JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis

Polynomial Functions on Classical Groups and Frobenius Groups

Dissertation

zur Erlangung des akademischen Grades

Doktor der Technischen Wissenschaften

Angefertigt am *Institut für Algebra*

Betreuung:

O.Univ.-Prof. Dr. Günter Pilz
Dr. C. J. Maxson

Eingereicht von:

Dipl.-Ing. Peter Mayr

Linz, März 2004

Johannes Kepler Universität
A-4040 Linz · Altenbergerstraße 69 · Internet: http://www.uni-linz.ac.at · DVR 0093696

Preface

The intuitive concept of polynomial functions on groups (or on arbitrary algebras) is rather straightforward: a polynomial function is a function that can be expressed by a certain term. While this definition can certainly be made more precise, its very nature makes it non-trivial to decide whether a given function is polynomial. Still, for certain classes of groups, polynomial functions can be characterized in a more convenient way. As an example, we state A. Fröhlich's result that all functions on finite simple non-abelian groups are polynomial.

In this thesis we want to deal with the following problems:

(1) How many unary polynomial functions are there on a given group?
(2) Are all automorphisms on a given group polynomial functions?
(3) Are all endomorphisms on a given group polynomial functions?

In Chapter 2 we describe the unary polynomial functions on the finite groups whose quotient by the center has a non-abelian unique minimal normal subgroup. This description was done and published jointly with E. Aichinger. It generalizes a number of existing results on non-solvable groups including the one by A. Fröhlich mentioned above. The main tool in the proof of our characterization is the interpolation of functions by using commutators. For this, we rely on the existence of a non-abelian chief factor.

In Chapter 3 the previous results are applied to the non-solvable groups G all of whose normal subgroups are either central or contain the derived subgroup of G. The finite linear, unitary, symplectic, and orthogonal groups (with the exception of certain groups acting on vector spaces of low dimension) satisfy this condition on normal subgroups. As a consequence, in Chapter 4, we are able to give complete solutions of the problems (1), (2), and (3) for these classical groups.

From Chapter 2 to 4 we specialize our results from the most general class of groups to the case of groups of regular linear transformations on finite vector spaces. We note that the original direction of research was actually reversed. The motivation was to understand polynomial functions on general linear groups. Phenomena that were observed for $\mathrm{GL}(n, q)$ were then generalized.

In Chapter 5 we pursue a different line of ideas. We start with E. Aichinger's description of unary polynomial functions on certain semidirect products that have a Frobenius group as quotient. Then we determine the number of polynomial functions on the finite solvable groups all of whose abelian subgroups are cyclic. This class contains the solvable Frobenius complements. Results from the previous chapters appear again, when we consider the non-solvable Frobenius complements. All in all, for Frobenius complements, we obtain a complete solution of problem (1) and partial solutions of (2) and (3). Finally the task of counting polynomial functions on a Frobenius group is reduced to that of counting the restrictions of these functions to the Frobenius kernel. We give these numbers explicitly for certain classes of groups.

Vorwort

Eine intuitive Definition von Polynomfunktionen auf Gruppen (oder auf beliebigen Algebren) ist recht einfach verständlich: eine Polynomfunktion kann als ein bestimmter Term geschrieben werden. Diese Definition ist zwar noch ungenau, aber sie zeigt schon, dass es nicht einfach ist zu entscheiden, ob eine gegebene Funktion eine Polynomfunktion ist. Im allgemeinen muss man dazu entweder eine konkrete Darstellung dieser Funktion finden oder zeigen, dass keine Darstellung existiert. Für manche Klassen von Gruppen kann man Polynomfunktionen einfacher charakterisieren Als ein Beispiel führen wir ein Resultat von A. Fröhlich an: Alle Funktionen auf endlichen einfachen nichtabelschen Gruppen sind Polynomfunktionen.

In dieser Arbeit möchte ich folgende Probleme behandeln:

(1) Wieviele Polynomfunktionen gibt es auf einer Gruppe?
(2) Sind alle Automorphismen auf einer Gruppe Polynomfunktionen?
(3) Sind alle Endomorphismen auf einer Gruppe Polynomfunktionen?

Im Kapitel 2 beschreiben wir die einstelligen Polynomfunktionen auf jenen endlichen Gruppen, deren Faktoren nach dem Zentrum einen einzigen minimalen Normalteiler besitzen, der auch nichtabelsch ist. Diese Beschreibung wurde gemeinsam mit E. Aichinger publiziert. Sie verallgemeinert eine Reihe von bestehenden Resultaten für nichtauflösbare Gruppen, insbesonders A. Fröhlich's Ergebnis. Ein wesentlicher Teil im Beweis unserer Charakterisation ist die Interpolation von Funktionen mithilfe von Kommutatoren. Dafür benötigen wir die Existenz eines nichtabelschen Hauptfaktors.

Im Kapitel 3 werden die vorhergehenden Resultate auf nichtauflösbare Gruppen G angewandt, die die Eigenschaft haben, dass jeder Normalteiler entweder zentral ist oder die Kommutatoruntergruppe enthält. Die endlichen linearen, unitären, symplektischen und orthogonalen Gruppen (mit Ausnahme von bestimmten Gruppen auf niedrigdimensionalen Vektorräumen) erfüllen diese Bedingung. Im Kapitel 4 können wir dann für diese klassischen Gruppen vollständige Lösungen für die Probleme (1), (2) und (3) angeben.

Von Kapitel 2 bis 4 betrachten wir immer speziellere Gruppen. Ursprünglich ist die Entwicklung anders verlaufen. Die Motivation war lineare Gruppen zu untersuchen. Die Ergebnisse für $\mathrm{GL}(n, q)$ konnten dann verallgemeinert werden.

Im Kapitel 5 verfolgen wir eine andere Richtung. Wir beginnen mit E. Aichinger's Beschreibung von Polynomfunktionen auf halbdirekten Produkten, die eine Frobeniusgruppe als Faktor besitzen. Damit bestimmen wir die Anzahl der Polynomfunktionen auf den endlichen auflösbaren Gruppen, deren sämtliche abelsche Untergruppen zyklisch sind. Zu dieser Klasse zählen insbesonders die auflösbaren Frobeniuskomplemente. Bei der Betrachtung der nichtauflösbaren Frobeniuskomplemente begegnen wir einigen Resultaten aus den vorigen Kapiteln wieder. Insgesamt erhalten wir für Frobeniuskomplemente eine vollständige Lösung für das Problem (1) und partielle Lösungen für (2) und (3). Schließlich reduziert sich die Bestimmung der Anzahl der Polynomfunktionen auf Frobeniusgruppen darauf, die Einschränkungen der Funktionen auf den Frobeniuskern zu zählen. Für einige Klassen von Gruppen geben wir diese Zahlen explizit an.

Acknowledgment

I want to thank Günter Pilz for the supervision and support of the work on this thesis. Erhard Aichinger invited me to collaborate with him in the paper [**AM03**] that is the foundation of the first part of this thesis. Also the latter part was instigated by a result of his. C. J. Maxson provided helpful suggestions.

For some time during my research, I was allowed to work at the University of Wisconsin at Madison; I want to thank Martin Isaacs for making this possible. I learned a lot from him and from Donald Passman.

Parts of this work were supported by grant P15691 of the Austrian Science Foundation (Fonds zur Förderung der wissenschaftlichen Forschung).

Contents

CHAPTER 1

Introduction

In this chapter we introduce notations and the concepts with which we will be dealing in the sequel. We write $\mathbb{Z}$ for the set of integers, $\mathbb{N}$ for the set of positive integers, and $\mathbb{N}_0$ for the set of non-negative integers. For $n \in \mathbb{N}$, we let $\mathbb{Z}_n$ denote the set of integers modulo n.

1. Groups

Let $(G, \cdot)$ be a group. We will not distinguish between the group $(G, \cdot)$ and its underlying set G provided that the intended group operation is clear. For a multiplicative group $(G, \cdot)$, we let 1 denote the identity element.

If H is a subgroup of a group G, then we will write $H \leq G$. If $H \leq G$ and $H \neq G$, then H is called a *proper subgroup*, denoted by $H < G$.

Let G be a group, let $g \in G$, and let $S \subseteq G$. Then we write $\langle g \rangle$ for the subgroup of G generated by g, and we write $\langle S \rangle$ for the subgroup of G generated by the elements in S.

The *order* of a group G is defined to be the cardinality of the underlying set G and is denoted $|G|$. For $x \in G$, the order of x is defined as $|\langle x \rangle|$ and denoted by $\operatorname{ord} x$. Elements of order 2 will be called *involutions* or *involutory.*

The *exponent* of a group G, denoted $\exp G$ is the smallest positive integer n such that $x^n = 1$ for all $x \in G$ if such an n exists; otherwise $\exp G = \infty$.

Let H be a subgroup of a group G. For $x, y \in G$, we write

$$x \sim_H y \text{ if } y^{-1}x \in H.$$

Then $\sim_H$ is an equivalence relation on G. The equivalence class of $x \in G$ is

$$xH := \{xh \mid h \in H\},$$

and xH is called the *left coset* of H containing x. Let $T \subseteq G$ be a set of representatives for $\sim_H$ on G. We call T a *transversal* for the left cosets of H in G. The cardinality of the set of left cosets of H in G is called the *index* of H in G, denoted $|G : H|$.

Let $(G, \cdot)$ be a group, and let $x, y \in G$. We call $x^y := y^{-1}xy$ the *conjugate* of x by y, and we call $[x, y] := x^{-1}y^{-1}xy$ the *commutator* of x and y. For subgroups X and Y of G, we write

$$[X, Y] := \langle \{[x, y] \mid x \in X, y \in Y\} \rangle.$$

The subgroup $G' := [G, G]$ is called the *derived subgroup* of G.

The *center* $Z(G)$ of a group G is defined as

$$Z(G) := \{z \in G \mid z^g = z \text{ for all } g \in G\}.$$

If $Z(G) = \{1\}$, then G is said to be *centerless*.

A subgroup N of a group G is a *normal subgroup* if $n^x \in N$ for all $n \in N$ and for all $x \in G$. If G has no normal subgroups apart from $\{1\}$ and G, then G is said to be *simple*. A normal subgroup N of G is called a *minimal normal subgroup* of G if $N \neq \{1\}$ and there is no normal subgroup K of G with $\{1\} < K < N$. Let L, N be normal subgroups G with $L < N$. If N/L is a minimal normal subgroup of G/L, then we say that N/L is a *chief factor* of G and write $L \prec_G N$.

For subgroups N and H of a group G, we let $NH := \{nh \mid n \in N, h \in H\}$. Then NH is a group if N is normal in G. If N is normal and $N \cap H = \{1\}$, then we say NH is the *semidirect product* of N and H. If N, H are normal and $N \cap H = \{1\}$, then we say that the product NH is *direct*.

Let G be a group, let H be a subgroup of G, and let X be a non-empty subset of G. We define the *centralizer of X in H* as the set

$$C_H(X) := \{h \in H \mid x^h = x \text{ for all } x \in X\}.$$

We also write $C_H(x)$ for $C_H(\{x\})$ with $x \in G$. For normal subgroups X, Y of G with $X < Y$, we define

$$C_G(Y/X) = \{g \in G \mid [y, g] \in X \text{ for all } y \in Y\}.$$

For groups N, Q, we say that a group G is an *extension of N by Q* if there exists a normal subgroup M of G such that M is isomorphic to N and G/M is isomorphic to Q.

The set of all functions from G into G will be denoted $M(G)$. For two functions $f, g \in M(G)$, the *composition* $f \circ g$ is defined by $f \circ g(x) = f(g(x))$ for all $x \in G$.

The set of endomorphisms of G, denoted End$G$, forms a monoid under composition. We let $\operatorname{Aut} G$ denote the set of automorphisms of a group G. Then $(\operatorname{Aut} G, \circ)$ is a group, called the *automorphism group* of G. The set of inner automorphisms of G is denoted $\operatorname{Inn} G$ and forms the *inner automorphism group* $(\operatorname{Inn} G, \circ)$.

A subgroup H of a group G is said to be *characteristic* in G if $\alpha(x) \in H$ for all $x \in H$ and for all automorphisms α of G. A subgroup H of a group G is said to be *fully-invariant* in G if $\alpha(x) \in H$ for all $x \in H$ and for all endomorphisms α of G.

2. Polynomials, polynomial functions, and endomorphism near-rings

Let $(G, \cdot)$ be a finite group. As in [**LN73**], [**MMT87**, Definition 4.4], a *unary polynomial function* $p : G \to G$ is a function that can be written in the form

$$p(x) := a_0 x^{e_0} a_1 x^{e_1} \cdots a_{n-1} x^{e_{n-1}} a_n,$$

where $n \in \mathbb{N}_0$, $a_0, \ldots, a_n$ are in G, and $e_0, \ldots, e_{n-1}$ are integers. The set of all polynomial functions on G will be denoted by $P(G)$, the set of all functions from G into G by $M(G)$. For two functions $f, g \in M(G)$, we define a product $f \cdot g$ by $f \cdot g\,(x) = f(x) \cdot g(x)$ for all $x \in G$. The group $(M(G), \cdot)$ is isomorphic to the direct product $(G^{|G|}, \cdot)$. We note that $(P(G), \cdot)$ is the subgroup of $(M(G), \cdot)$ that is generated by the identity function and the constant functions on G.

The subgroup of $M(G)$ that is generated by the inner automorphisms of G is denoted by $I(G)$. Then $I(G) = \{p \in P(G) \,|\, p(1) = 1\}$, and we have $|P(G)| = |I(G)| \cdot |G|$ (see Lemma 1.4). We define $A(G)$ as the subgroup of $M(G)$ that is generated by the automorphisms of G and $E(G)$ as the subgroup of $M(G)$ generated by the endomorphisms of G. Each of the sets $I(G)$, $A(G)$, $E(G)$ is closed under functional composition; so $(I(G), \cdot, \circ)$, $(A(G), \cdot, \circ)$, $(E(G), \cdot, \circ)$ are near-rings, and they are referred to as the *inner automorphism near-ring*, the *automorphism near-ring*, and the *endomorphism near-ring* of G (see [**Pil83**, §7], [**Mel85**, Chapter 10]).

3. The length of polynomials

The concept of *length* of a polynomial was introduced by S. D. Scott in [**Sco69**]. Let p be a polynomial (in the variety of all groups) in the variable x over the group G (cf. [**LN73**, p. 27]). We write p in the form $a_0 \mathsf{x}^{e_0} a_1 \mathsf{x}^{e_1} \cdots a_{n-1} \mathsf{x}^{e_{n-1}} a_n$, and define its *Scott-length* $\lambda(\mathsf{p})$ (cf. [**Sco69**, p. 251]) by

$$\lambda(\mathsf{p}) := \sum_{i=0}^{n-1} e_i.$$

For a polynomial p over G, let $\overline{\mathsf{p}}$ be the polynomial function induced by p on G. The *Scott-length of the group* G, denoted by $\lambda(G)$, is the smallest positive integer n such that there is a polynomial p with $\lambda(\mathsf{p}) = n$ and $\overline{\mathsf{p}}(x) = 1$ for all $x \in G$, and $\lambda(G)$ is defined to be 0 if no such n exists.

For example, if A is a finite abelian group, then we have $\lambda(A) = \exp(A)$. In [**Eck98**] we find examples of groups in which $\lambda(G) \neq \exp(G)$; actually from [**Sco69**, Proposition 3.4], we obtain that all finite, simple, non-abelian groups G satisfy $\lambda(G) = 1$.

We state those results of S. D. Scott's to which we will refer later.

Proposition 1.1 ([**Sco69**, Proposition 1.1]). *Let* p *be a polynomial of a group* G *such that* $\overline{\mathsf{p}}(x) = 1$ *for all* $x \in G$. *Then* $\lambda(G)$ *divides* $\lambda(\mathsf{p})$.

Proposition 1.2 ([**Sco69**, Theorem 1.2]). *Let* p *be a polynomial of a group* G *such that the function* $\overline{\mathsf{p}}$ *is bijective on* G. *Then* $\lambda(G)$ *and* $\lambda(\mathsf{p})$ *are relatively prime.*

Lemma 1.3. *Let* G *be a finite group. Then* $\exp(G/G')$ *divides* $\lambda(G)$, *and* $\exp(Z(G))$ *divides* $\lambda(G)$.

Proof: Straightforward. □

4. Counting polynomial functions

The observations gathered in the following lemma are quite elementary and will be used throughout this thesis without explicit reference.

Lemma 1.4. *Let* G *be a finite group. Then we have:*

(1) *Let* p *be a polynomial function on* G. *Then we have* $n \in \mathbb{N}$ *and* $a_1, \ldots, a_n, c \in G$ *such that*

$$p(x) = \prod_{i=1}^{n} x^{a_i} \cdot c \text{ for all } x \in G; \tag{1.1}$$

(2) $I(G) = \{p \in P(G) \mid p(1) = 1\}$;
(3) $|P(G)| = |I(G)| \cdot |G|$.

Proof: The assertions (2) and (3) follow from (1) immediately. For proving (1), we let $p \in P(G)$. By definition, we have $k \in \mathbb{N}$, $b_0, \ldots, b_k \in G$ and $e_0, \ldots, e_{k-1} \in \mathbb{Z}$ such that

$$p(x) = b_0 x^{e_0} b_1 x^{e_1} \cdots b_{k-1} x^{e_{k-1}} b_k \text{ for all } x \in G.$$

For $i \in \{1, \ldots, k\}$, we let $f_i \in \{1, \ldots, \exp G\}$ such that $f_i \equiv e_i$ modulo $\exp G$. Then we have

$$p(x) = b_0 x^{f_0} b_1 x^{f_1} \cdots b_{k-1} x^{f_{k-1}} b_k \text{ for all } x \in G.$$

Let $n := \sum_{i=0}^{k} f_i$. Since all exponents f_i are positive, we can find $d_0, \ldots, d_n \in G$ such that

$$p(x) = d_0 x d_1 x d_2 \cdots d_{n-1} x d_n \text{ for all } x \in G.$$

Hence we have

$$p(x) = d_0 x (d_0)^{-1} (d_0 d_1) x (d_0 d_1)^{-1} \cdots (d_0 \cdots d_{n-1}) x (d_0 \cdots d_{n-1})^{-1} (d_0 \cdots d_n)$$

for all $x \in G$. We define $a_i := (\prod_{j=0}^{i} d_j)^{-1}$ for $i \in \{1, \ldots, n\}$ and $c := d_0 \cdots d_n$. Then $p(x)$ has the form that is given in (1.1). The lemma is proved. □

Let G be a group with a normal subgroup N, and let T be a subgroup of $M(G)$. We define the *Noetherian quotient*

$$(N : G)_T := \{f \in T \mid f(G) \subseteq N\}.$$

Lemma 1.5. *Let G be a finite group, and let N be a normal subgroup of G. Then we have*

$$|I(G)| = |I(G/N)| \cdot |(N : G)_{I(G)}|.$$

Proof: This is an immediate consequence of the following Lemma 1.6 since all inner automorphisms of G/N are induced by inner automorphisms of G (see (1.5) in Section 5). □

We will use the next lemma for $S = \mathrm{Inn}\,(G), \mathrm{Aut}\,(G)$, or $\mathrm{End}(G)$, and hence $T = I(G)$, $A(G)$, or $E(G)$, where N is a normal, characteristic, or fully invariant subgroup of G.

Lemma 1.6. *Let G be a group, and let N be a normal subgroup of G. Let S be a set of endomorphisms of G such that $\alpha(N) \subseteq N$ for all $\alpha \in S$, and let $T := \langle S \rangle$. Then we have:*

1. *$f(N) \subseteq N$ for all $f \in T$;*
2. *The function $\bar{f} : G/N \to G/N$, $xN \mapsto f(x)N$, is well-defined, and $\bar{f}$ is an element of $E(G/N)$ for all $f \in T$;*
3. *The map $\varphi : T \to E(G/N)$, $f \mapsto \bar{f}$ (with $\bar{f}$ as in* (2)*), is a homomorphism with kernel $(N : G)_T$.*

Proof: We let $f \in T$. Then we have $n \in \mathbb{N}$, $e_1, \dots, e_n \in \{-1, 1\}$, and we have endomorphisms $\alpha_1, \dots, \alpha_n \in S$ such that

$$f(x) = \alpha_1^{e_1}(x) \cdots \alpha_n^{e_n}(x) \text{ for all } x \in G.$$

Now (1) follows from the assumption that $\alpha(N) \subseteq N$ for all $\alpha \in S$.

To show that $\bar{f}$ in (2) is well-defined, we let $x, y \in G$ such that $xN = yN$. For $\alpha \in S$, we use the linearity of α and the invariance of N to obtain

$$\alpha(x)N = N\alpha(y).$$

This yields

$$\alpha_1^{e_1}(x) \cdots \alpha_n^{e_n}(x)N = N\alpha_1^{e_1}(y) \cdots \alpha_n^{e_n}(y).$$

Hence we have $f(x)N = f(y)N$. Thus $\bar{f}$ is well-defined on G/N. Since $\bar{\alpha} \in E(G/N)$ for all $\alpha \in S$, we also have $\bar{f} \in E(G/N)$.

That φ is a homomorphism follows from $\overline{\alpha \cdot \beta} = \bar{\alpha} \cdot \bar{\beta}$ and $\overline{\alpha^{-1}} = \bar{\alpha}^{-1}$ for all $\alpha, \beta \in S$. Then $\mathrm{Ker}(\varphi) = (N : G)_T$ is immediate. The lemma is proved. □

The next lemma allows us to obtain information on endomorphism near-rings on G from the endomorphism near-rings on certain factors of G.

LEMMA 1.7. *Let G be a finite group, and let M, N be normal subgroups of G. We assume that M and N have relatively prime orders. Then we have the following:*

1. *The size of $I(G)$ is given by*
$$|I(G)| = \frac{|I(G/M)| \cdot |I(G/N)|}{|I(G/(MN))|}.$$
2. *If M, N are characteristic and $A(G/M) = I(G/M)$, $A(G/N) = I(G/N)$, $A(G/MN) = I(G/MN)$, then $A(G) = I(G)$.*
3. *If M, N are fully invariant and $E(G/M) = I(G/M)$, $E(G/N) = I(G/N)$, $E(G/MN) = I(G/MN)$, then $E(G) = I(G)$.*

We will prove Lemma 1.7 after the following Lemma 1.8. We point out that the assumption $\gcd(|M|, |N|) = 1$ is only used twice in the proofs of these lemmas. First to obtain $M \cap N = \{1\}$. Second to show that the projection π_M from MN to M is a polynomial function on MN (see (1.3)). Thus the Lemmas 1.7 and 1.8 may be generalized by replacing the hypothesis $\gcd(|M|, |N|) = 1$ by the 2 assumptions $M \cap N = \{1\}$ and $\pi_M \in I(MN)$.

LEMMA 1.8. *Let G be a group, and let $T = I(G), A(G)$, or $E(G)$. Let M, N be subgroups of G such that $T(M) \subseteq M, T(N) \subseteq N$, and $\gcd(|M|, |N|) = 1$. Then we have*

$$(MN : G)_T = (M : G)_T \cdot (N : G)_T, \tag{1.2}$$

and this product is direct.

Proof: We note that $M \cap N = \{1\}$ by assumption. Hence $H := MN$ is a direct product. The inclusion "$\supseteq$" of (1.2) is obvious. In order to prove "$\subseteq$", we consider the projections $\pi_M : H \to M$ and $\pi_N : H \to N$ that are defined by

$$\pi_M(xy) = x,\ \pi_N(xy) = y \text{ for all } x \in M, y \in N.$$

First we prove

$$\pi_M, \pi_N \in I(H). \tag{1.3}$$

Let $k \in \mathbb{Z}$ such that $k \equiv 1 \mod |M|$ and such that $|N|$ divides k. For $x \in M, y \in N$, we then have $(xy)^k = x$. Hence π_M is in $I(H)$. By $(xy)^{-k}xy = y$ for all $x \in M, y \in N$, we find $\pi_N \in I(H)$. Hence we have (1.3).

Let $f \in (H : G)_T$. By (1.3) and $I(G) \subseteq T$, we have $\pi_M \circ f \in (M : G)_T$ and $\pi_N \circ f \in (N : G)_T$. Together with $f(x) = \pi_M(f(x)) \cdot \pi_N(f(x))$ for all $x \in G$, this yields (1.2).

By $(M : G)_T \cap (N : G)_T = (M \cap N : G)_T$ and $M \cap N = \{1\}$, the product in (1.2) is direct. □

Proof of Lemma 1.7: Let G, M, N satisfy the assumptions of the lemma, and let $H := MN$. First we show (1). By Lemma 1.8, we have

$$|(H : G)_{I(G)}| = |(M : G)_{I(G)}| \cdot |(N : G)_{I(G)}|.$$

By Lemma 1.5, we have $|I(G)| = |(H : G)_{I(G)}| \cdot |I(G/H)|$. Hence we obtain $|I(G)| = |(M : G)_{I(G)}| \cdot |(N : G)_{I(G)}| \cdot |I(G/H)|$. After multiplying this equation by $|I(G/M)| \cdot |I(G/N)|$, we find

$$|I(G)| \cdot |I(G/M)| \cdot |I(G/N)| = |I(G)|^2 \cdot |I(G/H)|.$$

Now (1) follows.

For (2), we assume that M, N are characteristic and $A(G/K) = I(G/K)$ for $K \in \{M, N, H\}$. From Lemma 1.6 we obtain

$$|I(G/K)| \leq \frac{|A(G)|}{|(K : G)_{A(G)}|} \leq |A(G/K)|.$$

Hence we have $|A(G)| = |(K : G)_{A(G)}| \cdot |I(G/K)|$ for all $K \in \{M, N, H\}$. By Lemma 1.8, we have

$$|(H : G)_{A(G)}| = |(M : G)_{A(G)}| \cdot |(N : G)_{A(G)}|.$$

Multiplying this equation by $|A(G/M)| \cdot |A(G/N)|$ yields

$$|A(G)| \cdot |I(G/M)| \cdot |I(G/N)| = |A(G)|^2 \cdot |I(G/H)|.$$

Then we find $|I(G)| = |A(G)|$ by (1). Item (2) is proved. The proof of (3) follows that of (2). □

5. Polynomial automorphisms and endomorphisms

Let G be a group. We note that $I(G) = A(G)$ holds if and only if every automorphism of G is a polynomial function of G, and $I(G) = E(G)$ if and only if every endomorphism is polynomial (cf. [**Kow91**]; see [**Pet99**] for groups that satisfy $I(G) < A(G) = E(G)$). We give straightforward necessary conditions such that $I(G) = A(G)$, $I(G) = E(G)$, respectively.

PROPOSITION 1.9. *Let G be a group.*

(1) *If $I(G) = A(G)$, then all normal subgroups of G are characteristic.*
(2) *If $I(G) = E(G)$, then all normal subgroups of G are fully-invariant.*

Proof: This follows immediately from Lemma 1.6 (1). □

For a finite abelian group, the endomorphisms that fix all (normal) subgroups are polynomial functions by the next lemma. Later on, we will give another class of groups that have this property (see Lemma 3.8).

LEMMA 1.10. *Let H be a finite abelian group, and let α be an endomorphism of H such that α fixes all subgroups of H. Then there is an integer a such that*

$$\alpha(x) = x^a \text{ for all } x \in H. \tag{1.4}$$

Proof: Since H is abelian, we have $n \in \mathbb{N}$ and cyclic subgroups $H_1, \ldots, H_n$ of H such that the product $H = H_1 \ldots H_n$ is direct. Let x_i be a generator of H_i for $i \in \{1, \ldots, n\}$. By assumption, α fixes the cyclic subgroup of H that is generated by $\prod_{i=1}^n x_i$. Hence we have $a \in \mathbb{Z}$ such that $\alpha(\prod_{i=1}^n x_i) = (\prod_{i=1}^n x_i)^a = \prod_{i=1}^n x_i^a$. Since α is an endomorphism, we also have $\alpha(\prod_{i=1}^n x_i) = \prod_{i=1}^n \alpha(x_i)$. Now $\alpha(x_i) \in H_i$ and $H_i \cap \prod_{j=1, j \neq i}^n H_j = \{1\}$ yield $\alpha(x_i) = x_i^a$ for all $i \in \{1, \ldots, n\}$. Thus we obtain (1.4). □

Let N be a normal subgroup of G, and let α be an endomorphism of G such that $\alpha(N) \subseteq N$. Then the function

$$\bar{\alpha} : G/N \to G/N, \; xN \mapsto \alpha(x)N, \tag{1.5}$$

is well-defined and an endomorphism of G/N. We say that α *induces* the endomorphism $\bar{\alpha}$ on G/N. If α is in $I(G)$, then we have $\bar{\alpha} \in I(G/N)$. However, we note that $I(G) = E(G)$ does not imply $I(G/N) = E(G/N)$ in general. There may be endomorphisms of the factor G/N that are not induced by endomorphisms of G. The next result shows that $I(G/N) = E(G/N)$ is necessary if G splits over N (cf. Theorem 2.17).

PROPOSITION 1.11. *Let G be a finite group, and let $Z := Z(G)$. Let N be a normal subgroup of G, and let H be a complement for N in G. We assume that $I(G) = E(G)$. Then we have the following:*

(1) *$Z = (H \cap Z) \cdot (N \cap Z)$ is a direct product;*
(2) *$\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$;*
(3) *$I(G/N) = E(G/N)$.*

Proof: Let G, N, and H satisfy the hypotheses. We consider the projection α from G to H that is defined by

$$\alpha(nh) := h \text{ for all } n \in N, \text{ for all } h \in H.$$

First we prove (1). By $\alpha(G) = H$ and $\alpha \in I(G)$, we have

$$\alpha(Z) \subseteq H \cap Z. \tag{1.6}$$

The homomorphism theorem together with $\mathrm{Ker}(\alpha) = N$ yields that $\alpha(Z)$ is isomorphic to $Z/(N \cap Z)$. By (1.6), we then obtain $|Z| \leq |H \cap Z| \cdot |N \cap Z|$. Since $(H \cap Z)(N \cap Z) \subseteq Z$ and $N \cap H$ is trivial, this yields $Z = (H \cap Z)(N \cap Z)$. Thus (1) is proved.

Next we prove (2). By assumption, we have $k \in \mathbb{N}_0$ and $a_1, \dots, a_k \in G$ such that

$$\alpha(x) = \prod_{i=1}^{k} x^{a_i} \text{ for all } x \in G.$$

By the definition of α, we have

$$h^{-1} \cdot \prod_{i=1}^{k} h^{a_i} = 1 \text{ for all } h \in H.$$

Hence Proposition 1.1 yields that

$$\lambda(H) \text{ divides } k - 1. \tag{1.7}$$

Since $\alpha(z) = z^k$ for all $z \in Z$ and $N \cap Z \subseteq \operatorname{Ker}(\alpha)$, we have that

$$\exp(N \cap Z) \text{ divides } k. \tag{1.8}$$

We note that $\exp(Z)$ divides $\exp(N \cap Z) \cdot \exp(Z/(N \cap Z))$. Together with (1.7) and (1.8), this yields

$$\gcd(\lambda(H), \exp(Z)) \leq \gcd(k-1, k \cdot \exp(Z/(N \cap Z))) \leq \exp(Z/(N \cap Z)). \tag{1.9}$$

Since $H \cap Z$ is a subgroup of $Z(H)$ and since $\exp(Z(H))$ divides $\lambda(H)$, we have that $\exp(H \cap Z)$ divides $\lambda(H)$. By (1), $H \cap Z$ is isomorphic to $Z/(N \cap Z)$. Thus we obtain

$$\exp(Z/(N \cap Z)) \leq \gcd(\lambda(H), \exp(Z)).$$

Together with (1.9), this yields $\gcd(\lambda(H), \exp(Z)) = \exp(Z/(N \cap Z))$. Now (2) follows since H is isomorphic to G/N.

For proving (3), we let β be an endomorphism of H. Then the composition $\beta \circ \alpha$ is an endomorphism of G. Since $N \subseteq \operatorname{Ker}(\beta \circ \alpha)$, we may define the induced endomorphism,

$$\overline{\beta \circ \alpha} : G/N \to G/N, \ xN \mapsto \beta(\alpha(x))N.$$

First we will show that

$$\varphi : \operatorname{End}(H) \to \operatorname{End}(G/N), \ \beta \mapsto \overline{\beta \circ \alpha}$$

is a bijection. Let β, γ be endomorphisms of H such that $\overline{\beta \circ \alpha} = \overline{\gamma \circ \alpha}$. Let $h \in H$ be fixed. Then we have $\beta(\alpha(h))N = \gamma(\alpha(h))N$. Since the restriction of α to H is the identity map, this yields $\beta(h)N = \gamma(h)N$. Now $\gamma(h)^{-1} \cdot \beta(h)$ is in $N \cap H$. Since $N \cap H$ is trivial, we have $\beta(h) = \gamma(h)$. Thus $\beta = \gamma$, and φ is injective. Since H and G/N are isomorphic, we have $|\operatorname{End}(H)| = |\operatorname{End}(G/N)|$. Thus φ is bijective.

Now it suffices to prove

$$\overline{\beta \circ \alpha} \in I(G/N) \text{ for all } \beta \in \operatorname{End}(H). \tag{1.10}$$

Since $\beta \circ \alpha$ is an endomorphism of G, we have $k \in \mathbb{N}_0$ and $a_1, \ldots, a_k \in G$ such that

$$\beta(\alpha(x)) = \prod_{i=1}^{k} x^{a_i} \text{ for all } x \in G.$$

We write $\bar{x} := xN$ for $x \in G$. Then we have

$$\overline{\beta \circ \alpha}(\bar{x}) = \prod_{i=1}^{k} \bar{x}^{\overline{a_i}} \text{ for all } \bar{x} \in G/N$$

This proves (1.10). Thus we have (3), and the proof of the proposition is complete. □

We note that, under the hypotheses of the previous proposition, $\lambda(G/N)$ and $\exp(Z)$ are relatively prime if $I(G) = E(G)$ and $H \cap Z$ is trivial (cf. Theorem 3.20).

The next observation will be used in the characterization of linear groups that satisfy $I(G) = E(G)$ in Chapter 4.

Lemma 1.12. *Let G be a finite group, and let α be an endomorphism of G. We assume $\alpha \in I(G)$ and $\alpha(G) \cap Z(G) = \{1\}$. Then we have $Z(G) \subseteq \mathrm{Ker}(\alpha)$.*

Proof: Let $Z := Z(G)$. By assumption, we have $\alpha(Z) \subseteq Z \cap \alpha(G) = \{1\}$. Thus we have $Z \subseteq \mathrm{Ker}(\alpha)$. □

For Lemma 1.8, we have already noted that for a direct product $G = MN$ of groups M, N of relatively prime order the projection onto each component is in $I(G)$. The next result by S. A. Syskin is far less obvious.

Lemma 1.13 ([**Sys95**, Theorem 2]). *Let G be a finite group with a normal subgroup N and a subgroup H such that $G = NH$ and* $\gcd(|N|, |H|) = 1$. *Let*

$$\pi : G \to H, nh \to h.$$

Then we have $\pi \in I(G)$.

In Chapter 5 we will use the following consequence of the previous lemma and a result by C. G. Lyons and G. L. Peterson.

Proposition 1.14. *Let G be a finite group, and let N be a normal subgroup of G such that* $\gcd(|N|, |G : N|) = 1$. *We assume that $I(N) = E(N)$. Then the following are equivalent:*

(1) *$I(G) = E(G)$;*
(2) *$I(G/N) = E(G/N)$.*

Proof: By the Schur-Zassenhaus Theorem [**Rob96**, 9.1.2], we have a complement H for N in G. Now (1) ⇒ (2) follows from Proposition 1.11. The converse is obtained from [**LP95**, Theorem 2.1] together with Lemma 1.13. □

6. Endomorphisms into the center and automorphisms

In general, the product of endomorphisms of a non-abelian group is not an endomorphism. Still we would like to mention an important special case when multiplying two endomorphisms yields an endomorphism again. Let ρ be an endomorphism from G into $Z(G)$, and let σ be an endomorphism of G. Then the function

$$\alpha : G \to G,\ x \mapsto \rho(x) \cdot \sigma(x)$$

is an endomorphism of G. Under certain conditions, α might even be bijective on G.

This simple observation yields a necessary condition for $I(G) = A(G)$ by considering endomorphisms into the center of a group (see Chapter 3, Section 5).

LEMMA 1.15. *Let G be a finite group, and let $Z := Z(G)$. Let L be a subgroup of G such that $G' \subseteq L$, L/G' is a cyclic direct factor in G/G', and* $\gcd(|L : G'|, \exp(Z))$ *does not divide* $\exp(L \cap Z)$. *Then we have the following:*

(1) *There exists an endomorphism from G to Z that is not in $I(G)$;*
(2) *There exists an endomorphism ρ from G to Z such that $\bar\rho$, the induced endomorphism on G/G', is not in $I(G/G')$;*
(3) *$I(G) \neq A(G)$.*

Proof: Let G and L satisfy the assumptions of the lemma. First we will give a particular endomorphism ρ from G to Z that is not in $I(G)$ thus proving (1). Then we will obtain (2) by showing that this endomorphism ρ induces an endomorphism on G/G', which is not a polynomial function on G/G'. Finally we will use ρ to construct an automorphism that is not in $I(G)$ and hence prove (3).

For $x \in G$, we write $\bar{x} := xG'$, and for subgroups A of G, that contain G', we write $\bar{A} := A/G'$. By assumption, there is a prime p and an integer $n \geq 1$ such that $q := p^n$ divides $\gcd(\exp(\bar{L}), \exp(Z))$ and q does not divide $\exp(L \cap Z)$. Hence we have $c \in Z \setminus L$ with $\operatorname{ord} c = q$. By assumption, we have a subgroup H of G with $G' \subseteq H$ such that $\bar{H}$ is a direct complement for $\bar{L}$ in $\bar{G}$. Let $g \in G$ such that $\bar{g}$ generates $\bar{L}$. We note that $H\langle g^q \rangle$ is a normal subgroup of G with index q. Hence we have an endomorphism ρ from G to Z such that

$$\rho(g) = c \text{ and } \operatorname{Ker}(\rho) = H\langle g^q \rangle.$$

Since ρ does not fix L, which is a normal subgroup of G, we have $\rho \notin I(G)$. Hence (1) is proved.

For proving (2), we let $\bar\rho$ be induced on G/G' by that same endomorphism ρ as above. Then

$$\bar\rho(\bar{g}) = \bar{c}.$$

Since $c \notin L$ and $G' \subseteq L$, we have $\bar{c} \notin \bar{L}$. Hence $\bar\rho$ does not fix the normal subgroup $\bar{L}$ of $\bar{G}$. Thus $\bar\rho$ is not in $I(\bar{G})$. This proves (2).

For the proof of (3), we consider that same endomorphism ρ as above yet again. Let $C := \langle c \rangle$, and let $K := \mathrm{Ker}(\rho)$. First we assume that $C \cap K$ is not trivial. We will show that

$$\alpha : G \to G,\ x \mapsto \rho(x) \cdot x$$

is an automorphism and that $\alpha \notin I(G)$. Since $\rho(G) \subseteq Z$, the function α is an endomorphism of G. By the definition of ρ, we have $\mathrm{Ker}(\alpha) = \{x \in C \mid \rho(x) = x^{-1}\}$. Let $x \in C$ such that $\rho(x) = x^{-1}$. Since $|\langle \rho(x) \rangle| = |\langle x \rangle / (\langle x \rangle \cap K)|$, we then obtain $\langle x \rangle \cap K = \{1\}$. By the assumption that $C \cap K$ is not trivial, K contains the unique subgroup of order p of the cyclic p-group C. Hence $\langle x \rangle \cap K = \{1\}$ yields $x = 1$. Thus we have $\mathrm{Ker}(\alpha) = \{1\}$. Then α is an automorphism of G, and α is not in $I(G)$ because $\rho \notin I(G)$.

Next we will deal with the case that $C \cap K$ is trivial. Then we have $G = KC$ by the homomorphism theorem. We note that $G' = K'$ and that, by assumption, p divides $|L : (K'C) \cap L|$. In particular, p divides $|K : K'|$. Let $k \in K$, and let M be a subgroup of K with $K' \subseteq M$ such that $\bar{K}$ is the direct product of $\langle \bar{k} \rangle$ and $\bar{M}$. Furthermore, we assume that p divides $\mathrm{ord}\, \bar{k}$. Then we have an endomorphism σ from G to Z such that

$$\sigma(k) = c^{q/p} \text{ and } \mathrm{Ker}(\sigma) = M\langle k^p \rangle C.$$

Since σ does not fix the normal subgroup K of G, we have $\sigma \notin I(G)$. We now consider the function

$$\alpha : G \to G,\ x \mapsto \sigma(x) \cdot x.$$

Then α is an endomorphism of G because $\sigma(G) \subseteq Z$. We have $\mathrm{Ker}(\alpha) = \{x \in C \mid \sigma(x) = x^{-1}\}$. By $\mathrm{Im}(\sigma) \subseteq \mathrm{Ker}(\sigma)$, this yields $\mathrm{Ker}(\alpha) = \{1\}$. Thus α is an automorphism of G, and we have $\alpha \notin I(G)$ by $\sigma \notin I(G)$. The proof of (3) is complete. □

We will be interested in the following situation: Let G be a group with a normal subgroup N. We assume that an automorphism of N can be extended to an automorphism of G. What do the possible extensions look like?

For certain groups we can give an answer, and this answer uses endomorphisms into the center of G again. We will use the next lemma in particular for classical linear groups in Chapter 4. See also Proposition 3.15.

LEMMA 1.16. *Let A be a finite group, and let N be a normal subgroup of A. We write $C := C_A(N)$, $\bar{A} := A/C$, $\bar{N} := (NC)/C$, and $\bar{x} := xC$ for $x \in A$. We assume that $C_{\bar{A}}(\bar{N})$ is trivial, and that for all automorphisms φ of $\bar{N}$ there is $\bar{f} \in \bar{A}$ such that*

$$\varphi(\bar{n}) = \bar{n}^{\bar{f}} \text{ for all } \bar{n} \in \bar{N}.$$

Let G be a normal subgroup of A such that $N \subseteq G$ and $Z(G) = C \cap G$. Let α be an automorphism of G such that $\alpha(N) = N$.

Then there is $a \in A$, and there is an endomorphism $\rho : G \to C \cap G$ such that

$$\alpha(x) = \rho(x) \cdot x^a \text{ for all } x \in G.$$

Proof: We define an automorphism $\bar{\alpha}$ on $\bar{G} := (GC)/C$ by

$$\bar{\alpha}(xC) = \alpha(x)C \text{ for all } x \in G.$$

To check that $\bar{\alpha}$ is well-defined, we let $x, y \in G$ such that $xC = yC$. Then $y^{-1}x$ is an element of $C \cap G$. Since, by hypothesis, N is invariant under α, also the centralizer of N in G, that is $C \cap G$, is invariant under α. Thus we have $\alpha(y^{-1}x) \in C \cap G$. This yields $\alpha(x)C = \alpha(y)C$. Hence $\bar{\alpha}$ is well-defined. The definition immediately yields that $\bar{\alpha}$ is an automorphism on $\bar{G}$.

Since $\bar{\alpha}$ restricts to an automorphism on $\bar{N}$, we have $a \in A$ such that

$$\bar{\alpha}(\bar{n}) = \bar{n}^{\bar{a}} \text{ for all } \bar{n} \in \bar{N} \tag{1.11}$$

by hypothesis. Let $n \in N$ and $g \in G$ be fixed. By (1.11), we have

$$\bar{\alpha}(\bar{n}^{\bar{g}}) = \bar{\alpha}(\bar{n})^{\bar{\alpha}(\bar{g})} = \bar{n}^{\bar{a} \cdot \bar{\alpha}(\bar{g})}. \tag{1.12}$$

Since $\bar{n}^{\bar{g}}$ is in $\bar{N}$, we can evaluate the same expression as

$$\bar{\alpha}(\bar{n}^{\bar{g}}) = \bar{n}^{\bar{g}\bar{a}}. \tag{1.13}$$

By (1.12) and (1.13), we obtain that $\bar{a} \cdot \bar{\alpha}(\bar{g}) \cdot \bar{a}^{-1} \cdot \bar{g}^{-1}$ commutes with $\bar{n}$ for all $n \in N$, $g \in G$. Since $C_{\bar{A}}(\bar{N})$ is trivial by hypothesis, this yields

$$\bar{\alpha}(\bar{g}) = \bar{g}^{\bar{a}} \text{ for all } \bar{g} \in \bar{G}. \tag{1.14}$$

Now we prove that the function ρ on G defined by

$$\rho(x) = \alpha(x) \cdot (x^{-1})^a \text{ for all } x \in G$$

is an endomorphism from G to $C \cap G$. By (1.14) and by the hypothesis that G is normal in A, we have $\rho(G) \subseteq C \cap G$. For proving that ρ is a homomorphism, we let $x, y \in G$. By the hypothesis that $Z(G) = C \cap G$, we obtain $\alpha(x) \cdot \alpha(y) = \rho(x)x^a \cdot \rho(y)y^a = \rho(x)\rho(y) \cdot (xy)^a$. By comparing this with $\alpha(xy) = \rho(xy) \cdot (xy)^a$, we find $\rho(xy) = \rho(x) \cdot \rho(y)$. Hence ρ is an endomorphism. The lemma is proved. □

CHAPTER 2

Polynomial functions on certain non-solvable groups

We consider polynomial functions on those finite groups whose quotient by the center has a non-abelian unique minimal normal subgroup. The results obtained here will then be applied to linear groups in Chapter 4.

1. A characterization of polynomial functions

We present a criterion to decide whether a given function on a group is polynomial. The following lemma uses several ideas found in [**FK95**, Theorem 2.1] and [**Kow97**, Proposition 1].

LEMMA 2.1 ([**AM03**, Lemma 5.3]). *Let G be a finite group, let $Z := Z(G)$ be its center, and let N be a normal subgroup of G that satisfies the following properties:*

(C.1) *$N \neq \{1\}$ and $N' = N$;*

(C.2) *For all normal subgroups K of G we have $K \subseteq Z$ or $N \subseteq K$.*

Let $\lambda := \lambda(G/N)$ be the Scott-length of G/N. For a function $f : G \to N$, the following are equivalent:

(1) *The function f is in $I(G)$;*

(2) *There exists an integer μ such that $f(z) = z^{\lambda\mu}$ for all $z \in Z$, and we have*

$$f(g \cdot z) = f(g) \cdot f(z) \text{ for all } g \in G,\, z \in Z.$$

Proof: (1) ⇒ (2): Let p be a polynomial over G such that $\overline{\mathsf{p}} = f$. Then we have $\overline{\mathsf{p}}(G) \subseteq N$, and thus $\lambda(\mathsf{p})$ is a multiple of $\lambda(G/N)$. Since every polynomial p satisfies

$$\overline{\mathsf{p}}(g \cdot z) = \overline{\mathsf{p}}(g) \cdot z^{\lambda(\mathsf{p})} \text{ for all } z \in Z(G),\, g \in G,$$

we obtain condition (2).

(2) ⇒ (1): Let $k := |G : Z|$, and let $T = \{1, t_1, t_2, \ldots, t_{k-1}\}$ be a transversal for the cosets of Z in G. Let $f : G \to N$ be a function that satisfies (2). Then f is uniquely determined by μ such that $f(z) = z^{\lambda\mu}$ for all $z \in Z$, and by the values $f(t_1), \ldots, f(t_{k-1})$. We will show $f \in I(G)$ by proving that for all $\alpha \in \mathbb{Z}$ and for all $n_1, \ldots, n_{k-1} \in N$ there exists $p \in I(G)$ such that $p(z) = z^{\lambda\alpha}$ for all $z \in Z$, and $p(t_i) = n_i$ for all $i \in \{1, \ldots, k-1\}$. By (1) ⇒ (2), we will then obtain that there is some $p \in I(G)$ such that $p = f$. Hence f is in $I(G)$.

Step 1: We first construct a function $e \in I(G)$ that satisfies

$$e(G) \subseteq N \text{ and } e(z) = z^{\lambda} \text{ for all } z \in Z. \tag{2.1}$$

To construct e, we start with a polynomial p over G/N with $\overline{\mathsf{p}}(xN) = 1N$ for all $x \in G$, and $\lambda(\mathsf{p}) = \lambda(G/N)$. By lifting the coefficients of p from G/N to G, we obtain a polynomial p' with $\overline{\mathsf{p}'}(G) \subseteq N$ and $\lambda(\mathsf{p}') = \lambda$. Now the function $e : G \to G$ defined by $e(x) := (\overline{\mathsf{p}'}(1))^{-1} \cdot \overline{\mathsf{p}'}(x)$ satisfies the requirements of (2.1).

Step 2: By the assumptions (C.1) and (C.2), we have

$$N/(N \cap Z) \text{ is a non-abelian minimal normal subgroup of } G/(N \cap Z), \tag{2.2}$$

and

$$C_{G/(N \cap Z)}(N/(N \cap Z)) = Z/(N \cap Z). \tag{2.3}$$

Step 3: Let $S \subseteq T \setminus \{1\}$, let $s \in S$, and let $n \in N$. Then there exists $q \in I(G)$ such that

$$q(G) \subseteq N,$$
$$q(s) = n,$$
$$q(u) = 1 \text{ for all } u \in S, u \neq s,$$
$$q(z) = 1 \text{ for all } z \in Z.$$

For proving this statement, we use induction on $|S|$. First assume that $S = \{s\}$. For

$$Q := \{q(s) \mid q \in I(G), q(G) \subseteq N, \text{ and } q(z) = 1 \text{ for all } z \in Z\},$$

we have to prove $Q = N$. We note that Q is a normal subgroup of G. First we show

$$\exists n \in N \text{ such that } [s, n] \notin Z.$$

Otherwise, if $[s, n] \in Z$ for all $n \in N$, then $s(N \cap Z)$ centralizes $N/(N \cap Z)$. By (2.3), we then have $s \in Z$, which contradicts $s \in T \setminus \{1\}$. Now, let $n \in N$ such that $[s, n] \notin Z$, and let $q(x) := [x, n]$ for all $x \in G$. Then $q(G) \subseteq [G, N] \subseteq N$ and $q(z) = 1$ for all $z \in Z$. Hence $q(s) \in Q$ and $Q \not\subseteq Z$. By assumption (C.2), we then have $N \subseteq Q$. So $N = Q$, and the base case of the induction is proved.

Next, we assume that $|S| > 1$. Let $s \in S$. We consider

$$Q := \{q(s) \mid q \in I(G), q(G) \subseteq N, q(S \setminus \{s\}) = \{1\}, \text{ and } q(Z) = \{1\}\}.$$

For proving that the normal subgroup Q of G is equal to N, we show that $Q \not\subseteq Z$. Let $t \in S, t \neq s$, and let

$$M := \langle \{(s^{-1}t)^a \mid a \in G\} \rangle.$$

Then M is normal in G. Since $s^{-1}t \notin Z$, we have $M \not\subseteq Z$. So $N \subseteq M$. By the assumptions (C.1) and (C.2), there are $n_1, n_2 \in N$ such that $[n_1, n_2] \notin Z$. Since $n_1 \in M$, there is $l \in \mathbb{N}$ and there are $a_1, \ldots, a_l \in G$ such that $n_1 = \prod_{i=1}^{l} (s^{-1}t)^{a_i}$. We define $q_1(x) := \prod_{i=1}^{l} (x^{-1}t)^{a_i}$ for all $x \in G$.

By the induction hypothesis, there is $q_2 \in I(G)$ such that $q_2(G) \subseteq N, q_2(s) = n_2, q_2(u) = 1$ for all $u \in S \setminus \{s,t\}$, and $q_2(z) = 1$ for all $z \in Z$. We now have $q \in I(G)$ defined by $q(x) := [q_1(x), q_2(x)]$ which satisfies

$$q(G) \subseteq [G,N] \subseteq N,$$

$$q(t) = [1, q_2(t)] = 1,$$

$$q(u) = [q_1(u), 1] = 1 \text{ for all } u \in S \setminus \{s,t\},$$

$$q(Z) \subseteq [Z,Z] = \{1\}.$$

Thus $q(s) \in Q$. Since $q(s) = [n_1, n_2] \notin Z$, we have $Q \not\subseteq Z$ and $N \subseteq Q$. This completes the proof of Step 3.

Step 4: For $S = \{t_1, \ldots, t_{k-1}\}$, Step 3 yields that there exist the following "Lagrange interpolation functions". For each $i \in \{1, 2, \ldots, k-1\}$ and for each $n \in N$, there is $q_n^{(i)} \in I(G)$ such that

$$q_n^{(i)}(G) \subseteq N,$$

$$q_n^{(i)}(t_i) = n,$$

$$q_n^{(i)}(t_j) = 1 \text{ for all } j \in \{1, 2, \ldots, k-1\} \setminus \{i\},$$

$$q_n^{(i)}(z) = 1 \text{ for all } z \in Z.$$

We recall that $f : G \to N$ is a function that satisfies $f(z) = z^{\lambda\mu}$ for all $z \in Z$ and $f(gz) = f(g) \cdot f(z)$ for all $g \in G$, $z \in Z$. We define $p \in I(G)$ by

$$p(x) := e(x)^{\mu} \cdot \prod_{i=1}^{k-1} q^{(i)}_{e(t_i)^{-\mu} \cdot f(t_i)}(x) \text{ for } x \in G.$$

Then we have $f|_Z = p|_Z$ and $f(t_i) = p(t_i)$ for all $i \in \{1, \ldots, k-1\}$. We note that p satisfies $p(gz) = p(g) \cdot p(z)$ for all $g \in G$, $z \in Z$ by (1) ⇒ (2) of Lemma 2.1. To prove $p = f$, we fix $x \in G$. Then there exists $i \in \{0, 1, \ldots, k-1\}$ and there exists $z \in Z$ such that $x = t_i z$. We compute

$$f(x) = f(t_i z) = f(t_i) \cdot f(z) = p(t_i) \cdot p(z) = p(t_i z) = p(x).$$

This implies $p = f$. Hence $f \in I(G)$. □

Before we state consequences of Lemma 2.1 in the following sections, we investigate the structure of groups that satisfy the assumptions (C.1) and (C.2) of this result.

2. A description of groups with property (C)

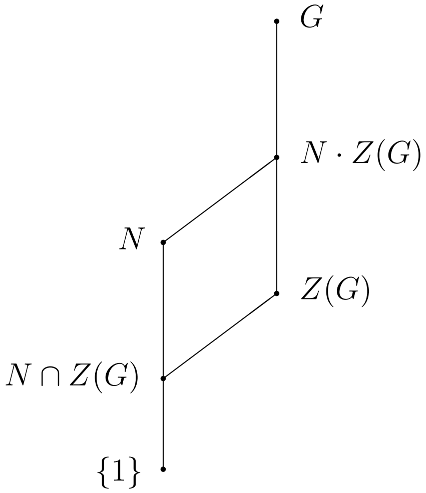
Let N be a normal subgroup of the group G such that the following properties are satisfied:

(C.1) $N \neq \{1\}$ and $N' = N$;
(C.2) For all normal subgroups K of G we have $K \subseteq Z(G)$ or $N \subseteq K$.

Then we say that N *satisfies* (C.1) *and* (C.2) *in* G.

We say that G *has property* (C) if there exists a normal subgroup N of G such that N satisfies (C.1) and (C.2) in G.

The next figure shows part of the lattice of normal subgroups of such a group G. By (C.2), any normal subgroup of G is central or contains N. In particular, there is no normal subgroup K of G with $N \cap Z(G) < K < N$ or $Z(G) < K < N \cdot Z(G)$.



As we will prove in Lemma 2.2, there is at most one normal subgroup N of G that satisfies (C.1) and (C.2) in G. Thus, if G has property (C), then the normal subgroup N that satisfies (C.1) and (C.2) is uniquely determined.

The class of groups with property (C) contains non-abelian simple groups, groups that have a non-abelian unique minimal normal subgroup (for example finite symmetric groups of degree at least 5), and quasisimple groups. A group G is called *quasisimple* if and only if $G' = G$ and $G/Z(G)$ is simple [**Suz86**, p. 446, Definition 6.1].

The finite classical linear and semi-linear groups provide a variety of examples with property (C) (see Chapter 4 and Appendix A). These are the groups for which Lemma 2.1 was made. Here we only want to mention that for every non-solvable finite general linear group $G := \mathrm{GL}(n, q)$, the special linear group $\mathrm{SL}(n, q)$ satisfies (C.1) and (C.2) in G.

We now give a list of properties that are equivalent to (C).

LEMMA 2.2. *Let G be a group, and let N be a normal subgroup of G. We write $Z := Z(G)$. Then the following are equivalent:*

(1) *N satisfies* (C.1) *and* (C.2) *in G.*

(2) *N is the unique normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G.*

(3) *N satisfies the following:*
   (a) *$N' = N$;*
   (b) *$N \cap Z \prec_G N$;*
   (c) *$C_G(N) = Z$.*

(4) *N satisfies the following:*
   (a) *$N' = N$;*
   (b) *$(NZ)/Z$ is a minimal normal subgroup of G/Z;*
   (c) *$C_{G/Z}((NZ)/Z)$ is trivial.*

(5) *N satisfies the following:*
   (a) *$N' = N$;*
   (b) *$(NZ)/Z$ is the unique minimal normal subgroup of G/Z.*

(6) *There exists a normal subgroup M of G such that $N = M'$ and the following are satisfied:*
   (a) *$Z \subseteq M$;*
   (b) *M/Z is a minimal normal subgroup of G/Z;*
   (c) *$C_{G/Z}(M/Z)$ is trivial.*

(7) *There exists a normal subgroup M of G such that $N = M'$ and the following are satisfied:*
   (a) *$Z \subseteq M$;*
   (b) *M/Z is the unique minimal normal subgroup of G/Z.*
   (c) *M/Z is non-abelian;*

By the equivalence of (1) and (7) in Lemma 2.2, a group G has property (C) if and only if $G/Z(G)$ has a non-abelian unique minimal normal subgroup.

We note that usually condition (3) is the one that is most convenient to check in order to determine whether a given normal subgroup N satisfies (C.1) and (C.2) in G.

Proof of Lemma 2.2: (1) ⇒ (2): We assume that N_1 and N_2 are normal subgroups of G that both satisfy (C.1) and (C.2) in G. By (C.1), we have $N_1 \not\subseteq Z$ and $N_2 \not\subseteq Z$. Thus (C.2) yields $N_1 \subseteq N_2$ and $N_2 \subseteq N_1$. Hence we have $N_1 = N_2$, and (2) is proved.

(2) ⇒ (3): We assume that N satisfies (C.1) and (C.2) in G. As a part of (C.1), condition (3a) is obviously satisfied. Since, by (C.1), N is not abelian, we have $N \cap Z < N$. We suppose that there is a normal subgroup K of G with $N \cap Z < K < N$. Then $K \subseteq Z$ by (C.2), and hence $K \subseteq N \cap Z$, which contradicts our assumption that $N \cap Z < K$. Thus we have (3b). Since $N \subseteq C_G(N)$ implies

$N' = \{1\}$, which contradicts (C.1), condition (C.2) yields $C_G(N) \subseteq Z$. The converse inclusion is obvious, and (3c) is proved.

(3) ⇒ (4): We assume that (3) holds for N. Condition (4a) is (3a). Since, by (3b), $N/(N \cap Z)$ is a minimal normal subgroup in $G/(N \cap Z)$, the homomorphism theorem yields that $(NZ)/Z$ is a minimal normal subgroup in G/Z. Thus we have (4b). For proving (4c), we let K be a normal subgroup of G with $Z \subseteq K$ such that $K/Z = C_{G/Z}((NZ)/Z)$. Then we have $[K, N] \subseteq Z$, which implies that $[K, N, N]$ and $[N, K, N]$ are trivial. The Three Subgroup Lemma (see [**Rob96**, p.122, 5.1.10]) yields that $[N, N, K]$ is trivial as well. By using (4a), we obtain $\{1\} = [N, N, K] = [N', K] = [N, K]$. Thus K centralizes N, and, by (3c), we have $K \subseteq Z$. Item (4c) is proved.

(4) ⇒ (5): We assume that (4) holds for N. Condition (5a) is (4a). For proving (5b), we let K be a normal subgroup of G with $Z < K$ such that K/Z is a minimal normal subgroup of G/Z. By (4c), $[(NZ)/Z, K/Z]$ is not trivial. Thus $[(NZ)/Z, K/Z] \subseteq (NZ)/Z$ and (4b) yield $(NZ)/Z = [(NZ)/Z, K/Z]$. Since $[(NZ)/Z, K/Z] \subseteq K/Z$ and K/Z is minimal, we then obtain $(NZ)/Z = K/Z$. Thus (5b) is proved.

(5) ⇒ (6): We assume that (5) holds for N. Let $M := NZ$. Then we have $M' = N'$ and, by (5a),

$$M' = N. \tag{2.4}$$

Conditions (6a) and (6b) are satisfied by the definition of M and by (5b). Seeking a contradiction, we suppose that $C_{G/Z}(M/Z)$ is non-trivial. Then we have $M/Z \subseteq C_{G/Z}(M/Z)$ by (5b). Thus the derived subgroup of M/Z is trivial, which yields $M' \subseteq Z$. With (2.4), we now obtain $N \subseteq Z$ and $M \subseteq Z$. This contradicts (6b). Hence $C_{G/Z}(M/Z)$ is trivial.

(6) ⇒ (7): Let M be a normal subgroup of G that satisfies (6). Then we have $M' = N$, $Z \subseteq M$, and that M/Z is a minimal normal subgroup in G/Z by assumption. Furthermore, by (6c), M/Z is non-abelian. It only remains to prove that M/Z is the unique minimal normal subgroup of G/Z. The argument is the same as in the proof of (4) ⇒ (5). Let K be a normal subgroup of G with $Z < K$ such that K/Z is a minimal normal subgroup of G/Z. By (6c), $[M/Z, K/Z]$ is not trivial. Then the minimality of M/Z and of K/Z yields $M/Z = [M/Z, K/Z] = K/Z$. Thus we have (7).

(7) ⇒ (1): Let M be a normal subgroup of G that satisfies (7) with $N = M'$. First we prove that N satisfies (C.1). By (7b) and (7c), we have $(M/Z)' = M/Z$. This yields $M'Z = M$. Hence we have $M'' = M'$ and $N' = N$. By (7c), M is not abelian. Thus $N \neq \{1\}$, and N satisfies (C.1). For proving (C.2), we let K be a normal subgroup of G, and we consider $X := (KZ) \cap M$. Since $Z \subseteq X \subseteq M$, property (7b) yields that either $X = M$ or $X = Z$. If $X = M$, then we have $K \supseteq K' = (KZ)' \supseteq M' = N$. Next we consider the case $X = Z$. By $[KZ, M] \subseteq$

X, we then obtain that $(KZ)/Z$ centralizes M/Z. We suppose that $(KZ)/Z$ is not trivial. Then we have $M/Z \subseteq (KZ)/Z$ by (7b) and $M/Z \subseteq C_{G/Z}(M/Z)$, which contradicts (7c). Hence $(KZ)/Z$ is trivial and $K \subseteq Z$. Condition (C.2) is satisfied. □

It is easy to see that the class of groups with property (C) is closed under certain homomorphic images and central extensions:

Lemma 2.3. *Let G be a group, and let Y be a subgroup of $Z(G)$. Then the following are equivalent:*

(1) *G has property* (C)*;*
(2) *G/Y has property* (C) *and $Z(G/Y) = Z(G)/Y$.*

Proof: Let G be a group, let $Z := Z(G)$, and let Y be a subgroup of Z.

(1) ⇒ (2): We assume that G has property (C). By Lemma 2.2, (1) ⇒ (6), we have a normal subgroup M of G with $Z \subseteq M$ such that M/Z is a minimal normal subgroup of G/Z and $C_{G/Z}(M/Z)$ is trivial.

First we prove $Z(G/Y) = Z/Y$. By $Z/Y \subseteq Z(G/Y)$, we have a normal subgroup K of G with $Z \subseteq K$ such that $K/Y = Z(G/Y)$. But $[M, K] \subseteq Y$ and $Y \subseteq Z$ yield that K/Z centralizes M/Z. Hence K/Z is trivial, and we have $Z(G/Y) = Z/Y$.

Now the homomorphism theorem yields that M/Y satisfies the conditions (6a), (6b), and (6c) of Lemma 2.2 for the group G/Y with center Z/Y. By Lemma 2.2, (6) ⇒ (1), G/Y has property (C).

(2) ⇒ (1): We assume that G/Y has property (C) and $Z(G/Y) = Z/Y$. By Lemma 2.2, (1) ⇒ (7), we have a normal subgroup M of G such that $Z/Y \subseteq M/Y$, that $(M/Y)/(Z/Y)$ is the unique minimal normal subgroup of $(G/Y)/(Z/Y)$, and that $(M/Y)/(Z/Y)$ is non-abelian. The homomorphism theorem yields that $Z \subseteq M$, that M/Z is the unique minimal normal subgroup of G/Z, and that M/Z is non-abelian. Hence G has property (C) by Lemma 2.2, (7) ⇒ (1). □

Obviously the class of groups with property (C) is not closed under taking direct products. Neither is property (C) inherited by all subgroups. Even if N satisfies (C.1) and (C.2) in a group G and if H is subgroup of G with $N \subseteq H$, in general N does not satisfy (C.1) and (C.2) in H as is shown by the following example.

Example 2.4. Let $N := A_5 \times A_5$ be the direct product of the alternating group of degree 5 by itself. Let i be an involution that acts on N by $(x, y)^i = (y, x)$ for all $(x, y) \in N$. We consider the semidirect product $G := N \rtimes \langle i \rangle$ defined by this action of $\langle i \rangle$ on N. Then N is a minimal normal subgroup of G with trivial centralizer. By Lemma 2.2, (6) ⇒ (1), the group G has property (C). Still N does not have property (C), since $Z(N)$ is trivial, and $A_5 \times \{()\}$, $\{()\} \times A_5$ are two distinct minimal normal subgroups of N (cf. Lemma 2.2, (1) ⇒ (7)). Here $()$ denotes the identity of A_5.

In the example above $(N \cdot Z(G))/Z(G)$ does not have property (C), because it is not simple. In the following lemma we prevent this flaw.

Lemma 2.5. *Let G be a group, and let N be a normal subgroup of G such that N satisfies* (C.1) *and* (C.2) *in G. We assume that $(N \cdot Z(G))/Z(G)$ is simple. Let H be a subgroup of G with $N \subseteq H$. Then we have:*

1. *$Z(H) = Z(G) \cap H$;*
2. *For all normal subgroups K of H, we have $K \subseteq Z(H)$ or $N \subseteq K$;*
3. *H has property* (C)*.*

Proof: Let G, N, and H satisfy the assumptions. By Lemma 2.2 (3c), we have

$$Z(G) = C_G(N). \tag{2.5}$$

Together with

$$Z(G) \cap H \subseteq Z(H) \subseteq C_G(N) \cap H,$$

this yields (1). For proving (2) and (3), we have to use the hypothesis that $(N \cdot Z(G))/Z(G)$ is simple. We consider (3) first. By Lemma 2.2, (3) ⇒ (1), it suffices to verify the following conditions:

$$N = N'; \tag{2.6}$$

$$N \cap Z(H) \prec_H N; \tag{2.7}$$

$$C_H(N) = Z(H). \tag{2.8}$$

Item (2.6) is true by assumption. From $N \subseteq H$ and $Z(H) = Z(G) \cap H$ we obtain $Z(H) \cap N = Z(G) \cap N$. Since $N/(Z(G) \cap N)$ is simple by assumption, we have (2.7). Equation (2.8) follows immediately from (2.5). Hence H has property (C). Item (3) of the lemma is proved. Thus we have (2) as well. □

A group T is said to be *almost simple* if there is a simple non-abelian group S and an embedding φ from T into $\operatorname{Aut} S$ such that $\operatorname{Inn} S \subseteq \varphi(T)$ [**KL90**, p.1]. We note the following:

Lemma 2.6. *A group T is almost simple if and only if T has a unique minimal normal subgroup and this subgroup is non-abelian simple.*

Thus, if $G/Z(G)$ is almost simple, then G has property (C) by Lemma 2.2, (7) ⇒ (1). We give the following reformulation of Lemma 2.5.

Lemma 2.7. *Let G be a group with center $Z := Z(G)$ such that G/Z is almost simple. Let M be the normal subgroup of G such that $Z \subseteq M$ and M/Z is the unique minimal normal subgroup of G/Z.*

Then all groups H with $M' \subseteq H \subseteq G$ have property (C).

Proof: We note that, by Lemma 2.6, the normal subgroup M that satisfies the assumptions of the lemma exists and that M is uniquely determined. Further M/Z is non-abelian simple, and M' satisfies (C.1) and (C.2) in G. Thus the result is given by Lemma 2.5 (3). □

We append the proof of the fact that every almost simple group has a non-abelian unique minimal normal subgroup.

Proof of Lemma 2.6: For proving the "if"-direction, we may assume that there exists a simple, non-abelian group S such that $\operatorname{Inn} S \subseteq T \subseteq \operatorname{Aut} S$. Since $\operatorname{Inn} S$ is isomorphic to S and normal in $\operatorname{Aut} S$, we have that $\operatorname{Inn} S$ is a minimal normal subgroup in T. It remains to show that this is the unique minimal normal subgroup. To this end, we prove

$$C_{\operatorname{Aut} S}(\operatorname{Inn} S) \text{ is trivial.} \tag{2.9}$$

Let $\alpha \in \operatorname{Aut} S$ such that α centralizes $\operatorname{Inn} S$. Then

$$\alpha(x^s) = \alpha(x)^s \text{ for all } x, s \in S$$

yields

$$\alpha(s) \cdot s^{-1} \in Z(S) \text{ for all } s \in S.$$

Since $Z(S) = \{1\}$ by assumption, we obtain $\alpha(s) = s$ for all $s \in S$. Hence α is the identity mapping on S, and (2.9) is proved.

For a non-trivial normal subgroup K of T, we then have $\{1\} < [K, \operatorname{Inn} S]$. Together with $[K, \operatorname{Inn} S] \subseteq K \cap \operatorname{Inn} S$ and the minimality of $\operatorname{Inn} S$, this yields $\operatorname{Inn} S \subseteq K$. Thus $\operatorname{Inn} S$ is the unique minimal normal subgroup of T.

For proving the converse implication, we let S be the non-abelian unique minimal normal subgroup of T. Since $S \not\subseteq C_T(S)$, we have $C_T(S) = \{1\}$. For each element $a \in T$, the function $\varphi_a : S \to S, x \mapsto x^a$, is an automorphism of S. Now

$$\varphi : T \to \operatorname{Aut} S,\ a \to \varphi_a,$$

is a homomorphism, and φ is injective by $C_T(S) = \{1\}$. Hence φ is an embedding of T into $\operatorname{Aut} S$ with $\operatorname{Inn} S \subseteq \varphi(T)$. Thus T is almost simple. The lemma is proved. □

3. Invariant subgroups

In this section we gather information on endomorphisms of groups with property (C) and related groups. First we show that the center of a group with property (C) is invariant under certain endomorphisms.

LEMMA 2.8. *Let G be a finite group such that $G/Z(G)$ is centerless. Let α be an endomorphism of G with* $\operatorname{Ker}(\alpha) \subseteq Z(G)$*. Then $\alpha(Z(G)) \subseteq Z(G)$.*

We note that by Lemma 2.2, (1) ⇒ (6), all groups with property (C) satisfy the hypotheses of the lemma above.

Proof of Lemma 2.8: Let $Z := Z(G)$. The homomorphism theorem yields:

$$\alpha(G)/\alpha(Z) \text{ is isomorphic to } G/Z. \tag{2.10}$$

Since G/Z is centerless by assumption, (2.10) implies that $Z(\alpha(G)) \subseteq \alpha(Z)$. The converse inclusion is immediate. Thus we obtain

$$Z(\alpha(G)) = \alpha(Z). \tag{2.11}$$

By the homomorphism theorem, we have

$$|Z \cdot \alpha(G)| \cdot |Z \cap \alpha(G)| = |\alpha(G)| \cdot |Z|. \tag{2.12}$$

The right hand side of (2.12) is $\frac{|G|}{|\operatorname{Ker}(\alpha)|} \cdot |Z|$. But $Z \cap \alpha(G) \subseteq Z(\alpha(G))$ and (2.11) yield that the left hand side of (2.12) is at most $|G| \cdot \frac{|Z|}{|\operatorname{Ker}(\alpha)|}$. Hence (2.12) implies $|Z \cap \alpha(G)| = \frac{|Z|}{|\operatorname{Ker}(\alpha)|}$, and thus $Z \cap \alpha(G) = Z(\alpha(G))$. By (2.11), we obtain $Z \cap \alpha(G) = \alpha(Z)$, which yields $\alpha(Z) \subseteq Z$. □

We note that the assumption $\operatorname{Ker}(\alpha) \subseteq Z(G)$ of the previous lemma cannot be omitted in general.

EXAMPLE 2.9. To illustrate this fact, we consider $G := A_5 \times \mathbb{Z}_2$, the direct product of the alternating group of degree 5 and the cyclic group of order 2. Let $()$ denote the identity of A_5. Then we have $Z(G) = \{()\} \times \mathbb{Z}_2$, and $G/Z(G)$ is centerless.

The function $\alpha : G \to G$ defined by $\alpha((x, 0)) := ((), 0)$ and $\alpha((x, 1)) := ((1, 2), 0)$ for $x \in A_5$ is an endomorphism of G with $\operatorname{Ker}(\alpha) = A_5 \times \{0\}$. We have $\operatorname{Ker}(\alpha) \not\subseteq Z(G)$, and $Z(G)$ is not invariant under α.

Unlike the center of a group with property (C), a normal subgroup N that satisfies (C.1) and (C.2) in G is invariant under all endomorphisms of G.

LEMMA 2.10. *Let G be a group, and let N be a normal subgroup of G such that N satisfies* (C.1) *and* (C.2) *in G. Then N is fully-invariant.*

This lemma yields in particular that for every endomorphism α of G, the induced function

$$\bar{\alpha} : G/N \to G/N,\ xN \mapsto \alpha(x)N,$$

is a well-defined endomorphism of G/N.

Proof of Lemma 2.10: Let α be an endomorphism of G. We will prove

$$\alpha(N) \subseteq N. \tag{2.13}$$

Let $Z := Z(G)$. By (C.2), we have either $\mathrm{Ker}(\alpha) \subseteq Z$ or $N \subseteq \mathrm{Ker}(\alpha)$. Since (2.13) is obvious for the latter case, it only remains to be proved under the assumption $\mathrm{Ker}(\alpha) \subseteq Z$. First we show

$$\alpha(N) \subseteq NZ \cap \alpha(G). \tag{2.14}$$

Since N satisfies (C.2) in G, the homomorphism theorem yields that every normal subgroup of $\alpha(G)$ is either contained in $\alpha(Z)$ or contains $\alpha(N)$. Obviously $NZ \cap \alpha(G)$ is normal in $\alpha(G)$. Hence we have $NZ \cap \alpha(G) \subseteq \alpha(Z)$ or (2.14). Seeking a contradiction, we suppose the former. From $|G| \geq |NZ\alpha(G)| = \frac{|NZ|\cdot|\alpha(G)|}{|NZ\cap\alpha(G)|}$ we obtain $|NZ \cap \alpha(G)| \geq \frac{|NZ|}{|\mathrm{Ker}(\alpha)|}$. By $\mathrm{Ker}(\alpha) \subseteq NZ$, we then have

$$|\alpha(NZ)| \leq |NZ \cap \alpha(G)|.$$

Together with our assumption $NZ \cap \alpha(G) \subseteq \alpha(Z)$, this yields $|\alpha(NZ)| \leq |\alpha(Z)|$ and consequently $|NZ| \leq |Z|$. Finally, we obtain $N \subseteq Z$, which contradicts (C.1), namely, $N' \neq \{1\}$. Thus (2.14) is proved.

Now, $\alpha(N) \subseteq NZ$ yields $\alpha(N') \subseteq N'$. By (C.1), we have $N' = N$. This completes the proof of (2.13) and of the lemma. □

4. Size of $I(G)$

The description of polynomial functions in Lemma 2.1 yields a formula for $|I(G)|$ for groups G that have property (C).

Theorem 2.11. *Let G be a finite group, let $Z := Z(G)$ be its center, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. Let $\lambda(G/N)$ be the Scott-length of G/N. Then we have*

$$|I(G)| = |I(G/N)| \cdot \frac{\exp(Z)}{\gcd(\exp(Z), \lambda(G/N))} \cdot |N|^{|G:Z|-1}.$$

We will state corollaries of this result for G/N abelian in Chapter 3, Section 2.

For the proof of Theorem 2.11, we first determine the size of the Noetherian quotient

$$(N : G)_{I(G)} := \{f \in I(G) \mid f(G) \subseteq N\}.$$

Lemma 2.12 ([**AM03**, cf. Lemma 5.2]). *Let G be a finite group, let $Z := Z(G)$, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. Let $\lambda := \lambda(G/N)$. Then we have*

$$|(N : G)_{I(G)}| = \frac{\exp(Z)}{\gcd(\exp(Z), \lambda)} \cdot |N|^{|G:Z|-1}.$$

Proof: Let $k := |G : Z|$, and let $1 = t_0, t_1, t_2, \ldots, t_{k-1}$ be a transversal for the cosets of Z in G. Let

$$B := \{b : Z \to Z, x \mapsto x^{\lambda\mu} \mid \mu \in \mathbb{N}_0\}, \tag{2.15}$$

By Lemma 2.1, (1) ⇒ (2), we may define the mapping

$$\begin{array}{rcrcl} \Phi & : & (N:G)_{I(G)} & \longrightarrow & B \times N^{k-1} \\ & & p & \longmapsto & \big(p|_Z, p(t_1), \dots, p(t_{k-1})\big) \end{array} .$$

Let $p \in (N:G)_{I(G)}$. Since we have

$$p(gz) = p(g) \cdot p(z) \text{ for all } g \in G, z \in Z,$$

the function p is uniquely determined by $p|_Z$ and $p(t_1), \dots, p(t_{k-1})$. Thus Φ is injective. That Φ is surjective follows from Lemma 2.1, (2) ⇒ (1). Hence Φ is bijective and

$$|(N:G)_{I(G)}| = |B| \cdot |N|^{k-1}. \tag{2.16}$$

It remains to compute the size of the set B defined in (2.15). We know that for all natural numbers r, s, the set $\{0, 1, \dots, r-1\}$ contains $\frac{r}{\gcd(r,s)}$ multiples of s. Setting $r := \exp(Z)$ and $s := \lambda(G/N)$, we obtain

$$|B| = \frac{\exp(Z)}{\gcd\big(\exp(Z), \lambda(G/N)\big)}. \tag{2.17}$$

The result follows (2.16) and (2.17). □

Proof of Theorem 2.11: By Lemma 1.5, we have

$$|I(G)| = |I(G/N)| \cdot |(N:G)_{I(G)}|.$$

Hence the result follows immediately from Lemma 2.12. □

5. Polynomial automorphisms

Based on Lemma 2.1, we give a criterion to decide whether $I(G) = A(G)$ for certain groups with property (C). In Section 3 of Chapter 3, we will obtain several variations of this result.

First we note that, by Lemma 2.10, a normal subgroup N of G that satisfies (C.1) and (C.2) in G is fully-invariant. Hence each endomorphism α of G induces an endomorphism $\bar{\alpha}$ on G/N defined by

$$\bar{\alpha} : G/N \to G/N,\ xN \mapsto \alpha(x)N.$$

Theorem 2.13. *Let G be a finite group, let $Z := Z(G)$, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that* $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$. *Then the following are equivalent:*

1. *$I(G) = A(G)$;*
2. *All subgroups of Z are characteristic, and for all automorphisms α of G, we have that $\bar{\alpha}$, induced by α on G/N, is in $I(G/N)$.*

We note that in general $I(G) = A(G)$ does not imply $I(G/N) = A(G/N)$. There may be automorphisms of the factor G/N that are not induced by automorphisms of G. For instance, let $G := \mathrm{U}(2, 5^2) \cdot \{a * 1_2 \mid a \in \mathrm{GF}(5^2)^*\}$ (see Appendix A, Section 6, for the definition and the structure of unitary groups). Then $N := G'$ satisfies (C.1) and (C.2) in G, and G/N is not cyclic. Hence not all automorphisms of the abelian group G/N are polynomial functions. Still we have $I(G) = A(G)$ by Corollary 4.17.

For the proof of Theorem 2.13, we establish the following auxiliary result.

LEMMA 2.14. *Let G be a finite group, let $Z := Z(G)$, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that* $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$. *Let α be an endomorphism of G that satisfies the following properties:*

(1) *$\alpha(K) \subseteq K$ for all subgroups K of Z;*
(2) *$\bar{\alpha}$, induced by α on G/N, is in $I(G/N)$.*

Then we have $\alpha \in I(G)$.

Proof: We will prove $\alpha \in I(G)$ by using our description of polynomial functions in Lemma 2.1.

By assumption (1), all subgroups of Z are invariant under α. Therefore, by Lemma 1.10, we have $a \in \mathbb{Z}$ such that

$$\alpha(z) = z^a \text{ for all } z \in Z.$$

By assumption (2), we have $k \in \mathbb{N}_0$ and $a_1, \ldots, a_k \in G$ such that

$$\alpha(x) \cdot N = \prod_{i=1}^{k} x^{a_i} \cdot N \text{ for all } x \in G.$$

We define the function $f \in E(G)$ by

$$f(x) = (\prod_{i=1}^{k} x^{a_i})^{-1} \cdot \alpha(x) \text{ for all } x \in G.$$

Then f maps G into N, and we have

$$f(z) = z^{a-k} \text{ for all } z \in Z.$$

Since $f(Z) \subseteq N \cap Z$, this yields that $\exp(Z/(N \cap Z))$ divides $a - k$. Let $\lambda := \lambda(G/N)$ be the Scott-length of G/N. By the assumption that $\gcd(\lambda, \exp(Z)) = \exp(Z/(N \cap Z))$, we can find $\mu \in \mathbb{Z}$ such that

$$\mu \cdot \lambda \equiv a - k \mod \exp(Z).$$

Now we have $f(z) = z^{\mu\lambda}$ for all $z \in Z$. For $g \in G$ and $z \in Z$, we compute

$$f(gz) = (\prod_{i=1}^{k} (gz)^{a_i})^{-1} \cdot \alpha(gz) = (\prod_{i=1}^{k} g^{a_i})^{-1} \cdot \alpha(g) \cdot z^{-k} \cdot \alpha(z) = f(g) \cdot f(z).$$

Therefore Lemma 2.1, (2) ⇒ (1), yields that f is a polynomial function. This implies that α is polynomial. The lemma is proved. □

Proof of Theorem 2.13: The implication (1) ⇒ (2) is obviously true for each group G and each normal subgroup N of G.

For the converse, we assume that G satisfies the hypothesis of Theorem 2.13 and (2). Then Lemma 2.14 yields that all automorphisms of G are polynomial functions. Thus we have $I(G) = A(G)$. □

We obtain the conclusion of Theorem 2.13 also for some groups where $\gcd(\lambda(G/N), \exp(Z))$ is slightly bigger than $\exp(Z/(N \cap Z))$.

THEOREM 2.15. *Let G be a finite group, let $Z := Z(G)$ and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that* $\gcd(\lambda(G/N), \exp(Z)) = 2 \cdot \exp(Z/(N \cap Z))$ *and that* $\exp(Z/(N \cap Z))$ *is odd. Then the following are equivalent:*

(1) *$I(G) = A(G)$;*

(2) *All subgroups of Z are characteristic, and for all automorphisms α of G, we have that $\bar{\alpha}$, induced by α on G/N, is in $I(G/N)$.*

Proof: Let G, N and Z satisfy the hypotheses. Obviously we have (1) ⇒ (2). It suffices to prove the converse. Let α be an automorphism of G such that $\alpha(K) = K$ for all normal subgroups K of Z and $\bar{\alpha} \in I(G/N)$. We will show $\alpha \in I(G)$ by a modification of the proof of Lemma 2.14.

By Lemma 1.10, we have $a \in \mathbb{Z}$ such that

$$\alpha(z) = z^a \text{ for all } z \in Z.$$

We note that a is odd because α is bijective on Z and $|Z|$ is even by assumption. Since $\bar{\alpha} \in I(G/N)$, we have $k \in \mathbb{N}_0$ and $a_1, \dots, a_k \in G$ such that

$$\alpha(x) \cdot N = \prod_{i=1}^{k} x^{a_i} \cdot N \text{ for all } x \in G.$$

Since $\bar{\alpha}$ is bijective on G/N and $|G : N|$ is even by assumption, Proposition 1.2 yields that k is odd. The function $f \in E(G)$ that is defined by

$$f(x) = (\prod_{i=1}^{k} x^{a_i})^{-1} \cdot \alpha(x) \text{ for all } x \in G$$

maps G into N, and we have

$$f(z) = z^{a-k} \text{ for all } z \in Z. \tag{2.18}$$

Let $\lambda := \lambda(G/N)$ be the Scott-length of G/N. By assumption, we have $\gcd(\lambda, \exp(Z)) = 2 \cdot \exp(Z/(N \cap Z))$. Since $f(Z) \subseteq N \cap Z$, (2.18) yields that $a - k$ is a multiple of $\exp(Z/(N \cap Z))$. Moreover, since both a and k are odd and since $\exp(Z/(N \cap Z))$ is odd by assumption, we have that $2 \cdot \exp(Z/(N \cap Z))$ divides $a - k$. Thus there is $\mu \in \mathbb{Z}$ such that

$$\mu \cdot \lambda \equiv a - k \mod \exp(Z).$$

Now we have $f(z) = z^{\mu\lambda}$ for all $z \in Z$. Since, by definition, f is a product of endomorphisms of G which fix the center Z of G, we have

$$f(gz) = f(g) \cdot f(z) \text{ for all } g \in G, z \in Z.$$

Hence f is a polynomial function by Lemma 2.1, (2) $\Rightarrow$ (1). Thus we have $\alpha \in I(G)$, and (2) $\Rightarrow$ (1) of the theorem is proved. □

6. Polynomial endomorphisms

Similar to our description of when all automorphisms of a group are polynomial functions in the previous section, we now give a criterion to decide whether $I(G) = E(G)$ for certain groups with property (C). In Chapter 3, Section 4, we will obtain some corollaries of this result.

THEOREM 2.16. *Let G be a finite group, let $Z := Z(G)$, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$. Then the following are equivalent:*

(1) *$I(G) = E(G)$;*
(2) *All subgroups of Z are fully-invariant, and for all endomorphisms α of G, we have that $\bar{\alpha}$, induced by α on G/N, is in $I(G/N)$.*

Proof: The implication (1) $\Rightarrow$ (2) is obviously true for any group G and any normal subgroup N of G.

For the converse, we assume that G satisfies the hypothesis of Theorem 2.16 and (2). Then Lemma 2.14 yields that all endomorphisms of G are polynomial functions. Thus we have $I(G) = E(G)$. □

All groups with property (C) such that $I(G) = E(G)$ that we know of satisfy $I(G/N) = E(G/N)$. Still we cannot find a reason why this should be true in general. Even if $I(G) = E(G)$, there may be endomorphisms of the factor G/N that are not induced by endomorphisms of G.

The assumption $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$ of Theorem 2.16 might seem a bit artificial. We recall that by Proposition 1.11, which holds regardless of whether G has property (C) or not, this condition is actually necessary for $I(G) = E(G)$ if N has a complement in G.

By combining Theorem 2.16 and Proposition 1.11, we are now able to characterize when $I(G) = E(G)$ for groups G that split over a normal subgroup N that satisfies (C.1) and (C.2) in G.

THEOREM 2.17. *Let G be a finite group, let $Z := Z(G)$, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that N has a complement in G. Then we have $I(G) = E(G)$ if and only if the following are satisfied:*

(1) *$I(G/N) = E(G/N)$;*
(2) *All subgroups of Z are fully-invariant;*
(3) $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$.

Proof: Let G be a group that satisfies the hypothesis. First we assume that G satisfies (1), (2), and (3) of the theorem. Then Theorem 2.16, (2) ⇒ (1), yields $I(G) = E(G)$.

For proving the converse, we assume $I(G) = E(G)$. Then (1) and (3) follow from Proposition 1.11, and (2) is obvious. □

7. Endomorphisms into the center

Although simple, the following observation on endomorphisms into the center of a group will help us when dealing with orthogonal groups in Chapter 4.

LEMMA 2.18. *Let G be a finite group, and let N be a normal subgroup of G that satisfies* (C.1) *and* (C.2) *in G. We assume that $\lambda(G/G')$ is square-free and that $Z(G)$ is cyclic. Let α be an endomorphism from G into $Z(G) \cap N$. Then we have $\alpha \in I(G)$.*

Proof: Let $\lambda := \lambda(G/N)$. Let $Z := Z(G)$, and let z be a generator of Z. We have an integer a such that $\alpha(z) = z^a$. By Lemma 2.1, (1) ⇒ (2), it suffices to show that $\gcd(\lambda, |Z|)$ divides a.

By $G' \subseteq \mathrm{Ker}(\alpha)$ and $|\alpha(Z)| = |Z/(Z \cap \mathrm{Ker}(\alpha))|$, we have that $|\alpha(Z)|$ divides $|Z|/|Z \cap G'|$. Hence $|Z \cap G'|$ divides a. Since $N \subseteq G'$, we have $\alpha(Z) \in Z \cap G'$. Then $|Z : (Z \cap G')|$ divides a. Thus a is a multiple of $\gcd(\lambda, |Z \cap G'|)$ and a multiple of $\gcd(\lambda, |Z : (Z \cap G')|)$. Since λ is square-free by assumption, we have $\gcd(\lambda, s) \cdot \gcd(\lambda, t) = \gcd(\lambda, st)$ for all $s, t \in \mathbb{Z}$. In particular, we have $\gcd(\lambda, |Z|) = \gcd(\lambda, |Z \cap G'|) \cdot \gcd(\lambda, |Z : (Z \cap G')|)$. Thus $\gcd(\lambda, |Z|)$ divides a. Lemma 2.1, (1) ⇒ (2), yields $\alpha \in I(G)$. □

CHAPTER 3

Consequences for groups with property (A)

We consider groups G with center Z such that $(G'Z)/Z$ is non-abelian and the unique minimal normal subgroup of G/Z. Additionally we assume that $G'' = G'$. Since these groups have property (C) by Lemma 2.2, (7) ⇒ (1), we may apply the characterization of polynomial functions in Lemma 2.1 of the previous chapter. First we investigate the structure of these groups.

1. A description of groups with property (A)

As in [**AM03**], we define a class of groups that is included in the class of groups with property (C). We say that a group G *has property* (A) if it satisfies the conditions (A.1), (A.2), and (A.3) that are given by

(A.1) $G' \cap Z(G) \prec_G G'$;
(A.2) $G' = G''$;
(A.3) $G/Z(G)$ is centerless.

From Chapter 2, Section 2, we recall that G has property (C) if and only if G has a normal subgroup N such that the following conditions are satisfied:

(C.1) $N \neq \{1\}$ and $N' = N$;
(C.2) For all normal subgroups K of N we have $K \subseteq Z(G)$ or $N \subseteq K$.

By comparing (A.1), (A.2), and (A.3) with the conditions in Lemma 2.2 (4) for $N := G'$, it becomes apparent that (A) implies (C). The relation between (A) and (C) is made explicit in Lemma (3.1).

Obviously, all non-abelian simple groups and all quasisimple groups have property (A). We also note that all non-solvable finite general linear groups have (A) (see Chapter 4 and Appendix A). Certain quotients of non-solvable finite semi-linear groups provide examples of groups that have (C) but not (A). We will investigate such groups in Theorem 4.11.

LEMMA 3.1. *Let G be a finite group, and let $Z := Z(G)$. Then the following are equivalent:*

(1) *G has property* (A)*;*
(2) *G' satisfies* (C.1) *and* (C.2) *in G;*
(3) *G has a normal subgroup N that satisfies* (C.1) *and* (C.2) *in G such that G/N is abelian;*

(4) *$(G'Z)/Z$ is the unique minimal normal subgroup of G/Z and $G'' = G'$.*

Proof: (1) ⇒ (2): We assume that G has property (A). Then (A.1) and (A.2) immediately imply that G' satisfies (C.1). For (C.2), we let K be a normal subgroup of G, and we consider $X := (K \cap G')(Z \cap G')$. Since $Z \cap G' \subseteq X$ and $X \subseteq G'$, property (A.1) yields that either $X = Z \cap G'$ or $X = G'$.

If $X = Z \cap G'$, then $K \cap G' \subseteq Z \cap G'$. Now $[K, G] \subseteq K \cap G' \subseteq Z$ implies that $(KZ)/Z$ is central in G/Z. Thus $KZ = Z$ by (A.3) and $K \subseteq Z$.

If $X = G'$, then (A.2) yields $G' = G'' = ((K \cap G')(Z \cap G'))' = (K \cap G')' \subseteq K \cap G'$. Thus we have $G' \subseteq K$, which completes the proof of condition (C.2).

(2) ⇒ (3) is obvious.

(3) ⇒ (4): We assume that G and N satisfy (3). By (C.1), we have $G' \nsubseteq Z$. Hence (C.2) yields $N \subseteq G'$. Since G/N is abelian, we have $G' \subseteq N$. Thus $N = G'$. Now Lemma 2.2, (1) ⇒ (5), yields that $(G'Z)/Z$ is non-abelian and the unique minimal normal subgroup of G/Z, and that $G'' = G'$.

(4) ⇒ (1): We assume that $(G'Z)/Z$ is the unique minimal normal subgroup of G/Z and that $G' = G''$. Then we have (A.2). By the homomorphism theorem, $G'/(G' \cap Z)$ is a minimal normal subgroup in $G/(G' \cap Z)$. Hence (A.1) is satisfied. (A.3) is immediate from the assumption that G/Z has a non-abelian unique minimal normal subgroup. □

We restate parts of Lemma 2.3 and Lemma 2.5 for groups with property (A).

Lemma 3.2. *Let G be a group with property* (A)*, and let Y be a subgroup of $Z(G)$. Then we have:*

(1) *$(G/Y)' = (G'Y)/Y$ and $Z(G/Y) = Z(G)/Y$;*

(2) *G/Y has property* (A).

Proof: This is an immediate consequence of Lemma 3.1 and Lemma 2.3, (1) ⇒ (2). □

We note that only the implication (1) ⇒ (2) of Lemma 2.3 can be adapted to groups with property (A). Let G be a finite group, and let Y be a subgroup of $Z(G)$. We assume $Z(G/Y) = Z(G)/Y$ and that G/Y has property (A). Then Lemma 2.3, (2) ⇒ (1), yields that G has property (C). However, in general, G does not have property (A).

Lemma 3.3. *Let G be a group with property* (A) *such that $(G' \cdot Z(G))/Z(G)$ is simple. Let H be a subgroup of G with $G' \subseteq H$. Then we have:*

(1) *$H' = G'$ and $Z(H) = Z(G) \cap H$;*

(2) *All normal subgroups of H are normal in G;*

(3) *H has property* (A).

Proof: Let G and H satisfy the hypotheses. Then $G'' \subseteq H' \subseteq G'$ and the assumption $G'' = G'$ yield $H' = G'$. We note that, by Lemma 3.1, (1) ⇒ (2),

$N := G'$ satisfies (C.1) and (C.2) in G. By Lemma 2.5 (1), we have $Z(H) = Z(G) \cap H$. Item (1) of the lemma is proved.

Lemma 2.5 (2) yields:

$$\text{For all normal subgroups } K \text{ of } H \text{ we have } K \subseteq Z(H) \text{ or } G' \subseteq K. \tag{3.1}$$

Hence all normal subgroups of H are central in G or contain the derived subgroup of G. Thus we have (2).

By (3.1) and $H' = G'$, we have that H' satisfies (C.1) and (C.2) in H. Hence Lemma 3.1, (2) ⇒ (1), yields (3). The proof is complete. □

Without making further use of this fact, we note that for groups that satisfy the assumptions of Lemma 3.3 all subnormal subgroups are normal.

2. Size of $I(G)$

The next result is an application of Theorem 2.11 to groups with property (A).

Theorem 3.4 ([**AM03**, Theorem 2.1]). *Let G be a finite group with property* (A). *Then we have*

$$|I(G)| = |G'|^{|G:Z(G)|-1} \cdot \operatorname{lcm}(\exp(G/G'), \exp(Z(G))). \tag{3.2}$$

Proof: Let G be a finite group with property (A). Then G' satisfies (C.1) and (C.2) in G by Lemma 3.1. Since G/G' is abelian, we have $\lambda(G/G') = \exp(G/G')$ and $|I(G/G')| = \exp(G/G')$. Lemma 2.12 yields

$$|(G' : G)_{I(G)}| = \frac{\exp(Z(G))}{\gcd\big(\exp(Z(G)), \exp(G/G')\big)} \cdot |G'|^{|G:Z(G)|-1}.$$

Now (3.2) follows from $|I(G)| = |(G' : G)_{I(G)}| \cdot |I(G/G')|$ (see Lemma 1.5). □

For central extensions by simple, non-abelian groups, and in particular for quasisimple groups, Theorem 3.4 specializes as follows.

Corollary 3.5 (cf. [**ST99**, Theorem 4.9]). *Let G be a finite group such that $G/Z(G)$ is simple and non-abelian. Then the size of $I(G)$ is given by*

$$|I(G)| = |G'|^{|G:Z(G)|-1} \cdot \exp(Z(G)).$$

Proof: Let $Z := Z(G)$. By hypothesis, we have $(G/Z)' = G/Z$, which yields

$$G'Z = G. \tag{3.3}$$

From this, we obtain $G'' = G'$. Thus G has property (A) by Lemma 3.1, (4) ⇒ (1). Since $(G'Z)/G'$ is isomorphic to $Z/(G' \cap Z)$, equation (3.3) yields that G/G' is isomorphic to $Z/(G' \cap Z)$. Hence $\exp(G/G')$ divides $\exp(Z)$. Now $\operatorname{lcm}(\exp(G/G'), \exp(Z)) = \exp(Z)$, and the result follows from Theorem 3.4. □

3. Polynomial automorphisms

The description of polynomial functions in Lemma 2.1 allows to prove the following facts about the automorphism near-ring of certain groups (cf. Theorem 2.13).

THEOREM 3.6. *Let G be a finite group with property* (A)*. We let $Z := Z(G)$, and we assume* $\gcd(\exp(G/G'), \exp(Z)) = \exp(Z/(G' \cap Z))$*. Then the following are equivalent:*

(1) *$I(G) = A(G)$;*
(2) *All normal subgroups of G are characteristic.*

We give two proofs of Theorem 3.6. In the first we will derive Theorem 3.6 from Theorem 2.13 by Lemma 3.7. The second uses Lemma 3.8, an observation concerning polynomial endomorphisms, which seems to be interesting in its own.

LEMMA 3.7. *Let G be a finite group with property* (A)*, and let α be an endomorphism of G. Then the following are equivalent:*

(1) *All subgroups K of G with $G' \subseteq K$ are fixed by α;*
(2) *$\bar{\alpha}$, induced by α on G/G', is in $I(G/G')$.*

Proof: We note that

$$\bar{\alpha} : G/G' \to G/G',\ xG' \mapsto \alpha(x)G',$$

that is induced by the endomorphism α on G/G', is well-defined since G' is fully-invariant.

First we assume (1). Then all subgroups of the abelian group G/G' are invariant under $\bar{\alpha}$. By Lemma 1.10, there exists an integer a such that $\bar{\alpha}(\bar{x}) = \bar{x}^a$ for all $\bar{x} \in G/G'$. Hence we have $\bar{\alpha} \in I(G/G')$, and (2) is proved.

For proving (2) ⇒ (1), we note that $\bar{\alpha} \in I(G/G')$ yields that all subgroups of G/G' are fixed by $\bar{\alpha}$. Hence the homomorphism theorem yields (1). □

Proof of Theorem 3.6, variant 1: Let G satisfy the hypothesis of the theorem. Then G' satisfies (C.1) and (C.2) in G by Lemma 3.1. Lemma 3.7 yields that all normal subgroups of G are characteristic if and only if all subgroups of $Z(G)$ are characteristic and all automorphisms of G induce polynomial functions on G/G'. Hence condition (2) of the theorem is equivalent to condition (2) of Theorem 2.13. Thus Theorem 2.13 yields the result. □

By Lemma 1.10, the endomorphisms which fix all (normal) subgroups of an abelian group are polynomial functions. The following lemma represents an equivalent result for certain groups with property (A).

LEMMA 3.8. *Let G be a finite group with property* (A)*, and let $Z := Z(G)$. We assume that* $\gcd(\exp(G/G'), \exp(Z)) = \exp(Z/(G' \cap Z))$*. Let α be an endomorphism of G such that $\alpha(K) \subseteq K$ for all normal subgroups K of G. Then we have $\alpha \in I(G)$.*

Proof: We will prove $\alpha \in I(G)$ by using Lemma 2.14. First we verify that the assumptions of this lemma are satisfied. By Lemma 3.1, $N := G'$ satisfies (C.1) and (C.2) in G. The group G/N is abelian and has Scott-length $\lambda(G/N) = \exp(G/N)$. Let $Z := Z(G)$. Then we have $\gcd(\lambda(G/N), \exp(Z)) = \exp(Z/(N \cap Z))$ by hypothesis. By assumption, all subgroups of Z are invariant under α. It remains to be shown that

$$\bar{\alpha} : G/N \to G/N, xN \mapsto \alpha(x)N$$

is in $I(G/N)$. This follows from Lemma 3.7, (1) ⇒ (2), or from Lemma 1.10. We may apply Lemma 2.14, which yields $\alpha \in I(G)$. The result is proved. □

Proof of Theorem 3.6, variant 2: By Proposition 1.9, $I(G) = A(G)$ implies that all normal subgroups of G are characteristic. For the converse, we assume that all normal subgroups of G are characteristic. Then Lemma 3.8 yields that all automorphisms of G are polynomial functions. Thus we have $I(G) = A(G)$, and the theorem is proved. □

The following corollary of Theorem 3.6 uses slightly stronger assumptions.

COROLLARY 3.9. *Let G be a finite group with property* (A)*. We assume that $|G : (G' \cdot Z(G))|$ and $|G' \cap Z(G)|$ are relatively prime. Then the following are equivalent:*

(1) *$I(G) = A(G)$;*
(2) *All normal subgroups of G are characteristic.*

Proof: Let G and $Z := Z(G)$ satisfy the assumptions. We will prove

$$\gcd(\exp(G/G'), \exp(Z)) = \exp(Z/(G' \cap Z)). \tag{3.4}$$

Since $(G'Z)/G'$ is isomorphic to $Z/(G' \cap Z)$, we have that $\exp(Z/(G' \cap Z))$ divides $\gcd(\exp(G/G'), \exp(Z))$. We also note that $\gcd(\exp(G/G'), \exp(Z))$ divides $\exp(Z/(G' \cap Z)) \cdot \gcd(\exp(G/(G'Z)), \exp(G' \cap Z))$. Hence the hypothesis $\gcd(|G : G'Z|, |G' \cap Z|) = 1$ yields that $\gcd(\exp(G/G'), \exp(Z))$ divides $\exp(Z/(G' \cap Z))$. Thus we have (3.4). Theorem 3.6 yields the result. □

For groups whose center and quotient by the derived subgroup are cyclic, Corollary 3.9 yields the following.

COROLLARY 3.10 ([**AM03**, Theorem 3.1]). *Let G be a finite group with property* (A)*, and let $Z := Z(G)$. We assume that the following conditions are satisfied:*

(1) *G/G' is cyclic,*
(2) *Z is cyclic,*
(3) $\gcd(|G : G'Z|, |G' \cap Z|) = 1$.

Then we have $I(G) = A(G)$.

Proof: Let G be a group satisfying the assumptions. Since Z and G/G' are cyclic, all normal subgroups of G are characteristic. Now (2) ⇒ (1) of Theorem 3.6 yields $I(G) = A(G)$. □

Theorem 3.6 applies to central extensions of cyclic groups by simple, non-abelian groups; in particular, it applies to quasisimple groups with cyclic center (cf. Theorem 4.22).

Corollary 3.11 ([**AM03**, Corollary 3.2]). *Let G be a finite group such that $G/Z(G)$ is simple and non-abelian, and such that $Z(G)$ is cyclic. Then we have $I(G) = A(G)$.*

Proof: As in the proof of Corollary 3.5, we obtain that G has property (A), and that $G'Z = G$. Now the result follows from Corollary 3.10. □

As we have done for groups with property (C) (cf. Theorems 2.13, 2.15), we can slightly modify the assumptions of Theorem 3.6 and still obtain the same conclusion.

Theorem 3.12. *Let G be a finite group with property* (A)*, and let $Z := Z(G)$. We assume that* $\gcd(\exp(G/G'), \exp(Z)) = 2 \cdot \exp(Z/(G' \cap Z))$ *and that* $\exp(Z/(G' \cap Z))$ *is odd. Then the following are equivalent:*

(1) *$I(G) = A(G)$;*
(2) *All normal subgroups of G are characteristic.*

Proof: The result follows from Theorem 2.15 by the same argumentation as in the first proof that we gave for Theorem 3.6. □

We now consider groups where the center or the quotient by the derived subgroup is an elementary abelian 2-group.

Corollary 3.13. *Let G be a finite group with property* (A)*. We assume that* $\exp(G/G') = 2$ *or* $\exp(Z(G)) = 2$*. Then the following are equivalent:*

(1) *$I(G) = A(G)$;*
(2) *All normal subgroups of G are characteristic.*

Proof: Let G and $Z := Z(G)$ satisfy the hypothesis. The implication (1) ⇒ (2) is obvious. By Lemma 3.8, it remains to prove (2) ⇒ (1) under the assumption that $\gcd(\exp(G/G'), \exp(Z)) = 2$ and $\exp(Z/(G' \cap Z)) = 1$. For this case, Theorem 3.12, (2) ⇒ (1) yields the result. □

The following corollary will be applied to orthogonal groups in Theorem 4.25 and to non-solvable Frobenius complements in Theorem 5.18.

Corollary 3.14. *Let G be a finite group with property* (A). *We assume that one of the following two conditions is satisfied:*

(1) $|Z(G)| = 2$ *and G/G' is cyclic;*
(2) $Z(G)$ *is cyclic and* $|G/G'| = 2$.

Then we have $I(G) = A(G)$.

Proof: Let G satisfy the assumptions. Since $Z(G)$ and G/G' are cyclic, all normal subgroups of G are characteristic. Now (2) ⇒ (1) of Corollary 3.13 yields $I(G) = A(G)$. □

The next result will come handy when we deal with classical linear groups in the following chapter (see Theorems 4.7, 4.22).

Proposition 3.15. *Let A be a finite group, and let G be a normal subgroup of A such that the following are satisfied:*

(1) *G has property* (A)*;*
(2) *G/G' is cyclic, and $Z(G)$ is cyclic;*
(3) $|A/C_A(G')| = |\mathrm{Aut}\,((G' \cdot C_A(G')/C_A(G'))|$.

We assume that the function $\varphi_a : G \to G$, $x \mapsto x^a$, is in $I(G)$ for all $a \in A$. Then we have $I(G/Y) = A(G/Y)$ for all subgroups Y of $Z(G)$.

Proof: The result will follow from Lemma 1.16 together with Lemma 3.23. We let $N := G'$ and $C := C_A(G')$. First we let K be a normal subgroup of A, and we show:

$$\text{If } [N, K] \subseteq C, \text{then } K \subseteq C. \tag{3.5}$$

We assume $[N, K] \subseteq C$. Hence $[K, N, N]$ and $[N, K, N]$ are trivial. By the Three Subgroup Lemma (see [**Rob96**, p.122, 5.1.10]) the commutator $[N, N, K]$ is trivial as well. By hypothesis (1), we have $N' = N$. This yields $[N, K] = [N', K] = [N, N, K] = \{1\}$. Hence K centralizes N, and (3.5) is proved.

Let Y be a subgroup of $Z(G)$. We will now prove that $\hat{A} := A/Y$, $\hat{G} := G/Y$, and $\hat{N} := (NC)/Y$ satisfy the assumptions of Lemma 1.16. Let $\hat{C} := C/Y$. From (3.5) we obtain $C_{\hat{A}}(\hat{N}) = \hat{C}$. Moreover, for $\bar{A} := \hat{A}/\hat{C}$ and $\bar{N} := \hat{N}/\hat{C}$, we have that $C_{\bar{A}}(\bar{N})$ is trivial. The homomorphism theorem and hypothesis (3) yield $|\bar{A}| = |\mathrm{Aut}\,\bar{N}|$. Thus each automorphism of $\bar{N}$ is induced by conjugation by an element of $\bar{A}$.

We note that $Z(G) = C \cap G$ by the hypothesis that G has property (A). Lemma 3.2 yields $Z(\hat{G}) = \hat{C} \cap \hat{G}$. Thus all assumptions of Lemma 1.16 are satisfied for $\hat{A}$, $\hat{N}$, and $\hat{G}$.

Let α be an automorphism of $\hat{G}$. We will prove

$$\alpha \in I(\hat{G}). \tag{3.6}$$

Since $\hat{N}$ is the derived subgroup of $\hat{G}$, we have $\alpha(\hat{N}) \subseteq \hat{N}$. By Lemma 1.16, we have an element $a \in A$ and an endomorphism ρ from $\hat{G}$ into $Z(\hat{G})$ such that

$$\alpha(\hat{x}) = \rho(\hat{x}) \cdot \hat{x}^{\hat{a}} \text{ for all } x \in G. \tag{3.7}$$

Here and until the end of the proof, we use the convention that $\hat{y}$ denotes yY for all $y \in A$. By hypothesis, we have $k \in \mathbb{N}_0$ and $g_1, \dots, g_k \in G$ such that

$$x^a = \prod_{i=1}^{k} x^{g_i} \text{ for all } x \in G.$$

When we consider this equation modulo C, it is clear that $\varphi_{\hat{a}} : \hat{G} \to \hat{G},\ \hat{x} \mapsto \hat{x}^{\hat{a}}$, is in $I(\hat{G})$.

Lemma 3.2 yields that $\hat{G}$ has property (A). By hypothesis (2), we obtain that $Z(\hat{G})$ and $\hat{G}/\hat{G}'$ are cyclic. Hence ρ is in $I(\hat{G})$ by Lemma 3.23. Now (3.6) follows from (3.7). Thus $I(\hat{G}) = A(\hat{G})$ is proved. □

4. Polynomial endomorphisms

We restate Theorem 2.16 for groups with property (A).

Theorem 3.16. *Let G be a finite group with property* (A)*, and let $Z := Z(G)$. We assume that* $\gcd(\exp(G/G'), \exp(Z)) = \exp(Z/(G' \cap Z))$*. Then the following are equivalent:*

(1) *$I(G) = E(G)$;*
(2) *All normal subgroups of G are fully-invariant.*

Theorem 3.16 could be derived directly from Theorem 2.16. Instead of using this approach, we give an argumentation that follows the second proof of Theorem 3.6.

Proof: By Proposition 1.9, we have (1) ⇒ (2). For the converse, we assume that all normal subgroups of G are fully-invariant. Then Lemma 3.8 yields that all endomorphisms of G are polynomial functions. Thus we have $I(G) = E(G)$. □

Corollary 3.17. *Let G be a finite group with property* (A)*. We assume that $|G : (G' \cdot Z(G))|$ and $|G' \cap Z(G)|$ are relatively prime. Then the following are equivalent:*

(1) *$I(G) = E(G)$;*
(2) *All normal subgroups of G are fully-invariant.*

Proof: As in the proof of Corollary 3.9, we obtain $\gcd(\exp(G/G'), \exp(Z)) = \exp(Z/(G' \cap Z))$ for $Z := Z(G)$. Thus the result follows immediately from Theorem 3.16. □

As in the case of automorphism near-rings, we specialize Theorem 3.16 for groups whose center and quotient by the derived subgroup are cyclic. We note that the normal subgroups of such a group are characteristic but not necessarily fully-invariant. Hence, in Corollary 3.18, we require the additional condition (3) on the sizes of the center and the derived subgroup to guarantee that all normal subgroups are fully-invariant.

Corollary 3.18 ([**AM03**, Theorem 4.1]). *Let G be a finite group with property* (A) *that satisfies the following conditions:*

(1) *G/G' is cyclic;*
(2) *$Z(G)$ is cyclic;*
(3) $\gcd(|G:G'|, |Z(G)|) = 1$.

Then we have $I(G) = A(G) = E(G)$.

We should note that all groups G with property (A) such that $I(G) = E(G)$ that we know of satisfy conditions (1) and (2) in the corollary above (see Chapter 4, in particular Theorems 4.21, 4.22, 4.25, 4.26).

In Example 3.30 at the end of this chapter, we give a group G with property (A) such that $I(G) = E(G)$ but G does not satisfy condition (3) in the corollary above.

Proof of Corollary 3.18: Let G be a group that satisfies the assumptions. It suffices to show that all normal subgroups of G are fully-invariant. Then Corollary 3.17, (2) $\Rightarrow$ (1), yields $I(G) = E(G)$.

Let α be an endomorphism of G. Since G' is fully-invariant, α induces an endomorphism $\bar{\alpha}$ on G/G' defined by $\bar{\alpha}(xG') = \alpha(x)G'$ for all $x \in G$. Then $\bar{\alpha}$ fixes all subgroups of the cyclic group G/G'. By the homomorphism theorem, α fixes all subgroups containing G'. Thus all normal subgroups of G that contain G' are fully-invariant.

Let $Z := Z(G)$. We claim that

$$Z \text{ is fully-invariant.} \tag{3.8}$$

We know that $(G'Z)/G'$ is isomorphic to $Z/(G' \cap Z)$. Since G/G' and Z have relatively prime orders by assumption, we have $Z \subseteq G'$. Let $Y := \operatorname{Ker}(\alpha)$. If $Y \supseteq Z$, then $\alpha(Z) \subseteq Z$ is obvious. Hence we will assume $Y \not\supseteq Z$. Then $Y \not\supseteq G'$. Since G' satisfies (C.1) and (C.2) in G by Lemma 3.1, this yields $Y \subseteq Z$. By assumption (A.3), G/Z is centerless. Hence Lemma 2.8 yields $\alpha(Z) \subseteq Z$. This completes the proof of (3.8).

Since Z is cyclic, (3.8) implies that all subgroups of Z are fully-invariant in G. Finally, by (C.2), we have that all normal subgroups of G are fully-invariant. Now $I(G) = E(G)$ follows from Corollary 3.17. □

We apply the results that we have developed so far to the non-solvable symmetric groups. Corollary 3.18 immediately yields

$$I(S_n) = E(S_n) \text{ for all } n \geq 5$$

(see [**Mel78**], [**FM81**]). From Theorem 3.4 we obtain

$$|I(S_n)| = 2 \cdot (\frac{n!}{2})^{n!-1} \text{ for all } n \geq 5.$$

For completeness, we mention that $|I(S_4)| = 2^{35} \cdot 3^3$ and that $I(S_4) = E(S_4)$ (see [**FM81**], [**FK95**, Example 3]). We also note that $|I(S_3)| = 54$ and that $I(S_3) = E(S_3)$ (see Corollaries 5.9, 5.10).

As a further corollary, we obtain a result announced in [**STS95**, Theorem 12] (cf. [**ST99**, Theorem 4.9]). It applies to special linear, special unitary and symplectic groups (see Theorems 4.5, 4.13, Corollary 4.19).

Corollary 3.19. *Let G be a finite quasisimple group with cyclic center. Then we have $I(G) = A(G) = E(G)$.*

Proof: We have $G = G'$. Corollary 3.18 yields the result. □

The conditions given in Corollary 3.18 are sufficient but not necessary for $I(G) = E(G)$ (see Example 3.30). However, for certain groups with property (A) we have the following characterization of when all endomorphisms are polynomial functions (cf. Theorem 2.17). We will use this result when investigating classical linear groups in the next chapter (see Theorems 4.5, 4.13, 4.25).

Theorem 3.20. *Let G be a finite group with property* (A). *We assume that G' has a complement H in G such that $Z(G) \cap H = \{1\}$. Then we have $I(G) = E(G)$ if and only if G satisfies the following conditions:*

(1) *G/G' is cyclic;*
(2) *All subgroups of $Z(G)$ are fully-invariant;*
(3) $\gcd(|G : G'|, |Z(G)|) = 1$.

Proof: Let G be a group that satisfies the hypothesis. First we assume that G satisfies the conditions (1), (2), and (3) of the theorem. By the same argument as in the proof of Corollary 3.18, we find that all normal subgroups of G that contain G' are fully-invariant. Since all subgroups of $Z(G)$ are fully-invariant by assumption, we then have that all normal subgroups of G are fully-invariant. Thus Theorem 3.16, (2) ⇒ (1), yields $I(G) = E(G)$.

For proving the converse, we assume $I(G) = E(G)$. Let $Z := Z(G)$, and let H be a complement for G' in G. We consider the projection α from G to H that is defined by $\alpha(nh) = h$ for all $n \in G'$ and $h \in H$. Seeking a contradiction, we suppose that H is not cyclic. Then there is an endomorphism β of H and a subgroup U of H such that $\beta(U) \not\subseteq U$. Now the composition $\beta \circ \alpha$ is an endomorphism of G, and $G'U$ is a normal subgroup of G. By definition, $G'U$ is not invariant under $\beta \circ \alpha$, which contradicts $\beta \circ \alpha \in I(G)$. Thus H is cyclic, and (1) is proved. Item (2) is obvious.

To prove (3), we let $k \in \mathbb{N}_0$ and $a_1, \dots, a_k \in G$ such that

$$\alpha(x) = \prod_{i=1}^{k} x^{a_i} \text{ for all } x \in G. \tag{3.9}$$

Then we have $\alpha(z) = z^k$ for all $z \in Z$. Since $\alpha(Z)$ is contained in $Z \cap H$, which is trivial by assumption, this yields that

$$\exp(Z) \text{ divides } k. \tag{3.10}$$

Next we consider the induced endomorphism $\bar{\alpha}$ on G/G' with $\bar{\alpha}(xG') = \alpha(x)G'$ for all $x \in G$. By the definition of α as projection, we have

$$\bar{\alpha}(xG') = xG' \text{ for all } x \in G.$$

From (3.9) we obtain

$$\bar{\alpha}(xG') = x^k G' \text{ for all } x \in G.$$

Thus we have that

$$\exp(G/G') \text{ divides } k - 1.$$

Together with (3.10), this yields $\gcd(\exp(G/G'), \exp(Z)) = 1$. Hence (3) is proved. □

The assumptions of the next result describe exactly the situation that occurs for homomorphic images of linear groups (see Theorems 4.8, 4.18, and 4.22).

Proposition 3.21. *Let G be a finite group with property* (A)*, and let $Z := Z(G)$. We assume that the following conditions are satisfied:*

1. *Z is cyclic;*
2. *G' has a cyclic complement H in G;*
3. *$H \cap Z = \{1\}$.*

Let Y be a subgroup of Z. Then we have $I(G/Y) = E(G/Y)$ if and only if $|Z(G/Y)|$ and $|(G/Y) : (G/Y)'|$ are relatively prime.

Proof: The "if"-direction is immediate by the homomorphism theorem and Corollary 3.18. For proving the converse, we assume $I(G/Y) = E(G/Y)$. We will construct a specific endomorphism $\bar{\alpha}$ of G/Y, and we will show that $\bar{\alpha} \in I(G/Y)$ implies that $|Z(G/Y)|$ and $|(G/Y) : (G/Y)'|$ are relatively prime.

Let $m := |H|$, and let $t := |G : G'Y|$. Since H is abelian, we have an endomorphism α from G to H such that

$$\alpha(nh) = h^{m/t} \text{ for all } n \in G' \text{ and for all } h \in H.$$

Then we have

$$\operatorname{Ker}(\alpha) = G'Y. \tag{3.11}$$

We now consider the induced endomorphism $\bar{\alpha}$ on G/Y defined by

$$\bar{\alpha}(xY) = \alpha(x)Y \text{ for all } x \in G.$$

We note that $\bar{\alpha}$ is well-defined because $Y \subseteq \operatorname{Ker}(\alpha)$. We show

$$\operatorname{Ker}(\bar{\alpha}) = (G'Y)/Y. \tag{3.12}$$

The inclusion "$\supseteq$" is obvious by 3.11. For proving "$\subseteq$", let x be in G such that $xY \in \operatorname{Ker}(\bar{\alpha})$. Then $\bar{\alpha}(xY) = \alpha(x)Y$ implies $\alpha(x) \in Y$. Since $\alpha(G) \cap Y \subseteq H \cap Z$ and the latter is trivial by assumption, we have $\alpha(x) = 1$. Thus x is in $\operatorname{Ker}(\alpha)$, and (3.12) is proved.

By assumption, $\bar{\alpha}$ is a polynomial function. We have $l \in \mathbb{N}_0$ and $a_1, \dots, a_l \in G$ such that

$$\bar{\alpha}(\bar{x}) = \prod_{i=1}^{l} \bar{x}^{\overline{a_i}} \text{ for all } \bar{x} \in G/Y, \tag{3.13}$$

where we denote a_iY by $\overline{a_i}$. Let $s := |Z : Y|$. By considering the restriction of $\bar{\alpha}$ to $Z(G/Y)$, we will now prove

$$l \equiv 0 \mod s. \tag{3.14}$$

We note that $Z(G/Y) = Z/Y$ by Lemma 3.2. Since the center of G/Y is invariant under $\bar{\alpha}$ and since $\bar{\alpha}(G/Y) \subseteq (HY)/Y$, we have

$$\bar{\alpha}(Z/Y) \subseteq (HY)/Y \cap Z/Y. \tag{3.15}$$

By $Y \subseteq Z$, the modular law yields $(HY) \cap Z = (H \cap Z)Y$. From the assumption $H \cap Z = \{1\}$, we then obtain $(HY) \cap Z = Y$. Now (3.15) yields that $\bar{\alpha}(Z/Y)$ is trivial and consequently

$$Z/Y \subseteq \operatorname{Ker}(\bar{\alpha}). \tag{3.16}$$

Hence we have

$$\alpha(z)Y = Y \text{ for all } z \in Z,$$

and, by (3.13), we find

$$\alpha(z)Y = z^l Y \text{ for all } z \in Z.$$

Thus (3.14) is proved.

Next we consider the endomorphism induced by $\bar{\alpha}$ on $(G/Y)/(G/Y)'$ to prove

$$l \equiv \frac{m}{t} \mod t. \tag{3.17}$$

Let $\hat{\alpha}$ be the endomorphism of $(G/Y)/(G/Y)'$ defined by $\hat{\alpha}(\bar{x} \cdot (G/Y)') = \bar{\alpha}(\bar{x}) \cdot (G/Y)'$ for all $\bar{x} \in G/Y$. We note that $\hat{\alpha}$ is well-defined by (3.12). In the following, let $\hat{x}$ denote the coset $(x \cdot Y) \cdot (G/Y)'$ for $x \in G$. By (3.13), we obtain

$$\hat{\alpha}(\hat{x}) = \hat{x}^l \text{ for all } x \in G.$$

By the definition of α, we have

$$\hat{\alpha}(\hat{h}) = \hat{h}^{m/t} \text{ for all } h \in H.$$

Together with $\operatorname{ord} \hat{h} = t$, this yields (3.17).

By the congruences (3.14) and (3.17), we obtain that

$$\gcd(s,t) \text{ divides } \frac{m}{t}. \tag{3.18}$$

Hence $\gcd(s,t)$ divides $\gcd(s, \frac{m}{t})$. We will now complete the proof by showing

$$\gcd(s, \frac{m}{t}) = 1. \tag{3.19}$$

First we note that (3.12) and (3.16) yield $G'Y = G'Z$. Hence we have $\frac{|Y|}{|Y \cap G'|} = \frac{|Z|}{|Z \cap G'|}$. We obtain $\frac{|Z|}{|Y|} = \frac{|Z \cap G'|}{|Y \cap G'|}$. The former has been defined as s. So we have

$$s = |(Z \cap G') : (Y \cap G')|.$$

Next $m = |G'H : G'|$ and $t = |G'H : G'Y|$ yield $\frac{m}{t} = |G'Y : G'|$. By the homomorphism theorem, we obtain

$$\frac{m}{t} = |Y : (Y \cap G')|.$$

We note that $(Z \cap G')/(Y \cap G')$ and $Y/(Y \cap G')$ are subgroups of the cyclic group $Z/(Y \cap G')$ and that their intersection is trivial. Hence the orders of $(Z \cap G')/(Y \cap G')$ and $Y/(Y \cap G')$ are relatively prime. This yields (3.19), which together with (3.18) implies $\gcd(s,t) = 1$. The proof is complete. □

5. Endomorphisms into the center

We conclude this chapter with an investigation of endomorphisms into the center of a group G with property (A). For us, the importance of these endomorphisms lies in their connection with the automorphisms of G, which we already exploited in Proposition 3.15 (see also Lemma 1.16). The main results of this section are the Propositions 3.26 and 3.28. For their proofs we will need a couple of technical lemmas. The following Lemma 3.22 will also be used when we investigate polynomial automorphisms on unitary groups (see Theorem 4.15).

LEMMA 3.22. *Let G be a finite group with property* (A), *and let $Z := Z(G)$. We assume the following:*

1. *Z is cyclic;*
2. *For all subgroups L of G such that $G' \subseteq L$ and L/G' is a cyclic direct factor in G/G', we have that* $\gcd(|L : G'|, |Z|)$ *divides* $|L \cap Z|$.

Let α be an endomorphism from G into Z. Then we have $\alpha \in I(G)$.

Some comments on the hypotheses of the lemma above seem to be in order. Condition (1) can actually be relaxed a little bit. Our proof (which we postpone until after the proof of Lemma 3.25) only requires that the Sylow p-subgroup of Z is cyclic for any prime divisor p of $|G : G'|$. However, the less technical condition that Z is cyclic suffices for our applications in the next chapter.

Condition (2) is necessary for the assertion of the lemma. It is even necessary for $I(G) = A(G)$ as we have seen in Lemma 1.15. Assuming (1), hypothesis (2) is equivalent to the statement that the uniquely determined subgroup of Z of order $\gcd(|L : G'|, |Z|)$ is contained in L.

Since condition (2) of Lemma 3.22 is trivially fulfilled when G/G' is cyclic, we obtain the next lemma as a consequence. See Proposition 4.9 for a curious application.

LEMMA 3.23. *Let G be a finite group with property* (A) *such that $Z(G)$ is cyclic and G/G' is cyclic. Let α be an endomorphism from G into $Z(G)$. Then we have $\alpha \in I(G)$.*

Proof: Let G be a group that satisfies the assumptions, and let $Z := Z(G)$. It suffices to show that G satisfies condition (2) of Lemma 3.22. To this end, we let L be a subgroup of G with $G' \subseteq L$, and let $d := \gcd(|L : G'|, |Z|)$. We will prove that

$$d \text{ divides } |L \cap Z|. \tag{3.20}$$

By assumption, we have a subgroup C of Z with $|C| = d$. Then the size of $(CG')/G'$ divides d. In particular, $|(CG')/G'|$ divides $|L/G'|$. Since G/G' is cyclic, we then have $(CG')/G' \subseteq L/G'$. Hence C is contained in L. This yields (3.20). Now Lemma 3.22 proves the result. □

Before we give the proof of Lemma 3.22, we establish two auxiliary results. The first one states that an endomorphism with abelian image is a polynomial function if and only if certain products of this endomorphism are polynomial. We note that this is true for all finite groups, not just for those with property (A).

LEMMA 3.24. *Let G be a finite group. For a prime p, let S_p be the subgroup of G such that $G' \subseteq S_p$ and S_p/G' is the Sylow p-subgroup of G/G'. Let α be an endomorphism of G with $G' \subseteq \mathrm{Ker}(\alpha)$, and let the function $\alpha^{\exp(G/S_p)}$ be defined by $\alpha^{\exp(G/S_p)}(x) = \alpha(x)^{\exp(G/S_p)}$ for all $x \in G$.*

Then we have $\alpha \in I(G)$ if and only if $\alpha^{\exp(G/S_p)} \in I(G)$ for all primes p.

Proof: If $\alpha \in I(G)$, then all powers of α are in $I(G)$. For proving the converse, let D denote the set of prime divisors of $|G : G'|$. We assume $\alpha^{\exp(G/S_p)} \in I(G)$ for all $p \in D$. For $p \in D$, let r_p be an integer such that $r_p \equiv 1 \bmod \exp(S_p/G')$ and $r_p \equiv 0 \bmod \exp(G/S_p)$. Let $x \in G$ be fixed. Then x^{r_p} is in S_p. Since G/G'

is abelian, we have

$$xG' = \prod_{p \in D} x^{r_p} G'.$$

By the assumption that $G' \subseteq \operatorname{Ker}(\alpha)$, this yields

$$\alpha(x) = \prod_{p \in D} \alpha(x^{r_p}).$$

Since $\alpha^{\exp(G/S_p)} \in I(G)$ and since $\exp(G/S_p)$ divides r_p, we have $f_p \in I(G)$ such that $\alpha(x)^{r_p} = f_p(x)$ for all $x \in G$. Hence we obtain

$$\alpha(x) = \prod_{p \in D} f_p(x) \text{ for all } x \in G.$$

Thus we have $\alpha \in I(G)$. The lemma is proved. □

Lemma 3.25. *Let G be a finite group with property* (A)*, let p be a prime, and let P be the Sylow p-subgroup of $Z(G)$. We assume the following:*

(1) *P is cyclic;*
(2) *For all subgroups L of G such that $G' \subseteq L$ and L/G' is a cyclic direct factor in G/G', we have that* $\gcd(|L : G'|, |P|)$ *divides* $|L \cap P|$.

Let α be an endomorphism from G into P. Then we have $\alpha \in I(G)$.

Proof: Let G be a group with center Z such that the assumptions are satisfied. Let p be a prime divisor of $|G : G'|$, and let α be an endomorphism from G into P, the Sylow p-subgroup of Z. If P is in G', then we have $\alpha(G) \subseteq G'$ and $Z \subseteq \operatorname{Ker}(\alpha)$. For $N := G'$, Lemma 2.1, (2) ⇒ (1), yields $\alpha \in I(G)$. The result remains to be proved under the assumption that $P \not\subseteq G'$.

For $x \in G$, we write $\bar{x} := xG'$, and for subgroups A of G, we write $\bar{A} := (AG')/G'$. Let H be the subgroup of G such that $G' \subseteq H$ and such that $\bar{H}$ is the Sylow p-subgroup of $\bar{G}$. Then we have $\bar{P} \subseteq \bar{H}$. Let $\lambda := \exp(\bar{H})$. We note that $\lambda > 1$ by the assumption $P \not\subseteq G'$. We will distinguish the cases $\exp(\bar{H}/\bar{P}) = \lambda$ and $\exp(\bar{H}/\bar{P}) < \lambda$. First we consider the former. We will prove $\alpha \in I(G)$ by using Lemma 2.1 with $N := G'$. As a first step, we show that

$$\lambda \text{ divides } |P \cap G'|. \tag{3.21}$$

By assumption, we have a subgroup L of H with $G' \subseteq L$ such that $\bar{L}$ is cyclic and $|\bar{L}/(\bar{P} \cap \bar{L})| = \lambda$. Then $\bar{P}$ intersects $\bar{L}$ trivially, and we have $P \cap L \subseteq G'$. Hence hypothesis (2) yields

$$\gcd(|L : G'|, |P|) = \gcd(|L : G'|, |P \cap G'|).$$

Since $\gcd(|L : G'|, |P : (P \cap G')|) > 1$ by $P \not\subseteq G'$ and $L \neq G'$, we obtain that $|L : G'|$ divides $|P \cap G'|$. Thus (3.21) is proved.

By (3.21), $\alpha(G)$ is contained in $P \cap G'$. In particular, we have

$$\alpha(G) \subseteq G'.$$

Hence we may apply Lemma 2.1 for $f := \alpha$, $N := G'$. Since $\lambda(G/G') = \exp(G/G')$, we have to find $\mu \in \mathbb{Z}$ such that

$$\alpha(z) = z^{\mu \cdot \exp(G/G')} \text{ for all } z \in Z. \tag{3.22}$$

To this end, let c be a generator of the cyclic group P. Since $\operatorname{ord} \alpha(c)$ divides $|P : (P \cap G')|$, there exists an integer ν such that

$$\alpha(c) = c^{\nu \cdot |P \cap G'|}. \tag{3.23}$$

Let $\mu \in \mathbb{Z}$ such that

$$\begin{array}{rclr} \mu \cdot \exp(G/G') & \equiv & \nu \cdot |P \cap G'| & \mod |P|, \\ \mu \cdot \exp(G/G') & \equiv & 0 & \mod |Z : P|. \end{array} \tag{3.24}$$

We note that such an integer μ exists since $\gcd(\exp(G/G'), |P|)$ divides $|P \cap G'|$ by (3.21), $\gcd(\exp(G/G'), |Z : P|)$ obviously divides 0, and $|P|$ and $|Z : P|$ are relatively prime. By (3.23), we obtain (3.22). We clearly have $\alpha(xz) = \alpha(x)\alpha(z)$ for all $x \in G$, $z \in Z$. Hence Lemma 2.1, (2) $\Rightarrow$ (1), yields $\alpha \in I(G)$.

Next we assume that $\exp(\bar{H}/\bar{P}) < \lambda$. Our first goal is to obtain a function f such that f satisfies the assumptions of Lemma 2.1 for $N := G'$ and such that $f \in I(G)$ yields $\alpha \in I(G)$. The definition of such a function in (3.30) requires some preparation. Let L be a subgroup of H with $G' \subseteq L$ such that $\bar{L}$ is cyclic and $|\bar{L}| = \lambda$. Then $\bar{P}$ intersects $\bar{L}$ non-trivially. As a maximal cyclic subgroup of the abelian p-group $\bar{H}$, the group $\bar{L}$ has a direct complement in $\bar{H}$ (see [**Rob96**, p.102, 4.2.7]). Since $\bar{P}$ intersects this complement trivially, we have $\exp(\bar{H}/\bar{L}) < \lambda$. Furthermore hypothesis (2) yields that

$$\exp(\bar{H}/\bar{L}) \text{ divides } |P \cap G'|. \tag{3.25}$$

Let $\nu := \exp(\bar{L}/(\bar{L} \cap \bar{P}))$, and let $q := \exp(\bar{P}/(\bar{L} \cap \bar{P}))$. We note that $\nu \geq q$. Then we have $g \in G$ with $\langle \bar{g} \rangle = \bar{L}$, and we have a generator c of the cyclic group P such that

$$\bar{g}^{\nu} = \bar{c}^{q}. \tag{3.26}$$

Let $a \in \mathbb{Z}$ such that $\alpha(g) = c^a$. We show that

$$q \text{ divides } a. \tag{3.27}$$

It suffices to prove this for $q > 1$. Since $G' \subseteq L$, we have $|P : (P \cap L)| = q$. Then hypothesis (2) in the form $\gcd(|L : G'|, |P|) = \gcd(|L : G'|, |P \cap L|)$ together with $q > 1$ yields that $|L : G'|$ divides $|P \cap L|$. Hence

$$\lambda \text{ divides } \frac{|P|}{q} \text{ if } q > 1. \tag{3.28}$$

Now (3.27) follows since $\operatorname{ord} c^a = \frac{|P|}{\gcd(a,|P|)}$ divides λ.

Since $\operatorname{lcm}(\lambda, |P|)$ and $\operatorname{lcm}(\exp(G/H), \exp(Z/P))$ are relatively prime, we have $b \in \mathbb{Z}$ such that

$$\begin{array}{rcll} b & \equiv & -\frac{a}{q} \cdot \nu & \bmod \operatorname{lcm}(\lambda, |P|), \\ b & \equiv & 0 & \bmod \operatorname{lcm}(\exp(G/H), \exp(Z/P)). \end{array} \tag{3.29}$$

We consider the function $f \in E(G)$ that is defined by

$$f(x) = x^b \cdot \alpha(x) \text{ for all } x \in G. \tag{3.30}$$

We will prove $f \in I(G)$ by using Lemma 2.1 with $N := G'$. First we verify that f satisfies the assumptions of this lemma. As noted above, $\bar{L}$ has a direct complement in $\bar{H}$ and hence in $\bar{G}$. For $x \in G$, we then have $i \in \mathbb{Z}$ and $y \in G$ such that $y^{\exp(\bar{G}/\bar{L})} \in G'$ and $x = g^i y$. Modulo G' we have

$$\overline{f(x)} = \bar{g}^{ib} \cdot \overline{\alpha(g^i)} \cdot \bar{y}^b \cdot \overline{\alpha(y)}.$$

By $\operatorname{ord} \bar{g} = \lambda$ and by (3.26), we find

$$\bar{g}^{ib} = \bar{g}^{-i\frac{a}{q}\nu} = \bar{c}^{-ia}.$$

Together with $\alpha(g^i) = c^{ia}$, this yields

$$\overline{f(x)} = \bar{y}^b \cdot \overline{\alpha(y)}. \tag{3.31}$$

As an intermediate result, we will prove that

$$\exp(\bar{H}/\bar{L}) \text{ divides } \frac{a}{q} \cdot \nu. \tag{3.32}$$

Since this is certainly true for $\exp(\bar{H}/\bar{L}) \leq \nu$, we will assume $\exp(\bar{H}/\bar{L}) > \nu$ in the following. Then, by (3.25), there exists $t \in \mathbb{Z}$ such that

$$t \cdot \nu = |P \cap G'|. \tag{3.33}$$

We recall $\lambda = \frac{|\bar{P}|}{q} \cdot \nu$ from the definition of ν and q. Hence we obtain $t \cdot \lambda = \frac{|\bar{P}|}{q} \cdot |P \cap G'|$, that is, $t \cdot \lambda = \frac{|P|}{q}$. Together with (3.33), this yields $\frac{|P|}{\lambda \cdot q} \cdot \nu = |P \cap G'|$. Since $\frac{|P|}{\lambda}$ divides a by definition, we then have that $|P \cap G'| \cdot q$ divides $a\nu$. Thus (3.25) yields (3.32).

We proceed to consider (3.31). By (3.29) and (3.32), the exponent of $\bar{G}/\bar{L}$ divides b. Hence we have $y^b \in G'$. Since $\alpha(y) \in Z \cap G'$ by (3.25), equation (3.31) yields $\overline{f(x)} = \bar{1}$. Thus we have $f(G) \subseteq G'$.

Next we show that f satisfies the first part of condition (2) of Lemma 2.1:

$$\text{There exists } \mu \in \mathbb{Z} \text{ such that } f(z) = z^{\mu \cdot \exp(G/G')} \text{ for all } z \in Z. \tag{3.34}$$

For $z \in Z$, we have $i \in \mathbb{Z}$ and $y \in Z$ such that $y^{\exp(Z/P)} = 1$ and $z = c^i y$. By (3.26), we have $n \in G'$ such that $c^q = g^\nu n$. Since $G' \subseteq \operatorname{Ker}(\alpha)$ and $y \in \operatorname{Ker}(\alpha)$, we obtain

$$\alpha(z)^q = (\alpha(g^\nu)\cdot\alpha(n))^i\cdot\alpha(y)^q = c^{ia\nu}.$$

By (3.29), we have

$$z^{bq} = c^{ibq}y^{bq} = c^{-ia\nu}.$$

Hence we obtain

$$f(z)^q = 1 \text{ for all } z\in Z. \tag{3.35}$$

If $q = 1$, then $\mu = 0$ shows that (3.34) is satisfied. In the following we assume $q > 1$. By (3.28), λ divides $\frac{|P|}{q}$. Hence, by (3.35), we have an integer r such that

$$f(z) = z^{r\cdot\lambda} \text{ for all } z\in P. \tag{3.36}$$

Let Y be the direct complement of P in Z. We have

$$f(y) = 1 \text{ for all } y\in Y. \tag{3.37}$$

Let $\mu\in\mathbb{Z}$ such that

$$\begin{array}{rcll} \mu\cdot\exp(G/G') & \equiv & r\cdot\lambda & \mod |P|, \\ \mu\cdot\exp(G/G') & \equiv & 0 & \mod \exp(Z/P). \end{array}$$

We note that such an integer μ exists since $\gcd(\exp(G/G'), |P|) = \lambda$ by (3.28), $\gcd(\exp(G/G'), \exp(Z/P))$ divides 0, and $|P|$ and $\exp(Z/P)$ are relatively prime. Since, by definition, f is a product of endomorphisms which map the abelian group Z into itself, the restriction of f to Z is an endomorphism of Z. Thus (3.36) and (3.37) together with the definition of μ yields $f(z) = z^{\mu\cdot\exp(G/G')}$ for all $z\in Z$. Hence (3.34) is satisfied.

The second part of condition (2) of Lemma 2.1, that is, $f(xz) = f(x)\cdot f(z)$ for all $x\in G, z\in Z$, is immediate. Now Lemma 2.1, (2) ⇒ (1), yields that f is a polynomial function. Thus we have $\alpha\in I(G)$. The proof of the lemma is complete. □

We are now prepared to show Lemma 3.22.

Proof of Lemma 3.22: Let G be a group with property (A) and a cyclic center Z. Let p be a prime divisor of $|G : G'|$, and let S_p be the subgroup of G with $G'\subseteq S_p$ such that S_p/G' is the Sylow p-subgroup of G/G'. We assume that for all subgroups L of S_p such that $G'\subseteq L$ and such that L/G' is a cyclic direct factor in S_p/G', we have that $\gcd(|L : G'|, |P|)$ divides $|L\cap P|$. This assumption is certainly satisfied under condition (2) of the lemma.

Let α be an endomorphism from G into Z. Then

$$\alpha^{\exp(G/S_p)} : G\to Z,\ x\mapsto \alpha(x)^{\exp(G/S_p)}$$

is an endomorphism from G into the Sylow p-subgroup P of Z. By Lemma 3.25, we have $\alpha^{\exp(G/S_p)}\in I(G)$. Lemma 3.24 yields $\alpha\in I(G)$. The result is proved. □

We are now able to formulate two more intuitive results. We have to emphasize however that we depend on the previous lemmas for their proofs.

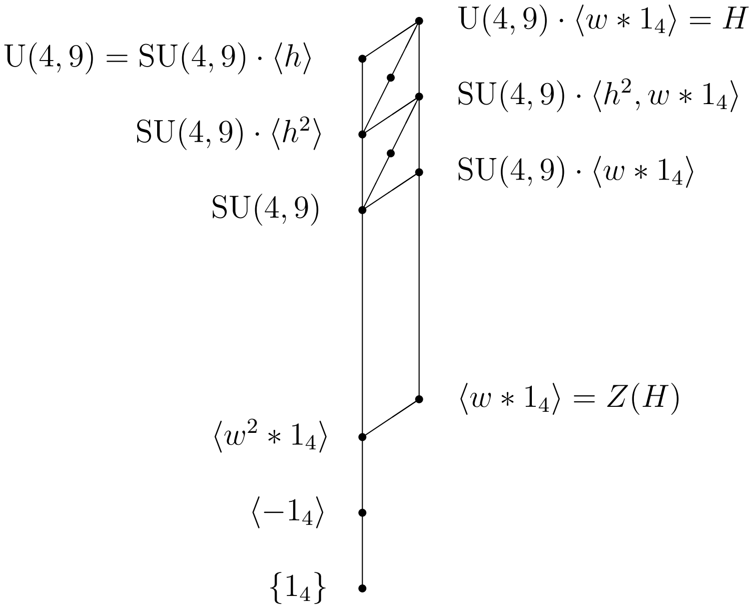
Proposition 3.26. *Let G be a finite group with property* (A) *and cyclic center. Then the following are equivalent:*

(1) *All endomorphisms from G to $Z(G)$ are in $I(G)$;*
(2) *All endomorphisms from G to $Z(G)$ induce polynomial functions on G/G'.*

Proof: The implication (1) ⇒ (2) is obviously true for all groups. For proving the converse, we need that G has property (A) and cyclic center. We assume that (2) of the proposition is satisfied. Then Lemma 1.15 yields that G satisfies condition (2) of Lemma 3.22. Thus Lemma 3.22 applies to prove (1). □

We will use Proposition 3.26 in the proof of Theorem 4.15. For a group G with property (A) and cyclic center, it is not true that a single endomorphism α into the center is in $I(G)$, if its induced endomorphism $\bar{\alpha}$ is in $I(G/G')$. We illustrate this by the following example.

Example 3.27. See Appendix A, Section 6, for definitions and the structure of unitary groups. Let w be a primitive element in $\mathrm{GF}(3^2)$. Then the unitary group $U := \mathrm{U}(4, 3^2)$ is the semidirect product of the special unitary group $S := \mathrm{SU}(4, 3^2)$ and the cyclic group that is generated by the diagonal matrix $h := \mathrm{diag}(w^2, 1, 1, 1)$. The next figure shows the lattice of normal subgroups of the group $H := U\langle w * 1_4\rangle$.


$\mathrm{U}(4,9)\cdot\langle w*1_4\rangle = H$
$\mathrm{U}(4,9) = \mathrm{SU}(4,9)\cdot\langle h\rangle$
$\mathrm{SU}(4,9)\cdot\langle h^2, w*1_4\rangle$
$\mathrm{SU}(4,9)\cdot\langle h^2\rangle$
$\mathrm{SU}(4,9)\cdot\langle w*1_4\rangle$
$\mathrm{SU}(4,9)$
$\langle w*1_4\rangle = Z(H)$
$\langle w^2*1_4\rangle$
$\langle -1_4\rangle$
$\{1_4\}$

We have $H' = S$, and $Z(H)$ is generated by $w * 1_4$. Then H has property (A). The factor H/H' is generated by hS of order 4 and $(w * 1_4)S$ of order 2. Since $h^2(w * 1_4) \notin S$, we have that H/H' is the direct product of $\langle hS \rangle$ and $\langle (w * 1_4)S \rangle$.

We consider $G := H/\langle -1_4 \rangle$. Then $Z(G)$ is generated by $z := (w * 1_4) \cdot \langle -1_4 \rangle$, and G/G' is isomorphic to H/H'. For $g := h \cdot \langle -1_4 \rangle$, we have that G/G' is the direct product of $\langle gG' \rangle$ of order 4 and $\langle zG' \rangle$ of order 2. We define an endomorphism α from G to $Z(G)$ by

$$\alpha(z) = z^2 \text{ and } \mathrm{Ker}(\alpha) = G'\langle g \rangle.$$

We note that α is a function from G to G'. Hence α induces the constant function $\bar{\alpha}(xG') = 1G'$ for all $x \in G$, which is in $I(G/G')$. However, since $\exp(G/G') = 4$ and $\alpha(c) = c^2$ for all $c \in Z(G)$, Lemma 2.1, (1) $\Rightarrow$ (2), yields that α is not a polynomial function on G. Hence we have $I(G) < A(G)$ by the following Proposition 3.28.

Proposition 3.28. *Let G be a finite group with property* (A) *and cyclic center. If $I(G) = A(G)$, then all endomorphisms from G into $Z(G)$ are in $I(G)$.*

Proof: Let G be a finite group with property (A). We assume that $Z(G)$ is cyclic and that $I(G) = A(G)$. By Lemma 1.15, we then have that G satisfies condition (2) of Lemma 3.22. Hence Lemma 3.22 yields that all endomorphisms from G into $Z(G)$ are in $I(G)$. □

6. Examples

Chapter 4 is devoted entirely to applications of the results that we developed up to this point. In this section we provide some supplementary examples of groups and polynomial functions to illustrate phenomena that do not occur in the case of classical groups.

Example 3.29. Let $N := \mathrm{SL}(2, 5)$, and let A be a cyclic group of order 4 with generator g. We define an action of A on N by

$$x^g = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)^{-1} \cdot x \cdot \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right) \text{ for all } x \in N.$$

Let $G := N \cdot A$ be the semidirect product of N and A defined by this action. We show that G has property (A). Since $\mathrm{SL}(2, 5)$ is perfect (see Lemma A.3), we have $G' = N$. Now we prove

$$C_G(N) = \langle -1_2 \rangle \cdot \langle g^2 \rangle. \tag{3.38}$$

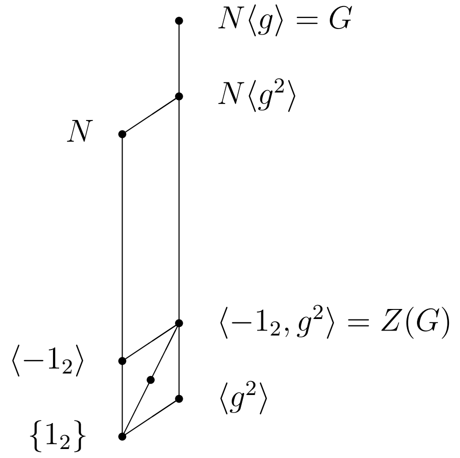
By Lemma A.5, we see that the map $\alpha : N \to N, x \mapsto x^g$ is an outer automorphism of N. Hence $C_G(N)$ is contained in $N\langle g^2 \rangle$. Since g^2 centralizes N, we then obtain (3.38) from $C_N(N) = \langle -1_2 \rangle$. We note that $C_G(N) = Z(G)$, that $N/(N \cap Z(G))$ is simple, and that $N' = N$ (see Lemma A.3). Then Lemma 2.2,

(3) ⇒ (1), yields that N satisfies (C.1) and (C.2) in G. Hence G has property (A) by $G' = N$, Lemma 3.1, (3) ⇒ (1).

We note that

$$G/Z(G) \cong (\mathrm{SL}(2,5) \cdot \langle (\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}) \rangle)/\langle 2 * 1_2 \rangle \cong \mathrm{PGL}(2,5) \cong S_5.$$

Below we give the lattice of normal subgroups of G.



From Theorem 3.4 we obtain

$$|I(G)| = 120^{119} \cdot 4. \tag{3.39}$$

Next we will show

$$I(G) = A(G). \tag{3.40}$$

By Theorem 3.6, it suffices to prove that all normal subgroups are characteristic. This is immediate for all normal subgroups of G with the exception of $\langle g^2 \rangle$ and $\langle -g^2 \rangle$. We can settle these cases by Lemma 1.16. The assumptions of this lemma are satisfied for $A := G$, G, N, and $C := Z(G)$ since each automorphism of $(NC)/C \cong A_5$ is induced by conjugation by an element in $G/C \cong S_5$ (see [**Sco87**, p.314 (11.4.8)]). Hence for every automorphism α of G, there exist $a \in G$ and an endomorphism ρ from G into $Z(G)$ such that

$$\alpha(x) = \rho(x) \cdot x^a \text{ for all } x \in G. \tag{3.41}$$

We proceed by proving that all normal subgroups are invariant under all endomorphisms from G to $Z(G)$. Let $\rho : G \to Z(G)$ be an endomorphism. By $\exp G/G' = 4$ and $\exp Z(G) = 2$, we find $NZ(G) \subseteq \mathrm{Ker}(\rho)$. Thus we have $\rho(K) \subseteq K$ for all normal subgroups K of G with $K \subseteq NZ(G)$. But then all normal subgroups of G are invariant under ρ. Hence, by (3.41), all normal subgroups are characteristic. Theorem 3.6 yields (3.40).

Since $\langle g^2 \rangle$ is not invariant under the endomorphism $\alpha : G \to G$ defined by $\alpha(g) = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) \in N$ and $\mathrm{Ker}(\alpha) = N$, we have

$$I(G) < E(G).$$

In the following we will now consider a certain factor H of the group given in the previous example such that $I(H) = E(H)$ and $\gcd(|Z(H)|, |H : H'|) > 1$. This shows that condition 3 of Corollary 3.18 is not necessary to have all endomorphisms as polynomial functions. We note that the group H that is constructed in the following is actually the unique non-solvable Frobenius complement of order 240 (see Appendix B and Chapter 5, Section 6).

Example 3.30. Let $G = N\langle g \rangle$ be the extension of $N = \mathrm{SL}(2, 5)$ as in defined in Example 3.30. Let $M := \langle -g^2 \rangle$, and let $H := G/M$. Then the lattice of normal subgroups of H forms the chain

$$\{1\} < Z(H) < H' < H.$$

We have $Z(H) = \langle -1_2, g \rangle / M \cong \mathbb{Z}_2$,

$$H' = (NM)/M \cong N/(N \cap M) \cong \mathrm{SL}(2, 5),$$

and $|H : H'| = 2$. By Theorem 3.4, we have

$$|I(H)| = 120^{119} \cdot 2, \tag{3.42}$$

and by Corollary 3.14, we have

$$I(H) = A(H). \tag{3.43}$$

Since $\gcd(|Z(H)|, |H : H'|) = 2$, our results from Section 4 are not applicable to prove

$$I(H) = E(H). \tag{3.44}$$

We note that there is no endomorphism ρ on H with $\mathrm{Ker}(\rho) = Z(H)$ since H' is the unique subgroup of index 2 in H and H' is not isomorphic to $H/Z(H)$. By (3.43), it then suffices to show that all endomorphisms ρ of H with $\mathrm{Ker}(\rho) = H'$ are contained in $I(H)$. Let ρ be an endomorphism with $\mathrm{Ker}(\rho) = H'$. Then $|\rho(H)| = 2$. We claim that

$$-1_2 M \text{ is the unique involution in } H. \tag{3.45}$$

From this we obtain $\rho(H) \subseteq Z(H) \subseteq H'$, and hence ρ is a polynomial function by Lemma 2.1, (2) $\Rightarrow$ (1). This proves (3.44). We note that ρ is actually unique by (3.45).

For the proof of (3.45), we note that $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) M$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) M$, and gM generate a generalized quaternion group Q of order 16. Then Q is a Sylow 2-subgroup of H. Hence every involution in H is conjugate to the unique involution $-1_2 M$ of Q. Since $-1_2 M$ is central in H, we have (3.45).

CHAPTER 4

Consequences for classical groups

Classical groups in the sense of [**KL90**] comprise of linear and semilinear, unitary, symplectic, and orthogonal groups on finite vector spaces as well as certain quotients and extensions of those. For a precise definition, see Section 3 in Appendix A.

We will apply the results from the previous chapter to those classical groups whose quotient by the center has a non-abelian unique minimal normal subgroup. These include all linear groups with certain exceptions that act on vector spaces of low dimension. Polynomial functions on solvable linear groups will be investigated in the next chapter. We refer to the Corollaries 5.9, 5.10 for $\mathrm{SL}(2,2)$ and to the Propositions 5.24, 5.25 for $\mathrm{SL}(2,3)$, $\mathrm{GL}(2,3)$, respectively.

The main results, which we will prove in this chapter, are summarized in the following. We note that all groups that satisfy the assumptions of the next three theorems have property (A), that the center is cyclic, and that the factor by the center has a unique minimal normal subgroup, which is non-abelian simple (see Appendix A).

THEOREM 4.1. *Let V be a vector space of dimension $n \geq 2$ over the field F with q elements. Let k be a bilinear form as in the cases* $\mathbf{L}, \mathbf{U}, \mathbf{S}$. *We assume that $(n,q) \notin \{(2,2),(2,3)\}$ in the cases* $\mathbf{L}$, $\mathbf{S}$, *and that $(n,q) \notin \{(2,2^2),(2,3^2),(3,2^2)\}$ in case* $\mathbf{U}$. *Let G be a group such that $S(V,F,k) \subseteq G \subseteq \Delta(V,F,k)$. Then we have:*

1. $|I(G)| = |G'|^{|G:Z(G)|-1} \cdot \mathrm{lcm}(\exp(G/G'), \exp(Z(G)))$;
2. $I(G) = A(G)$;
3. $I(G) = E(G)$ *iff G is centerless or $G = G'$.*

Theorem 4.1 will be proved in Sections 1, 2, and 3.

THEOREM 4.2. *Let V be a vector space of dimension $n \geq 5$ over the field F with q elements. Let k be a quadratic form as in the case* $\mathbf{O}$. *Let G be a group such that $S(V,F,k) \subseteq G \subseteq I(V,F,k)$. Then we have:*

1. $|I(G)| = |G'|^{|G:Z(G)|-1} \cdot \mathrm{lcm}(\exp(G/G'), \exp(Z(G)))$;
2. $I(G) = A(G)$ *iff q is even or $G < I(V,F,k)$;*
3. $I(G) = E(G)$ *iff G is centerless or $G = G'$.*

Theorem 4.2 will be proved in Section 4.

Theorem 4.3. *Let V be a vector space of dimension $n \geq 2$ over the field F with q elements. Let k be a bilinear form as in the cases $\mathbf{L}, \mathbf{U}, \mathbf{S}$. We assume that $(n,q) \notin \{(2,2),(2,3)\}$ in the cases $\mathbf{L}$, $\mathbf{S}$, and that $(n,q) \notin \{(2,2^2),(2,3^2),(3,2^2)\}$ in case $\mathbf{U}$. Let G be a group such that $S(V,F,k) \subseteq G \subseteq I(V,F,k)$, and let Y be a subgroup of $Z(G)$. For $\bar{G} := G/Y$, we have:*

1. *$|I(\bar{G})| = |\bar{G}'|^{|\bar{G}:Z(\bar{G})|-1} \cdot \mathrm{lcm}(\exp(\bar{G}/\bar{G}'), \exp(Z(\bar{G})))$;*
2. *$I(\bar{G}) = A(\bar{G})$;*
3. *$I(\bar{G}) = E(\bar{G})$ iff $|Z(\bar{G})|$ and $|\bar{G} : \bar{G}'|$ are relatively prime.*

Theorem 4.3 will be proved in Sections 1, 2, and 3.

1. Linear groups

Polynomial functions on the non-solvable groups $\mathrm{SL}(n,q)$ and $\mathrm{GL}(n,q)$ have been studied in Chapter 11 of [**Mel85**] (see also [**Mel79**]). In [**ST99**], answers have been announced to the question whether all automorphisms (all endomorphism) on, e. g., the general linear, the special linear, and the projective general linear groups are polynomial functions; a formula for $|I(\mathrm{SL}(n,q)|$ is given. In the proof of [**Kow97**, Proposition 2], the size of $I(\mathrm{GL}(n,q))$ is determined.

In this section we will revisit some results on classical linear groups G and their non-solvable quotients from our joint work with E. Aichinger in [**AM03**] and give some generalizations. First we obtain $|I(G)|$ as a corollary of Theorem 3.4.

Corollary 4.4 ([**AM03**, Corollary 2.3]). *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3)\}$. Let G be a group such that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$, and let Y be a subgroup of $Z(G)$. Let $m := |G : \mathrm{SL}(n,q)|$, let $s := |\mathrm{SL}(n,q)|$, and let $k := |Y|$. Then we have*

$$|I(G/Y)| = \mathrm{lcm}\left(\frac{m \cdot \gcd(n,k)}{k}, \frac{\gcd(nm,q-1)}{k}\right) \cdot \left(\frac{s}{\gcd(n,k)}\right)^{\frac{m \cdot s}{\gcd(nm,q-1)}-1}.$$

Proof: By Lemma A.4, the group G/Y has property (A). Furthermore the center of G/Y is cyclic and has size $\frac{\gcd(mn,q-1)}{k}$. From the definition of G/Y, we immediately obtain $|G/Y| = \frac{m \cdot s}{k}$. We compute

$$|(G/Y) : Z(G/Y)| = \frac{\frac{m \cdot s}{k}}{\frac{\gcd(mn,q-1)}{k}} = \frac{m \cdot s}{\gcd(mn,q-1)}.$$

By Lemma A.4, we have $(G/Y)' = (\mathrm{SL}(n,q)Y)/Y$ and $|(G/Y)'| = s/\gcd(n,k)$. By the homomorphism theorem, $(G/Y)/(G/Y)'$ is cyclic and has size, and hence exponent,

$$|(G/Y) : (G/Y)'| = \frac{m \cdot \gcd(n,k)}{k}.$$

Now the formula given in Theorem 3.4 yields the expression for $|I(G/Y)|$ stated in the corollary. □

From our characterization of polynomial functions in Lemma 2.1 and the description of automorphisms of linear groups in Lemma A.10, we obtain the following:

Theorem 4.5 ([**AM03**, Theorem 3.4, Theorem 4.3 (2)]). *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3)\}$. We assume that G is a group such that $\mathrm{SL}(n, q) \subseteq G \subseteq \mathrm{GL}(n, q)$. Then we have:*

(1) *$I(G) = A(G)$;*
(2) *$I(G) = E(G)$ if and only if $G = \mathrm{SL}(n, q)$.*

For the proof of (1) of the theorem, we use an intermediate result.

Lemma 4.6. *Let G be as in Theorem 4.5, and let α be an endomorphism of G with $\mathrm{Ker}(\alpha) \subseteq Z(G)$. Then we have $\alpha \in I(G)$.*

Proof: By Lemma A.4, G has property (A). By Lemma A.10, we have $a \in \mathbb{N}$ such that $\alpha(z) = z^a$ for all $z \in Z(G)$ and $\det \alpha(x) = (\det x)^a$ for all $x \in G$. We define the function $f \in A(G)$ as

$$f(x) = x^{-a} \cdot \alpha(x) \text{ for all } x \in G.$$

Then we have $f(G) \subseteq \mathrm{SL}(n, q)$ and $f(z) = 1$ for all $z \in Z(G)$. Since $f(gz) = f(g) \cdot f(z)$ for all $g \in G, z \in Z(G)$, Lemma 2.1, (2) $\Rightarrow$ (1), yields $f \in I(G)$. Thus α is a polynomial function. The lemma is proved. □

Proof of Theorem 4.5: Lemma 4.6 yields that all automorphisms of G are in $I(G)$. Hence we have (1).

We will reduce (2) to Theorem 3.20. First we we show that the assumptions of this result are satisfied. We recall that G has property (A) by Lemma A.4. Let $m := |G : \mathrm{SL}(n, q)|$, and let d be a primitive m-th root of unity in $\mathrm{GF}(q)$. Then $H := \langle \mathrm{diag}(d, 1, \ldots, 1) \rangle$ is a complement for $\mathrm{SL}(n, q)$ in G, and we have $Z(G) \cap H = \{1_n\}$. Hence Theorem 3.20 applies.

We assume $E(G) = I(G)$. Then $|G : G'|$ and $|Z(G)|$ are relatively prime by Theorem 3.20. Since $|G : G'| = m$ and $|Z(G)| = m \cdot \gcd(n, \frac{q-1}{m})$ by Lemma A.4, this yields $m = 1$. Thus we have $G = \mathrm{SL}(n, q)$.

The converse implication follows from Corollary 3.19 (or from Theorem 3.20 together with Lemma 2.8) since $\mathrm{SL}(n, q)$ is quasisimple and has cyclic center by Lemma A.3. □

The next result generalizes Theorem 4.5 (1). However, its proof depends on the characterization of the automorphism groups of the projective special groups by Dieudonnè (see Lemma A.2), which we do not prove here. We note that the proof of Theorem 4.5 (1) only requires Lemma A.10 which we will prove with a modest amount of representation theory.

Theorem 4.7. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2,2), (2,3)\}$. Let G be a group such that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$, and let Y be a subgroup of $Z(G)$.*

Then we have $I(G/Y) = A(G/Y)$.

Proof: We will use Proposition 3.15 to prove the result. Before we can apply this proposition, we have to introduce some notation.

Let F be the field $\mathrm{GF}(q)$. As in Appendix A, Section 1 (A.4), we have a semidirect product $\mathrm{GL}(n,q) \cdot \operatorname{Aut} F$. For $\varphi \in \operatorname{Aut} F$ and $a \in \mathrm{GL}(n,q)$, the matrix a^{φ} has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j. Now let $\hat{\imath}$ be the involutory automorphism of $\mathrm{GL}(n,q) \cdot \operatorname{Aut} F$ defined by

$$(x \cdot \varphi)^{\hat{\imath}} = (x^{-1})^t \cdot \varphi \text{ for all } x \in \mathrm{GL}(n,q), \varphi \in \operatorname{Aut} F.$$

With this action, we can define

$$A := \begin{cases} \mathrm{GL}(n,q) \cdot \operatorname{Aut} F & \text{for } n = 2 \\ (\mathrm{GL}(n,q) \cdot \operatorname{Aut} F) \cdot \langle \hat{\imath} \rangle & \text{for } n > 2 \end{cases}$$

We will now show that A and G satisfy the assumptions of Proposition 3.15. Let $N := \mathrm{SL}(n,q)$ and $C := \{a * 1_n \mid a \in F^*\}$. By Lemma A.4, the group G has property (A) and $G' = N$. We note that $Z(G) = C \cap G$ is cyclic and G/N is cyclic. Lemma A.5 yields $C_A(N) = C$. By Lemma A.2, the full automorphisms group of $(NC)/C$ is isomorphic to A/C.

Let $a \in A$. We will prove that the automorphism $\sigma_a : G \to G,\ x \mapsto x^a$, is an element of $I(G)$. To this end, we let $b \in \mathrm{GL}(n,q)$, $\varphi \in \operatorname{Aut} F$, and $j \in \langle \hat{\imath} \rangle$ such that $a = b\varphi j$. Let $m \in \mathbb{Z}$ such that $u^{\varphi} = u^m$ for all $u \in F$. We let $s := 1$ for $j = 1$ and $s := -1$ for $j = \hat{\imath}$. By the definition of the action of $\operatorname{Aut} F$ on $\mathrm{GL}(n,q)$, we obtain

$$z^a = z^{\varphi j} = z^{-ms} \text{ for all } z \in Z(G)$$

and

$$x^a \equiv x^{\varphi j} \equiv x^{-ms} \bmod N \text{ for all } x \in G.$$

Hence the function $f \in A(G)$ that is defined by

$$f(x) = x^{ms} \cdot x^a \text{ for all } x \in G$$

maps G into N and satisfies $f(z) = 1$ for all $z \in Z(G)$. Since, by definition, f is a product of endomorphisms which map $Z(G)$ into $Z(G)$, we have $f(xz) = f(x) \cdot f(z)$ for all $x \in G, z \in Z(G)$. Now Lemma 2.1, (2) $\Rightarrow$ (1), yields that f is a polynomial function. From this we obtain $\sigma_a \in I(G)$. Finally Proposition 3.15 applies to prove the theorem. □

From Proposition 3.21, we obtain a characterization of the non-solvable quotients of classical linear groups, whose endomorphisms are polynomial functions. We note that the following Theorem 4.8 implies Theorem 4.5 (2).

THEOREM 4.8 ([**AM03**, Theorem 4.3 (1)]). *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3)\}$. Let G be a group such that $\mathrm{SL}(n, q) \subseteq G \subseteq \mathrm{GL}(n, q)$, and let Y be a subgroup of $Z(G)$.*

Then we have $I(G/Y) = E(G/Y)$ if and only if $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime.

We note that for $m := |G : \mathrm{SL}(n, q)|$ and $k := |Y|$, Lemma A.4 yields

$$\gcd\left(|(G/Y) : (G/Y)'|, |Z(G/Y)|\right) = \gcd\left(\frac{m \cdot \gcd(n, k)}{k}, \frac{\gcd(nm, q-1)}{k}\right).$$

Proof of Theorem 4.8: It suffices to check that G satisfies the assumptions of Proposition 3.21 since this proposition immediately yields the result. To this end, we note that G has property (A) and $Z := Z(G)$ is cyclic by Lemma A.4. Furthermore we have $G' = \mathrm{SL}(n, q)$. For $m := |G : \mathrm{SL}(n, q)|$, let d be a primitive m-th root of unity in $\mathrm{GF}(q)$. Then $H := \langle \mathrm{diag}(d, 1, \ldots, 1) \rangle$ is a cyclic complement for $\mathrm{SL}(n, q)$ in G, and we have $H \cap Z = \{1_n\}$. Hence the assumptions of Proposition 3.21 are satisfied, and the theorem follows. □

As a further consequence of our characterization of polynomial functions in Lemma 2.1 we obtain that the determinant function can be represented by a polynomial.

PROPOSITION 4.9. *For n and G as in Theorem 4.8, let*

$$d : G \to G,\ x \mapsto (\det x) * 1_n.$$

Then we have $d \in I(G)$.

Since G/G' and $Z(G)$ are cyclic, and since d is an endomorphism from G into $Z(G)$, Lemma 3.23 immediately yields $d \in I(G)$. Because of its brevity, we also include a proof which refers to Lemma 2.1 directly. While this lemma guarantees the existence of a polynomial function whose values match the values of d, we are not able to give an actual presentation of d as polynomial function.

Proof of Proposition 4.9: By Lemma A.4, G has property (A). We will show that the function f defined by $f(x) := x^{-n} \cdot d(x)$ lies in $I(G)$ by using Lemma 2.1 with $N := \mathrm{SL}(n, q)$. First we show $f(G) \subseteq N$. We fix $x \in G$ and compute

$$\det f(x) = \det(x^{-n}) \cdot \det((\det x) * 1_n) = (\det x)^{-n} \cdot (\det x)^n = 1.$$

Hence $f(x) \in \mathrm{SL}(n, q)$. Next we prove

$$f(z) = 1_n \text{ for all } z \in Z(G). \tag{4.1}$$

Let z be a central element of G. Then there is $a \in \mathrm{GF}(q)^*$ such that $z = a * 1_n$. Thus we have $(\det z) * 1_n = (\det(a * 1_n)) * 1_n = a^n * 1_n = z^n$, which yields (4.1).

We obtain

$$f(gz) = f(g) \cdot f(z) \text{ for all } g \in G,\ z \in Z(G), \tag{4.2}$$

by computing $f(gz) = (gz)^{-n} \cdot (\det(gz) * 1_n) = g^{-n}z^{-n} \cdot ((\det(g)\det(z)) * 1_n) = g^{-n}z^{-n}((\det g) * 1_n)((\det z) * 1_n) = g^{-n}((\det g) * 1_n) \cdot z^{-n}((\det z) * 1_n) = f(g) \cdot f(z)$. By (4.1) and (4.2), condition (2) of Lemma 2.1 is satisfied for $\mu = 0$. This lemma now yields $f \in I(G)$. Hence we have $d \in I(G)$. □

The map that transposes all matrices is also polynomial. Let F be a (possibly infinite) field, and let x be a 2×2 matrix over F with $\det x = 1$. Then we have

$$x^t = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} \cdot x^{-1} \cdot \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right).$$

While we do not know a term presentation of $x \mapsto x^t$ in general, we still have the following:

Proposition 4.10. *For G as in Theorem 4.8, let*

$$\tau : G \to G,\ x \mapsto x^t.$$

Then we have $\tau \in I(G)$.

Proof: We consider the function f on G defined by $f(x) := x^{-1} \cdot x^t$. Then we have $f(G) \subseteq \mathrm{SL}(n, q)$. Since $f(z) = 1$ and $f(gz) = f(g) \cdot f(z)$ for all $g \in G, z \in Z(G)$, Lemma 2.1, (2) $\Rightarrow$ (1), yields that $f \in I(G)$. Hence we have $\tau \in I(G)$. □

Lemma 2.1 can be successfully applied to answer questions about polynomial functions on linear groups. Unfortunately, the groups of semilinear transformations of finite vector spaces (see Appendix 3, Section 1) do not have property (C). Hence Lemma 2.1 is not applicable to these groups in general. Still we can give one result that is related to semilinear groups.

Theorem 4.11. *Let n, f be natural numbers with $n \geq 2$, and let p be a prime such that $(n, p^f) \notin \{(2, 2), (2, 3)\}$. Let $H := \mathrm{GL}(n, p^f) \cdot \mathrm{Aut}\,\mathrm{GF}(p^f)$, and let $Y := \{a * 1_n \mid a^{p-1} = 1, a \in \mathrm{GF}(p^f)\}$. We write $G := H/Y$ and $N := (\mathrm{SL}(n, p^f) \cdot Y)/Y$. Then we have*

$$|(N : G)_{I(G)}| = |N|^{|G|/(p-1)-1}.$$

We note that Y is a normal subgroup of H. Here the automorphism group of the field acts on the matrix group as usual. For $\varphi \in \mathrm{Aut}\,\mathrm{GF}(p^f)$ and $a \in \mathrm{GL}(n, p^f)$, the matrix a^φ has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j.

Proof of Theorem 4.11: We will show that N satisfies (C.1) and (C.2) in G by Lemma 2.2, (3) $\Rightarrow$ (1). We write $q := p^f$, and $C := \{a * 1_n \mid a \in \mathrm{GF}(q)^*\}$. First we prove

$$C_G(N) = C/Y. \tag{4.3}$$

By Lemma A.5, we have $C_H(\mathrm{SL}(n,q)) = C$. By $\mathrm{SL}(n,q)' = \mathrm{SL}(n,q)$ and the Three Subgroup Lemma [**Rob96**, p.122, 5.1.10], this yields (4.3). Next we show

$$Z(G) = C/Y. \tag{4.4}$$

The inclusion "$\subseteq$" is obvious by (4.3). For the converse, we let $g \cdot \varphi \in H$ with $g \in \mathrm{GL}(n,q), \varphi \in \mathrm{Aut}\,\mathrm{GF}(q)$. We have $s \in \mathbb{Z}$ such that $\varphi(u) = u^{p^s}$ for all $u \in \mathrm{GF}(q)$. For $c \in C$, we then find

$$c^{g\cdot\varphi} = c^{\varphi} = c^{p^{-s}}.$$

Hence $c^{g\cdot\varphi} \equiv c \bmod Y$. Thus all elements in C/Y are central in H/Y. This completes the proof of (4.4).

Thus N satisfies $C_G(N) = Z(G)$, $N' = N$ and $N/(N \cap Z(G))$ is simple by Lemma A.3. Now Lemma 2.2, (3) $\Rightarrow$ (1), yields that N satisfies (C.1) and (C.2) in G.

Let $\lambda(G/N)$ be the Scott-length of G/N, and let $Z := Z(G)$. Lemma 2.12 yields

$$|(N:G)_{I(G)}| = \frac{\exp(Z)}{\gcd(\exp(Z),\lambda)} \cdot |N|^{|G:Z|-1}. \tag{4.5}$$

By (4.4), the center of G is a cyclic group of order $p-1$. It remains to prove that

$$p-1 \text{ divides } \lambda. \tag{4.6}$$

To this end, we let w be a primitive element of $\mathrm{GF}(q)$ and $g := \mathrm{diag}(w,1,\dots,1)$. We will show

$$G' = (\mathrm{SL}(n,q)\cdot\langle g^{p-1}\rangle)/Y. \tag{4.7}$$

We note that $Y \subseteq \mathrm{SL}(n,q)\cdot\langle g^{p-1}\rangle$ by definition. Since there is $\varphi \in \mathrm{Aut}\,\mathrm{GF}(q)$ such that $g^{\varphi} = g^p$, we have $[g,\varphi] = g^{p-1} \in G'$. This proves "$\supseteq$" in (4.7). For the converse inclusion, we argue that $H/(\mathrm{SL}(n,q)\cdot\langle g^{p-1}\rangle)$ is abelian. Since this factor is generated by the projections of g and φ, it suffices that $g \equiv g^{\varphi}$ modulo $\mathrm{SL}(n,q)\cdot\langle g^{p-1}\rangle$. This was shown above. Hence we have (4.7).

By the definition of H and by the previous arguments, G/G' is the direct product of $\langle gG'\rangle$ and $\langle \varphi G'\rangle$. Thus the exponent of G/G' is the least common multiple of the respective orders, that is, $\exp(G/G') = \mathrm{lcm}(p-1,f)$. In particular, $p-1$ divides $\exp(G/G')$. Since $N \subseteq G'$, we have that $\exp(G/G')$ divides $\lambda(G/N)$ by the homomorphism theorem and by Lemma 1.3. Thus (4.6) is proved. Now the result follows from (4.5). □

The previous proof shows why $\mathrm{GL}(n,q)\cdot\mathrm{Aut}\,\mathrm{GF}(q)$ does not have property (C). To obtain $Z(G) = C_G(N)$ (cf. (4.4)), it is necessary to consider a factor of the semilinear group.

We note that G as in Theorem 4.11 has property (A) if and only if $\mathrm{SL}(n,q)\cdot\langle g^{p-1}\rangle = \mathrm{SL}(n,q)\cdot Y$ (see (4.7)). Hence G has property (A) iff $\mathrm{Aut}\,\mathrm{GF}(q)$ is trivial (that is $H = \mathrm{GL}(n,q)$) or $Y \cap \mathrm{SL}(n,q)$ is trivial. In general, G/N is a metacyclic group, namely, the semidirect product of $\langle gN \rangle$ with $\langle \varphi N \rangle$. We recall that $|I(G)| = |I(G/N)| \cdot |(N:G)_{I(G)}|$. Hence Theorem 4.11 reduces the problem of computing the size of $I(G)$ to the problem of determining $|I(G/N)|$. In Corollary 5.9 we will give a formula for the number of polynomial functions on a metacyclic group M under the assumption that M' and M/M' are cyclic and have coprime order. We note that this assumption is satisfied for $M := G/N$ iff $p-1$ and f are relatively prime. We do not know $|I(G/N)|$ for arbitrary G. We admit that we do not know the Scott-length of G/N either. In the proof of Theorem 4.11, it sufficed to determine $\gcd(\exp(Z(G)), \lambda(G/N))$ which we achieved by finding a large enough factor of $\lambda(G/N)$.

2. Unitary groups

The structure of unitary groups is quite similar to that of linear groups. (see Lemma A.4 and Lemma A.9). Therefore, it is not too surprising that we obtain similar results for their endomorphism near-rings by essentially the same proofs.

Theorem 3.4 allows to describe $I(G)$ for classical linear groups G and their non-solvable quotients (cf. Corollary 4.4).

Corollary 4.12. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3),(3,2)\}$. Let G be a subgroup of the unitary group $U(n,q^2)$ with $\mathrm{SU}(n,q^2) \subseteq G$, and let Y be a subgroup of $Z(G)$. Let $m := |G : \mathrm{SU}(n,q)|$, let $s := |\mathrm{SU}(n,q)|$, and let $k := |Y|$. Then we have*

$$|I(G/Y)| = \operatorname{lcm}\left(\frac{m \cdot \gcd(n,k)}{k}, \frac{\gcd(nm, q+1)}{k}\right) \cdot \left(\frac{s}{\gcd(n,k)}\right)^{\frac{m \cdot s}{\gcd(nm,q+1)}-1}.$$

Proof: By Lemma A.8, G/Y has property (A). We also find that the center of G/Y is cyclic and has size $\frac{\gcd(mn,q+1)}{k}$ by Lemma A.9. From the definition of G/Y, we immediately obtain $|G/Y| = \frac{m \cdot s}{k}$. We compute

$$|G/Y : Z(G/Y)| = \frac{\frac{m \cdot s}{k}}{\frac{\gcd(mn,q+1)}{k}} = \frac{m \cdot s}{\gcd(mn, q+1)}.$$

By Lemma A.9, we have $(G/Y)' = (\mathrm{SL}(n,q)Y)/Y$ and $|(G/Y)'| = s/\gcd(n,k)$. By the homomorphism theorem, $(G/Y)/(G/Y)'$ is cyclic and has size, and, hence, exponent,

$$|(G/Y) : (G/Y)'| = \frac{m \cdot \gcd(n,k)}{k}.$$

Now the formula given in Theorem 3.4 yields the expression for $|I(G/Y)|$ stated in the corollary. □

The characterization of polynomial functions in Lemma 2.1 together with the description of automorphisms of unitary groups in Lemma A.10 yields the following:

THEOREM 4.13. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let G be a group such that $\mathrm{SU}(n, q^2) \subseteq G \subseteq \mathrm{U}(n, q^2)$. Then we have:*

1. *$I(G) = A(G)$;*
2. *$I(G) = E(G)$ if and only if $G = \mathrm{SU}(n, q^2)$.*

As in the case of linear groups (see Lemma 4.6), we will prove a slightly stronger version of Theorem 4.13 (1).

LEMMA 4.14. *Let G be as in Theorem 4.13, and let α be an endomorphism of G with $\mathrm{Ker}(\alpha) \subseteq Z(G)$. Then we have $\alpha \in I(G)$.*

Proof: By Lemma A.8, G has property (A). By Lemma A.10, we have $a \in \mathbb{N}$ such that $\alpha(z) = z^a$ for all $z \in Z(G)$ and $\det \alpha(x) = (\det x)^a$ for all $x \in G$. We define the function $f \in A(G)$ as

$$f(x) = x^{-a} \cdot \alpha(x) \text{ for all } x \in G.$$

Then we have $f(G) \subseteq \mathrm{SU}(n, q^2)$ and $f(z) = 1$ for all $z \in Z(G)$. Since $f(gz) = f(g) \cdot f(z)$ for all $g \in G, z \in Z(G)$, Lemma 2.1, (2) ⇒ (1), yields $f \in I(G)$. Thus α is a polynomial function. The lemma is proved. □

Proof of Theorem 4.13: Item (1) follows from Lemma 4.14. As in the case of linear groups, we will derive (2) from Theorem 3.20. By Lemma A.8, G has property (A). Let $m := |G : \mathrm{SU}(n, q^2)|$. Then G is a semidirect product,

$$G = \mathrm{SU}(n, q^2) \cdot \langle \mathrm{diag}(w, 1 \ldots, 1) \rangle$$

with w a primitive m-th root of unity in $\mathrm{GF}(q^2)$. Since the complement $\langle \mathrm{diag}(w, 1 \ldots, 1) \rangle$ of $\mathrm{SU}(n, q^2)$ intersects $Z(G)$ trivially by Lemma A.9, we may apply Theorem 3.20.

We assume $I(G) = E(G)$. Then $|G : G'|$ and $|Z(G)|$ are relatively prime by Theorem 3.20 (3). Since $|G : G'| = m$ and $|Z(G)| = m \cdot \gcd(n, \frac{q+1}{m})$ by Lemma A.9, this yields $m = 1$. Hence we have $G = \mathrm{SU}(n, q^2)$.

Conversely, $I(\mathrm{SU}(n, q^2)) = E(\mathrm{SU}(n, q^2))$ follows from Corollary 3.19 (or from Theorem 3.20 together with Lemma 2.8) since $\mathrm{SU}(n, q^2)' = \mathrm{SU}(n, q^2)$ and $Z(\mathrm{SU}(n, q^2))$ is cyclic. □

Assuming the characterization of automorphisms of projective special unitary groups by Dieudonnè (see Lemma A.2), we obtain a generalization of Theorem 4.13 (1).

THEOREM 4.15. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3),(3,2)\}$. Let H be a group such that $\mathrm{SU}(n,q^2) \subseteq H \subseteq \mathrm{U}(n,q^2) \cdot \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$, and let Y be a subgroup of $Z(H)$. For $G := H/Y$ and $Z := Z(G)$, the following are equivalent:*

(1) *$I(G) = A(G)$;*
(2) *For all subgroups L of G such that $G' \subseteq L$ and L/G' is a cyclic direct factor in G/G', we have that $\gcd(|L : G'|, |Z|)$ divides $|L \cap Z|$;*
(3) *G/G' is cyclic, or the size of the Sylow 2-subgroup of $G/(G'Z)$ divides $|G' \cap Z|$;*
(4) *All endomorphisms from G to Z induce polynomial functions on G/G';*
(5) *All endomorphisms from G to Z are in $I(G)$.*

There are groups that satisfy the assumptions of the theorem above and do not satisfy $I(G) = A(G)$. We refer to $G := (\mathrm{U}(4,3^2) \cdot \{a * 1_4 \mid a \in \mathrm{GF}(3^2)^*\})/\langle -1_4 \rangle$. as considered in Example 3.27 at the end of Chapter 3, Section 5. There we argued that G/G' is not cyclic and that there exists an endomorphism from G into $Z(G)$ that is not a polynomial function. By (5) ⇒ (1) of the theorem above, we then have $I(G) < A(G)$.

Proof of Theorem 4.15: Let H satisfy the assumptions of the theorem. By Lemma A.8, we have $H' = \mathrm{SU}(n,q^2)$ and $Z(H) = H \cap \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$. Furthermore, H has property (A). Let Y be a subgroup of $Z(H)$, and let $G := H/Y$. Then Lemma 3.2 yields that

$$G' = (\mathrm{SU}(n,q^2)Y)/Y \text{ and } Z(G) = Z(H)/Y, \tag{4.8}$$

and that G has property A.

(1) ⇒ (2) is immediate by Lemma 1.15.

(2) ⇒ (3): We assume that G satisfies (2) and that G/G' is not cyclic. Let s denote the size of the Sylow 2-subgroup of $G/(G'Z)$. We will prove that s divides $|G' \cap Z|$. By Lemma A.8, we have a group L with $G' \subseteq L \subseteq (\mathrm{U}(n,q^2)Y)/Y$ such that L/G' is a 2-group and a cyclic direct factor in G/G'. We also note that $|Z : (L \cap Z)|$ is even, because otherwise G/G' is cyclic. Since the Sylow 2-subgroup of G/G' is contained in $(LZ)/G'$, we have

$$\frac{|LZ|}{|ZG'|} = s. \tag{4.9}$$

By (2), $\gcd(|L : G'|, |Z|)$ is equal to $\gcd(|L : G'|, |L \cap Z|)$, which then yields that

$$|L : G'| \text{ divides } |L \cap Z|. \tag{4.10}$$

By the homomorphism theorem, we have

$$(L \cap Z)/(G' \cap Z) \cong ((L \cap Z)G')/G'.$$

By $G' \subseteq L$ and the modular law, we obtain $(L \cap Z)G' = L \cap (ZG')$. Hence we have

$$|L \cap Z| = |G' \cap Z| \cdot |(L \cap (ZG'))/G'|.$$

By using the homomorphism theorem, we compute

$$\frac{|L \cap Z|}{|L : G'|} = \frac{|G' \cap Z| \cdot |(L \cap (ZG'))/G'|}{|L/(L \cap (ZG')| \cdot |(L \cap (ZG')/G'|} = \frac{|G' \cap Z|}{|(L \cap (ZG')/G'|}.$$

Then (4.10) yields that $|L/(L \cap (ZG'))|$ divides $|G' \cap Z|$. Since $L/(L \cap (ZG'))$ and $(LZ)/(ZG')$ are isomorphic and since the latter has order s by (4.9), we finally obtain that s divides $|G' \cap Z|$. Thus (3) is proved.

(3) ⇒ (2): For $x \in G$, we write $\bar{x} := xG'$, and for subgroups A of G, we write $\bar{A} := (AG')/G'$. Let p be a prime divisor of $|\bar{G}|$, and let L be a subgroup of G with $G' \subseteq L$ such that $\bar{L}$ is a cyclic p-group. Let $d := \gcd(|\bar{L}|, |Z|)$. Assuming (3), we will show that

$$d \text{ divides } |L \cap Z|. \tag{4.11}$$

We have a uniquely determined, cyclic subgroup C of Z with $|C| = d$. Since $|\bar{C}|$ divides d, we find that $|\bar{C}|$ divides $|\bar{L}|$. If the Sylow p-subgroup of $\bar{G}$ is cyclic, this yields $\bar{C} \subseteq \bar{L}$. Then C is contained in L, and we have (4.11). It remains to consider the case that the Sylow p-subgroup of $\bar{G}$ is not cyclic. Then $p = 2$ by Lemma A.8. Condition (3) yields that $|(\bar{L}\bar{Z})/\bar{Z}|$ divides $|G' \cap Z|$. Hence

$$|\bar{L}| \text{ divides } |\bar{L} \cap \bar{Z}| \cdot |G' \cap Z|. \tag{4.12}$$

Since $G' \subseteq L$, we find the following chain of isomorphic groups:

$$\bar{L} \cap \bar{Z} \cong (L \cap (ZG'))/G' \cong ((L \cap Z)G')/G' \cong$$
$$\cong (L \cap Z)/(L \cap Z \cap G') \cong (L \cap Z)/(G' \cap Z).$$

By (4.12), we then have that $|\bar{L}|$ divides $|(L \cap Z)/(G' \cap Z)| \cdot |G' \cap Z|$, which yields (4.11). Now (2) follows from (4.11), since each cyclic group is a direct product of cyclic p-groups.

(2) ⇒ (5) follows from Lemma 3.22.

(5) ⇔ (4) is Proposition 3.26.

(5) ⇒ (1): We will prove this by using Lemma 1.16 and Lemma A.2 together with Lemma 2.1. First we have to introduce some notation. Let F be the field $\mathrm{GF}(q^2)$. By (A.24) of Appendix A, Section 1, we have a semidirect product of $\mathrm{U}(n, q^2) \cdot \{a * 1_n \mid a \in F^*\}$ with $\operatorname{Aut} F$. For $\varphi \in \operatorname{Aut} F$ and $a \in \mathrm{GL}(n, q^2)$, the matrix a^φ has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j. We note that both H and the subgroup Y of $Z(H)$ are invariant under the action of $\operatorname{Aut} F$. Hence we may define the factor

$$A := (\mathrm{U}(n, q^2) \cdot \{a * 1_n \mid a \in F^*\} \cdot \operatorname{Aut} F)/Y.$$

We proceed to show that A, $N := G'$, and G satisfy the assumptions of Lemma 1.16. Let $C := C_A(N)$, $\bar{A} := A/C$, and $\bar{N} := (NC)/C$. First we assume $n \geq 3$. Then Lemma A.7 and the Three Subgroup Lemma [**Rob96**, p.122, 5.1.10] yield $C = \{a * 1_n \mid a \in F^*\}/Y$ and that $C_{\bar{A}}(\bar{N})$ is trivial. By Lemma A.2 and by the homomorphism theorem, the full automorphism group of $\bar{N}$ is isomorphic to $\bar{A}$.

The case $n = 2$ requires some extra consideration. Lemma A.7 and the Three Subgroup Lemma [**Rob96**, p.122, 5.1.10] yield $|C| = (q^2 - 1) \cdot 2/|Y|$ and that $C_{\bar{A}}(\bar{N})$ is trivial. By the definition of A, we then have $|\bar{A}| = \frac{|\mathrm{U}(2,q^2)| \cdot (q-1) \cdot |\mathrm{Aut}\, F|}{(q^2-1) \cdot 2}$. By Lemma A.7, this yields $|\bar{A}| = \frac{q \cdot (q^2-1) \cdot |\mathrm{Aut}\, F|}{2}$. Since $\bar{N}$ is isomorphic to $\mathrm{PSL}(2, q)$ by [**KL90**, Proposition 2.9.1] and $|\mathrm{Aut}\ \mathrm{PSL}(2, q)| = q \cdot (q^2 - 1) \cdot |\mathrm{Aut}\, \mathrm{GF}(q)|$ by Lemma A.2, we find $|\bar{A}| = |\mathrm{Aut}\, \bar{N}|$.

Hence, for all pairs (n, q) that satisfy the assumptions of the theorem, every automorphisms of $\bar{N}$ is induced by conjugation by some element of $\bar{A}$. We note that G is normal in A and $N \subseteq G$. Since G has property (A), we have $Z(G) = C \cap G$. Thus all assumptions of Lemma 1.16 are satisfied.

We are now ready to prove (1) under the assumption of (5). Let α be an automorphism of G. We will show $\alpha \in I(G)$. Since $N = G'$ is characteristic, we have $\alpha(N) \subseteq N$. By Lemma 1.16, there is $a \in A$ and there is an endomorphism ρ from G into $Z(G)$ such that

$$\alpha(x) = \rho(x) \cdot x^a \text{ for all } x \in G.$$

By assumption (5), we have $\rho \in I(G)$. It remains to prove that the automorphism $\sigma_a : G \to G,\ x \mapsto x^a$, is an element of $I(G)$. To this end, we let $b \in \mathrm{U}(n, q^2)$ and $\varphi \in \mathrm{Aut}\, F$ such that $a = b\varphi Y$. Let $m \in \mathbb{Z}$ such that $u^\varphi = u^m$ for all $u \in F$. By the definition of the action of $\mathrm{Aut}\, F$ on H, we obtain

$$z^a = z^{\varphi Y} = z^{-m} \text{ for all } z \in Z(G)$$

and

$$x^a \equiv x^{\varphi Y} \equiv x^{-m} \bmod N \text{ for all } x \in G.$$

Hence the function $f \in A(G)$ that is defined by

$$f(x) = x^m \cdot x^a \text{ for all } x \in G$$

maps G into N and satisfies $f(z) = 1$ for all $z \in Z(G)$. Since, by definition, f is a product of endomorphisms which map $Z(G)$ into $Z(G)$, we have $f(xz) = f(x) \cdot f(z)$ for all $x \in G, z \in Z(G)$. Now Lemma 2.1, (2) $\Rightarrow$ (1), yields that f is a polynomial function. From this we obtain $\sigma_a \in I(G)$. Thus we have $\alpha \in I(G)$. The proof of the theorem is complete. □

We give two straightforward specializations of Theorem 4.15.

Corollary 4.16. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let G be a group such that $\mathrm{SU}(n, q^2) \subseteq G \subseteq \mathrm{U}(n, q^2)$, and let $Y \subseteq Z(G)$.*

Then we have $I(G/Y) = A(G/Y)$.

Proof: We note that G/Y is a group with property (A) and cyclic center. Furthermore, the factor of G/Y by its derived subgroup is cyclic. By Lemma 3.23, all endomorphisms from G/Y into $Z(G/Y)$ are in $I(G/Y)$. Hence Theorem 4.15, (5) ⇒ (1), yields $I(G/Y) = A(G/Y)$. □

Corollary 4.17. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let G be a group such that $\mathrm{SU}(n, q^2) \subseteq G \subseteq \mathrm{U}(n, q^2) \cdot \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$.*

Then we have $I(G) = A(G)$.

Proof: We write $U := \mathrm{U}(n, q^2)$, $S := \mathrm{SU}(n, q^2)$, and $Z := Z(G)$. By Theorem 4.15, (3) ⇒ (1), it suffices to show that $|G : (G'Z)|$ divides $|G' \cap Z|$. We note that $|G : (G'Z)|$ divides $|U : (S \cdot Z(U))|$. Since $|U : S| = |Z(U)|$ by Lemma A.7 and Lemma A.9, this yields that $|G : (G'Z)|$ divides $|S \cap Z(U)|$. Now the result follows from Theorem 4.15. □

The size of $I(G)$ for the groups in Theorem 4.15 and Corollary 4.17 can be easily obtained from Theorem 3.4. For the groups G/Y as in Corollary 4.16, there is an explicit formula for $|I(G/Y)|$ in Corollary 4.12.

Next we determine necessary and sufficient conditions such that all endomorphisms of a unitary group are polynomial functions. We note that the following result generalizes Theorem 4.13 (2).

Theorem 4.18. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let G be a group such that $\mathrm{SU}(n, q^2) \subseteq G \subseteq \mathrm{U}(n, q^2) \cdot \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$, and let Y be a subgroup of $Z(G)$.*

Then we have $I(G/Y) = E(G/Y)$ if and only if $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime.

By (4.15) of the following proof, we find that both the center of G/Y and the factor of G/Y by its derived subgroup are cyclic if $I(G/Y) = E(G/Y)$. Hence these extensions of unitary groups satisfy the assumptions of Corollary 3.18.

Proof of Theorem 4.18: By Lemma A.8, we have that $G' = \mathrm{SU}(n, q^2)$ and that G has property (A). We note that G/G' is not necessarily cyclic and that G' has not necessarily a complement in G. Thus we cannot apply Proposition 3.21 right away as we did in the proof of Theorem 4.8. We need some preparation first.

We note that $G = G \cap (\mathrm{U}(n,q^2) \cdot Z(G))$ and that the latter is equal to $(G \cap \mathrm{U}(n,q^2)) \cdot Z(G)$ by the modular law. Let $G_1 := G \cap \mathrm{U}(n,q^2)$. Since $|\mathrm{U}(n,q^2) \cap \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}| = q+1$, we have that

$$|G : G_1| \text{ divides } q-1. \tag{4.13}$$

We assume $I(G/Y) = E(G/Y)$. First we will prove

$$G/Y = (G_1Y)/Y. \tag{4.14}$$

This will then enable us to use Proposition 3.21 to finish the proof. Seeking a contradiction, we suppose that a prime p divides $|(G/Y) : (G_1Y)/Y|$. Then p divides $q-1$ by (4.13).

First we assume that $p > 2$. As a divisor of $q-1$, p divides $|\mathrm{SU}(n,q^2)|$ by Lemma A.7, and p does not divide $|Z(\mathrm{SU}(n,q^2))|$ by Lemma A.9. Thus we have an element $s \in \mathrm{SU}(n,q^2) \setminus Z(\mathrm{SU}(n,q^2))$ with $\operatorname{ord} s = p$. Let c be a generator of the cyclic group $Z(G)$. We consider the endomorphism $\rho : G/Y \to \langle sY \rangle$ defined by $\rho(cY) = sY$ and $\mathrm{Ker}(\rho) = (G_1\langle c^p \rangle)/Y$. Then $Z(G/Y)$ is not invariant under ρ, which is contradicted by the assumption that ρ is in $I(G/Y)$.

Thus we have $p = 2$. This implies that q is odd. If $n > 2$, then we find that $s := \mathrm{diag}(-1,-1,1,\ldots,1)$ is an element of $\mathrm{SU}(n,q^2) \setminus Z(\mathrm{SU}(n,q^2))$. As in the previous argument, we can construct an endomorphism that is not contained in $I(G/Y)$. Hence we have $n = 2$. Since -1_2 is an involution in $\mathrm{SU}(2,q^2) \subseteq G_1$ and 2 divides $|G : G_1|$, the center of G contains an element b of order 4. Let $s := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $s \in \mathrm{SU}(2,q^2)$ and $s^2 = -1_2$. Thus sb is an involution in $G \setminus Z(G)$. Since $Z(G/Y)$ is not invariant under the endomorphism ρ of G/Y defined by $\rho(cY) = sbY$ and $\mathrm{Ker}(\rho) = (G_1\langle c^2 \rangle)/Y$, we obtain a final contradiction. Thus we have $|G/Y| = |(G_1Y)/Y|$ and (4.14) is proved.

Since we now have that G/Y is isomorphic to $G_1/(G_1 \cap Y)$, we may assume that $G = G_1$ and that Y is a subgroup of $Z(G_1)$. For $m := |G : \mathrm{SU}(n,q^2)|$, let d be a primitive m-th root of unity in $\mathrm{GF}(q^2)$. Then $H := \langle \mathrm{diag}(d,1,\ldots,1) \rangle$ is a complement for $\mathrm{SU}(n,q^2)$ in G, and we have $H \cap Z(G) = \{1_n\}$. Also, $Z(G)$ is cyclic by Lemma A.9. Hence G satisfies the assumptions of Proposition 3.21, which yields that $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime.

For proving the converse implication, we assume that $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime. We will show that

$$(G/Y)/(G/Y)' \text{ is cyclic.} \tag{4.15}$$

As above, we have that $G = (G \cap \mathrm{U}(n,q^2)) \cdot Z(G)$ and that $G' = \mathrm{SU}(n,q^2)$ has a cyclic complement H in $G \cap \mathrm{U}(n,q^2)$. Thus we obtain $G = G'H \cdot Z(G)$. The assumption that $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime, yields $Z(G/Y) \subseteq (G/Y)'$. Hence we have $G' \cdot Z(G) = G'Y$. By the homomorphism theorem, $(G/Y)/(G/Y)'$ is isomorphic to $G/(G'Y)$. The latter is equal to $(G'H \cdot$

$Z(G))/(G' \cdot Z(G))$. Hence $(G/Y)/(G/Y)'$ is isomorphic to $H/(H \cap (G' \cdot Z(G)))$ and in particular cyclic. Thus (4.15) is proved. Now $I(G/Y) = E(G/Y)$ follows from Proposition 3.21. □

The next result follows from Theorem 4.18 and yields Theorem 4.13 (2).

Corollary 4.19. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let G be a group such that $\mathrm{SU}(n, q^2) \subseteq G \subseteq U(n, q^2) \cdot \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$. Then we have $I(G) = E(G)$ if and only if $G = \mathrm{SU}(n, q^2)$.*

Proof: We assume $I(G) = E(G)$. Then $|G : \mathrm{SU}(n, q^2)|$ and $|Z(G)|$ are relatively prime by Theorem 4.18. In particular, we have $Z(G) \subseteq \mathrm{SU}(n, q^2)$. This yields $G \subseteq U(n, q^2)$. By Lemma A.9, we find $\gcd(|G : \mathrm{SU}(n, q^2)|, |Z(G)|) = |G : \mathrm{SU}(n, q^2)|$. Thus we have $G = \mathrm{SU}(n, q^2)$.

The converse implication follows from Corollary 3.19 since $\mathrm{SU}(n, q^2)' = \mathrm{SU}(n, q^2)$ and $Z(\mathrm{SU}(n, q^2))$ is cyclic. □

For groups of unitary semilinear transformations, we could give a result similar to Theorem 4.11 but we abstain from doing so.

3. Symplectic groups

The structure of symplectic groups is less complex than that of linear or unitary groups (see Appendix A). Consequently, the results in this section are more easily obtained than those in the previous 2 sections.

Corollary 4.20. *Let n be an even natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3)\}$. Let $\mathrm{sp}(n, q) := |\mathrm{Sp}(n, q)|$.*

1. *If q is odd, then we have $|I(\mathrm{Sp}(n, q))| = 2 \cdot \mathrm{sp}(n, q)^{\mathrm{sp}(n,q)/2-1}$.*
2. *If q is even and $(n, q) \neq (4, 2)$, then $|I(\mathrm{Sp}(n, q))| = \mathrm{sp}(n, q)^{\mathrm{sp}(n,q)-1}$.*
3. *$|I(\mathrm{Sp}(4, 2))| = 2 \cdot \left(\frac{\mathrm{sp}(4,2)}{2}\right)^{\mathrm{sp}(4,2)-1}$.*

We note that $\mathrm{sp}(n, q) = q^{n^2/4} \prod_{i=1}^{n/2} (q^{2i} - 1)$ in the corollary above (see Lemma A.13).

Proof: In Lemma A.13 the structure of symplectic groups is described as follows: $\mathrm{Sp}(n, q)$ is quasisimple with center of size 2 for q odd, $(n, q) \neq (2, 3)$. For q even and $(n, q) \notin \{(2, 2), (4, 2)\}$, we have that $\mathrm{Sp}(n, q)$ is simple. Thus Corollary 3.5 yields (1) and (2). Item (3) follows from the fact that $\mathrm{Sp}(4, 2)$ is isomorphic to the symmetric group S_6 (see Lemma A.13) and Theorem 3.4. □

Theorem 4.21. *Let n be an even natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3)\}$. Let $G = \mathrm{Sp}(n, q)$ be a symplectic group. Then we have $I(G) = A(G) = E(G)$.*

Proof: By Lemma A.13, the symplectic group $\mathrm{Sp}(n,q)$ is quasisimple with cyclic center for $(n,q) \neq (4,2)$, and $\mathrm{Sp}(4,2)$ is isomorphic to the symmetric group S_6. Thus Theorem 4.21 is an immediate consequence of Corollary 3.18. □

We note that the proof of Theorem 4.21 did not require any information on what the automorphisms of $\mathrm{Sp}(n,q)$ look like. By using the description of the automorphisms of the projective symplectic group, we can generalize the previous result to extensions of $\mathrm{Sp}(n,q)$.

THEOREM 4.22. *Let n be an even natural number with $n \geq 2$, let q be a prime power such that $(n,q) \notin \{(2,2),(2,3)\}$. Let w be a primitive element of* $\mathrm{GF}(q)$. *Let G be a group such that* $\mathrm{Sp}(n,q) \subseteq G \subseteq \mathrm{Sp}(n,q) \cdot \langle \mathrm{diag}(w,1,\ldots,w,1)\rangle$, *and let Y be a subgroup of $Z(G)$. Then we have:*

(1) *$I(G/Y) = A(G/Y)$;*

(2) *$I(G/Y) = E(G/Y)$ if and only if $(G/Y)' = G/Y$ or $Z(G/Y)$ is trivial.*

Proof: Let $Z := Z(G)$. By Lemma A.13 and Lemma 2.2, (3) $\Rightarrow$ (1), we have that G and $N := \mathrm{Sp}(n,q)$ satisfy (C.1) and (C.2) in G. Since $G' = \mathrm{Sp}(n,q)$, Lemma 3.1 yields that G has property (A). We have that G/G' is cyclic by definition, and Z is cyclic by Lemma A.13.

First we will prove (1) for q even. For $n=4$, $q=2$, we have $G = \mathrm{Sp}(4,2)$, $|G:G'| = 2$, and that Z is trivial by Lemma A.13. Then the assertion follows from Corollary 3.10. We now assume $(n,q) \neq (4,2)$ and q even. By (A.39) in Appendix A, Section 8, we then have $\mathrm{Sp}(n,q) \cdot \langle \mathrm{diag}(w,1,\ldots,w,1)\rangle = \mathrm{Sp}(n,q) \cdot \langle w * 1_n \rangle$. Hence $G = G'Z$ and $G' \cap Z = \{1_n\}$. Since G' is simple, non-abelian and Z is cyclic, $I(G) = A(G)$ then follows from Corollary 3.11.

For proving (1) under the assumption that q is odd, we will use Proposition 3.15. Let F be the field $\mathrm{GF}(q)$. For $\varphi \in \mathrm{Aut}\, F$ and $a \in \mathrm{GL}(n,q)$, the matrix a^{φ} has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j. By (A.40) in Appendix A, Section 8, this action of $\mathrm{Aut}\, F$ defines the semidirect product

$$A := (\mathrm{Sp}(n,q) \cdot \langle \mathrm{diag}(w,1,\ldots,w,1)\rangle) \cdot \mathrm{Aut}\, F.$$

Let $C := C_A(\mathrm{Sp}(n,q))$. By Lemma A.2, A/C is isomorphic to $\mathrm{Aut}\,((\mathrm{Sp}(n,q)C)/C)$. Here we also use that $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$ (see Lemma A.13).

Hence A and G satisfy the assumptions (1), (2), and (3) of Proposition 3.15. For $a \in A$, we will now prove that $\sigma_a : G \to G,\ x \mapsto x^a$, is an element of $I(G)$. To this end, we let $b \in \mathrm{GL}(n,q)$ and $\varphi \in \mathrm{Aut}\, F$ such that $a = b\varphi$. Let $m \in \mathbb{Z}$ such that $u^{\varphi} = u^m$ for all $u \in F$. Then we have

$$z^a = z^{\varphi} = z^{-m} \text{ for all } z \in Z(G)$$

and

$$x^a \equiv x^{\varphi} \equiv x^{-m} \bmod \mathrm{Sp}(n,q) \text{ for all } x \in G.$$

Hence the function $f \in A(G)$ that is defined by

$$f(x) = x^m \cdot x^a \text{ for all } x \in G$$

maps G into $\mathrm{Sp}(n, q)$ and satisfies $f(z) = 1$ for all $z \in Z(G)$. We also find $f(xz) = f(x) \cdot f(z)$ for all $x \in G, z \in Z(G)$. Lemma 2.1, (2) $\Rightarrow$ (1), yields that f is a polynomial function. From this we obtain $\sigma_a \in I(G)$. Proposition 3.15 yields $I(G/Y) = A(G/Y)$.

Item (2) will follow from Proposition 3.21. We recall that Z is cyclic, and we note that there exists $d \in \mathrm{GF}(q)$ such that $H := \langle \mathrm{diag}(d, 1, \ldots, d, 1)\rangle$ is a complement for G' in G. Since $H \cap Z = \{1_n\}$, we have $I(G/Y) = E(G/Y)$ if and only if $|(G/Y) : (G/Y)'|$ and $|Z(G/Y)|$ are relatively prime by Proposition 3.21. We assume $\gcd(|(G/Y) : (G/Y)'|, |Z(G/Y)|) = 1$, and we show that

$$(G/Y)' = G/Y \text{ or } Z(G/Y) \text{ is trivial.} \tag{4.16}$$

By the assumption, we have $Z(G/Y) \subseteq (G/Y)'$. Then Z is contained in $G'Y$, which yields

$$G'Z = G'Y. \tag{4.17}$$

Hence we have $\frac{|Z|}{|Z \cap G'|} = \frac{|Y|}{|Y \cap G'|}$. By $Z \cap G' = \langle -1_n \rangle$, we then obtain that

$$|Z/Y| \text{ divides } 2. \tag{4.18}$$

Since $\langle d * 1_n \rangle \subseteq Z$ and $Z \cap G' = \langle -1_n \rangle$, we have that $|G : (G'Z)|$ divides 2. By (4.17), this yields that

$$|(G/Y) : (G/Y)'| \text{ divides } 2. \tag{4.19}$$

The assumption $\gcd(|(G/Y) : (G/Y)'|, |Z(G/Y)|) = 1$ together with (4.18) and (4.19) yield (4.16).

For proving the converse, we assume that (4.16) holds. Since both $(G/Y)/(G/Y)'$ and $Z(G/Y)$ are cyclic, Corollary 3.18 yields $I(G/Y) = E(G/Y)$. □

The size of $I(G/Y)$ for the groups in Theorem 4.22 can be obtained from Theorem 3.4.

Corollary 4.23. *Let n be an even natural number with $n \geq 2$, let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (4, 2)\}$. Let w be a primitive element of* $\mathrm{GF}(q)$*, and let G be a group such that* $\mathrm{Sp}(n, q) \subseteq G \subseteq \mathrm{Sp}(n, q) \cdot \langle \mathrm{diag}(w, 1, \ldots, w, 1)\rangle$*. Then we have $I(G) = E(G)$ if and only if $G = \mathrm{Sp}(n, q)$.*

Proof: This is immediate from Theorem 4.22 (2). □

4. Orthogonal groups

In Section 9 of Appendix A, we distinguish three types of orthogonal matrix groups, $\mathrm{O}^{\circ}(n,q)$, $\mathrm{O}^{+}(n,q)$, and $\mathrm{O}^{-}(n,q)$ for odd prime powers q. While there are some differences in the lattice of normal subgroups in these three cases, it turns out that the polynomial functions behave quite similar.

Theorem 4.24. *Let n be a natural number with $n \geq 5$, let q be an odd prime power, and let $\varepsilon \in \{\circ, +, -\}$. Then we have:*

(1) $|I(\mathrm{O}^{\varepsilon}(n,q))| = |\Omega^{\varepsilon}(n,q)|^{2\cdot|\Omega^{\varepsilon}(n,q)|-1} \cdot 2$;

(2) $|A(\mathrm{O}^{\varepsilon}(n,q))| = 2 \cdot |I(\mathrm{O}^{\varepsilon}(n,q))|$.

Formulae for the size of $\Omega^{\varepsilon}(n,q)$ can be obtained from the Lemmas A.15, A.16, and A.17.

Proof of Theorem 4.24: By Proposition A.14, $G := \mathrm{O}^{\varepsilon}(n,q)$ has property (A) and

$$G' = \Omega^{\varepsilon}(n,q) \text{ and } Z(G) = \langle -1_n \rangle.$$

Since G/G' is elementary abelian of order 4 and $|Z(G)| = 2$, Lemma 2.12 yields

$$|(G' : G)_{I(G)}| = |G'|^{|G|/2-1}.$$

Now (1) follows from $|I(G/G')| = 2$ and $|I(G)| = |(G' : G)_{I(G)}| \cdot |I(G/G')|$.

Next we prove (2). For $f \in A(G)$, we let $\bar{f} : G/G' \to G/G'$, $xG' \mapsto f(x)G'$. Then $\bar{f}$ is well-defined, and

$$\varphi : A(G) \to A(G/G'),\ f \to \bar{f}$$

is a homomorphism by Lemma 1.6. We show

$$|\varphi(A(G))| = 4. \tag{4.20}$$

By Lemma A.18 we have a unique normal subgroup H of G with $|H : G'| = 2$ that is characteristic. Hence $\operatorname{Aut} G$ acts on G/G' as $\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}$ acts on the vector-space $(\mathbb{Z}_2)^2$. Thus we obtain (4.20). We show that

$$(G' : G)_{A(G)} = (G' : G)_{I(G)}. \tag{4.21}$$

The inclusion "$\supseteq$" is obvious. For proving "$\subseteq$", we let $f \in A(G)$ such that $f(G) \subseteq G'$. Then we have $k \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_k \in \operatorname{Aut} G$ such that

$$f(x) = \alpha_1(x) \cdots \alpha_k(x) \text{ for all } x \in G.$$

Since the automorphisms $\alpha_1, \ldots, \alpha_k$ fix H with $|H : G'| = 2$ and since $f(H) \subseteq G'$ by assumption, we obtain that k is even. By $|Z(G)| = 2$, we then have $f(z) = 1$ for all $z \in Z(G)$. Since f is a product of automorphisms, we have $f(xz) = f(x) \cdot f(z)$ for all $x \in G, z \in Z(G)$. Lemma 2.1, (2) $\Rightarrow$ (1), yields $f \in I(G)$. Hence (4.21) is proved. From $|I(G/G')| = 2$ and (4.20) together with (4.21) we obtain $|A(G)| = 2 \cdot |I(G)|$. The proof is complete. □

When determining $|A(G)|$ for $G := \mathrm{O}^{\varepsilon}(n,q)$ in the theorem above, we were lucky that all elements of $A(G)$ that map G into G' are polynomial functions (see (4.21)). We note that $(G' : G)_{I(G)} < (G' : G)_{E(G)}$. Hence we are not able to determine $|E(G)|$. However, we know that $A(G) < E(G)$.

The next result describes relations between endomorphism near-rings for subgroups of $\mathrm{O}^{\varepsilon}(n,q)$.

THEOREM 4.25. *Let n be a natural number with $n \geq 5$, let q be an odd prime power, and let $\varepsilon \in \{\circ, +, -\}$. We assume that G is a group such that $\Omega^{\varepsilon}(n,q) \subseteq G \subseteq \mathrm{O}^{\varepsilon}(n,q)$. Then we have:*

(1) *$I(G) = A(G)$ if and only if $G < \mathrm{O}^{\varepsilon}(n,q)$;*
(2) *$I(G) = E(G)$ if and only if $G = \Omega^{\varepsilon}(n,q)$ or $-1_n \notin G$;*
(3) *$A(G) = E(G)$ if and only if $I(G) = E(G)$.*

As in the corresponding results for classical groups in the previous sections, item (2) of the theorem above simply states that $I(G) = E(G)$ if and only if $G = G'$ or $Z(G) = \{1\}$.

We note that for groups G that satisfy the assumptions of the previous theorem, $|I(G)|$ and $|A(G)|$ are given in Theorem 4.24 or can be obtained from Theorem 3.4.

Proof of Theorem 4.25: For $\varepsilon \in \{\circ, +, -\}$ fixed, we write $O := \mathrm{O}^{\varepsilon}(n,q)$, $S := \mathrm{SO}^{\varepsilon}(n,q)$, and $\Omega := \Omega^{\varepsilon}(n,q)$. By Proposition A.14, G has property (A), and we have

$$G' = \Omega \text{ and } Z(G) = G \cap \langle -1_n \rangle.$$

For proving (1), we note that $|G : G'| \leq 2$ and $|Z(G)| \leq 2$ for $G < O$. Then Corollary 3.14 yields $I(G) = A(G)$. By Theorem 4.24, we have $I(O) < A(O)$. This completes the proof of (1).

Next we will show (2). If $G = \Omega$ or $Z(G) = \{1_n\}$, then we have $I(G) = E(G)$ by Corollary 3.18. Since $I(O) < E(O)$ by (1), it remains to prove that $I(G) < E(G)$ for G such that $|G : \Omega| = 2$ and $Z(G) = \langle -1_n \rangle$. First we assume that $-1_n \notin \Omega$. Then G is the direct product of Ω and $\langle -1_n \rangle$. Since Ω has even order by Lemma A.15, A.16, A.17, respectively, there exists an involution i in Ω. We have an endomorphism ρ of G such that $\rho(-1_n) = i$ and $\mathrm{Ker}(\rho) = \Omega$. Then $Z(G)$ is not invariant under ρ. Hence ρ is not in $I(G)$, and we have $I(G) < E(G)$.

Next we assume $-1_n \in \Omega$. By Proposition A.14, Ω has a complement H in G. Since $Z(G)$ and H intersect trivially by assumption and since $|G : G'| = |Z(G)| = 2$, Theorem 3.20 yields $I(G) < E(G)$. Item (2) is proved.

For (3), it suffices to show that $A(O) < E(O)$. Since Ω has a complement in O by Proposition A.14, the homomorphism theorem yields

$$|E(O)| = |(\Omega : O)_{E(O)}| \cdot |E(O/\Omega)|.$$

We have $|E(O/\Omega)| = 16$ and $(\Omega : O)_{I(O)} \subseteq (\Omega : O)_{E(O)}$. Hence we have $|E(O)| \geq 8 \cdot |I(O)|$. Theorem 4.24 yields (3). The lemma is proved. □

By Lemma A.19, we have that the orthogonal groups on vector spaces over fields of even characteristic are extensions of a non-abelian simple groups by the cyclic group of order 2. Furthermore, these groups are centerless. Due to this very plain structure, our questions concerning endomorphism near-rings are easily answered.

Theorem 4.26. *Let V be a vector space of dimension at least* 6 *over a finite field F of even characteristic, and let Q be a non-degenerate quadratic form on V over F. We write $O := I(V, F, Q)$ and $\Omega := \Omega(V, F, Q)$. Then we have:*

1. $|I(\Omega)| = |\Omega|^{|\Omega|-1}$ *and* $|I(O)| = 2 \cdot |\Omega|^{2 \cdot |\Omega|-1}$*;*
2. $I(\Omega) = E(\Omega)$ *and* $I(O) = E(O)$*.*

The assertions on Ω in the previous theorem follow immediately from [**Frö58**] since Ω is non-abelian and simple. By this work, all functions on Ω are polynomial. Since Ω is the unique minimal normal subgroup in O, the results on $I(O)$ and $E(O)$ are readily obtained by the methods of [**FK95**]. For completeness and because of its brevity, we also give a proof using our own arguments.

Proof of Theorem 4.26: The group Ω is simple and non-abelian by Lemma A.19. Hence Theorem 3.4 and Corollary 3.18 yield the assertions on Ω. Since, by Lemma A.19, O is centerless and $|O : \Omega| = 2$, Lemma 3.1 yields that O has property (A). The results on O follow from Theorem 3.4 and Corollary 3.18. □

CHAPTER 5

Polynomial functions on certain semidirect products

We shall determine the number of polynomial functions on all finite solvable groups all of whose abelian subgroups are cyclic and on all Frobenius complements. Then the problem of computing $|I(G)|$ for a Frobenius group G with kernel N is reduced to that of computing the number of restrictions of functions in $I(G)$ to N. The starting point for all this is a description due to E. Aichinger of the polynomial functions on certain semidirect products that have a Frobenius group as quotient.

1. A characterization

We rewrite E. Aichinger's original result on the number of polynomial functions in such a way that we have a formula for $|I(G)|$.

Theorem 5.1 ([**Aic02**, Theorem 1.1]). *Let G be a finite group. We assume that $G = AB$ is the semidirect product of a normal subgroup A and a subgroup B. We let $Z := C_B(A)$, and we assume that the following conditions are satisfied:*

1. *For all $b \in B \setminus Z$, we have $C_A(b) = \{1\}$;*
2. *For all normal subgroups X, Y of B with $X \prec_B Y \subseteq Z$, we have $C_B(Y/X) \nsubseteq Z$.*

Let the set S be defined by

$$S := \{f|_A \mid f \in I(G)\}.$$

Then we have

$$|I(G)| = |I(B)| \cdot |S|^{|B:Z|} \cdot |A|^{|B:Z|-1}.$$

In the following we use the notation of the theorem above. We note that $I(A) \subseteq S \subseteq A(A)$, where the latter denotes the subgroup of $M(A)$ that is generated by all automorphisms of the group A. Hence we have bounds for the size of S,

$$|I(A)| \leq |S| \leq |A(A)|. \tag{5.1}$$

If A is abelian and every element of B acts on A as an automorphism of the form $a \mapsto a^r$ for some $r \in \mathbb{Z}$, then the size of S is given by $|S| = \exp A$. We will use this fact for cyclic groups A in Section 3. See Section 7 for more information on

S if A is abelian. In Section 8 we will determine S for a certain class of groups AB with A non-abelian.

We have to add some comments on the hypotheses of Theorem 5.1. In (1), the condition $C_A(b) = \{1\}$ is equivalent to

$$a^b \neq a \text{ for all } a \in A, a \neq 1. \tag{5.2}$$

Some authors express (5.2) by saying that the map $\varphi_b : A \to A, a \mapsto a^b$, is a *fixed-point-free automorphism* on A with the understanding that 1 is the only fixed point of φ_b in A.

In Lemma 5.4, we will show that for $|B| > 1$, condition (1) of Theorem 5.1 can be replaced by the assumption that G/Z is a Frobenius group with complement B/Z (see Appendix B for definitions).

Our condition (2) of Theorem 5.1 is weaker than the original formulation (2′) in [**Aic02**] which is stated as:

(2′) For all normal subgroups X, Y of B with $X \prec_B Y \subseteq Z$, we have $C_B(Y/X) > Z$.

The proof of Theorem 5.1 as given in [**Aic02**] actually uses only the weaker statement (2). See the definition of the function $\mathbf{i}_2^{(w)}$ in the proof of Lemma 2.1 in [**Aic02**, p.66].

As we did with the theorem above, we restate E. Aichinger's description of the elements of $P(G)$ as a description of the elements of $I(G)$. We will not use this result in this thesis.

Corollary 5.2 ([**Aic02**, Corollary 2.3]). *Let $G = AB$ be a group satisfying the assumptions of Theorem 5.1, let $Z := C_B(A)$, let $k := |B : Z|$, let $b_0 = 1, b_1, \ldots, b_{k-1}$ be a transversal for the cosets of Z in B. For a function $f : G \to A$, the following are equivalent:*

1. *$f \in I(G)$;*
2. *We have $f(1) = 1$, and for every $j \in \{0, 1, \ldots, k-1\}$ there is $p_j \in P(G)$ such that for all $a \in A$, $z \in Z$: $f(ab_jz) = p_j(a)$.*

2. A description of groups that satisfy the assumptions of Theorem 5.1

It is not difficult to see that Theorem 5.1 applies to Frobenius groups.

Lemma 5.3. *Let G be a Frobenius group with Frobenius kernel A and Frobenius complement B. Then G, A, and B satisfy conditions* (1) *and* (2) *of Theorem 5.1.*

Proof: We have $C_B(A) = \{1\}$ by the definition of Frobenius complement and kernel. Thus $C_A(b) = \{1\}$ for all $b \in B, b \neq 1$. Hence we have condition (1) of Theorem 5.1, and condition (2) is trivially satisfied. □

Frobenius groups and polynomial functions have also been considered in a different context. J. Ecker characterized the Frobenius groups G with the property that all compatible functions on G are polynomial functions [**Eck03**].

Let $G = AB$ be a semidirect product. The assumptions of Theorem 5.1 are certainly satisfied if $|B| = 1$. However the assertion of the theorem is trivial for this case. For $|B| > 1$, condition (2) of Theorem 5.1 yields $B > C_B(A)$. Hence the following lemma shows that Theorem 5.1 is of interest in the case of extensions by Frobenius groups only.

Lemma 5.4. *Let $G = AB$ be the semidirect product of a normal subgroup A and a subgroup B. Let $Z := C_B(A)$. Then the following are equivalent:*

(1) *$B > Z$ and $C_A(b) = \{1\}$ for all $b \in B \setminus Z$;*

(2) *G/Z is a Frobenius group with Frobenius complement B/Z and Frobenius kernel $(AZ)/Z$.*

Proof: We write $\bar{U} := (UZ)/Z$ for subgroups U of G and $\bar{x} := xZ$ for $x \in G$.

(1) ⇒ (2): We assume (1) and show that $\bar{B} \cap \bar{B}^{\bar{g}} = \{\bar{1}\}$ for all $\bar{g} \in \bar{G} \setminus \bar{B}$. To this end, let $g \in G \setminus B$, $b \in B$ such that $b^g \in B$. By $g \notin B$, we have $a \in A, a \neq 1$, $c \in B$ such that $g = ac$. Then we obtain $b^a \in B$, which yields $[b, a] \in B$. Since A is normal in G, we have $[b, a] \in A$. From $[b, a] \in A \cap B = \{1\}$ we finally obtain that a centralizes b. By (1), b is in Z. Thus $\bar{B} \cap \bar{B}^{\bar{g}} = \{\bar{1}\}$, and $\bar{G}$ is a Frobenius group with complement $\bar{B} \neq \{\bar{1}\}$ and kernel $\bar{A}$.

(2) ⇒ (1): We assume that $\bar{G}$ is a Frobenius group with complement $\bar{B}$. Then $B > Z$ and we have $B \cap B^a \subseteq Z$ for all $a \in A, a \neq 1$. Thus if $b^a = b$ for some $a \in A, a \neq 1$, then $b \in Z$. This proves (1). □

We note that as a Frobenius kernel the group A of Theorem 5.1 is nilpotent (see Theorem B.4). For the structure of the Frobenius complement B/Z see Appendix B.

By the next lemma, condition (2) of Theorem 5.1 is trivially fulfilled if B is nilpotent and the product AB is not direct.

Lemma 5.5. *Let $G = AB$ be the semidirect product of a normal subgroup A and a subgroup B. We assume that B is nilpotent and $B > Z$. Then we have:*

(1) *If $C_A(b) = \{1\}$ for all $b \in B \setminus Z$, then B/Z is either cyclic or the direct product of a cyclic group of odd order and a generalized quaternion group;*

(2) *For all normal subgroups X, Y of B with $X \prec_B Y \subseteq Z$, we have $C_B(Y/X) \not\subseteq Z$.*

Proof: For (1), we note that B/Z is nilpotent and a Frobenius complement by Lemma 5.4. Hence B/Z is the direct product of its Sylow p-subgroups which are cyclic for p odd, cyclic or generalized quaternion groups for $p = 2$ by Theorem B.4. Thus we have (1). Item (2) is immediate from $B > Z$ and the fact that B centralizes Y/X for all normal subgroups X, Y of B with $X \prec_B Y \subseteq Z$. □

3. Extensions of cyclic groups

From the description of polynomial functions in Section 1, we will obtain results on arbitrary semidirect products of a cyclic group and a group of coprime order. One of our goals is to describe $I(G)$ for metacyclic groups G where $|G'|$ and $|G : G'|$ are relatively prime (see Corollary 5.9). We start with a more general setting.

THEOREM 5.6. *Let G be a finite group, and let A be a cyclic normal subgroup of G such that $|A|$ and $|G : A|$ are relatively prime. Let M be the set of Sylow subgroups of A. Then we have*

$$|I(G)| = |I(G/A)| \cdot |A| \cdot (\prod_{P \in M} |P|^{|G:C_G(P)|-1})^2. \tag{5.3}$$

We note that unlike for Theorem 5.1, we do not require any additional conditions on the structure of G/A in the statement of Theorem 5.6. For its proof, we will use the following auxiliary result.

LEMMA 5.7. *Let G be a finite group, let p be a prime, and let P be a Sylow p-subgroup of G. We assume that P is cyclic and normal in G. Let $N := \{x \in P \mid x^p = 1\}$, and let $C := C_G(P)$. Then we have:*

1. *$C = C_G(N)$, and G/C is a cyclic group whose order divides $p - 1$;*
2. *For all $b \in G \setminus C$, we have $C_P(b) = \{1\}$;*
3. *$|I(G)| = |I(G/P)| \cdot |P|^{2 \cdot |G:C|-1}$.*

Proof: Let G, p, and P satisfy the assumptions of the lemma. For proving (1), we let $b \in G$. We will show that

$$C_N(b) > \{1\} \text{ implies } b \in C. \tag{5.4}$$

Let $a \in C_N(b), a \neq 1$. Since P is cyclic, we have $r \in \mathbb{N}$ such that $x^b = x^r$ for all $x \in P$. Hence $a^b = a$ yields $p|r - 1$. Let $f \in \mathbb{N}$ such that $|P| = p^f$. Since $(1 + dp)^{p^{f-1}} \equiv 1 \bmod p^f$ for all $d \in \mathbb{N}$ by [**Hup67**, p.83, Hilfssatz 13.18], we have $b^{p^{f-1}} \in C$. Then b is in C since $P \subseteq C$ and, consequently, p does not divide $|G : C|$. Thus (5.4) is proved. From this we obtain $C_G(N) \subseteq C$. Since the inclusion "$\supseteq$" is obviously true by the fact that P is a p-group, we have $C_G(N) = C$. The first part of (1) is proved. Now G/C can be embedded into $\operatorname{Aut} N$, which is a cyclic group of order $p - 1$. Hence we have the second part of (1).

Item (2) follows from (5.4) since P is a p-group.

We use Theorem 5.1 to prove (3). By the Schur-Zassenhaus Theorem [**Rob96**, 9.1.2], we have a complement K for P in C. Since P is central in C, the subgroup K is normal in C. Since the orders of P and K are relatively prime, K is characteristic in C. Hence K is normal in G. By Lemma 1.7, we then have

$$|I(G)| = \frac{|I(G/P)| \cdot |I(G/K)|}{|I(G/(PK))|}. \tag{5.5}$$

By (2), G/K is a Frobenius group with a cyclic Frobenius kernel of order $|P|$ and a cyclic Frobenius complement of order $|G : C|$. Theorem 5.1 (cf. [**Aic02**, Theorem 4.1]) yields

$$|I(G/K)| = |G : C| \cdot |P|^{2 \cdot |G:C| - 1}. \tag{5.6}$$

By $|I(G/(PK))| = |G : C|$, assertion (3) follows from (5.5) and (5.6). The lemma is proved. □

Proof of Theorem 5.6: Let G and A satisfy the assumptions of the theorem. We will prove (5.3) by induction on the number of prime divisors of $|A|$. For $|A| = 1$ the theorem is trivially true. Now we assume $|A| > 1$. Let Q be a non-trivial Sylow subgroup of A. From Lemma 5.7 (3) we obtain

$$|I(G)| = |I(G/Q)| \cdot |Q| \cdot (|Q|^{|G:C_G(Q)| - 1})^2. \tag{5.7}$$

Let M denote the set of Sylow subgroups of A. Then the Sylow subgroups of A/Q are given by $(PQ)/Q$ for $P \in M$. Since the number of prime divisors of $|A : Q|$ is smaller than that of $|A|$, we may apply the induction assumption to obtain

$$|I(G/Q)| = |I(G/A)| \cdot |A/Q| \cdot (\prod_{P \in M \setminus \{Q\}} |P|^{|G:C_G(P)| - 1})^2. \tag{5.8}$$

Here we have used that G/A is isomorphic to $(G/Q)/(A/Q)$ and that $C_{G/Q}((PQ)/Q) = C_G(P)/Q$ for $P \in M \setminus \{Q\}$. From (5.7) and (5.8) we obtain (5.3). The theorem is proved. □

For groups with a cyclic normal subgroup, whose order is coprime to its index, it is easy to decide whether all endomorphism are polynomial functions. It is not even necessary to use Corollary 5.2 for this case.

THEOREM 5.8. *Let G be a finite group, and let A be a cyclic normal subgroup of G such that $|A|$ and $|G : A|$ are relatively prime. Then we have $I(G) = E(G)$ if and only if $I(G/A) = E(G/A)$.*

Proof: Since A is cyclic, we have $I(A) = E(A)$. Now the result follows from Proposition 1.14. □

From Theorem 5.6 we obtain a formula for the number of polynomial functions on those groups all of whose Sylow subgroups are cyclic. By Theorem B.5, these are exactly the groups G that have a presentation as given in the following Corollary 5.9.

Corollary 5.9. *We let $m, n, r \in \mathbb{N}$ such that* $\gcd(m, n(r-1)) = 1$ *and* $m | r^n - 1$. *Let G be the group defined by*

$$G := \langle a, b \mid a^m = b^n = 1, a^b = a^r \rangle.$$

For a prime divisor p of m, let m_p denote the maximal power of p that divides m, and let t_p denote the multiplicative order of r modulo p. Then we have

$$|I(G)| = mn \cdot (\prod_{p|m,\ p\ prime} {m_p}^{t_p - 1})^2.$$

In [**MM94**, Theorem 3.11], the size of $I(G)$ has been determined by a different approach. We state the formula given there using the parameters of Corollary 5.9:

$$|I(G)| = mn \cdot (\prod_{i=2}^{n} s_i)^2,$$

where s_i is the additive order of $(r-1)(r^2-1)\cdots(r^{i-1}-1)$ modulo m.

We note that G is the semidirect product of $\langle a \rangle$ and $\langle b \rangle$ and that the orders of a and b are relatively prime. In particular, G is metacyclic. A group H is said to be *metacyclic* if it has a cyclic normal subgroup N such that H/N is cyclic.

Proof of Corollary 5.9: Let $A := \langle a \rangle$, $B := \langle b \rangle$. By assumption, $|G : A| = |B| = n$ and $|A| = m$ are relatively prime. We apply Theorem 5.6.

Let p be a prime divisor of m, and let P be a Sylow p-subgroup of A. Then P has order m_p. Let t_p be the smallest positive integer such that $p | r^{t_p} - 1$. Then we have $|G : C_G(\{x \in P \mid x^p = 1\})| = t_p$, which yields $|G : C_G(P)| = t_p$ by Lemma 5.7 (1). From Theorem 5.6 we obtain

$$|I(G)| = |I(B)| \cdot m \cdot (\prod_{p|m,\ p \text{ prime}} {m_p}^{t_p - 1})^2.$$

Since B is cyclic, we have $|I(B)| = n$ and the result follows. □

Corollary 5.10 ([**MM94**, Theorem 3.12], [**LP95**, Theorem 3.2]).
Let G be a group as defined in Corollary 5.9. Then we have $I(G) = E(G)$.

We note that, by the previous result, all normal subgroups of G as in Corollary 5.9 are fully invariant (see Proposition 1.9).

The non-abelian metacyclic groups G that satisfy $I(G) = E(G)$ have been characterized in 2 papers by G. L. Peterson. These groups are semidirect products of 2 cyclic groups (not necessarily of coprime order) [**Pet95**, Theorem 4.2], [**Pet96**].

Proof of Corollary 5.10: Let $a \in G$ be as in Corollary 5.9, and let $A := \langle a \rangle$. By the definition of G, we have that $|A|$ and $|G : A|$ are relatively prime. Since G/A is cyclic, we have $I(G/A) = E(G/A)$. Hence the result follows from Theorem 5.8. □

We mention that the previous Corollaries 5.9 and 5.10 apply to the dihedral group D_{2m} of order $2m$ for odd m. We have $|I(D_{2m})| = 2m^3$ and $I(D_{2m}) = E(D_{2m})$ (see [**LM72**]). In particular, we obtain $|I(S_3)| = 54$ and $I(S_3) = E(S_3)$. For investigating polynomial functions on D_{2m} for even m, a different approach is necessary (see [**LM73**]).

4. Extensions of metacyclic groups

We consider groups G that have a normal subgroup N all of whose Sylow subgroups are cyclic.

Theorem 5.11. *Let G be a finite group, and let N be a normal subgroup of G such that all Sylow subgroups of N are cyclic. We assume that $|N|$ and $|G : N|$ are relatively prime. Let M_1 denote the set of Sylow subgroups of N', and let M_2 denote the set of Sylow subgroups of N/N'. Then we have*

$$|I(G)| = |I(G/N)| \cdot |N| \cdot (\prod_{P \in M_1} |P|^{|G:C_G(P)|-1})^2 \cdot (\prod_{P \in M_2} |P|^{|G/N':C_{G/N'}(P)|-1})^2.$$

We note that N' and N/N' are in fact cyclic of relatively prime orders and that N has a presentation as given in Corollary 5.9. Hence the formula for $|I(G)|$ that is given in this corollary can be obtained from Theorem 5.11 for $G = N$ and the appropriate choice of the parameter m, n, r.

Proof of Theorem 5.11: We will obtain the result by applying Theorem 5.6 twice. By Theorem B.5, N' is cyclic and $\gcd(|N'|, |N : N'|) = 1$. Hence $|N'|$ and $|G : N'|$ are relatively prime. By Theorem 5.6, we obtain

$$|I(G)| = |I(G/N')| \cdot |N'| \cdot (\prod_{P \in M_1} |P|^{|G:C_G(P)|-1})^2. \tag{5.9}$$

Since N/N' is cyclic, Theorem 5.6 yields

$$|I(G/N')| = |I(G/N)| \cdot |N/N'| \cdot (\prod_{P \in M_2} |P|^{|G/N':C_{G/N'}(P)|-1})^2. \tag{5.10}$$

The result follows from (5.9) and (5.10). □

We give a criterion for $I(G) = E(G)$ for the groups that are dealt with in Theorem 5.11.

Theorem 5.12. *Let G be a finite group, and let N be a normal subgroup of G such that all Sylow subgroups of N are cyclic. We assume that $|N|$ and $|G : N|$ are relatively prime. Then we have $I(G) = E(G)$ if and only if $I(G/N) = E(G/N)$.*

Proof: By Corollary 5.10, we have $I(N) = E(N)$. Proposition 1.14 yields the result. □

5. Solvable Frobenius complements

Let G be a finite solvable group all of whose abelian subgroups are cyclic. We note that every solvable Frobenius complement satisfies this assumption (see Theorem B.4 (2) in Appendix B). By Theorem B.6, the group G is some extension of a metacyclic group. The results that we have developed in this chapter so far are almost sufficient to compute $|I(G)|$. What we still need is a description of the polynomial functions on a certain quotient of G which is isomorphic to one of the following: a generalized quaternion group (see [**Mal73**] and Example 5.28), $\mathrm{SL}(2,3)$ (see Proposition 5.24), or the binary octahedral group (see Proposition 5.26).

In the following we consider groups of types I to IV according to the classification in Theorem B.6. Since for the groups of type I all Sylow subgroups are cyclic, they are covered by Corollary 5.9. Next we apply Theorem 5.11 to the groups of type II.

Theorem 5.13. *Let G be a group of type* II. *Then G has a normal subgroup N such that all Sylow subgroups of N are cyclic, $|N|$ is odd, and G/N is a generalized quaternion group of order 2^{t+1} with $t \geq 2$. Let M_1 denote the set of Sylow subgroups of N', and let M_2 denote the set of Sylow subgroups of N/N'. Then we have*

$$|I(G)| = 2^{3t-2} \cdot |N| \cdot (\prod_{P \in M_1} |P|^{|G:C_G(P)|-1})^2 \cdot (\prod_{P \in M_2} |P|^{|G/N':C_{G/N'}(P)|-1})^2.$$

We will prove Theorem 5.13 together with the following result.

Theorem 5.14. *Let G be a group of type* II. *Then we have $I(G) < E(G)$.*

Proof of Theorem 5.13 and 5.14: Let a, b, q be generators of the group G with relations as given in Theorem B.6. Then $N := \langle a, b^{2^t} \rangle$ satisfies the assumptions of the theorem. The generalized quaternion group $Q := \langle b^{n/2^t}, q \rangle$ of order 2^{t+1} is a complement for N in G. The size of $I(Q)$ is given as $|I(Q)| = 2^{3t-2}$ in [**Mal73**]. Then Theorem 5.13 follows from Theorem 5.11.

Since $I(N) = E(N)$ by Corollary 5.10 and $I(Q) < E(Q)$ by [**Mal73**], Proposition 1.14, (1) $\Rightarrow$ (2), yields $I(NQ) < E(NQ)$. Theorem 5.14 is proved. □

In the case of groups of type III and IV, we make use of the existence of normal subgroups of relatively prime order and of Lemma 1.7.

Theorem 5.15. *Let G be a group of type* III, *and let Q be the normal Sylow* 2*-subgroup of G, which is isomorphic to the quaternion group of order* 8. *Then all Sylow subgroups of G/Q are cyclic, and we have*

$$|I(G)| = |I(G/Q)| \cdot 2^{22}.$$

Proof: Let a, b, p, q be generators of the group G with relations as given in Theorem B.6. Then $Q := \langle p, q\rangle$ is the normal Sylow 2-subgroup of G, which is isomorphic to the quaternion group of order 8. We note that $\langle a, b\rangle$ is a complement for Q in G and that all Sylow subgroups of $\langle a, b\rangle$ are cyclic. Let $H := \langle a, b^3\rangle$. Then H is normal in G, and H has odd order. By Lemma 1.7, we have

$$|I(G)| = \frac{|I(G/Q)| \cdot |I(G/H)|}{|I(G/(HQ))|}.$$

Since HQ has index 3 in G, we find $|I(G/(HQ))| = 3$. The quotient G/H is isomorphic to $\mathrm{SL}(2, 3)$. Since we have $|I(\mathrm{SL}(2, 3))| = 3 \cdot 2^{22}$ by Proposition 5.24, the result follows. □

THEOREM 5.16. *Let G be a group of type IV, and let $Q := \langle p, q\rangle$ be the normal subgroup of G, which is isomorphic to the quaternion group of order 8. Then all Sylow subgroups of G/Q are cyclic, $|G : Q|$ is 2 times an odd number, and we have*

$$|I(G)| = |I(G/Q)| \cdot 2^{57}.$$

Proof: Let a, b, p, q, z be generators of the group G with relations as given in Theorem B.6. We use the same reasoning as in the case of Theorem 5.15. We consider the normal subgroups $Q := \langle p, q\rangle$ and $H := \langle a, b^3\rangle$ of G. Then Q is a quaternion group of order 8, all Sylow subgroups of H are cyclic, and H has odd order. By Lemma 1.7, we have

$$|I(G)| = \frac{|I(G/Q)| \cdot |I(G/H)|}{|I(G/(HQ))|}.$$

The quotient $G/(HQ)$ is isomorphic to S_3. By Corollary 5.9, we have $|I(S_3)| = 54$. The quotient G/H is an extension of $\mathrm{SL}(2, 3)$, the so called binary octahedral group of order 48. By Proposition 5.26, we have $|I(G/H)| = 3^3 \cdot 2^{58}$. Hence the result follows. □

We note that for G/Q as in Theorems 5.15 and 5.16, the size of $I(G/Q)$ can be obtained from Corollary 5.9.

6. Non-solvable Frobenius complements

Let G be a non-solvable Frobenius complement. By Appendix B, Theorem B.7, there is a normal subgroup H in G with $|G : H| \leq 2$ such that H is isomorphic to the direct product of $\mathrm{SL}(2, 5)$ and a group M with $\gcd(|M|, 30) = 1$ such that all Sylow subgroups of M are cyclic. In particular, G has a normal subgroup S that is isomorphic to $\mathrm{SL}(2, 5)$.

Hence $|I(G)|$ follows immediately from our results on groups with property (A) (see Theorem 3.4) and on metacyclic groups (see Corollary 5.9) together with Lemma 1.7.

Theorem 5.17. *Let G be a Frobenius complement with a normal subgroup S that is isomorphic to* $\mathrm{SL}(2,5)$.

(1) *If $|G:S|$ is odd, then $|I(G)| = |I(G/S)| \cdot 120^{59} \cdot 2$.*
(2) *If $|G:S|$ is even, then $|I(G)| = |I(G/S)| \cdot 120^{119}$.*

We note that all Sylow subgroups of G/S as in Theorem 5.17 are cyclic. Hence $|I(G/S)|$ can be obtained from Corollary 5.9. We will prove Theorem 5.17 together with the next result.

Theorem 5.18. *Let G be a non-solvable Frobenius complement. Then we have $I(G) = E(G)$.*

Proof of Theorem 5.17 and 5.18 : Let G be a non-solvable Frobenius complement. By Theorem B.7, we have a unique normal subgroup S in G such that S is isomorphic to $\mathrm{SL}(2,5)$.

First we assume that G/S has odd order. Then S has a direct complement M in G and $\gcd(|S|,|M|) = 1$ by Theorem B.7. Hence $|I(G)| = |I(S)| \cdot |I(M)|$ by Lemma 1.7 (1). By Corollary 4.4, we have $|I(\mathrm{SL}(2,5))| = 120^{59} \cdot 2$. Thus Theorem 5.17 (1) is proved.

We note that $I(S) = E(S)$ by Theorem 4.5 (2) and that $I(M) = E(M)$ by Corollary 5.10. Since SM is the direct product of groups S, M of relatively prime order, we then have $I(SM) = E(SM)$ by Lemma 1.7 (3). This proves Theorem 5.18 for the case that $|G:S|$ is odd.

Next we assume that G/S has even order. By Theorem B.7, we have a normal subgroup M of G such that $\gcd(|S|,|M|) = 1$ and $|G:SM| = 2$. Lemma 1.7 yields

$$|I(G)| = \frac{|I(G/S)| \cdot |I(G/M)|}{2}. \tag{5.11}$$

It remains to determine $|I(G/M)|$. We note that M has a complement H in G with $S \subseteq H$. We show that H has property (A) (see Chapter 3) so that we can apply Theorem 3.4 to obtain $|I(H)|$. To this end, we prove that S and $Z := Z(S)$ are the only non-trivial, proper normal subgroups of H.

Seeking a contradiction, we let N be a proper normal subgroup of H such that $N \not\subseteq S$. Then we have $NS = H$ by $|H:S| = 2$. Thus

$$H/N \cong S/(N \cap S). \tag{5.12}$$

Since S is quasisimple, we have $N \cap S \subseteq Z$. Thus $|N \cap S| \leq 2$. First we assume that $N \cap S = \{1\}$. Then $|N| = 2$ by (5.12). Now NZ is an elementary abelian group of order 4. This contradicts the fact that the Sylow 2-subgroups of H are generalized quaternion groups of order 16 by Theorem B.4 (2).

Next we assume that $N \cap S = Z$. By (5.12), we have $|N| = 4$ and that H/N is isomorphic to S/Z, that is to A_5. Since $N \subseteq C_H(N)$ and since $H/C_H(N)$ can be embedded into $\operatorname{Aut} N$, we obtain $H = C_H(N)$. Then N is a central subgroup of order 4 in H. Again we obtain a contradiction since the Sylow 2-subgroups of H are generalized quaternion groups. Thus all proper normal subgroups of H are contained in S.

The normal subgroups of S are given by $\{1\}, Z, S$. By $Z = Z(H)$ and $S = H'$, all of them are normal in H, and H has property (A) (see Chapter 3). Theorem 3.4 yields

$$|I(H)| = |S|^{|H:Z|-1} \cdot \operatorname{lcm}(\exp H/S, \exp Z).$$

Thus $|I(H)| = 120^{119} \cdot 2$. Since G/M is isomorphic to H, Theorem 5.17 (2) follows from (5.11).

We will prove $I(G) = E(G)$ by using Lemma 1.7 (3). We note that S and M are fully invariant. The quotient G/M is isomorphic to H. We show

$$I(H) = E(H). \tag{5.13}$$

We recall that the normal subgroups of H are given by $\{1\}, Z(H), H', H$, and that we have $|H : H'| = |Z(H)| = 2$. Let α be an endomorphism of H. If α is an automorphism of H, then $\alpha \in I(H)$ by Corollary 3.14. If $\operatorname{Ker}(\alpha) = Z(H)$, then $\alpha(H)$ has index 2 in H. Hence $\alpha(H)$ is normal in H which yields the contradiction $\alpha(H) = H'$. Next we assume $\operatorname{Ker}(\alpha) \supseteq H'$. Then $|\alpha(H)| \leq 2$. We note that central element of order 2 is the unique involution in H since the Sylow 2-subgroups of H are generalized quaternion groups. Hence $\alpha(H) \subseteq Z$. By Lemma 3.23, we have $\alpha \in I(G)$. Thus all endomorphisms of H are polynomial functions, and (5.13) is proved.

Since all Sylow subgroups of G/S are cyclic, Corollary 5.10 yields $I(G/S) = E(G/S)$. Clearly all endomorphisms of $G/(SM)$ are polynomial functions. Together with (5.13), Lemma 1.7 (3) yields $I(G) = E(G)$. This completes the proof of Theorem 5.18 □

7. Frobenius actions on abelian groups

Let $G = AB$ be a group with A abelian such that the assumptions of Theorem 5.1 are satisfied. We note that A is necessarily abelian if the order of $B/C_B(A)$ is even (see Lemma B.3).

In [**Aic02**] it is already noted that an abelian group A is an R-module for the group ring $R := \mathbb{Z}_e[B/C_B(A)]$ where $e := \exp A$ and $B/C_B(A)$ acts on A by

$$(bC_B(A)) * a := a^b \text{ for all } a \in A, b \in B.$$

See Appendix C for notation and basic results on modules over group rings. For $r \in R$, we define a map $r_A : A \to A, x \mapsto r * x$. Then $h : R \to \operatorname{End}(A), r \mapsto r_A$, is a ring homomorphism with kernel $\operatorname{Ann}_R(A)$. We have

$$\{f|_A \mid f \in I(G)\} = \{r_A \mid r \in R\},$$

that is $S = h(R)$ and

$$|\{f|_A \mid f \in I(G)\}| = |R : \mathrm{Ann}_R(A)|. \tag{5.14}$$

By Lemma 5.4 and by Lemma B.2, the order of $B/C_B(A)$ and e are relatively prime. In Appendix C we present a decomposition of the R-module A and show that $\mathrm{Ann}_R(A)$ is the intersection of certain powers of maximal ideals in R (see Lemmas C.6, C.5). Thus we will obtain a formula for $|R : \mathrm{Ann}_R(A)|$ in terms of the indecomposable summands of A.

In the sequel we consider Frobenius groups with abelian kernel and complement which is either cyclic, the quaternion group of order 8, or $\mathrm{SL}(2,3)$. For these groups, the action of the complement on the kernel is easy to describe. See Appendix C, Section 3.

Proposition 5.19. *Let H be a Frobenius group with abelian Frobenius kernel V of exponent e and cyclic Frobenius complement G. Let $R := \mathbb{Z}_e[G]$, and let $M_1, \ldots, M_n$ be pairwise non-isomorphic simple R-modules such that $V = M_1(V) \dot{+} \cdots \dot{+} M_n(V)$. For $i \in \{1, \ldots, n\}$, let $q_i := \exp M_i(V)$, and let f_i be the rank of M_i as $\mathbb{Z}_e$-module. Then we have*

$$|I(H)| = |G| \cdot |V|^{|G|-1} \cdot (\prod_{i=1}^{n} q_i^{f_i})^{|G|}.$$

We note that by Lemma C.6, every abelian Frobenius kernel V has a decomposition as required in the proposition above.

Proof: The result follows from

$$|R : \mathrm{Ann}_R(V)| = \prod_{i=1}^{n} {q_i}^{f_i} \tag{5.15}$$

by (5.14) and Theorem 5.1. By Lemma B.2, e and $|G|$ are relatively prime. Hence we may apply the results of Appendix C, Section 2. Let M be a simple R-module of exponent p and rank f over $\mathbb{Z}_e$. We note that, since G is abelian, R is a commutative ring. Then $M(R/pR)$ is a field of order $|M|$ by Theorem C.4. Further $R/\mathrm{Ann}_R(M)$ is isomorphic to $\mathrm{GF}(p^f)$. Let $k \in \mathbb{N}$ such that $\exp M(V) = p^k$. Lemma C.5 yields $\mathrm{Ann}_R(M(V)) = (\mathrm{Ann}_R(M))^k$ and $|R : \mathrm{Ann}_R(M(V))| = p^{kf}$. By Lemma C.6, we then have (5.15). The proposition is proved. □

Example 5.20. As an application of Proposition 5.19, we determine the number of polynomial functions on A_4, the alternating group on 4 elements. We note that A_4 is a Frobenius group with an elementary abelian kernel K_4 of order 4 and a complement G of order 3. Obviously K_4 is simple as $\mathbb{Z}_2[G]$-module and has rank 2 over $\mathbb{Z}_2$. Proposition 5.19 yields

$$|I(A_4)| = 3 \cdot 4^2 \cdot 2^{2 \cdot 3} = 3072. \tag{5.16}$$

PROPOSITION 5.21. *Let H be a Frobenius group with Frobenius kernel V and Frobenius complement G.*

(1) *If G has order 2, then*
$$|I(H)| = 2 \cdot |V| \cdot (\exp V)^2.$$

(2) *If G is the quaternion group Q_8 of order 8, then*
$$|I(H)| = 2^4 \cdot |V|^7 \cdot (\exp V)^{32}.$$

(3) *If G is isomorphic to* $\mathrm{SL}(2,3)$*, then*
$$|I(H)| = 2^{22} \cdot 3 \cdot |V|^{23} \cdot (\exp V)^{96}.$$

Proof: For (1), we let i be the generator of G of order 2. Then we have $x^i = x^{-1}$ for all $x \in V$ by Lemma B.3. Hence $\{f|_V \mid f \in I(H)\} = I(V)$. The result now follows from Theorem 5.1.

We prove (2) and (3) together. Let $e := \exp G$, and let G be isomorphic to the quaternion group Q_8 or to $\mathrm{SL}(2,3)$. By Lemma B.3, V is abelian. By Lemma B.2, e and $|G|$ are relatively prime. Hence we may apply the results of Appendix C, Section 2, to $R := \mathbb{Z}_e[G]$. We will show

$$|R : \mathrm{Ann}_R(V)| = (\exp V)^4. \tag{5.17}$$

Let p be a prime divisor of e, and let M_p be a simple R-submodule of V such that $\exp M_p = p$. We show that

$$M_p(V) \text{ is the Sylow } p\text{-subgroup of } V. \tag{5.18}$$

We note that M_pG is a Frobenius group with kernel M_p and complement G. Let $\bar{R} := R/pR$. Then M_p is a simple $\bar{R}$-module by Lemma C.7. By Lemma C.9, C.10, respectively, all simple $\bar{R}$-modules that occur as kernels of Frobenius groups with complement G are isomorphic to M_p. Further $|\bar{R} : \mathrm{Ann}_{\bar{R}}(M_p)| = p^4$. Hence we have

$$|R : \mathrm{Ann}_R(M_p)| = p^4. \tag{5.19}$$

By Lemma C.7, all minimal R-submodules of V with exponent p are isomorphic to M_p. Hence we have (5.18).

Let k be maximal such that p^k divides $\exp V$. Then Lemma C.5 together with (5.19) yields $|R : \mathrm{Ann}_R(M_p(V))| = p^{4k}$. By Lemma C.6 and by (5.18), we have $|R : \mathrm{Ann}_R(V)| = \prod_{p | \exp V} |R : \mathrm{Ann}_R(M_p(V))|$. Hence we obtain (5.17). Now (2) follows from Theorem 5.1 with $|I(Q_8)| = 2^4$ (see Example 5.28) and (5.14). Item (3) is obtained with $|I(\mathrm{SL}(2,3))| = 2^{22} \cdot 3$ (see Proposition 5.24). □

8. Frobenius actions on unitriangular matrix groups

We present an example of a Frobenius group with non-abelian kernel and apply Theorem 5.1 to obtain the number of polynomial functions.

For a prime p and $m, n \in \mathbb{N}$ with $m > 1$, let

$$\mathrm{T}(m, p^n) := \{a \in \mathrm{GL}(m, p^n) \mid a_{ii} = 1, a_{ij} = 0 \text{ for all } i, j \in \{1, \dots, m\}, j < i\}.$$

The elements in $\mathrm{T}(m, p^n)$ are matrices over $\mathrm{GF}(p^n)$ with 1 on the diagonal and 0 below it and are called *upper unitriangular matrices.* We note that $\mathrm{T}(m, p^n)$ is a Sylow p-subgroup of $\mathrm{GL}(m, p^n)$. The nilpotent class of $\mathrm{T}(m, p^n)$ is $m - 1$ (see [**Hup67**, p.382, Satz 16.3 (b)]). These matrix groups occur as kernels of Frobenius groups [**Hup67**, p.499, 8.6 (c)].

Proposition 5.22. *For a prime p and $n \in \mathbb{N}$, let $u \in \mathrm{GF}(p^n)$ be of odd order k with $k > 1$, and let e be the multiplicative order of p modulo k. Let $A := \mathrm{T}(3, p^n)$, let $s := \mathrm{diag}(1, u, u^2)$, and let $G := A \cdot \langle s \rangle$. We write $S := \{f|_A \mid f \in I(G)\}$. Then we have:*

(1) *For all $f \in S$ there are $m_1, \dots, m_k \in \mathbb{N}$ and $r \in A$ such that*

$$f(g) = \prod_{i=1}^{k} (g^{m_i})^{s^i} \cdot [g, r] \text{ for all } g \in A.$$

(2) $|S| = p^e \cdot |(Z(A) : A)_S|$.

(3) *Let $f : A \to Z(A)$. Then $f \in S$ iff there are $a, b \in \mathrm{GF}(p^n)$, $c \in \mathrm{GF}(p^e)$ such that for all $x, y, z \in \mathrm{GF}(p^n)$:*

$$f(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}) = \begin{pmatrix} 1 & 0 & 2cz - cxy + bx - ay \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

(4) $|I(G)| = k \cdot p^{2(n+e)k} \cdot p^{3n(k-1)}$.

We note that

$$Z(T(3, p^n)) = T(3, p^n)' = \{a \in T(3, p^n) \mid a_{12} = a_{23} = 0\}.$$

In [**Aic02**, p. 78] an example of a semidirect product of $A := T(3, p^n)$ by a certain non-abelian group B is considered but the restrictions of polynomial functions of $A \cdot B$ to A are not determined. Since $(A \cdot B)/C_B(A)$ is isomorphic to some group G as in Proposition 5.22, our result yields a description of these functions.

We will prove Proposition 5.22 by using Theorem 5.1 and the following auxiliary result.

Lemma 5.23. *For a prime p and $n \in \mathbb{N}$, we have the following:*

(1) *Let $f : \mathrm{T}(3, p^n) \to \mathrm{T}(3, p^n)$. Then $f \in I(\mathrm{T}(3, p^n))$ iff there are $m \in \mathbb{N}$, $a, b \in \mathrm{GF}(p^n)$ such that for all $x, y, z \in \mathrm{GF}(p^n)$:*

$$f(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}) = \begin{pmatrix} 1 & mx & mz + \binom{m}{2} xy + bx - ay \\ 0 & 1 & my \\ 0 & 0 & 1 \end{pmatrix}.$$

(2) $|I(\mathrm{T}(3, p^n))| = p^{2n+1}$ *for p odd.*
(3) $|I(\mathrm{T}(3, 2^n))| = 2^{2n+2}$.

Proof: Let $G := \mathrm{T}(3, p^n)$, and let $f \in I(G)$. Since G is nilpotent of class 2, we have $m \in \mathbb{N}$ and $r \in G$ such that

$$f(g) = g^m \cdot [g, r] \text{ for all } g \in G \tag{5.20}$$

(see [**Eck98**, Theorem 1] or [**Eck01**, Proposition 1.7]). Now let $x, y, z \in \mathrm{GF}(p^n)$. By induction, we find that

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & mx & mz + \binom{m}{2} xy \\ 0 & 1 & my \\ 0 & 0 & 1 \end{pmatrix} \tag{5.21}$$

for $m \in \mathbb{N}$. For $a, b, c \in \mathrm{GF}(p^n)$, we have

$$[\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}] = \begin{pmatrix} 1 & 0 & bx - ay \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{5.22}$$

Thus, by (5.20), we have (1). From this we obtain $|I(G)| = \exp G \cdot p^{2n}$. Since $\exp \mathrm{T}(3, p^n) = p$ for p odd and $\exp \mathrm{T}(3, 2^n) = 4$ by (5.21), the assertions (2) and (3) follow. □

Proof of Proposition 5.22: Since k is odd, G is a Frobenius group with kernel $A = T(3, p^n)$ and complement $B := \langle \mathrm{diag}(1, u, u^2) \rangle$ (cf. [**Hup67**, p.499, 8.6 (c)]). By Theorem 5.1, we have

$$|I(G)| = |I(B)| \cdot |S|^{|B|} \cdot |A|^{|B|-1}. \tag{5.23}$$

For (4) it remains to determine $|S|$.

First we prove (1). As a subgroup of the group $M(A)$, S is generated by the automorphisms of A that are induced by conjugation by an element of G. We show that

$$S \text{ is abelian.} \tag{5.24}$$

Let $g := \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$, $r := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ be elements of A, and let $h := \operatorname{diag}(1, d, d^2) \in B$. We compute

$$g \cdot g^{rh} = \begin{pmatrix} 1 & x+dx & z+d^2(z+bx-ay)+dxy \\ 0 & 1 & y+dy \\ 0 & 0 & 1 \end{pmatrix} = g^{rh} \cdot g.$$

From this we obtain (5.24).

Let $f \in I(G)$. We recall that $s = \operatorname{diag}(1, u, u^2)$ is the generating element of B. By (5.24), we have $f_i \in I(A)$ for $i \in \{1, \dots, k\}$ such that

$$f(g) = \prod_{i=1}^{k} (f_i(g))^{s^i} \text{ for all } g \in A.$$

For $i \in \{1, \dots, k\}$, we have $m_i \in \mathbb{N}$ and $r_i \in A$ such that

$$f_i(g) = g^{m_i} \cdot [g, r_i] \text{ for all } g \in A$$

by Lemma 5.23 (1). Since A' is central in A, we find

$$f(g) = \prod_{i=1}^{k} (g^{m_i})^{s^i} \cdot \prod_{i=1}^{k} [g, r_i]^{s^i} \text{ for all } g \in A.$$

From (5.22) we obtain that there are $a, b \in \mathrm{GF}(p^n)$ such that

$$\prod_{i=1}^{k} [\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, r_i]^{s^i} = \begin{pmatrix} 1 & 0 & bx-ay \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence (1) is proved. For (2), we use (5.21) to compute

$$\prod_{i=1}^{k} (\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^{m_i})^{s^i} = \prod_{i=1}^{k} \begin{pmatrix} 1 & m_i u^i x & m_i u^{2i} z + \binom{m_i}{2} u^{2i} xy \\ 0 & 1 & m_i u^i y \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \sum_{i=1}^{k} m_i u^i x & \sum_{i=1}^{k} (m_i u^{2i} z + \binom{m_i}{2} u^{2i} xy) + \sum_{1 \le i < j \le k} m_i m_j u^{i+j} xy \\ 0 & 1 & \sum_{i=1}^{k} m_i u^i y \\ 0 & 0 & 1 \end{pmatrix}$$

where $m_1, \dots, m_k \in \mathbb{N}$. Consequently, by (1), the functions in S act on $A/Z(A)$ by multiplication with elements of the extension of $\mathrm{GF}(p)$ by u, that is, by multiplication with elements of $\mathrm{GF}(p^e)$. Then Lemma 1.6 yields (2).

Now we show (3). For the "only if"-direction, we let $m_1, \dots, m_k \in \mathbb{N}$, and let $f \in S$ be defined by $f(g) := \prod_{i=1}^{k} (g^{m_i})^{s^i}$ for $g \in A$. For $x \in \mathrm{GF}(p^n)$, we write $q(x) := \sum_{i=1}^{k} m_i x^i$ and $t(x) := \sum_{i=1}^{k} \binom{m_i}{2} x^{2i} + \sum_{1 \le i < j \le k} m_i m_j x^{i+j}$. As in the proof of (2) above, we have for all $x, y, z \in \mathrm{GF}(p^n)$:

$$f(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}) = \begin{pmatrix} 1 & q(u)x & q(u^2)z + t(u)xy \\ 0 & 1 & q(u)y \\ 0 & 0 & 1 \end{pmatrix}. \tag{5.25}$$

By $f(A) \subseteq Z(A)$, we have $q(u) = 0$. If p is odd, then $t(u) = \frac{1}{2}[q(u)^2 - q(u^2)]$. If $p = 2$, then $q(u^2) = 0$ since u and u^2 have the same minimal polynomial over $\mathrm{GF}(2)$. In any case it follows that all functions in $(Z(A) : A)_S$ are of the form given in (3).

For the converse implication, it suffices to show that for each $c \in \mathrm{GF}(p^e)$ the function $f : A \to A$ defined by

$$f(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}) := \begin{pmatrix} 1 & 0 & 2cz - cxy \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{5.26}$$

is in S. For $p = 2$, this follows from

$$(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^2)^{s^i} = \begin{pmatrix} 1 & 0 & u^{2i}xy \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for $i \in \mathbb{N}$ and the fact that every $c \in \mathrm{GF}(2^e)$ is a sum of powers of u^2. Next we assume that p is odd. Let $l(x) = \sum_{i=0}^{e} m_i x^i$ be the minimal polynomial of u over $\mathrm{GF}(p)$. Then the function $h_i : A \to A$ defined by

$$h_i(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}) := \begin{pmatrix} 1 & 0 & u^{2i} \cdot l(u^2) \cdot (z - \frac{1}{2}xy) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is in $(Z(A) : A)_S$ for all $i \in \mathbb{N}$. We note that $l(u^2) \neq 0$ because p is odd. The extension of $\mathrm{GF}(p)$ by u^2 is $\mathrm{GF}(p^e)$ because, by assumption, u has odd order. Hence all elements in $\mathrm{GF}(p^e)$ are of the form $\sum_{i=1}^{e} m_i u^{2i} l(u^2)$ for some $m_1, \dots, m_e \in \mathbb{N}$. Thus, for each $c \in \mathrm{GF}(p^e)$, f as in (5.26) is a product of functions in $\{h_1, \dots, h_e\}$. Finally $f \in S$ and (3) is proved.

From (2) and (3), we obtain $|S| = p^{2(e+f)}$. Now (4) follows from (5.23). The proof of the proposition is complete. □

9. $\mathrm{SL}(2,3)$, $\mathrm{GL}(2,3)$, and the binary octahedral group

In this section we determine the polynomial functions on $\mathrm{SL}(2,3)$ and on 2 of its extensions, namely $\mathrm{GL}(2,3)$ and the binary octahedral group. These groups already appeared in Section 5. Although the sizes of their endomorphism near-rings can be obtained from the computer algebra package [**ABE**$^+$**99**] under [**GAP02**], we are not aware that proofs of the results given in the following Propositions 5.24, 5.25, and 5.26 have been published. Hence we will present the interpolation arguments that allow us to reduce the problems to A_4 and S_4, respectively.

PROPOSITION 5.24. *For* $z := -1_2$ *in* $\mathrm{SL}(2,3)$ *and* $Z := \langle z \rangle$, *we have the following:*

(1) *Let* $f : \mathrm{SL}(2,3) \to Z$ *with* $f(1_2) = 1_2$. *Then* f *is in* $I(\mathrm{SL}(2,3))$ *iff* $f(xz) = f(x)f(z)$ *for all* $x \in \mathrm{SL}(2,3)$.
(2) $|I(\mathrm{SL}(2,3))| = 2^{22} \cdot 3$.
(3) $A(\mathrm{SL}(2,3)) = E(\mathrm{SL}(2,3))$ *and* $|E(\mathrm{SL}(2,3))| = 2^{28} \cdot 3$.

We note that $\mathrm{SL}(2,3)$ is an example of a group such that all normal subgroups are characteristic, even fully-invariant, but not all automorphisms are polynomial functions. For all other finite special linear groups, all endomorphisms are polynomial (see Theorem 4.5 and Corollary 5.10 for $\mathrm{SL}(2,2)$).

PROPOSITION 5.25. *For* $z := -1_2$ *in* $\mathrm{GL}(2,3)$ *and* $Z := \langle z \rangle$, *we have the following:*

(1) *Let* $f : \mathrm{GL}(2,3) \to Z$ *with* $f(1_2) = 1_2$. *Then* f *is in* $I(\mathrm{GL}(2,3))$ *iff* $f(xz) = f(x)$ *for all* $x \in \mathrm{GL}(2,3)$.
(2) $|I(\mathrm{GL}(2,3))| = 2^{58} \cdot 3^3$.
(3) $I(\mathrm{GL}(2,3)) = A(\mathrm{GL}(2,3))$.
(4) *Let* $f : \mathrm{GL}(2,3) \to Z$ *with* $f(1_2) = 1_2$. *Then* f *is in* $E(\mathrm{GL}(2,3))$ *iff* $f(xz) = f(x)f(z)$ *for all* $x \in \mathrm{GL}(2,3)$.
(5) $|E(\mathrm{GL}(2,3))| = 2^{59} \cdot 3^3$.

The group

$$G := \langle a, b, c, d \mid a^4 = 1, b^2 = a^2, c^3 = 1, d^2 = a^2, a^b = a^{-1}, \quad a^c = b, b^c = ab, a^d = ba, b^d = b^{-1}, c^d = c^{-1} \rangle \tag{5.27}$$

is called the *binary octahedral group*. We note that G has a normal subgroup of index 2 which is isomorphic to $\mathrm{SL}(2,3)$ and that G is distinct from $\mathrm{GL}(2,3)$. We have $Z(G) = \langle a^2 \rangle$ and that $G/Z(G)$ is isomorphic to S_4. The binary octahedral group is a Frobenius complement of type IV (see Theorem B.6).

PROPOSITION 5.26. *Let* G *be the binary octahedral group, and let* $Z := Z(G)$. *Then we have the following:*

(1) *Let $f : G \to Z$ with $f(1) = 1$. Then f is in $I(G)$ iff $f(xz) = f(x)$ for all $x \in G$ and for all $z \in Z$.*
(2) $|I(G)| = 2^{58} \cdot 3^3$.
(3) $I(G) = A(G) = E(G)$.

We note that $\mathrm{GL}(2, 3)$ and the binary octahedral group have the same lattice of normal subgroups and the same number of polynomial functions. Further all their normal subgroups are fully invariant. Still $\mathrm{GL}(2, 3)$ has an endomorphism that is not polynomial, while all endomorphisms of the binary octahedral group are polynomial functions.

For the proof of the Propositions 5.24, 5.25, and 5.26, we use the following criterion to decide whether a given function is polynomial.

Lemma 5.27. *Let G be a finite group, let Q be a normal subgroup of G such that Q is a quaternion group of order 8, and let $Z := Q'$. We assume that G/Z is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, A_4, or S_4. Let $\lambda := \lambda(G/Z)$ be the Scott-length of G/Z. Then the following are equivalent for each function $f : G \to Z$:*
(1) *The function f is in $I(G)$;*
(2) *We have $f(1) = 1$, and there exists an integer μ such that*

$$f(x \cdot z) = f(x) \cdot z^{\lambda\mu} \text{ for all } x \in G,\ z \in Z.$$

The assumptions of this lemma are satisfied for the quaternion group of order 8, $\mathrm{SL}(2, 3)$, $\mathrm{GL}(2, 3)$, and the binary octahedral group. We note that $\lambda(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$, $\lambda(A_4) = 3$, and $\lambda(S_4) = 2$.

Proof of Lemma 5.27: Since Z is characteristic in Q, we have that Z is normal in G. Together with $|Z| = 2$, this yields that Z is central in G. Hence the implication (1) ⇒ (2) is immediate (cf. proof of Lemma 2.1, (1) ⇒ (2)).

It remains to prove (2) ⇒ (1). To this end, we will show the existence of certain interpolation functions in $(Z : G)_{I(G)}$. As in the proof of Lemma 2.1, (2) ⇒ (1), Step 1, we have a function $i \in I(G)$ that satisfies

$$i(G) \subseteq Z \text{ and } i(z) = z^\lambda \text{ for all } z \in Z. \tag{5.28}$$

By assumption, Q/Z is the unique minimal normal subgroup of G/Z and $C_{G/Z}(Q/Z) = Q/Z$. Hence, by [**FK95**, Theorem 4.1 (2)], we have $e \in I(G)$ such that

$$e(q) \in qZ \text{ for all } q \in Q \text{ and } e(G \setminus Q) \subseteq Z. \tag{5.29}$$

Let a be an element of order 4 in Q. Then $c := a^2$ generates Z. We define $p \in I(Q)$ by

$$p(x) = x \cdot x^a \text{ for all } x \in Q.$$

Then p satisfies

$$p(aZ) = \{c\} \text{ and } p(Q \setminus aZ) = \{1\}. \tag{5.30}$$

For $t \in G \setminus Z$, we define $p_t \in I(G)$ by

$$p_t(x) = p(e(at^{-1}x)) \text{ for all } x \in G.$$

From (5.29) and (5.30), we obtain that

$$p_t(tZ) = \{c\} \text{ and } p_t(G \setminus tZ) = \{1\}. \tag{5.31}$$

We are ready for the interpolation argument. Let f be a function that satisfies (2) with $\mu \in \mathbb{N}$. We consider the function g on G that is defined by

$$g(x) = f(x) \cdot i(x)^{-\mu} \text{ for all } x \in G.$$

Then $g(G) \subseteq Z$ and $g(xz) = g(x)$ for all $x \in G, z \in Z$ by (5.28). Since g is constant on each coset of Z in G, we have that g is the product of certain functions p_t for $t \in G \setminus Z$ by (5.31). Hence $g \in I(G)$. By $i \in I(G)$, this implies $f \in I(G)$. The lemma is proved. □

The number of polynomial functions on the quaternion group of order 8 follows easily. For results on the generalized quaternion groups we have to refer to [**Mal73**].

Example 5.28. Let Q be the quaternion group of order 8. Since Q/Q' is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, the Scott-length of Q/Q' is 2. By Lemma 5.27, a function $f : Q \to Q'$ is in $I(Q)$ iff $f(1) = 1$ and f is constant on the cosets of Q' in Q. Hence

$$|(Q' : Q)_{I(Q)}| = 2^3.$$

By $|I(Q/Q')| = 2$ and Lemma 1.5, we obtain

$$|I(Q)| = 2^4.$$

We are now ready to prove our results on extensions of the quaternion group.

Proof of Proposition 5.24: Let $G := \mathrm{SL}(2, 3)$, let $z := -1_2$, and let $Z := \langle z \rangle$. Then $Z = Z(G)$. We note that

$$Q := \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$$

is a normal subgroup in G and that Q is isomorphic to the quaternion group of order 8. Further $Q' = Z$. Since G/Z is isomorphic to A_4 and $\lambda(A_4) = 3$, Lemma 5.27 yields (1). Thus we have

$$|(Z : G)_{I(G)}| = 2^{11} \cdot 2. \tag{5.32}$$

Together with $|I(A_4)| = 2^{10} \cdot 3$ (see Example 5.20 or [**FK95**, Example 2]), this yields (2).

For (3), we note that each automorphism of A_4 is induced by conjugation by an element in S_4 (see [**Sco87**, p.314 (11.4.8)]). Hence for every automorphism α of G/Z there is $a \in \mathrm{GL}(2, 3)/Z$ such that $\alpha(x) = x^a$ for all $x \in G/Z$. In particular, each automorphism of G/Z is induced by an automorphism of G. From Lemma 1.6, we obtain

$$|A(G)| = |(Z : G)_{A(G)}| \cdot |A(G/Z)|. \tag{5.33}$$

We proceed to show that

$$(Z : G)_{I(G)} = (Z : G)_{E(G)}. \tag{5.34}$$

The inclusion "$\subseteq$" is clear. The converse follows from (1) because Z is fully invariant in G. Together with (5.32), (5.33), and $|A(A_4)| = 2^{16} \cdot 3$ (see [**FK95**, Example 2]), this yields

$$|A(G)| = 2^{28} \cdot 3. \tag{5.35}$$

By Lemma 1.6, we have

$$|E(G)| \leq |(Z : G)_{E(G)}| \cdot |E(G/Z)|.$$

From $A(A_4) = E(A_4)$ (see [**FK95**, Example 2]) and (5.34) we obtain $|E(G)| \leq |A(G)|$. Hence we have (3). The proposition is proved. □

Proof of Proposition 5.25: Let $G := \mathrm{GL}(2, 3)$, let $z := -1_2$, and let $Z := \langle z \rangle$. Then $Z = Z(G)$. The group

$$Q := \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$$

is normal in G and isomorphic to the quaternion group of order 8.

$$H := \langle \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$$

is a complement for Q in G.

We note that G/Z is isomorphic to S_4 and that the Scott-length of S_4 is even since $|S_4 : A_4| = 2$. Hence Lemma 5.27 yields (1). We have

$$|(Z : G)_{I(G)}| = 2^{23}. \tag{5.36}$$

Together with $|I(S_4)| = 2^{35} \cdot 3^3$ (see [**FK95**, Example 3]), this yields (2).

Next we prove (3). By Lemma 1.6 and by $I(S_4) = A(S_4)$ (see [**Sco87**, p.314 (11.4.8)] or [**FK95**, Example 3]), we have

$$|A(G)| = |(Z : G)_{A(G)}| \cdot |I(G/Z)|. \tag{5.37}$$

It remains to show that

$$(Z : G)_{I(G)} = (Z : G)_{A(G)}. \tag{5.38}$$

The inclusion "$\subseteq$" is clear. For "$\supseteq$", we let $\alpha_1, \ldots, \alpha_n$ be automorphisms of G such that $f \in A(G)$ defined by $f(x) = \alpha_1(x) \cdots \alpha_n(x)$ for $x \in G$ satisfies $f(G) \subseteq Z$. Since $Z \subseteq \mathrm{SL}(2, 3)$ and $\mathrm{SL}(2, 3)$ is a characteristic subgroup of index 2 in G, we have that n is even. Hence $f(z) = z^n = 1$. Item (1) yields $f \in I(G)$. Thus (5.38) is proved, and (3) follows from (5.37).

Next we show (4). Since Z is fully invariant in G, every function $f \in E(G)$ satisfies $f(xz) = f(x)f(z)$ for all $x \in G$. For the converse implication, by (1), it suffices to show that there exists $f \in (Z : G)_{E(G)}$ such that $f(z) = z$. To construct such a function, we recall that, by [**FK95**, Theorem 4.1 (2)], there are $a_1, \ldots, a_n \in G$ such that

$$e : G \to G, x \mapsto \prod_{i=1}^{n} x^{a_i},$$

induces the identity function on Q/Z and $e(G \setminus Q) \subseteq Z$. Since G/Q is isomorphic to S_3, it has even Scott-length. Thus n is even, and we have $e(z) = 1$.

Now let π be the natural projection homomorphism from G onto the complement H of Q. We consider the map $f \in E(G)$ defined by

$$f(x) = (x\pi(x)^{-1})^{-1} \cdot e(x\pi(x)^{-1}) \text{ for all } x \in G.$$

Let $q \in Q, h \in H$. Then $f(qh) = q^{-1} \cdot e(q)$. Since $e(q) \in qZ$, we have $f(G) \subseteq Z$. Further $f(z) = z^{-1}e(z) = z$. Together with (1), this yields (4).

Since Z is fully invariant in G and $I(S_4) = E(S_4)$ (see [**FK95**, Example 3]), Lemma 1.6 yields

$$|E(G)| = |(Z : G)_{E(G)}| \cdot |I(G/Z)|. \tag{5.39}$$

From (4), we obtain

$$|(Z : G)_{E(G)}| = |(Z : G)_{I(G)}| \cdot 2.$$

Together with (5.39), this yields $|E(G)| = |I(G)| \cdot 2$. Hence (5) follows from (2). The proof of the proposition is complete. □

Proof of Proposition 5.26: Let G be the binary octahedral group with generators a, b, c, d satisfying the relations given in (5.27). Then $Q := \langle a, b \rangle$ is a quaternion group of order 8, and Q is normal in G. We note that $Z := \langle a^2 \rangle$ is the center of G and that G/Z is isomorphic to S_4. Since the Scott-length of S_4 is even, Lemma 5.27 yields (1). Hence we have

$$|(Z : G)_{I(G)}| = 2^{23}. \tag{5.40}$$

Together with $|I(S_4)| = 2^{35} \cdot 3^3$ (see [**FK95**, Example 3]), this yields (2).

Since Z is fully invariant in G and $I(S_4) = E(S_4)$ (see [**FK95**, Example 3]), Lemma 1.6 yields

$$|E(G)| = |(Z : G)_{E(G)}| \cdot |I(G/Z)|. \tag{5.41}$$

Hence, for (3), it suffices to show that

$$(Z : G)_{I(G)} = (Z : G)_{E(G)}. \tag{5.42}$$

The inclusion "$\subseteq$" is clear. For "$\supseteq$", we let $\alpha_1, \dots, \alpha_n$ be endomorphisms of G such that $f \in E(G)$ defined by

$$f(x) = \alpha_1(x) \cdots \alpha_n(x) \text{ for all } x \in G$$

satisfies $f(G) \subseteq Z$. Since $z := a^2$ is the unique involution in G, all endomorphisms of G either are bijective or map into Z. Let k be number of automorphisms in $\{\alpha_1, \dots, \alpha_n\}$. Then k is even since $|G : G'| = 2$ and $Z \subseteq G'$. Hence we obtain $f(xz) = f(x) \cdot z^k \cdot 1^{n-k} = f(x)$ for all $x \in G$. Item (1) yields $f \in I(G)$. Thus we have (5.42), and (3) follows from (5.41). The proposition is proved. □

APPENDIX A

Classical groups

We define finite classical groups as in [**KL90**]. The properties of these groups of linear and semilinear transformations on vector spaces are heavily studied and well documented. We only gather information on their normal subgroups and automorphisms to the extent that is necessary for proving our results of Chapter 4. For the vast majority of facts stated in this chapter, we refer to proofs in textbooks that are widely available. In the rare case that we cannot find the proof of a result in the literature, we supply one in the most elementary terms and without the pretense of originality.

1. Linear and semilinear transformations

Let V be a vector space of finite dimension n over the finite field $F := \mathrm{GF}(q)$ with q elements. We write $\mathrm{GL}(V, F)$ for the *general linear group* of V over F, which is the group of all invertible F-linear transformations of V. Let $B = (b_1, \ldots, b_n)$ be a basis of V over F, and let $g \in \mathrm{GL}(V, F)$. Then there are uniquely determined coefficients $a_{ij} \in F$ with $i, j \in \{1, \ldots, n\}$ such that $g(b_i) = \sum_{j=1}^{n} a_{ij} b_j$. Let g_B denote the $n \times n$ matrix with entry a_{ij} in row i and column j. We have an isomorphism,

$$h_B : \mathrm{GL}(V, F) \to \mathrm{GL}(n, q),\ g \mapsto g_B, \tag{A.1}$$

where $\mathrm{GL}(n, q)$ is the group of invertible $n \times n$ matrices with entries in $\mathrm{GF}(q)$. We define $\det g = \det g_B$ for all $g \in G$, and we note that this definition is independent of the choice of the basis B. Let $\mathrm{SL}(n, q) := \{x \in \mathrm{GL}(n, q) \mid \det x = 1\}$, and let $\mathrm{SL}(V, F) := \{g \in \mathrm{GL}(V, F) \mid \det g = 1\}$ denote the *special linear group* of V over F. We write F^* for the non-zero elements in F. For each $\lambda \in F^*$, the map from V to V given by $v \mapsto \lambda v$ is called a *scalar linear transformation* or simply a *scalar*. Thus we have an embedding of F^* into $\mathrm{GL}(V, F)$. We will abuse notation and write $F^* \leq \mathrm{GL}(V, F)$.

A map g from V to V is called an *F-semilinear transformation* of V if there is a field automorphism $\sigma(g) \in \operatorname{Aut} F$ such that

$$\begin{aligned} g(v + w) &= g(v) + g(w) && \text{for all } v, w \in V, \\ g(\lambda v) &= \lambda^{\sigma(g)} g(v) && \text{for all } \lambda \in F, v \in V. \end{aligned}$$

We define $\Gamma\mathrm{L}(V, F)$ to be the set of all invertible F-semilinear transformations. Then $\Gamma\mathrm{L}(V, F)$ forms a group, called the *general semilinear group* of V over F, and the map σ from $\Gamma\mathrm{L}(V, F)$ to $\mathrm{Aut}\, F$ is an epimorphism with kernel $\mathrm{GL}(V, F)$. We recall that $F = \mathrm{GF}(q)$. Let p be a prime, and let f be a natural number such that $q = p^f$. Let $\phi \in \Gamma\mathrm{L}(V, F)$ such that

$$\phi(\lambda v) = \lambda^p v \text{ for all } \lambda \in F, v \in V. \tag{A.2}$$

Then

$$\Gamma\mathrm{L}(V, F) = \mathrm{GL}(V, F) \cdot \langle \phi \rangle \tag{A.3}$$

is a semidirect product and $|\Gamma\mathrm{L}(V, F) : \mathrm{GL}(V, F)| = f$. We define a corresponding action of $\mathrm{Aut}\, F$ on $\mathrm{GL}(n, q)$. An automorphism $\varphi \in \mathrm{Aut}\, F$ acts on $a \in \mathrm{GL}(n, q)$ such that the matrix a^φ has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j. The semidirect product $\mathrm{GL}(n, q) \cdot \mathrm{Aut}\, F$ is defined accordingly. For a fixed basis $B = (b_1, \ldots, b_n)$ of V over F, we now have an isomorphism,

$$h_B : \Gamma\mathrm{L}(V, F) \to \mathrm{GL}(n, q) \cdot \mathrm{Aut}\, F,\ g \mapsto g_B \cdot \sigma(g) \tag{A.4}$$

where $g_B := a \in \mathrm{GL}(n, q)$ such that $g(b_i) = \sum_{j=1}^{n} a_{ij} b_j$ for all $i \in \{1, \ldots, n\}$.

We note that the map $x \mapsto (x^{-1})^t$ is an automorphism of $\mathrm{GL}(n, q)$. We can extend this inverse-transpose automorphism to $\Gamma\mathrm{L}(V, F)$ by defining

$$i(g \cdot \phi^j) = h_B^{-1}(((g_B)^{-1})^t) \cdot \phi^j \text{ for all } g \in \mathrm{GL}(V, F), j \in \mathbb{Z}, \tag{A.5}$$

where h_B is as in (A.1). We note that i is independent of the choice of B and that i is an involutory automorphism of $\Gamma\mathrm{L}(V, F)$.

2. Bilinear and quadratic forms

A map $\mathbf{f} : V \times V \to F$ is called a *bilinear form* if for each $v \in V$ the maps from V to F given by $x \mapsto \mathbf{f}(x, v)$ and $x \mapsto \mathbf{f}(v, x)$ are linear. If $x \mapsto \mathbf{f}(x, v)$ and $x \mapsto \mathbf{f}(v, x)$ are non-zero for all $v \in V \setminus \{0\}$, then $\mathbf{f}$ is *non-degenerate.* A bilinear form $\mathbf{f}$ is said to be *Hermitian* if F has an involutory field automorphism α, and

$$\mathbf{f}(v, w) = \mathbf{f}(w, v)^\alpha \text{ for all } v, w \in V.$$

We define $\mathbf{f}$ to be *symplectic* if

$$\mathbf{f}(v, w) = -\mathbf{f}(w, v) \text{ and } f(v, v) = 0 \text{ for all } v, w \in V.$$

Finally, $\mathbf{f}$ is *symmetric* if

$$\mathbf{f}(v, w) = \mathbf{f}(w, v) \text{ for all } v, w \in V.$$

We call a map $Q : V \to F$ a *quadratic form* if $Q(\lambda v) = \lambda^2 Q(v)$ for all $v \in V, \lambda \in F$, and if

$$\mathbf{f}_Q : V \times V \to F, (v, w) \mapsto Q(v + w) - Q(v) - Q(w)$$

is a bilinear form. We note that $\mathbf{f}_Q$ is symmetric by definition. A quadratic form Q is said to be *non-degenerate* if $\mathbf{f}_Q$ is non-degenerate.

3. Definition of classical groups

Let k be a bilinear form or a quadratic form on the vector space V over F such that one of the following holds:

case **L**: k is identically 0;
case **U**: $k = \mathbf{f}$ is a non-degenerate Hermitian bilinear form;
case **S**: $k = \mathbf{f}$ is a non-degenerate symplectic bilinear form;
case **O**: $k = Q$ is a non-degenerate quadratic form.

Then k is a map from V^l to F, where $l \in \{1, 2\}$. Let $\mathbf{v} = (v_1, \ldots, v_l)$ denote an element in V^l, and let $g \in \Gamma\mathrm{L}(V, F)$. Then we write $g(\mathbf{v})$ for $(g(v_1), \ldots, g(v_l))$ in V^l. We will consider the following groups:

$$\begin{array}{rcl}
\Gamma(V,F,k) & := & \{g \in \Gamma\mathrm{L}(V,F) \mid \exists\lambda \in F, \exists\alpha \in \mathrm{Aut}\,F, \forall\mathbf{v} \in V^l,\ k(g(\mathbf{v})) = \lambda k(\mathbf{v})^\alpha\}, \\
\Delta(V,F,k) & := & \{g \in \mathrm{GL}(V,F) \mid \exists\lambda \in F, \forall\mathbf{v} \in V^l,\ k(g(\mathbf{v})) = \lambda k(\mathbf{v})\}, \\
I(V,F,k) & := & \{g \in \mathrm{GL}(V,F) \mid \forall\mathbf{v} \in V^l,\ k(g(\mathbf{v})) = k(\mathbf{v})\}, \\
S(V,F,k) & := & \{g \in \mathrm{SL}(V,F) \mid \forall\mathbf{v} \in V^l,\ k(g(\mathbf{v})) = k(\mathbf{v})\}.
\end{array}$$

We recall that, in case **L**, $\Gamma(V, F, k)$ has an involutory automorphism i. Thus we can define the semidirect product of $\Gamma\mathrm{L}(V, F)$ with $\langle i \rangle$ where i acts on $\Gamma\mathrm{L}(V, F)$ as in (A.5). We extend our list of groups by the following:

$$\begin{array}{rcl}
A(V,F,k) & := & \left\{\begin{array}{ll} \Gamma(V,F,k)\cdot\langle i\rangle & \text{in case } \mathbf{L} \text{ with } n \geq 3 \\ \Gamma(V,F,k) & \text{otherwise} \end{array}\right. \\
\Omega(V,F,k) & := & \left\{\begin{array}{ll} S(V,F,k)' & \text{in case } \mathbf{O} \\ S(V,F,k) & \text{otherwise} \end{array}\right.
\end{array}$$

We note that the authors of [**KL90**] choose to define $\Omega(V, F, k)$ in case **O** differently. There $\Omega(V, F, k)$ is the unique subgroup of index 2 in $S(V, F, k)$ (see [**KL90**, p.14, (2.1.14), and p.29, Prop. 2.5.7]). However their definition and ours, which follows [**Die48**], [**Asc86**], and other textbooks, describe the same group if the dimension of V over F is at least 5. See Section 9 for more details.

Suppressing the (fixed) parameters V, F, k for notational convenience, we now have a series,

$$\Omega \leq S \leq I \leq \Delta \leq \Gamma \leq A,$$

where each group is normal in A. We also note that F^* is normal in A. A *finite classical group* is now defined (see [**KL90**, p. 14]) to be a group G such that $\Omega \leq G \leq A$ or $(\Omega \cdot F^*)/F^* \leq G \leq A/F^*$ in one of the cases $\mathbf{L}, \mathbf{U}, \mathbf{S}$, or $\mathbf{O}$. If G is such a group, then G is called a *linear*, *unitary*, *symplectic*, or *orthogonal* group, accordingly.

4. Properties of classical groups

We state the following result on the structure of classical groups.

Proposition A.1 ([**KL90**, Proposition 2.9.2, Proposition 2.10.6]). *Let V be a vector space of dimension $n > 1$ over the field F with $|F| =: q$. Let k be as in the cases $\mathbf{L}, \mathbf{U}, \mathbf{S}, \mathbf{O}$, and let $\Omega := \Omega(V, F, k)$. Then we have the following:*

(1) *Ω is soluble if and only if Ω is isomorphic to one of the following groups:* $\mathrm{SL}(2,2)$, $\mathrm{SL}(2,3)$, $\mathrm{Sp}(2,2)$, $\mathrm{Sp}(2,3)$, $\mathrm{SU}(2,2)$, $\mathrm{SU}(2,3)$, $\Omega^{\pm}(2,q)$, $\mathrm{SU}(3,2)$, $\Omega(3,3)$, $\Omega^{+}(4,2)$, $\Omega^{+}(4,3)$.

(2) *If Ω is insoluble, then one of the following holds:*
   (a) *$\Omega/(\Omega \cap F^*)$ is simple;*
   (b) *$\Omega \cong \mathrm{Sp}(4,2)$, that is, Ω is isomorphic to S_6 and almost simple;*
   (c) *$\Omega \cong \Omega^{+}(4,q)$ with $q \geq 4$ and $\Omega/(\Omega \cap F^*)$ is isomorphic to* $\mathrm{PSL}(2,q)^2$.

(3) *$C_{\mathrm{GL}(V,F)}(\Omega) = F^*$ if and only if $\Omega \not\cong \Omega^{\pm}(2,q)$.*

Proof: Assertions (1) and (2) are given in [**KL90**, Proposition 2.9.2]. Item (3) follows from [**KL90**, Proposition 2.10.1, Proposition 2.10.6]. □

By Proposition A.1 (2), Ω is perfect if Ω is insoluble and $\Omega \neq \mathrm{Sp}(4,2)$.

Lemma A.2 ([**KL90**, Theorem 2.1.3, Theorem 2.1.4]). *Let V be a vector space of dimension n over the field F with $|F| =: q$. Let k be as in the cases $\mathbf{L}, \mathbf{U}, \mathbf{S}, \mathbf{O}$. We assume that $n \geq 2$ and $(n,q) \notin \{(2,2),(2,3)\}$ in case $\mathbf{L}$, that $n \geq 3$ and $(n,q) \notin \{(3,2)\}$ in case $\mathbf{U}$, that $n \geq 4$ and $(n,q) \neq (4,2)$ in case $\mathbf{S}$, that $n \geq 7$ in case $\mathbf{O}$. Let $\Omega := \Omega(V,F,k)$ and $A := A(V,F,k)$. Then we have:*

(1) *$C_A(\Omega) = F^*$;*
(2) *$(\Omega \cdot F^*)/F^*$ is non-abelian simple;*
(3) *A/F^* is isomorphic to the full automorphism group of $(\Omega \cdot F^*)/F^*$ except when $\Omega \cong \mathrm{Sp}(4,q)$ with q even or $\Omega \cong \mathrm{O}^{+}(8,q)$.*

For the proof of Lemma A.2 (3), the authors of [**KL90**] refer to [**Die51**] as well as to [**Car89**].

5. Properties of linear groups

In this section we consider linear groups and their normal subgroups. The following facts can be found in various textbooks on group theory.

Lemma A.3. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3)\}$. Then we have:*

(1) *$|\mathrm{GL}(n,q)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - 1)$;*
(2) *$|\mathrm{SL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1)$;*
(3) *$C_{\mathrm{GL}(n,q)}(\mathrm{SL}(n,q)) = \{a * 1_n \mid a \in \mathrm{GF}(q)^*\}$;*
(4) *$\mathrm{SL}(n,q)' = \mathrm{SL}(n,q)$;*

(5) $\mathrm{SL}(n,q)/Z(\mathrm{SL}(n,q))$ *is simple.*

Proof: The assertions (1) and (2) are given in [**Rob96**, p.74, 3.2.7, (i),(ii)]. Item (3) is [**Rob96**, p.73, 3.2.5] and also follows from Lemma A.5. By [**Sco87**, p.292, 10.8.2] (or [**Hup67**, p.181, Satz 6.10]), we have (4). Assertion (5) is proved in [**Rob96**, p.74, 3.2.9]. □

We proceed to describe certain quotients of subgroups of general linear groups.

LEMMA A.4. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3)\}$. Let G be a group such that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$, let $Z := \{a * 1_n \mid a \in \mathrm{GF}(q)^*\}$, and let Y be a subgroup of $Z \cap G$. Let $k := |Y|$ and $m := |G : \mathrm{SL}(n,q)|$. Then we have:*

(1) $Z(G/Y) = (Z \cap G)/Y$;
(2) $|Z(G/Y)| = \frac{\gcd(mn,q-1)}{k}$;
(3) $(G/Y)' = (\mathrm{SL}(n,q) \cdot Y)/Y$;
(4) $|(G/Y)'| = \frac{|\mathrm{SL}(n,q)|}{\gcd(n,k)}$;
(5) *All normal subgroups of G/Y are central or contain the derived subgroup;*
(6) *G/Y has property* (A).

Proof: Properties (3), (4), (5) of Lemma A.3 yield that $\mathrm{SL}(n,q)$ satisfies (3) of Lemma 2.2. Thus $\mathrm{GL}(n,q)$ has property (C) (see Chapter 2, Section 2). Since $\mathrm{GL}(n,q)/\mathrm{SL}(n,q)$ is abelian, Lemma 3.1 yields that

$$\mathrm{GL}(n,q) \text{ has property (A).} \tag{A.6}$$

(see Chapter 3, Section 1). Since $\mathrm{SL}(n,q)$ is quasisimple by Lemma A.3 (5), Lemma 3.3 applies to show

$$Z(G) = Z \cap G \text{ and } G' = \mathrm{SL}(n,q) \tag{A.7}$$

and that

$$G \text{ has property (A).} \tag{A.8}$$

Together with (A.7) and (A.8), Lemma 3.2 yields (1), (3), and (6). Item (5) follows from (6).

It remains to prove (2) and (4). We note that G is given by $G = \{x \in \mathrm{GL}(n,q) \mid (\det x)^m = 1\}$. By (A.7), we have $Z(G) = \{a * 1_n \mid a \in \mathrm{GF}(q)^* \text{ and } (\det(a * 1_n))^m = 1\}$, which implies

$$Z(G) = \{a * 1_n \mid a \in \mathrm{GF}(q)^*, a^{mn} = 1\}.$$

Since the subgroup $\{a \in \mathrm{GF}(q)^* \mid a^{mn} = 1\}$ of the cyclic group $\mathrm{GF}(q)^*$ has exactly $\gcd(mn, |\mathrm{GF}(q)^*|)$ elements, we obtain $|Z(G)| = \gcd(mn, q-1)$. Now (1) and $|Y| = k$ yield (2).

For proving (4), we note that $Y = \{a * 1_n \mid a \in \mathrm{GF}(q)^* \text{ and } a^k = 1\}$. Hence

$$Y \cap \mathrm{SL}(n,q) = \{a * 1_n \mid a \in \mathrm{GF}(q)^*, a^k = 1 \text{ and } a^n = 1\}.$$

This yields $|Y \cap \mathrm{SL}(n,q)| = \gcd(n,k)$. Thus, with (3), we obtain $|(G/Y)'| = \frac{|\mathrm{SL}(n,q)|}{\gcd(n,k)}$. The proof of the lemma is complete. □

Lemma A.5. *Let V be a vector space of dimension n over a field F.*

(1) *For $n = 2$ and $|F| > 3$, we have $C_{\Gamma\mathrm{L}(V,F)}(\mathrm{SL}(V,F)) = F^*$;*
(2) *For $n > 2$, we have $C_{\Gamma\mathrm{L}(V,F)\cdot\langle i\rangle}(\mathrm{SL}(V,F)) = F^*$.*

Here i acts on $\Gamma\mathrm{L}(V,F)$ as defined in (A.5).

Proof: Let $|F| =: q$. Let p be a prime, and let f be an integer such that $p^f = q$. Let B be a basis for V over F, and let h_B as defined in (A.4), that is,

$$h_B : \Gamma\mathrm{L}(V,F) \to \mathrm{GL}(n,q) \cdot \mathrm{Aut}\, F, g \mapsto g_B \cdot \sigma(g).$$

An automorphism $\varphi \in \mathrm{Aut}\, F$ acts on $a \in \mathrm{GL}(n,q)$ such that the matrix a^φ has the entry $(a_{ij})^{(\varphi^{-1})}$ in row i, column j. First we prove

$$\text{(A.9)} \qquad C_{\mathrm{GL}(2,q)\cdot\mathrm{Aut}\, F}(\mathrm{SL}(2,q)) = \{a * 1_2 \mid a \in \mathrm{GF}(q)^*\}.$$

Let $g \in \mathrm{GL}(2,q)$, and let $\varphi \in \mathrm{Aut}\, F$ such that $g \cdot \varphi$ centralizes $\mathrm{SL}(2,q)$. For a primitive element w of $\mathrm{GF}(q)$, we consider $s := \mathrm{diag}(w, w^{-1})$, which is in $\mathrm{SL}(2,q)$. By $s^g = s^{(\varphi^{-1})}$, the eigenvalues of s and of $s^{(\varphi^{-1})}$ are equal. But then $s^{(\varphi^{-1})} = \mathrm{diag}(w^\varphi, (w^\varphi)^{-1})$ yields $w = w^\varphi$. Hence φ is trivial. Let $a, b, c, d \in F$ such that $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we have

$$g^s = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}^{-1} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} = \begin{pmatrix} a & bw^{-2} \\ cw^2 & d \end{pmatrix} = g.$$

By the assumption that $q > 3$, we have $w^2 \neq 1$ and $b = c = 0$. Conjugating $g = \mathrm{diag}(a,d)$ by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}(2,q)$ yields

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -a \\ d & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}.$$

Thus we have $a = d$. This proves (A.9) and (1) of Lemma A.5.

Next we assume $n > 2$. From the definition of the action of i on $\Gamma\mathrm{L}(V,F)$ in (A.5), we observe that $\Gamma\mathrm{L}(V,F) \cdot \langle i\rangle$ is isomorphic to the semidirect product $(\mathrm{GL}(n,q) \cdot \mathrm{Aut}\, F) \cdot \langle \hat{i}\rangle$ where $\hat{i}$ is the involutory automorphism defined by

$$(x \cdot \varphi)^{\hat{i}} = (x^{-1})^t \cdot \varphi \text{ for all } x \in \mathrm{GL}(n,q), \varphi \in \mathrm{Aut}\, F.$$

As a first step we prove

$$\text{(A.10)} \qquad C_{\mathrm{GL}(n,q)\cdot\mathrm{Aut}\, F\cdot\langle\hat{i}\rangle}(\mathrm{SL}(n,q)) \subseteq \mathrm{GL}(n,q) \cdot \mathrm{Aut}\, F.$$

We suppose that $g \cdot \varphi \cdot \hat{i}$ with $g \in \mathrm{GL}(n,q)$, $\varphi \in \mathrm{Aut}\, F$ centralizes $\mathrm{SL}(n,q)$. For a primitive element w of F, we consider $s := \mathrm{diag}(w^{1-n}, w, \ldots, w)$, which is in $\mathrm{SL}(n,q)$. Then we have $s^g = (s^{-1})^{(\varphi^{-1})}$. By comparing the eigenvalues of s and

$(s^{-1})^{(\varphi^{-1})}$ with their respective multiplicities, we obtain $w = (w^{-1})^{\varphi}$. Since w is primitive in F, this yields $x^{\varphi} = x^{-1}$ for all $x \in F^*$. Then φ is an automorphism only if $|F| = 2$ and φ is the identity map. Thus we are left with

$$y^g = (y^{-1})^t \text{ for all } x \in \mathrm{SL}(n,2). \tag{A.11}$$

We consider the matrices

$$r := \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & 1 \\ & & 1 & 0 \end{pmatrix} \text{ and } r^{-1} = \begin{pmatrix} 1 & 1 & & & \\ \vdots & 0 & 1 & & \\ 1 & & \ddots & \ddots & \\ 0 & & & 0 & 1 \\ 1 & & & & 0 \end{pmatrix}$$

in $\mathrm{SL}(n,2)$. The characteristic polynomial c_r of r (in the variable x) is equal to $x^n + x^{n-2} + \cdots + x + 1$, and the characteristic polynomial $c_{r^{-1}}$ of r^{-1} is equal to $x^n + x^{n-1} + \cdots + x^2 + 1$ (see [**AW92**, p.237, Proposition (4.14)]). We have $c_{(r^{-1})^t} = c_{r^{-1}}$ and, by $n > 3$, $c_{r^{-1}} \neq c_r$. Hence r and $(r^{-1})^t$ are not conjugate in $\mathrm{GL}(n,2)$, which contradicts (A.11). Assertion (A.10) is proved. Next we show

$$C_{\mathrm{GL}(n,q)\cdot \mathrm{Aut}\, F}(\mathrm{SL}(n,q)) \subseteq \mathrm{GL}(n,q). \tag{A.12}$$

Let $g \in \mathrm{GL}(n,q)$, $\varphi \in \mathrm{Aut}\, F$ such that $g \cdot \varphi$ centralizes $\mathrm{SL}(n,q)$. For a primitive element w of F, we consider $s := \mathrm{diag}(w^{1-n}, w, \ldots, w)$, which is in $\mathrm{SL}(n,q)$. Then we have $s^g = s^{(\varphi^{-1})}$. Comparing the eigenvalues of s and $s^{(\varphi^{-1})}$ yields $w = w^{\varphi}$. Thus φ is the identity map, and (A.12) is proved. Finally,

$$C_{\mathrm{GL}(n,q)\cdot \mathrm{Aut}\, F \cdot \langle \hat{\imath} \rangle}(\mathrm{SL}(n,q)) = \{a * 1_n \mid a \in \mathrm{GF}^*\} \tag{A.13}$$

follows from (A.10), (A.12) and Lemma A.6. From this we immediately obtain (2) of Lemma A.5. □

Let F be a field. For $i \in \{2, \ldots, n\}$, we define a matrix $e_i \in \mathrm{GL}(n, |F|)$ with -1 in the $(1,i)$-th position, 1 in the $(i,1)$-th position, 1 in the diagonal except in positions $(1,1)$ and (i,i), and 0 everywhere else. Then we have $\det e_i = 1$, $e_i^{-1} = e_i^t$, and $e_i^{\varphi} = e_i$ for all $\varphi \in \mathrm{Aut}\, F$.

Lemma A.6. *Let F be a field, and let n be a natural number, $n \geq 3$. Then we have*

$$C_{\mathrm{GL}(n,|F|)}(\langle e_2, \ldots, e_n \rangle) = \{a * 1_n \mid a \in F^*\}.$$

Proof: Let $a \in C_{\mathrm{GL}(n,|F|)}(\langle e_2, \ldots, e_n \rangle)$. For a fixed index $k \in \{2, \ldots, n\}$, we then have

$$a \cdot e_k = e_k \cdot a. \tag{A.14}$$

We note that the matrix $a \cdot e_k$ is obtained from a by multiplying the first column by -1 and by changing the first and the k-th column after that. Similarly, $e_k \cdot a$

is obtained from a by multiplying the k-th row by -1 and then changing the first and the k-th row. Let $i, j \in \{1, \dots, n\} \setminus \{1, k\}$. We compare the entries in the first row of (A.14) and obtain

$$-a_{11} = -a_{kk}, \tag{A.15}$$

$$a_{1k} = -a_{k1}, \tag{A.16}$$

$$a_{1j} = -a_{kj}. \tag{A.17}$$

From the k-th row we find

$$a_{kk} = a_{11}, \tag{A.18}$$

$$-a_{k1} = a_{1k}, \tag{A.19}$$

$$a_{kj} = a_{1j}. \tag{A.20}$$

The remaining entries of the first column yield

$$a_{ik} = a_{i1}, \tag{A.21}$$

and from the k-th column we have

$$-a_{i1} = a_{ik}. \tag{A.22}$$

By (A.15), (A.18), we have $a_{11} = a_{kk}$. By (A.17), (A.20), we obtain $a_{1j} = a_{kj} = 0$ and, by (A.21), (A.22), $a_{i1} = a_{ik} = 0$ for all $i, j \in \{1, \dots, n\} \setminus \{1, k\}$. Since this holds for all $k \in \{2, \dots, n\}$, we have that a is a scalar matrix. □

Since the matrices $e_2, \dots, e_n$ are in $\mathrm{SL}(n, |F|)$, the above lemma yields for $n \geq 3$ that

$$C_{\mathrm{GL}(n,|F|)}(\mathrm{SL}(n, |F|) = \{a * 1_n \mid a \in F^*\}.$$

6. Properties of unitary groups

Let V be a vector space of dimension n over a field F with a non-degenerate Hermitian bilinear form $\mathbf{f}$ (see Section 2). Then F has an automorphism of order 2, that is, there is a prime power q such that $F = \mathrm{GF}(q^2)$. By [**KL90**, Proposition 2.3.1] or [**Hup67**, p.237, Bemerkung 10.5 b)], we have a basis $B = \{b_1, \dots, b_n\}$ of V such that

$$\mathbf{f}(b_i, b_j) = \delta_{ij} \text{ for all } i, j \in \{1, \dots, n\}.$$

Under the homomorphism $h_B : \Gamma\mathrm{L}(V, F) \to \mathrm{GL}(n, q^2)$ of (A.1) for this basis B, the unitary group $I(V, F, \mathbf{f})$ is isomorphic to the matrix group

$$\mathrm{U}(n, q^2) := \{a \in \mathrm{GL}(n, q^2) \mid a^t \cdot \bar{a} = 1_n\}.$$

For $a \in \mathrm{GL}(n, q^2)$, the matrix $\bar{a}$ is defined by $\bar{a}_{ij} = (a_{ij})^q$ for all $i, j \in \{1, \ldots, n\}$. We call $\mathrm{U}(n, q^2)$ the *unitary group* of $n \times n$ matrices over $\mathrm{GF}(q^2)$. Let

$$\mathrm{SU}(n, q^2) := \{a \in \mathrm{U}(n, q^2) \mid \det a = 1\}$$

denote the *special unitary group.* We also observe

$$h_B(\Delta(V, F, \mathbf{f})) = \mathrm{U}(n, q^2) \cdot \langle w * 1_n \rangle, \tag{A.23}$$

where w is a primitive element of $\mathrm{GF}(q^2)$, and

$$h_B(\Gamma(V, F, \mathbf{f})) = (\mathrm{U}(n, q^2) \cdot \langle w * 1_n \rangle) \cdot \mathrm{Aut}\, F, \tag{A.24}$$

where we have the usual action of $\mathrm{Aut}\, F$ on a matrix group.

Lemma A.7. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Then we have:*

(1) $|\mathrm{U}(n, q^2)| = q^{n(n-1)/2} \prod_{i=1}^{n} (q^i - (-1)^i)$;
(2) $|\mathrm{SU}(n, q^2)| = |\mathrm{U}(n, q^2)|/(q + 1)$;
(3) $C_{\mathrm{GL}(2,q^2) \cdot \mathrm{Aut}\, \mathrm{GF}(q^2)}(\mathrm{SU}(2, q^2)) = \{a * 1_2 \mid a \in \mathrm{GF}(q^2)^*\} \cdot \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \alpha \rangle$ *where* $\alpha(x) = \bar{x}$ *for all* $x \in \mathrm{SU}(2, q^2)$;
(4) $C_{\mathrm{GL}(n,q^2) \cdot \mathrm{Aut}\, \mathrm{GF}(q^2)}(\mathrm{SU}(n, q^2)) = \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*\}$ *for* $n > 2$;
(5) $\mathrm{SU}(n, q^2)' = \mathrm{SU}(n, q^2)$;
(6) $\mathrm{SU}(n, q^2)/Z(\mathrm{SU}(n, q^2))$ *is simple.*

Lemma A.7 (3) and (4) immediately yield that for $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$ the centralizer of $\mathrm{U}(n, q^2)$ in $\mathrm{GL}(n, q^2) \cdot \mathrm{Aut}\, \mathrm{GF}(q^2)$ comprises of scalar matrices only.

Proof: Item (1) is [**KL90**, Proposition 2.3.3]. By definition, we have $(\det x)^{q+1} = 1$ for all $x \in \mathrm{U}(n, q^2)$. Let $F := \mathrm{GF}(q^2)$, and let w be a primitive element of F. Then $a := \mathrm{diag}(w^{q-1}, 1, \ldots, 1)$ is in $\mathrm{U}(n, q^2)$. By $\det a = w$, we now obtain that $|\det \mathrm{U}(n, q^2)| = q + 1$. Since $\mathrm{SU}(n, q^2)$ is the kernel of det on $\mathrm{U}(n, q^2)$, this yields (2). For the proof of (3), we observe

$$\mathrm{SU}(2, q^2) = \{\left(\begin{smallmatrix} a & b \\ -b^q & a^q \end{smallmatrix}\right) \mid a, b \in F, a^{q+1} + b^{q+1} = 1\}.$$

Let $g \in \mathrm{GL}(2, q^2)$ and $\varphi \in \mathrm{Aut}\, F$ such that $g \cdot \varphi$ centralizes $\mathrm{SU}(2, q^2)$. For a primitive element w of F, we have that $s := \mathrm{diag}(w, w^{-1})^{q-1}$ is in $\mathrm{SU}(2, q^2)$. Since $s^g = s^{(\varphi^{-1})}$, the eigenvalues of s and of $s^{(\varphi^{-1})}$ are equal. But then $s^{(\varphi^{-1})} = \mathrm{diag}(w^\varphi, (w^\varphi)^{-1})^{q-1}$ yields either $(w^{q-1})^\varphi = w^{q-1}$ or $(w^{q-1})^\varphi = w^{1-q}$. Hence φ is trivial or $w^\varphi = w^q$.

First we assume that φ is trivial. Let $a, b, c, d \in F$ such that $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we have

$$g^s = \left(\begin{smallmatrix} w & 0 \\ 0 & w^{-1} \end{smallmatrix}\right)^{-(q-1)} \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} w & 0 \\ 0 & w^{-1} \end{smallmatrix}\right)^{q-1} = \begin{pmatrix} a & bw^{-2(q-1)} \\ cw^{2(q-1)} & d \end{pmatrix} = g.$$

By the assumption that $q > 3$, we have $w^{2(q-1)} \neq 1$ and $b = c = 0$. Conjugating $g = \operatorname{diag}(a, d)$ by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SU}(2, q^2)$ yields

$$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} \cdot \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & -a \\ d & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} d & 0 \\ 0 & a \end{smallmatrix}\right).$$

Thus we have $a = d$, and g is in $\{a * 1_2 \mid a \in F^*\}$.

Next we consider the case that

$$x^g = \bar{x} \text{ for all } x \in \mathrm{SU}(2, q^2).$$

Let $a, b, c, d \in F$ such that $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we have $s^g = s^{-1}$, which yields

$$sgs = \left(\begin{smallmatrix} w & 0 \\ 0 & w^{-1} \end{smallmatrix}\right)^{q-1} \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} w & 0 \\ 0 & w^{-1} \end{smallmatrix}\right)^{q-1} = \begin{pmatrix} aw^{2(q-1)} & b \\ c & dw^{-2(q-1)} \end{pmatrix} = g.$$

By $w^{2(q-1)} \neq 1$, we obtain $a = d = 0$. Since $w^{q+1} \in \mathrm{GF}(q)^*$, there is $v \in \mathrm{GF}(q^2)^*$ such that $v^{q+1} = 1 - w^{q+1}$. Then the matrix $x := \left(\begin{smallmatrix} w & v \\ -v^q & w^q \end{smallmatrix}\right)$ is in $\mathrm{SU}(2, q^2)$. We consider the conjugate of x by g,

$$x^g = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)^{-1} \cdot \left(\begin{smallmatrix} w & v \\ -v^q & w^q \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & c^{-1} \\ b^{-1} & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} vc & wb \\ w^q c & -v^q b \end{smallmatrix}\right) = \left(\begin{smallmatrix} w^q & -v^q bc^{-1} \\ vcb^{-1} & w \end{smallmatrix}\right).$$

Now $x^g = \bar{x}$ yields $c = -b$. Thus g is a scalar multiple of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The proof of (3) is complete.

For proving (4), we let $g \in \mathrm{GL}(n, q^2)$ and $\varphi \in \operatorname{Aut} F$ such that $g \cdot \varphi$ centralizes all elements of $\mathrm{SU}(n, q^2)$. For a primitive element w of F, we consider $s := \operatorname{diag}(w^{1-n}, w, \dots, w)^{q-1}$. By $s \in \mathrm{SU}(n, q^2)$, we have $s^g = s^{(\varphi^{-1})}$. The comparison of the eigenvalues of s and of $s^{(\varphi^{-1})}$ with their respective multiplicities yields $(w^{q-1})^{\varphi} = w^{q-1}$. Hence φ is trivial, and we have

$$C_{\mathrm{GL}(n,q^2) \cdot \operatorname{Aut} \mathrm{GF}(q^2)}(\mathrm{SU}(n, q^2)) \subseteq \mathrm{GL}(n, q^2).$$

We observe that the matrices $e_i \in \mathrm{GL}(n, q^2)$ for $i \in \{2, \dots, n\}$ of Lemma A.6 are elements of $\mathrm{SU}(n, q^2)$. Thus we obtain (4).

By [**Die48**, p.70, Theorem 5], all proper normal subgroups of $\mathrm{SU}(n, q^2)$ are central. Hence we have (6). Since $\mathrm{SU}(n, q^2)/Z(\mathrm{SU}(n, q^2))$ is not abelian, we obtain (5). □

Based on Lemma A.7, we now study certain quotients of subgroups of unitary groups.

Lemma A.8. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n, q) \notin \{(2, 2), (2, 3), (3, 2)\}$. Let H be a group with $\mathrm{SU}(n, q^2) \subseteq H \subseteq \mathrm{U}(n, q^2) \cdot \langle w * 1_n \rangle$ where w is a primitive element in $\mathrm{GF}(q^2)$. Let Y be a subgroup of $Z(H)$, and let $G := H/Y$. Then we have:*

1. *G has property* (A)*;*
2. *$G' = (\mathrm{SU}(n, q^2) \cdot Y)/Y$ and $Z(G) = (H \cap \langle w * 1_n \rangle)/Y$;*
3. *The Sylow p-subgroup of G/G' is cyclic for all odd primes p;*

(4) *If the Sylow* 2*-subgroup of* G/G' *is not cyclic, then there is a group* L *with* $G' \subseteq L \subseteq G \cap (\mathrm{U}(n,q^2) \cdot Y)/Y$ *such that* L/G' *is a cyclic* 2*-group with a cyclic direct complement in* G/G'.

Proof: For proving (1) and (2), we first show that $D := \mathrm{U}(n,q^2) \cdot \langle w * 1_n \rangle$ has property (A) (see Chapter 3, Section 1). Let $Z := \langle w * 1_n \rangle$, and let $N := \mathrm{SU}(n,q^2)$. Then N is a normal subgroup of D. By (3), (4), (5), and (6) of Lemma A.7, N satisfies condition (3) of Lemma 2.2. Thus N satisfies (C.1) and (C.2) in D (see Chapter 2, Section 2). We note that D/N is abelian. Hence

$$\mathrm{U}(n,q^2) \cdot \langle w * 1_n \rangle \text{ has property (A).} \tag{A.25}$$

by Lemma 3.1. Since $\mathrm{SU}(n,q^2)$ is quasisimple by Lemma A.7 (6), Lemma 3.3 yields

$$Z(H) = Z \cap H \text{ and } H' = \mathrm{SU}(n,q^2) \tag{A.26}$$

and that

$$H \text{ has property (A).} \tag{A.27}$$

For $G := H/Y$, Lemma 3.2 yields (1) and (2).

For the remainder of the proof, we write $\bar{x} := x \cdot G'$ for $x \in G$, and we write $\bar{A} := (A \cdot G')/G'$ for subgroups A of G. Let $G_1 := G \cap (\mathrm{U}(n,q^2) \cdot Y)/Y$. Then $\bar{G}_1$ can be embedded into $\mathrm{U}(n,q^2)/\mathrm{SU}(n,q^2)$ and is cyclic. Let $g \in G_1$ such that $\bar{g}$ generates $\bar{G}_1$, and let z be a generator of $Z(G)$. Then the abelian group $\bar{G}$ is generated by $\bar{g}$ and $\bar{z}$. We have that $\operatorname{ord} \bar{g}$ divides $q+1$ and that $|\bar{G} : \bar{G}_1|$ divides $q-1$.

Let p be a prime. The Sylow p-subgroup P of $\bar{G}$ is cyclic if and only if the Sylow p-subgroup of $\langle \bar{g} \rangle$ is contained in the Sylow p-subgroup of $\langle \bar{z} \rangle$ or vice versa. Hence P is cyclic iff either p does not divide $|\bar{G} : \langle \bar{g} \rangle|$ or p does not divide $|\bar{G} : \langle \bar{z} \rangle|$. We have that

$$|\bar{G} : \langle \bar{g} \rangle| \text{ divides } q-1,$$

and

$$|\bar{G} : \langle \bar{z} \rangle| \text{ divides } |\mathrm{U}(n,q^2) : \mathrm{SU}(n,q^2)|, \text{ which is } q+1.$$

Hence $\gcd(|\bar{G} : \langle \bar{g} \rangle|, |\bar{G} : \langle \bar{z} \rangle|)$ divides 2. Thus the Sylow p-subgroup of $\bar{G}$ is cyclic, when p is odd. This proves (3).

Now we assume that the Sylow 2-subgroup of $\bar{G}$ is not cyclic. Then we have $\gcd(|\bar{G} : \langle \bar{g} \rangle|, |\bar{G} : \langle \bar{z} \rangle|) = 2$, and q is odd. Let $a, c \in G$ such that $\bar{a}$ is a generator for the Sylow 2-subgroup of $\langle \bar{g} \rangle$ and $\bar{c}$ is a generator for the Sylow 2-subgroup of $\langle \bar{z} \rangle$. Let $L := G' \cdot \langle a \rangle$. We will show that

$$\bar{L} \text{ has a cyclic direct complement in } \bar{G}. \tag{A.28}$$

If $\operatorname{ord} \bar{a} = 2$, then $\bar{a} \notin \langle \bar{c} \rangle$ yields that $\langle \bar{a} \rangle \cdot \langle \bar{c} \rangle$ is a direct product. Since the Sylow 2-subgroup of $\bar{G}$ is generated by $\bar{a}$ and $\bar{c}$, we then obtain (A.28) from (3).

Next we assume that 4 divides $\operatorname{ord}\bar{a}$. Then 4 divides $q+1$, and $(q-1)/2$ is odd. Hence c^2 is in G_1, that is, $\bar{c}^2$ is in $\langle \bar{a} \rangle$. By the assumption that $\langle \bar{a}, \bar{c} \rangle$ is not cyclic, we obtain $\operatorname{ord}\bar{a} \geq \operatorname{ord}\bar{c}$. As a maximal cyclic subgroup of the abelian 2-group $\langle \bar{a}, \bar{c} \rangle$, the group $\langle \bar{a} \rangle$ has a direct complement in $\langle \bar{a}, \bar{c} \rangle$ (see [**Rob96**, p.102, 4.2.7]). Then (3) yields (A.28). Thus we have (4). The proof of the lemma is complete. □

We determine some additional parameters for certain groups that are described in Lemma A.8.

LEMMA A.9. *Let n be a natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3),(3,2)\}$. Let G be a group such that $\mathrm{SU}(n,q^2) \subseteq G \subseteq \mathrm{U}(n,q^2)$, let $Z := \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*, a^{q+1} = 1\}$, and let Y be a subgroup of $Z \cap G$. Let $k := |Y|$ and $m := |G : \mathrm{SU}(n,q^2)|$. Then we have:*

(1) *$Z(G/Y) = (Z \cap G)/Y$;*
(2) *$|Z(G/Y)| = \frac{\gcd(mn,q+1)}{k}$;*
(3) *$(G/Y)' = (\mathrm{SU}(n,q^2) \cdot Y)/Y$;*
(4) *$|(G/Y)'| = \frac{|\mathrm{SU}(n,q^2)|}{\gcd(n,k)}$.*

Proof: The assertions (1) and (3) follow immediately from Lemma A.8 (2). We note that G is given by $G = \{x \in \mathrm{U}(n,q^2) \mid (\det x)^m = 1\}$ and $Z \cap G = \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*, a^{q+1} = 1, \text{ and } (\det(a * 1_n))^m = 1\}$. Thus we have

$$Z(G) = \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*, a^{\gcd(q+1,mn)} = 1\},$$

which implies $|Z(G)| = \gcd(mn, q+1)$. Hence (1) and $|Y| = k$ yield (2).

To compute the size of the derived subgroup of G/Y, we note $Y = \{a * 1_n \mid a \in \mathrm{GF}(q^2)^* \text{ and } a^k = 1\}$. Hence

$$Y \cap \mathrm{SU}(n,q^2) = \{a * 1_n \mid a \in \mathrm{GF}(q^2)^*, a^k = 1, \text{ and } a^n = 1\}.$$

This yields $|Y \cap \mathrm{SU}(n,q^2)| = \gcd(n,k)$. Now (4) follows from (3). □

7. Endomorphisms of linear and unitary groups

Since the structure of linear and unitary groups is very similar (see Sections 5 and 6), we will be able to deal with the endomorphisms of these groups using the same methods. For many of our applications, it suffices to know that the automorphisms of linear and unitary groups have the following property:

LEMMA A.10. *Let n be a natural number with $n \geq 2$, and let q be a prime power. Let G be a group such that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$ or $\mathrm{SU}(n,q^2) \subseteq G \subseteq \mathrm{U}(n,q^2)$. Let α be an endomorphism of G with $\mathrm{Ker}(\alpha) \subseteq Z(G)$. Then there is $a \in \mathbb{N}$ such that $\alpha(z) = z^a$ for all $z \in Z(G)$ and*

$$\det \alpha(x) = (\det x)^a \textit{ for all } x \in G. \tag{A.29}$$

We will prove this lemma from first principles, without making use of the description of automorphisms of finite simple groups as given in [**Die51**] or in [**Car89**, Chapter 12]. Before we can do the actual proof, we have to state a few auxiliary results.

We recall the definition of $e_i \in \mathrm{SL}(n,q) \cap \mathrm{SU}(n,q^2)$ from Lemma A.6: For $i \in \{2,\dots,n\}$, the matrix e_i has -1 in the $(1,i)$-th position, 1 in the $(i,1)$-th position, 1 in the diagonal except in positions $(1,1)$ and (i,i), and 0 everywhere else.

Lemma A.11. *Let n be a natural number with $n \geq 2$, and let q be a prime power. Let $v_1,\dots,v_n,w_1,\dots,w_n \in \mathrm{GF}(q^2)^*$, and let $v := \mathrm{diag}(v_1,\dots,v_n), w := \mathrm{diag}(w_1,\dots,w_n)$. Then the following are equivalent:*

1. *There is a bijection $\pi : \{1,\dots,n\} \to \{1,\dots,n\}$ such that $v_i = w_{\pi(i)}$ for all $i \in \{1,\dots,n\}$;*
2. *There is $g \in \langle e_2,\dots,e_n\rangle$ with $v = w^g$;*
3. *There is $g \in \mathrm{GL}(n,q)$ with $v = w^g$;*
4. *There is $g \in \mathrm{GL}(n,q^2)$ with $v = w^g$.*

Proof: (1) ⇒ (2): For $i \in \{2,\dots,n\}$, let $(1,i)$ denote the transposition on the set $\{1,\dots,n\}$ that interchanges 1 and i. The permutation π can be written as a product $\pi = \prod_{j=1}^{k}\prod_{i=2}^{n}(1,i)^{l_{i,j}}$ for some natural number k and $l_{i,j} \in \{0,1\}$. We note that we write functions to the left of the argument. With $g := \prod_{j=1}^{k}\prod_{i=2}^{n} e_i^{l_{i,j}}$, we then have $v = g^{-1}\cdot w \cdot g$.

(2) ⇒ (3) and (3) ⇒ (4) are obvious.

(4) ⇒ (1): The characteristic polynomial c_v of v (in the variable x) is equal to $\prod_{i=1}^{n}(x-v_i)$, and the characteristic polynomial c_w of w is equal to $\prod_{i=1}^{n}(x-w_i)$. By (4), we have $c_v = c_w$, which implies (1). □

Lemma A.12. *Let n be a natural number with $n \geq 2$, and let q be a prime power. Let $v \in \mathrm{GL}(n,q^2)$ be a diagonal matrix and assume that v has s distinct eigenvalues of respective multiplicities $n_1 \geq n_2 \geq \dots \geq n_s$. Let G be a group such that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$ or $\mathrm{SU}(n,q^2) \subseteq G \subseteq \mathrm{U}(n,q^2)$.*

Then $q^{\frac{1}{2}\cdot\sum_{i=1}^{s} n_i(n_i-1)}$ is the largest power of q that divides $C_G(v)$.

Proof: Let $v_1,\dots,v_s$ be the distinct eigenvalues of v with multiplicities $n_1 \geq n_2 \geq \dots \geq n_s$. By Lemma A.11, we have $g \in \langle e_2,\dots,e_n\rangle \subseteq G$ such that

$$v^g = \mathrm{diag}(v_1,\dots,v_1,v_2,\dots,v_2,\dots,v_s,\dots,v_s).$$

Let $w := v^g$, and let $a \in G$ such that $aw = wa$. Then the matrix a is a block-diagonal matrix,

$$a = \begin{pmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_s \end{pmatrix},$$

where a_i is an $n_i \times n_i$ matrix for $i \in \{1, \ldots, s\}$. We now distinguish the cases that G is a linear or a unitary group. First we assume that $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$. Then the matrices a_i are elements of $\mathrm{GL}(n_i,q)$ for $i \in \{1, \ldots, s\}$. Thus we have an embedding of $C_G(w)$ into $H := \prod_{i=1}^{s} \mathrm{GL}(n_i,q)$. We note that $|H| = \prod_{i=1}^{s} \prod_{j=1}^{n_i} (q^{n_i} - q^j)$. Hence $r := q^{\frac{1}{2} \cdot \sum_{i=1}^{s} n_i(n_i-1)}$ is the largest q-power that divides $|H|$. Let $m := |G : \mathrm{SL}(n,q)|$. Then $C_G(w)$ is isomorphic to the kernel of the homomorphism $h : H \to \mathrm{GF}(q)^*$, $x \mapsto (\det x)^m$. Now, $|\mathrm{Im}(h)|$ divides $q-1$, and $|\mathrm{Im}(h)|$ is therefore coprime to q. By the homomorphism theorem, we then have that r divides $|\mathrm{Ker}(h)|$. By $C_G(v) = g \cdot C_G(w) \cdot g^{-1}$, we finally obtain that r divides $|C_G(v)|$.

Next we consider the case $\mathrm{SU}(n,q^2) \subseteq G \subseteq \mathrm{U}(n,q^2)$. Then we have $a_i \in \mathrm{U}(n_i,q^2)$ for $i \in \{1, \ldots, s\}$, and we can embed $C_G(w)$ into $H := \prod_{i=1}^{s} \mathrm{U}(n_i,q^2)$. Lemma A.7 (1) tells that $|H| = \prod_{i=1}^{s} q^{n_i(n_i-1)/2} \prod_{j=1}^{n_i} (q^j - (-1)^j)$. Hence $r := q^{\frac{1}{2} \cdot \sum_{i=1}^{s} n_i(n_i-1)}$ is the largest p-power that divides $|H|$. With $m := |G : \mathrm{SU}(n,q^2)|$, the centralizer $C_G(w)$ is isomorphic to the kernel of $h : H \to \mathrm{GF}(q^2)^*$, $x \mapsto (\det x)^m$. Now $|\mathrm{Im}(h)|$ is coprime to q because $|\mathrm{Im}(h)|$ divides $q+1$. Thus, by the homomorphism theorem, r divides $|\mathrm{Ker}(h)|$. By $C_G(v) = g \cdot C_G(w) \cdot g^{-1}$, we finally obtain that r divides $|C_G(v)|$. The lemma is proved. □

Now we are able to prove Lemma A.10.

Proof of Lemma A.10: We write $I = \mathrm{GL}(n,q)$, $F = \mathrm{GF}(q)$ if $\mathrm{SL}(n,q) \subseteq G \subseteq \mathrm{GL}(n,q)$, and $I = \mathrm{GL}(n,q^2), F = \mathrm{GF}(q^2)$ else. Let α be an endomorphism of G with $\mathrm{Ker}(\alpha) \subseteq Z(G)$. We note that $G/Z(G)$ is centerless because G has property (A) by the Lemmas A.4, A.8. Then $\alpha(Z(G)) \subseteq Z(G)$ by Lemma 2.8. Since $Z(G)$ is cyclic, we have an element $a \in \mathbb{N}$ such that $\alpha(z) = z^a$ for all $z \in Z(G)$. We will now show that (A.29) holds for this a. To this end, we let $m := |G : G'|$. Since (A.29) is obvious if $m = 1$, we will assume $m > 1$ in the sequel. Let w be a primitive m-th root of unity in F. For $i \in \{1, 2, \ldots, n\}$, we define a matrix d_i by

$$d_i = \mathrm{diag}(1, \ldots, 1, w, 1, \ldots, 1),$$

where w stands at the i-th place. Let H denote the subgroup of G generated by $d_1, \ldots, d_n$. Then the restriction $\alpha|_H : H \to I$ is a representation of H over the field F. Let $(\mathbb{Z}_m, \cdot)$ be the cyclic group with m elements. Then H is isomorphic to

$(\mathbb{Z}_m)^n$. Since m divides $|F|-1$, m and q are relatively prime. Hence by Maschke's Theorem [**Rob96**, p.216], $\alpha|_H$ is equivalent to a representation $\beta : H \to I$ such that β is a sum of irreducible representations of H over F. By the definition of equivalence [**Rob96**, p.215], we have $t \in I$ such that

$$\alpha(h) = t^{-1} \cdot \beta(h) \cdot t \text{ for all } h \in H. \tag{A.30}$$

We will now prove

$$\beta(H) \subseteq H. \tag{A.31}$$

Since $(F^*, \cdot)$ is cyclic, and since m divides $|F| - 1$, the polynomial $x^m - 1$ has precisely m roots in F. Hence conditions (1) and (2) in [**AW92**, p. 439, Definition (1.3)] are satisfied, and so, by [**AW92**, p.451, Theorem 2.1] all irreducible representations of the abelian group H over F are of degree 1. Therefore, β is a sum of representations of degree 1, and so for each $h \in H$, $\beta(h)$ is a diagonal matrix. Furthermore, H has exponent m. Hence every representation ρ of H of degree 1 maps H into a subgroup of $(F^*, \cdot)$ of exponent dividing m. This shows that for every $h \in H$, we have $(\rho(h))^m = 1$, and hence $\rho(h)$ is a power of w. This implies (A.31). We define a mapping $\tilde{\beta} : G \to I$ by

$$\tilde{\beta}(g) := t \cdot \alpha(g) \cdot t^{-1} \text{ for all } g \in G. \tag{A.32}$$

We will now investigate the diagonal matrix $\tilde{\beta}(d_1)$. We assume that $\tilde{\beta}(d_1)$ has s distinct eigenvalues of multiplicities $n_1, \dots, n_s$. Let r be the largest power of q which divides $|C_G(d_1)|$. Since $\tilde{\beta}(C_G(d_1) \subseteq C_{\tilde{\beta}(G)}(\tilde{\beta}(d_1))$ and $|\mathrm{Ker}(\tilde{\beta})|$ is coprime to q, we have that r divides $|C_{\tilde{\beta}(G)}(\tilde{\beta}(d_1))|$. By $C_{\tilde{\beta}(G)}(\tilde{\beta}(d_1)) \subseteq C_G(\tilde{\beta}(d_1))$ and Lemma A.12, we then obtain that $r = q^{\frac{1}{2}(n-1)(n-2)}$ divides $q^{\frac{1}{2}\cdot\sum_{i=1}^{s} n_i(n_i-1)}$. Hence

$$(n-1)(n-2) \leq \sum_{i=1}^{s} n_i(n_i - 1) \tag{A.33}$$

with $\sum_{i=1}^{s} n_i = n$. We first assume that $n_i \leq n-2$ for all $i = 1, \dots, s$. Then $\sum_{i=1}^{s} n_i(n_i - 1) \leq \sum_{i=1}^{s} n_i(n-3) = n(n-3)$, and $n(n-3) < n - 3n + 2 = (n-1)(n-2)$ contradicts (A.33). Now we assume that $s = 1$ and $n_1 = n$. Then $\tilde{\beta}(d_1)$ is in $Z(\beta(G))$, which yields the contradiction that $[d_1, g] \in \mathrm{Ker}(\tilde{\beta}) \subseteq Z(G)$ for all $g \in G$. Thus we have $s = 2$ and $n_1 = n-1$, $n_2 = 1$. There is $k, l \in \{0, 1, \dots, m-1\}$ with $k \neq l$, and there is $i \in \{1, \dots, n\}$ such that

$$\tilde{\beta}(d_1) = \mathrm{diag}(w^k, w^k, \dots, w^k, w^l, w^k, \dots, w^k), \tag{A.34}$$

where w^l stands at the i-th place. We denote the matrix on the right hand side of (A.34) by $e(i, k, l)$. By Lemma A.11, the elements $d_1, \dots, d_n \in H$ are pairwise conjugate in G. So $\tilde{\beta}(d_1), \dots, \tilde{\beta}(d_n) \in \tilde{\beta}(H)$ are pairwise conjugate in $\tilde{\beta}(G)$. By $\tilde{\beta}(H) \subseteq H$ and by Lemma A.11, we have

$$\tilde{\beta}(\{d_1, d_2, \dots, d_n\}) \subseteq \{e(1, k, l), e(2, k, l), \dots, e(n, k, l)\}. \tag{A.35}$$

Since $\tilde{\beta}(d_1), \ldots, \tilde{\beta}(d_n)$ are pairwise distinct, equality holds in (A.35). Next we show that

$$\text{for all } x \in G: \ \det \alpha(x) = (\det x)^{k+l(n-1)} \tag{A.36}$$

To prove (A.36), we fix $x \in G$. Then there is r with $0 \leq r \leq m-1$ such that $\det x = w^r$. For $s := (d_1)^{-r} \cdot x$, we have $\det s = 1$ and $x = (d_1)^r \cdot s$. Now $\det \tilde{\beta}(x)$ can be computed by $\det \tilde{\beta}(x) = \det(\tilde{\beta}((d_1)^r \cdot s)) = \det \tilde{\beta}((d_1)^r) \cdot \det \tilde{\beta}(s)$. Since s is in G', which is fully-invariant in G, we also have $\det \tilde{\beta}(s) = 1$. Hence we obtain $\det \tilde{\beta}((d_1)^r) \cdot \det \tilde{\beta}(s) = \det \tilde{\beta}((d_1)^r) = w^{(k+l(n-1)) \cdot r} = (\det x)^{k+l(n-1)}$. By (A.32), we have $\det \alpha(x) = \det \tilde{\beta}(x)$, which implies (A.36). Now we show that

$$m \text{ divides } a - (k + l(n-1)). \tag{A.37}$$

Let $c := \prod_{i=1}^n d_i$. Then $\tilde{\beta}(c) = \prod_{i=1}^n e(i,k,l) = \operatorname{diag}(w^{k+l(n-1)}, \ldots, w^{k+l(n-1)})$. Since $c \in Z(G)$, the choice of a yields $\tilde{\beta}(c) = t \cdot \alpha(c) \cdot t^{-1} = t \cdot \operatorname{diag}(w^a, \ldots, w^a) \cdot t^{-1} = \operatorname{diag}(w^a, \ldots, w^a)$. Thus we have $w^a = w^{k+l(n-1)}$, which implies (A.37).

Finally we will prove (A.29). We fix $x \in G$. Then $(\det x)^m = 1$, and thus by (A.37) we have $(\det x)^{k+l(n-1)} = (\det x)^a$. With (A.36) we obtain $\det \alpha(x) = (\det x)^a$, which proves (A.29) and completes the proof of Lemma A.10. □

8. Properties of symplectic groups

Let V be a vector space over a field F with a non-degenerate symplectic bilinear form $\mathbf{f}$ (see Section 2). By [**KL90**, Proposition 2.4.1] or [**Hup67**, p.217, Satz 9.6, Definition 9.7)], the dimension n of V over F is even, and we have a basis $B = \{b_1, c_1, \ldots, b_{n/2}, c_{n/2}\}$ of V such that

$$\mathbf{f}(b_i, b_j) = \mathbf{f}(c_i, c_j) = 0 \text{ and } \mathbf{f}(b_i, c_j) = \delta_{ij} \text{ for all } i, j \in \{1, \ldots, n/2\}.$$

Under the homomorphism $h_B : \Gamma\mathrm{L}(V,F) \to \mathrm{GL}(n,q)$ of (A.1) for this basis B, the symplectic group $I(V,F,\mathbf{f})$ is isomorphic to the matrix group

$$\mathrm{Sp}(n,q) := \{a \in \mathrm{GL}(n,q) \mid x^t \cdot a \cdot x = a\}$$

with

$$a := \begin{pmatrix} 0 & -1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & -1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & -1 \\ & & & & & 1 & 0 \end{pmatrix}.$$

We call $\mathrm{Sp}(n,q)$ the *symplectic group* of $n \times n$ matrices over $\mathrm{GF}(q)$. For w a primitive element of $\mathrm{GF}(q)$, we observe

$$h_B(\Delta(V,F,\mathbf{f})) = \mathrm{Sp}(n,q) \cdot \langle \operatorname{diag}(w,1,\ldots,w,1) \rangle. \tag{A.38}$$

If q is even, then $\mathrm{Sp}(n,q) \cap \langle w * 1_n \rangle$ is trivial, which yields

$$\mathrm{Sp}(n,q) \cdot \langle \mathrm{diag}(w,1,\dots,w,1) \rangle = \mathrm{Sp}(n,q) \cdot \langle w * 1_n \rangle. \tag{A.39}$$

In any case we have

$$h_B(\Gamma(V,F,\mathbf{f})) = (\mathrm{Sp}(n,q) \cdot \langle \mathrm{diag}(w,1,\dots,w,1) \rangle) \cdot \mathrm{Aut}\, F, \tag{A.40}$$

where $\mathrm{Aut}\, F$ acts on the matrix group as usual.

Lemma A.13. *Let n be an even natural number with $n \geq 2$, and let q be a prime power such that $(n,q) \notin \{(2,2),(2,3),(4,2)\}$. Then we have:*

1. $|\mathrm{Sp}(n,q)| = q^{n^2/4} \prod_{i=1}^{n/2} (q^{2i}-1)$;
2. $\mathrm{Sp}(n,q) \subseteq \mathrm{SL}(n,q)$;
3. $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$;
4. $\mathrm{Sp}(4,2)$ *is isomorphic to the symmetric group* S_6;
5. $C_{\mathrm{GL}(n,q)\cdot \mathrm{Aut}\,\mathrm{GF}(q)}(\mathrm{Sp}(n,q)) = \{a * 1_n \mid a \in \mathrm{GF}(q)^*\}$;
6. $Z(\mathrm{Sp}(n,q)) = \langle -1_n \rangle$;
7. $\mathrm{Sp}(n,q)' = \mathrm{Sp}(n,q)$;
8. $\mathrm{Sp}(n,q)/\langle -1_n \rangle$ *is simple.*

Proof: Assertion (1) is [**Hup67**, p.220, Satz 9.13 b] or [**KL90**, Prop. 2.4.2], and (2) is [**Hup67**, p.224, Satz 9.19] For proving (3), we let $g := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\mathrm{SL}(n,q)$. By

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^t \cdot \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} -c & -d \\ a & b \end{smallmatrix}\right) = \begin{pmatrix} 0 & -(ad-bc) \\ ad-bc & 0 \end{pmatrix} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),$$

we have $g \in \mathrm{Sp}(2,q)$. Thus $\mathrm{SL}(2,q) \subseteq \mathrm{Sp}(2,q)$. The converse inclusion is given by (2). Assertion (4) is proved in [**Hup67**, p.227, Satz 9.21].

Next we show (5). Let $g \in \mathrm{GL}(n,q)$, and let $\varphi \in \mathrm{Aut}\,\mathrm{GF}(q)$ such that $g \cdot \varphi$ centralizes all elements in $\mathrm{Sp}(n,q)$. For a primitive element $w \in \mathrm{GF}(q)$, we consider $s := \mathrm{diag}(w, w^{-1}, 1, \dots, 1)$ in $\mathrm{Sp}(n,q)$. Now $s^g = s^{(\varphi^{-1})}$ yields that φ is trivial. Thus we have

$$C_{\mathrm{GL}(n,q)\cdot \mathrm{Aut}\,\mathrm{GF}(q)}(\mathrm{Sp}(n,q)) \subseteq \mathrm{GL}(n,q).$$

Since $C_{\mathrm{GL}(n,q)}(\mathrm{Sp}(n,q)) = \{a * 1_n \mid a \in \mathrm{GF}(q)^*\}$ by [**KL90**, p. 51, (2.10.2)], we then have (5).

Now (6) follows immediately from (5). Finally (7) and (8) are [**Hup67**, p.224, Satz 9.20, p.227 Hauptsatz 9.22]. □

9. Properties of orthogonal groups

Let V be a vector space over a finite field F with a non-degenerate quadratic form Q. For vectors $v, w \in V$, let $(v,w) := Q(v+w) - Q(v) - Q(w)$ be the bilinear form corresponding to Q (cf. Section 2). For $v \in V$ such that $Q(v) \neq 0$, we define the *reflection in* v (cf. [**KL90**, p. 29, (2.5.7)]) by

$$r_v : V \to V,\ x \mapsto x - \frac{(v,x)}{Q(v)}v. \tag{A.41}$$

We note that $r_v \in I(V,F,Q)$, $\det r_v = -1$, and that r_v is an involution. By [**KL90**, Prop. 2.5.6], we have $I(V,F,Q) = \langle\{r_v \mid Q(v) \neq 0\}\rangle$. Hence we may define the *spinor norm* θ as a map from G to $F^*/(F^*)^2$ given by

$$\theta(\prod_{i=1}^{k} v_i) = \prod_{i=1}^{k}(v_i, v_i) \cdot (F^*)^2.$$

By [**Asc86**, 22.11], θ is well-defined and a homomorphism.

Proposition A.14. *Let V be a vector space of dimension at least 5 over a finite field F of odd characteristic, and let Q be a non-degenerate quadratic form on V over F. We write $O := I(V,F,Q)$, $S := S(V,F,Q)$, and $\Omega := \Omega(V,F,Q)$. Let G be a group such that $\Omega \subseteq G \subseteq O$. Then we have:*

1. *$Z(O) = \langle\alpha\rangle$ for $\alpha : V \to V$, $x \mapsto -x$;*
2. *$\Omega = \mathrm{Ker}(\theta) \cap S$;*
3. *$|O : S| = 2$ and $|S : \Omega| = 2$;*
4. *Ω has an elementary abelian complement in O;*
5. *$N \subseteq F^*$ or $\Omega \subseteq N$ for all normal subgroups N of G;*
6. *$Z(G) = G \cap F^*$ and $G' = \Omega$.*

Proof: Item (1) is straightforward by considering the isometries of V that commute with all reflections r_v for $v \in V$ as defined above. Item (2) is part of [**Asc86**, p.102, Exercise 6.1]. Since the determinant of an element in O is 1 or -1, the homomorphism theorem yields the first part of (3). We will prove the second together with (4). Since V has dimension at least 5, there exists a basis B of V with distinct vectors $e_1, e_2, f_1, f_2 \in B$ such that $Q(e_i) = Q(f_i) = 0$ and $(e_i, f_i) = \delta_{ij}$ for all $i, j \in \{1,2\}$ by [**KL90**, Prop. 2.5.3]. Let $k \in F^*$ be not a square, and let $v = e_1 + f_1, w = ke_2 + f_2$. Since v and w are orthogonal by definition, the reflections r_v and r_w commute. Hence

$$H := \langle r_v, r_w\rangle \text{ is an elementary abelian group of order 4.} \tag{A.42}$$

Now we will prove

$$H \cap \Omega = \{1\}. \tag{A.43}$$

The elements of H are $1, r_v, r_w$, and $r_v \cdot r_w$. By $\det r_v = \det r_w = -1$, we have $r_v, r_w \in O \setminus S$ and $r_v \cdot r_w \in S$. We compute

$$\theta(r_v \cdot r_w) = (v, v) \cdot (w, w) \cdot (F^*)^2 = 2 \cdot 2k \cdot (F^*)^2.$$

Since k is not a square, this yields $r_v \cdot r_w \notin \Omega$ by (2). Hence we have (A.43) and $|S : (S \cap \mathrm{Ker}(\theta))| \geq 2$. By the homomorphism theorem, we have $|S : (S \cap \mathrm{Ker}(\theta))| \leq 2$. Together with (2), we then obtain $|S : \Omega| = 2$. This completes the proof of (3). Now $O = \Omega \cdot H$ follows from (A.42) and (3). Thus (4) is proved. Assertion (5) is [**Die48**, p. 34, Proposition 13]. For proving (6), we suppose $Z(G) \neq G \cap F^*$. Then (5) yields that $\Omega \subseteq Z(G)$ and that $\Omega/(\Omega \cap F^*)$ is an abelian, simple group. This contradicts that $\Omega/(\Omega \cap F^*)$ has not prime order by the formulae for $|\Omega|$ obtained from Lemmas A.15, A.16, A.17. Hence we have $Z(G) = G \cap F^*$. Next we suppose $G' \neq \Omega$. Since $G' \subseteq \Omega$, assertion (5) yields that $G' \subseteq F^*$. Furthermore, by (5), $\Omega/(\Omega \cap F^*)$ is an abelian, simple group, which yields a contradiction as above. Hence we have $G' = \Omega$. The proof of the proposition is complete. □

We note that, by Proposition A.14 (3), the index of Ω in S is 2. Under the assumptions of this proposition, $I(V, F, Q)'$ is thus equal to the group $\Omega(V, F, Q)$ as defined in [**KL90**] (see the related remark in Section 3).

We will now present matrix representations of the orthogonal groups. Let V be a vector space of dimension n over the field $\mathrm{GF}(q)$ with a non-degenerate quadratic form Q and the associated bilinear form $\mathbf{f}_Q$ (see Section 2).

First we assume that q and n are odd. By [**Hup67**, p.237, Satz 10.9] or by [**KL90**, Prop. 2.5.3 (iii)], there is a basis B such that h_B is an isomorphism from $I(V, F, Q)$ to

$$\mathrm{O}^\circ(n, q) := \{x \in \mathrm{GL}(n, q) \mid x^t \cdot a^\circ \cdot x = a^\circ\}$$

with

$$a^\circ := \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & \ddots & & & \\ & & & 0 & 1 & \\ & & & 1 & 0 & \\ & & & & & 1 \end{pmatrix}.$$

For q odd and n even, there are two non-equivalent quadratic forms, denoted Q^+ and Q^-. We write v_B to denote the coordinates of a vector $v \in V$ with respect to a basis B. Let $\varepsilon \in \{+, -\}$. By [**Hup67**, p.237, Satz 10.9] (or by [**KL90**, Prop. 2.5.3 (i),(ii)] with some manipulations), there are bases B^+, B^- of V such that

(A.44) $$f_{Q^\varepsilon}(v, w) = v_{B^\varepsilon}^t \cdot a^\varepsilon \cdot w_{B^\varepsilon} \text{ for all } v, w \in V$$

with

$$a^+ := \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{pmatrix} \text{ and } a^- := \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & \ddots & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 0 & & \\ & & & & & 1 & 0 \\ & & & & & 0 & -k \end{pmatrix}$$

for a fixed element $k \in \mathrm{GF}(q)$ such that k is not a square. Corresponding to the two non-equivalent quadratic forms for $\varepsilon \in \{+,-\}$, we then obtain two non-isomorphic matrix groups, denoted

$$\mathrm{O}^\varepsilon(n,q) := \{x \in \mathrm{GL}(n,q) \mid x^t \cdot a^\varepsilon \cdot x = a^\varepsilon\}.$$

Let $\varepsilon \in \{\circ,+,-\}$. The elements of $\mathrm{O}^\varepsilon(n,q)$ have determinant 1 or -1; the elements of determinant 1 form a subgroup of $\mathrm{O}^\varepsilon(n,q)$, which is denoted $\mathrm{SO}^\epsilon(n,q)$. Let $\Omega^\varepsilon(n,q)$ denote the derived subgroup of $\mathrm{O}^\varepsilon(n,q)$.

Lemma A.15. *Let n be an odd natural number with $n \geq 3$, and let q be an odd prime power such that $(n,q) \neq (3,3)$. Then we have:*

(1) $|\mathrm{O}^\circ(n,q)| = 2q^{(n-1)^2/4} \prod_{i=1}^{(n-1)/2}(q^{2i}-1)$;
(2) $\mathrm{O}^\circ(n,q) = \mathrm{SO}^\circ(n,q) \cdot \langle -1 \rangle$ *is a direct product.*

Proof: For (1) see [**KL90**, Prop. 2.5.5]. Item (2) follows immediately from Proposition A.14 (3) since $-1_n \notin \mathrm{SO}^\circ(n,q)$. □

Lemma A.16. *Let n be an even natural number with $n \geq 6$, and let q be an odd prime power. Then we have:*

(1) $|\mathrm{O}^+(n,q)| = 2q^{n(n-2)/4} \prod_{i=1}^{n/2}(q^{2i}-1)$;
(2) $-1_n \in \Omega^+(n,q)$ *if and only if* $n(q-1)/4$ *is even;*

Lemma A.17. *Let n be an even natural number with $n \geq 4$, and let q be an odd prime power. Then we have:*

(1) $|\mathrm{O}^-(n,q)| = 2q^{n(n-2)/4}(q^{n/2}+1) \cdot \prod_{i=1}^{n/2-1}(q^{2i}-1)$;
(2) $-1_n \in \Omega^-(n,q)$ *if and only if* $n(q-1)/4$ *is odd;*

Proof of Lemma A.16 and A.17: Item (1) is in [**KL90**, Prop. 2.5.5], and (2) follows from [**KL90**, Prop. 2.5.13]. □

Lemma A.18. *Let V be a vector space of dimension at least 5 over a finite field F of odd characteristic, and let Q be a non-degenerate quadratic form on V. Then $I(V,F,Q)$ has exactly one normal subgroup of index that is characteristic.*

Proof: We write $O := I(V, F, Q)$, $S := S(V, F, Q)$, and $\Omega := \Omega(V, F, Q)$. By Proposition A.14, the factor O/Ω is an elementary abelian group of order 4. Hence O has 3 normal subgroups of index 2. The result is proved by establishing the following:

(1) There exists a normal subgroup N of index 2 in O that is invariant under $\operatorname{Aut} O$;

(2) There exists a normal subgroup H of index 2 in O that is not invariant under $\operatorname{Aut} O$.

First we will show (1) under the assumption $\Omega \cap Z(O) = \{1\}$. Since $|Z(O)| = 2$ by Proposition A.14 (1), we then have that $N := \Omega \cdot Z(O)$ has index 2 in O. Proposition A.14 (6) yields $O' = \Omega$. As the product of 2 characteristic subgroups, N is characteristic in O.

Next we assume $\Omega \cap Z(O) \neq \{1\}$, that is $Z(O) \subseteq \Omega$. We will show that $N := S$ is characteristic in O by using the description of automorphisms of O in [**Die51**, p.51, Theorem 15]. By this result, all automorphisms of O are of the form

$$\alpha : O \to O,\ x \mapsto \rho(x) \cdot x^a,$$

where ρ is some endomorphism from O to $Z(O)$ and $a \in A(V, F, Q)$ is some semilinear transformation of E. Since S is normal in $A(V, F, Q)$ and $Z(O) \subseteq S$ by assumption, we then obtain that $\alpha(S) \subseteq S$ for all $\alpha \in \operatorname{Aut} O$. The proof of (1) is complete.

For proving (2), we first assume that n is odd. Let $i : V \to V$, $x \mapsto -x$. Then we have $Z(O) = \langle i \rangle$ by Proposition A.14 (1). Since $Z(O) \not\subseteq \Omega$, Proposition A.14 (4) yields that $\langle -1_n \rangle$ has a direct complement H in O. By Proposition A.14 (3), Ω has index 2 in H. Let $h \in H \setminus \Omega$. We define an endomorphism ρ from O to $Z(O)$ by

$$\rho(h) = i \text{ and } \operatorname{Ker}(\rho) = \Omega \cdot \langle i \rangle.$$

Then the normal subgroup H of O is not invariant under ρ. By $\rho(O) \subseteq Z(O)$, the map

$$\alpha : O \to O,\ x \mapsto \rho(x) \cdot x,$$

is an endomorphism of O. Since $\rho(O) \subseteq \operatorname{Ker}(\rho)$, we also have that α is bijective. Hence α is an automorphism of O that does not fix H because $\rho(H) \not\subseteq H$. This proves the result for odd n.

Next we assume that n is even. Let w be primitive element in F. As mentioned above, there are 2 non-equivalent quadratic forms. First we consider the case that $\varepsilon = +$. Let $B^+ = \{e_1, f_1, \ldots, e_{n/2}, f_{n/2}\}$ be the basis of V mentioned in (A.44). We define a linear map δ on V by

$$\delta(e_i) = we_i,\ \delta(f_i) = f_i \text{ for all } i \in \{1, \ldots, n/2\}.$$

Let $d := h_{B^+}(\delta)$. Then $d = \operatorname{diag}(w, 1, \dots, w, 1)$, and we have $d^t \cdot a^+ d = w * a^+$. We note that $d \notin \mathrm{O}^+(n,q)$ and hence $\delta \notin O$. Still we have $\mathrm{O}^+(n,q)^d = \mathrm{O}^+(n,q)$ and $O^\delta = O$. We may now define

$$\alpha : O \to O,\ x \mapsto x^\delta.$$

Obviously α is an automorphism of O.

For $\varepsilon = -$, the construction of an appropriate automorphism of O is a bit tedious. We start by constructing an element $d \in \mathrm{GL}(n,q)$ that normalizes $O^-(n,q)$. Let $k \in \mathrm{GF}(q)^*$ be the fixed non-square used in the definition of a^- and $\mathrm{O}^-(n,q)$ above. Let $r, s \in \mathrm{GF}(q)$ such that $r^2 - s^2k = w$. The existence of such elements can be seen as follows: If $-k$ is not a square, then there exists $s \in GF(q)$ such that $-s^2k = w$. We may choose $r = 0$. If $-k$ is a square, then such r, s exist since each element of $\mathrm{GF}(q)$ can be written as sum of 2 squares [**Hup67**, p.237, Hilfssatz 10.6]. We compute

$$\begin{pmatrix} r & sk \\ s & r \end{pmatrix}^t \cdot \begin{pmatrix} 1 & 0 \\ 0 & -k \end{pmatrix} \cdot \begin{pmatrix} r & sk \\ s & r \end{pmatrix} = \begin{pmatrix} r & s \\ sk & r \end{pmatrix} \cdot \begin{pmatrix} r & sk \\ -sk & -rk \end{pmatrix} = \begin{pmatrix} r^2-s^2k & 0 \\ 0 & s^2k^2-r^2k \end{pmatrix} = w * \begin{pmatrix} 1 & 0 \\ 0 & -k \end{pmatrix}.$$

We let

$$d := \begin{pmatrix} w &&&&&& \\ & 1 &&&&& \\ && \ddots &&&& \\ &&& w &&& \\ &&&& 1 && \\ &&&&& r & sk \\ &&&&& s & r \end{pmatrix}.$$

Then we have $d^t \cdot a^- d = w * a^-$, and consequently d normalizes $\mathrm{O}^-(n,q)$. Let $B^- = \{e_1, f_1, \dots, e_{n/2}, f_{n/2}\}$ be the basis of V mentioned in (A.44). We define a linear map δ on V by

$$\delta(e_i) = we_i,\ \delta(f_i) = f_i \text{ for all } i \in \{1, \dots, n/2 - 1\},$$

and $\delta(e_{n/2}) = re_{n/2} + sf_{n/2}, \delta(f_{n/2}) = ske_{n/2} + rf_{n/2}$. Then δ normalizes O. We have an automorphism α of O given by

$$\alpha : O \to O,\ x \mapsto x^\delta.$$

We will now show that α defined according to $\varepsilon = +$ or $\varepsilon = -$ is not in $I(O)$. Let $B := B^\varepsilon$, and let $h \in O$ be defined by

$$h(e_1) = f_1, h(f_1) = e_1 \text{ and } h(b) = b \text{ for all } b \in B \setminus \{e_1, f_1\}.$$

Then $\det h = -1$. Hence $H := \Omega \cdot \langle h \rangle$ is a subgroup of index 2 in O, and we have $H \neq S$. In order to show $\alpha(H) \nsubseteq H$, we consider h^δ. We have

$$h^\delta(e_1) = w^{-1}f_1, h^\delta(f_1) = we_1, \text{ and } h(b) = b \text{ for all } b \in B \setminus \{e_1, f_1\}.$$

Now $g := h^{-1} \cdot h^{\delta}$ satisfies

$$g(e_1) = w^{-1}e_1, g(f_1) = wf_1, \text{ and } g(b) = b \text{ for all } b \in B \setminus \{e_1, f_1\}.$$

Hence we have $\det g = 1$ and $g \in S$. We proceed to show $g \in S \setminus H$, that is, we show $g \notin \Omega$ by using the characterization of Ω as kernel of the spinor norm (see Proposition A.14 (2)). For this, we need a representation of g as product of reflections (cf. (A.41)).

For $u, v \in V$, we let (u, v) denote the bilinear form corresponding to the quadratic form Q on V. Since $n \geq 6$ by assumption, we have $(e_1, e_1) = (f_1, f_1) = 0$ and $(e_1, f_1) = 1$ by the definition of a^+, a^-. For $t \in \mathrm{GF}(q)^*$ and $v := te_1 + f_1$, we now consider the reflection

$$r_v : V \to V, \ x \mapsto x - \frac{(v, x)}{Q(v)} v.$$

Since the characteristic of F is odd by assumption, we have $Q(v) = \frac{1}{2}(v, v)$. We compute

(A.45)

$$Q(te_1 + f_1) = \frac{1}{2}[(te_1, te_1) + (te_1, f_1) + (f_1, te_1) + (f_1, f_1)] = \frac{1}{2} \cdot 2 \cdot t(e_1, f_1) = t.$$

Here we used that the bilinear form is symmetric. Now we find that

$$\begin{aligned} r_v(e_1) &= e_1 - \tfrac{1}{t}(te_1 + f_1) = -t^{-1} f_1, \\ r_v(f_1) &= f_1 - \tfrac{t}{t}(te_1 + f_1) = -te_1, \\ r_v(b) &= b \text{ for all } b \in B \setminus \{e_1, f_1\}. \end{aligned}$$

Let $v_1 := e_1 + f_1$, and let $v_2 := we_1 + f_1$. By comparing the images of the elements of B, we obtain $g = r_{v_1} \cdot r_{v_2}$. Then the spinor norm of g is

$$\theta(g) = (v_1, v_1) \cdot (v_2, v_2) \cdot (F^*)^2.$$

By (A.45), we have $(v_1, v_1) = 2$ and $(v_2, v_2) = 2w$. Hence $\theta(g) = w \cdot (F^*)^2$, and $g \notin \mathrm{Ker}(\theta)$ since w is a primitive element in a field of odd characteristic, and hence w is not a square. Thus we have $g \in S \setminus \Omega$ by Proposition A.14 (2). In particular, $g = h^{-1} \cdot h^{\delta}$ is not contained in H, which yields $h^{\delta} \notin H$. Hence the normal subgroup H of O is not invariant under the automorphism α of O. This proves (2). Thus the lemma is proved. □

Until now we only considered orthogonal groups for fields in odd characteristic q. We will now turn our attention to groups $I(V, F, Q)$ for which $|F|$ is even.

Lemma A.19. *Let V be a vector space of dimension at least 6 over a finite field F of even characteristic, and let Q be a non-degenerate quadratic form on V over F. We write $O := I(V, F, Q)$, $S := S(V, F, Q)$, and $\Omega := \Omega(V, F, Q)$. Then we have:*

(1) $\dim_F V$ *is even;*

(2) *O is centerless;*
(3) *$S = O$ and $|O : \Omega| = 2$;*
(4) *Ω is non-abelian simple.*

Proof: Item (1) is [**KL90**, p. 26, Proposition 2.5.1], and the first part of (3) is [**KL90**, p. 31, (2.5.11)]. The second part of (3) follows from [**Die48**, p.45, Proposition 15]. A straightforward investigation of the isometries of V that commute with all reflections r_v for $v \in V$ yields (2). Finally, we have (4) by [**Asc86**, p.222, (43.12) (4)]. □

Let V be a vector space of even dimension n over the field F of even characteristic q. We note that, by Lemma A.19 (3), the index of Ω in S is 2. For $\dim_F V \geq 6$, we then have that $I(V, F, Q)'$ is equal to $\Omega(V, F, Q)$ as defined in [**KL90**]. We have already shown this equality for F with odd characteristic and $\dim_F V \geq 5$ (see the related remark in Section 3).

We also note that there exist 2 non-equivalent quadratic forms on V. The orders of the corresponding orthogonal groups are given by the formulae in Lemma A.16, A.17, respectively (See [**KL90**, Prop. 2.5.5]).

APPENDIX B

Frobenius groups

We collect the properties of Frobenius groups that are used in Chapter 5.

1. Definitions and general results

Let G be a group with a subgroup H such that $\{1\} < H < G$. Then we say that H is a *Frobenius complement in G* if

$$H \cap H^g = \{1\} \text{ for all } g \in G \setminus H. \tag{B.1}$$

More general, we call a group H is a *Frobenius complement* if there exists a group G and an embedding φ from H into G such that $\varphi(H)$ is a Frobenius complement in G.

A group G is a *Frobenius group* if there is a subgroup H of G with $\{1\} < H < G$ that satisfies (B.1).

Theorem B.1 (Frobenius). *Let G be a finite group, and let H be a Frobenius complement in G. Then $N := G \setminus \bigcup_{x\in G}(H \setminus \{1\})^x$ is a normal subgroup of G such that $G = NH$ and $N \cap H = \{1\}$.*

Proof: [**Rob96**, 8.5.5]. □

Let H be a Frobenius complement in the finite group G. Then

$$N := G \setminus \bigcup_{x\in G}(H \setminus \{1\})^x$$

is called the *Frobenius kernel* of G.

Lemma B.2 ([**Hup67**, p. 497, Satz 8.3]). *Let G be a finite Frobenius group with kernel N and complement H. Then $|H|$ divides $|N| - 1$.*

Lemma B.3 ([**Hup67**, p. 506, Satz 8.18]). *Let G be a finite Frobenius group with kernel N and complement H. We assume that $|H|$ is even. Then we have:*

1. *There is exactly one involution in H, say i. We have $x^i = x^{-1}$ for all $x \in N$.*
2. *N is abelian.*

Theorem B.4 ([**Rob96**, 10.5.6]). *Let G be a finite Frobenius group with kernel N and complement H. Then we have:*

1. (Thompson). *N is nilpotent.*

(2) (Burnside). *The Sylow p-subgroups of H are cyclic for odd p and cyclic or generalized quaternion groups for $p = 2$.*

2. The structure of Frobenius complements

The groups all of whose Sylow subgroups are cyclic are characterized as the semidirect products of cyclic groups of coprime order in the following theorem. In particular, these groups are metacyclic. We note that not all of the groups described in Theorem B.5 are Frobenius complements. See the remark below Theorem B.6.

THEOREM B.5 ([**Hup67**, p.420, Satz 2.11]). *Let G be a finite group such that all Sylow subgroups of G are cyclic. Then there are $m, n, r \in \mathbb{N}$ with* $\gcd(m, n(r-1)) = 1$ *and* $m | r^n - 1$ *such that*

(1) $G \cong \langle a, b \mid a^m = b^n = 1, a^b = a^r \rangle$*;*
(2) G' *is cyclic of order* m*, and* G/G' *is cyclic of order* n*.*

By Theorem B.4 (2), all abelian subgroups of a Frobenius complement are cyclic. The next result provides presentations for all such groups that are solvable.

THEOREM B.6 ([**Wol67**, 6.1.11]). *Let G be a finite solvable group. Then every abelian subgroup of G is cyclic if and only if G has one of the following four presentations:*

Type	*Generators*	*Relations*	*Conditions*
I	a, b	$a^m = b^n = 1$, $a^b = a^r$	$\gcd(m, n(r-1)) = 1$, $r^n \equiv 1 \bmod m$
II	a, b, q	*as in* I*; also* $b^{n/2} = q^2$, $a^q = a^k$, $b^q = b^l$	*as in* I*; also* $n = 2^t u, t \geq 2, u$ *odd,* $l \equiv -1 \bmod 2^t$, $l^2 \equiv 1 \bmod u$, $r^{l-1} \equiv k^2 \equiv 1 \bmod m$
III	a, b, p, q	*as in* I*; also* $p^4 = 1, p^2 = q^2$, $p^q = p^{-1}$, $p^a = p, q^a = q$, $p^b = q, q^b = pq$	*as in* I*; also* m, n *odd,* $n \equiv 0 \bmod 3$
IV	a, b, p, q, z	*as in* III*; also* $p^2 = z^2, p^z = qp$, $q^z = q^{-1}$, $a^z = a^k, b^z = b^l$	*as in* III*; also* $r^{l-1} \equiv k^2 \equiv 1 \bmod m$, $l^2 \equiv 1 \bmod n$, $l \equiv 2 \bmod 3$

We assume that G satisfies one of four presentations given in Theorem B.6 with fixed parameter m, r, n. Let d be the smallest natural number such that $r^d \equiv 1 \bmod m$. Then G is a Frobenius complement if and only if n/d is divisible by all prime divisors of d (see [**Wol67**, 6.1.11]).

We note that the groups of type I are exactly the groups characterized in Theorem B.5.

The structure of non-solvable Frobenius complements can be described as follows.

THEOREM B.7 ([**Pas68**, Theorem 18.6], [**Wol67**, 6.3.1]). *Let G be a non-solvable Frobenius complement. Then G has a normal subgroup H with $|G : H| \leq 2$ such that H is isomorphic to the direct product of* $\mathrm{SL}(2,5)$ *and a group M with* $\gcd(|M|, 30) = 1$ *all of whose Sylow subgroups are cyclic.*

For completeness, we add yet another classification of Frobenius complements as certain extensions of metacyclic groups.

THEOREM B.8 ([**Bro01**, Theorem 1.4]). *Every Frobenius complement G has a unique normal subgroup N such that all Sylow subgroups of N are cyclic and G/N is isomorphic to one of the following* 6 *groups:*

$$1, \mathbb{Z}_2 \times \mathbb{Z}_2, A_4, S_4, A_5, S_5.$$

APPENDIX C

Group rings and modules

We recall and develop results on group rings $\mathbb{Z}_e[G]$ to the extent that is necessary for dealing with Frobenius groups with abelian kernel in Chapter 5.

1. Definitions

Let R be a ring with 1, let $(M, +)$ be an abelian group, and let $*$ be a function from $R \times M$ to M that maps (r, m) to $r * m$ such that for all $r, s \in R$, for all $x, y \in M$ the following are satisfied:

(1) $r * (x + y) = r * x + r * y$;
(2) $(r + s) * x = r * x + s * x$;
(3) $(rs) * x = r * (s * x)$;
(4) $1 * x = x$.

Then M is an *R-module*. We note that the ring R itself can be considered as an R-module by

$$r * x = rx \text{ for all } r, x \in R.$$

To make notation easier, in the following, we will write rm instead of $r * m$ for $r \in R$ and $m \in M$ where M is an R-module.

We say that a non-trivial R-module M is *simple* if $\{0\}$ and M are the only R-submodules of M. Let U, V be submodules of an R-module M. If $U \cap V = \{0\}$, then we write $U \dot{+} V$ for $U + V$ and say that the sum is *direct*. We say that M is *indecomposable* if $M = U \dot{+} V$ yields $U = \{0\}$ or $V = \{0\}$. The *annihilator* of an R-module M is defined as the set

$$\operatorname{Ann}_R(M) := \{r \in R \mid rM = \{0\}\}.$$

For a ring R and a finite group G, we consider the set of formal sums, $R[G] := \{\sum_{g \in G} a_g g \mid a_g \in R\}$. For elements of $R[G]$, we define

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g := \sum_{g \in G} (a_g + b_g) g,$$

$$\sum_{g \in G} a_g g \cdot \sum_{g \in G} b_g g := \sum_{g \in G} (\sum_{xy = g} a_x b_y) g.$$

Then $(R[G], +, \cdot)$ is a ring called the *group ring* of G with coefficients from R.

2. The structure of $\mathbb{Z}_e[G]$

Convention: Throughout this section, G is a finite group, e is a natural number (not necessarily prime) such that $\gcd(e, |G|) = 1$, and $R := \mathbb{Z}_e[G]$.

In the following we will adjust some ideas that have been used for investigating $F[G]$-modules (F a field) in [**Isa94**, Chapter 1] to the case of $\mathbb{Z}_e[G]$-modules.

Lemma C.1 (Maschke). *Let V be a finite R-module, let N be an R-submodule of V, and let H be subgroup of V such that $V = N + H$ and $N \cap H = \{0\}$. Then there exists an R-submodule L of V such that $V = N \dotplus L$.*

Proof: [**Hup67**, p.122, Satz 17.6] □

Lemma C.2. *Let N be a finite, indecomposable R-module. Then there exists a prime p, and there exist integers k, d such that the following hold:*

1. *N is isomorphic to $(\mathbb{Z}_{p^k})^d$ as a group;*
2. *$N = Rn$ for all $n \in N \setminus pN$;*
3. *N is isomorphic to some direct summand of R/p^kR as an R-module;*
4. *For all R-submodules U of N there is $l \in \mathbb{N}$ such that $U = p^lN$;*
5. *For all $l \in \{0, \ldots, k-1\}$ the R-modules N/pN and $p^lN/p^{l+1}N$ are isomorphic and simple.*

Proof: Let N be a finite, indecomposable R-module. Since N is the direct sum of its Sylow subgroups, which are R-submodules as well, N is a p-group. Let $k \in \mathbb{N}$ such that $\exp N = p^k$. From Lemma C.1, we obtain that $N = U \dotplus V$ for some R-submodules U, V of N with $U \cong (\mathbb{Z}_{p^k})^d$ for some $d \in \mathbb{N}$ and $\exp V < p^k$ (cf. [**Hup67**, p.125, Aufgabe 68], a full proof is given in [**May98**, Lemma 6.4]). Since N is indecomposable, we have $V = \{0\}$ and (1) is proved. For the rest of the proof, we let p, k, d be fixed.

Next we show (2). For $n \in N \setminus pN$, we consider the R-module homomorphism

$$h : R \to N, r \mapsto rn.$$

Then $h(R) = Rn$ is an R-module of exponent p^k. As in the proof of (1), we have R-submodules U, V of Rn such that $U \cong (\mathbb{Z}_{p^k})^f$ for some $f \in \mathbb{N}$, $\exp V < p^k$, and $Rn = U \dotplus V$. Every subgroup isomorphic to $(\mathbb{Z}_{p^k})^f$ has a complement in $(\mathbb{Z}_{p^k})^d$ [**Fuc60**, p. 53, Exercise 23], [**Sze49**]. Hence there exists a complement for U in N, and we have an R-submodule L such that $N = U \dotplus L$ by Lemma C.1. Thus $L = \{0\}$ and $N = Rn$. Item (2) is proved.

For (3), we consider h as defined above. Let $K := \operatorname{Ker}(h)$. We have $p^kR \subseteq K$. So K/p^kR is a subgroup of R/p^kR. From $R/K \cong (\mathbb{Z}_{p^k})^d$ and $R/p^kR \cong (\mathbb{Z}_{p^k})^{|G|}$ we obtain $K/p^kR \cong (\mathbb{Z}_{p^k})^{|G|-d}$. Hence K/p^kR has a complement in R/p^kR by [**Fuc60**, p. 53, exercise 23]. By Lemma C.1, there exists an R-submodule L

of R/p^kR such that $R/p^kR = K/p^kR \dotplus L$. Then R/K is isomorphic to L by the homomorphism theorem. Item (3) is proved.

Next we show (4). Let U be a non-trivial R-submodule of N. Then we have $l \in \mathbb{N}_0$ such that $p^{l+1}N \subset U \subseteq p^lN$. Let $n \in N \setminus pN$ such that $p^ln \in U \setminus p^{l+1}N$. By (2), we obtain $R(p^ln) = p^lRn = p^lN \subseteq U$. Hence $U = p^lN$.

It remains to prove (5). For $l \in \{1, \dots, k-1\}$, the map

$$h : N/pN \to p^lN/p^{l+1}N,\ x + pN \mapsto p^lx + p^{l+1}N.$$

is well-defined and an R-module isomorphism. The module N/pN is simple since $R(n + pN) = N/pN$ for all $n \in N \setminus pN$ by (2). Hence $p^lN/p^{l+1}N$ is simple. The lemma is proved. □

By Lemma C.2, a finite indecomposable R-module is simple if and only if it has prime exponent. Furthermore each finite indecomposable R-module N has a unique minimal R-submodule, which we will denote by $N_{\min}$.

For an R-module V and a simple R-module M, we define

$$M(V) := \sum\{N \leq V \mid N \text{ indecomposable}, N_{\min} \cong M\}.$$

Here isomorphism is understood as isomorphism between R-modules.

Lemma C.3. *Let V be a finite R-module, and let M be a finite simple R-module. Then all minimal R-submodules of $M(V)$ are isomorphic to M.*

Proof: Let U be a minimal R-submodule of $M(V)$, and let l be the smallest positive integer such that there exist indecomposable submodules $N_1, \dots, N_l$ of V with their respective minimal submodules isomorphic to M and $U \subseteq N_1 + \cdots + N_l$. Such an integer l exists by the finiteness of $M(V)$. Let $W := N_1 + \cdots + N_{l-1}$, and let $W := \{0\}$ if $l = 1$. Then $U \not\subseteq W$ and hence $U \cap W = \{0\}$. Since $(W + U)/W$ is a submodule of $(W + N_l)/W$, U can then be embedded into $N_l/(W \cap N_l)$ by the homomorphism theorem. By Lemma C.2, the minimal submodule of $N_l/(W \cap N_l)$ is isomorphic to M. Thus U is isomorphic to M. The lemma is proved. □

Let p be a prime divisor of e. Then pR is an ideal of R, and R/pR is isomorphic to the group ring $\mathbb{Z}_p[G]$. By the next theorem, R/pR is a direct product of simple rings.

Theorem C.4 (Wedderburn). *Let p be a prime divisor of e. We write $\bar{R} := R/pR$. Then there exists $n \in \mathbb{N}$ and there exist simple R-submodules $M_1, \dots, M_n$ of $\bar{R}$ such that the following hold:*

(1) *Every finite simple R-module of exponent p is isomorphic to exactly one of the R-modules $M_1, \dots, M_n$;*
(2) $\bar{R} = M_1(\bar{R}) \dotplus \cdots \dotplus M_n(\bar{R})$*;*
(3) $M_i(\bar{R})$ *is a minimal ideal of $\bar{R}$ for all $i \in \{1, \dots, n\}$;*

(4) *For all* $i \in \{1, \dots, n\}$ *there exists a finite field* F *of characteristic* p *and there exists* $d \in \mathbb{N}$ *such that* $M_i(\bar{R})$ *is isomorphic to the matrix ring* F_d^d.

Proof: By Lemma C.2 (3), every finite simple R-module of exponent p is isomorphic to some R-submodule of $\bar{R}$. Since $\bar{R}$ is finite, the number of isomorphism classes of simple R-modules of exponent p is finite, say n. Let $M_1, \dots, M_n$ be representatives for these isomorphism classes. Then we have (1).

Next we show (2). Clearly $\bar{R}$ is the sum of indecomposable modules. Since each indecomposable module contains a unique minimal submodule by Lemma C.2, we have $\bar{R} = M_1(\bar{R}) + \cdots + M_n(\bar{R})$. By Lemma C.3, this sum is direct.

For proving (3), we let $r \in R$ and consider the map $t : \bar{R} \to \bar{R}, x \mapsto x(r+pR)$. Let M be a minimal R-submodule of $\bar{R}$. Since t is an R-module homomorphism, $t(M)$ is either trivial or isomorphic to M. Then we have $M(\bar{R})(r+pR) \subseteq M(\bar{R})$, and $M(\bar{R})$ is a right ideal. As an R-module, $M(\bar{R})$ is also a left ideal of $\bar{R}$. Hence

$$M_i(\bar{R}) \text{ is an ideal for all } i \in \{1, \dots, n\}. \tag{C.1}$$

Let $i \in \{1, \dots, n\}$. To show that $M_i(\bar{R})$ is minimal, we let I be an ideal of $\bar{R}$ with $I < M_i(\bar{R})$. Then we have an R-submodule L of $M_i(\bar{R})$ such that $L \cong M_i$ and $L \not\subseteq I$. Since L is simple, we have $I \cap L = \{0\}$. So $IL \subseteq I \cap L$ yields $IL = \{0\}$. Consequently I annihilates $M_i(\bar{R})$. From (C.1) and (2) we obtain $IM_j(\bar{R}) = I \cap M_j(\bar{R}) = \{0\}$ for all $j \in \{1, \dots, n\}, j \neq i$. Hence $I = I\bar{R} = \{0\}$ by (2). Thus $M_i(\bar{R})$ is a minimal ideal. Item (3) is proved.

It remains to show (4). Let $i \in \{1, \dots, n\}$. From (2) and (3), we obtain $\operatorname{Ann}_{\bar{R}}(M_i) = \sum_{j=1, j\neq i}^{n} M_j(\bar{R})$. By [**Isa94**, Theorem (1.16)], $\bar{R}/\operatorname{Ann}_{\bar{R}}(M_i)$ is isomorphic to $\operatorname{End}_F(M_i)$ where $F = \operatorname{End}_{\bar{R}}(M_i)$ is a division ring. Consequently $M_i(\bar{R})$ is isomorphic to some $d \times d$ matrix ring over F. Since a finite division ring is a field [**Sco87**, (14.1.4)], we have (4). The theorem is proved. □

Lemma C.5. *Let* V *be a finite* R*-module, let* M *be a simple* R*-submodule of* V *with* $\exp M = p$, *and let* $A := \operatorname{Ann}_R(M)$. *Then there exists* $k \in \mathbb{N}$ *such that the following hold:*

(1) A *is a maximal ideal of* R *and* $pR \subseteq A$;
(2) $\exp M(V) = p^k$ *and* $\operatorname{Ann}_R(M(V)) = A^k$;
(3) $|R : A^k| = |R : A|^k$.

Proof: Since $\exp M = p$, we have $pR \subseteq A$. By Theorem C.4, R/A is isomorphic to $M(R/pR)$, which is a simple ring. Hence A is maximal. We have (1).

For (2), we note that $M(V)$ is a sum of p-groups by Lemma C.2. Hence we have $k \in \mathbb{N}$ such that $\exp M(V) = p^k$. For an indecomposable R-submodule N

of $M(V)$, we show

$$A^l N = p^l N \text{ for all } l \in \mathbb{N}. \tag{C.2}$$

By Lemmas C.2, C.3, N/pN is isomorphic to M. Then $\mathrm{Ann}_R(N/pN) = A$ yields $AN \subseteq pN$. The converse inclusion follows from (1). Now $AN = pN$ yields (C.2).

By $\exp M(V) = p^k$, we have an indecomposable R-submodule L of $M(V)$ with $\exp L = p^k$. From (C.2) we then obtain $\mathrm{Ann}_R(L) = A^k$. Consequently $\mathrm{Ann}_R(M(V)) \subseteq A^k$. The converse inclusion is obviously true. Item (2) is proved.

For (3), we note that

$$|R : A^k| = |R : A| \cdot |A : A^2| \cdots |A^{k-1} : A^k|. \tag{C.3}$$

Let $l \in \{1, \ldots, k-1\}$, and let $A^0 := R$. We consider the map

$$h : A^{l-1}/A^l \to A^l/A^{l+1},\ x + A^l \mapsto px + A^{l+1}.$$

Then h is well-defined and a homomorphism between groups. We shall prove that h is an isomorphism. Let $x \in \mathrm{Ker}(h)$. Then $px \in A^{l+1}$ yields $x(pN) \subseteq p^{l+1}N$ by (C.2). Hence $x \in \mathrm{Ann}_R(pN/p^{l+1}N)$. From (2) we obtain $\mathrm{Ann}_R(pN/p^{l+1}N) = A^l$. Thus h is injective.

To show that h is surjective, we observe that A/pR is a direct sum of simple rings with 1 by Theorem C.4. Then we have $(A/pR)^2 = A/pR$, that is

$$A^2 + pR = A.$$

From this we obtain $A^{l+1} + pA^{l-1} = A^l$. Hence h is surjective. Consequently (3) follows from (C.3). The lemma is proved. □

For an R-module V and for $r \in R$, we define a map $r_V : V \to V$ by $x \mapsto rx$. We give a direct decomposition of V and of $R/\mathrm{Ann}_R(V)$.

Lemma C.6. *Let V be a finite R-module. Then there are pairwise non-isomorphic simple R-modules $M_1, \ldots, M_n$ such that the following hold:*

(1) *$V = M_1(V) \dotplus \cdots \dotplus M_n(V)$;*
(2) *$R/\mathrm{Ann}_R(V) \cong R/\mathrm{Ann}_R(M_1(V)) \times \cdots \times R/\mathrm{Ann}_R(M_n(V))$.*

Proof: Since every module is the sum of indecomposable modules, the Lemmas C.2 and C.3 yield (1). For proving (2), we assume that the summands in the decomposition given in (1) are non-trivial and that $n > 1$. For $i \in \{1, \ldots, n\}$ and $A_i := \mathrm{Ann}_R(M_i)$, we have $k_i \in \mathbb{N}$ such that $\mathrm{Ann}_R(M_i(V)) = A_i^{k_i}$ by Lemma C.5. From (1) we obtain $\mathrm{Ann}_R(V) = \bigcap_{i=1}^n A_i{}^{k_i}$. We consider the ring homomorphism

$$f : R \to R/A_1^{k_1} \times \cdots \times R/A_n^{k_n},\ r \mapsto (r + A_1^{k_1}, \ldots, r + A_n^{k_n}).$$

Then $\mathrm{Ker}(f) = \mathrm{Ann}_R(V)$. We show that f is surjective. Let $i \in \{1, \ldots, n\}$ be fixed. For $j \in \{1, \ldots, n\}, i \neq j$, we let $a_j \in A_j \setminus A_i$. We note that such an element a_j exists since A_i, A_j are distinct maximal ideals in R by Theorem C.4.

Let $s := \prod_{j=1,j\neq i}^{n} a_j^{k_j}$. Then s annihilates $M_j(V)$ for $j \neq i$. Since $a_j M_i = M_i$ for $j \neq i$, we have $sM_i = M_i$. Hence the map s_{M_i} is bijective on the finite module M_i. By Lemma C.3, we have $\operatorname{Ker}(s_{M_i(V)}) = \{0\}$. Thus $s_{M_i(V)}$ is bijective on $M_i(V)$. Some power of $s_{M_i(V)}$ is equal to the identity map $1_{M_i(V)}$. Hence we have

$$(0 + A_1^{k_1}, \ldots, 0 + A_{i-1}^{k_{i-1}}, 1 + A_i^{k_i}, 0 + A_{i+1}^{k_{i+1}}, \ldots, 0 + A_n^{k_n}) \in f(R)$$

for all $i \in \{1, \ldots, n\}$. Consequently f is surjective. By the homomorphism theorem we have (2). The lemma is proved. □

We conclude this section with some relations between R-modules of prime exponent p and $\mathbb{Z}_p[G]$-modules.

Lemma C.7. *Let p be a prime divisor of e, and let $\bar{R} := R/pR$. For R-modules U, V of exponent p, we have the following:*

1. *V is an $\bar{R}$-module by $(r + pR)x = rx$ for all $r \in R, x \in V$;*
2. *$R/\operatorname{Ann}_R(V) \cong \bar{R}/\operatorname{Ann}_{\bar{R}}(V)$;*
3. *V is a simple R-module if and only if V is a simple $\bar{R}$-module;*
4. *U and V are isomorphic as R-modules if and only if U and V are isomorphic as $\bar{R}$-modules.*

Proof: Since $pR \subseteq \operatorname{Ann}_R(V)$, the action of $\bar{R}$ on V is well-defined. Hence V is an $\bar{R}$-module. The proofs of the remaining assertions are straightforward. □

3. Frobenius groups and representations

Let F be a field, and let G a group. For $d \in \mathbb{N}$, let $\operatorname{GL}(d, F)$ denote the group of invertible $d \times d$ matrices with entries in F. Let $\varphi : G \to \operatorname{GL}(d, F)$ be a group homomorphism. Then φ is called a *representation* of G over F of *degree d*. Let $V := F^d$. We define an action of G on V by

$$v^g := \varphi(g)v \text{ for all } g \in G, v \in V. \tag{C.4}$$

Here an $d \times d$ matrix r with entry r_{ij} in row i, column j acts on a vector $v = (v_1, \ldots, v_n)$ by multiplication, $rv := (\sum_{j=1}^{n} r_{1j}v_j, \ldots, \sum_{j=1}^{n} r_{nj}v_j)$. We let $V \cdot_\varphi G$ denote the semidirect product of V and G that is defined by (C.4). We may view V as an $F[G]$-module by

$$(\sum_{g\in G} a_g g) * v := \sum_{g\in G} a_g \varphi(g)v \text{ for all } v \in V.$$

Then we say that V is the $F[G]$-module that is associated to φ.

Conversely, let V be any $F[G]$-module. Then we obtain a representation of G over F from the matrix representations (with respect to a fixed basis) of the linear transformations $g_V : V \to V, x \mapsto g * x$ for $g \in G$.

Representations with isomorphic associated $F[G]$-modules are said to be *equivalent.* A representation of G over F is *irreducible* if its associated $F[G]$-module V is simple.

A representation φ of a group G over the field F is *fixed-point-free* if we have for all $g \in G \setminus \{1\}$ that 1 is not an eigenvalue of $\varphi(g)$. The following connection between fixed-point-free representations and Frobenius groups is quite obvious.

LEMMA C.8. *Let G be a finite group, $|G| > 1$, and let F be a finite field. For a representation φ of G over F of degree d, the following are equivalent:*

(1) *φ is fixed-point-free;*
(2) *$F^d \cdot_\varphi G$ is a Frobenius group with complement G and kernel F^d.*

Proof: Straightforward. □

Fixed-point-free representations have been investigated over the complex numbers in [**Wol67**] and over fields of prime characteristic in [**May00**]. We give the irreducible fixed-point-free representations of Q_8 over $\mathrm{GF}(p)$ in Lemma C.9 and of $\mathrm{SL}(2,3)$ in Lemma C.10.

LEMMA C.9 ([**May98**, cf. Proposition 5.19]). *Let Q_8 be the quaternion group of order* 8*,*

$$Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle.$$

Let p be an odd prime, and let $u, v \in \mathrm{GF}(p)$ such that $u^2 + v^2 = -1$. Then $\rho : Q_8 \to \mathrm{GL}(2,p)$ defined by

$$\rho(a) = \left(\begin{smallmatrix} u & v \\ v & -u \end{smallmatrix} \right), \rho(b) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right)$$

is an irreducible fixed-point-free representation of Q_8. All irreducible fixed-point-free representations of Q_8 over $\mathrm{GF}(p)$ are equivalent to ρ.

We note that every element of $\mathrm{GF}(p)$ is the sum of 2 squares. Hence elements u, v as in the lemma above exist.

Proof of Lemma C.9: It is straightforward to check that ρ is irreducible and fixed-point-free. To prove the uniqueness of ρ, let $R := \mathbb{Z}_p[Q_8]$. We note that p and $|Q_8|$ are relatively prime by assumption. Since Q_8 is not abelian, we have a simple R-submodule M of R such that $R/\mathrm{Ann}_R(M)$ is not a field. Let d be the dimension of M over $\mathbb{Z}_p$. Then we have $d \geq 2$ and $|R/\mathrm{Ann}_R(M)| \geq p^{d^2}$. From $|R| = p^8$ we obtain $d = 2$. Theorem C.4 yields that $R \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times (\mathbb{Z}_p)^2_2$. Hence all simple R-modules whose dimension is greater than 1 are isomorphic to M. Because of this, all irreducible representations of Q_8 whose degree is greater than 1 are equivalent. The representations of Q_8 of degree 1 are not fixed-point-free since they are not injective. Thus all irreducible fixed-point-free representations are equivalent to ρ. □

Lemma C.10 ([**May00**, cf. Proposition 7]). *Let*

$$G = \langle a, b, c \mid a^4 = 1, a^2 = b^2, a^b = a^{-1}, a^c = b, b^c = ab, c^3 = 1 \rangle.$$

Let p be a prime, $p \notin \{2, 3\}$, and let $u, v \in \mathrm{GF}(p)$ such that $u^2 + v^2 = -1$. Then $\tau : G \to \mathrm{GL}(2, p)$ defined by

$$\tau(a) = \left(\begin{smallmatrix} u & v \\ v & -u \end{smallmatrix} \right), \tau(b) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right), \tau(c) = \frac{1}{2} \left(\begin{smallmatrix} -1+u+v & -1-u+v \\ 1-u+v & -1-u-v \end{smallmatrix} \right)$$

is an irreducible fixed-point-free representation of G. All irreducible fixed-point-free representations of G over $\mathrm{GF}(p)$ are equivalent to τ.

Proof: Let F be the algebraic closure of $\mathrm{GF}(p)$. We note that p and $|G| = 24$ are relatively prime by assumption. The squares of the degrees of the non-equivalent irreducible F-representations of $G/Z(G)$ sum up to 12 (see [**Isa94**, Corollary 1.17 (d)]). Certainly none of the representations of G that are lifted from these are fixed-point-free. The sum of the squares of the degrees of the non-equivalent irreducible F-representations that do not have $Z(G)$ in their kernel is 12 as well. One of them is τ. We shall define the others explicitly. Let f be a primitive third root of unity in $\bar{F}$. For $i \in \{1, 2\}$, we define $\tau_i : G \to \mathrm{GL}(2, F)$ such that

$$\tau_i(a) := \tau(a), \tau_i(b) := \tau(b), \text{ and } \tau_i(c) := f^i * \tau(c).$$

The order of $\tau(c)$ is 3 and $\det \tau(c) = 1$. Thus $\tau(c)$ has eigenvalues f, f^2. Consequently the eigenvalues of $\tau_1(c)$ are given by $f^2, 1$; those of $\tau_2(c)$ by $1, f$. Hence τ, τ_1, τ_2 are pairwise non-equivalent. Since $3 \cdot 2^2 = 12$, every irreducible representation φ of G with $Z(G) \nsubseteq \mathrm{Ker}(\varphi)$ is equivalent to τ, τ_1, or τ_2. Neither τ_1 nor τ_2 is fixed-point-free. If an irreducible fixed-point-free representation of G over F exists, then it is equivalent to τ.

It remains to prove that τ is fixed-point-free. We have that $\langle a, b \rangle$ is isomorphic to Q_8 and $\tau|_{\langle a,b \rangle} = \rho$ with ρ as in Lemma C.9. Hence the restriction of τ to $\langle a, b \rangle$ is fixed-point-free. We note that every element of $G \setminus \langle a, b \rangle$ has order 3 or 6. By Sylow's theorem, all elements of order 3 in G are conjugate to c or c^{-1}. Hence $\tau(x)$ has eigenvalues f, f^2 for all $x \in G$ with $\operatorname{ord} x = 3$. Since a^2 is the unique involution in G, all elements of order 6 in G are conjugate to a^2c or a^2c^{-1}. Hence $\tau(x)$ has eigenvalues $-f, -f^2$ for all $x \in G$ with $\operatorname{ord} x = 6$. Thus τ is fixed-point-free. The lemma is proved. □

Bibliography

[ABE$^+$99] E. Aichinger, F. Binder, J. Ecker, P. Mayr, and C. Nöbauer. SONATA - system of near-rings and their applications, package for the group theory system GAP4. Division of Algebra, Johannes Kepler University Linz, Austria, 1999.

[Aic02] E. Aichinger. The polynomial functions on certain semidirect products of groups. *Acta Sci. Math. (Szeged)*, 68:63–81, 2002.

[AM03] E. Aichinger and P. Mayr. Polynomial functions and endomorphism near-rings on certain linear groups. *Communications in Algebra*, 31(11):5627–5651, 2003.

[Asc86] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[AW92] W. A. Adkins and S. H. Weintraub. *Algebra. An approach via module theory.* Springer-Verlag, New York, 1992.

[Bro01] R. Brown. Frobenius groups and classical maximal orders. *Mem. Amer. Math. Soc.*, 151(717):viii+110, 2001.

[Car89] R. W. Carter. *Simple groups of Lie type.* Wiley Classics Library. John Wiley & Sons Inc., New York, 1989. Reprint of the 1972 original, A Wiley-Interscience Publication.

[Die48] J. Dieudonné. *Sur les groupes classiques.* Actualités Sci. Ind., no. 1040 = Publ. Inst. Math. Univ. Strasbourg (N.S.) no. 1 (1945). Hermann et Cie., Paris, 1948.

[Die51] J. Dieudonné. On the automorphisms of the classical groups. With a supplement by Loo-Keng Hua. *Mem. Amer. Math. Soc.,*, 1951(2):vi+122, 1951.

[Eck98] J. Ecker. On the number of polynomial functions on nilpotent groups of class 2. In *Contributions to General Algebra*, volume 10. Verlag Johannes Heyn, Klagenfurt, 1998.

[Eck01] J. Ecker. *Functions on groups. Compatibility vs. Polynomiality.* PhD thesis, Johannes Kepler University Linz, 2001.

[Eck03] J. Ecker. The finite 1-affine complete Frobenius groups. *Abh. Math. Sem. Univ. Hamburg*, 73:229–239, 2003.

[FK95] Y. Fong and K. Kaarli. Unary polynomials on a class of groups. *Acta Sci. Math. (Szeged)*, 61(1-4):139–154, 1995.

[FM81] Y. Fong and J. D. P. Meldrum. The endomorphism near-ring of the symmetric group of degree four. *Tamkang J. Math.*, 12(2):193–203, 1981.

[FM81] Y. Fong and J. D. P. Meldrum. The endomorphism near-rings of the symmetric groups of degree at least five. *J. Austral. Math. Soc. Ser. A*, 30(1):37–49, 1980/81.

[Frö58] A. Fröhlich. The near-ring generated by the inner automorphisms of a finite simple group. *J. London Math. Soc.*, 33:95–107, 1958.

[Fuc60] L. Fuchs. *Abelian groups.* Pergamon Press, New York, 1960.

[GAP02] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. (`http://www.gap-system.org`).

[Hup67] B. Huppert. *Endliche Gruppen. I.* Springer-Verlag, Berlin, 1967.

[Isa94] I. M. Isaacs. *Character theory of finite groups.* Dover Publications Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR **57** #417].

[KL90] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1990.

[Kow91] G. Kowol. Polynomautomorphismen von Gruppen. *Arch. Math. (Basel)*, 57(2):114–121, 1991.

[Kow97] G. Kowol. Near-rings of endomorphisms of finite groups. *Comm. Algebra*, 25(7):2333–2342, 1997.

[LM72] C. G. Lyons and J. J. Malone. Finite dihedral groups and d.g. near rings. I. *Compositio Math.*, 24:305–312, 1972.

[LM73] C. G. Lyons and J. J. Malone. Finite dihedral groups and d.g. near rings. II. *Compositio Math.*, 26:249–259, 1973.

[LN73] H. Lausch and W. Nöbauer. *Algebra of polynomials.* North-Holland, Amsterdam, London; American Elsevier Publishing Company, New York, 1973.

[LP95] C. G. Lyons and G. L. Peterson. Semidirect products of *I-E* groups. *Proc. Amer. Math. Soc.*, 123(8):2353–2356, 1995.

[Mal73] J. J. Malone. Generalised quaternion groups and distributively generated near-rings. *Proc. Edinburgh Math. Soc. (2)*, 18:235–238, 1973.

[May98] P. Mayr. Finite fixed point free automorphism groups. Master's thesis, Johannes Kepler University Linz, December 1998.

[May00] P. Mayr. Fixed-point-free representations over fields of prime characteristic. Reports of the Mathematical Institutes 554, Johannes Kepler University Linz, 2000.

[Mel78] J. D. P. Meldrum. On the structure of morphism near-rings. *Proc. Roy. Soc. Edinburgh Sect. A*, 81(3-4):287–298, 1978.

[Mel79] J. D. P. Meldrum. The endomorphism near-ring of finite general linear groups. *Proc. Roy. Irish Acad. Sect. A*, 79(10):87–96, 1979.

[Mel85] J. D. P. Meldrum. *Near-rings and their links with groups.* Pitman (Advanced Publishing Program), Boston, Mass., 1985.

[MM94] J. J. Malone and G. Mason. ZS-metacyclic groups and their endomorphism near-rings. *Monatsh. Math.*, 118(3-4):249–265, 1994.

[MMT87] R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, lattices, varieties, Volume I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[Pas68] D. Passman. *Permutation groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Pet95] G. L. Peterson. Finite metacyclic *I-E* and *I-A* groups. *Comm. Algebra*, 23(12):4563–4585, 1995.

[Pet96] G. L. Peterson. The semidirect products of finite cyclic groups that are *I-E* groups. *Monatsh. Math.*, 121(3):275–290, 1996.

[Pet99] G. L. Peterson. Split metacyclic p-groups that are *A-E* groups. *Results Math.*, 36(1-2):160–183, 1999.

[Pil83] G. F. Pilz. *Near-rings.* North-Holland Publishing Company – Amsterdam, New York, Oxford, 2nd edition, 1983.

[Rob96] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1996.

[Sco69] S. D. Scott. The arithmetic of polynomial maps over a group and the structure of certain permutational polynomial groups. I. *Monatsh. Math.*, 73:250–267, 1969.

[Sco87] W. R. Scott. *Group theory*. Dover Publications Inc., New York, second edition, 1987.

[ST99] G. Saad and M. J. Thomsen. Endomorphism nearrings: foundations, problems and recent results. *Discrete Math.*, 208/209:507–527, 1999. Combinatorics (Assisi, 1996).

[STS95] G. Saad, M. J. Thomsen, and S. A. Syskin. Endomorphism nearrings on finite groups. A report. In *Near-rings and near-fields (Fredericton, NB, 1993)*, pages 227–238. Kluwer Acad. Publ., Dordrecht, 1995.

[Suz86] M. Suzuki. *Group theory. II*, volume 248 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1986. Translated from the Japanese.

[Sys95] S. A. Syskin. Endomorphisms of projections in finite groups. *Algebra i Logika*, 34(5):550–557, 609, 1995.

[Sze49] T. Szele. Über die direkten Teiler der endlichen Abelschen Gruppen. *Comment. Math. Helv.*, 22:117–124, 1949.

[Wol67] J. A. Wolf. *Spaces of constant curvature*. McGraw-Hill Book Co., New York, 1967.

Index