, for $j = 0,\ldots,m-2$, the permutation matrix R_j permutes only $\ell^{j+1} < \ell^m$ diagonal entries of D, it follows that $c_0 = \cdots = c_{m-2} = 1$.
Now, $D = c_{m-1}R_{m-1}DR_{m-1}^{-1}$ implies

$$D = \mathrm{diag}(\underbrace{c_{m-1}^{\ell}}_{=1} D_{\ell^{m-1}}, c_{m-1}\cdot D_{\ell^{m-1}}, c_{m-1}^2\cdot D_{\ell^{m-1}},\ldots,c_{m-1}^{\ell-1}\cdot D_{\ell^{m-1}}).$$

Let $j := m-2$. Then, $D = R_jDR_j^{-1}$ implies

$$d_k = d_{(\ell-1)\ell^j+k} = d_{(\ell-2)\ell^j+k} = \cdots = d_{\ell^j+k} = d_k$$

for all $k = 1, \dots, \ell^{j-1}$, so

$$D_{\ell^j} = \operatorname{diag}(\underbrace{D_{\ell^{j-2}}, \dots, D_{\ell^{j-2}}}_{\ell}).$$

Repeating the argument for $j = m-3$ up to $j = 0$, we obtain

$$\begin{aligned} D &= \operatorname{diag}(d_1 \cdot \mathbb{1}_{\ell^{m-1}}, c_{m-1} \cdot d_1 \cdot \mathbb{1}_{\ell^{m-1}}, c_{m-1}^2 \cdot d_1 \cdot \mathbb{1}_{\ell^{m-1}}, \dots, c_{m-1}^{\ell-1} \cdot d_1 \cdot \mathbb{1}_{\ell^{m-1}}) \\ &\in Z(G)A. \end{aligned}$$

The inclusions $Z(G) \subseteq H$ and $A \subseteq H$ are obvious.

(c) First, note that for $(\ell, n, r) \in \{(2,2,2), (3,3,1)\}$ we obtain

$$|\tilde{G}Z/Z| = \frac{\ell^{r(n-1)}(n!)_\ell}{\gcd(n, q-1)_\ell} \in \{4, 9\},$$

so $\tilde{G}Z/Z$ is abelian in this case. Considering the exponents in Proposition 2.7.5, we obtain that $\tilde{G}Z/Z$ is not cyclic and, thus, elementary abelian.

Now, let $(\ell, n, r) \notin \{(2,2,2), (3,3,1)\}$ and show first that

$$Z(\tilde{G}Z/Z) = (H \cap \mathrm{SL}_n(q))Z/Z.$$

If $X \in H \cap \mathrm{SL}_n(q) \subseteq H$, then it follows from part (b) that $XZ \in H/Z = Z(G/Z)$, and as XZ belongs to $\tilde{G}Z/Z$, this shows that $XZ \in Z(\tilde{G}Z/Z)$.
For the converse inclusion, let first $\ell > 2$. Let $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S)$ be such that $X := DP$ satisfies $XZ \in Z(\tilde{G}Z/Z)$. Let $R \in \mathrm{PerMat}(S)$. Then, as in the proof of part (b),

$$DPRP^{-1}D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$, and it follows that $PRP^{-1}R^{-1} = c_R D^{-1}RDR^{-1}$. Again, as the right-hand side of this equation is a diagonal matrix and the left-hand side is an element of $\mathrm{PerMat}(S)$, it follows that both sides are $\mathbb{1}_n$. Thus, $D = c_R(RDR^{-1})$ and $PRP^{-1}R^{-1} = 1$. As R has been chosen arbitrarily, it follows that $P \in Z(\mathrm{PerMat}(S))$. If $Y \in \tilde{T}$, then $PY^{-1}P^{-1}$ belongs to the abelian group $\tilde{T}$, so the matrix

$$YPY^{-1}P^{-1} = YDPY^{-1}P^{-1}D^{-1} = YXY^{-1}X^{-1} \in Z$$

is a scalar matrix, say $y \cdot \mathbb{1}_n$, and it follows that $Y = y(PYP^{-1})$. Thus, part (b) of Lemma 2.7.8 implies $P = \mathbb{1}_n$. Hence, $Z(\tilde{G}Z/Z) = (H \cap \mathrm{SL}_n(q))Z/Z$ holds for $\ell > 2$.
Now, let $\ell = 2$. First, let $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ be such that $X := DP$ satisfies $XZ \in Z(\tilde{G}Z/Z)$. Let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n)) \subseteq \tilde{G}$, and let $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. As in the proof of part (b),

$$DPRP^{-1}D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$, and so is

$$DP\delta UP^{-1}D^{-1}U^{-1}\delta = X(\delta U)X^{-1}(\delta U)^{-1} \in Z,$$

say $c_U \cdot \mathbb{1}_n$. It follows that $PRP^{-1}R^{-1} = c_R D^{-1}RDR^{-1}$ and that $PUP^{-1}U^{-1} = c_U(P\delta P^{-1})D^{-1}\delta(UDU^{-1})$. In both equations, the right-hand side is a diagonal matrix and the left-hand side is an element of $\mathrm{PerMat}(S)$, so it follows that both sides are $\mathbb{1}_n$. In particular, $P \in Z(\mathrm{PerMat}(S))$. As before, if $Y \in \tilde{T}$, then $PY^{-1}P^{-1}$ belongs to the abelian group $\tilde{T}$, so the matrix

$$YPY^{-1}P^{-1} = YDPY^{-1}P^{-1}D^{-1} = YXY^{-1}X^{-1} \in Z$$

is a scalar matrix, say $y \cdot \mathbb{1}_n$, and it follows that $Y = y(PYP^{-1})$. Thus, part (b) of Lemma 2.7.8 implies $P = 1$. It follows that $D = c_U(UDU^{-1})$, so $X = D$ lies in $H \cap \mathrm{SL}_n(q)$.
Finally, suppose that there exist $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$ such that $X := D\delta P$ satisfies $XZ \in Z(\tilde{G}Z/Z)$. Again, let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n)) \subseteq \tilde{G}$ and $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. Then

$$D\delta PRP^{-1}\delta D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$, and so is

$$D\delta P\delta UP^{-1}\delta D^{-1}U^{-1}\delta = X(\delta U)X^{-1}(\delta U)^{-1} \in Z,$$

say $c_U \cdot \mathbb{1}_n$. It follows that $PRP^{-1}R^{-1} = c_R\delta D^{-1}RD\delta R^{-1}$ and that $PUP^{-1}U^{-1} = c_U P\delta P^{-1}D^{-1}UD\delta U^{-1}$. As before, in both equations, the right-hand side is a diagonal matrix and the left-hand side is an element of $\mathrm{PerMat}(S)$, so it follows that both sides are $\mathbb{1}_n$. In particular, $P \in Z(\mathrm{PerMat}(S))$. Again, if $Y \in \tilde{T}$, then $PY^{-1}P^{-1}$ belongs to the abelian group $\tilde{T}$, so the matrix

$$YPY^{-1}P^{-1} = YD\delta PY^{-1}P^{-1}\delta D^{-1} = YXY^{-1}X^{-1} \in Z$$

is a scalar matrix, say $y \cdot \mathbb{1}_n$, and it follows that $Y = y(PYP^{-1})$. Now, part (b) of Lemma 2.7.8 implies $P = \mathbb{1}_n$. This is a contradiction to the choice $P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$.
Now, the proof of the equation $Z(\tilde{G}Z/Z) = (H \cap \mathrm{SL}_n(q))Z/Z$ is complete.

It remains to show that $(H \cap \mathrm{SL}_n(q))Z/Z \cong Z(G/Z)$. The map $H \cap \mathrm{SL}_n(q) \to H/Z : X \mapsto XZ$ is a homomorphism with kernel $Z \cap \mathrm{SL}_n(q)$, so there exists a monomorphism from

$$(H \cap \mathrm{SL}_n(q))Z/Z \cong (H \cap \mathrm{SL}_n(q))/(Z \cap \mathrm{SL}_n(q)) \hookrightarrow H/Z = Z(G/Z).$$

Therefore, it suffices to show that

$$|(H \cap \mathrm{SL}_n(q))/(Z \cap \mathrm{SL}_n(q))| = |Z(G/Z)|.$$

By Lemma 2.7.9, we have $|Z \cap \mathrm{SL}_n(q)| = \min\{\ell^r, n_\ell\}$.

First case: $Q > 1$.

Then we have $|Z(G/Z)| = \ell^{r(Q-1)}$ by part (b), and it remains to show that $|H \cap \mathrm{SL}_n(q)| = \ell^{r(Q-1)} \cdot \min\{\ell^r, n_\ell\}$. As we have

$$|H \cap \mathrm{SL}_n(q)| = |Z(G) \cap \mathrm{SL}_n(q)| = |Z(\tilde{G})| = \ell^{r(Q-1)} \cdot \min\{\ell^r, n_\ell\}$$

by parts (a) and (b), the claim follows.

Second case: $Q = 1$.

Here, we have $n = n_\ell = \ell^m$ for some $m \in \mathbb{N}_{>0}$. Part (b) implies that $|Z(G/Z)| = \ell$, so it remains to show that $|H \cap \mathrm{SL}_n(q)| = \ell^{\min\{r,m\}+1}$. We also have $H = Z(G)A$ and $|H| = |Z||H/Z| = \ell^r |Z(G/Z)| = \ell^{r+1}$ by part (b). Let us consider the determinant homomorphism

$$\varphi : H \to \mathbb{F}_q^\times : X \mapsto \det(X).$$

The elements of $H = Z(G)A$ are of the form

$$\alpha^i \cdot \mathrm{diag}(\mathbb{1}_{n/\ell},\ \alpha^{j\ell^{r-1}} \cdot \mathbb{1}_{n/\ell},\ \alpha^{2j\ell^{r-1}} \cdot \mathbb{1}_{n/\ell},\ \ldots,\ \alpha^{(\ell-1)j\ell^{r-1}} \cdot \mathbb{1}_{n/\ell}),$$

so the image of φ is

$$\langle \alpha^n \rangle \cdot \left\langle \alpha^{(1+2+\dots+\ell-1)\frac{n}{\ell}\ell^{r-1}} \right\rangle = \langle \alpha^n \rangle \cdot \left\langle \alpha^{\frac{\ell-1}{2}\ell^{r-1+m}} \right\rangle.$$

First subcase: $m \geq r$.

Clearly, then $\alpha^n = \alpha^{\ell^m} = (\alpha^{\ell^r})^{\ell^{m-r}} = 1$.
If $\ell > 2$, then $\frac{\ell-1}{2} \in \mathbb{Z}$ and therefore

$$\alpha^{\frac{\ell-1}{2}\ell^{r-1+m}} \in \left\langle \alpha^{\ell^{r-1+m}} \right\rangle = \left\langle (\alpha^{\ell^r})^{m-1} \right\rangle = \{1\}.$$

If $\ell = 2$, then $q \equiv 1 \bmod 4$ implies $r \geq 2$, so also $m \geq 2$. Thus, $\ell \cdot \frac{\ell-1}{2} \in \mathbb{Z}$ and

$$\alpha^{\ell \cdot \frac{\ell-1}{2} \cdot \ell^{r-1+m-1}} \in \left\langle \alpha^{\ell^{r-2+m}} \right\rangle = \left\langle (\alpha^{\ell^r})^{m-2} \right\rangle = \{1\}.$$

It follows that the image of φ is the trivial homomorphism and, therefore, $H \subseteq \mathrm{SL}_n(q)$. Now, we have $|H \cap \mathrm{SL}_n(q)| = |H| = \ell^{r+1} = \ell^{\min\{r,m\}+1}$.

Second subcase: $m < r$.

If $(\ell, n) \neq (2, 2)$, then the image of φ is clearly $\langle \alpha^n \rangle$ and has, thus, order ℓ^{r-m}. Now, consider the case $(\ell, n) = (2, 2)$. Then the image of φ is

$$\left\langle \alpha^2 \right\rangle \cdot \left\langle \alpha^{2^{r-1}} \right\rangle \leq \langle \alpha \rangle.$$

The order of $\alpha^{2^{r-1}} = 2$, and since both $\langle\alpha\rangle$ and $\langle\alpha^2\rangle$ have a unique element of order 2, it follows that $\alpha^{2^{r-1}} \in \langle\alpha^2\rangle$, that is, the image of φ is $\langle\alpha^2\rangle$ of order 2^{r-1}. Hence, in any case we have $|\operatorname{im}(\varphi)| = \ell^{r-m}$.
Now, it follows that

$$|H \cap \mathrm{SL}_n(q)| = |\ker(\varphi)| = \frac{|H|}{|\operatorname{im}(\varphi)|} = \frac{\ell^{r+1}}{\ell^{r-m}} = \ell^{m-1} = \ell^{\min\{r,m\}+1}.$$

□

2.7.6 Results about small self-centralizing subgroups

As a consequence of Theorem 2.7.10, we obtain the following result for the case that n is not a power of ℓ:

Corollary 2.7.11. *Let n not be a power of ℓ, let V be a finite group, and write $c_V := |V|^{|V|}\log_\ell(|V|)$.*

(a) *If V is a self-centralizing subgroup of $\tilde{G}$ or of G/Z, then*

$$|\tilde{G}| = |G/Z| \leq |V|^{c_V} \cdot (c_V + 1)!.$$

(b) *If V is a self-centralizing subgroup of $\tilde{G}Z/Z$, then*

$$|\tilde{G}Z/Z| \leq (|V|^{c_V} + 1) \cdot (c_V + 2)!.$$

Proof.

(a) It follows from Proposition 2.7.6 and Theorem 2.1.5 that $\ell^{n-1} \leq |V|^{|V|^{|V|}}$. Moreover, as n is not a power of ℓ, Theorem 2.7.10 implies $\ell^r \leq |Z(X)| \leq |C_X(V)| \leq |V|$ for $X \in \left\{\tilde{G}, G/Z\right\}$. Now, the claim follows from

$$|G/Z| = |\tilde{G}| = \ell^{r(n-1)}(n!)_\ell.$$

(b) Proposition 2.7.6 and Theorem 2.1.5 imply $\ell^{n-2} \leq |V|^{|V|^{|V|}}$, and since n is not a power of ℓ, we have $\ell^r \leq |Z(\tilde{G}Z/Z)| \leq |C_{\tilde{G}Z/Z}(V)| \leq |V|$ by Theorem 2.7.10. Thus, the claim follows from

$$|\tilde{G}Z/Z| \leq |G/Z| = \ell^{r(n-1)}(n!)_\ell.$$

□

In the next statements, we consider the case where n is a power of ℓ. We recall that in this case, the elements of $Z(G)$ are scalar matrices by Proposition 2.7.2.

Theorem 2.7.12. *Let* $n = \ell^m$ *for some* $m \in \mathbb{N}_{>0}$.

(a) *If* $\ell > 2$, *then* $Z(\tilde{G})\,\mathrm{PerMat}(S)$ *is a self-centralizing subgroup of* $\tilde{G}$ *of order* $\ell^{\min\{r,m\}+1+\ell+\ell^2+\cdots+\ell^{m-1}}$.

(b) *The group* $(Z(G)A\,\mathrm{PerMat}(S))/Z$ *is a self-centralizing subgroup of* G/Z *of order* $\ell^{1+(1+\ell+\ell^2+\cdots+\ell^{m-1})}$.

(c) *If* $\ell > 2$, *then* $(Z(\tilde{G})A\,\mathrm{PerMat}(S))Z/Z$ *is a self-centralizing subgroup of* $\tilde{G}Z/Z$ *of order* $\ell^{1+(1+\ell+\ell^2+\cdots+\ell^{m-1})}$.

Proof.

(a) By Theorem 2.7.10, the order of $Z(\tilde{G})\,\mathrm{PerMat}(S)$ is

$$|Z(\tilde{G})| \cdot |\mathrm{PerMat}(S)| = \ell^{\min\{r,m\}} \cdot (\ell^m!)_\ell = \ell^{\min\{r,m\}+1+\ell+\ell^2+\cdots+\ell^{m-1}}.$$

Let $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S)$ be such that $DP \in C_{\tilde{G}}(Z(\tilde{G})\,\mathrm{PerMat}(S))$. By Proposition 2.7.2 and Theorem 2.7.10, D lies in $Z(G) \cap \mathrm{SL}_n(q) = Z(\tilde{G})$. Thus, $DP \in Z(\tilde{G})\,\mathrm{PerMat}(S)$.

(b), (c) $Z(G)A$ is normal in G since $(Z(G)A)/Z = Z(G/Z)$ is a normal subgroup of G/Z. Thus, $Z(G)A\,\mathrm{PerMat}(S)$ is a subgroup of G containing Z, so $(Z(G)A\,\mathrm{PerMat}(S))/Z$ is a subgroup of G/Z. As we have $Z(G)A \cap \mathrm{PerMat}(S) = \{1\}$ and $Z(G) \cap A = \{1\}$, we have

$$\frac{|Z(G)| \cdot |A| \cdot |\mathrm{PerMat}(S)|}{|Z|} = \frac{\ell^r \cdot \ell \cdot \ell^{1+\ell+\ell^2+\cdots+\ell^{m-1}}}{\ell^r} = \ell^{1+(1+\ell+\ell^2+\cdots+\ell^{m-1})}$$

by Theorem 2.7.10. If $\ell > 2$, then it follows from $A \subseteq \mathrm{SL}_n(q)$ and $\mathrm{PerMat}(S) \subseteq \mathrm{SL}_n(q)$, together with part (a) of Theorem 2.7.10 that

$$Z(\tilde{G})A\,\mathrm{PerMat}(S) = ((Z(G) \cap \mathrm{SL}_n(q))A\,\mathrm{PerMat}(S)) = (Z(G)A\,\mathrm{PerMat}(S) \cap \mathrm{SL}_n(q))$$

is a subgroup of $G \cap \mathrm{SL}_n(q) = \tilde{G}$, so $(Z(\tilde{G})A\,\mathrm{PerMat}(S))Z/Z$ is a subgroup of $\tilde{G}Z/Z$. By Lemma 2.7.9 we have

$$|Z \cap Z(\tilde{G})A\,\mathrm{PerMat}(S)| = |Z \cap \mathrm{SL}_n(q)| = \ell^{\min\{r,m\}},$$

so the order of $(Z(\tilde{G})A\,\mathrm{PerMat}(S))Z/Z$ is

$$\frac{|Z(\tilde{G})| \cdot |A| \cdot |\mathrm{PerMat}(S)|}{|Z \cap \mathrm{SL}_n(q)|} = \frac{\ell^{\min\{r,m\}} \cdot \ell \cdot \ell^{1+\ell+\ell^2+\cdots+\ell^{m-1}}}{\ell^{\min\{r,m\}}} = \ell^{1+(1+\ell+\ell^2+\cdots+\ell^{m-1})}.$$

Let ℓ be arbitrary and let $D \in T$ and $P \in \mathrm{PerMat}(S)$ be such that $DPZ \in C_{G/Z}((Z(G)A\,\mathrm{PerMat}(S))/Z)$. Moreover, let $R \in \mathrm{PerMat}(S)$. Write $X := DP$. Then

$$DPRP^{-1}D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$. It follows that $PRP^{-1}R^{-1} = c_R D^{-1}RDR^{-1}$. As the right-hand side of this equation is a diagonal matrix and the left-hand side is an element of $\mathrm{PerMat}(S)$, it follows that both sides are $\mathbb{1}_n$. In particular, $D = c_R(RDR^{-1})$.

Thus, $D \in Z(G)A$ by Theorem 2.7.10, so $DPZ \in (Z(G)A\,\mathrm{PerMat}(S))/Z$. Moreover, if $\ell > 2$ and $D \in \tilde{T}$, then $D \in (Z(G)A) \cap \mathrm{SL}_n(q) = Z(\tilde{G})A$, and thus, $DPZ \in (Z(\tilde{G})A\,\mathrm{PerMat}(S))Z/Z$.

□

It remains to consider the groups $\tilde{G}$ and $\tilde{G}Z/Z$ for $\ell = 2$. If $n = 2$, then we have already seen in Theorem 2.5.7 and Proposition 2.1.8 that small self-centralizing subgroups exist. Therefore, it suffices to consider the case $n \geq 4$:

Theorem 2.7.13. *Let $n = 2^m$ for some $m \in \mathbb{N}_{>1}$. For $i \in \{1, -1\}$ write*

$$E_i := \{\mathrm{diag}(d_1, \ldots, d_n) \in T \ : \ d_1, \ldots, d_n \in \{1, -1\}, \ d_1 \cdots d_n = i\}.$$

(a) *The disjoint union*

$$\begin{aligned} W \ := \ & \{DP \ : \ D \in E_1, \ P \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))\} \\ & \sqcup \ \{DP \ : \ D \in E_{-1}, \ P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))\} \end{aligned}$$

is a subgroup of $\tilde{G}$ of order $2^{2^{m+1}-2}$.

(b) $Z(\tilde{G})W$ *is a self-centralizing subgroup of $\tilde{G}$ of order $2^{\min\{m,r\}+2^{m+1}-3}$.*

(c) WZ/Z *is a self-centralizing subgroup of $\tilde{G}Z/Z$ of order $2^{2^{m+1}-3}$.*

Proof.

(a) The order of E_1 is the number of subsets of $\{1, \ldots, n\}$ of even cardinality, and the order of E_{-1} is the number of subsets of $\{1, \ldots, n\}$ of odd cardinality. As the sum of these two numbers is the number 2^n of all subsets of $\{1, \ldots, n\}$ and the second is

$$\frac{1}{2}\Big(\sum_{k=0}^{n} \binom{n}{k} - \sum_{k=0}^{n} (-1)^k \binom{n}{k}\Big) = \frac{1}{2}((1+1)^n - (1-1)^n) = 2^{n-1},$$

it follows that the first must be 2^{n-1} as well. Therefore,

$$|W| = \frac{2^{n-1}(n!)_2}{2} + \frac{2^{n-1}(n!)_2}{2} = 2^{n-1}(n!)_2 = 2^{2^m-1} \cdot 2^{2^m-1} = 2^{2^{m+1}-2}.$$

If $P, Q \in \mathrm{PerMat}(S)$, $D_P \in E_{\det(P)}$, and $D_Q \in E_{\det(Q)}$, then

$$D_P P D_Q Q = (D_P P D_Q P^{-1}) PQ \in W,$$

so W is a subgroup of $\tilde{G}$.

(b) As $Z(\tilde{G}) \cap W = \{\mathbb{1}_n, -\mathbb{1}_n\}$ has order 2, it follows that $Z(\tilde{G})W$ is a subgroup of $\tilde{G}$ of order $2^{\min\{m,r\}+2^{m+1}-3}$.
Recall from Proposition 2.7.3 that

$$\tilde{G} = (\tilde{T} \rtimes \mathrm{PerMat}(S \cap \mathrm{Alt}(n))) \sqcup (\tilde{T} \cdot \delta \cdot \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))).$$

First, let $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n)) \subseteq W$ be such that $DP \in C_{\tilde{G}}(Z(\tilde{G})W)$. Let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n)) \subseteq \tilde{G}$, and let $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. As in the proof of part (a) of Theorem 2.7.10, it follows from

$$(RDR^{-1})(RPR^{-1}) = RDPR^{-1} = DP$$

and

$$\delta(UDU^{-1})(UPU^{-1})\delta = (\delta U)DP(\delta U)^{-1} = DP$$

that $RDR^{-1} = D$, $RPR^{-1} = P$, $\delta(UDU^{-1}) = D(P\delta P^{-1})$, and $UPU^{-1} = P$. In particular, $P \in Z(\mathrm{PerMat}(S)) = \mathrm{PerMat}(\{\mathrm{id}, (1,2)(3,4)\cdots(n-1,n)\})$.

Suppose that $P = \mathrm{PerMat}((1,2)\cdots(n-1,n))$. Then $P\delta P^{-1} = \mathrm{diag}(1,-1,1,\ldots,1)$, so $\delta(UDU^{-1}) = D(P\delta P^{-1})$ implies $UDU^{-1} = D\,\mathrm{diag}(-1,-1,1,\ldots,1)$.
We write $D = \mathrm{diag}(d_1,\ldots,d_n)$. Then taking $U := \mathrm{PerMat}(1,2)$ in $UDU^{-1} = D\,\mathrm{diag}(-1,-1,1,\ldots,1)$, we obtain $d_1 = -d_2$, and taking $R := \mathrm{PerMat}((1,2)(3,4))$ in $RDR^{-1} = D$ implies $d_1 = d_2$, a contradiction.

Thus, P must be the identity matrix. It follows that $P\delta P^{-1} = \delta$, so $\delta(UDU^{-1}) = D(P\delta P^{-1})$ implies $UDU^{-1} = D$. Therefore, Proposition 2.7.2 and Theorem 2.7.10 imply

$$D \in C_T(\mathrm{PerMat}(S)) \cap \mathrm{SL}_n(q) = Z(G) \cap \mathrm{SL}_n(q) = Z(\tilde{G}),$$

so $DP \in Z(\tilde{G})W$.
Now, suppose that there exist $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$ be such that $D\delta P \in C_{\tilde{G}}(Z(\tilde{G})W)$. Again, let $R \in \mathrm{PerMat}(S\cap\mathrm{Alt}(n))$ and $U \in \mathrm{PerMat}(S\setminus\mathrm{Alt}(n))$. As in the proof of part (a) of Theorem 2.7.10, it follows from

$$(RD\delta R^{-1})(RPR^{-1}) = RD\delta PR^{-1} = D\delta P$$

and

$$\delta(UD\delta U^{-1})(UPU^{-1})\delta = (\delta U)D\delta P(\delta U)^{-1} = D\delta P$$

that $RD\delta R^{-1} = D\delta$, $RPR^{-1} = P$, $UD\delta U^{-1} = D(P\delta P^{-1})$, and $UPU^{-1} = P$. In particular, we have

$$P \in Z(\mathrm{PerMat}(S)) = \mathrm{PerMat}(\{\mathrm{id}, (1,2)(3,4)\cdots(n-1,n)\}) \subseteq \mathrm{PerMat}(\mathrm{Alt}(n))$$

contradicting the choice of P.

(c) It is clear that

$$|WZ/Z| = \frac{|W|}{|W \cap Z|} = \frac{|W|}{|\{\pm \mathbb{1}_n\}|} = \frac{|W|}{2} = 2^{2^{m+1}-3}.$$

Now, let $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ be such that $X := DP$ satisfies $XZ \in C_{\tilde{G}Z/Z}(WZ/Z)$. As above, let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ and $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. Then

$$DPRP^{-1}D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

is a scalar matrix, say $c_R \cdot \mathbb{1}_n$, and it follows that $PRP^{-1}R^{-1} = c_R D^{-1}RDR^{-1}$, so both sides are $\mathbb{1}_n$. Also

$$DP\delta UP^{-1}D^{-1}U^{-1}\delta = X(\delta U)X^{-1}(\delta U)^{-1} \in Z$$

is a scalar matrix, say $c_U \cdot \mathbb{1}_n$, and it follows that

$$PUP^{-1}U^{-1} = c_U D^{-1}UDU^{-1}\delta P\delta P^{-1},$$

so both sides are $\mathbb{1}_n$ again. In particular,

$$P \in Z(\mathrm{PerMat}(S)) = \mathrm{PerMat}(\{\mathrm{id}, (1,2)(3,4)\cdots(n-1,n)\}).$$

Let us write $D = \mathrm{diag}(d_1, \dots, d_n)$.

Suppose that $P = \mathrm{PerMat}((1,2)\cdots(n-1,n))$. Then $P\delta P^{-1} = \mathrm{diag}(1,-1,1,\dots,1)$ and $D = c_U UDU^{-1}\,\mathrm{diag}(-1,-1,1,\dots,1)$.
Next, suppose that $n > 4$. Taking $U := \mathrm{PerMat}(1,2)$, we obtain $c_U = 1$ and $d_1 = -d_2$, and taking $R := (1,2)(3,4)$, we obtain $c_R = 1$ and $d_1 = d_2$, a contradiction. Thus, we have $n = 4$.
For $U := \mathrm{PerMat}(1,2)$, we get $d_1 = -d_2$, and for $U := \mathrm{PerMat}(3,4)$, we get $d_3 = -d_4$. Therefore, $D = \mathrm{diag}(d_1, -d_1, d_3, -d_3)$. By assumption, $DPZ = XZ$ commutes with

$$\underbrace{\delta\,\mathrm{PerMat}(1,3,2,4)}_{\in W} Z \in WZ/Z,$$

so we obtain that

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \frac{d_1}{d_3} \\ 1 & 0 & 0 & 0 \\ 0 & \frac{d_1}{d_3} & 0 & 0 \end{pmatrix} = DP\delta\,\mathrm{PerMat}(1,3,2,4)(DP)^{-1}(\delta\,\mathrm{PerMat}(1,3,2,4))^{-1}$$

must be a scalar matrix, which is obviously not true. This contradiction shows that P must be the identity matrix.

It follows that $\delta P\delta P^{-1} = \mathbb{1}_n$, so $D = c_U UDU^{-1}$, and part (b) of Theorem 2.7.10 implies that D lies in $Z(G)A$. Now, by the definition of A we have

$$A = \left\{\mathbb{1}_n, \begin{pmatrix} \mathbb{1}_{n/2} & \\ & -\mathbb{1}_{n/2} \end{pmatrix}\right\} \subseteq W,$$

and moreover, we have $Z(\tilde{G}) = Z(G) \cap \mathrm{SL}_n(q) = Z \cap \mathrm{SL}_n(q) \subseteq Z$. Therefore, $D \in Z(G)A \subseteq WZ$, and it follows that $XZ = DPZ = DZ \in WZ/Z$.

Finally, suppose that there exist $D \in \tilde{T}$ and $P \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$ such that $X := D\delta P$ satisfies $XZ \in C_{\tilde{G}Z/Z}(Z(\tilde{G})AWZ/Z)$. Again, let $R \in \mathrm{PerMat}(S \cap \mathrm{Alt}(n))$ and $U \in \mathrm{PerMat}(S \setminus \mathrm{Alt}(n))$. As in the proof of parts (b) and (c) of Theorem 2.7.10,

$$D\delta PRP^{-1}\delta D^{-1}R^{-1} = XRX^{-1}R^{-1} \in Z$$

and

$$D\delta P\delta UP^{-1}\delta D^{-1}U^{-1}\delta = X(\delta U)X^{-1}(\delta U)^{-1} \in Z$$

are scalar matrices, say $c_R \cdot \mathbb{1}_n$ and $c_U \cdot \mathbb{1}_n$, respectively. It follows that

$$PRP^{-1}R^{-1} = c_R(D\delta)^{-1}R(D\delta)R^{-1}$$

and

$$PUP^{-1}U^{-1} = c_U(D\delta)^{-1}U(D\delta)U^{-1}P\delta P^{-1}\delta.$$

The right-hand sides of both of these equations are diagonal matrices, and the left-hand sides are permutation matrices, so in both equations both sides must be $\mathbb{1}_n$. Now, as in the proof of part (b), we have that

$$P \in Z(\mathrm{PerMat}(S)) = \mathrm{PerMat}(\{\mathrm{id}, (1,2)(3,4)\cdots(n-1,n)\}) \subseteq \mathrm{PerMat}(\mathrm{Alt}(n))$$

contradicts the choice of P.

$\square$

We obtain the following result for this section:

Theorem 2.7.14. *Let $n \in \mathbb{N}_{>0}$, let $\ell \in \mathbb{P}$, and let q be a prime power such that $\ell \nmid q$ and such that $q \equiv 1 \bmod 4$ if $\ell = 2$. Moreover, let L be a Sylow ℓ-subgroup of one of the groups $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, or $\mathrm{PSL}_n(q)$. Then the following are equivalent:*

(a) *The group order $|L|$ cannot be bounded in terms of an arbitrary self-centralizing subgroup.*

(b) *We have $\ell \mid q-1$ and $n > 1$ is a power of ℓ.*

Proof. If $\ell \nmid q-1$, then this follows from Observation 2.5.11 and from part (a) of Theorem 2.5.10. Now, let $\ell \mid q-1$. If $\ell \nmid n$, then the claim follows from Proposition 2.7.1 and from part (a) of Theorem 2.5.10. If $\ell \mid n$, then Corollary 2.7.11, Theorem 2.7.12, Theorem 2.5.7, Proposition 2.1.8, and Theorem 2.7.13 show that $|L|$ can be bounded in terms of an arbitrary self-centralizing subgroup if and only if n is not a power of ℓ. □

The previous theorem implies its analogue for special and projective (special) unitary groups. Here we have to restrict ℓ to be odd, since we did not study the Sylow 2-subgroups of those groups for $\ell = 2$.

Corollary 2.7.15. *Let $n \in \mathbb{N}_{>0}$, let $\ell \in \mathbb{P}_{>2}$, and let q be a prime power such that $\ell \nmid q$. Moreover, let L be a Sylow ℓ-subgroup of one of the groups $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, or $\mathrm{PSU}_n(q)$. Then the following are equivalent:*

(a) *The group order $|L|$ cannot be bounded in terms of an arbitrary self-centralizing subgroup.*

(b) *We have $\ell \mid q+1$ and $n > 1$ is a power of ℓ.*

Proof. If $\ell \nmid q+1$, then we are done by part (b) of Corollary 2.6.6 and Theorem 2.6.7. If $\ell \mid q+1$, then the claim follows from Theorem 2.7.14, together with part (c) of Corollary 2.6.6 and Theorem 2.6.7. □

We also obtain the following result in view of Corollary 2.1.6:

Corollary 2.7.16. *For all prime numbers $\ell \in \mathbb{P}$, it is not possible to bound the order of a finite ℓ-group in terms of the order of an arbitrary self-centralizing subgroup. This generalizes Corollary 2.1.9 which states this result for $\ell = 2$.*

Proof. If $r \in \mathbb{N}_{>0}$ is given, then by Dirichlet's Theorem on arithmetic progressions [56, see, for example, 4.IV.A on page 265] there exist infinitely many prime numbers $q \in \mathbb{P}$ such that $\ell^r \mid q-1$. Therefore, r can get arbitrarily large, but the orders of the self-centralizing subgroups given in Theorem 2.7.12 and Theorem 2.7.13 do not depend on r if $m < r$ is fixed. □

We did not consider the groups $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ for $\ell = 2$ and $q \equiv 3 \bmod 4$ in this section. The reason is that in this case, Corollary 2.5.4 does not apply, so we cannot work with monomial matrices as in the situation above. More precisely, Proposition 2.5.6 shows that for $\ell = 2$ and $q \equiv 3 \bmod 4$, a Sylow 2-subgroup of $\mathrm{GL}_n(q)$ is of the form $G \wr S$, where $G \in \mathrm{Syl}_2(\mathrm{GL}_2(q))$ and $S \in \mathrm{Syl}_2(\mathrm{Sym}(\frac{n}{2}))$, that is, we have to replace the diagonal part of the monomial matrices by block diagonal matrices whose blocks come from G, and then have to intersect with $\mathrm{SL}_n(q)$ or view the matrices modulo scalar matrices for $\mathrm{PGL}_n(q)$. This is much more complicated than the situation that we have considered above. Therefore, this case remains open.

3 Bounding defect groups in terms of self-centralizing subgroups

In this chapter, we introduce properties of sets of finite groups motivated by Puig's Question and then investigate sets of finite classical groups with respect to these properties using the results from Chapter 2 of this thesis and results from [28] and [29]. Moreover, we also consider sets of Chevalley groups $G_2(q)$ and of twisted Chevalley groups ${}^3D_4(q^3)$.

3.1 The self-centralizing-bounded-defect property

Motivated by Puig's Question 1.5.1 and Knörr's Theorem 1.4.7, we make the following definitions.

Definition 3.1.1. Let $\ell \in \mathbb{P}$, let X be a set of finite groups, and let V be a finite ℓ-group.

(a) X has the ***vertex-bounded-defect property (VBDP) with respect to*** V, if there is an $n_V \in \mathbb{N}$ such that for all $G \in X$ and all simple $\overline{\mathbb{F}}_\ell G$-modules M with vertices isomorphic to V, the defect groups D of the block of $\overline{\mathbb{F}}_\ell G$ containing M satisfy $|D| \leq n_V$.

(b) X has the ***strongly-bounded-defect property (SBDP) with respect to*** V, if there is an $n_V \in \mathbb{N}$ such that if (V, b_V) is any self-centralizing Brauer pair of $\overline{\mathbb{F}}_\ell G$ then the defect groups D of b_V^G satisfy $|D| \leq n_V$.

(c) X has the ***self-centralizing-bounded-defect property (SCBDP) with respect to*** V, if there is an $n_V \in \mathbb{N}$ such that for all $G \in X$ and all defect groups D of blocks of $\overline{\mathbb{F}}_\ell G$ such that V is isomorphic to a self-centralizing subgroup of D, we have $|D| \leq n_V$.

(d) X has the ***self-centralizing-bounded-Sylow property (SCBSP) with respect to*** V, if there is an $n_V \in \mathbb{N}$ such that for all $G \in X$ and all Sylow ℓ-subgroups D of G such that V is isomorphic to a self-centralizing subgroup of D, we have $|D| \leq n_V$.

The definition of the VBDP and the SBDP are similar as in [18, Def. 3.2, Rmk. 3.12]. In this thesis, we prefer to consider the SCBDP which is the strongest among these properties, see Observation 3.1.4.

First, we define the following set:

Remark 3.1.2. Let S be the set of all finite subgroups of $\mathrm{Sym}(\mathbb{N})$, and let $\mathcal{F}$ be a set of representatives of S with respect to the equivalence relation given by isomorphism. Then, by Cayley's Theorem (see, for example, [37, Satz I.6.3]), for each finite group G there exists a unique element of $\mathcal{F}$ which is isomorphic to G. Thus, $\mathcal{F}$ can be seen as the *set of all finite groups up to isomorphism.*

Puig's Question 1.5.1 can now be reformulated as follows:

Remark 3.1.3 (Puig's Question reformulated)**.** Given $\ell \in \mathbb{P}$, does $\mathcal{F}$ have the VBDP with respect to every finite ℓ-group?

We have the following implications among the properties from Definition 3.1.1:

Observation 3.1.4. *Let $\ell \in \mathbb{P}$, let X be a set of finite groups, and let V be a finite ℓ-group.*

(a) *If X has the SCBDP with respect to V, then it has also the SCBSP and the SBDP with respect to V.*

(b) *If X has the SBDP with respect to V, then it has also the VBDP with respect to V.*

In particular, the SCBDP implies all the other properties.

Proof.

(a) As the Sylow subgroups of a finite groups always occur as defect groups, it is clear that the SCBDP implies the SCBSP. Moreover, by Theorem 1.4.5 and Theorem 1.4.6, the SCBDP implies the SBDP.

(b) This follows immediately from Theorem 1.4.7.

□

The following example shows that the set of all finite symmetric groups has the VBDP with respect to every finite ℓ-group:

Example 3.1.5 ([55],[17])**.** Let $\ell \in \mathbb{P}$, and let $n \in \mathbb{N}$. If V is a vertex of a simple $\overline{\mathbb{F}}_\ell \operatorname{Sym}(n)$-module and D is a defect group of the corresponding block of $\overline{\mathbb{F}}_\ell \operatorname{Sym}(n)$, then $|\mathsf{D}| \leq |\mathsf{V}|!$.

We continue this section with the investigation of the SCBDP and the VBDP. First, we have some easy consequences and examples.

Remark 3.1.6. Let $\ell \in \mathbb{P}$, and let X and Y be sets of finite groups.

(a) It is clear that the union $\mathsf{X} \cup \mathsf{Y}$ has the VBDP or the SCBDP or the SCBSP with respect to a finite ℓ-group V if and only if both X and Y have the VBDP or the SCBDP or the SCBSP with respect to V.

(b) If X and Y have the VBDP or the SCBDP or the SCBSP with respect to every finite ℓ-group, then the same is true for the set $\{\mathsf{G} \times \mathsf{H} \,:\, \mathsf{G} \in \mathsf{X},\ \mathsf{H} \in \mathsf{Y}\}$. This is obvious for the SCBSP, and for the other two properties it follows from Lemma 1.3.2.

Proposition 3.1.7. *Let $\ell \in \mathbb{P}$.*

(a) *The set*

$$\{G \in \mathcal{F} \ : \ G \textit{ has abelian Sylow } \ell\textit{-subgroups}\}$$

has the SCBDP with respect to every finite ℓ-group.

(b) *For every $k \in \mathbb{N}$, the set $\{G \in \mathcal{F} \ : \ \mathrm{Exp}_\ell(G) < k\}$, where $\mathrm{Exp}_\ell(G)$ is the exponent of a Sylow ℓ-subgroup of G, has the SCBDP with respect to every finite ℓ-group. In particular, every finite subset of $\mathcal{F}$ and the set $\{G \in \mathcal{F} \ : \ \ell \nmid |G|\}$ have the SCBDP with respect to every finite ℓ-group.*

(c) *The set $\{G \in \mathcal{F} \ : \ |\mathrm{Syl}_\ell(G)| = 1\}$ has the VBDP with respect to every finite ℓ-group. In particular, the set $\{G \in \mathcal{F} \ : \ G \textit{ nilpotent}\}$ has the VBDP with respect to every finite ℓ-group.*

(d) *$\mathcal{F}$ has the VBDP with respect to every cyclic ℓ-group.*

Proof.

(a) This is clear by Observation 2.1.2.

(b) This follows immediately from Corollary 2.1.6.

(c) This is a consequence of part (d) of Proposition 1.2.6.

(d) This is clear by part (d) of Proposition 1.3.1. □

Example 3.1.8. Let $\ell \in \mathbb{P}$.

(a) As all of its elements have abelian Sylow ℓ-subgroups, the set $\{\mathrm{AGL}_1(q) \ : \ q \text{ prime power}\}$ has the SCBDP with respect to every finite ℓ-group. Here, the ***affine linear group*** $\mathrm{AGL}_1(q) \cong \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ is the group of all maps $\mathbb{F}_q \to \mathbb{F}_q : x \mapsto ax + b$ where $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$.

(b) The finite set of all sporadic simple groups has the SCBDP with respect to every finite ℓ-group.

(c) Example 1.5.2 shows that $\{\mathrm{PSL}_2(q) \ : \ q \text{ prime power}\}$ does not have the VBDP with respect to the Klein four-group.

The following theorem is an immediate consequence of [7, Thm. 4.3]:

Theorem 3.1.9. *For all $\ell \in \mathbb{P}$, the subset $\{G \in \mathcal{F} \ : \ G \textit{ is } \ell\textit{-solvable}\}$ of $\mathcal{F}$ has the VBDP with respect to every finite ℓ-group.*

In particular, it follows that the set $\{\mathrm{Dih}_{2n} \ : \ n \in \mathbb{N}_{>2}\}$ has the VBDP with respect to every finite ℓ-group. Therefore, part (c) of the following proposition shows that the SCBDP is really stronger than the VBDP:

Proposition 3.1.10.

(a) *If $\ell \in \mathbb{P}_{>2}$, then the set* $\{\mathrm{Dih}_{2n} \ : \ n \in \mathbb{N}_{>2}\}$ *has the SCBDP with respect to every finite ℓ-group.*

(b) *The set* $\{\mathrm{Dih}_{2n} \ : \ 4 \nmid n \in \mathbb{N}_{>2}\}$ *has the SCBDP with respect to every finite 2-group.*

(c) *The set* $\{\mathrm{Dih}_{2n} \ : \ 4 \mid n \in \mathbb{N}_{>2}\}$ *does not have the SCBSP with respect to the Klein four-group. In particular, the subset of $\mathcal{F}$ of all ℓ-solvable groups does not have the SCBSP with respect to the Klein four-group.*

Proof.

(a), (b) For odd ℓ, the Sylow ℓ-subgroups of Dih_{2n} are cyclic and, therefore, abelian. Moreover, in the situation of part (b), the Sylow 2-subgroups of Dih_{2n} have order at most 4, so they are abelian, too. Thus, the claim follows from part (a) of Proposition 3.1.7.

(c) Let $4 \mid n \in \mathbb{N}_{>2}$. A Sylow 2-subgroup P of Dih_{2n} cannot be contained in the cyclic subgroup of order n (since otherwise it cannot have order $(2n)_2$). Thus, it is a dihedral group itself or has order at most four, see, for example, [57, 2.37 (page 54)]. As $4 \mid n$, it follows that $|P| \geq 8$, so P must be dihedral itself. Now, by part (a) of Proposition 2.1.8, P has a self-centralizing subgroup isomorphic to the Klein four-group.

□

We continue with some auxiliary results that will be applied in the next section. First, we need the following lemmas:

Lemma 3.1.11. *Let $\ell \in \mathbb{P}$, let X be a set of finite groups, and let V be a finite ℓ-group.*

(a) *X has the SCBDP with respect to V if and only if there exists a monotonously increasing function $f_V : \mathbb{N}_{>0} \to \mathbb{R}$ such that for all $G \in X$ and all defect groups D of blocks of $\overline{\mathbb{F}}_\ell G$ having a self-centralizing subgroup isomorphic to V, we have $|D| \leq f_V(|V|)$.*

(b) *X has the SCBSP with respect to V if and only if there exists a monotonously increasing function $f_V : \mathbb{N}_{>0} \to \mathbb{R}$ such that for all $G \in X$ and all $S \in \mathrm{Syl}_\ell(G)$ having a self-centralizing subgroup isomorphic to V, we have $|S| \leq f_V(|V|)$.*

(c) *X has the VBDP with respect to V if and only if there exists a monotonously increasing function $f_V : \mathbb{N}_{>0} \to \mathbb{R}$ such that for all $G \in X$, all defect groups D of blocks of $\overline{\mathbb{F}}_\ell G$, and all vertices V of simple $\overline{\mathbb{F}}_\ell G$-modules lying in a block with defect group D we have $|D| \leq f_V(|V|)$.*

Proof.

(a) Up to the monotony this is just the definition. If f is such a function which is not necessarily monotonously increasing, then define $g : \mathbb{N}_{>0} \to \mathbb{R}$ inductively by $g(1) := f(1)$ and $g(n+1) := \max\{g(n), f(n+1)\}$ for $n \in \mathbb{N}_{>1}$. Then g is monotonously increasing and $|D| \leq f(|V|) \leq g(|V|)$ for all D and all self-centralizing $V \leq D$.

(b), (c) The proof is analogous to the one of part (a).

□

Lemma 3.1.12. *Let G be a finite group, let $N \trianglelefteq G$, let $H \leq G$, and let V be a self-centralizing subgroup of HN/N. Then H has a self-centralizing subgroup $\tilde{V}$ satisfying $H \cap N \subseteq \tilde{V}$ and $\tilde{V}/(H \cap N) \cong V$.*

Proof. Let

$$\alpha : H/(H \cap N) \to HN/N : h(H \cap N) \mapsto hN$$

be the isomorphism from the Isomorphism Theorem, and let $H \cap N \leq \tilde{V} \leq H$ be such that $V = \alpha(\tilde{V}/(H \cap N))$. Let $h \in C_H(\tilde{V})$. Then $h(H \cap N) \in C_{H/(H \cap N)}(\tilde{V}/(H \cap N))$, and applying α, we have $hN = \alpha(h(H \cap N)) \in C_{HN/N}(V) \subseteq V$. Thus, $hN \in V = \alpha(\tilde{V}/(H \cap N))$, so $h(H \cap N) = \alpha^{-1}(hN) \in \tilde{V}/(H \cap N)$. This shows that $h \in \tilde{V}$. □

Lemma 3.1.13. *Let $\ell \in \mathbb{P}$, let G be a finite group and let N be a normal subgroup of G such that $\ell \nmid |G : N|$. Moreover, let D be a defect group of a block B of $\overline{\mathbb{F}}_\ell G$. Then D is contained in N and it is also a defect group for all $\overline{\mathbb{F}}_\ell N$-blocks covered by B.*

Proof. Let $b \in \mathrm{Bl}(\overline{\mathbb{F}}_\ell N)$ be covered by B. By Proposition 1.3.4, $D \cap N$ is a defect group of b. Moreover, it follows from $\ell \nmid |G : N|$ that the Sylow ℓ-subgroups of G are contained in N. Therefore, every ℓ-subgroup of G is contained in N. In particular, D is contained in N and we have $D \cap N = D$. □

Proposition 3.1.14. *Let $k \in \mathbb{N}$, and let X be a set of finite groups. If X has the SCBSP with respect to every finite ℓ-group (or every finite abelian ℓ-group), then so does the set $\{U \ : \ G \in X, \ U \leq G, \ |G : U|_\ell \leq k\}$.*

Proof. Let $G \in X$, and let $U \leq G$ be such that $|G : U|_\ell \leq k$. Let $S \in \mathrm{Syl}_\ell(U)$, and let $V \leq S$ be a self-centralizing subgroup. There exists some $P \in \mathrm{Syl}_\ell(G)$ such that $S = P \cap U$, and by Proposition 2.5.8, there exists some self-centralizing subgroup $\tilde{V}$ of P such that

$$|\tilde{V} : V| \leq |P : S| = |G : U|_\ell \leq k.$$

Thus, if $f_{\tilde{V}} : \mathbb{N}_{>0} \to \mathbb{R}$ is as in Lemma 3.1.11, then

$$|S| \leq |P| \leq f_{\tilde{V}}(|\tilde{V}|) \leq f_{\tilde{V}}(k|V|).$$

□

Proposition 3.1.15. *Let $\ell \in \mathbb{P}$ and let X be a set of finite groups having the SCBDP with respect to every finite ℓ-group.*

(a) *For every $k \in \mathbb{N}$, the set $\{G/N \;:\; G \in X,\; N \trianglelefteq G,\; |N|_\ell \leq k\}$ has the SCBDP with respect to every finite ℓ-group.*

(b) *For every $k \in \mathbb{N}$, the set $\{N \;:\; G \in X,\; N \trianglelefteq G,\; |G : N|_\ell \leq k\}$ has the SCBDP with respect to every finite ℓ-group.*

(c) *The set $\{G \in \mathcal{F} \;:\; \exists\, N \in X,\; N \trianglelefteq G,\; \ell \nmid |G : N|\}$ has the SCBDP with respect to every finite ℓ-group.*

Proof.

(a) Let $G \in X$, and let $N \trianglelefteq G$ be such that $|N|_\ell \leq k$. Let B be a block of $\overline{\mathbb{F}}_\ell[G/N]$, let $D \in \mathrm{Def}(B)$, and let V be a self-centralizing subgroup of D. Moreover, let $\tilde{B}$ and $\tilde{D}$ be as in Proposition 1.3.5. By Lemma 3.1.12, $\tilde{D}$ has a self-centralizing subgroup $\tilde{V}$ such that $\tilde{V}/(\tilde{D} \cap N) \cong V$. Now, with $f_{\tilde{V}} : \mathbb{N}_{>0} \to \mathbb{R}$ as in Lemma 3.1.11, it follows that

$$|D| \leq |\tilde{D} \cap N| \cdot |D| \leq |\tilde{D}| \leq f_{\tilde{V}}(|\tilde{V}|) = f_{\tilde{V}}(|\tilde{D} \cap N| \cdot |V|) \leq f_{\tilde{V}}(|N|_\ell \cdot |V|) \leq f_{\tilde{V}}(k \cdot |V|).$$

(b) Let $G \in X$, and let $N \trianglelefteq G$ such that $|G : N|_\ell \leq k$. Let B be a block of $\overline{\mathbb{F}}_\ell N$, and let D be a defect group of B. There is a block of $\overline{\mathbb{F}}_\ell G$ covering B and having a defect group $\tilde{D}$ such that $D = \tilde{D} \cap N$ by Proposition 1.3.4. If $V \leq D$ is self-centralizing, then by Proposition 2.5.8 there exists some self-centralizing subgroup $\tilde{V} \leq \tilde{D}$ such that

$$|\tilde{V} : V| \leq |\tilde{D} : D| = |\tilde{D} : (\tilde{D} \cap N)| = |\tilde{D}N : N| \;\Big|\; |G : N|_\ell \leq k.$$

Now, with $f_{\tilde{V}} : \mathbb{N}_{>0} \to \mathbb{R}$ as in Lemma 3.1.11, it follows that

$$|D| \leq |\tilde{D}| \leq f_{\tilde{V}}(|\tilde{V}|) \leq f(k \cdot |V|).$$

(c) This follows immediately from Lemma 3.1.13.

□

Proposition 3.1.16. *Let $\ell \in \mathbb{P}$ and let X be a set of finite groups having the VBDP with respect to every finite ℓ-group.*

(a) *For every $k \in \mathbb{N}$, the set $\{G/N \ :\ G \in X,\ N \trianglelefteq G,\ |N|_\ell \leq k\}$ has the VBDP with respect to V.*

(b) *The set $\{G \in \mathcal{F} \ :\ \exists\ N \in X,\ N \trianglelefteq G,\ \ell \nmid |G : N|\}$ has the VBDP with respect to V.*

(c) *The set $\{G \in \mathcal{F} \ :\ \exists\ N \leq O_\ell(Z(G)),\ G/N \in X\}$ has the VBDP with respect to V.*

Proof.

(a) As in the proof of part (a) of the previous proposition, let $G \in X$, let $N \trianglelefteq G$ be such that $|N|_\ell \leq k$, let B be a block of $\overline{\mathbb{F}}_\ell[G/N]$, and let $D \in \mathrm{Def}(B)$. Now, let $V \leq D$ be a vertex of some simple module M lying in B. Again, let $\tilde{B}$ and $\tilde{D}$ be as in Proposition 1.3.5. Now, $\mathrm{Inf}^G_{G/N}(M)$ is a simple module of $\overline{\mathbb{F}}_\ell G$, and by the definitions of inflation and domination it is clear that $\mathrm{Inf}^G_{G/N}(M)$ lies in $\tilde{B}$. Let $\tilde{V}$ be a vertex of $\mathrm{Inf}^G_{G/N}(M)$ contained in $\tilde{D}$. Then [46, Prop. 2.1] implies that $\tilde{V}N/N$ is a vertex of M. In particular, we have $|V| = |\tilde{V}N/N|$. With $f_{\tilde{V}}$ as in Lemma 3.1.11 it follows that

$$|D| \leq |\tilde{D} \cap N| \cdot |D| \leq |\tilde{D}| \leq f_{\tilde{V}}(|\tilde{V}|) = f_{\tilde{V}}(|\tilde{V} \cap N| \cdot |V|) \leq f_{\tilde{V}}(|N|_\ell \cdot |V|) \leq f_{\tilde{V}}(k \cdot |V|).$$

(b) Let $G \in \mathcal{F}$ and $N \trianglelefteq G$ be such that $N \in X$ and $\ell \nmid |G : N|$. Let B be a block of $\overline{\mathbb{F}}_\ell G$, and let M be a simple $\overline{\mathbb{F}}_\ell G$-module lying in B. Then M is relatively $N \cap O_\ell(G)$-projective by part (d) of Proposition 1.2.6. Thus, M is also relatively N-projective by part (b) of Proposition 1.2.4. Now, part (c) of Proposition 1.2.6 shows that $\mathrm{Res}^G_N(M)$ has an indecomposable summand S whose vertices are already vertices of M. Thus, if V is a vertex of M, then there exists some $g \in G$ such that ${}^gV$ is a vertex of S. Now, by Clifford's Theorem [52, Thm. 3.3.1], $\mathrm{Res}^G_N(M)$ is semisimple, so S must be simple. Moreover, [52, Lem. 5.5.7] implies that S belongs to a block b of $\overline{\mathbb{F}}_\ell N$ covered by B. Thus, Lemma 3.1.13 implies that each defect group of B is also a defect group of b. Therefore, if $f_{{}^gV}$ is as in Lemma 3.1.11, then we have $|D| \leq f_{{}^gV}(|{}^gV|) = f_{{}^gV}(|V|)$.

(c) Let $G \in \mathcal{F}$ and let $N \leq O_\ell(Z(G))$ be such that $G/N \in X$. Let D be a defect group of a block B of $\overline{\mathbb{F}}_\ell G$, let M be a simple module lying in B, and let $V \leq D$ be a vertex of M. Then $N \subseteq V$ by part (d) of Proposition 1.2.6. By Clifford's Theorem [52, Thm. 3.3.1], $\mathrm{Res}^G_N(M)$ is semisimple. As the trivial $\overline{\mathbb{F}}_\ell N$-module is the only simple $\overline{\mathbb{F}}_\ell N$-module up to isomorphism, it follows that $\mathrm{Res}^G_N(M)$ is a direct sum of copies of the trivial $\overline{\mathbb{F}}_\ell N$-module. Therefore, we have $N \subseteq \ker(M)$ and there exists a simple $\overline{\mathbb{F}}_\ell[G/N]$-module E lying in some block b of $\overline{\mathbb{F}}_\ell[G/N]$ such that $M = \mathrm{Inf}^G_{G/N}(E)$. By [46, Prop. 2.1], V/N is a vertex of E. As before, by the definitions of inflation and domination it is clear that B dominates b. Now, it follows from [6, Lem. 6.4.2] that D/N is a defect group of b. Therefore, if $\mathsf{f}_{\mathsf{V}/\mathsf{N}}$ is as in Lemma 3.1.11, we have

$$|\mathsf{D}| = |\mathsf{D}/\mathsf{N}||\mathsf{N}| \leq \mathsf{f}_{\mathsf{V}/\mathsf{N}}(|\mathsf{V}/\mathsf{N}|)|\mathsf{N}| \leq \mathsf{f}_{\mathsf{V}/\mathsf{N}}(|\mathsf{V}|)|\mathsf{N}| \leq \mathsf{f}_{\mathsf{V}/\mathsf{N}}(|\mathsf{V}|)|\mathsf{O}_{\ell}(\mathsf{G})| \leq \mathsf{f}_{\mathsf{V}/\mathsf{N}}(|\mathsf{V}|)|\mathsf{V}|.$$

□

Instead of the set in part (c) of Proposition 3.1.16, one might expect that the set

$$\{\mathsf{G} \in \mathcal{F} \ : \ \exists\ \mathsf{N} \trianglelefteq \mathsf{G},\ \ell \nmid |\mathsf{N}|,\ \mathsf{G}/\mathsf{N} \in \mathsf{X}\}$$

has the VBDP, or even the SCBDP, if X does. We can only prove this statement for the SCBSP, where the proof is trivial:

Observation 3.1.17. *Let $\ell \in \mathbb{P}$, let V be a finite ℓ-group, and let X be a set of finite groups having the SCBSP with respect to V. Then so does the set*

$$\{\mathsf{G} \in \mathcal{F} \ : \ \exists\ \mathsf{N} \trianglelefteq \mathsf{G},\ \ell \nmid |\mathsf{N}|,\ \mathsf{G}/\mathsf{N} \in \mathsf{X}\}.$$

Proof. If $\mathsf{S} \in \mathrm{Syl}_{\ell}(\mathsf{G})$ and $\mathsf{N} \trianglelefteq \mathsf{G}$ such that $\ell \nmid |\mathsf{N}|$, then $\mathsf{S} \cong \mathsf{S}/(\mathsf{S} \cap \mathsf{N}) \cong \mathsf{SN}/\mathsf{N} \in \mathrm{Syl}_{\ell}(\mathsf{G}/\mathsf{N})$. □

Next, we consider semidirect products with an abelian normal subgroup.

Remark 3.1.18 ([43, Thm. 1.13])**.** Let G be a finite group, let $\mathsf{H} \trianglelefteq \mathsf{G}$ be abelian, and let $\mathsf{U} \leq \mathsf{G}$ be such that $\mathsf{G} = \mathsf{H} \rtimes \mathsf{U}$ is an inner semidirect product. Let E be a simple $\overline{\mathbb{F}}_{\ell}\mathsf{H}$-module, and let $\mathsf{T} \supseteq \mathsf{H}$ denote its inertia group in G. Then E can be extended to all of T via $\mathsf{hu}\cdot\mathsf{x} := \mathsf{h}\cdot\mathsf{x}$, and by abuse of notation, we denote this module again by E. Moreover, let E' be a simple $\overline{\mathbb{F}}_{\ell}[\mathsf{T}/\mathsf{H}]$-module. Then the $\overline{\mathbb{F}}_{\ell}\mathsf{G}$-module $\mathrm{Ind}_{\mathsf{T}}^{\mathsf{G}}(\mathsf{E} \otimes_{\overline{\mathbb{F}}_{\ell}} \mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}'))$ is simple, and every simple $\overline{\mathbb{F}}_{\ell}\mathsf{G}$-module is of this form.

Lemma 3.1.19. *Let G, H, U, E, T, and E' be given as in Remark 3.1.18. Let V be a vertex of $\mathrm{Ind}_{\mathsf{T}}^{\mathsf{G}}(\mathsf{E} \otimes_{\overline{\mathbb{F}}_{\ell}} \mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}'))$ or of $\mathsf{E} \otimes_{\overline{\mathbb{F}}_{\ell}} \mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}')$ or of $\mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}')$. Then $\mathsf{V} \cap \mathsf{H}$ is the Sylow ℓ-subgroup of H (and, therefore, normal in G).*

Proof. As H is abelian and normal in G, it follows that the same is true for the Sylow ℓ-subgroup P of H. Therefore, by part (d) of Proposition 1.2.6, P is contained in V. On the other hand, $\mathsf{V} \cap \mathsf{H}$ is an ℓ-subgroup of H and, thus, contained in P. □

Lemma 3.1.20. *Let G, H, U, E, and T be given as in Remark 3.1.18. Moreover, let E' and E'' be simple $\overline{\mathbb{F}}_{\ell}[\mathsf{T}/\mathsf{H}]$-modules that lie in the same block. Then $\mathrm{Ind}_{\mathsf{T}}^{\mathsf{G}}(\mathsf{E} \otimes_{\overline{\mathbb{F}}_{\ell}} \mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}'))$ and $\mathrm{Ind}_{\mathsf{T}}^{\mathsf{G}}(\mathsf{E} \otimes_{\overline{\mathbb{F}}_{\ell}} \mathrm{Inf}_{\mathsf{T}/\mathsf{H}}^{\mathsf{T}}(\mathsf{E}''))$ lie in the same block as well, and the latter block is the Brauer induction of the $\overline{\mathbb{F}}_{\ell}\mathsf{H}$-block of E.*

Proof. Let e denote the block idempotent of $\overline{\mathbb{F}}_\ell[T/H]$ corresponding to the block of E' and E''. Moreover, let $\mu : \overline{\mathbb{F}}_\ell T \to \overline{\mathbb{F}}_\ell[T/H]$ be the linear extension of the residue class homomorphism. By Proposition 1.3.5, e is dominated by a unique block idempotent c of $\overline{\mathbb{F}}_\ell T$. Therefore, for all $x \in \mathrm{Inf}_{T/H}^T(E') \cup \mathrm{Inf}_{T/H}^T(E'')$ we have $c \cdot x = f(c) \cdot x \neq 0$, which shows that both $\mathrm{Inf}_{T/H}^T(E')$ and $\mathrm{Inf}_{T/H}^T(E'')$ lie in the block of $\overline{\mathbb{F}}_\ell T$ that corresponds to c. Now, E has dimension 1 as H is abelian, so the simple module $E^* \otimes_{\overline{\mathbb{F}}_\ell} E$ is isomorphic to the trivial module by [53, Lem. 2.4], where E^* denotes the dual module of E.
By [2, Prop. 4.3], there exist simple modules $T_1, \dots, T_r$ and non-split exact sequences

$$0 \to T_i \to M_i \to T_{i+1} \to 0$$

for all $i = 1, \dots, r-1$ such that $\mathrm{Inf}_{T/H}^T(E') = T_1$ and $\mathrm{Inf}_{T/H}^T(E'') = T_r$. As the tensor product is taken over a field, we thus get exact sequences

$$0 \to E \otimes_{\overline{\mathbb{F}}_\ell} T_i \to E \otimes_{\overline{\mathbb{F}}_\ell} M_i \to E \otimes_{\overline{\mathbb{F}}_\ell} T_{i+1} \to 0$$

for $i = 1, \dots, r-1$. The latter cannot be split exact, since by tensoring again with E^*, we get the original sequences back. Using [2, Prop. 4.3] again, it follows that $E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E')$ and $E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E'')$ lie in the same $\overline{\mathbb{F}}_\ell T$-block, say b_T.
Now, by Clifford's Theorem [52, Thm. 3.3.1], the restriction $\mathrm{Res}_H^T(\mathrm{Inf}_{T/H}^T(E'))$ is semisimple, so it is a direct sum of simple modules. Being an inflation from T/H, the module $\mathrm{Inf}_{T/H}^T(E')$ contains H in its kernel. Thus, $\mathrm{Res}_H^T(\mathrm{Inf}_{T/H}^T(E'))$ must be a direct sum of copies of the trivial $\overline{\mathbb{F}}_\ell H$-module. It follows that

$$\mathrm{Res}_H^T(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E')) \cong \mathrm{Res}_H^T(E) \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Res}_H^T(\mathrm{Inf}_{T/H}^T(E'))$$

is isomorphic to a direct sum of $\dim_{\overline{\mathbb{F}}_\ell}(E')$ copies of $\mathrm{Res}_H^T(E)$, so [52, Lem. 5.5.7(ii)] implies that b_T covers the block b_H of E. Now, let $S := \{g \in G : {}^g b_H = b_H\}$ be the inertia group of b_H.
It is obvious that T is contained in S. Conversely, if $g \in S$, then the simple module ${}^g E$ lies in the block ${}^g b_H = b_H$. As H is abelian, E is the only simple module in b_H up to isomorphism by [53, Cor. 2.10, Thm. 4.8, Prop. 4.8], so it follows that ${}^g E = E$, which shows that we actually have $T = S$.
Therefore, by the Fong–Reynold Theorem [52, Thm. 5.5.10], both $\mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E'))$ and $\mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E''))$ lie in the block b_H^G of G. □

Corollary 3.1.21. *Let* G, H, U, E, T, *and* E' *be given as in Remark 3.1.18. If a vertex* D *of the simple* $\overline{\mathbb{F}}_\ell G$*-module* $\mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E'))$ *is a defect group of the corresponding* $\overline{\mathbb{F}}_\ell G$*-block, then* DH/H *is a defect group of the* $\overline{\mathbb{F}}_\ell[T/H]$*-block that contains* E'*. Moreover,* $|DH/H| = |D|/|H|_\ell$.

Proof. Lemma 3.1.19 implies that $|DH/H| = |D/(D \cap H)| = |D|/|H|_\ell$. Moreover, it follows from [46, Prop. 2.1] that if D is a vertex of $\mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E'))$, then DH/H is a vertex of E'. Thus, if DH/H is not a defect group of the $\overline{\mathbb{F}}_\ell[T/H]$-block b containing E', then there exists some simple module E'' in b such that a vertex Q of $\mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E''))$ satisfies $|QH/H| > |DH/H|$. Again, Lemma 3.1.19 shows that $|QH/H| = |Q/(Q \cap H)| = |Q|/|H|_\ell$, so we have $|Q| > |D|$, a contradiction. □

Proposition 3.1.22. *Let* H *be a finite abelian group, and let* $k \in \mathbb{N}$*. Moreover, let* X *be a set of finite groups such that the set* $Y := \{U \leq G \ : \ G \in X\}$ *has the VBDP with respect to every finite* ℓ*-group and satisfies* $|U|_\ell \leq |D| \cdot k$ *for all* $U \in Y$ *and all defect groups* D *of blocks of* U*. Then the set*

$$\{H \rtimes_\varphi U \ : \ U \in Y, \ \varphi : U \to \mathrm{Aut}(H)\}$$

has the VBDP with respect to every finite ℓ*-group, as well, where* $H \rtimes_\varphi U$ *denotes the outer semidirect product of* H *and* U *via the group homomorphism* $\varphi : U \to \mathrm{Aut}(H)$*.*

Proof. Let M be a simple $\overline{\mathbb{F}}_\ell G$-module, where $G := H \rtimes_\varphi U$ for some $U \in X$ and some group homomorphism $\varphi : U \to \mathrm{Aut}(H)$. By Remark 3.1.18, there exist a simple $\overline{\mathbb{F}}_\ell H$-module E with inertia group T, and a simple $\overline{\mathbb{F}}_\ell[T/H]$-module E' such that $M \cong \mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E'))$. Let V be a vertex of M, and let B be the $\overline{\mathbb{F}}_\ell G$-block containing M. By part (b) of Proposition 1.3.1 there exists a simple module $\tilde{M}$ in B whose vertices are the defect groups of B, and by Remark 3.1.18, we can write $\tilde{M} \cong \mathrm{Ind}_{\tilde{T}}^G(\tilde{E} \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{\tilde{T}/H}^{\tilde{T}}(\tilde{E}'))$ for a simple $\overline{\mathbb{F}}_\ell H$-module $\tilde{E}$ with inertia group $\tilde{T}$ and a simple $\overline{\mathbb{F}}_\ell[\tilde{T}/H]$-module $\tilde{E}'$.
Now, Lemma 3.1.20 implies that the block B covers the blocks b_E of E and $b_{\tilde{E}}$ of $\tilde{E}$. Therefore, by part (a) of Proposition 1.3.4, there exists some $g \in G$ such that ${}^g b_E = b_{\tilde{E}}$. As in the proof of Lemma 3.1.20, it follows from [53, Cor. 2.10, Thm. 4.8, Prop. 4.8] that ${}^g E \cong \tilde{E}$ and, thus, also ${}^g T = \tilde{T}$. Thus, we have

$$\begin{aligned}
\tilde{M} &\cong \mathrm{Ind}_{\tilde{T}}^G(\tilde{E} \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{\tilde{T}/H}^{\tilde{T}}(\tilde{E}')) \\
&= \mathrm{Ind}_{{}^gT}^G({}^gE \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{{}^gT/H}^{{}^gT}(\tilde{E}')) \\
&= \mathrm{Ind}_{{}^gT}^G({}^gE \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{{}^gT/H}^{{}^gT}({}^{gg^{-1}}\tilde{E}')) \\
&= \mathrm{Ind}_{{}^gT}^G({}^gE \otimes_{\overline{\mathbb{F}}_\ell} {}^g\,\mathrm{Inf}_{T/H}^{T}({}^{g^{-1}}\tilde{E}')) \\
&= \mathrm{Ind}_{{}^gT}^G({}^g(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^{T}({}^{g^{-1}}\tilde{E}'))) \\
&\cong \mathrm{Ind}_{T}^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^{T}({}^{g^{-1}}\tilde{E}')),
\end{aligned}$$

where the last isomorphism follows from [16, Lem. 10.12]. Now, writing $E'' := {}^{g^{-1}}\tilde{E}'$ we have $\tilde{M} \cong \mathrm{Ind}_T^G(E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E''))$.
Let $D \in \mathrm{Vx}(\tilde{M}) = \mathrm{Def}(B)$. Then Corollary 3.1.21 implies that DH/H is a defect group of the block b of $\overline{\mathbb{F}}_\ell[T/H]$ containing E''. Moreover, as V is a vertex of M, it follows from [52, Lem. 4.3.5] that V is G-conjugate to the vertices of $E \otimes_{\overline{\mathbb{F}}_\ell} \mathrm{Inf}_{T/H}^T(E')$. Thus, replacing V by a G-conjugate, we have that VH/H is a vertex of E'. Now, if C is a defect group of the $\overline{\mathbb{F}}_\ell[T/H]$-block containing E', it follows from Lemma 3.1.19 that

$$\begin{array}{rcccccc} |D| & = & \frac{|D|}{|D\cap H|} & \cdot & |D\cap H| & & \\ & = & \frac{|D|}{|D\cap H|} & \cdot & |H|_\ell & & \\ & = & \underbrace{|C|}_{\leq f_{VH/H}(|VH/H|)\leq f_{VH/H}(|V|)} & \cdot & |H|_\ell & \cdot & \underbrace{\frac{|D|/|D\cap H|}{|C|}}_{\leq |T/H|_\ell \leq k} \\ & \leq & f_{VH/H}(|V|) & \cdot & |H|_\ell & \cdot & k, \end{array}$$

where $f_{VH/H} : \mathbb{N}_{>0} \to \mathbb{R}$ is as in Lemma 3.1.11. □

An example for the set X in the previous proposition is given by the set $X := \{G \in \mathcal{F} : G \text{ nilpotent}\}$, as subgroups of nilpotent groups are nilpotent again, and the defect groups of nilpotent groups are always the Sylow subgroups. Moreover, X has the VBDP by part (c) of Proposition 3.1.7.

We finish this section with the SCBDP for symmetric and alternating groups. In fact, this statement is already a consequence of the proofs of Example 3.1.5 from [17] and of [18, Thm 3.9] together with [18, part (ii) of the proof of Thm 3.10]. We give a different proof here:

Theorem 3.1.23. *Let* $\ell \in \mathbb{P}$*. Then the set* $\{\mathrm{Sym}(n), \mathrm{Alt}(n) : n \in \mathbb{N}\}$ *has the SCBDP with respect to every finite* ℓ*-group.*

Proof. By part (b) of Proposition 3.1.15, it suffices to show that the set $\{\mathrm{Sym}(n) : n \in \mathbb{N}\}$ has the SCBDP. Let $n \in \mathbb{N}_{>0}$, let D be a defect group of a block of $\overline{\mathbb{F}}_\ell \mathrm{Sym}(n)$, and let $V \leq D$ be a self-centralizing subgroup. From [42, Thm. 6.2.45] it follows that D is isomorphic to a Sylow ℓ-subgroup of $\mathrm{Sym}(\ell w)$ for some $w \in \mathbb{N}$ (actually, w is the ℓ-weight of the corresponding block). Hence, the assertion follows from part (b) of Proposition 2.3.6 and Theorem 2.1.5. □

3.2 Results for finite classical groups

Now, we come to our results for sets of finite classical groups. First, we obtain the following two theorems from our results in Section 2:

Theorem 3.2.1. *Let* $\ell \in \mathbb{P}$*. The following sets of classical groups have the SCBSP with respect to every finite* ℓ*-group:*

(a) *for all* $n \in \mathbb{N}_{>0}$*, the sets*

$$\{\mathrm{GL}_n(q),\ \mathrm{SL}_n(q),\ \mathrm{PGL}_n(q), \mathrm{PSL}_n(q) \ :\ q \text{ *power of* } \ell\};$$

(b) *if $\ell = 2$, then the sets*

$$\{\mathrm{GL}_n(q) \ :\ n \in \mathbb{N}_{>0},\ q \textit{ prime power, } q \equiv 1 \bmod 4\},$$
$$\{\mathrm{GU}_n(q) \ :\ n \in \mathbb{N}_{>0},\ q \textit{ prime power, } q \equiv 3 \bmod 4\},$$

$$\left\{\mathrm{SL}_n(q),\ \mathrm{PSL}_n(q),\ \mathrm{PGL}_n(q) \ :\ \begin{matrix} q \textit{ prime power, } q \equiv 1 \bmod 4, \\ n \in \mathbb{N}_{>0} \setminus \left\{2, 4, \ldots, \frac{1}{2}(q-1)_2\right\} \end{matrix}\right\};$$

(c) *if $\ell > 2$, then the sets*

$$\{\mathrm{GL}_n(q),\ \mathrm{GU}_n(q) \ :\ n \in \mathbb{N}_{>0},\ q \textit{ prime power, } \ell \nmid q\},$$

$$\left\{\mathrm{SL}_n(q),\ \mathrm{PSL}_n(q),\ \mathrm{PGL}_n(q) \ :\ \begin{matrix} q \textit{ prime power, } \ell \nmid q, \\ n \in \mathbb{N}_{>0} \setminus \left\{\ell, \ell^2, \ldots, \frac{1}{\ell}(q-1)_\ell\right\} \end{matrix}\right\},$$

$$\left\{\mathrm{SU}_n(q),\ \mathrm{PSU}_n(q),\ \mathrm{PGU}_n(q) \ :\ \begin{matrix} q \textit{ prime power, } \ell \nmid q, \\ n \in \mathbb{N}_{>0} \setminus \left\{\ell, \ell^2, \ldots, \frac{1}{\ell}(q^2-1)_\ell\right\} \end{matrix}\right\};$$

(d) *if $\ell > 2$, then the set*

$$\{\mathrm{Sp}_{2n}(q),\ \mathrm{PSp}_{2n}(q) \ :\ n \in \mathbb{N},\ q \textit{ prime power, } \ell \nmid q\};$$

(e) *if $\ell > 2$, then the set*

$$\begin{aligned} \{&\mathrm{GO}_{2n+1}(q),\ \mathrm{GO}^+_{2n}(q),\ \mathrm{GO}^-_{2n}(q), \\ &\mathrm{PGO}_{2n+1}(q),\ \mathrm{PGO}^+_{2n}(q),\ \mathrm{PGO}^-_{2n}(q), \\ &\mathrm{PSO}^+_{2n}(q),\ \mathrm{PSO}^-_{2n}(q) \\ &\Omega_{2n+1}(q),\ \Omega^+_{2n}(q),\ \Omega^-_{2n}(q), \\ &\mathrm{Spin}_{2n+1}(q),\ \mathrm{Spin}^+_{2n}(q),\ \mathrm{Spin}^-_{2n}(q), \\ &\mathrm{P}\Omega^+_{2n}(q),\ \mathrm{P}\Omega^-_{2n}(q) \qquad :\ n \in \mathbb{N}_{>1},\ q \textit{ odd prime power, } \ell \nmid q\}. \end{aligned}$$

Proof.

(a) Part (c) of Observation 2.5.12 implies $|G| = q^{n(n-1)/2} \leq |V|^{n(n-1)/2}$ for all $G \in \mathrm{Syl}_\ell(\mathrm{GL}_n(q)) \cup \mathrm{Syl}_\ell(\mathrm{SL}_n(q)) \cup \mathrm{Syl}_\ell(\mathrm{PGL}_n(q)) \cup \mathrm{Syl}_\ell(\mathrm{PSL}_n(q))$ and all self-centralizing $V \leq G$.

(b), (c) For the sets containing the general groups of linear and unitary type, this follows immediately from part (a) of Proposition 2.5.10 and part (a) of Proposition 2.6.10. For the sets containing the special and projective (special) groups of linear and unitary type, it suffices to prove the claim for the linear case by part (c) of Corollary 2.6.6. Let us write

$$X_1 := \left\{ \mathrm{SL}_n(q),\ \mathrm{PSL}_n(q),\ \mathrm{PGL}_n(q)\ :\ \begin{array}{c} q \text{ prime power},\ \ell \nmid q, \\ n \in \mathbb{N}_{>0} \setminus \left\{\ell, \ell^2, \ldots, \frac{1}{\ell}(q-1)_\ell\right\}, \\ \ell \mid \gcd(n, q-1) \end{array} \right\}$$

and

$$X_2 := \left\{ \mathrm{SL}_n(q),\ \mathrm{PSL}_n(q),\ \mathrm{PGL}_n(q)\ :\ \begin{array}{c} q \text{ prime power},\ \ell \nmid q, \\ n \in \mathbb{N}_{>0} \setminus \left\{\ell, \ell^2, \ldots, \frac{1}{\ell}(q-1)_\ell\right\}, \\ \ell \nmid n \text{ or } \ell \nmid q-1 \end{array} \right\}.$$

Then X_2 has the SCBSP with respect to every finite ℓ-group by part (b) and Proposition 2.7.1. Moreover, X_1 has the SCBSP with respect to every finite ℓ-group by Corollary 2.7.7 and Corollary 2.7.11. Therefore, also

$$X_1 \cup X_2 = \left\{ \mathrm{SL}_n(q),\ \mathrm{PGL}_n(q),\ \mathrm{PSL}_n(q)\ :\ n,\ q;\ n \neq \ell, \ell^2, \ldots, (q-1)_\ell/\ell,\ \ell \nmid q \right\}$$

has the SCBSP with respect to every finite ℓ-group.

(d), (e) This follows immediately from Theorem 2.6.7.

□

Theorem 3.2.2. *Let $\ell \in \mathbb{P}$. The following sets of classical groups (and, therefore, also any set containing one of the following) do not have the SCBSP with respect to every finite ℓ-group. In particular, these sets do not have the SCBDP with respect to every finite ℓ-group.*

(a) *if $\ell = 2$, then for all $n \in \mathbb{N}_{>0}$ the sets*

$$\{\mathrm{GL}_n(q)\ :\ q \in \mathbb{P}_{>2},\ q \equiv 3 \bmod 4\},$$
$$\{\mathrm{GU}_n(q)\ :\ q \in \mathbb{P}_{>2},\ q \equiv 1 \bmod 4\};$$

(b) *if $\ell = 2$, then for $k \in \{1, 3\}$ the sets*

$$\{\mathrm{SL}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\},$$
$$\{\mathrm{PGL}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\},$$
$$\{\mathrm{PSL}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\},$$
$$\{\mathrm{SU}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\},$$
$$\{\mathrm{PGU}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\},$$
$$\{\mathrm{PSU}_2(q)\ :\ q \textit{ prime power},\ q \equiv k \bmod 4\};$$

(c) *if* $\ell = 2$*, then for all* $m \in \mathbb{N}_{>0}$ *the sets*

$$\begin{aligned}\{\mathrm{SL}_{2^m}(q) &: q \in \mathbb{P},\ q \equiv 1 \bmod 4\},\\ \{\mathrm{PGL}_{2^m}(q) &: q \in \mathbb{P},\ q \equiv 1 \bmod 4\},\\ \{\mathrm{PSL}_{2^m}(q) &: q \in \mathbb{P},\ q \equiv 1 \bmod 4\};\end{aligned}$$

(d) *if* $\ell > 2$*, then for all* $m \in \mathbb{N}_{>0}$ *the sets*

$$\begin{aligned}\{\mathrm{SL}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q-1\},\\ \{\mathrm{PGL}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q-1\},\\ \{\mathrm{PSL}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q-1\},\\ \{\mathrm{SU}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q+1\},\\ \{\mathrm{PGU}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q+1\},\\ \{\mathrm{PSU}_{\ell^m}(q) &: q \in \mathbb{P},\ \ell \mid q+1\}.\end{aligned}$$

Proof.

(a) We fix some $n \in \mathbb{N}_{>0}$. If $r \in \mathbb{N}_{>0}$ is given, then by Dirichlet's Theorem on arithmetic progressions [56, see, for example, 4.IV.A on page 265] there exist infinitely many prime numbers $q \in \mathbb{P}$ such that $2^r \mid q-1$ and also infinitely many prime numbers $q \in \mathbb{P}$ such that $2^r \mid q+1$. As we can choose r arbitrarily large, it follows from Corollary 2.5.3 and Proposition 2.6.4 that also the order of the Sylow 2-subgroup of $\mathrm{GL}_n(q)$, or $\mathrm{GU}_n(q)$, respectively, can get arbitrarily large. However, we have seen in part (b) of Theorem 2.5.10 and part (b) of Corollary 2.6.10 that such Sylow 2-subgroups always have a self-centralizing subgroup of order 2^n.

(b) This follows immediately from Proposition 2.1.8, Theorem 2.5.7, and Theorem 2.6.9.

(c) For $m = 1$ this follows from part (b). Now, we fix some $m \in \mathbb{N}_{>1}$. If $r \in \mathbb{N}_{>0}$ is given, then by Dirichlet's Theorem on arithmetic progressions there exist infinitely many prime numbers $q \in \mathbb{P}$ such that $2^r \mid q-1$.
As we can choose r arbitrarily large, it follows from the order formulae in Proposition 2.7.4 that the order of a Sylow 2-subgroup of $\mathrm{SL}_{2^m}(q)$, $\mathrm{PGL}_{2^m}(q)$, or $\mathrm{PSL}_{2^m}(q)$ can get arbitrarily large, too. Now, the claim follows from Theorem 2.7.12 and Theorem 2.7.13, as the orders of the self-centralizing subgroups given there do not depend on r for large $r \geq m$.

(d) For the first three sets, the proof is analogous to the proof of part (c): We fix some $m \in \mathbb{N}_{>0}$. If $r \in \mathbb{N}_{>0}$ is given, then by Dirichlet's Theorem on arithmetic progressions there exist infinitely many prime numbers $q \in \mathbb{P}$ such that $\ell^r \mid q-1$, so the order of the Sylow ℓ-subgroups of $\mathrm{SL}_{\ell^m}(q)$, $\mathrm{PGL}_{\ell^m}(q)$, and $\mathrm{PSL}_{\ell^m}(q)$ can get arbitrarily large. Now, the claim for the first three sets follows from Theorem 2.7.12, as the orders of the self-centralizing subgroups given there do not depend on r for large $r \geq m$. Finally, the claim for the last three sets follows from part (c) of Corollary 2.6.6.

$\square$

For most of the sets in Theorem 3.2.2, we cannot say whether the assertion is still true if we replace the properties by the VDBP. However, with results from Chapter 4, we have the following:

Theorem 3.2.3. *The set*

$$\{\mathrm{SL}_2(q) \ : \ q \text{ prime power, } q \equiv 1 \bmod 4\}$$

(and, therefore, also any set containing this one) does not have the VBDP with respect to the quaternion group of order 8.

Proof. It follows from part (b) of Corollary 4.1.4 that for every prime power q satisfying $q \equiv 1 \bmod 4$, there exists a simple $\overline{\mathbb{F}}_2 \mathrm{SL}_2(q)$-module in the principal block such that its vertices are quaternion groups of order 8. As $|\mathrm{SL}_2(q)|_2$ can become arbitrarily large, the assertion follows. $\square$

To generalize results from Theorem 3.2.1 to the SCBDP instead of the SCBSP, we need the following result due to Fong and Srinivasan:

Theorem 3.2.4. *Let* $n \in \mathbb{N}_{>0}$*, let* q *be a prime power, let* $\tilde{q}$ *be an odd prime power, and let* $\ell \in \mathbb{P}_{>2}$ *be such that* $\ell \nmid q \cdot \tilde{q}$.
Let

$$G \in \left\{\mathrm{GL}_n(q),\ \mathrm{GU}_n(q),\ \mathrm{Sp}_{2n}(\tilde{q}),\ \mathrm{SO}_{2n+1}(\tilde{q}),\ \mathrm{SO}^+_{2n}(\tilde{q}),\ \mathrm{SO}^-_{2n}(\tilde{q})\right\}.$$

If D *is a defect group of a block of* $\overline{\mathbb{F}}_\ell G$*, then there exist* $k, r_1, \ldots, r_k, n_1, \ldots, n_k \in \mathbb{N}$ *such that* $D \cong \bigtimes_{i=1}^{k}(C_{\ell^{r_i}} \wr X_{n_i})$*, where* $X_{n_i} \in \mathrm{Syl}_\ell(\mathrm{Sym}(n_i))$ *for all* $i = 1, \ldots, k$.

Proof. See [28, page 126] and [29, pages 142-146]. $\square$

Using this, we obtain the following result for the SCBDP:

Theorem 3.2.5. *Let* $\ell \in \mathbb{P}_{>2}$*. Then the set*

$$\{\mathrm{GL}_n(q),\ \mathrm{GU}_n(q),\ \mathrm{Sp}_{2n}(\tilde{q}),\ \mathrm{SO}_{2n+1}(\tilde{q}),\ \mathrm{SO}^+_{2n}(\tilde{q}),\ \mathrm{SO}^-_{2n}(\tilde{q}) \ : \ n \in \mathbb{N},\ q \text{ prime power},\ \tilde{q} \text{ odd prime power},\ \ell \nmid q \cdot \tilde{q}\}$$

has the SCBDP (and, thus, also the VBDP) with respect to every finite ℓ*-group.*

Proof. Let G be an arbitrary group from this set, and let D be a defect group of a block of $\overline{\mathbb{F}}_\ell G$. By Theorem 3.2.4 there exist $k, r_1, \ldots, r_k, n_1, \ldots, n_k \in \mathbb{N}$ such that $D \cong \bigtimes_{i=1}^{k}(C_{\ell^{r_i}} \wr X_{n_i})$, where $X_{n_i} \in \mathrm{Syl}_\ell(\mathrm{Sym}(n_i))$ for all i. We identify D with this direct product and assume that each $C_{\ell^{r_i}} \wr X_{n_i}$ is non-trivial (otherwise, we have the same situation for a smaller k). Let $V \leq D$ be a self-centralizing subgroup. Then we have

$$k = \sum_{i=1}^{k} 1 \leq \sum_{i=1}^{k} \mathrm{nrk}(C_{\ell^{r_i}} \wr X_{n_i}) = \mathrm{nrk}(D) \leq |V|^{|V|} \log_\ell |V|$$

by Theorem 2.1.5. Moreover, it is clear that for each i we have

$$\ell^{r_i} = |C_{\ell^{r_i}}| = |\,Z(C_{\ell^{r_i}})| \leq |\,Z(C_{\ell^{r_i}} \wr X_{n_i})| \leq |\,Z(D)| \leq |V|,$$

where the first inequality follows from Proposition 2.2.5. It remains to bound the n_i in terms of $|V|$. If $r_i = 0$, then $C_{\ell^{r_i}} \wr X_{n_i} \cong X_{n_i}$, and by part (b) of Proposition 2.3.6 it follows that

$$n_i \leq \mathrm{nrk}(X_{n_i})\ell + \ell - 1 = \mathrm{nrk}(C_{\ell^{r_i}} \wr X_{n_i})\ell + \ell - 1 \leq \mathrm{nrk}(D)\ell + \ell - 1 \leq (|V|^{|V|} \log_\ell |V|)\ell + \ell - 1.$$

Finally, if $r_i > 0$, then Proposition 2.2.5 implies

$$n_i = n_i \,\mathrm{nrk}(C_{\ell^{r_i}}) \leq \mathrm{nrk}(C_{\ell^{r_i}} \wr X_{n_i}) \leq \mathrm{nrk}(D) \leq |V|^{|V|} \log_\ell |V|.$$

$\square$

Corollary 3.2.6. *Let $\ell \in \mathbb{P}_{>2}$. The following sets of classical groups have the SCBDP (and, thus, also the VBDP) with respect to every finite ℓ-group:*

(a) *the sets*

$$\begin{gathered}\{\mathrm{PGL}_n(q),\ \mathrm{SL}_n(q)\ :\ n \in \mathbb{N},\ q \textit{ prime power},\ \ell \nmid q,\ \ell \nmid q-1\},\\ \{\mathrm{PSL}_n(q)\ :\ n \in \mathbb{N},\ q \textit{ prime power},\ \ell \nmid q,\ \ell \nmid \gcd(n, q-1)\},\\ \{\mathrm{PGU}_n(q),\ \mathrm{SU}_n(q)\ :\ n \in \mathbb{N},\ q \textit{ prime power},\ \ell \nmid q,\ \ell \nmid q+1\},\\ \{\mathrm{PSU}_n(q)\ :\ n \in \mathbb{N},\ q \textit{ prime power},\ \ell \nmid q,\ \ell \nmid \gcd(n, q+1)\};\end{gathered}$$

(b) *for fixed prime powers q satisfying $\ell \nmid q$, the set*

$$\{\mathrm{PGL}_n(q),\ \mathrm{PU}_n(q),\ \mathrm{SL}_n(q),\ \mathrm{SU}_n(q),\ \mathrm{PSL}_n(q),\ \mathrm{PSU}_n(q)\ :\ n \in \mathbb{N}\};$$

(c) *the set*

$$\{\mathrm{PSp}_{2n}(q)\ :\ n \in \mathbb{N},\ q \textit{ odd prime power},\ \ell \nmid q\};$$

(d) *the set*

$$\begin{aligned}\{&\mathrm{GO}_{2n+1}(q),\ \mathrm{GO}^+_{2n}(q),\ \mathrm{GO}^-_{2n}(q),\\ &\mathrm{PGO}_{2n+1}(q),\ \mathrm{PGO}^+_{2n}(q),\ \mathrm{PGO}^-_{2n}(q),\\ &\mathrm{PSO}^+_{2n}(q),\ \mathrm{PSO}^-_{2n}(q)\\ &\Omega_{2n+1}(q),\ \Omega^+_{2n}(q),\ \Omega^-_{2n}(q),\\ &\mathrm{P}\Omega^+_{2n}(q),\ \mathrm{P}\Omega^-_{2n}(q) \qquad : \ n \in \mathbb{N}_{>1},\ q \text{ odd prime power, } \ell \nmid q\}.\end{aligned}$$

Proof.

(a), (b) We have

$$|Z(\mathrm{GL}_n(q))| = q-1 = |\mathrm{GL}_n(q) : \mathrm{SL}_n(q)|,$$
$$|Z(\mathrm{GU}_n(q))| = q+1 = |\mathrm{GU}_n(q) : \mathrm{SU}_n(q)|,$$
$$|Z(\mathrm{SL}_n(q))| = \gcd(n, q-1),$$

and

$$|Z(\mathrm{SU}_n(q))| = \gcd(n, q+1).$$

Thus, the claim follows from Theorem 3.2.5 together with parts (a) and (b) of Proposition 3.1.15.

(c), (d) This is a consequence of Theorem 3.2.5 together with Proposition 3.1.15. □

Now, we also obtain the SCBSP for the following set of spin groups:

Corollary 3.2.7. *Let* $\ell \in \mathbb{P}_{>2}$. *The set*

$$\left\{\mathrm{Spin}_{2n+1}(q),\ \mathrm{Spin}^+_{2n}(q),\ \mathrm{Spin}^-_{2n}(q)\ :\ n \in \mathbb{N}_{>1},\ q \text{ odd prime power, } \ell \nmid q\right\}$$

has the SCBSP with respect to every finite ℓ*-group.*

Proof. The spin groups have a normal subgroup of order 2 such that the corresponding quotient group is the corresponding group Ω, see Remark 1.6.18. Thus, the claim follows from part (d) of Corollary 3.2.6 together with Observation 3.1.17 as the SCBDP implies the SCBSP. □

Using a result of Michel Broué, we can prove Theorem 3.2.4 for general linear groups also for the case $\ell = 2$ and $q \equiv 1 \bmod 4$:

Theorem 3.2.8. *The set*

$$\{\mathrm{GL}_n(q)\ :\ n \in \mathbb{N},\ q \text{ prime power},\ q \equiv 1 \bmod 4\}$$

has the SCBDP (and, thus, also the VBDP) with respect to every 2*-group.*

Proof. Let $n \in \mathbb{N}$, and let q be a prime power satisfying $q \equiv 1 \bmod 4$. If D is a defect group of some block of $\overline{\mathbb{F}}_\ell \, \mathrm{GL}_n(q)$, then by [9, Prop. 3.6] D is isomorphic to a direct product $\bigtimes_{i=1}^{k} D_i$ with $D_i \in \mathrm{Syl}_\ell(\mathrm{GL}_{n_i}(q_i))$ for some integers $n_1, \ldots, n_k \leq n$ and powers $q_1, \ldots, q_k$ of q. In particular, each q_i satisfies $q_i \equiv 1 \bmod 4$. Thus, each D_i is isomorphic to $C_{(q-1)_2} \wr S_i$, where $S_i \in \mathrm{Syl}_2(\mathrm{Sym}(n_i))$. Now, the proof is the same as for Theorem 3.2.5. $\square$

Finally, we state a result due to Dipper which considers the case $\ell \mid q$:

Theorem 3.2.9 ([20], [21])**.** *Let $\ell \in \mathbb{P}$, and let G be a Chevalley group or a twisted Chevalley group over a finite field of characteristic ℓ. Then the vertices of the simple non-projective $\overline{\mathbb{F}}_\ell G$-modules are the Sylow ℓ-subgroups of G.*

Corollary 3.2.10. *For every $\ell \in \mathbb{P}$, the set of all Chevalley groups and all twisted Chevalley groups over finite fields of characteristic ℓ has the VBDP with respect to every finite ℓ-group. In particular, this is also true for the subset of all simple classical groups over finite fields of characteristic ℓ.*

3.3 Results for the groups $G_2(q)$ and ${}^3D_4(q^3)$

Let q be a prime power. In this short section, we consider the Chevalley groups $G_2(q)$ and the twisted Chevalley groups ${}^3D_4(q^3)$ with respect to the SCBDP for $\ell > 2$, where the notation is as in Remark 1.6.19. The orders of these groups are

$$|G_2(q)| = q^6(q^6-1)(q^2-1)$$

and

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

see [49, page 208].

For $5 \leq \ell \nmid q$, the Sylow ℓ-subgroups of $\overline{\mathbb{F}}_\ell G_2(q)$ and $\overline{\mathbb{F}}_\ell {}^3D_4(q^3)$ are abelian, see [49]. In particular, the set

$$\left\{ G_2(q), {}^3D_4(q^3) \;:\; q \text{ primer power}, \ell \nmid q \right\}$$

has the SCBDP with respect to every finite ℓ-group if $\ell \geq 5$.

Now, we consider the case $\ell := 3 \nmid q$. Here, the defect groups of the blocks of $\overline{\mathbb{F}}_\ell G_2(q)$ and $\overline{\mathbb{F}}_\ell {}^3D_4(q^3)$ are abelian or Sylow 3-subgroups by [35, page 371] and [19, Prop. 5.4]. With our results from Section 2.7, we obtain the following:

Theorem 3.3.1. *Let q be a prime power not divisible by 3.*

(a) *The Sylow 3-subgroups of $G_2(q)$ have self-centralizing subgroups isomorphic to C_3^2.*

(b) *The Sylow* 3*-subgroups of* ${}^3\mathsf{D}_4(\mathsf{q}^3)$ *have self-centralizing subgroups isomorphic to* C_3^2 *or abelian self-centralizing subgroups of order* 27*.*

In particular, the sets

$$\{\mathsf{G}_2(\mathsf{q}) \;:\; \mathsf{q} \text{ prime power},\; 3 \nmid \mathsf{q}\}$$

and

$$\left\{{}^3\mathsf{D}_4(\mathsf{q}^3) \;:\; \mathsf{q} \text{ prime power},\; 3 \nmid \mathsf{q}\right\}$$

do not have the SCBSP and, thus, also not the SCBDP, with respect to every 3*-group.*

Proof.

(a) The group $\mathsf{G}_2(\mathsf{q})$ has subgroups isomorphic to $\mathrm{SL}_3(\mathsf{q})$ and $\mathrm{SU}_3(\mathsf{q})$ by [4, page 24]. Comparing orders, it follows that the Sylow 3-subgroups of $\mathsf{G}_2(\mathsf{q})$ are isomorphic to those of $\mathrm{SL}_3(\mathsf{q})$ if $\mathsf{q} \equiv 1 \bmod 3$, and isomorphic to those of $\mathrm{SU}_3(\mathsf{q})$ if $\mathsf{q} \equiv -1 \bmod 3$. Now, it follows from Theorem 2.7.12 and Corollary 2.6.6 that these Sylow 3-subgroups have self-centralizing subgroups of order 9.

(b) Let $\mathsf{G} \in \mathrm{Syl}_3({}^3\mathsf{D}_4(\mathsf{q}^3))$. By [44], ${}^3\mathsf{D}_4(\mathsf{q}^3)$ has a subgroup H isomorphic to $\mathsf{G}_2(\mathsf{q})$, and replacing G by a suitable conjugate yields $\mathsf{G} \cap \mathsf{H} \in \mathrm{Syl}_3(\mathsf{H})$. Comparing the orders of ${}^3\mathsf{D}_4(\mathsf{q}^3)$ and $\mathsf{G}_2(\mathsf{q})$ and considering the cases $\mathsf{q} \equiv 1 \bmod 3$ and $\mathsf{q} \equiv -1 \bmod 3$, we obtain

$$|\mathsf{G} : \mathsf{G} \cap \mathsf{H}| = \frac{|{}^3\mathsf{D}_4(\mathsf{q}^3)|_3}{|\mathsf{G}_2(\mathsf{q})|_3} = 3.$$

Now, the claim follows from part (a) and Proposition 2.5.8.

□

Unfortunately, it seems that the arguments used in the proof of Theorem 3.3.1 do not generalize to other Chevalley groups or twisted Chevalley groups.

4 On the vertices of the unipotent simple $\overline{\mathbb{F}}_\ell \operatorname{GL}_n(q)$-modules labeled by partitions $(n-1,1)$

In this chapter, we consider a particular simple module for $\operatorname{GL}_n(q)$. For $\ell \in \mathbb{P}_{>2}$, the vertices of this module are known to be the Sylow ℓ-subgroups of $\operatorname{GL}_n(q)$. For $\ell = n = 2$, we will determine the vertices in Theorem 4.2.1.

4.1 The module

Let $\ell \in \mathbb{P}$, let $n \in \mathbb{N}_{>1}$, and let q be a prime power such that $\ell \nmid q$. It is well known that the groups $\operatorname{GL}_n(q)$ and $\operatorname{SL}_n(q)$ act 2-transitively on the set of one-dimensional subspaces of $\mathbb{F}_q^n$. For both groups, the kernel of this action is the center of the corresponding group. The number of one-dimensional subspaces of $\mathbb{F}_q^n$ is given by $[n] := 1+q+\cdots+q^{n-1}$.

Let

$$G \in \{\operatorname{GL}_n(q), \operatorname{PGL}_n(q), \operatorname{SL}_n(q), \operatorname{PSL}_n(q)\}.$$

If $\omega_1, \dots, \omega_{[n]}$ denote the one-dimensional subspaces of $\mathbb{F}_q^n$, then we obtain a permutation $\overline{\mathbb{F}}_\ell G$-module $M = \langle \omega_1, \dots, \omega_{[n]} \rangle_{\overline{\mathbb{F}}_\ell}$.

Now, we consider $G := \operatorname{GL}_n(q)$. As M is a transitive permutation module, it is well known and easily verified that

$$U := \langle \omega_1 + \cdots + \omega_{[n]} \rangle_{\overline{\mathbb{F}}_\ell}$$

is the unique submodule of M that is isomorphic to the trivial module. Moreover, M has the submodule

$$S := \left\{ \sum_{i=1}^{[n]} a_i \omega_i \ : \ \sum_{i=1}^{[n]} a_i = 0 \right\},$$

which is the kernel of the augmentation map $M \to \overline{\mathbb{F}}_\ell$. For each fixed $i \in \{1, \dots, [n]\}$, the set $\{\omega_j - \omega_i \ : \ j \neq i\}$ is an $\overline{\mathbb{F}}_\ell$-basis of S.

With the notation from [41], the $\overline{\mathbb{F}}_\ell \operatorname{GL}_n(q)$-module M from above is the permutation module $M_{(n-1,1)}$ labeled by the partition $(n-1,1)$, and S is the corresponding module $S_{(n-1,1)}$, see [41, page 16, page 47]. As we will see, M has a unique non-trivial composition factor D, and with the notation from [41] this is the unipotent simple $\overline{\mathbb{F}}_\ell \operatorname{GL}_n(q)$-module $D_{(n-1,1)}$ that can be seen to be the analogue of the simple $\overline{\mathbb{F}}_\ell \operatorname{Sym}(n)$-module labeled by the partition $(n-1,1)$. For the latter, the vertices are known by work of Jürgen Müller and René Zimmermann, see [51]. In this chapter, we investigate the vertices of the simple $\overline{\mathbb{F}}_\ell\,\mathrm{GL}_n(q)$-module D.

We have two cases:

- If $\ell \nmid [n]$, then $U \not\subseteq S$, and it follows that $M = U \oplus S$. As U is the unique submodule of M that is isomorphic to the trivial module, the module S must be simple by [41, (11.12)(iii), Thm. 16.3, Thm. 20.7], so S is the unique non-trivial composition factor of M. Moreover, by [26, Lem. 2.6], the vertices of S are the Sylow ℓ-subgroups of the group $L_{(n-1,1)} = \mathrm{GL}_{n-1}(q) \times \mathrm{GL}_1(q)$. Via the embedding $L_{(n-1,1)} \hookrightarrow \mathrm{GL}_n(q)$ from part (a) of Lemma 2.5.1, the order formula $|\,\mathrm{GL}_n(q)| = q^{n(n-1)/2}\prod_{j=1}^{n}(q^j - 1)$ implies
$$|\,\mathrm{GL}_n(q) : L_{(n-1,1)}|_\ell = \frac{(q^n-1)_\ell}{(q-1)_\ell} = [n]_\ell = 1.$$
Therefore, the vertices of S must be the Sylow ℓ-subgroups of $\mathrm{GL}_n(q)$.
- If $\ell \mid [n]$, then $U \subseteq S$, and the quotient module $D := S/U$ is simple by [41, (11.12)(iii), Thm. 16.3, Thm. 20.7]. Thus, $\{0\} \subseteq U \subseteq S \subseteq M$ is a composition series for M and D is the unique non-trivial composition factor. As the trivial module U occurs in S and as S/U is simple, we have that D lies in the principal block of $\overline{\mathbb{F}}_\ell\,\mathrm{GL}_n(q)$. Clearly, here the same results hold if we replace $\mathrm{GL}_n(q)$ by $\mathrm{PGL}_n(q)$.
If $\ell > 2$, then $\ell \nmid [n] - 2 = \dim_{\overline{\mathbb{F}}_\ell}(D)$. Therefore, by part (d) of Proposition 1.2.4, we have $\mathrm{Vx}(D) = \mathrm{Syl}_\ell(G)$ for both $G = \mathrm{GL}_n(q)$ and $G = \mathrm{PGL}_n(q)$.

It remains to determine the vertices of D for $\ell = 2 \mid [n]$. It follows immediately from the definition of $[n]$ that n must be even in this case. The aim of this chapter is to provide the vertices of D for $\ell = 2$ and $n = 2$. We state our result in Theorem 4.2.1.

For arbitrary $n \in \mathbb{N}_{>0}$, it is well known and easily verified that the map
$$\mathrm{PSL}_n(q) \to \mathrm{PGL}_n(q) : A\,\mathrm{Z}(\mathrm{SL}_n(q)) \mapsto A\,\mathrm{Z}(\mathrm{GL}_n(q))$$
is a (well-defined) group monomorphism whose image is a normal subgroup in $\mathrm{PGL}_n(q)$ of index $\gcd(n, q-1)$. In what follows, we will identify $\mathrm{PSL}_2(q)$ with its image in $\mathrm{PGL}_2(q)$ under this group monomorphism. Thus, $\mathrm{PSL}_2(q)$ is a normal subgroup of $\mathrm{PGL}_2(q)$ of index 2.

We need the following lemmas:

Lemma 4.1.1. *Let q be a prime power, and let $U \leq \mathrm{SL}_2(q)$ be a 2-subgroup containing $Z := \mathrm{Z}(\mathrm{SL}_2(q))_2 = \{\pm \mathbb{1}_2\}$ such that $U/Z \leq \mathrm{PSL}_2(q)$ is isomorphic to the Klein four-group. Then U is isomorphic to the quaternion group of order 8.*

Proof. As Z has order 2 and C_2^2 has order 4, it is clear that U has order 8. It is well known that $-\mathbb{1}_2$ is the unique element of order 2 in $\mathrm{SL}_2(q)$, so $-\mathbb{1}_2$ is also the unique element of order 2 in U. Moreover, U is not cyclic, since otherwise U/Z would be cyclic of order 4. Thus, U is a non-cyclic group of order 8 which has a unique element of order 2. By the classification of groups of order 8 (see, for example, [37, Satz I.14.10(a)]), it follows that U is isomorphic to the quaternion group. □

Lemma 4.1.2. *Let G be a finite group, let $\ell \in \mathbb{P}$, and let N be a subgroup of $Z(G)$.*

(a) *Let D be a simple $\overline{\mathbb{F}}_\ell[G/N]$-module. Then $\tilde{D} := \mathrm{Inf}_{G/N}^{G}(D)$ is a simple KG-module, and we have $V/N_\ell \cong VN/N \in \mathrm{Vx}(D)$ for all $V \in \mathrm{Vx}(\tilde{D})$. In particular, $\mathrm{Vx}(D) = \mathrm{Syl}_\ell(G/N)$ if and only if $\mathrm{Vx}(\tilde{D}) = \mathrm{Syl}_\ell(G)$.*

(b) *Let $\tilde{D}$ be a composition factor of a transitive permutation $\overline{\mathbb{F}}_\ell G$-module M such that N is contained in the corresponding stabilizer subgroups, and let $V \in \mathrm{Vx}(\tilde{D})$. Then there exists a simple $\overline{\mathbb{F}}_\ell[G/N]$-module D such that $\tilde{D} = \mathrm{Inf}_{G/N}^{G}(D)$ and $V/N_\ell \cong VN/N \in \mathrm{Vx}(D)$.*

Proof.

(a) It follows immediately from [46, Prop. 2.1] that $VN/N \in \mathrm{Vx}(D)$. Moreover, by part (d) of Proposition 1.2.6 we have $N_\ell \subseteq V$, and Lagrange's Theorem from group theory implies $N_{\ell'} \cap V = \{1\}$. Thus, $VN/N \cong V/(V \cap N) = V/N_\ell$.

(b) Let M be a transitive permutation module such that $\tilde{D}$ is a composition factor of M. Then $M \cong \mathrm{Ind}_H^G(\overline{\mathbb{F}}_\ell)$ for some subgroup $H \leq G$, where $\overline{\mathbb{F}}_\ell$ is the trivial $\overline{\mathbb{F}}_\ell H$-module. By Mackey's Theorem 1.1.3, the $\overline{\mathbb{F}}_\ell N$-module $\mathrm{Res}_N^G(M)$ is isomorphic to

$$\bigoplus_{g \in [N\backslash G/H]} \mathrm{Ind}_{{}^gH \cap N}^{N}(\mathrm{Res}_{{}^gH \cap N}^{{}^gH}({}^g\overline{\mathbb{F}}_\ell)) = \bigoplus_{g \in [N\backslash G/H]} \overline{\mathbb{F}}_\ell,$$

since $H \leq N \leq Z(G)$, so N acts trivially on M and, thus, also on $\tilde{D}$. Therefore, $N \subseteq \ker(\tilde{D})$ and $\tilde{D} = \mathrm{Inf}_{G/N}^{G}(D)$ for some simple $\overline{\mathbb{F}}_\ell[G/N]$-module D. Now, the claim follows from part (a). □

We will use the following facts from the literature:

Theorem 4.1.3.

(a) *The $\overline{\mathbb{F}}_2\,\mathrm{PGL}_2(q)$-module D is, up to isomorphism, the unique non-trivial simple module lying in the principal block of $\overline{\mathbb{F}}_2\,\mathrm{PGL}_2(q)$.*

(b) *As an $\overline{\mathbb{F}}_2\,\mathrm{PSL}_2(q)$-module, D is the direct sum of two non-trivial simple modules S_1 and S_2 both of which have dimension $\frac{q-1}{2}$. If $q \equiv 1 \bmod 4$, then the vertices of S_1 and S_2 are Klein four-groups. If $q \equiv 3 \bmod 4$, then the vertices of S_1 and S_2 are the Sylow 2-subgroups of $\mathrm{PSL}_2(q)$.*

Proof.

(a) By [31, Thm 5.1] (see also the proof of [30, Prop. 2.4]), the principal block of $\overline{\mathbb{F}}_2 \,\mathrm{PGL}_2(\mathsf{q})$ has a unique non-trivial simple module up to isomorphism. By our considerations above, D is such a module.

(b) The description of the conjugacy classes of $\mathrm{SL}_2(\mathsf{q})$ in [22, Thm. 38.1] shows that the elements of order 4 in $\mathrm{SL}_2(\mathsf{q})$ form a single conjugacy class (as either $\mathsf{q}-1$ is divisible by 4 or $\mathsf{q}+1$ is). Therefore, in $\mathrm{PSL}_2(\mathsf{q})$, any two involutions are conjugate. Moreover, we have seen in Theorem 2.5.7 that the Sylow 2-subgroups of $\mathrm{PSL}_2(\mathsf{q})$ are dihedral. Thus, [8, Section VII, Case I] implies that the principal block of $\mathrm{PSL}_2(\mathsf{q})$ has exactly two non-trivial simple modules S_1 and S_2 up to isomorphism.
Now, [25, page 666, Lem. 4.3, Cor. 5.2] shows that both have dimension $\frac{\mathsf{q}-1}{2}$.

Finally, Clifford's Theorem [52, Thm. 3.3.1] implies that there exists some $\mathsf{g} \in \mathrm{PGL}_2(\mathsf{q}) \setminus \mathrm{PSL}_2(\mathsf{q})$ such that ${}^{\mathsf{g}}\mathsf{S}_1 = \mathsf{S}_2$ and $\mathrm{Res}^{\mathrm{PGL}_2(\mathsf{q})}_{\mathrm{PSL}_2(\mathsf{q})}(\mathsf{D}) = \mathsf{S}_1 \oplus \mathsf{S}_2$. The assertion about the vertices of S_1 and S_2 follows from [25, Thm. 1, Thm. 3]. □

From these facts, we can deduce the following:

Corollary 4.1.4.

(a) *As an* $\overline{\mathbb{F}}_2 \,\mathrm{PGL}_2(\mathsf{q})$*-module,* D *is relatively* $\mathrm{PSL}_2(\mathsf{q})$*-projective, and the vertices of* D *are Klein four-groups* C_2^2 *if* $\mathsf{q} \equiv 1 \bmod 4$*, and Sylow* 2*-subgroups of* $\mathrm{PSL}_2(\mathsf{q})$ *for* $\mathsf{q} \equiv 3 \bmod 4$*.*

(b) *As an* $\overline{\mathbb{F}}_2 \,\mathrm{SL}_2(\mathsf{q})$*-module,* D *is the direct sum of the inflations of the two modules* S_1 *and* S_2 *from part (a). The vertices of these inflations are quaternion groups of order* 8 *if* $\mathsf{q} \equiv 1 \bmod 4$*, and Sylow* 2*-subgroups of* $\mathrm{SL}_2(\mathsf{q})$ *if* $\mathsf{q} \equiv 3 \bmod 4$*.*

(c) *As an* $\overline{\mathbb{F}}_2 \,\mathrm{GL}_2(\mathsf{q})$*-module, the vertices of* D *have order* $4(\mathsf{q}-1)_2$ *if* $\mathsf{q} \equiv 1 \bmod 4$*, and order* $2(\mathsf{q}+1)_2$ *if* $\mathsf{q} \equiv 3 \bmod 4$*.*

Proof.

(a) By part (b) of Theorem 4.1.3, the inertia group I of the module S_1 is strictly contained in $\mathrm{PGL}_2(\mathsf{q})$, and so it follows from $|\mathrm{PGL}_2(\mathsf{q}) : \mathrm{PSL}_2(\mathsf{q})| = 2$ that $\mathrm{I} = \mathrm{PSL}_2(\mathsf{q})$. By Clifford's Theorem [52, Thm. 3.3.1], we thus have $\mathsf{D} = \mathrm{Ind}^{\mathrm{PGL}_2(\mathsf{q})}_{\mathrm{PSL}_2(\mathsf{q})}(\mathsf{S}_1)$. In particular, D is relatively $\mathrm{PSL}_2(\mathsf{q})$-projective. Now, the assertion about the vertices follows immediately from Proposition 1.2.6.

(b) This follows immediately from parts (b) and (c) of Theorem 4.1.3 together with Lemma 4.1.1 and Lemma 4.1.2.

(c) This follows immediately from part (c) of Theorem 4.1.3 together with Lemma 4.1.2.

□

4.2 The theorem

For the remainder of this chapter, we keep the following notation:

We fix an odd prime power q and an element $c \in O_2(\mathbb{F}_q^\times)$ of order $(q-1)_2$. Then $\langle c\mathbb{1}_2 \rangle = O_2(Z(\operatorname{GL}_2(q)))$. Moreover, we write

$$A := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \operatorname{GL}_2(q)$$

and

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \operatorname{GL}_2(q).$$

Then

$$\langle A, B \rangle = \{\pm\mathbb{1}_2, \pm A, \pm B, \pm AB\} \cong \operatorname{Dih}_8 .$$

We also define $V := \langle c\mathbb{1}_2, A, B \rangle$. As $\langle c\mathbb{1}_2 \rangle$ is normal in V, we have $V = \langle c\mathbb{1}_2 \rangle \langle A, B \rangle$, so $\langle c\mathbb{1}_2 \rangle \cap \langle A, B \rangle = \{\pm\mathbb{1}_2\}$ implies $|V| = 4(q-1)_2$.

With the notation from [32, Thm. 5.3], V is a central product of $\langle c\mathbb{1}_2 \rangle \cong O_2(\mathbb{F}_q^\times)$ and $\langle A, B \rangle \cong \operatorname{Dih}_8$ with respect to $\{\pm\mathbb{1}_2\} \cong C_2$.

It is clear that if $q \equiv 3 \bmod 4$, then $c = -1$ and therefore $V = \langle A, B \rangle \cong \operatorname{Dih}_8$.

The main result of this chapter is the following theorem which we did not find in the literature.

Theorem 4.2.1.

(a) *If* $q \equiv 1 \bmod 4$*, then the vertices of the* $\overline{\mathbb{F}}_2 \operatorname{GL}_2(q)$*-module* D *are conjugate to* V*. In particular,* D *is then not relatively* $\operatorname{SL}_2(q)$*-projective.*

(b) *If* $q \equiv 3 \bmod 4$*, then the vertices of the* $\overline{\mathbb{F}}_2 \operatorname{GL}_2(q)$*-module* D *are the Sylow* 2*-subgroups of* $\operatorname{SL}_2(q)$ *(and, therefore, generalized quaternion by Theorem 2.5.7). In particular,* D *is then relatively* $\operatorname{SL}_2(q)$*-projective.*

Remark 4.2.2. We observe that Theorem 4.2.1 fits together with Theorem 2.5.10: If $q \equiv 1 \bmod 4$, then the vertices of the $\overline{\mathbb{F}}_2 \operatorname{GL}_2(q)$-module D are conjugate to V, and we have

$$|\operatorname{GL}_2(q)|_2 = (q-1)_2(q^2-1)_2 = 2(q-1)_2^2 < 16(q-1)_2^2 = |V|^2,$$

which gives a much better bound for this particular self-centralizing subgroup V of a Sylow 2-subgroup of $\mathrm{GL}_2(q)$ than the bound from part (a) of Theorem 2.5.10.
If $q \equiv 3 \mod 4$, then the vertices of the $\overline{\mathbb{F}}_2 \mathrm{GL}_2(q)$-module D are the Sylow 2-subgroups of $\mathrm{SL}_2(q)$, and

$$|\mathrm{GL}_2(q)|_2 = (q-1)_2 |\mathrm{SL}_2(q)|_2 = 2|\mathrm{SL}_2(q)|_2 < |\mathrm{SL}_2(q)|_2^2.$$

Thus, the vertices of D do not occur among the self-centralizing subgroups of order 4 stated in part (b) of Theorem 2.5.10.

4.3 The proof

To prove Theorem 4.2.1, we will apply a method known as ***Brauer construction***:

Let $\ell \in \mathbb{P}$, let G be a finite group, and let $Q \leq G$ be an ℓ-subgroup. Let D be an $\overline{\mathbb{F}}_\ell G$-module, let

$$D^Q := \{m \in D \ : \ gm = m \ \forall \ g \in Q\},$$

and for a subgroup P of Q let

$$\mathrm{Tr}_P^Q : D^P \to D^Q : m \mapsto \sum_{g \in [Q/P]} gm,$$

where $[Q/P]$ denotes a set of representatives for Q/P.

Theorem 4.3.1 ([10, page 403, (1.3)]). *If* $D^Q / \sum_{P<Q} \mathrm{Tr}_P^Q(D^P) \neq 0$*, then* Q *is contained in some vertex of* D*.*

Here, it is actually enough to only consider the maximal subgroups of Q: If $R \leq P \leq Q$ are given and if S is a set of representatives for P/R and T is a set of representatives for Q/P, then $S \cdot T$ is a set of representatives for Q/R. Thus, we have $\mathrm{Tr}_R^Q = \mathrm{Tr}_P^Q \circ \mathrm{Tr}_R^P$. It follows that with $\mathrm{Tr}^Q(D) := \sum_{P<Q \text{ maximal}} \mathrm{Tr}_P^Q(D^P)$, we have:

If $D^Q / \mathrm{Tr}^Q(D) \neq 0$*, then* Q *is contained in some vertex of* D*.*

The converse of Theorem 4.3.1 is not true, in general. The idea of our proof here is to determine all maximal subgroups of the 2-groups stated in Theorem 4.2.1, and then to apply Theorem 4.3.1 for these maximal subgroups. As we already know the order of the vertices of the $\overline{\mathbb{F}}_2 \mathrm{GL}_2(q)$-module D by part (c) of Corollary 4.1.4, this will suffice.

In order to determine the maximal subgroups of the 2-groups of our interest, we will use the following lemma, which is probably well known. For the reader's convenience, we also provide a proof.

Lemma 4.3.2. *Let G be a finite ℓ-group, and let M be a minimal generating set of G. Then G has exactly $1+\ell+\ell^2+\cdots+\ell^{|M|-1}$ maximal subgroups.*

Proof. The maximal subgroups of G correspond bijectively to the maximal subgroups of $G/\Phi(G)$, where $\Phi(G)$ is the Frattini subgroup of G. As the cardinality of M is the dimension of the $\mathbb{F}_\ell$-vector space $G/\Phi(G)$ by Burnside's Basis Theorem [37, Thm. III.3.15], and the maximal subgroups of $G/\Phi(G)$ are exactly the subspaces of $G/\Phi(G)$ of dimension $(\dim_{\mathbb{F}_\ell}(G/\Phi(G))-1)$, the claim follows. □

For an arbitrary field K, a set of representatives for the one-dimensional subspaces of K^2 is $\{(0,1)^t,(1,x)^t \;:\; x\in K\}$.

For the remainder of this chapter, we write

$$\omega_x := \langle (1,x)^t\rangle_{\mathbb{F}_q} \quad \text{for} \quad x\in\mathbb{F}_q,$$

and

$$\omega := \langle (0,1)^t\rangle_{\mathbb{F}_q}.$$

Moreover, we define

$$\delta_x := (\omega_x+\omega)+U \quad \text{for} \quad x\in\mathbb{F}_q,$$

where U is the module from Section 4.1. Then the set $\{\delta_x \;:\; x\in\mathbb{F}_q^\times\}$ has cardinality $q-1=\dim_{\overline{\mathbb{F}}_2}(D)$ and generates D, as the sum of its elements is δ_0. Therefore, $\{\delta_x \;:\; x\in\mathbb{F}_q^\times\}$ is an $\overline{\mathbb{F}}_2$-basis of D.

Before we distinguish the two cases $q\equiv 1$ mod 4, and $q\equiv 3$ mod 4, we will prove the following lemma which will be applied in both cases later on.

Lemma 4.3.3. *Let $x\in\mathbb{F}_q$.*

(a) *We have $A\cdot\delta_x=\delta_{-x}$.*

(b) *If $x\neq 0$, then $B\cdot\delta_x=\delta_{x^{-1}}+\delta_0$. Moreover, $B\cdot\delta_0=\delta_0$.*

In particular, both $\delta_1+\delta_{-1}$ and δ_0 belong to D^V.

Proof.

(a) We have

$$A\cdot\omega_x = A\cdot\langle\left(\begin{smallmatrix}1\\x\end{smallmatrix}\right)\rangle_{\mathbb{F}_q} = \left\langle\left(\begin{smallmatrix}1\\-x\end{smallmatrix}\right)\right\rangle_{\mathbb{F}_q} = \omega_{-x}$$

and

$$A\cdot\omega = A\cdot\left\langle\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\right\rangle_{\mathbb{F}_q} = \left\langle\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\right\rangle_{\mathbb{F}_q} = \omega.$$

It follows that

$$A\cdot\delta_x = A\cdot(\omega_x+\omega)+U = (A\cdot\omega_x+A\cdot\omega)+U = (\omega_{-x}+\omega)+U = \delta_{-x}.$$

(b) If $x \neq 0$, then

$$B \cdot \omega_x = B \cdot \langle \left(\begin{smallmatrix} 1 \\ x \end{smallmatrix}\right) \rangle_{\mathbb{F}_q} = \langle \left(\begin{smallmatrix} x \\ 1 \end{smallmatrix}\right) \rangle_{\mathbb{F}_q} = \left\langle \left(\begin{smallmatrix} 1 \\ x^{-1} \end{smallmatrix}\right) \right\rangle_{\mathbb{F}_q} = \omega_{x^{-1}},$$

and moreover,

$$B \cdot \omega = B \cdot \left\langle \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \right\rangle_{\mathbb{F}_q} = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \right\rangle_{\mathbb{F}_q} = \omega_0.$$

As B has order 2, it follows that also $B \cdot \omega_0 = \omega$. Thus, we have

$$\begin{aligned} B \cdot \delta_x = B \cdot (\omega_x + \omega) + U &= (B \cdot \omega_x + B \cdot \omega) + U = (\omega_{x^{-1}} + \omega_0) + U \\ &= (\omega_{x^{-1}} + \omega_0 + 2\omega) + U = \delta_{x^{-1}} + \delta_0 \end{aligned}$$

for $x \neq 0$, and finally,

$$B \cdot \delta_0 = B \cdot (\omega_0 + \omega) + U = (B \cdot \omega_0 + B \cdot \omega) + U = (\omega + \omega_0) + U = \delta_0.$$

□

4.3.1 The case $q \equiv 1 \bmod 4$

First, we consider the case $q \equiv 1 \bmod 4$.

Lemma 4.3.4. *The group V has precisely seven maximal subgroups. They are given by $\langle c^2\mathbb{1}_2, A, B\rangle$, $\langle c\mathbb{1}_2, A\rangle$, $\langle c\mathbb{1}_2, B\rangle$, $\langle c\mathbb{1}_2, AB\rangle$, $\langle A, cB\rangle$, $\langle cA, B\rangle$, and $\langle cA, cB\rangle$.*

Proof. It is clear that $\{c\mathbb{1}_2, A, B\}$ is a minimal generating set for V, so it follows from Lemma 4.3.2 that V has precisely $1 + 2 + 2^2 = 7$ maximal subgroups. From $\langle c^2\mathbb{1}_2, A, B\rangle = \langle c^2\mathbb{1}_2\rangle \langle A, B\rangle$ and $\langle c^2\mathbb{1}_2\rangle \cap \langle A, B\rangle = \{\pm\mathbb{1}_2\}$ it follows that $\langle c^2\mathbb{1}_2, A, B\rangle$ has order $2(q-1)_2$.

Moreover, for $Z \in \{A, B, AB\}$ we have $\langle c\mathbb{1}_2, Z\rangle = \langle c\mathbb{1}_2\rangle \langle Z\rangle$, so it follows from $\langle c\mathbb{1}_2\rangle \cap \langle A\rangle = \{\mathbb{1}_2\}$, $\langle c\mathbb{1}_2\rangle \cap \langle B\rangle = \{\mathbb{1}_2\}$, and $\langle c\mathbb{1}_2\rangle \cap \langle AB\rangle = \{\pm\mathbb{1}_2\}$ that the three subgroups $\langle c\mathbb{1}_2, A\rangle$, $\langle c\mathbb{1}_2, B\rangle$, and $\langle c\mathbb{1}_2, AB\rangle$ have order $2(q-1)_2$.

Next, consider the subgroups $\langle A, cB\rangle$ and $\langle cA, B\rangle$. The equation $(cB)^{(q-1)_2/2} = -\mathbb{1}_2$ implies that $A(cB)A^{-1} = -cB \in \langle cB\rangle$, so $\langle cB\rangle$ is normal in $\langle A, cB\rangle$. As A has order 2, the quotient group $\langle A, cB\rangle / \langle cB\rangle$ has only two elements. Thus, $|\langle A, cB\rangle| = 2|\langle cB\rangle| = 2\operatorname{ord}(cB) = 2\operatorname{ord}(c) = 2(q-1)_2$.
Similarly, we have $(cA)^{(q-1)_2/2} = -\mathbb{1}_2$, so $B(cA)B^{-1} = -cA \in \langle cA\rangle$ shows that $\langle cA\rangle$ is normal in $\langle cA, B\rangle$. As B has order 2, the quotient group $\langle cA, B\rangle / \langle cA\rangle$ has only two elements, so we have $|\langle cA, B\rangle| = 2|\langle cA\rangle| = 2\operatorname{ord}(cA) = 2\operatorname{ord}(c) = 2(q-1)_2$.

It remains to consider the subgroup $\langle cA, cB\rangle$. We have $(cA)^{(q-1)_2/2} = -\mathbb{1}_2$, so $(cB)(cA)(cB)^{-1} = -cA \in \langle cA\rangle$. Thus, $\langle cA\rangle$ is normal in $\langle cA, cB\rangle$. As $(cB)^2 = c^2\mathbb{1}_2 = (cA)^2 \in \langle cA\rangle$, the quotient group $\langle cA, cB\rangle / \langle cA\rangle$ has only two elements. It follows that $|\langle cA, cB\rangle| = 2|\langle cA\rangle| = 2\operatorname{ord}(cA) = 2\operatorname{ord}(c) = 2(q-1)_2$. □

Lemma 4.3.5. *Let P be a maximal subgroup of V, and let $\nu = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x \in D^P$. Then $\lambda_1 = \lambda_{-1}$ and $\sum_{x\in\mathbb{F}_q^\times} \lambda_x = 0$.*

Proof. Note that since $\nu \in D^P$, we have $\nu = A\nu$ or $\nu = B\nu$ or $\nu = AB\nu$.

First case: $\nu = A\nu$.

Then

$$\sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_{-x},$$

and comparing the coefficients at δ_x on both sides yields $\lambda_x = \lambda_{-x}$ for all $x \in \mathbb{F}_q^\times$. In particular, $\lambda_1 = \lambda_{-1}$.

Moreover, we have an equivalence relation on $\mathbb{F}_q^\times$ defined by

$$x \sim y \;:\Longleftrightarrow\; x \in \{y, -y\}.$$

If R denotes a set of representatives, then

$$\sum_{x\in\mathbb{F}_q^\times} \lambda_x = \sum_{x\in R} \underbrace{\lambda_x + \lambda_{-x}}_{=0} = 0.$$

Second case: $\nu = B\nu$.

Then

$$\sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_{x^{-1}} + \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_0.$$

Comparing the coefficients at δ_1 on both sides yields $\lambda_1 = \lambda_1 + \sum_{x\in\mathbb{F}_q^\times} \lambda_x$, so $\sum_{x\in\mathbb{F}_q^\times} \lambda_x = 0$. Now, comparing the coefficients at δ_x for $x \notin \{1, -1\}$ shows that $\lambda_x = \lambda_{x^{-1}}$ for all those x. As

$$x \sim y \;:\Longleftrightarrow\; x \in \left\{y, y^{-1}\right\}$$

defines an equivalence relation on $\mathbb{F}_q^\times \setminus \{1, -1\}$, we have

$$0 = \sum_{x\in\mathbb{F}_q^\times} \lambda_x = \lambda_1 + \lambda_{-1} + \sum_{x\in R} \underbrace{\lambda_x + \lambda_{x^{-1}}}_{=0} = \lambda_1 + \lambda_{-1},$$

where R denotes a set of representatives.

Third case: $\nu = AB\nu$.

Then

$$\sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_{-x^{-1}} + \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_0.$$

Since $q \equiv 1 \bmod 4$, there exists an element $y \in \mathbb{F}_q^\times$ of order 4. It follows that $y = -y^{-1}$, and comparing the coefficients at δ_y implies $\sum_{x\in\mathbb{F}_q^\times} \lambda_x = 0$. Now, comparing all coefficients, we get $\lambda_x = \lambda_{-x^{-1}}$ for all $x \in \mathbb{F}_q^\times$. In particular, $\lambda_1 = \lambda_{-1}$.

□

Lemma 4.3.6. *Let P be a maximal subgroup of V, and let $\nu \in \mathsf{D}^{\mathsf{P}}$. Then the coefficient of $\mathrm{Tr}_{\mathsf{P}}^{\mathsf{V}}(\nu) \in \mathsf{D}^{\mathsf{V}}$ at δ_1 is zero. In particular, both $\delta_1+\delta_{-1}$ and δ_0 do not belong to $\mathrm{Tr}^{\mathsf{V}}(\mathsf{D})$.*

Proof. We write $\nu = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x$. By Lemma 4.3.5, we have $\lambda_1 = \lambda_{-1}$ and $\sum_{x\in\mathbb{F}_q^\times} \lambda_x = 0$.

<u>First case: $A, B \in P$.</u>
It follows that $c\mathbb{1}_2 \notin P$, and the the claim is trivially true since then $\mathrm{Tr}_{\mathsf{P}}^{\mathsf{V}}(\nu) = \nu + c\mathbb{1}_2\nu = \nu+\nu = 0$.

<u>Second case: $A \notin P$.</u>
Then

$$\begin{aligned}
\mathrm{Tr}_{\mathsf{P}}^{\mathsf{V}}(\nu) &= \nu + A\nu \\
&= \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x + \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_{-x} \\
&= \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x + \sum_{x\in\mathbb{F}_q^\times} \lambda_{-x}\delta_x,
\end{aligned}$$

and the claim follows since $\lambda_1 = \lambda_{-1}$.

<u>Third case: $B \notin P$.</u>
Then

$$\begin{aligned}
\mathrm{Tr}_{\mathsf{P}}^{\mathsf{V}}(\nu) &= \nu + B\nu \\
&= \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x + \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_{x^{-1}} + \underbrace{\sum_{x\in\mathbb{F}_q^\times} \lambda_x}_{=0}\,\delta_0 \\
&= \sum_{x\in\mathbb{F}_q^\times} (\lambda_x + \lambda_{x^{-1}})\delta_x,
\end{aligned}$$

and the claim follows.

□

We are, now, in position to prove part (a) of Theorem 4.2.1:

Proof of part (a) of Theorem 4.2.1. By Lemma 4.3.3 and Lemma 4.3.6, the vectors $\delta_1 + \delta_{-1}$ and δ_0 belong to $\mathsf{D}^{\mathsf{V}} \setminus \mathrm{Tr}^{\mathsf{V}}(\mathsf{D})$. Thus, V is contained in some vertex of D. As the vertices have order $4(q-1)_2 = |\mathsf{V}|$, this proves part (a) of Theorem 4.2.1. □

4.3.2 The case $q \equiv 3 \bmod 4$

Now, we consider the case $q \equiv 3 \bmod 4$.

Let $\alpha \in \mathbb{F}_{q^2}^\times$ be such that $\operatorname{ord}(\alpha) = (q^2-1)_2 = 2(q+1)_2$. Then $\operatorname{Tr}_{\mathbb{F}_{q^2}|\mathbb{F}_q}(\alpha) = \alpha+\alpha^q \in \mathbb{F}_q$. We write

$$X := \begin{pmatrix} 0 & 1 \\ 1 & \alpha+\alpha^q \end{pmatrix} \qquad \text{and} \qquad Y := AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then X is the matrix of the $\mathbb{F}_q$-linear map $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2} : x \mapsto \alpha x$ with respect to the $\mathbb{F}_q$-basis $\{1, \alpha\}$. By [13, page 142], the semidihedral group $\langle X, Y\rangle$ of order $4(q+1)_2$ is a Sylow 2-subgroup of $\operatorname{GL}_2(q)$ (as we have already seen in part (b) Theorem 2.5.7).

Lemma 4.3.7. *For all* $k \in \mathbb{N}$, *we have*

$$X^k = \frac{1}{\alpha^q - \alpha}\begin{pmatrix} \alpha^{q+k} - \alpha^{qk+1} & \alpha^{qk} - \alpha^k \\ \alpha^{qk} - \alpha^k & \alpha^{q(k+1)} - \alpha^{k+1} \end{pmatrix}.$$

Proof. This follows immediately by induction: The claim is clearly true for $k = 0$, and moreover,

$$\begin{aligned} &\begin{pmatrix} \alpha^{q+k} - \alpha^{qk+1} & \alpha^{qk} - \alpha^k \\ \alpha^{qk} - \alpha^k & \alpha^{q(k+1)} - \alpha^{k+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & \alpha+\alpha^q \end{pmatrix} \\ = &\begin{pmatrix} \alpha^{qk} - \alpha^k & \alpha^{q(k+1)} - \alpha^{k+1} \\ \alpha^{q(k+1)} - \alpha^{k+1} & \alpha^{qk} - \alpha^k + \alpha^{qk+q+1} - \alpha^{k+2} + \alpha^{q(k+2)} - \alpha^{k+q+1} \end{pmatrix} \\ = &\begin{pmatrix} \alpha^{q+k+1} - \alpha^{q(k+1)+1} & \alpha^{q(k+1)} - \alpha^{k+1} \\ \alpha^{q(k+1)} - \alpha^{k+1} & \alpha^{q(k+2)} - \alpha^{k+2} \end{pmatrix}, \end{aligned}$$

where the last equality holds since $\alpha^{q+1} = -1$. $\square$

Since $\operatorname{ord}(X) = \operatorname{ord}(\alpha) = 2(q+1)_2 \geq 8$ and $\det(X) = -1$, we have that $X^{(q+1)_2} \in \operatorname{SL}_2(q)$ is an involution. It is well known that the only involution in $\operatorname{SL}_2(q)$ is $-\mathbb{1}_2$, so $X^{(q+1)_2/2}$ satisfies $(X^{(q+1)_2/2})^2 = -\mathbb{1}_2$. As the matrix $X^{(q+1)_2/2}$ is symmetric, we may write

$$X^{(q+1)_2/2} = \begin{pmatrix} a & b \\ b & d \end{pmatrix},$$

and from $(X^{(q+1)_2/2})^2 = -\mathbb{1}_2$ it follows that $a^2 + b^2 = -1$ and $d = -a$.
Moreover, the group $\left\langle X^{(q+1)_2/2}, Y\right\rangle$ is isomorphic to the quaternion group of order 8. The maximal subgroups of $\left\langle X^{(q+1)_2/2}, Y\right\rangle$ are, thus, given by $\left\langle X^{(q+1)_2/2}\right\rangle$, $\langle Y\rangle$, and $\left\langle X^{(q+1)_2/2}Y\right\rangle$.

Remark 4.3.8. Note that we can also compute a and b explicitly in terms of α: For $k := (q+1)_2/2$, we have $\alpha^{qk+k} = (\alpha^{q+1})^k = (-1)^k = 1$ and $\alpha^{2k} = -1$, so it follows that $\alpha^{qk} = \alpha^{-k} = -\alpha^k$. Thus, Lemma 4.3.7 shows that

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix} = \frac{1}{\alpha^q - \alpha}\begin{pmatrix} \alpha^{q+k} + \alpha^{k+1} & -2\alpha^k \\ -2\alpha^k & -\alpha^{q+k} - \alpha^{k+1} \end{pmatrix}.$$

In particular, for any odd prime power $q \equiv 3 \bmod 4$, we can compute explicitly two elements $a, b \in \mathbb{F}_q^\times$ in terms of a primitive root of $\mathbb{F}_{q^2}$ such hat $a^2 + b^2 = -1$.

Next, we write $F := \mathbb{F}_q^\times \setminus \{-\frac{a}{b}, \frac{b}{a}\}$, and consider the two maps

$$\sigma : S \to \mathbb{F}_q : x \mapsto \frac{-ax+b}{bx+a} \quad \text{and} \quad \tau : S \to \mathbb{F}_q : x \mapsto -x^{-1}.$$

Lemma 4.3.9. *Both σ and τ are permutations on F with $\sigma^2 = \tau^2 = \mathrm{id}_F$ and $\sigma \circ \tau = \tau \circ \sigma$. The orbits of F under the action of $\langle \tau, \sigma \rangle$ are of the form $\{x, \sigma(x), \tau(x), \sigma(\tau(x))\}$ and have cardinality 4.*

Proof. First, we show that the images of σ and τ lie in F. This is clear for τ, since $-(-\frac{a}{b})^{-1} = \frac{b}{a}$ and $-(\frac{b}{a})^{-1} = -\frac{a}{b}$. Moreover, from $\frac{-ax+b}{bx+a} = 0$ it follows that $x = \frac{b}{a} \notin F$, and from $\frac{-ax+b}{bx+a} = \frac{b}{a}$, it follows that $x = 0 \notin F$. Finally, $\frac{-ax+b}{bx+a} = -\frac{a}{b}$ implies $-1 = a^2 + b^2 = 0$, a contradiction. Thus, the image of σ is contained in F, too.

Let $x \in F$. Then we have

$$\sigma^2(x) = \frac{-a\frac{-ax+b}{bx+a} + b}{b\frac{-ax+b}{bx+a} + a} = \frac{\frac{1}{bx+a}}{\frac{1}{bx+a}} \cdot \frac{x(a^2+b^2) - ab + ab}{a^2 + b^2 - abx + abx} = x$$

and $\tau^2(x) = -(-x^{-1})^{-1} = x$. Moreover,

$$(\tau \circ \sigma \circ \tau)(x) = -\left(\frac{ax^{-1} + b}{-bx^{-1} + a}\right)^{-1} = -\frac{-bx^{-1} + a}{ax^{-1} + b} = -\frac{x^{-1}}{x^{-1}} \frac{ax - b}{bx + a} = \sigma(x).$$

If x is a fixed point of τ, then $x^2 = -1$ implies that $x \in \mathbb{F}_q^\times$ has order 4, contradicting the fact $q \equiv 3 \bmod 4$. If x is a fixed point of σ, then $x(bx + a) = -ax + b$ implies $x^2 + 2\frac{a}{b}x - 1 = 0$, so

$$b^2(x + \tfrac{a}{b})^2 = b^2(1 + (\tfrac{a}{b})^2) = a^2 + b^2 = -1.$$

It follows that $b(x + \frac{a}{b}) \in \mathbb{F}_q^\times$ has order 4, a contradiction.

Finally, it is clear that the orbits of F are of the form

$$\{x, \sigma(x), \tau(x), \sigma(\tau(x))\}.$$

As $\sigma \circ \tau = \tau \circ \sigma$, we have $|\langle \tau, \sigma \rangle| = 4$, and since σ and τ have no fixed points, their cardinality is always at least 2.
Suppose that there exists some $x \in F$ such that $\sigma(x) = \tau(x)$. Then $-x^{-1} = \frac{-ax+b}{bx+a}$, so $x^2 - 2\frac{b}{a}x - 1 = 0$, and it follows that

$$a^2(x - \tfrac{b}{a})^2 = a^2(1 + (\tfrac{b}{a})^2) = a^2 + b^2 = -1,$$

which is a contradiction as before. $\square$

Lemma 4.3.10. *Let $x \in \mathbb{F}_q^\times$.*

(a) *If $x \neq -\frac{a}{b}$, then we have $X^{(q+1)_2/2} \cdot \delta_x = \delta_{\sigma(x)} + \delta_{-\frac{a}{b}}$. Moreover, $X^{(q+1)_2/2} \cdot \delta_{-\frac{a}{b}} = \delta_{-\frac{a}{b}}$.*

(b) *We have $Y \cdot \delta_x = \delta_{\tau(x)} + \delta_0$, where we extend τ to all of $\mathbb{F}_q^\times$ by $\tau(-\frac{a}{b}) := \frac{b}{a}$ and $\tau(\frac{b}{a}) := -\frac{a}{b}$.*

Proof.

(a) For $x \in \mathbb{F}_q^\times \setminus \{-\frac{a}{b}\}$ we have

$$X^{(q+1)_2/2} \cdot \omega_x = X^{(q+1)_2/2} \cdot \langle\left(\begin{smallmatrix}1\\x\end{smallmatrix}\right)\rangle_{\mathbb{F}_q} = \langle\left(\begin{smallmatrix}a+bx\\b-ax\end{smallmatrix}\right)\rangle_{\mathbb{F}_q} = \left\langle\left(\begin{smallmatrix}1\\\sigma(x)\end{smallmatrix}\right)\right\rangle_{\mathbb{F}_q} = \omega_{\sigma(x)}.$$

Moreover,

$$X^{(q+1)_2/2} \cdot \omega = X^{(q+1)_2/2} \cdot \langle\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)\rangle_{\mathbb{F}_q} = \langle\left(\begin{smallmatrix}b\\-a\end{smallmatrix}\right)\rangle_{\mathbb{F}_q} = \left\langle\left(\begin{smallmatrix}1\\-\frac{a}{b}\end{smallmatrix}\right)\right\rangle_{\mathbb{F}_q} = \omega_{-\frac{a}{b}}.$$

As $(X^{(q+1)_2/2})^2 = -\mathbb{1}_2$ acts trivially on each one-dimensional subspace, it follows that also $X^{(q+1)_2/2} \cdot \omega_{-\frac{a}{b}} = \omega$.
Now, we have $x \in \mathbb{F}_q^\times \setminus \{-\frac{a}{b}\}$, then

$$X^{(q+1)_2/2} \cdot \delta_x = X^{(q+1)_2/2} \cdot ((\omega_x + \omega) + U) = (X^{(q+1)_2/2} \cdot \omega_x + X^{(q+1)_2/2} \cdot \omega) + U$$

$$= (\omega_{\sigma(x)} + \omega_{-\frac{a}{b}}) + U = (\omega_{\sigma(x)} + \omega_{-\frac{a}{b}} + 2\omega) + U = \delta_{\sigma(x)} + \delta_{-\frac{a}{b}}.$$

Finally,

$$X^{(q+1)_2/2} \cdot \delta_{-\frac{a}{b}} = X^{(q+1)_2/2} \cdot (\omega_{-\frac{a}{b}} + \omega) + U = (X^{(q+1)_2/2} \cdot \omega_{-\frac{a}{b}} + X^{(q+1)_2/2} \cdot \omega) + U$$

$$= (\omega + \omega_{-\frac{a}{b}}) + U = \delta_{-\frac{a}{b}}.$$

(b) This follows immediately from Lemma 4.3.3 since $Y = AB$.

∎

Lemma 4.3.11. *Let* P *be a maximal subgroup of* $\left\langle X^{(q+1)_2/2}, Y\right\rangle$*, and let* $\nu \in D^P$*. Then the coefficient of* $\mathrm{Tr}_P^{\left\langle X^{(q+1)_2/2}, Y\right\rangle}(\nu) \in D^{\left\langle X^{(q+1)_2/2}, Y\right\rangle}$ *at* $\delta_{\frac{b}{a}}$ *is zero.*

Proof. Write $\nu = \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_x$, and let $s := \sum_{x \in \mathbb{F}_q^\times} \lambda_x$.

First case: $P = \left\langle X^{(q+1)_2/2}\right\rangle$.

Then

$$\begin{aligned}
\mathrm{Tr}_P^{\left\langle X^{(q+1)_2/2}, Y\right\rangle}(\nu) &= \nu + Y\nu \\
&= \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_x + \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_{\tau(x)} + \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_0 \\
&= \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_x + \sum_{x \in \mathbb{F}_q^\times} \lambda_{\tau(x)} \delta_x + s\delta_0 \\
&= \sum_{x \in \mathbb{F}_q^\times} (\lambda_x + \lambda_{\tau(x)} + s)\delta_x.
\end{aligned}$$

It suffices that show that $s = \lambda_{-\frac{a}{b}} + \lambda_{\frac{b}{a}}$, since then the coefficient at $\delta_{\frac{b}{a}}$ is clearly zero. Since ν is fixed by $X^{(q+1)_2/2} \in P$, we have

$$\begin{aligned}
\nu &= X^{(q+1)_2/2}\nu \\
&= \sum_{x \in F} \lambda_x \delta_{\sigma(x)} + \sum_{x \in F} \lambda_x \delta_{-\frac{a}{b}} + \lambda_{-\frac{a}{b}} \delta_{-\frac{a}{b}} + \lambda_{\frac{b}{a}} (\delta_{-\frac{a}{b}} + \delta_0),
\end{aligned}$$

and comparing the coefficient at $\delta_{-\frac{a}{b}}$ on both sides, we have $\lambda_{-\frac{a}{b}} = s + \lambda_{\frac{b}{a}}$.

Second case: $P = \langle Y \rangle$ or $P = \left\langle X^{(q+1)_2/2} Y\right\rangle$.

Then

$$\begin{aligned}
\mathrm{Tr}_P^{\left\langle X^{(q+1)_2/2}, Y\right\rangle}(\nu) &= \nu + X^{(q+1)_2/2}\nu \\
&= \sum_{x \in \mathbb{F}_q^\times} \lambda_x \delta_x + \sum_{x \in F} \lambda_x \delta_{\sigma(x)} + \sum_{x \in F} \lambda_x \delta_{-\frac{a}{b}} \\
&\quad + \lambda_{-\frac{a}{b}} \delta_{-\frac{a}{b}} + \lambda_{\frac{b}{a}} (\delta_{-\frac{a}{b}} + \delta_0) \\
&= \sum_{x \in F} \lambda_x \delta_x + \lambda_{-\frac{a}{b}} \delta_{-\frac{a}{b}} + \lambda_{\frac{b}{a}} \delta_{\frac{b}{a}} + \sum_{x \in F} \lambda_{\sigma(x)} \delta_x + \sum_{x \in F} \lambda_x \delta_{-\frac{a}{b}} \\
&\quad + \lambda_{-\frac{a}{b}} \delta_{-\frac{a}{b}} + \lambda_{\frac{b}{a}} (\delta_{-\frac{a}{b}} + \delta_0) \\
&= \sum_{x \in F} (\lambda_x + \lambda_{\sigma(x)} + \lambda_{\frac{b}{a}}) \delta_x + \sum_{x \in F} \lambda_x \delta_{-\frac{a}{b}}.
\end{aligned}$$

Thus, the coefficient at $\delta_{\frac{b}{a}}$ is zero, since $\frac{b}{a} \notin F$. $\square$

Lemma 4.3.12. *There exists a vector $v = \sum_{x\in\mathbb{F}_q^\times} \lambda_x\delta_x \in D^{\langle X^{(q+1)_2/2},Y\rangle}$ such that $\lambda_{-\frac{a}{b}} = \lambda_{\frac{b}{a}} = 1$, and $\lambda_x = \lambda_{\tau(x)} = \lambda_{\sigma(x)} + 1$ for all $x \in F$.*

Proof. We fix a set of representatives R for the orbits of F under the action of $\langle\sigma,\tau\rangle$, and define $\lambda_x := \lambda_{\tau(x)} := 0$ and $\lambda_{\sigma(x)} := \lambda_{\sigma(\tau(x))} := 1$ for all $x \in R$. If $y \in F$ is given, then considering the cases $y \in R$, $\tau(y) \in R$, $\sigma(y) \in R$, and $\sigma(\tau(y)) \in R$, one sees immediately that $\lambda_y = \lambda_{\tau(y)} = \lambda_{\sigma(y)} + 1$. Therefore, the vector

$$v := \delta_{-\frac{a}{b}} + \delta_{\frac{b}{a}} + \sum_{x\in R}\sum_{f\in\langle\sigma,\tau\rangle} \lambda_{f(x)}\delta_{f(x)}$$

has all the properties from the claim, except maybe the property $v \in D^{\langle X^{(q+1)_2/2},Y\rangle}$ which is still to prove. First, note that

$$\sum_{x\in F}\lambda_x = \sum_{x\in R}\underbrace{\lambda_x + \lambda_x + \lambda_x + 1 + \lambda_x + 1}_{=0} = 0.$$

Therefore, we have

$$\begin{aligned}
X^{(q+1)_2/2}v &= \sum_{x\in F}\lambda_x\delta_{\sigma(x)} + \underbrace{\sum_{x\in F}\lambda_x}_{=0}\,\delta_{-\frac{a}{b}} + \delta_{-\frac{a}{b}} + \delta_{-\frac{a}{b}} + \delta_0 \\
&= \sum_{x\in F}\lambda_{\sigma(x)}\delta_x + \delta_0 \\
&= \sum_{x\in F}\underbrace{(\lambda_{\sigma(x)} + 1)}_{=\lambda_x}\delta_x + \delta_{-\frac{a}{b}} + \delta_{\frac{b}{a}} \\
&= \sum_{x\in F}\lambda_x\delta_x + \delta_{-\frac{a}{b}} + \delta_{\frac{b}{a}} \\
&= v.
\end{aligned}$$

Finally,

$$\begin{aligned}
Yv &= \sum_{x\in F}\lambda_x\delta_{\tau(x)} + \underbrace{\sum_{x\in F}\lambda_x}_{=0}\,\delta_0 + \delta_{\frac{b}{a}} + \delta_0 + \delta_{-\frac{a}{b}} + \delta_0 \\
&= \sum_{x\in F}\lambda_{\tau(x)}\delta_x + \delta_{\frac{b}{a}} + \delta_{-\frac{a}{b}} \\
&= \sum_{x\in F}\lambda_x\delta_x + \delta_{\frac{b}{a}} + \delta_{-\frac{a}{b}} \\
&= v.
\end{aligned}$$

∎

Lemma 4.3.13. *The Sylow 2-subgroup* $\langle X, Y\rangle$ *of* $\mathrm{GL}_2(q)$ *has precisely three maximal subgroups. They are given by the cyclic subgroup* $\langle X\rangle$*, the dihedral group* $\left\langle X^2, YX\right\rangle$*, and the generalized quaternion group* $\left\langle X^2, Y\right\rangle$*. The latter is a Sylow 2-subgroup of* $\mathrm{SL}_2(q)$*.*

Proof. It is clear that $\{X, Y\}$ is a minimal generating set for $\langle X, Y\rangle$, so Lemma 4.3.2 implies that the number of maximal subgroups of $\langle X, Y\rangle$ is $1 + 2 = 3$.

The order of $\langle X, Y\rangle$ is $4(q + 1)_2$, so it follows from $\mathrm{ord}(X) = \mathrm{ord}(\alpha) = 2(q + 1)_2$ that the subgroup $\langle X\rangle$ is maximal.

The matrix YX has order 2. As Y is not a power of X, we have $YX \notin \left\langle X^2\right\rangle$, so the order of $\left\langle X^2, YX\right\rangle$ is at least

$$|\langle X^2\rangle \cdot \langle YX\rangle| = \tfrac{\mathrm{ord}(X^2)\,\mathrm{ord}(YX)}{1} = \tfrac{|\langle X,Y\rangle|}{4} \cdot 2 = 2(q+1)_2.$$

Moreover, $(YX)X^2(YX) = X^{-2}$ shows that $\left\langle X^2, YX\right\rangle$ is a dihedral group which is strictly contained in $\langle X, Y\rangle$.

Finally, the order of $\left\langle X^2, Y\right\rangle$ of is at least

$$|\langle X^2\rangle \langle Y\rangle| = \tfrac{\mathrm{ord}(X^2)\,\mathrm{ord}(Y)}{|\{\pm \mathbb{1}_2\}|} = \tfrac{|\langle X,Y\rangle|/4\cdot 4}{2} = 2(q+1)_2.$$

As $X \notin \left\langle X^2, Y\right\rangle$, it must have order $|\left\langle X^2, Y\right\rangle| = 2(q + 1)_2$. Since $\det(X^2) = \det(Y) = 1$, it follows that $\left\langle X^2, Y\right\rangle$ is a Sylow 2-subgroup of $\mathrm{SL}_2(q)$. It is generalized quaternion by Theorem 2.5.7. □

Now, we can prove part (b) of Theorem 4.2.1:

Proof of part (b) of Theorem 4.2.1. Every vector as in Lemma 4.3.12 belongs to

$$D^{\left\langle X^{(q+1)_2/2}, Y\right\rangle} \setminus \mathrm{Tr}^{\left\langle X^{(q+1)_2/2}, Y\right\rangle}(D).$$

Thus, the quaternion group $\left\langle X^{(q+1)_2/2}, Y\right\rangle$ is contained in some vertex of D.
We already know that these vertices have order $2(q + 1)_2$ and are, thus, isomorphic to a maximal subgroup of $\langle X, Y\rangle$. It is clear that the cyclic group $\langle X\rangle$ has no subgroup isomorphic to the quaternion group. Alternatively, by part (d) of Proposition 1.3.1, the cyclic group $\langle X\rangle$ cannot be a vertex of any simple module if the corresponding defect group is non-cyclic.
Moreover, as non-abelian subgroups of dihedral groups are dihedral again (see, for example, [57, 2.37 (page 54)]), we have shown that the dihedral group $\left\langle X^2, XY\right\rangle$ cannot be a vertex of D. Thus, the vertices of D must be conjugate to $\left\langle X^2, Y\right\rangle \subseteq \mathrm{SL}_2(q)$. □

Open problems

At this point, we want to collect some open questions which occurred while working on this thesis.

Let $\ell \in \mathbb{P}_{>2}$. In Theorem 3.2.5 and Corollary 3.2.6, we present certain sets of finite classical groups that have the SCBDP and, therefore, also the VBDP with respect to every finite ℓ-group. It is natural to ask the following:

Question 1: Do Theorem 3.2.5 and Corollary 3.2.6 also hold true for $\ell = 2$?

Moreover, the classical groups of symplectic and orthogonal type occurring in Theorem 3.2.5 and Corollary 3.2.6 are always matrix groups over finite fields of odd characteristic. This is because in the proof we use a result due to Fong and Srinivasan that is only formulated for this situation:

Question 2: Do Theorem 3.2.5 and Corollary 3.2.6 still hold true if the prime powers q and $\tilde{q}$ are also allowed to be even?

Again, let $\ell \in \mathbb{P}_{>2}$. Theorem 3.2.2 shows that the set $\{\mathrm{SL}_n(q) : n \in \mathbb{N},\ q \text{ prime power}\}$ does not have the SCBDP with respect to every finite ℓ-group, and the same is true when we replace $\mathrm{SL}_n(q)$ by $\mathrm{PGL}_n(q)$, $\mathrm{PSL}_n(q)$, $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, or $\mathrm{PSU}_n(q)$. But we cannot say whether these sets have the VBDP with respect to every finite ℓ-group, as it is not clear whether the small self-centralizing subgroups from Theorem 2.7.12 actually occur as vertices of simple modules lying in blocks of maximal defects. Here, we can also ask the analogous question for parts (a), (b), and (c) of Theorem 2.7.12:

Question 3: Do some parts of Theorem 3.2.2 also hold if we replace the SCBSP by the VBDP?

If one can show that the answer to Question 3 is positive for part (d) of Theorem 3.2.2, then this gives a counterexample to Puig's question for odd ℓ.

In Section 2.7 we did not consider the case $\ell = 2$ and $q \equiv 3 \bmod 4$. The reason is that in this case we cannot find a Sylow 2-subgroup of $\mathrm{GL}_n(q)$ in $\mathrm{MonGL}_n(q)$, so the structural arguments used in Section 2.7 do not apply. As already explained at the end of Section 2.7, for $\ell = 2$ the case $q \equiv 3 \bmod 4$ is much more complicated than the case $q \equiv 1 \bmod 4$. It would be of interest to know whether the results of Section 2.7 can be generalized such that they also apply to the case $\ell = 2$ and $q \equiv 3 \bmod 4$:

Question 4: What can one say about exponents, elementary abelian normal subgroups, the structure and the order of the centers and, mainly, the existence of small self-centralizing subgroups for the Sylow 2-subgroups of $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ if $q \equiv 3 \bmod 4$?

Corollary 3.2.7 states that the set of spin groups over fields of odd characteristic have the SCBSP with respect to every finite ℓ-group.

Question 5: Does Corollary 3.2.7 also hold if we replace the SCBSP by the SCBDP?

In this thesis, whenever we show that a set of finite classical groups has the SCBSP or the SCBDP with respect to every finite ℓ-group (and the corresponding defect groups are non-abelian), we use the doubly exponential bound $|N| \leq |V|^{|V|^{|V|}}$ from Theorem 2.1.5. As a consequence, we obtain very complicated bounds as in Corollary 2.7.7 and Corollary 2.7.11 (and not even state precise bounds in Chapter 3). Of course, one can expect that there exist better bounds.

Question 6: How can one give better bounds for the positive results of Chapter 2 and Chapter 3?

Finally, in Chapter 4, we only determine the vertices of the simple $\overline{\mathbb{F}}_2\,\mathrm{GL}_n(q)$-module D in the case $n = 2$. For even $n > 2$, the vertices still seem to be unknown. As the dimension $[n] - 2 = 1 + q + \cdots + q^{n-1} - 2$ of the module D gets big very fast, it is hard to compute examples for small q already for $n = 4$ in order to get a feeling what the vertices could be.

Question 7: What groups occur as vertices of the simple $\overline{\mathbb{F}}_2\,\mathrm{GL}_n(q)$-module D in case that $n > 2$ is even?

Notation

General notation

δ_{ij}	the Kronecker delta, that is, 1 for $i = j$, and 0 for $i \neq j$
$A \sqcup B$	the disjoint union of the sets A and B
$\mathbb{P}$	the set $\{2, 3, 5, 7, \ldots\}$ of prime numbers
$\mathbb{N}$	the set $\{0, 1, 2, 3, \ldots\}$ of non-negative integers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$m \mid n$	the integer m divides the integer n
$m \nmid n$	the integer m does not divide the integer n
$\lfloor x \rfloor$	the integral part of the real number x
$\gcd(a, b)$	the positive greatest common divisor of the integers a and b
n_ℓ	the largest power of the prime number ℓ that divides the integer $n \neq 0$
$K^\times$	the unit group $K \setminus \{0\}$ of the field K
$\mathbb{F}_\ell$	the prime field of characteristic ℓ
$\mathbb{F}_q$	the finite field of q elements
$(\mathbb{F}_q^\times)^2$	the group of squares in $\mathbb{F}_q^\times$
$\overline{\mathbb{F}}_\ell$	the algebraic closure of $\mathbb{F}_\ell$
$\mathrm{Map}(A, B)$	the set of maps $A \to B$
$\mathrm{Hom}_A(M, N)$	the set of all A-module homomorphisms $M \to N$
$\mathrm{End}_A(M)$	the set of all A-module homomorphisms $M \to M$
$\mathrm{Z}(A)$	the center of the algebra A
$\mathbb{1}_n$	the identity matrix of size $n \times n$
$\mathrm{diag}(a_1, \ldots, a_n)$	the diagonal matrix of size $n \times n$ with diagonal entries $a_1, \ldots, a_n$
$\mathrm{GL}_K(V)$	the group of K-vector space automorphisms $V \to V$
$\mathrm{GL}_n(K)$	the group of invertible matrices of size $n \times n$ over the field K
$\mathrm{Gal}(K)$	the group of field automorphisms of the field K
$\mathrm{PerMat}(\sigma)$	the permutation matrix of the permutation σ, see Section 2.4
$\mathrm{PerMat}(S)$	the set of permutation matrices of the permutations in $S \subseteq \mathrm{Sym}(n)$
$\mathcal{F}$	the set of finite groups up to isomorphism, see Remark 3.1.2

Notation from group theory

$\lvert G \rvert$	the order of the finite group G
$\mathrm{ord}(g)$	the order of the group element $g \in G$

$\mathrm{Exp}(G)$	the exponent of the group G
$Z(G)$	the center of the group G
G'	the commutator subgroup of the group G
$H \leq G$	H is a subgroup of G
G/H	the set of left cosets of G with respect to a subgroup $H \leq G$
$\|G : H\|$	the cardinality of G/H
$\ker(f)$	the kernel of the group homomorphism f
$\mathrm{im}(f)$	the image of the group homomorphism f
$\mathrm{Aut}(G)$	the group of group automorphisms $G \to G$
${}^{g}H$	for a subgroup $H \leq G$ and $g \in G$, the conjugate gHg^{-1}
$H \leq_G U$	a G-conjugate of H is a subgroup of U
$O_\ell(G)$	the largest normal ℓ-subgroup of the finite group G
$C_G(H)$	the centralizer of H in G
$N_G(H)$	the normalizer of H in G
$G \wr H$	the wreath product of the groups G and H, see Remark 2.2.3
$\mathrm{Syl}_\ell(G)$	the set of Sylow ℓ-subgroups of the group G
$\mathrm{rk}(G)$	the rank of the group G, see Definition 2.2.1
$\mathrm{nrk}(G)$	the normal rank of the group G, see Definition 2.2.1
$\Omega_1(G)$	see Definition 2.2.1
$\mathrm{Exp}_\ell(G)$	the exponent of the Sylow ℓ-subgroups of G, see Proposition 3.1.7

Particular groups

C_n	the cyclic group $\mathbb{Z}/n\mathbb{Z}$ of n elements
C_n^k	the group $\underbrace{C_n \times \cdots \times C_n}_{k}$
Klein four-group	the group C_2^2
$\mathrm{Sym}(M)$	the group of permutations $M \to M$, where M is a set
$\mathrm{Sym}(n)$	the symmetric group $\mathrm{Sym}(\{1, \dots, n\})$ on n letters
$\mathrm{Alt}(n)$	the alternating group on n letters
Dih_{2n}	the dihedral group of order $2n$
$\mathrm{MonGL}_n(q)$	the subgroup of $\mathrm{GL}_n(q)$ of monomial matrices, see Definition 2.4.1

$\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$, and $\mathrm{PSL}_n(q)$ denote the finite classical groups of linear type, see Theorem 1.6.1

$\mathrm{Sp}_{2n}(q)$ and $\mathrm{PSp}_{2n}(q)$ denote the finite classical groups of symplectic type, see Theorem 1.6.10

$\mathrm{GU}_n(q)$, $\mathrm{SU}_n(q)$, $\mathrm{PGU}_n(q)$, and $\mathrm{PSU}_n(q)$ denote the finite classical groups of unitary type, see Theorem 1.6.12

$\mathrm{GO}_{2n+1}(q)$, $\mathrm{SO}_{2n+1}(q)$, $\mathrm{PGO}_{2n+1}(q)$, $\Omega_{2n+1}(q)$, $\mathrm{GO}^+_{2n}(q)$, $\mathrm{SO}^+_{2n}(q)$, $\mathrm{PGO}^+_{2n}(q)$, $\mathrm{PSO}^+_{2n}(q)$, $\Omega^+_{2n}(q)$, $\mathrm{P}\Omega^+_{2n}(q)$, $\mathrm{GO}^-_{2n}(q)$, $\mathrm{SO}^-_{2n}(q)$, $\mathrm{PGO}^-_{2n}(q)$, $\mathrm{PSO}^-_{2n}(q)$, $\Omega^-_{2n}(q)$, and $\mathrm{P}\Omega^-_{2n}(q)$ denote the finite classical groups of orthogonal type, see Theorem 1.6.13 and Theorem 1.6.14

$\mathrm{Spin}_{2n+1}(q)$, $\mathrm{Spin}^+_{2n}(q)$ and $\mathrm{Spin}^-_{2n}(q)$ denote the spin groups introduced in Remark 1.6.18

Notation from representation theory

${}^gX$	the conjugation of the module X by the element g, see Section 1.1
$\mathrm{Vx}(M)$	the set of vertices of the module M, see Theorem 1.2.5
$\mathrm{Bl}(KG)$	the set of blocks of the group algebra KG, see Section 1.3
$\mathrm{Def}(B)$	the set of defect groups of the block B, see Section 1.3
$\mathrm{Inf}^G_{G/H}(M)$	the inflation of the module M, see Section 1.1
$\mathrm{Res}^G_H(M)$	the restriction of the module M, see Section 1.1
$\mathrm{Ind}^G_H(M)$	the induction of the module M, see Section 1.1

Index

absolutely irreducible, 10
absolutely simple, 10
alternating sesquilinear form, 19

base group, 35
bilinear form, 19
block, 13
block idempotent, 13
block induction, 14
Brauer pair, 15

Chevalley group, 28, 29
classical group, 27
conjugation, 9
cover, 14

defect group, 13
degenerate, 19
dicyclic group, 33
dihedral group, 33
dominate, 15

Erdmann's Theorem, 14
exponent, 10

generalized quaternion group, 33
geometry, 21
group algebra, 7

hermitian sesquilinear form, 19

idempotent, 13
indecomposable, 10
induction, 9
inertia group, 9
inflation, 9
irreducible, 10
isometry, 22
isometry group, 22
isotropic, 19

Jacobson radical, 10

Klein four-group, 27
Knörr's Theorem, 17

Lie group, 28

matrix of a sesquilinear form, 21
matrix representation, 8
Michler's Theorem, 14
module, 8
monomial matrix, 42

normal rank, 34

orthogonal group, 25, 26

permutation module, 7
principal block, 13
projective, 10
projective general linear group, 18
projective special linear group, 18
Puig's Question, 17

quadratic form, 19
quadratic geometry, 21
quaternion group, 33

rank, 34
reflexive sesquilinear form, 19
relatively projective, 11
representation, 8
restriction, 9

SBDP, 79
scalar extension, 9
SCBDP, 79
SCBSP, 79
self-centralizing Brauer pair, 16

self-centralizing-bounded-defect
property, 79
self-centralizing-bounded-Sylow
property, 79
semidihedral group, 33
sesquilinear form, 19
similar, 8
simple, 10
spin groups, 27
splitting field, 10
strongly-bounded-defect property, 79
Sylow Brauer pair, 16
symmetric sesquilinear form, 19
symplectic geometry, 21
symplectic group, 23

totally isotropic, 19

unitary geometry, 21
unitary group, 24

VBDP, 79
vertex, 12
vertex-bounded-defect property, 79

Witt's Extension Theorem, 22
Witt-Index, 22
wreath product, 35

Bibliography

[1] M. I. AlAli, C. Hering, A. Neumann, *A number theoretic approach to Sylow r-subgroups of classical groups*, Rev. Mat. Complut. **18** (2005), 329–338.

[2] J. L. Alperin, *Local Representation Theory*, Cambridge University Press, Cambridge, 1986.

[3] J. L. Alperin, M. Broué, *Local methods in block theory*, Ann. of Math. **110** (1979), 143–157.

[4] J. An, *Weights for the Chevalley groups* $G_2(q)$, Proc. London Math. Soc. **69** (1994), 22–46

[5] S. Ball, *Finite Geometry and Combinatorial Applications*, Cambridge University Press, Cambridge, 2015.

[6] D. Benson, *Representations and Cohomology I*, Cambridge Studies in Advanced Mathematics, 30, Cambridge University Press, Cambridge, 1995.

[7] C. Bessenrodt, W. Willems, *Relations between complexity and modular invariants and consequences for* p*-solvable groups*, J. Algebra **86** (1984), 445–456.

[8] R. Brauer, *Some applications of the theory of blocks of characters of finite groups III*, J. Algebra **3** (1966), 225–255.

[9] M. Broué, *Les* ℓ*-blocs des groupes* $\mathrm{GL}(n, q)$ *et* $\mathrm{U}(n, q^2)$ *et leurs structures locales*, Asterisque **133–134** (1986), 159–188

[10] M. Broué, *On Scott modules and* p*-permutation modules: An approach through the Brauer morphism*, Proc. Amer. Math. Soc. **39** (1985), 401–408.

[11] M. Cabanes, M. Enguehard, *Representation Theory of Finite Reductive Groups*, Cambridge University Press, Cambridge, 2004.

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

[13] R. W. Carter, P. Fong, *The Sylow* 2*-subgroups of the finite classical groups*, J. Algebra **1** (1964), 139–151.

[14] C. Chevalley, *The Algebraic Theory of Spinors and Clifford Algebras. Collected works, vol. 2*, Springer-Verlag, Berlin, 1997.

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

[16] C. W. Curtis, I. Reiner, *Methods of Representation Theory with Applications to Finite Groups and Orders I*, Wiley, New York, 1981.

[17] S. Danz, B. Külshammer, *Vertices of small order for simple modules of finite symmetric groups*, Algebra Colloq. **17** (2010), 75–86.

[18] S. Danz, J. Müller, *Source algebras of blocks, sources of simple modules, and a conjecture of Feit*, J. Algebra **353** (2012), 187–211.

[19] D. Deriziotis, G. Michler, *Character table and blocks of finite simple triality groups* ${}^3\mathrm{D}_4(\mathrm{q})$, Trans. Amer. Math. Soc. **303** (1987), 39–70.

[20] R. Dipper, *On irreducible modules of twisted groups of Lie type*, J. Algebra **81** (1983), 370–389.

[21] R. Dipper, *Vertices of irreducible representations of finite Chevalley groups in the describing characteristic*, Math. Zeitschrift **175** (1980), 143–159.

[22] L. Dornhoff, *Group Representation Theory. Part A: Ordinary Representation Theory*, Pure and Applied Mathematics, New York, 1971.

[23] M. Enguehard, J. Michel, *The Sylow Subgroups of a Finite Reductive Group*, arXiv:1602.01424.

[24] K. Erdmann, *Blocks and simple modules with cyclic vertices*, Bull. London Math. Soc. **9** (1977), 216–218.

[25] K. Erdmann, *Principal blocks of groups with dihedral Sylow 2-subgroups*, Comm. Algebra **5** (1977), 665–694.

[26] K. Erdmann, S. Schroll, *On Young modules of general linear groups*, J. Algebra **310** (2007), 434–451.

[27] W. Feit, *The Representation Theory of Finite Groups*, North-Holland Mathematical Library, Amsterdam, 1982.

[28] P. Fong, B. Srinivasan, *The blocks of finite general linear and unitary groups*, Invent. Math. **69** (1982), 109–153.

[29] P. Fong, B. Srinivasan, *The blocks of finite classical groups*, J. Reine Angew. Math. **396** (1989), 122–191.

[30] M. Geck, *Basic sets of Brauer characters of finite groups of Lie type III*, Manuscripta math. **85** (1994), 195–216.

[31] M. Geck, G. Hiss, *Basic sets of Brauer characters of finite groups of Lie type*, J. Reine Angew. Math. **418** (1991), 173–188.

[32] D. Gorenstein, *Finite Groups*, 2nd edition, Chelsea, New York, 1980.

[33] L. C. Grove, *Classical Groups and Geometric Algebra*, Graduate Studies in Mathematics, 39, American Mathematical Society, 2002.

[34] G. Hiss, *On the decomposition numbers of* $\mathsf{G}_2(\mathsf{q})$, J. Algebra **120** (1989), 339–360.

[35] G. Hiss, J. Shamash, 3*-blocks and* 3*-modular characters of* $\mathsf{G}_2(\mathsf{q})$, J. Algebra **131** (1990), 371–387.

[36] J. F. Humphreys, *A Course in Group Theory*, Oxford University Press, Oxford, 1996.

[37] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.

[38] B. Huppert, N. Blackburn *Finite Groups II*, Die Grundlehren der Mathematischen Wissenschaften, Band 243, Springer-Verlag, Berlin, 1982.

[39] M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[40] N. Jacobson, *Basic Algebra I*, Dover Publications, New York, 1985.

[41] G. James, *Representations of General Linear Groups*, London Mathematical Society Lecture Note Series 94, Cambridge University Press, Cambridge, 1984.

[42] G. James, A. Kerber, *The Representation Theory of the Symmetric Group*, Addison-Wesley, London, 1980.

[43] G. Karpilovsky, *Group Representations*, Vol. 3, North-Holland, 1994.

[44] P. Kleidman, *The maximal subgroups of the Steinberg triality groups* ${}^3\mathrm{D}_4(\mathsf{q})$ *and of their automorphism groups*, J. Algebra **115** (1988), 182–199.

[45] R. Knörr, *On the vertices of irreducible modules*, Ann. of Math. **110** (1979), 487–499.

[46] B. Külshammer, *Some indecomposable modules and their vertices*, J. Pure Appl. Algebra **86** (1993), 65–73.

[47] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep, *Commutators in finite quasisimple groups*, Bull. Lond. Math. Soc. **43** (2011), 1079–1092.

[48] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, 131, Springer-Verlag, Heidelberg, 1991.

[49] G. Malle, D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge Studies in Advanced Mathematics, 133, Cambridge University Press, Cambridge, 2011.

[50] G. O. Michler, *Green correspondence between blocks with cyclic defect groups I*, J. Algebra **39** (1976), 26–51.

[51] J. Müller, R. Zimmermann, *Green vertices and sources of simple modules of the symmetric group labelled by hook partitions*, Arch. Math. **89** (2007), 97–108.

[52] H. Nagao, Y. Tsushima, *Representations of Finite Groups*, Academic Press, San Diego, 1989.

[53] G. Navarro, *Characters and Blocks of Finite Groups*, London Mathematical Society Lecture Note Series 250, Cambridge University Press, Cambridge, 1998.

[54] J. B. Olsson, *On subpairs and modular representation theory*, J. Algebra **76** (1982), 261–279.

[55] L. Puig, *On Joanna Scopes' criterion of equivalence for blocks of symmetric groups*, Algebra Colloq. **1** (1994), 25–55.

[56] P. Ribenboim, *The New Book Of Prime Number Records*, Springer-Verlag, New York, 1996.

[57] S. Roman, *Fundamentals of Group Theory*, Birkhäuser, Basel, 2012.

[58] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann Verlag, Berlin, 1992.

[59] A. J. Weir, *Sylow* $\mathfrak{p}$*-subgroups of the classical groups over finite fields with characteristic prime to* $\mathfrak{p}$, Proc. Amer. Math. Soc. **6** (1955), 529–533.

[60] J. Zhang, *Vertices of irreducible representations and a question of L. Puig*, Algebra Colloq. **1** (1994), 139–148.

Scientific Background

Pablo Luka

2007	**Abitur** at Saarpfalz-Gymnasium Homburg, Germany
2008-2013	**Study of mathematics** at the University of Kaiserslautern, Germany
2013	**Diploma in mathematics**
since 2013	**Doctoral student** at the Department of Mathematics, University of Kaiserslautern
since 2015	**Research assistant** at the Department of Mathematics, University of Kaiserslautern

Wissenschaftlicher Werdegang

Pablo Luka

2007	**Abitur** am Saarpfalz-Gymnasium Homburg
2008-2013	**Studium der Mathematik** an der TU Kaiserslautern
2013	**Diplom in Mathematik**
seit 2013	**Doktorand** am Fachbereich Mathematik der TU Kaiserslautern
seit 2015	**wissenschaftlicher Mitarbeiter** am Fachbereich Mathematik der TU Kaiserslautern